비밀등급
대외비

정보보호 담당자	정보보호 관리자	정보보호 최고책임자
/	/	/

위험분석 보고서

2021. 01

제니퍼 

목 차

1. 개요

1.1. 목적

본 위험분석보고서는 제니퍼(이하 "회사"라 함)의 업무에 대한 정보보호관리체계 구축 및 운영을 위해서 관련 정보자산들에 대한 위협 및 취약점을 식별하고, 그 위협 및 취약점에 해당하는 위험의 수준을 평가하여 비용 대비 효과적인 정보보호 대책을 수립 및 적용함으로써 위험관리가 지속적으로 구현될 수 있는 토대를 마련하고자 하는 데 그 목적이 있다.

1.2. 수행인력

위험관리 계획에 따라 위험 식별 및 평가를 수행하기 위하여 회사의 정보시스템 운영 업무에 대한 이해도, 경험 및 지식을 보유한 인력이 주체가 되어 위험분석과 관련된 전문 지식을 보유한 외부 전문인력의 지원을 받아 현황 점검 및 위험분석을 수행하였다.

구분	수행 내용	수행 인력
위험관리 방법 및 계획 수립	조직 및 자산 범위 선정 수행 기간, 방법 등 계획 수립	이창준 주임
현황 분석 및 취약점 점검	인터뷰, 현장실사, 문서확인, IT인프라(OS, DB, 네트워크 등) 취약점 점검, 웹 모의해킹	
위험 식별 및 평가	자산분석, 위협분석, 취약성 분석, 위험 시나리오 분석, 위험 식별 및 평가	
보호대책 선정	위험에 대한 DoA 선정, 위험에 대한 보호대책 선정, 보호대책 적용 계획 수립 등	

[표 1] 위험분석 수행인력

1.3. 수행 기간

2021 년 01 월 18 일부터 2021 년 01 월 22 일 까지 현황 점검 및 위험분석을 수행하였다.

구분	수행 내용	수행 일정
위험관리 방법 및 계획 수립	수행조직현황 분석, 취약점진단 대상 및 자산 분석	2021.01.18 ~ 2021.01.19
위험 식별 및 평가	관리적/물리적/기술적 현황분석 (취약점 분석)	2021.01.19 ~ 2021.01.20
	자산분석, 위협분석, 취약성 분석, 위험 식별 및 평가	2021.01.20 ~ 2021.00.21
보호대책 선정	위험에 대한 보호대책 선정, 보호대책 적용 계획 수립 등	2021.01.21 ~ 2021.01.22

[표 2] 위험분석 수행일정

1.4. 수행 대상 및 범위

위험분석 대상은 회사의 정보시스템을 운영·관리하는 서비스 제공을 위한 조직, 시설, IT 인프라 자원(서버, 네트워크, 보안시스템 등) 및 전자정보 등을 대상으로 한다.

위험분석 수행 범위는 보안업무 및 운영, 관리를 위해 기존에 수립되어 있는 정보보호 정책, 지침, 정보보호 계획문서, 정보보호 담당조직, 운영 시스템 등으로 정의하고 정보보호 관리체계 평가 항목에서 정의하고 있는 평가내용을 기반으로 평가를 수행한다.

- ✓ 검토문서 범위: 정보보호 정책서, 보안활동 관련 증적자료 등
- ✓ 정보보호 조직 검토 범위: 정보자산 및 물리적 보안, 운영 조직(서버, DBMS, 보안장비), 정보보호 담당 조직
- ✓ 정보시스템: 웹서비스, 내부 관리용 CS 프로그램 유관 OS, DB, 네트워크, 보안장비, Application 등

1.5. 수행 방법

관리적, 물리적, 기술적 영역에 대한 현황 및 취약점 점검을 위해 인터뷰, 문서심사, 현장실사 및 점검도구를 통해 보안수준을 점검한다.

- ✓ 관리/물리적 영역(이하 "관리적 영역"이라 함): 인터뷰, 문서심사, 현장실사
- ✓ 기술적 영역: 취약점 점검 도구(스크립트 등), 수동 점검(설정 등 수동 확인)

1.6. 용어정리

- ■ 기밀성(Confidentiality)

  정보가 인가되지 않은 개인(Individuals)이나, 처리과정(Processes) 등에 누설되거나 공개되지 않는 속성을 말한다.

- ■ 무결성(Integrity)

  정보가 고의적 또는 우발적으로 변경, 파괴되지 않고 일관성을 유지하는 속성을 말한다.

- ■ 가용성(Availability)

  인가된 사용자가 정보시스템으로부터 필요한 정보를 필요할 때 항상 접근하여 사용이 가능한 속성을 말한다.

- ■ 자산(Assets)

  정보시스템 운영과 관련하여 조직에 가치 있는 모든 것(Entity)을 말한다.

- ■ 위협(Threat)

  정보 및 유형 자산에 피해를 주어 시스템이나 조직에 손실을 유발할 수 있는 잠재적인 요소를 말한다.

- ■ 취약성(Vulnerability)

  위협에 의해 손실을 입을 수 있는 자산의 약점을 말한다.

- ■ 위험(Risk)

  자산의 주변에 존재하는 위협이 자산의 취약성에 영향을 주어 손실을 줄 수 있는 잠재성을 말한다.

■ 대응책(Safeguard)

위험을 감소시키는 행위, 절차 또는 방법을 말한다.

■ 잔여위험(Residual Risk)

대응책이 구현된 후에도 남아있는 위험을 말한다.

■ 영향(Impact)

위험으로 인해 자산에 대한 직간접적 피해를 유발하는 원하지 않는 사건의 결과를 말한다.

■ 위험분석(Risk Analysis)

자산을 식별하고 그 자산에 영향을 주는 위협 및 취약성을 분석하여 위험을 식별하고, 범위를 결정하여 대응책을 수립하는 일련의 과정을 말한다.

■ 위험관리(Risk Management)

자산에 영향을 줄 수 있는 위협 및 취약성을 포함한 위험을 식별, 통제하여 그 위험을 최소화하는 전체 과정이며 위험관리의 종류는 다음과 같다.

구분	내용	예
위험 수용	위험을 인지한 후 그 위험이 크지 않다고 판단될 때 해당 위험을 받아 들이고 별도의 활동을 하지 않음	백업센터 구축 전까지 자연재해로 인한 서비스 장애 위험 수용
위험 회피	위험이 발생할 근본적인 가능성을 제거함	물리적인 보안이 강화된 건물로 회사를 이전함
위험 전이	위험에 대한 직접적인 대응 대신 간접적인 대응 방법을 적용함	보험 가입
위험 감소	보호해야 할 자산에 대해서 보안 대응책을 적용하여 취약성을 제거 또는 감소시켜 그 결과 위험을 감소시킴	서버 장비의 보안 설정 강화

[표 3] 위험관리 종류

2. 위험관리

2.1. 위험분석 방법

위험 분석 방법은 대상의 조직 및 특징, 수행 기간 등에 따라 다양한 방법론이 활용될 수 있으며, 이러한 조건들을 고려하여 가장 적절한 방법을 선택하는 것이 중요하다. 일반적인 위험분석 방법론이라고 일컬어지는 4 가지 관점의 접근방법은 다음과 같다.

(출처: ISO 13335 GMITS-Guidelines for Management of IT Security Part III)

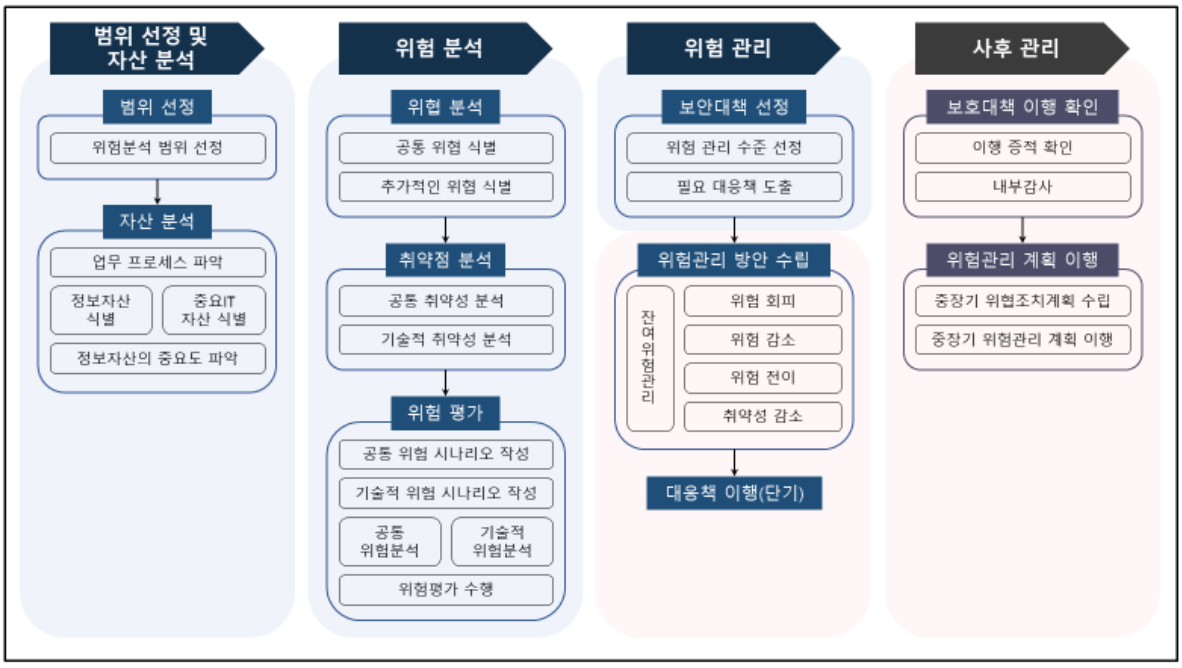
구분	내용
기본통제 접근법 (Baseline Approach)	● 모든 대상에 대하여 보안의 기본수준을 정하고 이를 달성하기 위하여 일련의 보호 대책 선택 ● 시간과 비용이 많이 들지 않고 모든 조직에서 기본적으로 필요한 보호대책 선택 가능 ● 조직의 특성을 고려하지 않았기 때문에, 조직 내에 부서별로 적정 보안 수준보다도 높게 혹은 낮게 보안통제 적용
비형식적 접근법 (Informal Approach)	● 정형화된 방법을 사용하지 않고, 전문가의 지식과 경험에 따라 위험을 분석 ● 작은 조직에서 비용 효과적인 방법 ● 구조화된 접근 방법이 없기 때문에, 위험을 제대로 평가하기 어렵고 보호대책의 선택 및 소요비용을 합리적으로 도출하기 어려우며 계속적으로 반복되는 보안관리의 보안감사 및 사후관리가 제한
상세위험 분석법 (Detailed Risk Analysis)	● 자산의 가치를 측정하고 자산에 대한 위협의 정도와 취약점을 분석하여 위험의 정도를 결정 ● 조직에 특성화된 적절한 보안수준 마련이 가능 ● 전문적인 지식, 시간 및 비용, 노력이 많이 소요
복합적 접근법 (Combined Approach)	● 기본통제 접근법과 상세위험 분석법의 혼합적 형태의 방법론 ● 먼저 조직활동에 필수적인 높은 위험의 시스템을 식별하고 이러한 시스템에 대해서는 '상세위험 분석법'을, 그렇지 않은 시스템에는 '기본통제 접근법' 사용 ● 보안전략을 빠르게 구축할 수 있고, 상대적으로 시간과 노력을 효율적으로 활용 가능

[표 4] 위험분석 접근방법

본 위험분석 보고서는 복합적 접근법(Combined Approach)을 채택하여, 핵심 자산에 해당하는 자산들에 대해서는 상세위험 분석법(자산의 가치 측정 및 자산에 대한 위험도를 결정)을 적용하고, 모든 자산들에 공통적으로 적용될 수 있는 공통 영역(관리적 영역)에 대해서는 기본통제 접근법을 적용한다.

2.2. 위험관리 절차

위험 관리는 아래의 그림과 같이 범위 설정 및 정보자산 식별, 위험분석, 위험관리 및 사후관리 4 단계로 수행된다.



[그림 1] 위험관리 절차

본 위험분석 보고서 내에는 범위선정 및 정보자산 식별, 위험분석 및 보호대책 선정과 같은 위험관리의 일부 영역을 포함하고 있으며, 보호대책 이행계획 수립 등 남아 있는 위험관리의 일부 활동과 사후 관리는 유관부서 담당자와의 협의를 거쳐 향후 수행한다.

3. 자산 분석

3.1. 자산 분석 개요

회사의 정보시스템 서비스와 관련된 정확한 자산 분석을 위해 업무처리 방식을 파악하고 이와 관련한 자산 현황을 파악하여 서비스의 근간이 되는 정보자산을 중심으로 관련 IT 자산을 식별하며, 정보자산 가치의 피해 정도를 중심으로 3 단계(상, 중, 하)로 평가한다. 또한, 자산 평가는 기밀성, 무결성, 가용성의 측면에서 해당 특성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 평가한다.

3.2. 자산 중요도평가 기준

정보자산의 중요도평가는 기밀성(C), 무결성(I), 가용성(A) 측면에서 각 자산이 보안 위협에 노출되었을 경우 예상되는 잠재적 손실 규모를 반영하여 측정되며, 이는 "ISMS-04-03 정보자산 중요도 평가기준"의 내용에 따라 다음과 같이 평가한다.

평가 구분	등급 (값)	설 명
기밀성 (Confidential)	High (3)	□ 자산이 유출되는 경우 조직내에 중대한 손실을 미치는 경우 □ 자산 소유자인 해당부서 또는 담당자만 접근 및 관리 가능한 자산
	Medium (2)	□ 자산이 유출되는 경우 조직의 부분적인 손실을 미치는 경우 □ 자산소유부서/담당자 이외에 관련부서 등 조직 내부에 국한하여 접근 및 열람이 가능한 정보를 가지고 있는 자산
	Low (1)	□ 자산이 유출되어도 관계없거나 손실을 거의 발생시키지 않는 경우 □ 회사 조직 외부인이 접근 및 열람이 가능한 정보를 담고 있는 자원
무결성 (Integrity)	High (3)	□ 자산(정보) 변조 시, 업무수행 또는 서비스에 중대한 장애를 유발하거나 조직전체에 중대한 손실을 입히는 경우 □ 자산(정보) 변조의 가능성이 높고 변조 시 데이터의 무결성을 검증하기 힘든 경우

평가 구분	등급 (값)	설 명
	Medium (2)	□ 자산(정보) 변조 시, 업무수행 또는 서비스에 부분적인 장애를 유발하는 경우 □ 데이터 변조의 가능성은 있으나, 데이터 변조 시 무결성 검증이 가능한 경우
	Low (1)	□ 자산이 변조되어도 업무 수행에 미치는 영향이 미흡한 경우 □ 자산에 포함된 정보의 변조 가능성이 희박하고, 정보 변조 시 무결성 검증이 용이한 경우
가용성 (Availability)	**H**igh (3)	□ 장애 발생 시 즉시 복구되어야 하는 경우 □ 해당 자산(장비)에 대한 장애 또는 침해사고 발생시 직접적인 서비스 중단을 야기하는 경우
	Medium (2)	□ 장애 발생 시 1시간 이내에 복구되어야 하는 경우 □ 장비 장애로 인하여 서비스 중단은 발생하지 않으나 성능에 영향을 미치는 경우
	Low (1)	□ 장애 발생 시 수시간 이내에 복구되어야 하는 경우 □ 장비 장애 시 서비스 중단 또는 성능 저하에 직접적인 영향을 미치지 않는 경우

[표 5] 자산 평가기준

정보자산의 기밀성, 무결성, 가용성의 보안 요구 정도를 각각 산출하여 다음 공식에 따라 정보자산 중요도를 평가하고 평가결과에 따라 중요도 합 3-4 를 '다', 5-6 을 '나', 7-9 를 '가'로 구분한다.

정보자산 중요도 = (기밀성 + 무결성 + 가용성)

보안등급		설 명
가	3점	비밀성(C), 무결성(I), 가용성(A)의 합이 8~9
나	2점	비밀성(C), 무결성(I), 가용성(A)의 합이 5~7
다	1점	비밀성(C), 무결성(I), 가용성(A)의 합이 3~4

[표 6] 보안등급 산정 기준

3.3. 자산 분석 결과

3.3.1. 자산 분류

회사의 정보자산 분류는 제출된 자산목록과 인터뷰 또는 실사를 통해서 확인된 자산을 기준으로 아래의 표와 같이 크게 9 개의 자산 그룹으로 구분하여 분류하였다.

※ "부대설비" 자산의 경우 외부 IDC 자체 관리 자산으로 분석 및 등급평가 제외

분류	설명	비고
서버	업무를 위하여 대·내외적으로 사용되고 있는 운영체계가 설치된 서버 장비	
PC	업무 수행 목적으로 정보를 처리하는 단말기 (PC, 노트북 등의 이동형 단말기)	
DBMS	업무수행 목적으로 운영되고 있는 데이터베이스	
WEB	HTTP 를 통해 웹 브라우저에서 요청하는 HTML 문서나 오브젝트(이미지 파일 등)을 전송해주는 서비스 프로그램	
웹애플리케이션	서비스 제공 및 업무 수행 목적으로 개발/구축한 어플리케이션 (웹사이트 프로그램)	
애플리케이션	서비스 제공 및 업무 수행 목적으로 개발/구축한 어플리케이션 (모바일 프로그램)	

[표 7] 자산분류 기준

3.3.2. 자산 목록 및 중요도

인증범위의 선정을 통해 파악된 조직의 규모와 운영 목적, 환경을 바탕으로 위험평가 대상 자산을 실제적으로 파악하였으며, 정보자산 목록은 다음과 같다.

구분	Hostname	IP	용도	보안 등급
서버	012e9e8b578dd7e1d	52.3.110.55	web server(Apache)	M(2)
	0523879f208cc2c36	3.82.141.228	DB	M(2)

구분	Hostname	IP	용도	보안 등급
	0b23e3288158e31a0	172.31.27.16	사내 PC 관리 및 웹 서비스	M(2)
DBMS	0523879f208cc2c36	3.82.141.228	DB	M(2)
WEB	012e9e8b578dd7e1d	52.3.110.55	web server(Apache)	M(2)
웹 애플리케이션	012e9e8b578dd7e1d	52.3.110.55	web server(Apache)	M(2)
애플리케이션	012e9e8b578dd7e1d	52.3.110.55	web server(Apache)	M(2)

[표 8] 자산목록 및 중요도

위험도 산출 시 관리적 영역의 경우, 자산의 가치는 인증 범위 내 보호되어야 할 정보자산의 평균 값(C, I, A [3, 3, 3])을 적용하여 산출하며, 기술적 영역은 개별 정보자산의 가치 평가 값을 반영하여 산출한다.

※관리적, 기술적 영역에 대한 통합 자산 가치 평가 값 산출 결과는 다음과 같다.

구분	보안등급	가치	설명
기밀성(C)	H	3	조직 내부에서도 높은 비밀 등급의 부여가 요구되며, 일반에게 공개되는 경우 개인이나 조직의 안전 및 프라이버시에 심각한 영향을 초래할 수 있고 조직의 사업 진행에 치명적인 피해를 줄 수 있는 수준
	M	2	조직 내부에서만 공유되어야 하며, 일반에게 공개되는 경우 개인이나 조직의 안전 및 프라이버시에 일정부분 영향을 초래할 수 있고 조직의 사업 진행에 상당한 문제를 발생시킬 수 있는 수준
	L	1	일반에게 공개되어도 개인이나 조직의 안전 및 프라이버시에 영향이 크지 않고 조직의 사업 진행에 대한 피해가 무시할 수 있는 수준
무결성(I)	H	3	고의나 사고에 의해 변조되거나 일부 오류가 발생하는 경우 조직의 사업진행에 치명적인 피해를 줄 수 있고, 이로 인한 손실의 크기가 막대함
	M	2	고의나 사고에 의해 변조되거나 일부 오류가 발생하는 경우 조직의 일부 사업진행에 일정부문 문제를 발생시킬 수 있고, 이로 인한 손실의 크기가 보통임
	L	1	고의나 사고에 의해 변조/조작되는 경우 조직의 사업진행에 피해가 거의 없고, 이로 인한 손실의 크기가 크지 않음
가용성(A)	H	3	접근 또는 서비스가 중단되는 경우 조직의 사업진행을 중단하게 하는 치명적인 수준이며, 이로 인한 손실의 크기가 막대함

	M	2	접근 또는 서비스가 중단되는 경우 사업진행에 일정부분 지장을 줄 수 있는 수준이며, 이로 인한 손실의 크기가 보통임
	L	1	접근 또는 서비스가 중단되는 경우 사업진행에 대한 지장이 무시할 수 있는 수준이며, 이로 인한 손실의 크기가 크지 않음

구분	C [기밀성]	I [무결성]	A [가용성]	보안등급
통합 자산 등급	**3**	**3**	**3**	**H**

[표 9] 통합 자산 등급 평가 결과

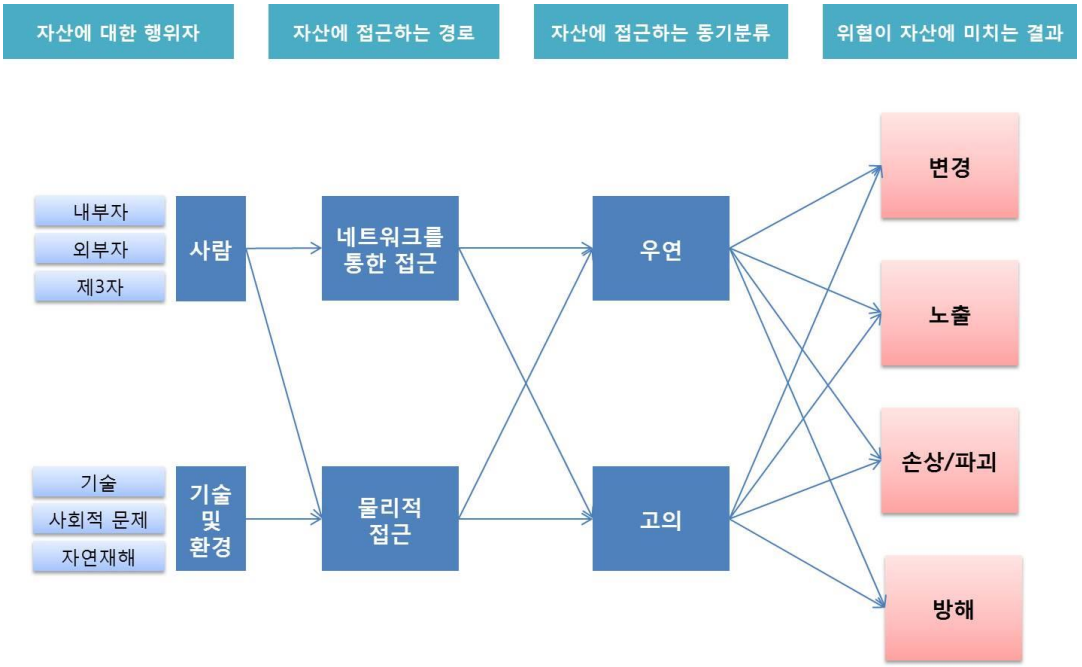
4. 위협 및 취약성 분석

4.1. 위협 분석

4.1.1. 위협 분석 개요

위협 분석은 정보자산에 해를 입힐 수 있는 위협을 규정하고 적절한 방법으로 분류하여 각 위협들의 성질을 파악하고 위협들의 발생 확률 또는 발생 빈도와 자산에 미치는 손해의 정도를 평가하는 것이다.

정보자산에 피해를 입힐 수 있는 위협은 자산에 영향을 주는 행위자, 접근하는 경로, 접근하는 동기 및 미치는 결과 유형에 따라 여러 종류가 존재한다.



[그림 2] 위협의 유형

4.1.2. 위협 등급 평가 기준

위협은 정보시스템 운영 시 경험한 과거자료나 일반적 통계치를 이용하여 구해야 하나, 이와 같은 자료를 정량화 하기는 용이하지 않을 뿐만 아니라 서비스 게시 이후 서비스

안정화 측면에 중점을 두어 이와 같은 자료가 존재하지 않으므로 주관적인 인식에 의해 위협의 발생빈도 및 영향도를 추정하여 정성적으로 평가하였다.

위협의 측정 등급 기준은 다음과 같다.

등급	등급 평가 기준
3	가능성 높음 (70% 정도의 확률) / 위협의 영향 높음
2	가능성 존재함 (40% 정도의 확률) / 위협의 영향 보통
1	가능성 어느정도 있음 (10% 정도의 확률) / 위협의 영향 낮음

[표 9] 위협 등급 평가 기준

4.1.3. 위협 분석 결과

위협을 적절히 식별하기 위해서는 다양한 위협 요소가 서로 중복되지 않게 전 분야에 걸쳐 포괄적으로 파악하는 것이 중요하다. 다만, 포괄적으로 파악한다고 하여 조직 내에서 파악될 수 있는 위협 요소 모두를 파악할 수 있는 것은 아니다.

위협 목록은 추후 진행되는 위험도 산정에 있어 관련 취약점과 더불어 기초적인 판단 근거가 된다.

위협의 유형에 따라 식별된 조직 내 전반적인 위협 목록은 다음과 같다.

위협 코드	위협 카테고리			영향 구분			위협 등급
	대분류	중분류	소분류	기밀성	무결성	가용성	
TC1-01	일반 위협 (General Threats)	관리 및 운영 절차의 미비 및 부재	검증/모니터링, 보고 절차 미흡/부재	O	O	O	3
TC1-02			운영/접근통제 절차 미흡/부재	O	O	O	3
TC1-03			비상대책 미흡/부재	O	O	O	2
TC1-04			관리 및 운영 통제 미흡	O	O	O	3
TC1-05		운영 및 테스트 환경 미분리	운영 및 테스트 데이터의 혼용 사용	O	O	O	1
TC1-06		인적 운영 관리의 미비	조직 구성 미흡	O	O	O	2
TC1-07			R&R 정의 미흡	O	O	O	2

위협 코드	위협 카테고리			영향 구분			위협 등급
	대분류	중분류	소분류	기밀성	무결성	가용성	
TC1-08			외부직원 통제 미흡	O	O		2
TC1-09			교육 및 인식 부족	O	O	O	2
TC1-10		보안문서의 미비 및 부재	보안 정책/지침/체계 부재	O	O		2
TC1-11			보안 문서(정책,지침,절차 등) 부재	O	O		2
TC1-12			보안 문서 현행화 미흡	O	O		3
TC1-13			보안 정책/지침 시행 당위성 부재	O	O		2
TC1-14			보안 문서(정책,지침,절차 등) 관리 미흡	O	O		2
TC1-15		비인가 저장매체의 사용	저장 매체(USB, CD, HDD)에 대한 비인가 사용	O	O		3
TC2-01	식별, 인가 위협 (Identification/ Authorization Threats)	신분위장(Spoofing ID)	인가된 사용자/고객 위장 내부 공격	O	O	O	3
TC2-02		식별 및 인증 실패	식별 및 인증 절차/기능 부재	O	O	O	3
TC2-03			식별 및 인증 절차/기능 우회	O	O	O	3
TC2-04		정상프로그램 위장공격	Trojan 프로그램 사용 공격	O	O	O	2
TC3-01	서비스 신뢰도 위협 (Reliability of Service Threats)	자연재해	화재, 홍수, 지진 등			O	2
TC3-02		환경재해	온습도 조절장치 고장, 장애			O	1
TC3-03			전원공급 실패 (불완전한 전원공급)			O	1
TC3-04		서비스 실패	네트워크 서비스 지연, 실패			O	3
TC3-05			HW 서비스 실패(HW, OS)		O	O	3
TC3-06			SW 서비스 실패(미들웨어, 프로그램)		O	O	3

위협 코드	위협 카테고리			영향 구분			위협 등급
	대분류	중분류	소분류	기밀성	무결성	가용성	
TC3-07			DB 서비스 실패		O	O	3
TC3-08		서비스 거부 (Denial of Service)	네트워크 Traffic 과부하			O	3
TC3-09			서버 과부하			O	3
TC3-10			Email Bombing(& SPAM)			O	3
TC3-11			DOS(Denial of Service) 공격			O	3
TC3-12		비인가 소프트웨어의 유입	웜(Worm)/바이러스	O	O	O	3
TC3-13			스파이웨어/에드웨어	O	O	O	3
TC3-14			불법소프트웨어 사용	O	O	O	3
TC4-01	기밀성 위협 (Confidentiality Threats)	문서 유출	개인정보 문서 유출(PC, 책상, 휴지통, 복사기 등)	O			2
TC4-02		스니핑(Sniffing)	인터넷 스니핑을 통한 민감한 데이터 접근	O	O	O	2
TC4-03			내부 네트워크 스니핑을 통한 민감한 데이터 접근	O			3
TC4-04		피싱(Phishing) & 파밍(Pharming)	사이트 위조(사용자 도용)	O			2
TC4-05		Application 프로그램 악용	Application 프로그램을 통한 개인정보 조회, 유출	O			2
TC4-06			Client 프로그램 개인정보(cache 정보)의 조회, 유출	O			2
TC4-07		취약한 시스템 설정 악용	시스템 정보, 설정 정보 등 중요 정보 유출	O	O		2
TC4-08		저장매체 정보 유출	저장 매체를 통한 중요 정보 유출	O			2
TC5-01	무결성 위협 (Integrity Threats)	정보 및 정보처리 프로세스의 변조	정보의 의도적 변조 및 손상		O	O	2
TC5-02			시스템 주요 파일 및 프로그램의 의도적 변조 및		O	O	2

위협 코드	위협 카테고리			영향 구분			위협 등급
	대분류	중분류	소분류	기밀성	무결성	가용성	
			손상				
TC6-01	접근제어 위협 (Access Control Threats)	정보 수집(Information Gathering)	Scanning 등을 통한 시스템 정보 수집	O			3
TC6-02			네트워크 정보 수집	O			3
TC6-03		패스워드 Cracking	패스워드 추측 공격	O			2
TC6-04			패스워드 파일 접근	O			3
TC6-05		취약한 권한접근	사용자/프로그램 권한 상승	O	O	O	2
TC6-06			불필요하게 부여된 권한에 따른 권한 오남용	O	O	O	2
TC6-07			파일/디렉토리 취약한 권한 설정 악용	O	O	O	2
TC6-08		비인가된 시스템 및 네트워크 접근	네트워크 구성(접근통제 등)의 오류 이용	O	O	O	2
TC6-09			시스템(OS, DB, App 등) 설정 오류		O	O	2
TC6-10			네트워크 프로토콜의 버그 이용	O		O	2
TC6-11			비인가 시스템 접근(필터링 미설정, 방화벽 미설치 이용한 공격)	O	O	O	2
TC6-12			비인가 PC 및 단말기의 사용	O	O		2
TC6-13		웹 서비스 공격	취약한 웹 서버 설정 이용	O		O	2
TC6-14			악성 스크립트 또는 명령 실행	O		O	2
TC6-15			Buffer Overflow 공격 등을 통한 관리자 권한 획득	O		O	2
TC6-16			어플리케이션에 내재된 취약성 이용 공격	O		O	2
TC6-17		비인가된 물리적 접근	사무실, 지점의 비인가 접근	O		O	3

위협 코드	위협 카테고리			영향 구분			위협 등급
	대분류	중분류	소분류	기밀성	무결성	가용성	
TC7-01	부인 위협 (Repudiation Threats)	침해 부인	비인가 및 공격 행위 부인(Log 미설정 등)		O		2
TC7-02			침해 증거(로그) 변조 및 파괴		O		2
TC8-01	법적 위협 (Legal Threats)	규제 및 법적 요건의 미준수	상위기관 규정 위배에 따른 벌금, 징계 등			O	2

[표 10] 위협 분석 결과

4.2. 취약성 분석

4.2.1. 취약성 분석 개요

취약성은 정보시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 잠재된 약점으로, 이러한 취약성은 그 자체가 자산의 손상을 초래하지는 않으며, 단지 위협이 자산에 영향을 줄 수 있는 조건을 제공한다.

취약성 분석은 위협이 자산에 영향을 줄 수 있는 문제점을 확인하고 분류하여 위협을 감소시키도록 하는 것을 목적으로 한다.

4.2.2. 취약점 등급 평가 기준

취약점 분석은 관리적 영역 및 기술적 영역을 구분하여 평가를 수행하였다. 관리적 영역은 평가 기준에 대한 객관성, 신뢰성을 확보하고자 정보보호 및 개인정보보호 관리체계 (ISMS-P) 통제 항목에 기반한 체크리스트를 활용하여 평가를 수행하였다. 기술적 영역은 보안가이드라인에 따른 취약성 진단 항목의 각 중요도에 따라 취약점 등급을 평가하였다.

점검 결과	취약점 등급 평가 기준	
	관리적 영역	인프라 영역
취약(N)	보안통제가 이루어 지지 않고 있음 - 평가 점수(ISMS) : 3 점	점검 항목 중요도 : 상(3)
미흡(P)	보안통제가 부분적으로 이루어짐 - 평가 점수(ISMS) : 1.5 점	점검 항목 중요도 : 중(2)
양호(Y)	보안통제가 비교적 잘 이루어짐 - 평가 점수(ISMS) : 0 점	점검 항목 중요도 : 하(1)
N/A	해당하지 않음	해당하지 않음

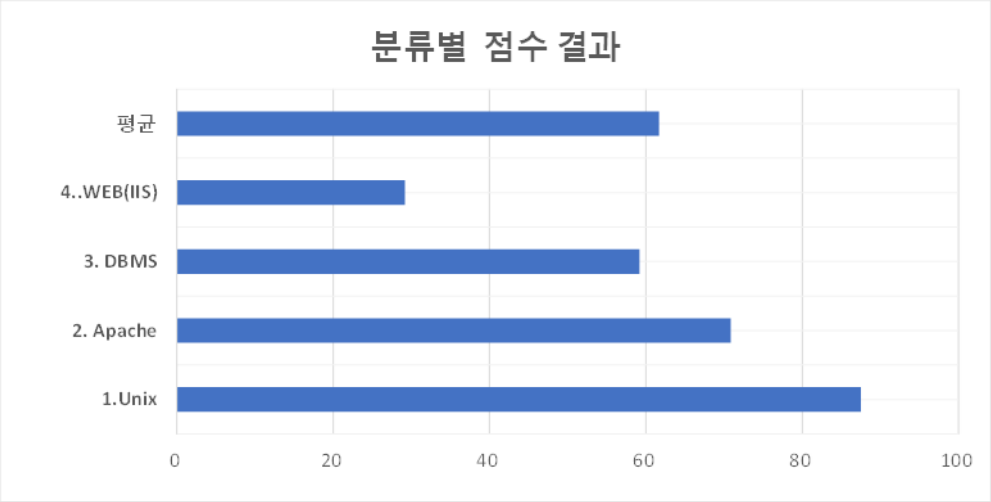
[표 11] 취약점 등급 평가 기준

4.2.3. 취약점 분석 결과

4.2.3.3. 기술적 취약점 분석

1) 진단결과 요약

기술적 취약점 분석 결과 취약점이 발견되지 않았다.



취약점분석 결과 (기술적 영역)

2) 기술적 취약점 점검 결과

구분	진단항목	세부 진단항목		취약점 등급	점검결과
WEB	1. 계정관리	U-03	계정 잠금 임계값 설정	3	취약
	1. 계정관리	U-06	root 계정 su 제한	1	취약
	1. 계정관리	U-07	패스워드 최소 길이 설정	2	취약
	1. 계정관리	U-08	패스워드 최대 사용 기간 설정	2	취약
	1. 계정관리	U-09	패스워드 최소 사용기간 설정	2	취약
	1. 계정관리	U-10	불필요한 계정 제거	1	취약
	1. 계정관리	U-14	사용자 shell 점검	1	취약
	1. 계정관리	U-15	Session Timeout 설정	1	취약
	2. 파일 및 디렉터리 관리	U-19	/etc/shadow 파일 소유자 및 권한 설정	3	취약
	2. 파일 및 디렉터리 관리	U-24	SUID, SGID, Sticky bit 설정 파일 점검	3	취약
	2. 파일 및 디렉터리 관리	U-26	world writable 파일 점검	3	취약

구분	진단항목	세부 진단항목		취약점 등급	점검결과
	2. 파일 및 디렉터리 관리	U-29	접속 IP 및 포트 제한	2	취약
	2. 파일 및 디렉터리 관리	U-32	UMASK 설정 관리	2	취약
	2. 파일 및 디렉터리 관리	U-34	홈디렉토리로 지정한 디렉토리의 존재 관리	3	취약
	2. 파일 및 디렉터리 관리	U-35	숨겨진 파일 및 디렉토리 검색 및 제거	3	취약
	3. 서비스관리	U-60	로그온 시 경고 메시지 제공	1	취약
DB	1. 계정관리	U-03	계정 잠금 임계값 설정	3	취약
	1. 계정관리	U-09	패스워드 최소 사용기간 설정	2	취약
	1. 계정관리	U-15	Session Timeout 설정	1	취약
	2. 파일 및 디렉터리 관리	U-24	SUID, SGID, Sticky bit 설정 파일 점검	3	취약
	2. 파일 및 디렉터리 관리	U-26	world writable 파일 점검	3	취약
	2. 파일 및 디렉터리 관리	U-29	접속 IP 및 포트 제한	2	취약
	2. 파일 및 디렉터리 관리	U-32	UMASK 설정 관리	2	취약
	2. 파일 및 디렉터리 관리	U-34	홈디렉토리로 지정한 디렉토리의 존재 관리	3	취약
	2. 파일 및 디렉터리 관리	U-35	숨겨진 파일 및 디렉토리 검색 및 제거	3	취약
	3. 서비스관리	U-60	로그온 시 경고 메시지 제공	1	취약
	1. 서비스관리	APC-03	Apache 상위 디렉토리 접근 금지	3	취약
	1. 서비스관리	APC-06	Apache 파일 업로드 및 다운로드 제한	3	취약
	1. 서비스관리	APC-07	Apache 웹 서비스 영역의 분리	3	취약
	2. 접근 통제	APC-11	Apache 에러 메시지 관리	3	취약
	2. 접근 통제	APC-12	Apache HTTP Method 제한	2	취약

구분	진단항목	세부 진단항목		취약점 등급	점검결과
WEB	1. 서비스 관리	IIS-15	IIS 웹서비스 정보 숨김	2	취약
	1. 서비스 관리	IIS-16	스크립트 실행 제거	1	취약
	2. 로그 관리	IIS-17	로그 관리 진단	3	취약
	3. 패치 관리	IIS-18	최신 패치 적용	3	취약
RDS	1. 계정관리	D-02	scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용	3	취약
	1. 계정관리	D-03	패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정	3	취약
	1. 계정관리	D-05	패스워드 재사용에 대한 제약	2	취약
	2. 접근관리	D-11	일정 횟수의 로그인 실패 시 잠금 정책 설정	2	취약
	2. 접근관리	D-12	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022이상으로 설정	1	취약
	2. 접근관리	D-13	데이터베이스 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정	2	취약
	3. 옵션관리	D-16	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	3	취약
	5. 로그관리	D-24	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정	1	취약

[표 15] 취약점 위험도 평가 결과(기술적 영역)

5. 위험평가

5.1. 위험평가 개요

위험 평가는 자산의 취약성에 의하여 위협이 발생할 수 있는 가능성 및 이로 인해 입을 수 있는 자산의 손실 정도를 평가하는 것이다.

본 위험분석 보고서에서는 정보자산에 대한 평가, 위협 및 취약점을 고려한 위험 시나리오에 대한 평가 결과를 종합하여 위험의 수준을 산정하고 자산의 최종적인 위험 수준을 평가한다.

5.2. 위험 평가 방법

최종 위험도를 산출하는 공식은 기본적으로 다음에 따른다.

구분	내용
위험도	위험도 = 자산 중요도 등급 X 위협등급 X 취약점등급

[표 16] 위험도 산출 공식

예를들어, A라는자산의 등급이 '가'이면 자산가치가 3으로 환산되며, 위협이 3이고, 취약점등급이 2 로 조사되었을 때 위험도를 다음의 표를 이용하여 구하면 18(=3 X 3 X 2)이 된다.

위협		3			2			1		
취약점		3	2	1	3	2	1	3	2	1
자산 중요도 등급	가 (3)	9	8	7	8	7	6	7	6	5
	나 (2)	8	7	6	7	6	5	6	5	4
	다 (1)	7	6	5	6	5	4	5	4	3

5.3. 위험 평가 결과

위험 평가 절차 및 위험 평가 방법에 의하여 상세 위험 평가 결과를 산출하였다.

5.3.1. 기술적 부문

인프라 취약점 점검 및 모의해킹 결과에 따른 기술적 부문에 대한 위험 평가 결과는 다음과 같다.

위험			위협			자산		취약점		
위험 코드	위험내용	위험도	위협 코드	위협내용	위협 등급	분류	보안 등급	대수	점검항목	항목 중요도
Ii_01	계정 잠금에 대한 임계값 설정을 하지 않은 경우, 반복되는 로그인 시도에 대한 차단이 없어, 비인가자에게 사용자 계정 패스워드가 유출될 수 있음	12	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	계정 잠금 임계값 설정	상
Ii_01	su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 root계정 권한을 얻기 위한 각종 공격으로 root 계정 패스워드가 유출될 수 있음	4	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	root 계정 su 제한	하
Ii_01	패스워드 최소 길이 설정이 적용되지 않은 경우, 비인가자의 각종 공격에 취약하여 사용자 계정 패스워드 유출될 수 있음	8	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	패스워드 최소 길이 설정	중
Ii_01	패스워드 최대 사용기간을 설정하지 않은 경우, 비인가자의 각종 공격을 시도할 수 있는 기간 제한이 없으므로 사용자 패스워드가 유출될 수 있는 확률이 증가함	8	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	패스워드 최대 사용 기간 설정	중
Ii_01	패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음	8	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	패스워드 최소 사용기간 설정	중
Ii_01	OS나 Package 설치 시 default로 생성되는 불필요한 계정들은 비인가자의 공격에 의해 패스워드가 유출될 수 있음	4	TC6-03	패스워드 추측 공격	2	WEB	M(2)	1	불필요한 계정 제거	하
Ii_01	로그인이 불필요한 계정의 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 통하여 중요파일 유출이나 악성코드를 이용한 root 권한 획득 등의 공격을 할 수 있음	4	TC4-07	시스템 정보, 설정 정보 등 중요 정보 유출	2	WEB	M(2)	1	사용자 shell 점검	하
Ii_01	Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의	4	TC4-07	시스템 정보, 설정	2	WEB	M(2)	1	Session Timeout 설정	하

위험			위협			자산		취약점		
위험 코드	위험내용	위험도	위협 코드	위협내용	위협 등급	분류	보안 등급	대수	점검항목	항목 중요도
	시스템 접근으로 인해 내부 정보가 노출될 수 있음			정보 등 중요 정보 유출						
Ii_01	해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있음	18	TC6-04	패스워드 파일 접근	3	WEB	M(2)	1	/etc/shadow 파일 소유자 및 권한 설정	상
Ii_01	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음	12	TC6-05	사용자/프로그램 권한 상승	2	WEB	M(2)	1	SUID, SGID, Sticky bit 설정 파일 점검	상
Ii_01	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 변경할 수 있어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있음	12	TC6-07	파일/디렉토리 취약한 권한 설정 악용	2	WEB	M(2)	1	world writable 파일 점검	상
Ii_01	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고가 발생할 수 있음	8	TC6-08	네트워크 구성(접근통제 등)의 오류 이용	2	WEB	M(2)	1	접속 IP 및 포트 제한	중
Ii_01	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인해 파일 시스템 악용이 우려됨	8	TC6-06	불필요하게 부여된 권한에 따른 권한 오남용	2	WEB	M(2)	1	UMASK 설정 관리	중
Ii_01	사용자에게 지정된 디렉터리가 아닌 곳이 홈 디렉터리로 설정될 경우 해당 디렉터리 내 명령어 사용이 가능하며 이에 따라 시스템 관리·보안상 문제가 발생할 수 있음	12	TC6-07	파일/디렉토리 취약한 권한 설정 악용	2	WEB	M(2)	1	홈디렉토리로 지정한 디렉토리의 존재 관리	상
Ii_01	공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음	12	TC4-07	시스템 정보, 설정 정보 등 중요 정보 유출	2	WEB	M(2)	1	숨겨진 파일 및 디렉토리 검색 및 제거	상
Ii_01	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음	4	TC6-09	시스템(OS, DB, App 등) 설정 오류	2	WEB	M(2)	1	로그온 시 경고 메시지 제공	하
Ii_02	계정 잠금에 대한 임계값 설정을 하지 않은 경우, 반복되는 로그인 시도에 대한 차단이 없어, 비인가자에게 사용자 계정 패스워드가 유출될 수 있음	12	TC6-03	패스워드 추측 공격	2	DB	M(2)	1	계정 잠금 임계값 설정	상
Ii_02	패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질	8	TC6-03	패스워드 추측 공격	2	DB	M(2)	1	패스워드 최소 사용기간 설정	중

위험			위협			자산		취약점		
위험 코드	위험내용	위험도	위협 코드	위협내용	위협 등급	분류	보안 등급	대수	점검항목	항목 중요도
	수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음									
Ii_02	Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 내부 정보가 노출될 수 있음	4	TC4-07	시스템 정보, 설정 정보 등 중요 정보 유출	2	DB	M(2)	1	Session Timeout 설정	하
Ii_02	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음	12	TC6-05	사용자/프로그램 권한 상승	2	DB	M(2)	1	SUID, SGID, Sticky bit 설정 파일 점검	상
Ii_02	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 변경할 수 있어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있음	12	TC6-07	파일/디렉토리 취약한 권한 설정 악용	2	DB	M(2)	1	world writable 파일 점검	상
Ii_02	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고가 발생할 수 있음	8	TC6-08	네트워크 구성(접근통제 등)의 오류 이용	2	DB	M(2)	1	접속 IP 및 포트 제한	중
Ii_02	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인해 파일 시스템 악용이 우려됨	8	TC6-06	불필요하게 부여된 권한에 따른 권한 오남용	2	DB	M(2)	1	UMASK 설정 관리	중
Ii_02	사용자에게 지정된 디렉터리가 아닌 곳이 홈 디렉터리로 설정될 경우 해당 디렉터리 내 명령어 사용이 가능하며 이에 따라 시스템 관리·보안상 문제가 발생할 수 있음	12	TC6-07	파일/디렉토리 취약한 권한 설정 악용	2	DB	M(2)	1	홈디렉토리로 지정한 디렉토리의 존재 관리	상
Ii_02	공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음	12	TC4-07	시스템 정보, 설정 정보 등 중요 정보 유출	2	DB	M(2)	1	숨겨진 파일 및 디렉토리 검색 및 제거	상
Ii_02	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음	4	TC6-09	시스템(OS, DB, App 등) 설정 오류	2	DB	M(2)	1	로그온 시 경고 메시지 제공	하
Ii_02	상위 경로로 이동하는 것이 가능할 경우 하위 경로에 접속하여 상위 경로로 이동함으로써 해킹을 당할 위험이 있으며, 유니코드 버그(Unicode Bug) 및 서비스 거부 공격에 취약해지기 쉬움	12	TC6-13	취약한 서버 설정 이용	2	DB	M(2)	1	Apache 상위 디렉토리 접근 금지	상
Ii_02	불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드로	18	TC3-09	서버 과부하	3	DB	M(2)	1	Apache 파일 업로드 및 다운로드 제한	상

위험			위협			자산		취약점		
위험 코드	위험내용	위험도	위협 코드	위협내용	위협 등급	분류	보안 등급	대수	점검항목	항목 중요도
	인한 서비스 불능 상태가 발생할 수 있음									
Ii_02	Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs 디렉터리는 공개되어서는 안될(또는, 공개 될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있어 유출 발생 가능성이 있음	12	TC4-07	시스템 정보, 설정 정보 등 중요 정보 유출	2	DB	M(2)	1	Apache 웹 서비스 영역의 분리	상
Ii_02	웹 서버에서 제공하는 default 에러 메시지가 출력되도록 설정되어 있는 경우, 공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 발생되는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있음	12	TC6-13	취약한 서버 설정 이용	2	DB	M(2)	1	Apache 에러 메시지 관리	상
Ii_02	OPTIONS, GET, POST 이외의 다른 HTTP Method를 지원하는 경우, 악의적인 공격자가 임의의 파일을 삭제하거나 업로드 하여 서버의 정상 운영에 지장을 줄 수 있음	8	TC6-13	취약한 서버 설정 이용	2	DB	M(2)	1	Apache HTTP Method 제한	중
WIN_01	IIS 웹서비스 정보 숨김 설정이 적용되지 않은 경우 악의적인 사용자에게 불필요한 정보가 노출되어 외부 공격을 위한 기초 자료로 이용될 수 있음	8	TC6-16	어플리케이션에 내재된 취약성 이용 공격	2	WEB	M(2)	1	IIS 웹서비스 정보 숨김	중
WIN_01	게시판이나 자료실과 같이 업로드 된 파일이 저장되는 디렉터리에 CGI 스크립트가 실행 가능하다면 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고의 통로로 이용될 수 있음	4	TC6-14	악성 스크립트 또는 명령 실행	2	WEB	M(2)	1	스크립트 실행 제거	하
WIN_01	로그 파일에는 공격자에게 유용한 정보가 들어있을 수 있으므로 권한 관리가 필요함 일반 사용자에 의한 정보 유출이 불가능 하도록 권한 설정 필요하며, 비인가자가 접근하여 로그상의 중요정보 유출할 수 있음	12	TC7-01	비인가 및 공격 행위 부인(Log 미설정 등)	2	WEB	M(2)	1	로그 관리 진단	상
WIN_01	공개된 취약점에 노출되지 않은 최신 보안 패치를 적용하지 않으면 exploit 공격, 제로데이 공격 등의 서버 침해가 발생할 수 있음	12	TC6-13	취약한 서버 설정 이용	2	WEB	M(2)	1	최신 패치 적용	상
RDS-01	데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비 인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 존재함	12	TC5-02	시스템 주요 파일 및 프로그램의 의도적 변조 및 손상	2	RDS	M(2)	1	scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금 설정 후 사용	상

위험			위협			자산		취약점		
위험 코드	위험내용	위험도	위협 코드	위협내용	위협 등급	분류	보안 등급	대수	점검항목	항목 중요도
RDS-01	주기적인 패스워드 변경이 없을 경우 공격자는 Brute force 공격을 통하여 패스워드를 획득할 위험이 존재함	12	TC6-03	패스워드 추측 공격	2	RDS	M(2)	1	패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정	상
RDS-01	데이터베이스의 사용자 계정을 공용 및 공유 사용하게 될 경우, 침해사고 발생 시 책임 추적에 영향을 주며, 계정 별 권한 부여가 불가능해지고 사용하지 않는 계정을 이용한 비인가 사용자 접속이 가능함	8	TC5-01	정보의 의도적 변조 및 손상	2	RDS	M(2)	1	패스워드 재사용에 대한 제약	중
RDS-01	일정한 횟수의 로그인 실패 횟수 발생 시 이를 제한하지 않으면 무작위 추측 공격 (Brute force)을 통하여 데이터베이스에 접근이 가능함	8	TC6-03	패스워드 추측 공격	2	RDS	M(2)	1	일정 횟수의 로그인 실패 시 잠금 정책 설정	중
RDS-01	설정되어 있지 않은 경우 인가되지 않은 사용자가 이를 이용하여 관련 소프트웨어를 실행할 수 있는 위험이 있음	4	TC6-07	파일/디렉토리 취약한 권한 설정 악용	2	RDS	M(2)	1	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022이상으로 설정	하
RDS-01	비인가자가 redo 파일, 데이터베이스 설정 파일, 데이터 파일, 네트워크 설정 파일, Oracle 패스워드 관련 파일인 orapw.ora, listener.ora,init<SID>.ora 등의 주요 파일에 접근하여 수정·삭제하면 Oracle 데이터베이스 운영에 오류가 발생함	8	TC5-02	시스템 주요 파일 및 프로그램의 의도적 변조 및 손상	2	RDS	M(2)	1	데이터베이스 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 설정	중
RDS-01	OS_ROLES 설정 파라미터는 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락되며, REMOTE_OS_ROLES가 TRUE로 설정되어 있는 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있음	12	TC6-06	불필요하게 부여된 권한에 따른 권한 오남용	2	RDS	M(2)	1	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상
RDS-01	Audit Table은 반드시 SYS, SYSTEM과 같은 데이터베이스 관리자 계정에 속해 있어야 하며, 그렇지 않은 경우 인가되지 않은 사용자가 감사 데이터의 수정, 삭제 등의 수행이 가능함	4	TC7-02	침해 증거(로그) 변조 및 파괴	2	RDS	M(2)	1	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정	하

[표 18] 위험 평가 결과 (기술)

6. 위험 관리 수준 선정 및 보안 대책 수립

6.1. 위험 관리 수준 선정 개요

도출된 모든 위험에 대해 관리한다는 것은 시간과 비용을 고려할 때 비현실적이고, 비효율적이므로 위험의 평가 결과를 검토 및 평가하여 회사에서 필요로 하는 위험관리 수준(DoA : Degree of Assurance)을 결정한다.

DoA 선정은 비즈니스 수행에 무리를 주지 않는 수준에서 보안 통제를 구현하기 위함이다. 즉, 비즈니스 수행 시 필수적으로 요구되는 보안성 보장 및 대내·외적인 보안 요구 사항을 충족하는 수준까지만 위험을 관리하기 위한 위험 관리의 수준을 의미한다.

이때, 위험관리 수준보다 낮은 수준의 위험은 Acceptable Risk 라 하여 위험을 감수하겠다는 것을 의미하며, 위험관리 수준보다 높게 나타난 위험을 Unacceptable Risk 라 하여 위험을 관리하기 위한 보안 대책을 검토하여 수립하겠다는 것을 의미한다.

6.2. 위험 관리 수준 선정

위험관리 수준(DoA)은 회사의 현황을 고려하여 위험도 **6** 이상으로 선정하였다.

위험관리 수준(DoA)를 고려하여 기술적 취약성에 대한 위험관리 수준을 위험도 6 이상인 것을 우선적으로 조치하고, 단기간 내에 조치가 가능하다고 판단되는 위험에 대해서는 위험도 6 미만의 항목에 대해서도 조치를 수행한다.

6.3. 보호 대책 선정결과

✓ 위험 평가 결과에 의하여 해당 위험을 통제하기 위한 세부적인 보호 대책을 수립하였다.

6.3.1. 기술적 부문

위험 코드	위험 내용	위험도	보호대책
li_01	계정 잠금에 대한 임계값 설정을 하지 않은 경우, 반복되는 로그인 시도에 대한 차단이 없어, 비인가자에게 사용자 계정 패스워드가 유출될 수 있음	12	계정 잠금 임계값을 5 이하로 설정
li_01	su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 root계정 권한을 얻기 위한 각종 공격으로 root 계정 패스워드가 유출될 수 있음	4	일반사용자의 su 명령 사용 제한
li_01	패스워드 최소 길이 설정이 적용되지 않은 경우, 비인가자의 각종 공격에 취약하여 사용자 계정 패스워드 유출될 수 있음	8	패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정
li_01	패스워드 최대 사용기간을 설정하지 않은 경우, 비인가자의 각종 공격을 시도할 수 있는 기간 제한이 없으므로 사용자 패스워드가 유출될 수 있는 확률이 증가함	8	패스워드 정책 설정파일을 수정하여 패스워드 최대 사용기간을 90일(12주)로 설정
li_01	패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음	8	패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정
li_01	OS나 Package 설치 시 default로 생성되는 불필요한 계정들은 비인가자의 공격에 의해 패스워드가 유출될 수 있음	4	현재 등록된 계정 현황 확인 후 불필요한 계정 삭제
li_01	로그인이 불필요한 계정의 쉘이 설정되어 있을 경우, 공격자는 기본 계정들을 통하여 중요 파일 유출이나 악성코드를 이용한 root 권한 획득 등의 공격을 할 수 있음	4	로그인이 필요하지 않은 계정에 대해 /bin/false(/sbin/nologin) 쉘 부여
li_01	Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 내부 정보가 노출될 수 있음	4	600초(10분) 동안 입력이 없을 경우 접속 된 Session 을 끊도록 설정

위험 코드	위험 내용	위험도	보호대책
li_01	해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있음	18	/etc/shadow 파일의 소유자를 root, 권한을 400로 변경
li_01	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음	12	불필요한 SUID, SGID 파일 제거
li_01	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 변경할 수 있어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있음	12	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거
li_01	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고가 발생할 수 있음	8	TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정
li_01	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인해 파일 시스템 악용이 우려됨	8	설정파일에 UMASK 값을 022로 설정
li_01	사용자에게 지정된 디렉터리가 아닌 곳이 홈 디렉터리로 설정될 경우 해당 디렉터리 내 명령어 사용이 가능하며 이에 따라 시스템 관리·보안상 문제가 발생할 수 있음	12	홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는 계정 삭제
li_01	공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음	12	[.]으로 시작하는 숨겨진 파일 존재 여부 확인 후 불법적이거나 의심스러운 파일을 삭제
li_01	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음	4	Telnet, FTP , SMPT, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작
li_02	계정 잠금에 대한 임계값 설정을 하지 않은 경우, 반복되는 로그인 시도에 대한 차단이 없어, 비인가자에게 사용자 계정 패스워드가 유출될 수 있음	12	계정 잠금 임계값을 5 이하로 설정
li_02	패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음	8	패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정
li_02	Session timeout 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해	4	600초(10분) 동안 입력이 없을 경우 접속 된 Session 을 끊도록 설정

위험 코드	위험 내용	위험도	보호대책
	내부 정보가 노출될 수 있음		
li_02	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음	12	불필요한 SUID, SGID 파일 제거
li_02	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 변경할 수 있어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있음	12	world writable 파일 존재 여부를 확인하고 불필요한 경우 제거
li_02	UNIX 시스템이 제공하는 Telnet, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고가 발생할 수 있음	8	TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정
li_02	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인해 파일 시스템 악용이 우려됨	8	설정파일에 UMASK 값을 022로 설정
li_02	사용자에게 지정된 디렉터리가 아닌 곳이 홈 디렉터리로 설정될 경우 해당 디렉터리 내 명령어 사용이 가능하며 이에 따라 시스템 관리·보안상 문제가 발생할 수 있음	12	홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는 계정 삭제
li_02	공격자는 숨겨진 파일 및 디렉터리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있음	12	[.]으로 시작하는 숨겨진 파일 존재 여부 확인 후 불법적이거나 의심스러운 파일을 삭제
li_02	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있음	4	Telnet, FTP , SMPT, DNS 서비스를 사용할 경우 설정파일 조치 후 inetd 데몬 재시작
li_02	상위 경로로 이동하는 것이 가능할 경우 하위 경로에 접속하여 상위 경로로 이동함으로써 해킹을 당할 위험이 있으며, 유니코드 버그(Unicode Bug) 및 서비스 거부 공격에 취약해지기 쉬움	12	상위 디렉토리에 이동 제한을 설정한 경우
li_02	불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드로 인한 서비스 불능 상태가 발생할 수 있음	18	파일 업로드 및 다운로드를 제한한 경우
li_02	Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs 디렉터리는	12	DocumentRoot를 별도의 디렉터리로 지정한 경우

위험 코드	위험 내용	위험도	보호대책
	공개되어서는 안될(또는, 공개 될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있어 유출 발생 가능성이 있음		
Ii_02	웹 서버에서 제공하는 default 에러 메시지가 출력되도록 설정되어 있는 경우, 공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 발생되는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있음	12	별도의 에러 메시지를 생성하여 관리
Ii_02	OPTIONS, GET, POST 이외의 다른 HTTP Method를 지원하는 경우, 악의적인 공격자가 임의의 파일을 삭제하거나 업로드 하여 서버의 정상 운영에 지장을 줄 수 있음	8	OPTIONS, GET, POST 이외의 다른 HTTP Method가 설정되어 있지 않은 경우
WIN_01	IIS 웹서비스 정보 숨김 설정이 적용되지 않은 경우 악의적인 사용자에게 불필요한 정보가 노출되어 외부 공격을 위한 기초 자료로 이용될 수 있음	8	웹 서비스 에러 페이지가 별도 지정
WIN_01	게시판이나 자료실과 같이 업로드 된 파일이 저장되는 디렉터리에 CGI 스크립트가 실행 가능하다면 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고의 통로로 이용될 수 있음	4	해당 디렉토리 Everyone에 모든 권한, 수정 권한, 쓰기 권한 제거
WIN_01	로그 파일에는 공격자에게 유용한 정보가 들어있을 수 있으므로 권한 관리가 필요함 일반 사용자에 의한 정보 유출이 불가능 하도록 권한 설정 필요하며, 비인가자가 접근하여 로그상의 중요정보 유출할 수 있음	12	임의의 사용자가 접근 할 수 없도록 권한 설정
WIN_01	공개된 취약점에 노출되지 않은 최신 보안 패치를 적용하지 않으면 exploit 공격, 제로데이 공격 등의 서버 침해가 발생할 수 있음	12	IIS 에 대한 최신의 버전과 패치를 확인 후 업그레이드 및 패치 수행
RDS-01	데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비 인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 존재함	12	DBMS에 불필요한 계정 삭제
RDS-01	주기적인 패스워드 변경이 없을 경우 공격자는 Brute force 공격을 통하여 패스워드를 획득할 위험이 존재함	12	패스워드를 주기적으로 변경하고, 패스워드 정책 적용
RDS-01	데이터베이스의 사용자 계정을 공용 및 공유 사용하게 될 경우, 침해사고 발생 시 책임 추	8	사용자 별 개별 계정을 사용

위험 코드	위험 내용	위험도	보호대책
	적에 영향을 주며, 계정 별 권한 부여가 불가능해지고 사용하지 않는 계정을 이용한 비인가 사용자 접속이 가능함		
RDS-01	일정한 횟수의 로그인 실패 횟수 발생 시 이를 제한하지 않으면 무작위 추측 공격 (Brute force)을 통하여 데이터베이스에 접근이 가능함	8	로그인 시도 횟수를 제한하는 값 설정
RDS-01	설정되어 있지 않은 경우 인가되지 않은 사용자가 이를 이용하여 관련 소프트웨어를 실행할 수 있는 위험이 있음	4	계정의 umask가 022 이상으로 설정
RDS-01	비인가자가 redo 파일, 데이터베이스 설정 파일, 데이터 파일, 네트워크 설정 파일, Oracle 패스워드 관련 파일인 orapw.ora, listener.ora,init<SID>.ora 등의 주요 파일에 접근하여 수정·삭제하면 Oracle 데이터베이스 운영에 오류가 발생함	8	주요 설정 파일 및 디렉터리의 퍼미션 설정
RDS-01	OS_ROLES 설정 파라미터는 데이터베이스 접근 제어로 컨트롤되지 않는 OS 그룹에 의해 grant된 퍼미션이 허락되며, REMOTE_OS_ROLES가 TRUE로 설정되어 있는 경우, 원격 사용자가 OS의 다른 사용자로 속여 데이터베이스에 접근할 수 있음	12	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES설정이 FALSE로 설정
RDS-01	Audit Table은 반드시 SYS, SYSTEM과 같은 데이터베이스 관리자 계정에 속해 있어야 하며, 그렇지 않은 경우 인가되지 않은 사용자가 감사 데이터의 수정, 삭제 등의 수행이 가능함	4	Audit Table 접근 권한 관리자 계정으로 설정

[표 20] 보호대책 선정 결과 (기술)

6.4. 위험 관리 방안

본 위험평가에서는 위험관리수준(DoA)을 6으로 정의하였다.

즉, 위험도가 6 미만인 경우에는 위험을 수용하고 위험도가 6 이상인 경우에 위험경감의 전략 적용을 위해 보호대책을 선정한다.

보호대책의 적용 시 단기 조치 가능한 위험과 중/장기 조치 가능한 위험을 구분하여 대책을 적용한다.

또한, 기술적 취약성에 대한 위험관리 수준을 위험도 6 이상인 것을 우선적으로 조치하고, 단기간 내에 조치가 가능하다고 판단되는 위험에 대해서는 위험도 6 미만의 항목에 대해서도 조치를 수행한다.

단기 조치 가능한 위험 및 중/장기 조치 가능한 위험에 대한 사항을 정리하여 『정보보호 계획서』를 작성하여 위험을 조치·관리한다.