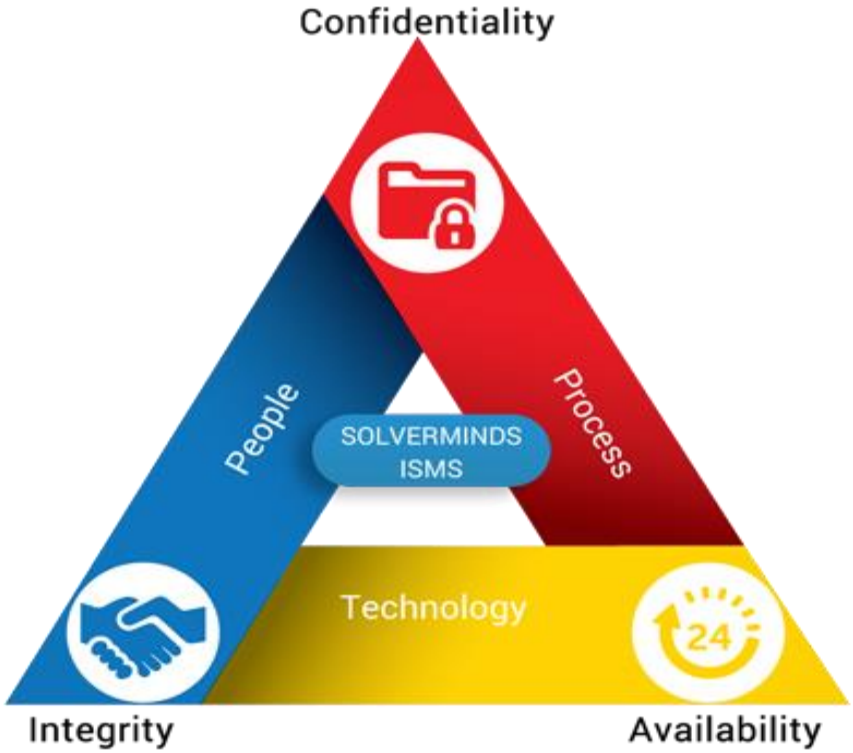
2장. 정보보호 관리체계 개론



목차

목차

1.1 정보보호 관리체계 이해

정보보호의 속성

속성	설명
효과성(Effectiveness)	비즈니스프로세스에 관련성 있고 타당하고 사용 가능한 정보라야 한다는 것
효율성(Efficiency)	최적의(가장 생산적이고 경제적인) 자원 활용을 통해서 정보를 제공하는 것
기밀성(Confidentiality)	민감한 정보를 불법적인 유출로부터 보호하는 것
무결성(Integrity)	정보의 정확성 및 무결성, 일관성
가용성(Availability)	필요한 때에(적시에) 정보가 사용 가능하다는 것
준거성(Compliance)	사업에 적용될 수 있는 법률, 규정, 계약사항 등과 같이 외부적으로 부과된 경영 기준, 그리고 내부 정책 등을 준수하는 것
신뢰성(Reliability)	경영진이 조직을 운영하고, 주주에 대한 책임(수탁책임)을 수행하기 위해 필요한 적절한 정보, 즉 타당하고 믿을 수 있는 정보를 제공하는 것

※ 준거성 (Compliance)
준거(準據): 기준(基準)이나 근거(根據), Compliance: (법 · 명령 등의)준수

1.1 정보보호 관리체계 이해

정보자산 분류표

정보 유형	설명
데이터	전산화된 정보로 문서파일, 데이터파일(개인정보, 산업기밀, 영업기밀 등)로 분류
소프트웨어	패키지 소프트웨어, 시스템 소프트웨어, 응용프로그램 등
서버	공용자원을 갖고 여러 사용자에게 서비스를 제공하는 시스템
시설	건물, 사무실, 데이터 센터 등의 물리적 시설
인력	소유자, 관리자, 사용자, 운영자, 개발자 등 정보시스템 관련 인력
무형 자산	기업이미지, 업무프로세스, 특허 및 지적재산권 등

1.1 정보보호 관리체계 이해

정보보호 핵심 원칙

정보보호

정보의 기밀성, 무결성, 가용성의 유지

기밀성	접근을 허가받은 자만이 정보에 액세스할 수 있도록 확실히 할 것
무결성	정보 및 처리방법이 정확하고 완전하도록 보호할 것
가용성	허가된 이용자가 필요시에 정보 및 관련 자산에 접근할 수 있도록 할 것

1.1 정보보호 관리체계 이해

정보보호 필요성

- 사회 전반에 ICT 의존도 증가 →사이버 위협의 영향이 커지고
- IT 발전에 따른 새로운 기술의 등장 → 국가 및 기업 全 분야로의 IT 위험성 확대

새로운 기술의 등장

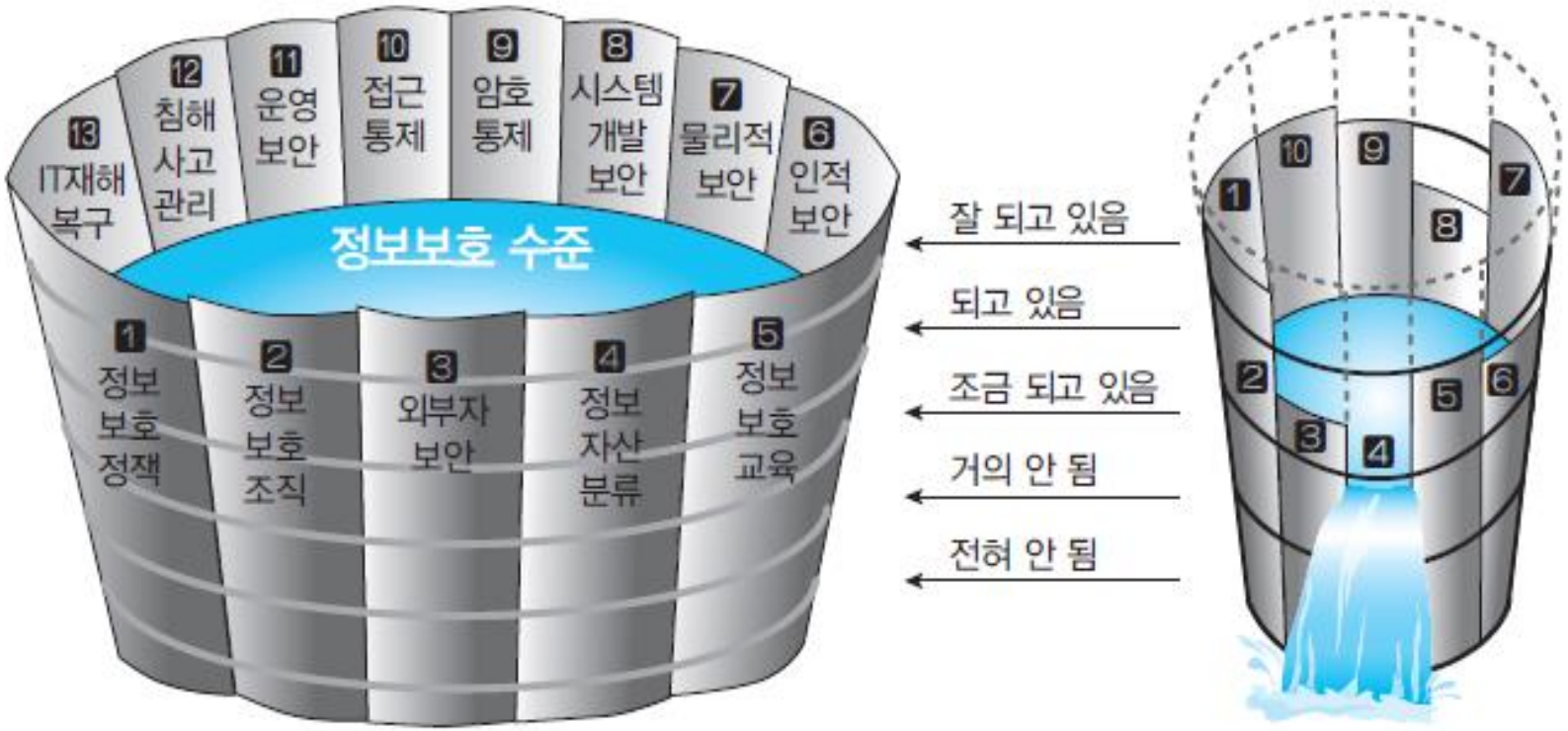
네트워크 고도화 GbE, 10GbE & 4G Network	Smart Phone
	Tablet Device
유비쿼터스 환경 IPv6, USN, Internet of Things	Cloud Computing
	Machine-to-Machine
전사회적인 디지털화 집적성, 편재성, 연결성 증가	SCADA System
	Smart Grid
전통산업과 IT의 결합 제어시스템/자동차/전력망 + IT	Smart Building
	Smart Car

전분야로의 IT 위험성 확대

디지털 디바이스의 증가 및 유비쿼터스화	유무선 전세계 네트워크화, IT 기술의 사회적 편재성 증가
IT 기술의 대형화/융합화/디지털컨버전스화	기술간 결합도와 복잡도 증가
국가기반시설의 정보 네트워크화 경향	IT기술의 사회적 중요성 증대 및 의존도 심화
새로운 IT 기술 및 서비스의 증가	다양성, 예측불가능성 증가

1.1 정보보호 관리체계 이해

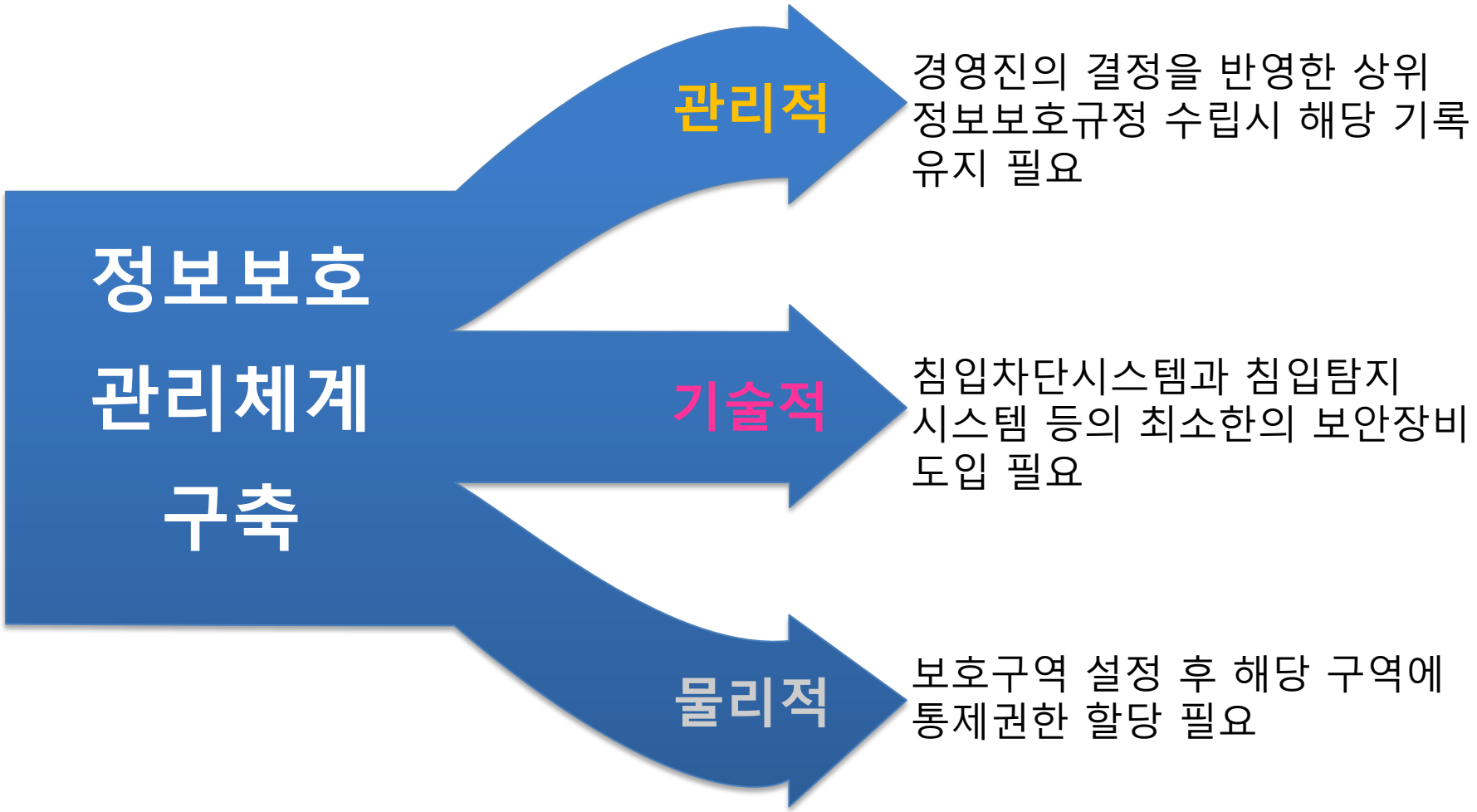
리비히(Liebig)의 최소율(最小律)의 법칙(法則)



나무물통의 법칙: 물이 통에 담기는 양은 다른 나무 판자의 길이에 상관 없이 길이가 가장 짧은 판자에 의해 결정된다.

1.1 정보보호 관리체계 이해

• 구축 간 고려사항



1.1 정보보호 관리체계 이해

정보보호의 특성

✓ **100% 정보보호는 달성될 수 없다.**

- 많은 투자와 연구를 하여도 완벽한 보안이란 있을 수 없기 때문에 투자 대비효과를 고려한 보안 적정선을 설정

✓ **사용자의 편의성을 제한한다.**

- 정보보호의 보안성과 편의성은 반비례적이어서 보안의 강도가 높아질 수록 사용자의 불편을 초래

✓ **가시적인 이익을 얻을 수 없다.**

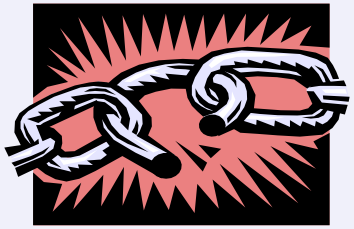
- 투자에 따른 이익을 계산하기가 힘들기 때문에 이를 기획하기가 쉽지 않음
- 최고 경영자가 지니고 있는 정보보호의 필요성에 대한 확고한 의지로 극복 가능

✓ **다단계의 복합 대책 구현 시 위험이 크게 감소한다.**

- 방화벽이나 암호화 적용 등과 같은 특정 솔루션에 의존하기 보다는 포괄적으로 커버 될 수 있는 정책 마련 필요

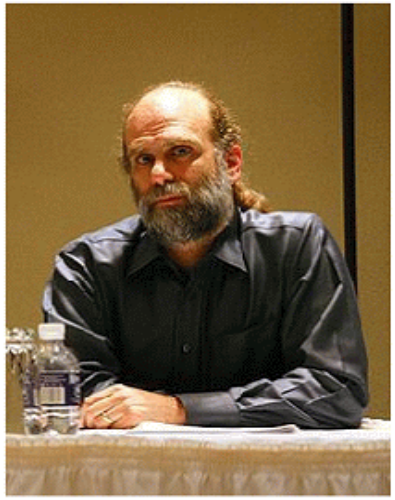
1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 필요성



- "Security is a process, not a product"
  - 보안은 제품(기술)이 아니라, 프로세스이다.
- "Security is a chain; it's only as secure as the weakest link"
  - 보안은 사슬이다. 사슬의 가장 약한 고리만큼만 안전하다.
  - 정보보호란 사슬처럼 연결되어 있어서 전체 정보보호 수준은 가장 취약한 연결 부분의 수준을 넘을 수 없다는 것
- 완벽한 보안은 없다. 그러나 보안은 .. 있다"
  - 완벽한 보안이 불가능해도 최선을 다 해야 하며, 그것은 보안에 대한 올바른 인식으로부터 출발

-미국의 정보보호 전문가인 브루스 슈나이어(Bruce Schneier)저서 비밀과 거짓말(Secrets and Lies)'에서 -



▲ 브루스 슈나이어 박사

1.1 정보보호 관리체계 이해

보안 담당자의 어려움

보안 사고 및 위협 증가
사고유형 다양, 첨단, 대형화

경영진의 보안인식 부족
보안 지식 부족

보안 업무 급증
보안 비용 급증

보안 조직·인력 부족
보안 예산 부족

개인정보법 등
준수해야 할 법규 증가

현업부서의 비 협조
보안은 잘해야 본전

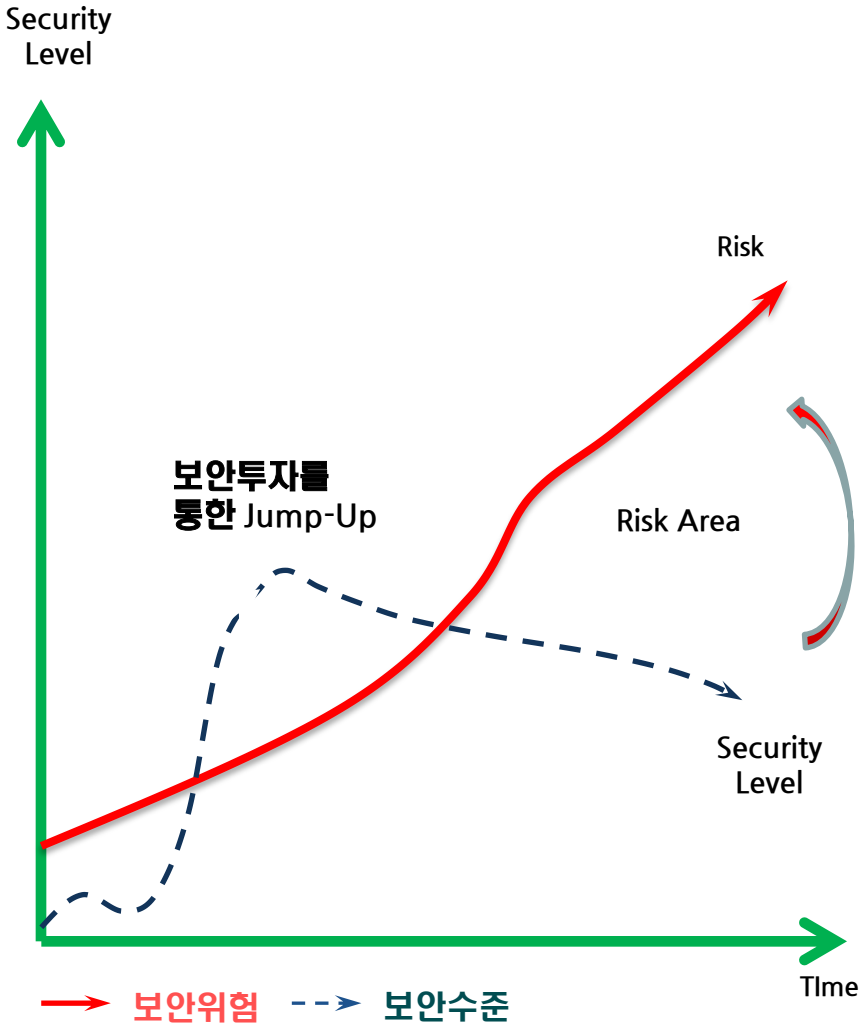
1.1 정보보호 관리체계 이해

보안사고 사례로 본 시사점 (정보보호 디자인 필요)

1. 정보보호는 경영의 문제로 CEO의 참여와 관심, 의지가 중요
2. 정보보호 최고책임자 지정(CISO), 겸직 금지
   - 이해관계 상충 시 정보보호 가치의 훼손 없이 의사결정
3. 기술적, 관리적, 물리적 보호대책을 종합한 **체계적이고 지속적인 위험관리 기반의 정보보호 관리체계 수립**
4. 정보보호 업무 전담 독립된 조직 구성
   - 사전 통제 및 감사추적, 업무성과를 위해 내부통제 느슨
5. 전 직원 대상 교육훈련 프로그램 운영
6. 보안관리 전략 수립 및 보안 프로그램 운영

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 필요성



● Risk 증가요인

- Asset의 증가로 인한 새로운 Risk 발생
- Vulnerability의 관리 소홀로 인한 Risk 증가
- 외부 Threat의 증가로 인한 Risk 증가
- 환경 변화로 인한 새로운 Hole의 발생

최소의 투자로 기업의 보안을 안심할 수 있는 해결책은?

- 지속적인 보안에 대한 관심
- 취약점 점검통한 최적의 해결책
- 조직원에 대한 보안 의식 함양
- 보안 시스템 구축

정보보호 관리체계 구축

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 필요성

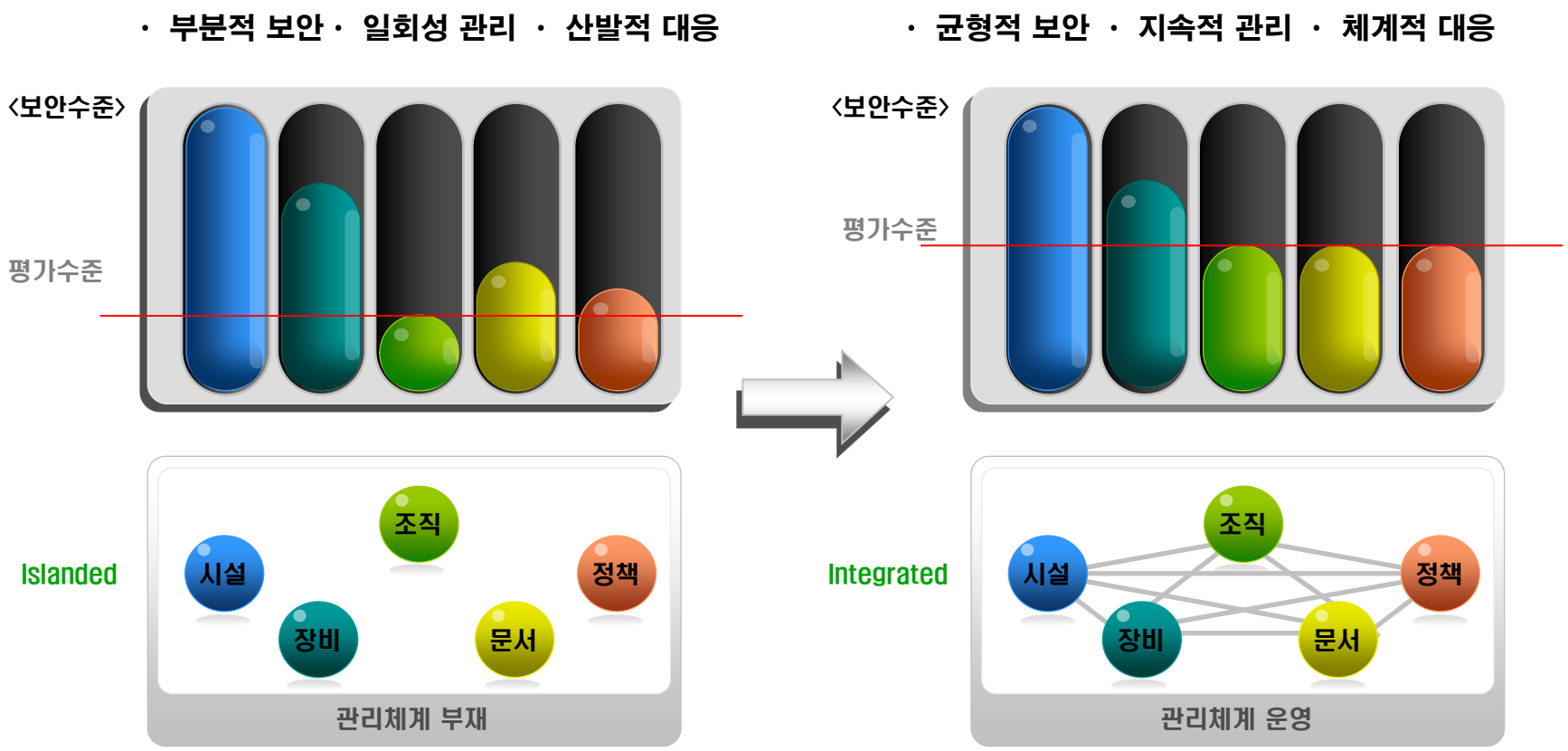
- 많은 위협과 위험에 대응하기 위해

- 보안에 대한 위협과 위험을 분석하여 체계적인 관리가 필요

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 정의

- **조직에서 비즈니스의 연속성 확보를 위하여** 각종 위협으로 부터 정보자산을 보호하기 위한 **위험관리** 기반의 **체계적**이고 **지속적**인 **프로세스** 개선 활동



ISMS
(Information Security Management System)

1.1 정보보호 관리체계 이해

관리체계

- 일반적으로 관리체계 (Management System)는 PDCA(Plan-Do-Check-Act) 사이클 기반으로 실행된다.

- 정보보호 관리체계란, 정보보호에 관한 관리체계이며 조직의 내부통제 시스템으로 '위험 관리' 와 동일한 개념이라 해도 과언이 아니다.

- 본서에서 언급되는 정보보호 관리체계(이하 "관리체계" 라 한다)는 국내 공통 표준 프레임워크로 ISMS(Information Security Management System)는 물론, PIMS(Personal Information Management System) 등의 프레임워크를 통칭하는 용어로 사용

- 관리체계에서는 조직 및 기업에서 취급하는 '대상' 의 형태를 불문하고 그 조직 또는 기업의 중요한 자산으로써 '정보자산' 이라는 개념을 사용한다. 기업 내에 있는 다양한 '정보자산' 이 유출되거나 조작되거나, 도난 당하는 위험을 방지하는 설비와 대책을 개선 · 관리하기 위한 규칙을 정하고, 안전하게 사업을 전개하는 것이 정보보호 관리체계이다.

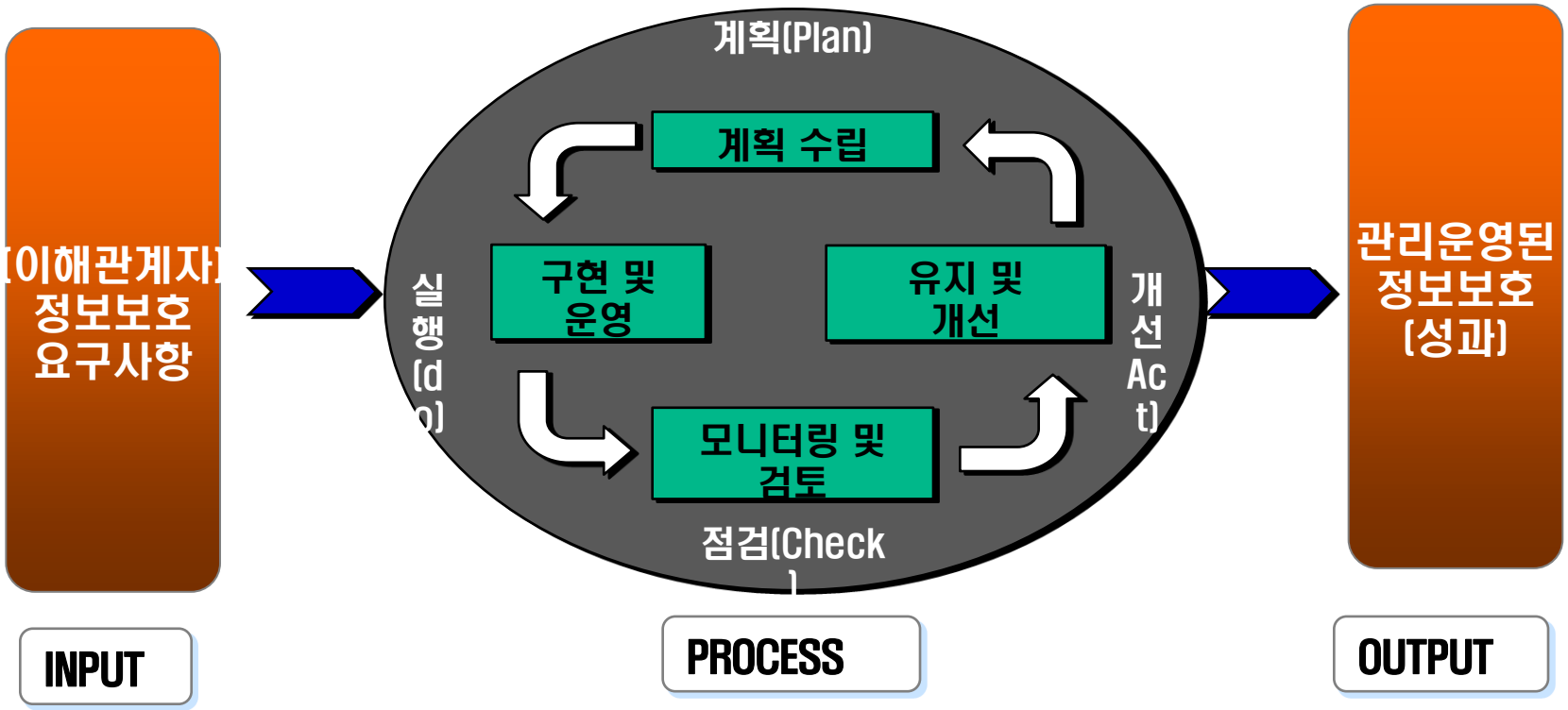
1.1 정보보호 관리체계 이해

프로세스 접근방법

- 프로세스: 입력을 출력으로 변환하기 위해 경영자원을 이용하여 운영,관리하는 모든 활동
- ISMS의 기본 철학인 관리방법으로 프로세스 접근방법을 활용하며, 이를 이행하기 위한 개념으로 'PDCA 모델' 을 제시
- 이해관계자의 정보보호 요구사항 및 기대를 Input으로, 이들의 요구사항 및 기대를 충족시키는 정보보호의 결과(운용·관리된 정보보호)을 Output으로 이끌어 내기 위해 필요한 활동 및 프로세스를 ISMS 프로세스
- 조직의 사업활동은 Input이 처리되어 Output으로서 가치를 낳는 프로세스의 연속인 것처럼 ISMS에서도 PDCA 사이클에 의해 정보보호의 계속적 개선을 추구하는 프로세스 접근방법인 매니지먼트 시스템

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 프레임워크



- ISMS구축을 일련의 프로세스로 간주하여 각각의 프로세스를 프로세스 접근방법에 따라 명확화하고, 상호관계를 파악하여 시스템화하여 운영 관리하는 접근방법

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 프레임워크

Plan-계획 (ISMS 구축)	조직의 전반적인 비즈니스와 연계하여 정보보호 정책, 목적, 프로세스 등 수립
Do-실행 (ISMS 도입 및 운영)	정보보호 정책, 관리방안, 프로세스 등 도입 및 운영
Check-점검 (ISMS 모니터링 및 검토)	정보보호 정책, 목적 및 실제경험에 비추어 본 프로세스의 성과평가 및 그 결과검토를 위한 경영진에 대한 보고
Act-개선 (ISMS 유지 및 개선)	ISMS의 지속적인 개선을 위한 ISMS의 내부감사 및 관리검토 결과 또는 시정조치 및 예방조치 실시

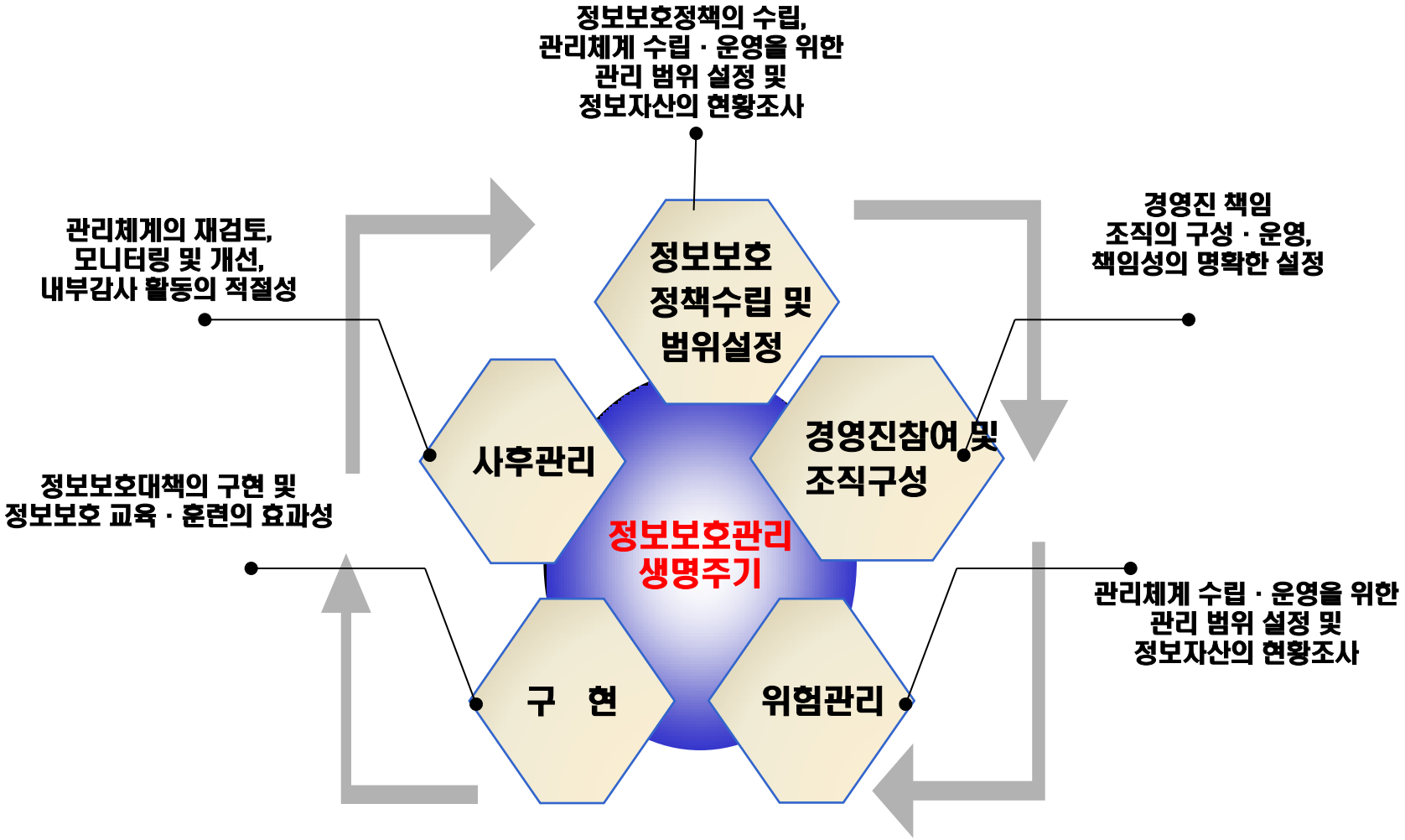
1.1 정보보호 관리체계 이해

국내 공통표준 프레임워크와 일반적인 PDCA 비교

국내공통 표준 프레임워크(ISMS)	PDCA 모델
정보보호 정책 수립 및 범위설정	계획(Plan)
경영진 책임 및 조직 구성	
위험관리	
구현	실행(Do)
사후관리	점검(Check)
	개선(Act)

1.1 정보보호 관리체계 이해

정보보호 관리체계(ISMS) 프레임워크



1.1 정보보호 관리체계 이해

관리체계 인증 취득의 이점

- 조직의 정보보호 인식 제고
- 종합적이고 효과적인 정보보호대책의 적용
- 위험의 감소
- 침해사고에 대한 피해 최소화
- 기업 체질의 강화와 조직의 지속성장 및 비즈니스 확대
- 고객 만족 및 신뢰도 향상, 경쟁사와 차별화
- 입찰 및 거래 조건 충족
- 범규 준수(컴플라이언스)
- 기업의 사회적 책임 및 공헌

※ 인증: 공인되고 객관적인 제3자가 기업의 관리체계 운영의 적절성에 대해 인증심사 과정을 거쳐 증명하여 주는 것

ISMS 인증 취득 혜택

구분	시행기관	혜택 내용	근거
가산점 부 여	산업통상부	공공부문 정보시스템 기획.구축.운영 사업자,SW개발사업자 선정 시 평가항목(기밀보안) 만점 부여	지경부 고시 제2010-53호
	산업통상부	보안관제 전문업체 지정 시 평가항목(신뢰도) 만점 부여	지경부 공고 제2010-478호
	KISA	정보보호대상, 입찰, 과제선정 평가 시 가점 부여	KISA 지침
	신용평가 기관	한국신용평가정보의 기업신용평가 시 가점 부여	업무 협약 (공문)
	한국기업지배구조원	상장기업 대상 ESG(환경, 사회, 지배구조) 평가 시, 소비자항목에 가산점 부여	업무 협약 (공문)
요금 할인	보험사	정보보호관련 보험(배상책임보험 등) 가입 시 할인(AIG, LIG, 그린손해보험, 동부화재, 롯데손해보험, 메리츠화재, 삼성화재, 제일화재, 한화손해보험, 현대해상, 흥국화재)	업무 협약 (공문)
권고	교육부	원격교육설비기준에 ISMS 인증 취득 권고	교과부 고시 제2008-93호
	국토교통부	유비쿼터스도시기반시설에 대하여 ISMS 인증 취득 권고	유비쿼터스 도시의 건설 등에 관한 법률 제22조
ISMS 인증 수수료 할인	KISA	정보보호 大賞 수상 기업의 경우 할인 (대상.우수상.특별상, 100~50%)	KISA 지침
		소규모 기업의 경우 할인(상시 근로자 수 50명 미만 또는 매출액 50억 미만, 50%)	

정보보호 관리체계(ISMS) 구축 운영상의 어려움

① 관리체계의 수립 및 운영은 기술적인 문제라기보다는 프로세스와 사람이 연계된 문제

② 정보보호와 관련된 조직/책임/역할/권한이 불분명하고 협조체계가 미흡

③ 기업내에 관리체계의 핵심요소인 위험 관리의 기법들이 제대로 활용되고 내재화되지 않음

④ 관리체계의 운영은 장기간의 꾸준한 유지보수 활동을 요구

⑤ 관리체계에 대한 주기적인 감사와 측정이 부족

⑥ 강력한 추진요인이 필요한데 이러한 추진요인을 확보하기 어려움

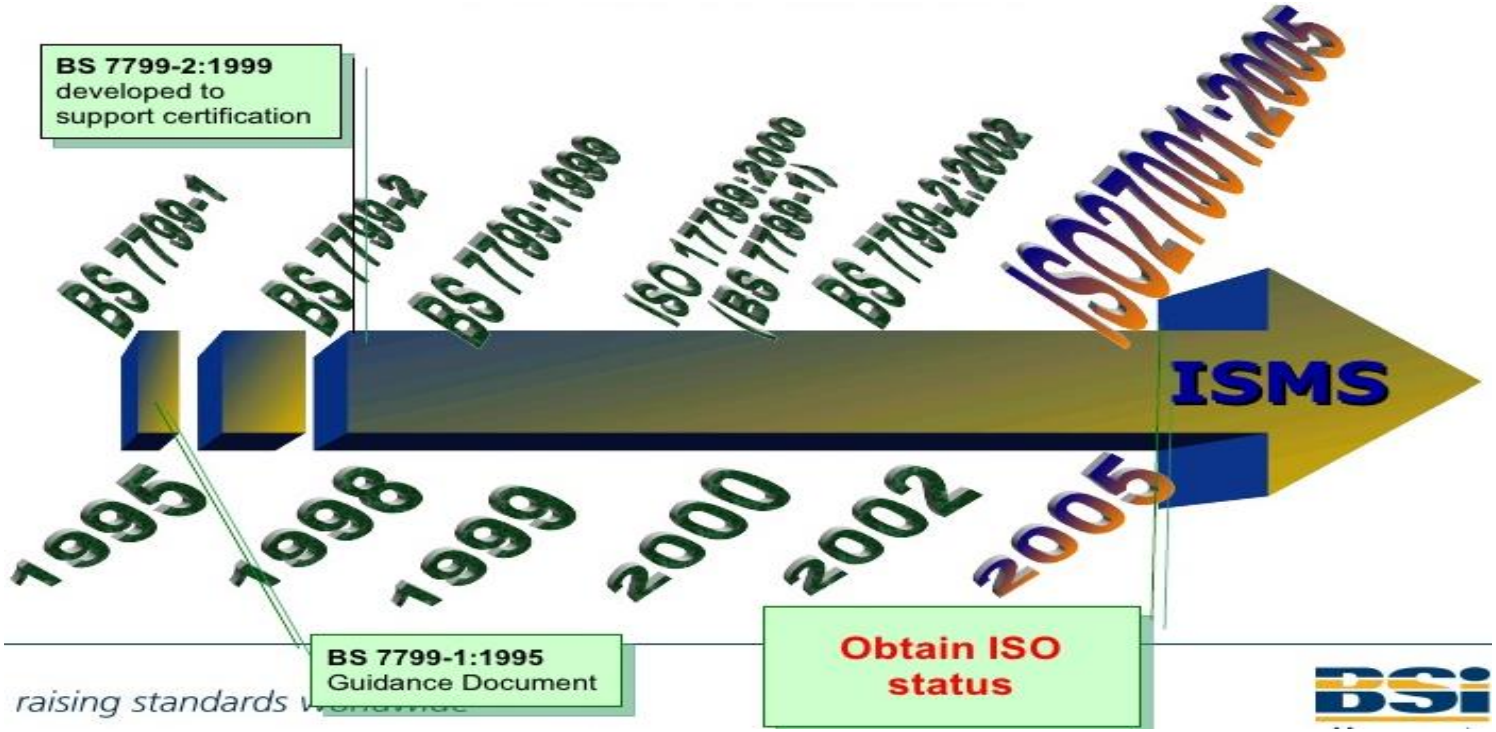
⑦ 경영층의 지속적인 의지, 강력한 추진요인이 없다면 포기하기 쉽고 유지되기 어려움

1.2 정보보호 관리체계 분류

ISO/IEC 27001(국제표준 정보보호 관리체계)의 이해

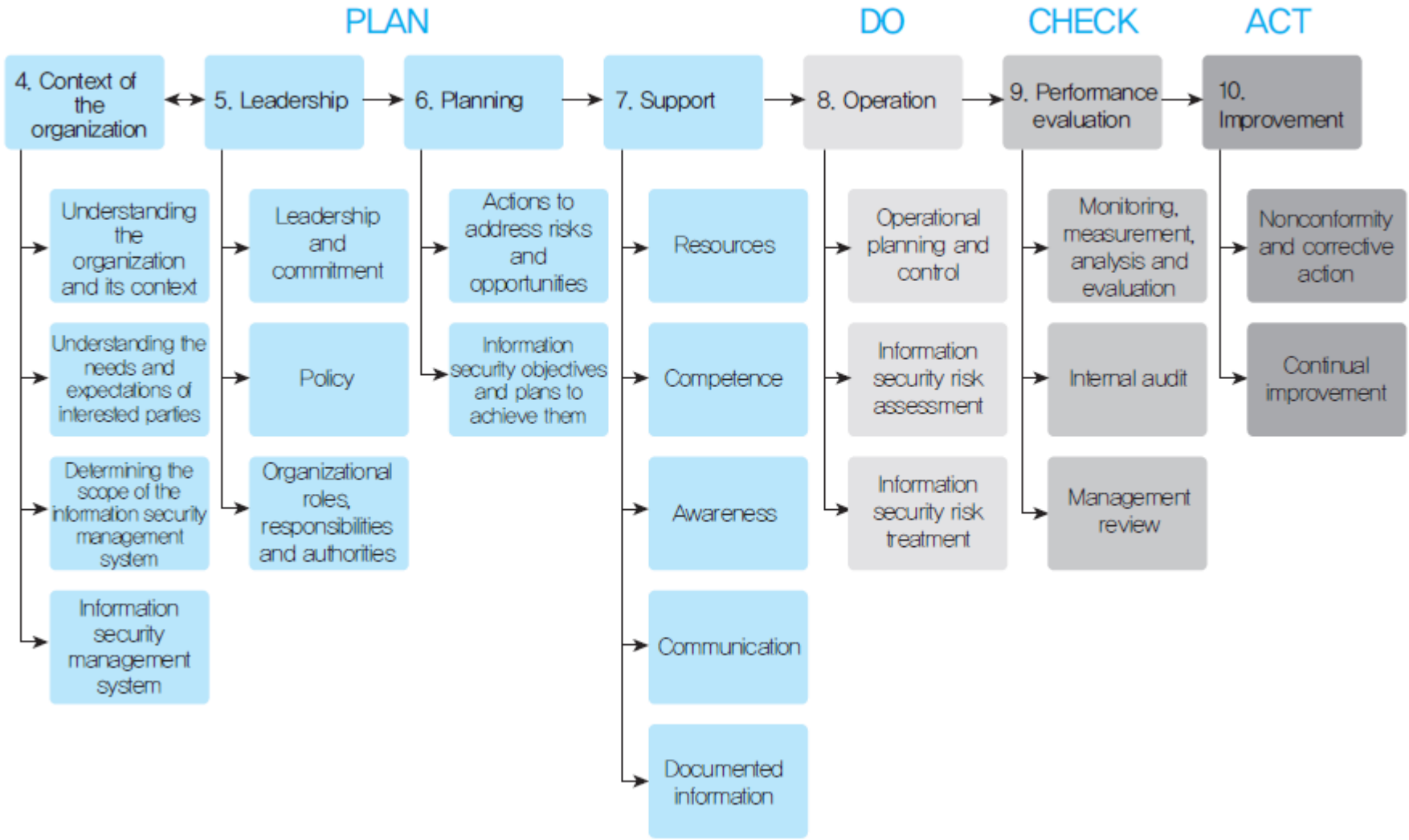
- ISO/IEC 27001은 1995년도에 영국이 자체 개발한 BS7799(Part1, Part2)를 국제표준으로 상정하여 2005년도에 국제 표준인 ISO/IEC27001과 ISO/IEC27002로 표준화되었다.

- ISO/IEC 27001:2013 개정판에서는 기존 ISO/IEC 27001:2005의 통제항목 11개 영역 137개에서 통제항목 14개 영역 114개로 개정되었다.



1.2 정보보호 관리체계 분류

ISO/IEC 27001:2013 프레임워크



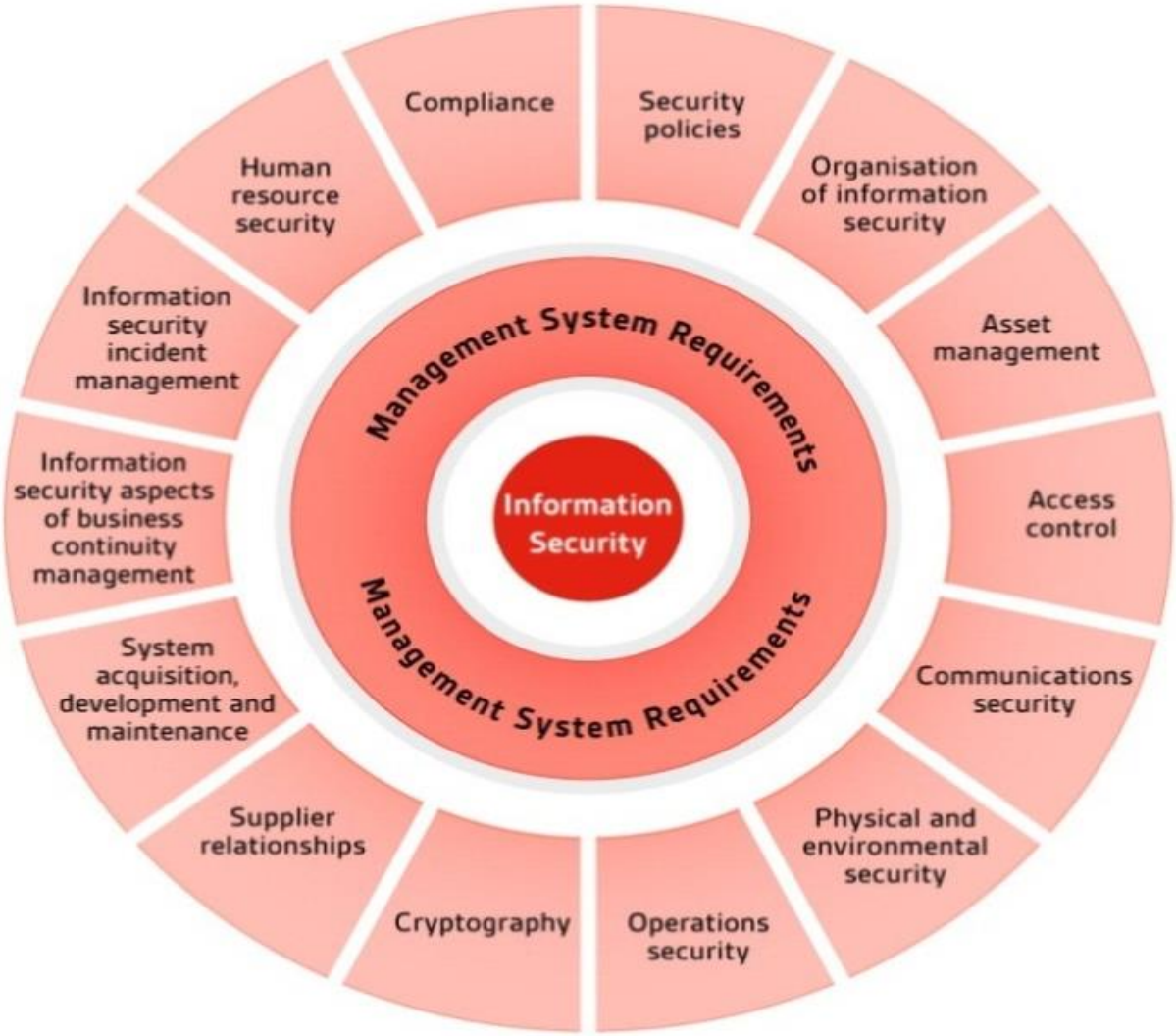
1.2 정보보호 관리체계 분류

ISMS와 ISO27001 프레임워크 비교

국내 ISMS	ISO27001(2013 개정안)
정보보호 정책 수립 및 범위설정	Policy
경영진 책임 및 조직 구성	Leadership, Context of the organization
위험관리	Planning
구현	Support
	Operation
사후관리	Performance evaluation
	Improvement

1.2 정보보호 관리체계 분류

ISO/IEC 27001(정보보호 관리체계 통제영역)



출처: http://blog.naver.com/PostView.nhn?blogId=n_privacy&logNo=80195220578

ISO 27001 통제 영역 및 항목들

정보보호영역	통제항목	통제항목 수
정보보호 정책	정보보호 정책	2
정보보호 조직	정보보호 조직 구성	7
인적자원 보호	내부조직, 외부기업, 고용 전, 고용기간, 고용 변경 및 종료	6
자산 관리	자산책임, 정보 분류	10
접근 통제	접근통제 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근통제, 운영시스템 접근통제, 접근통제, 모바일컴퓨팅	14
암호화	암호 통제 정책, 키관리 등	2
물리적 정보보호	정보보호구역, 정보처리설비정보보호	15
운영관리	운영절차와 책임, 제3자 서비스관리, 시스템계획과 인수, 악성 및 이동, 코드로부터 보호, 백업, 네트워크 정보보호 관리,매체취급, 정보교환, 전자상거래서비스, 모니터링	14
통신 보안	네트워크 정보보호 관리,매체취급, 정보교환, 전자상거래서비스, 모니터링	7
정보시스템 도입.개발 및 .유지보수	정보시스템, 정보보호 요구사항, 어플리케이션의 정확한 처리, 암호통제, 시스템파일 정보보호, 개발프로세스 정보보호, 기술적취약성관리	13
위탁관리	공급자 보안 정책, 계약(SLA), 서비스 모니터링 및 검토, 변화관리 등	5
정보보호 사고관리	정보보호사건보고, 정보보호 사고관리	7
업무연속성 관리	업무연속성관리	4
준거성	법적 요구사항 준거, 적합성 준수, 정보보호감사 고려사항	8
총계		114

ISO/IEC 27000 Family

ISO 과제 번호	제목
ISO/IEC 27000	Overview & vocabulary
ISO/IEC 27001	Information Security Management Systems Requirements
ISO/IEC 27002	Code of practice for information security management
ISO/IEC 27003	ISMS Implementation guidelines
ISO/IEC 27004	ISMS measurement
ISO/IEC 27005	Information Security Risk management
ISO/IEC 27006	Requirements for certification body of ISMS
ISO/IEC 27007	Guidelines for ISMS auditors
ISO/IEC 27008	Guidelines for ISMS controls audit
ISO/IEC 27010	ISM for Inter-sector communications
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002(x.1051/27011)
ISO/IEC 27013	Guidelines on integrated implementation of ISMS & ITSM
ISO/IEC 27014	Governance of information security * 한국 제안
ISO/IEC 27015	ISM for financial services
ISO/IEC 27016	ISM-Organizational economics
ISO/IEC 27017	Cloud computing security and privacy

1.2 정보보호 관리체계 분류

국내 정보보호 관리체계

정보보호 관리체계(ISMS) 개요

- 국내 공통 표준 관리체계 프레임워크는 슈하트 사이클 또는 데밍 사이클이라고 하는PDCA(Plan, Do, Check, Act) 경영관리의 순환 주기(Management 사이클) 기법을 정보보호에 적용하였다.

- 이는 어떠한 일이든 계획을 세우고 실행하면서 그 일이 잘 되었는가를 평가하고, 그 결과를 새로운 계획에 반영하거나 개선활동을 통한 환류 체계가 이루어져 조직 성과가 좋아진다는 개념으로 PDCA 모델을 기반으로 정보보호 관리 순환 주기를 개발 하여 S PDCA (Security PDCA)로 5개 프로세스로 설계하였다.

- 개발된 관리체계 모델은 국내 보안관리 공통 표준 및 정보보호 컨설팅 방법론으로 활용하게 되었다.

1.2 정보보호 관리체계 분류

국내 관리체계 인증 제도를 도입하고자 했던 초기 배경

- 당시 영국의 정보보호 관리 표준문서인 BS7799는 프로세스 관점의 경영시스템으로는 부족하였다.
- 국가의 정보보호 정책은 특정 국가의 표준보다는 국내 환경을 반영한 국가 정보보호 정책이 반영된 모델이 필요하였다.
- 외국 인증기관, 인증심사원, 컨설팅 업체 등으로부터 국내 시장을 보호하고, 해외 인증기관으로 기업 정보 유출 및 국부 유출을 막고자 하였다.
- 국내 기업의 정보보호 수준 향상을 위해서는 경영진의 참여와 전 직원들의 동참하는 전사적인 의식 개혁이 필요하였다.
- 기업지속성장을 위한 기업 비즈니스와 정보보호를 연계하는 경영시스템을 접목 시키고자 하였다.
- 국가의 정보보호 수준 제고를 위한 효율적이며 효과적인 접근방법인 정보보호 프레임워크제시가 필요하였다.
- 국내 기업에서 전략적이며 체계적으로 정보보호 관리 활동을 할 수 있는 모델을 보급하고자 하였다.
- 국내 정보보호 컨설팅 등 정보보호 서비스 산업을 활성화하고자 하였다.

1.2 정보보호 관리체계 분류

<표 1-11> 관리체계 인증 제도 도입 추진 경과

제도화 법개정 주요 내용	추진 일시
정보보호 관리체계 인증 제도 법제화(정보통신망법 개정)	2001.01.
정보보호 관리체계 인증기준 고시 및 지침 공표	2002.05.
정보보호 관리체계 인증심사 본격 시행	2002.08.
정보보호 안전진단 제도 도입(정보통신망법 개정)	2004.01.
전자정부 정보보호 관리체계 인증 제도 도입	2010.6
정보보호 관리체계 인증 제도 의무화 도입(정보통신망법 개정)	2012.12.(시행 2013.2.18)
정보보호 관리 등급제 및 개인정보보호 관리체계 인증 제도 도입(정보통신망법 개정)	2012.12.(시행 2013.2.18)
정보보호 관리체계 인증기준 개정안 고시 공표	2013.2.17
정보보호 안전진단 제도 폐지 및 정보보호 관리체계 인증 제도 의무화 시행	2013.2.18

1.2 정보보호 관리체계 분류

관리체계 모델 개발 방향 및 취지

- 국내의 정보기술을 포함한 조직이나 환경적인 측면을 반영하고자 노력
- 국제흐름을 반영하고 국내실정에 적합한 새로운 정보보호관리 표준개발
- 일반 조직에서 쉽게 활용 가능토록 개발
- 조직 규모나 형태 등 상관없이 모든 조직 및 산업에서 유연하게 적용 가능토록 개발
- 관리적인 부분뿐만 아니라 기술적인 부분을 강화하고 문서화 작업의 최소화
- 국내 정보보호 컨설팅 업체들이 활용할 컨설팅 방법론으로도 고려
- 국내 정보보호 관리 표준화와 향후 국제 표준화를 고려

1.2 정보보호 관리체계 분류

국내 공통 표준 관리체계(ISMS) 모델 특징과 주요내용

- 관리체계 프레임워크는 조직이 관리체계를 수립, 운영, 모니터링 및 검토, 유지 및 개선을 위한 경영기법인 PDCA 모델 적용
- 조직의 정보보호를 관리하기 때문에 많은 활동을 명확히 한 프로세스 접근(Process Approach) 방식을 도입
- 프로세스의 상호관계를 파악하여 시스템으로 적용하여 운용 · 관리
- 조직의 정보보호 요구사항을 이해하고 정보보호 정책 및 목적 수립의 필요성 이해
- 조직의 사업 위험 전반에 대해 고려하여 정보보호 위험을 운영 · 관리하기 위한 관리 방법을 도입 · 운영
- 관리체계의 성과 및 유효성을 모니터링하고 검토
- 객관적인 평가를 통해 지속적인 개선
- 우리나라가 제안하여 국제표준으로 제정된 정보보호 거버넌스 개념을 반영

1.2 정보보호 관리체계 분류

국내 보안관리의 표준, 기본 틀, 공통 프레임워크

- ISMS는 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적 · 기술적 · 물리적 보호조치를 종합한 것으로, 조직의 관리체계를 효과적으로 수립하도록 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.

- 이는 새로운 정보보호 위협 및 취약점이 점차적으로 증가하는 시점에서, 조직의 주요 정보자산을 보호하기 위해 정보보호 관리 절차 및 과정을 전사적인 차원에서 체계적이고 지속적으로 관리하기 위한 **국내 보안관리 모델의 효시이며 구축 지침서, 컨설팅 방법론으로 활용되고 있다.**

- 특히 그 동안 국내 조직에서 단편적이고 일회적이며 산발적으로 대응하던 침해사고 예방에 대해 보다 체계적이고 종합적이고 균형적인 관리체계가 무엇보다 시급하였다. 이에 방법론을 제시하고자 개발되어 국내조직에 적합한 표준적인 정보보호 관리 모델을 제시하여 국내 정보보호 수준제고와 정보보호 서비스 산업 활성화를 가져왔다.

- **ISMS는 현재 국내관리체계 ISMS, PIMS, 개인정보 영향평가 등의 공통 프레임워크로 기본 틀이 되었다.**

1.2 정보보호 관리체계 분류

관리체계 공통 표준 프레임워크

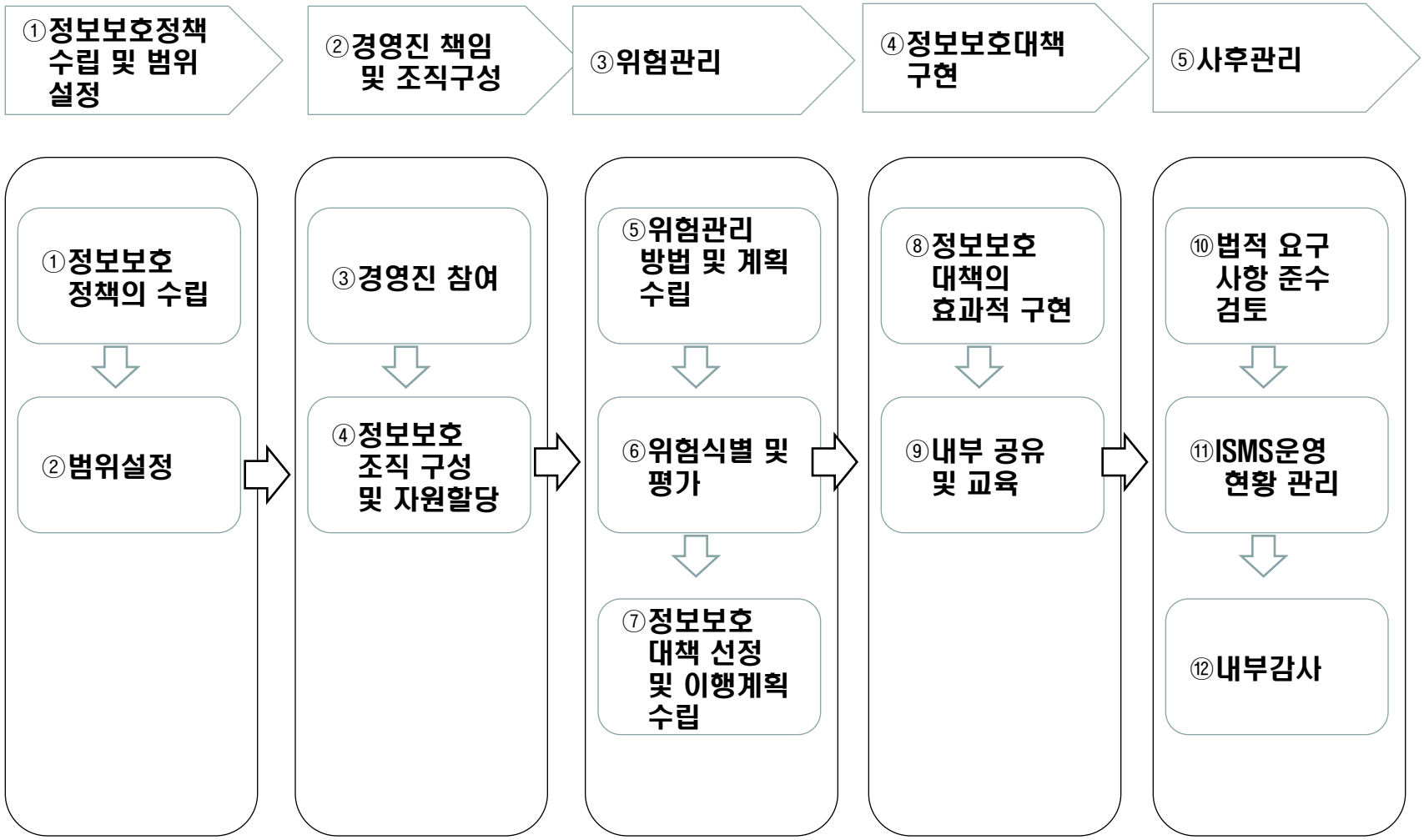
- 조직의 비즈니스와 연계한 정보보호 활동을 융합하기 위하여 경영이론인 경영사이클(Plan-Do- Check-Act)에 기초한 5단계 정보보호 관리과정인 S(Security) - PDCA를 고안 개발하여 관리체계 공통 프레임워크로 활용되고 있으며, 현재의 국내 표준 모델인 ISMS가 2013년 개정을 통해 그림 1-11이 탄생하게 되었다.

- 기본적으로 정보보호 관리체계는 5개 보안 관리사이클(S-PDCA)의 정보보호 관리 전 과정을 정의하고 있으며, 관리과정의 각 단계별 구현 전략과 통제항목 선택 등 누구나 쉽게 각각의 과정별 단계별 구축 방법을 제시하였다.

- 국내 최초로 개발한 정보보호 관리체계는 개발 당시 정보보호에 대한 문제를 조직의 비즈니스와 연계하고자 하였던 것이 기본 사상으로 관리과정을 S-PDCA(Security PDCA)로 정의하고 국내 표준으로 채택하여 활용하게 되었다. 국내 모든 조직에서 활용 가능하도록 철저하게 위험 분석 기반으로 설계되었으며 국내 법규준수사항에 대한 컴플라이언스 대응을 위해 통제항목을 구성하고 관리과정뿐만 아니라 경영진 책임 및 역할 강화, 성과 측정 등 정보보호 거버넌스 적용 모든 통제항목에 S-PDCA 기법을 적용한 것이 특징이다.

1.2 정보보호 관리체계 분류

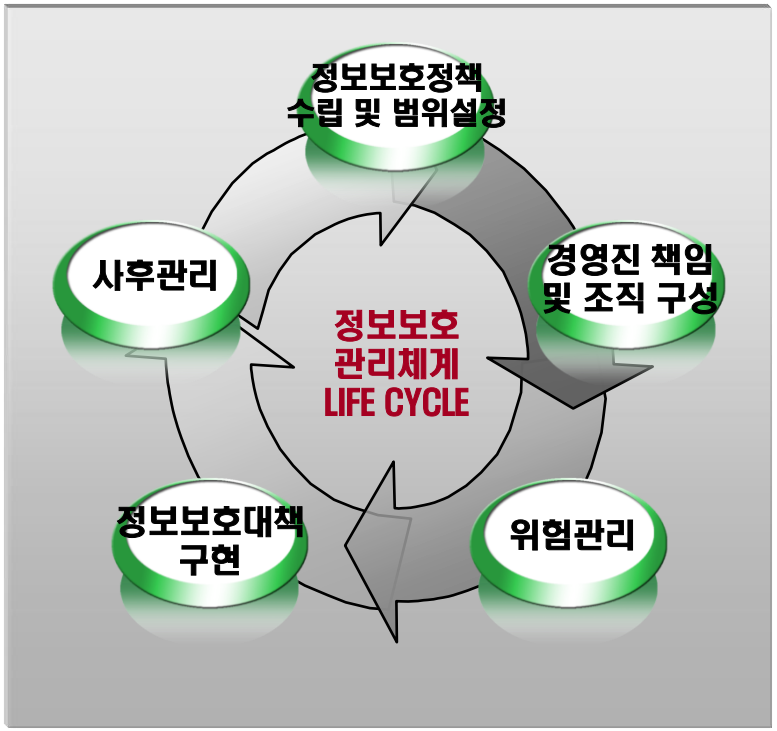
<그림 1-11> 관리체계 공통 프레임워크



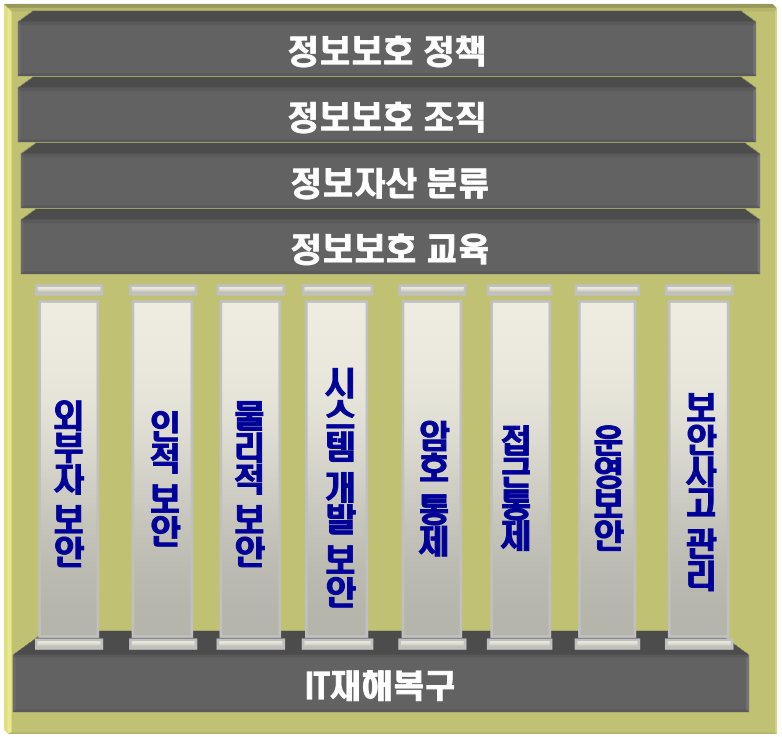
ISMS 인증 모델

ISMS 인증기준

1. 정보보호관리과정[5단계, 12개 통제사항]



2. 정보보호대책[15개 분야, 92개 통제사항]



ISMS 인증 기준

분야		통제항목 수	세부점검항목
정보보호 관리과정 (구축단계)	1. 정보보호 정책 수립 및 범위설정	2	4
	2. 경영진 책임 및 조직구성	2	4
	3. 위험관리	3	11
	4. 정보보호대책 구현	2	3
	5. 사후관리	3	6
정보보호대책	1. 정보보호 정책	6	13
	2. 정보보호 조직	4	7
	3. 외부자 정보보호	3	4
	4. 정보자산분류	3	7
	5. 정보보호 교육	4	10
	6. 인적 정보보호	5	11
	7. 물리적 정보보호	9	21
	8. 시스템 개발 정보보호	10	22
	9. 암호통제	2	8
	10. 접근통제	14	46
	11. 운영정보보호	22	56
	12. 침해사고 관리	7	14
	13. IT재해복구	3	6

1.2 정보보호 관리체계 분류

국내 ISMS 인증 체계

- 현재의 국내 ISMS 인증 체계는 과학기술정보통신부가 인정기관 역할을 수행하고 있으며 인증기관으로 한국인터넷진흥원(KISA)이 수행하고 있다. 인증심사원은 KISA에서 양성 · 관리하고 있으며, 인증기관(KISA)이 인증위원회를 운영하고 있다.

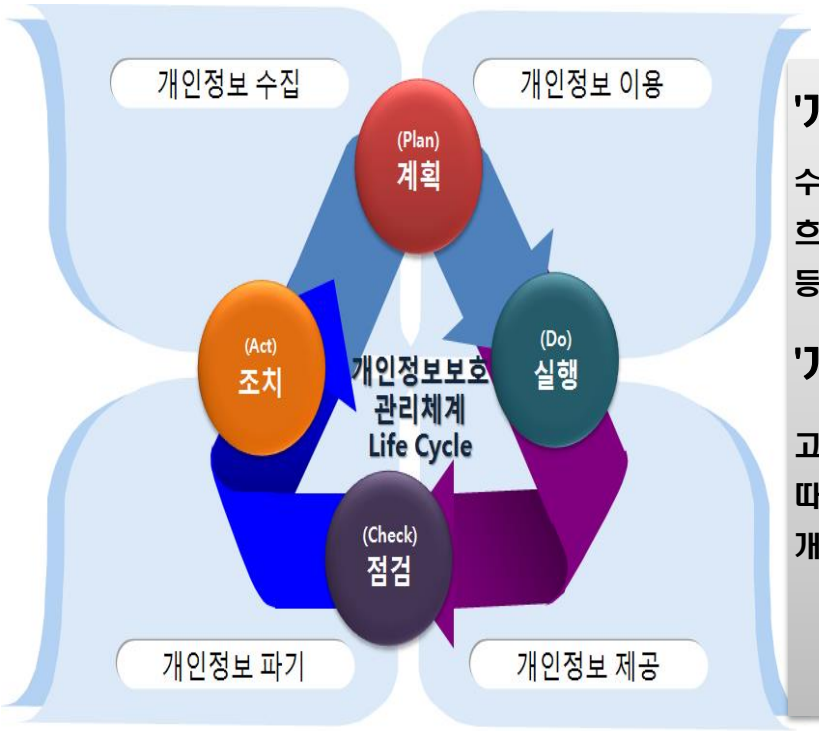
인증제도 비교

구분	ISO 27001	ISMS	PIMS
인증 기관	BSI, DNV, DQS, TUV 등	KISA	KISA
근거	국제표준	정통망법 제 47조	망법 제47조2
제도성격	권고	권고 + 의무('13.2.18)	권고
인증 대상	민간, 공공기업	민간기업 (통신, 금융, 운송, 제조, 병원, 학교 등)	개인정보를 수집 취급하는 자 (별도 기준 마련)
인증 기준	ISO 27001	방통위고시ITA표준	PIMS 인증기준
구조	관리과정 4단계 15개 통제항목, 문서화 3개 통제항목, 정보보호대책 133개 통제항목 **(총 151개 항목)**	관리과정 5단계 14개 통제항목, 문서화 3개 통제항목, 정보보호대책 15개 도메인 120개 통제항목 (총 137개 통제항목에 **446개 세부항목**)	관리과정 5단계 13개 통제항목, 생명주기 4개 도메인 31개 통제항목, 보호대책 9개 도메인 88개 통제항목 (총 124개 통제항목에 340개 세부항목)
시행시기	2005년	2002년	2009년
사례	6,037건 인증서 (국내 105건) 발급	128건 인증서 발급 (' 12년 11월 기준)	16건
심사원	**ISO 27001 심사원**	**KISA 교육 및 평가 후 선정**	**KISA 교육 및 평가 후 선정**
인증 유효기간	3년	3년	3년
사후관리 심사주기	매년 2회	매년 1회	매년 1회

개인정보보호 관리체계(PIMS)

- 조직이 수집, 이용, 제공, 파기하는 모든 고객 개인정보의 안전성과 신뢰성 제공 및 이용자 권리보호를 위해 체계적이고 지속적인 개인정보보호 활동 수행 여부를 확인하고 인증을 부여
- [법적근거] 정보통신망법 제 47조3
  ※ PIMS : Personal Information Management System

개인정보 생명주기에 따른 자율적 보호대책 마련



'개인정보 생명주기'

수집/이용/제공/파기의 개인정보 흐름에 따른 위험관리가 보안위협 등의 효과적인 대응 체계 제공

'개인정보보호 관리체계'

고객의 개인정보 생명주기 특성에 따른 종합적 개인정보 관리를 통해 개인정보 침해 가능성 최소화 필요

➢ **[점검 항목] : 137개**
- 관리과정 요구사항 14개
- 정보보호대책 3개
- 생명주기 요구사항 120개

➢ **[인증 효과]**
- 조직의 개인정보보호 활동에 대한 객관적 자료제시 및 사회적 책임이행
- 경영진의 개인정보보호 정책수립 의사결정 지원

➢ **[인증 혜택]**
- 인증 취득기업이 개인정보 사고 발생 시 과징금, 과태료 경감

(근거 : 정보통신망법 시행령 및 방통위 고시)

1.2 정보보호 관리체계 분류

개인정보보호 관리체계(PIMS) 개요

- 개인정보보호 관리체계(PIMS, Personal Information Management System)란 개인정보를 안전하게 관리하는 조직을 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.

- 개인정보를 취급하는 조직이 전사차원에서 개인정보 보호 활동을 체계적이고 지속적으로 수행하도록 하기 위한 필요한 보호체계를 구축하여 개인정보를 안전하게 보호할 수 있도록 하는 것이다. 정보통신망법에 명시된 최소한의 보호조치만으로 개인정보 침해사고 방지에 어려움을 겪었던 조직들에게 체계적인 개인정보 보호활동을 위한 세부 기준 및 방법을 제시하였다.

1.2 정보보호 관리체계 분류

개인정보보호 관리체계(PIMS) 개요

- **PIMS 프레임워크는 국내 공통 표준 프레임워크인 ISMS를 기반으로 하였으며 PIPL과도 전반적인 프레임워크는 유사하다. PIMS 또한 인증기준 자체가 구축 모델이며 개인정보보호 컨설팅의 방법론으로 활용되고 있다.**

Tip ••• 개인정보보호 관리체계의 인증(정보통신망법)

제47조의3(개인정보보호 관리체계의 인증) ① 방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "개인정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 방송통신위원회는 제1항에 따른 개인정보보호 관리체계 인증을 위하여 관리적 · 기술적 · 물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

③ 개인정보보호 관리체계의 수행기관, 사후관리 등에 대하여는 제47조제5항부터 제10항까지의 규정을 준용한다. 이 경우 "제1항 및 제2항"은 "제1항"으로 본다.

④ 개인정보보호 관리체계 인증기관의 지정취소 등에 대하여는 제47조의2를 준용한다.

1.2 정보보호 관리체계 분류

PIMS 인증심사기준

- PIMS의 통제항목은 개인정보 생명주기에 따라 정보보호 분야에 개인정보의 특수성을 감안하여 개인정보 수집, 이용, 관리, 파기라는 개인정보 생명주기를 반영하였다는 것이 특징이며, 관리과정 등은 공통 표준 프레임워크인 ISMS 모델을 따르고 있다.

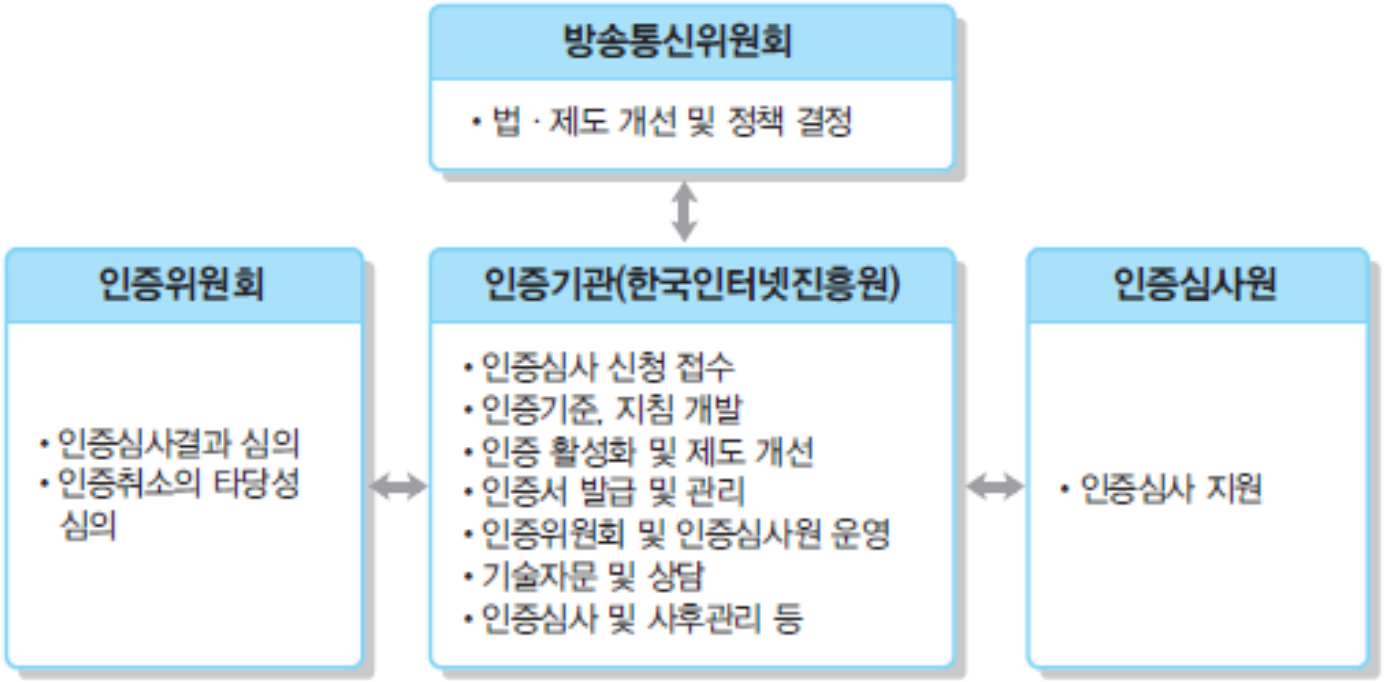
〈표 1-13〉 PIMS 통제항목 및 세부점검 항목

요구사항	통제 분야	통제항목
개인정보보호 관리과정	1. 개인정보보호 정책 수립 및 범위설정	3
	2. 경영진 책임 및 조직구성	2
	3. 위험 관리	3
	4. 개인정보보호대책 구현	2
	5. 사후관리	3
보호대책	1. 개인정보보호 정책	6
	2. 개인정보보호 조직	5
	3. 개인정보 자산분류	2
	4. 개인정보보호교육	4
보호대책	5. 인적보안	4
	6. 침해사고관리	7
	7. 기술적 보호조치	36
	8. 물리적 보호조치	8
생명주기	1. 개인정보수집에 따른 조치	10
	2. 개인정보이용 및 제공에 따른 조치	16
	3. 개인정보관리 및 파기에 따른 조치	6
총계		124

1.2 정보보호 관리체계 분류

PIMS 인증체계

- 국내 관리체계 인증체계와 동일하며 인정기관 역할은 방송통신위원회가 인증기관은 KISA가 인증위원회를 운영



[그림 1-13] PIMS 인증체계

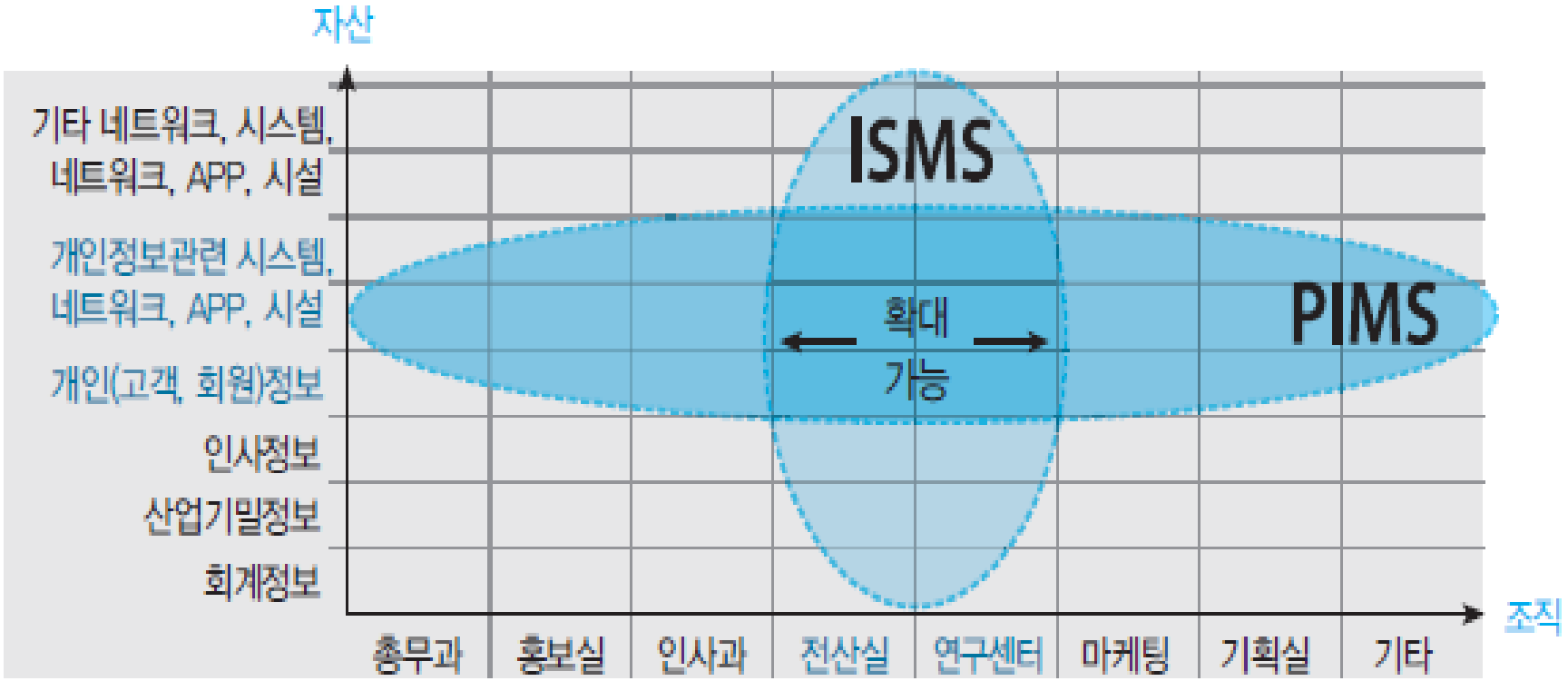
1.2 정보보호 관리체계 분류

ISMS와 PIMS 차이점

- PIMS 프레임워크는 국내 관리체계 공통 표준인 ISMS를 기본 틀은 따르고 일부 통제항목 부분에서 개인정보보호 생명주기 등 개인정보 보호에 필요한 부분이 반영되었다.
- ISMS는 범위 내 모든 정보자산과 보호대책을 전반적으로 취급하는 데 반해, PIMS는 정보자산 중 개인정보에 특화한 보호와 정보보호를 대상으로 한다는 점이다. ISMS는 정보자산의 기밀성, 무결성, 가용성 모두를 확인하지만 PIMS의 경우는 가용성에 대해서는 중요하게 다루지 않고 있다.
- PIMS 인증은 구체적인 '개인정보의 정의 및 검토' 를 요구하고 있으며, '목적 외 이용의 금지' 등 개인정보 소유자 본인의 권리 보호와 개인정보를 취급할 경우의 관리 책임 등이 고려되고 있다.
- 인증 범위에 대해서는 제도상의 차이가 있다.
- 개인정보의 권리 보호에 대한 엄밀한 취급

1.2 정보보호 관리체계 분류

- PIMS에서는 개인정보의 공개, 정정, 삭제 요구에 응하지 않는다거나, 정보 유출에 의해 제3자가 목적 외 이용을 함으로써 정보 주체에게 불이익을 입힌 경우 등 컴플라이언스(법규 준수)의 관점에서 개인정보만을 취급하는 것이며, ISMS는 정보시스템 전체의 정보보호를 취급한다.



[그림 1-14] PIMS와 ISMS의 범위 비교

감사합니다^^
Happinessisnowhere!

조 병 철
bcho@naver.com 010-5247-5178