

중소기업을 위한 정보보안경영시스템(IS027001) 가이드라인

2007. 12. 18

목차

- 1. 배경 및 목적
- 2. 구성 및 구축단계
- 3. 구축 방법 소개
- 4. ISO27001 소개

1. 배경 및 목적

1.1 배경

□ 첨단기술 및 중요 정보 유출

- 최근에 첨단기술을 가진 국내 중소기업들에서 정보유출 사건이 빈번히 일어나고 있으며, 그 피해도 심각한 수준임
- 중소기업의 특성상, 한정된 자원과 인원으로 회사업무를 수행하기에도 빠듯한 실정에 보안업무까지 수행하기에는 어려움
- 고가의 외부 컨설팅 의뢰도 현실적으로 불가능

□ 정보보호 관리체계 요구

- 중소기업에서도 정보유출의 예방 및 사건/사고 발생시 신속 대응 체계 구축 필요
- 사건/사고 발생시 피해를 최소화 할 수 있는 정보보호 관리 체계 필요
- 영국에서 이미 1993년도에 정보보안경영시스템에 필요한 베스트프랙티스들을 모아 영국 표준인 **BS7799**를 제정

□ 국제표준으로 제정

- 해킹 사이버테러 및 정보유출 사건/사고가 전세계적인 위협 대두
- 국제표준화 기구인 **ISO**에서 **BS7799**를 기반으로 국제표준인 정보보안 경영시스템 **ISO 27001**을 제정

□ 인증기업의 증가

- **ISO27001** 인증을 획득한 기업이 전세계적으로 5,000여 기업되며, 계속 증가하고 있는 추세
- 국내에서도 삼성전자, 현대자동차 등 글로벌기업으로 성장한 기업들과, 대부분의 은행들을 포함하여 50여 기업이 인증 획득
- 인증기업의 수가 전세계적으로 빠른 속도로 증가

1. 배경 및 목적

1.2 목적

□ 자체적인 보안활동 수립을 지원

- 이미 국내외의 대기업 또는 중소기업인 선진 기업에서 도입하여 널리 사용하여 효과성이 증명된 정보보안경영시스템을 첨단기술을 가진 국내의 중소기업에서 적극적으로 도입을 유도
- 정보보안경영시스템을 자신의 조직에 구현하고자 할 때 외부의 도움을 최소화하고 해당 기업이 스스로 할 수 있도록 지원하기 위함

□ 실제적 내용을 최대한 제공

- 정보보안경영시스템 구축의 각 단계별 수행되어야 하는 업무에 대한 자세한 설명
- 업무 수행에 필요한 양식 및 각종 규정의 예시를 최대한 제공
- 가이드라인을 활용하여 최소한의 수정 등의 노력으로 정보보안 경영시스템 구축을 지원

2.1 구성

본문과 첨부로 구성이 되어 있으며, 본문은 정보보안경영시스템 구축의 각 단계와 이 단계에서 수행되어야 하는 일을 자세히 설명하고 있으며, 첨부에는 본문의 각 단계에서 업무 수행 시 필요한 양식, 규정(예) 등을 제공

정보보호관리체계 구축

정보보호관리체계 실행

인증심사

1단계

2단계

3단계

4단계

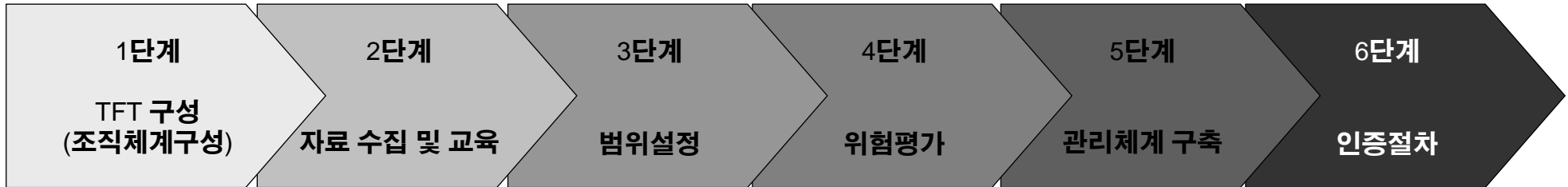
5단계

6단계

구분		내용
본문	1단계	TFT 구성(조직체계 구성) 부문으로 조직의 조직도를 활용하여 정보보호 관련 조직을 구성하는 단계
	2단계	자료 수집 및 교육 부문으로 정보보호관리체계 구축에 첫 번째 단계에서 만들어진 조직체계상의 이해 관계자들에게 관련된 정보의 제공 및 교육을 실시하는 단계
	3단계	범위설정 부문으로 조직의 어느 범위까지 수행할 것인지 설정하는 단계
	4단계	위험평가 부문으로 정보자산이 지니는 취약성 및 위험요소를 정보보호 대상 별로 총체적으로 분석하는 단계
	5단계	관리체계구축(대응책 구현) 부문으로 조직의 정보보호관리체계를 구축하기 위한 선행단계로서 위험분석 결과를 바탕으로 도출된 대응책을 조직 환경에 적용하기 위해서 프로세스를 상세 설계하는 단계
	6단계	인증절차 부문으로 ISO 27001 인증을 준비하는 기업을 위하여 인증 절차를 설명하는 단계
첨부	1장	정보보호 관련 규정 작성을 위한 샘플 지침들을 제공
	2장	위험평가 수행 시 필요한 절차, 평가 방법, 템플릿 및 샘플 위험분석보고서 등을 제공
	3장	정보보호 관리체계(ISMS) 구축을 위하여 선정, 구현중인 ISO 27001의 보안 통제항목을 정의하기 위한 방법 및 샘플 제공
	4장	정보보호관리체계를 수립하기 위한 범위 선정 템플릿 제공
	5장	위험분석 결과를 바탕으로 도출된 대응책을 조직 환경에 적용하기 위해서 프로세스를 상세 설계하는 방법 및 샘플 제공

2.2 구축단계

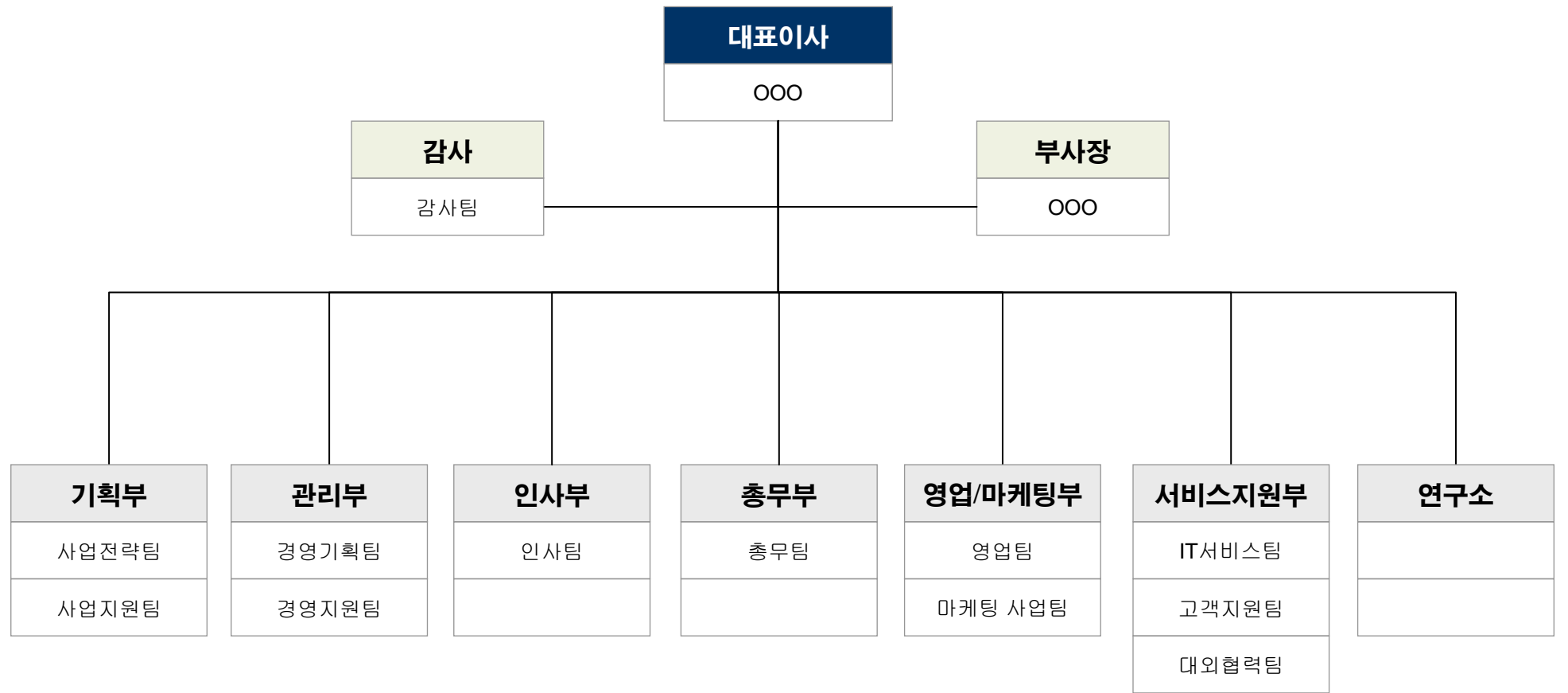
정보보호관리체계를 구축하기 위한 단계는 아래와 같이 크게 6개 부분으로 나누어 볼 수 있음



단계	구축 내용
1	정보보호관리체계 구축에 필요한 조직 체계를 구성
2	관련 자료 수집 및 구성된 조직에 대하여 충분한 교육을 실시
3	단계구축하기 위한 범위선정
4	정보자산에 대한 위협평가를 실시하여 문제점을 도출
5	대응책들을 체계적으로 구성하고 관련 보안 프로세스들을 수립하여 정보보안경영시스템을 설계
6	신뢰할 수 있는 제3의 기관으로부터 인증 획득

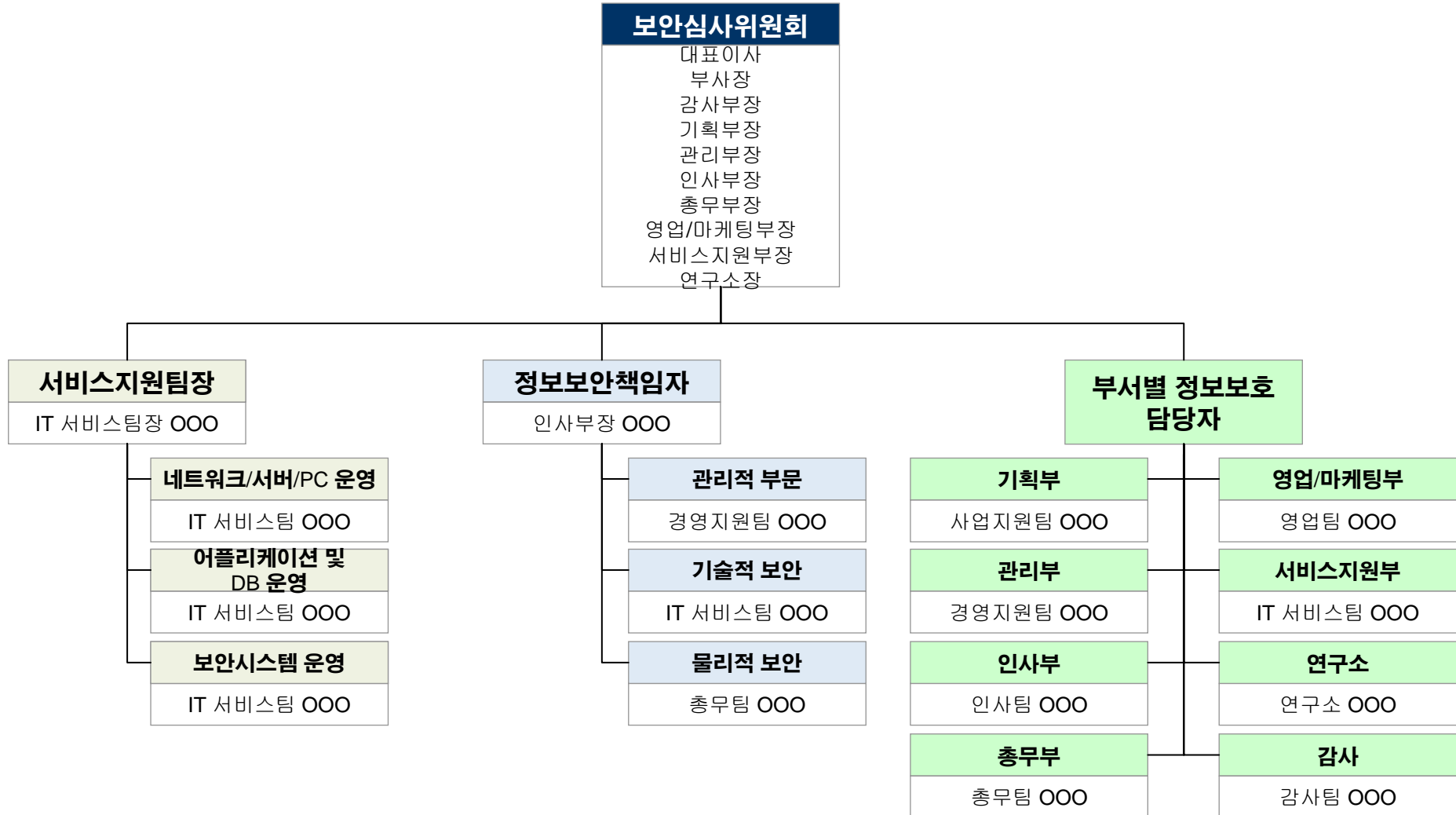
3.1 1단계 – TFT구성 (조직체계 구성)

- 조직 내에서 효과적이며, 효율적인 정보보안 활동을 수행할 수 있는 조직 체계를 갖추
- 회사 조직도(예)



3.1 1단계 – TFT구성 (조직체계 구성)

□ 보안조직도



3.2 2단계 – 자료 수집 및 교육 단계

□ 정보(자료) 수집

- 정보보안경영시스템 구축에 필요한 정보를 수집하기 위해 다음 웹 사이트들을 참고
- 필요 시 정보보호 컨설팅 회사들을 활용하여 조언을 구함

회사	설명
BSI Management Systems (구 BSI Korea, asia.bsi-global.com/Korea)	<ul style="list-style-type: none"> •국제 규격, 테스트, 심사 및 인증 •ISO 27001 인증준비절차 및 인증서비스, 인증 및 심사문의 양식, 규격, 설문서/신청서양식, 관련교육 및 세미나 등
정보보호 관련기관 및 업체	<ul style="list-style-type: none"> •기업의 (기밀)정보를 보호하기 위하여 종합적인 보안 컨설팅을 제공, 인증 컨설팅 관련 자료 및 자문 •컨설팅 업체: 시큐아이닷컴 (www.secui.com), 인포섹 (www.goinfosec.co.kr), 안철수 연구소 (www.ahnlab.com), 안랩 코코넷 (www.coconut.co.kr), 이니텍 (www.initech.com), 에스티지시큐리티 (www.stgsecurity.co.kr), 에이쓰리시큐리티컨설팅 (www.a3sc.co.kr), 인젠 (www.inzen.com), 제이에스시큐리티 (www.jssecurity.co.kr)
산업기밀보호센터 (www.nisc.go.kr)	<ul style="list-style-type: none"> •국가정보원은 2003년 10월에 산업기밀센터를 설립하여 기업의 첨단기술을 보호하고 기업이 안전하게 활동할 수 있도록 지원하기 위한 산업보안 활동을 수행하고 있다. 산업기술의 유출방지 및 보호, 기술유출 현황에 대한 최근 국내발생 산업스파이 사건 분석 및 사례, 보안대책 및 법령정보 등을 제공 •산업보안교육 및 컨설팅, 산업보안 설명회 및 워크숍, 산업보안관련 정책 자료
검찰청 (www.spo.go.kr)	<ul style="list-style-type: none"> •기술유출방지 정보 교류를 위해 정보수사기관 협의회에 구성되어 산업기밀 유출 보호를 위해 기술유출범죄수사센터를 운영하여 기술유출범죄에 대한 체계적·집중적으로 동향을 파악 •신종 기술유출범죄에 대한 효율적인 규제방안 관련 정보
경찰청 (www.police.go.kr)	<ul style="list-style-type: none"> •정보수사기관 협의회에 구성되어 산업기밀보안을 수행 •사이버범죄에 대한 분류, 현황, 관련법규, 범죄사례 및 범죄피해 예방방법 등의 관련 정보
한국정보보호진흥원 (www.kisa.or.kr)	<ul style="list-style-type: none"> •정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위하여 “정보통신망이용촉진 및 정보보호등에 관한 법률 제52조”에 근거하여 설립하였으며, 정보보호를 위한 정책 및 제도의 조사·연구, 정보보호 기술개발, 정보시스템 침해사고 처리 및 대응체계 운영 등을 수행함 •인터넷 침해사고 대응, 불법 스팸방지, 개인정보침해, 정보보호관리체계인증, 보안성 평가 등의 관련 정보

3.2 2단계 – 자료 수집 및 교육 단계

□ 관련교육 실시

- 조직체계상의 이해 관계자들에게 관련된 정보의 제공 및 교육을 실시
- 필요 시 외부 전문교육 실시

구분		설명
내부자체 교육		<ul style="list-style-type: none"> •정보보호의 개요 •ISO 27001 규격에 대한 설명 •정보보호관리체계 구축 절차 등
외부 교육	ISO 27001 선임심사원 과정	<ul style="list-style-type: none"> •ISO 27001(정보보호경영시스템) 심사를 수행할 수 있는 선임심사원 양성 •정보보호의 개요, ISO 27001 요건해설, ISO 27001 심사계획 및 수행(문서심사, 본심사), 심사수행을 위한 Case Study •(Workshop) 및 과정시험
	ISO 27001 실무추진자 과정	<ul style="list-style-type: none"> •ISO 17799/ ISO 27001 (BS7799-2002) 규격에 준하는 정보보호경영시스템 구축, 인증 및 운영을 담당하는 실무자 및 내부감사를 수행할 핵심요원을 대상으로 정보보호경영시스템 전 과정 운영, 감사의 방법론을 학습 •ISO 17799 / ISO 27001(BS 7799-2)의 핵심요구사항 해설 •ISO 19011:2002에 규정된 내부감사 Best Practice 학습 •정보보호경영시스템 내부감사의 계획, 실행 및 보고 방법론 습득 •정보보호 및 적합성 준수의 중요성 인식 •내부감사를 통한 정보보호 통제의 지속적 개선의 달성에 대한 노하우 공유 •정보보호경영시스템 운영의 시정 및 예방조치 실행의 기대효과 •PDCA Process •ISMS의 적합성 및 효과성 평가 방법 그리고 인증준비 및 취득 과정

3.3 3단계 – 범위설정 단계

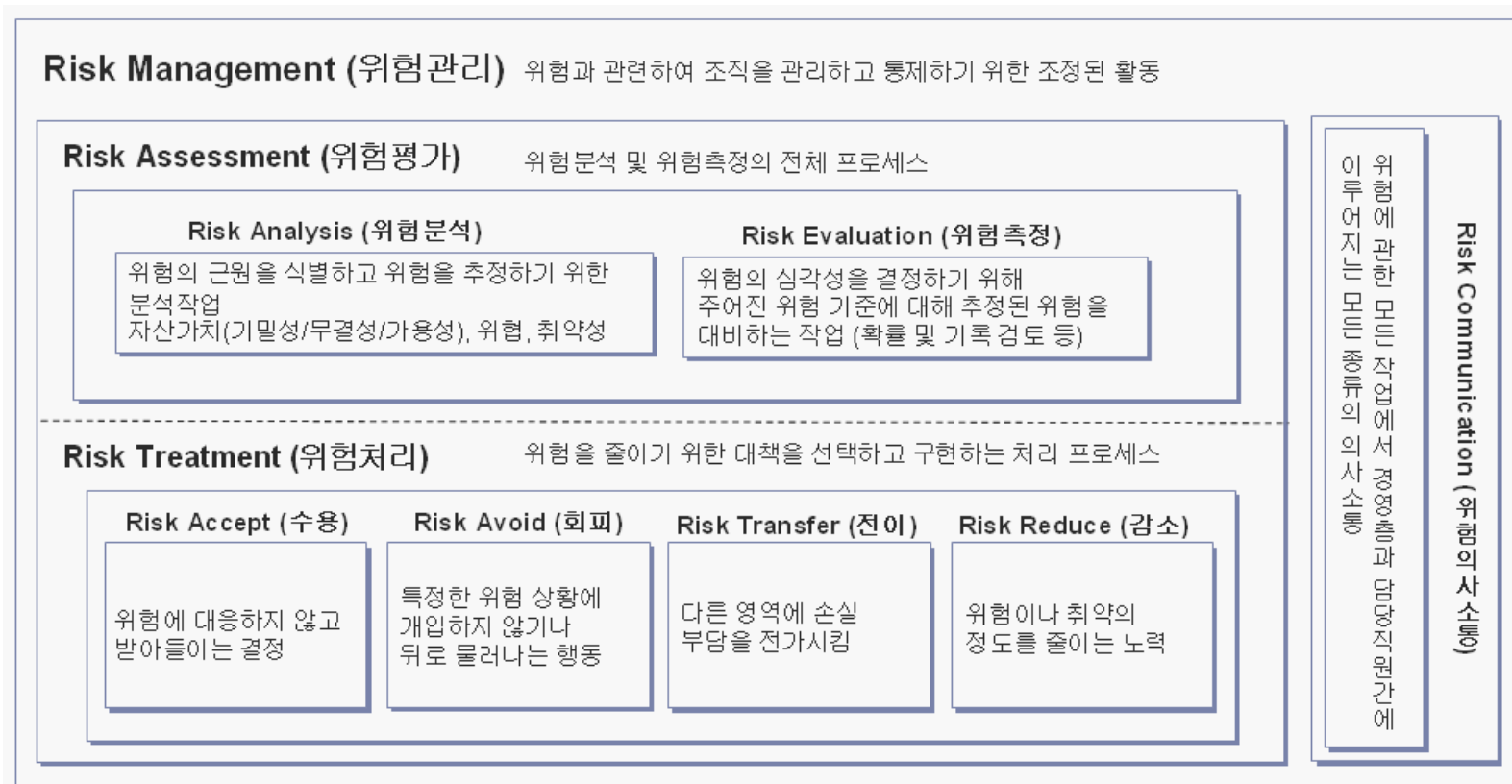
정보보호관리체계 구축 시 조직의 어느 범위까지 설정하여 수행할 것인지 정의하는 부분으로 세 가지의 대상 관점에서 논의될 수 있음

구분	설명	장담점	
전사관점	조직의 전체를 대상으로 범위 설정	장점	<ul style="list-style-type: none"> •향후 전사적인 확산에 애로사항이 없으나 일부만 한 경우 전사적인 확산이 매우 어려움 •최소한의 법칙에서 벗어날 수 있음, 즉, 일부만 한 경우 하지 않은 부분에서 지속적인 사고 발생 가능성이 높음
		단점	<ul style="list-style-type: none"> •비 협조 및 저항 예상 •프로젝트 관리의 위험성 증가 •프로젝트 기간의 중기화 (6개월 ~ 9개월 소요)
특정부서의 관점	중요 정보를 취급하는 연구소와 같이 특정 부서를 대상으로 범위 설정	장점	<ul style="list-style-type: none"> •저항의 최소화 •프로젝트 관리의 용이 •프로젝트 기간의 단축으로 인한 결과 및 성과를 빨리 제공할 수 있음 (약 3개월 소요)
		단점	<ul style="list-style-type: none"> •향후 전사적인 확산에 애로사항 발생 •보안의 특성상 해당(특정)부서에서 부정적 의견을 더 많이 내어 놓는 경향이 있음
중요 정보의 유통 단계별 관점	특정 정보의 생산, 유통, 저장 및 폐기의 전 단계를 대상으로 범위 설정	장점	<ul style="list-style-type: none"> •비 협조 및 저항 예상 •프로젝트 관리의 위험성 증가 •프로젝트 기간의 중기화 (6개월 ~ 9개월 소요)
		단점	<ul style="list-style-type: none"> •향후 전사적인 확산에 애로사항 발생 •보안의 특성상 나머지는 보안의 중요성이 낮다고 보고 확산을 하지 않음 •중요정보의 모든 유통단계가 다 파악되어 대책이 수립되었다고 확신하기 어려움

3.4 4단계 – 위험평가 단계

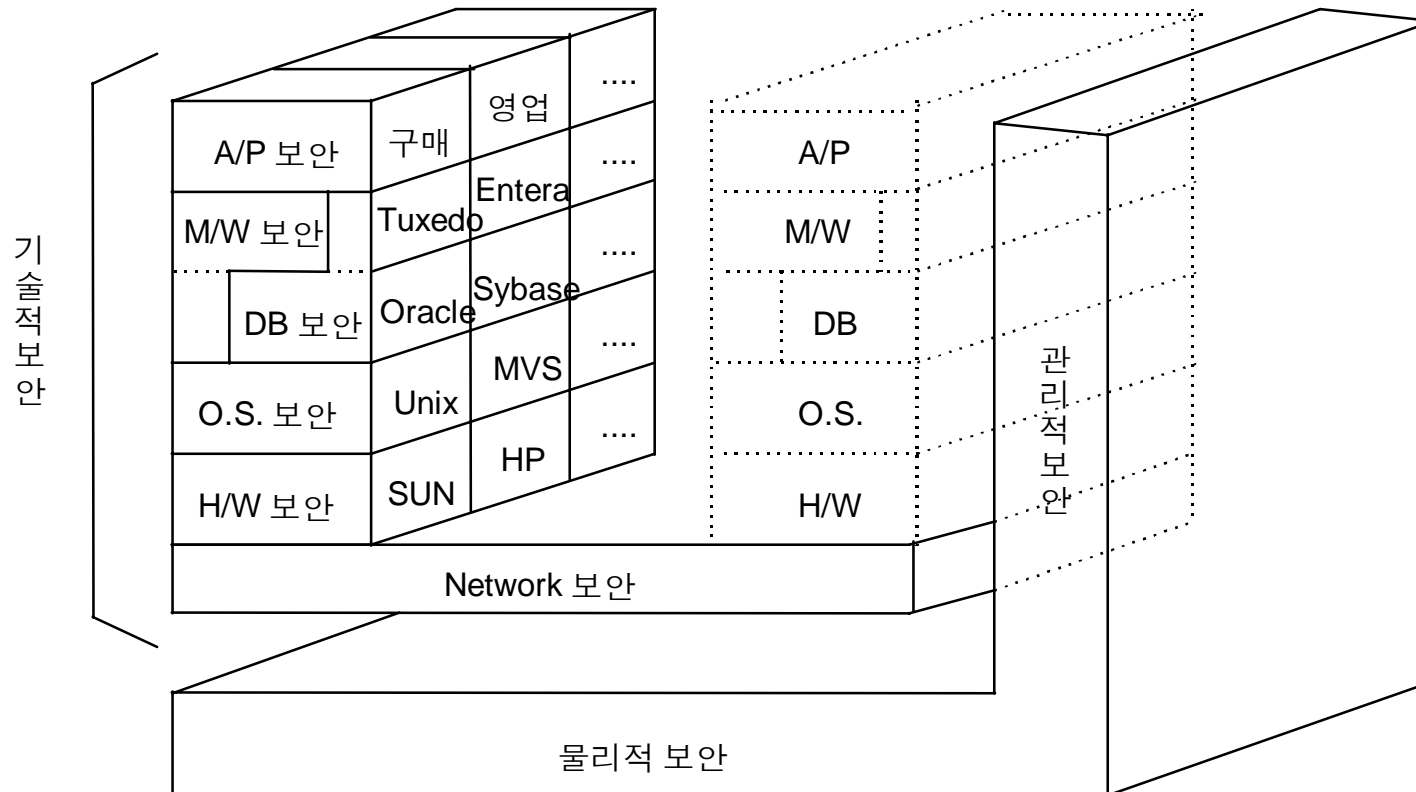
□ 위험관리

- 위험평가와 위험처리로 구분되면 위험 평가된 결과를 토대로 조직의 위험 처리를 수행하는 것이다. 경영층과 담당자간의 원활한 소통을 위한 위험의사소통이 있음



3.4 4단계 – 위험평가 단계

□ 보



3. 구축 방법 소개

3.4 5단계 – 관리체계 구축

□ 관리적 보안

- 조직 구성
- 보안 정책/지침/규정/절차 수립
- 보안 프로세스 정립

□ 물리적 보안

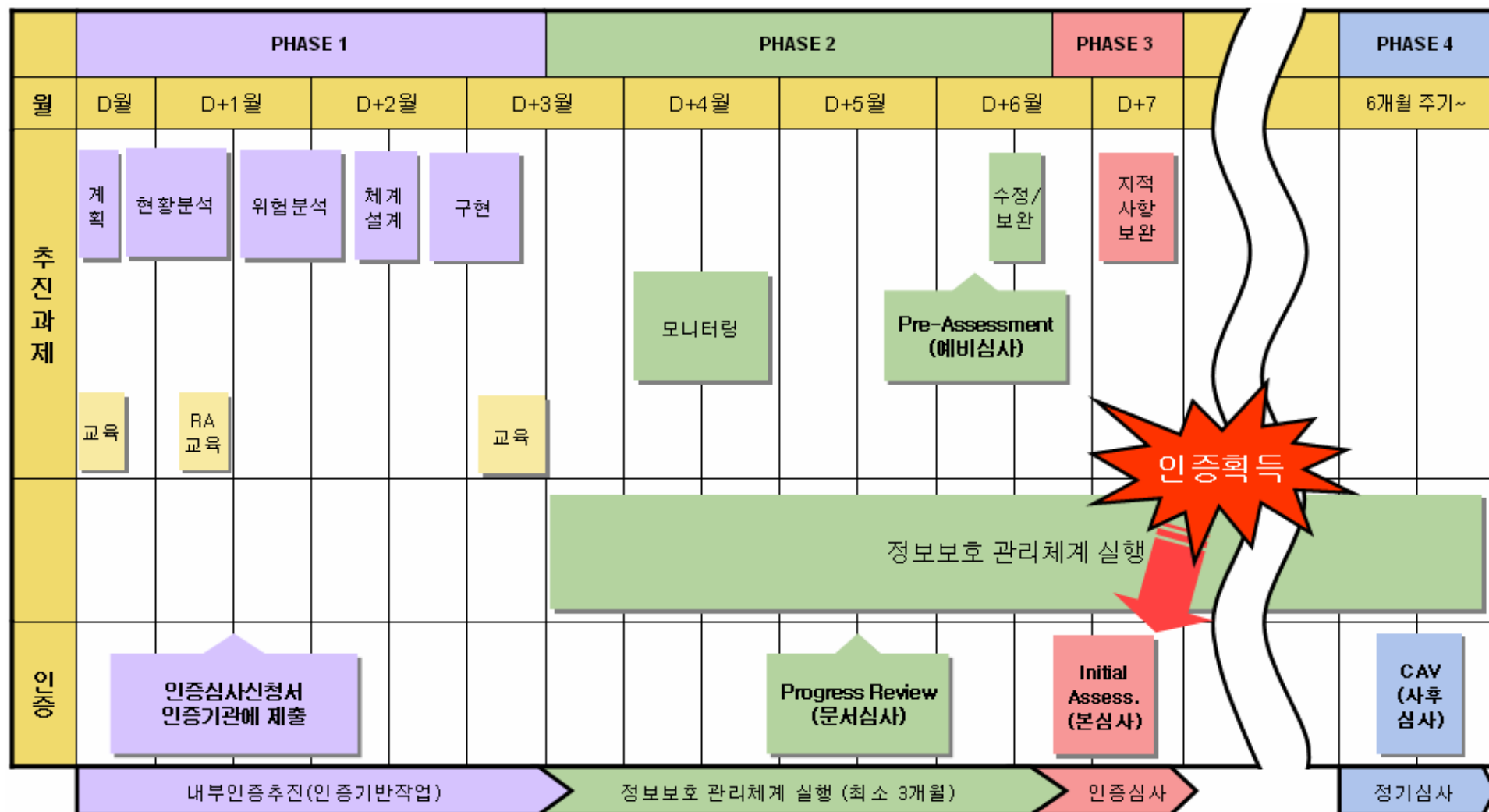
- 출입 통제
- 천재지변/자연 재해에 대비한 비상 대책

□ 기술적 보안

- 네트워크 보안
- 시스템 보안
- DB/응용시스템 보안
- PC보안
- 보안 솔루션 도입

3. 구축 방법 소개

3.4 6단계 – 인증 절차



4.1 11개 통제 영역//38개 통제 목표/133개의 통제항목

항목	설명
정보보안 방침 (Security policy)	정보보안에 대한 경영방침과 지원사항에 대한 통제구조 확인
정보보안 조직 (Organization of Information Security)	조직 내에서 보안을 효과적으로 관리하기 위한 보안조직 구성 및 책임과 역할에 대한 규명
자산 관리 (Assets management)	조직의 자산에 대한 분류 및 이에 따른 적절한 보호 프로세스 검토
인적 자원 보안 (Human resources security)	사람에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 위험을 감소하기 위한 대응방안 확인
물리 및 환경 보안 (Physical and environment security)	비 인가된 접근, 손상과 사업장과 정보에 대한 영향을 방지하기 위한 대응책 여부
의사소통 및 운영관리 (Communication and operations management)	정보처리 설비의 정확하고 안전한 운영을 보장하기 위한 대응방안 존재 여부
접근통제 (Access control)	정보에 대한 접근통제를 하기 위한 대응책 여부
정보시스템 인수, 개발 및 유지보수 (Information system acquisition development & maintenance)	정보 시스템 내에 보안이 수립되었음을 보장하기 위한 대응방안 존재 여부
정보보안 사고 관리 (Information security incident management)	정보 시스템과 관련된 정보보안 사고와 취약점이 허용된 시기 이내에 적절한 교정 행동과 의사가 전달되는지 여부
사업 연속성 관리 (Business continuity management)	사업활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업활동을 보호하기 위한 프로세스 존재 여부 검토
부합성 (Compliance)	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보안 요구사항의 불일치를 회피하기 대응책 여부

[표 6-1] ISO27001의 11개 통제 영역

5.1 보안 정책/지침/규정/절차



5.2 위험 분석 방법

전략기획팀

자산명	전략기획 정보	자산구분	정보/문서	자산가치	비밀성(C)	무결성(I)	가용성(A)
					2	2	2
위험		취약성			위험도		
위험요소	Value	취약성 요소	Value		C	I	A
외부인에 의한 정보 유출	M(2)	사무실공간에 대한 인력 접근 통제 가 안됨	H(3)	7			1-1
내부인에 의한 의도적 정보 유출	M(2)	이 메일을 통한 정보 유출 가능성	H(3)	7			1-2

구매팀

자산명	단가정보	자산구분	정보	자산가치	비밀성(C)	무결성(I)	가용성(A)
					3	2	2
위험		취약성			위험도		
위험요소	Value	취약성 요소	Value		C	I	A
바이러스 감염에 의한 파일서버 저장 데이터 손실	H(3)	보안 인식 부족하여 바이러스 백신 업데이트를 주기적으로 하지 않음	H(3)	9	8	8	4-1
시스템 장애에 의한 데이터 손실	L(1)	시스템 불안정으로 인한 DB 손실	L(1)			4	
내부자에 의한 정보변경	L(1)	ERP MM 모듈의 사용자 계정 공유 로 인하여 데이터 실제 입력자 확인 불가능	H(3)		6		
		보안인식 부족으로 암호 설정된 화 면보호기 미 사용	M(2)		5		
데이터 입력 오류	L(1)	사용자 부주의로 인하여 키보드에 이물질 접촉으로 인한 입력 오류 발 생 가능	M(2)		5		
문서 분실	M(2)	문서 관리 부실로 인한 분실 우려 존재	M(2)	7		7	4-2

5.3 적용성 보고서 (SOA, Statement of Applicability)

보안통제 항목	Adopted Y, N, P or N/A	구현 현황	Reference
5. 보안 방침			
5.1 정보보안 방침			
5.1.1. 정보보안 정책서			
정보 보안 정책 문서는 관리에 의해 승인되어 출판되고 직원들 및 관련 된 외부 부서들로 전달되어야 한다.	Y	ISMS 정책서가 제정되어 최고책임자인 CEO 가 승인하였으며, 그룹웨어에 저장되어 모든 임 직원이 열람할 수 있도록 되어 있음.	정보보호정책서
5.1.2 정보보안 정책문서의 검토			
정보 보안 정책은 계획된 간격으로 또는 지속적인 적합성, 타당성과 유 효성을 보장하기 위하여 중요한 수정이 발생했을 때 검토되어야 한다	Y	최소 1년에 한번 검토	정보보호정책서 제44조

11. 접근 통제			
11.1 접근 통제에 대한 업무 요구 사항			
11.1.1 접근 통제 방침			
접근 통제 정책은 수립되어 문서화되어야 하며 접근을 위한 업무 요구 사항과 보안 요구사항을 기반으로 검토되어야 한다.			
11.2 사용자 접근관리			
11.2.1 사용자 등록			
모든 정보 시스템과 서비스의 접근에 대한 허가과 취소가 적절하게 이루어지는 정식 사용자 등록과 말소 절차가 있어야 한다.			

Q&A

감사합니다