New Lens, 2014
Data 보안 가이드라인

U-LIFE & U-BIZ CREATOR

UZEN

2014

Data보안

1. DB보안 현황

1.1 DB보안 시장

(단위 : 백만 원)

중분류		2009년	2010년	2011년	2012년	2013년(E)	증감률 ('11-12)	증감률 ('12-'13)	CAGR ('09-'13)
컨설팅		2,553	2,463	3,439	4,499	5,549	30.8%	23.3%	21.4%
		8.7%	7.7%	8.5%	6.8%	6.1%			
솔루션	SW	22,122	23,531	31,638	53,222	74,587	68.2%	40.1%	35.5%
		75.1%	73.7%	78.2%	80.9%	81.4%			
	유지보수	4,777	5,948	5,381	8,035	11,543	49.3%	43.7%	24.7%
		16.2%	18.6%	13.3%	12.2%	12.6%			
합계		29,452	31,942	40,458	65,756	91,679	62.5%	39.4%	32.8%
		100.0%	100.0%	100.0%	100.0%	100.0%			

[한국데이터베이스진흥원: 2013년도 DB산업 시장 분석 결과보고서]

지속 성장 / 내재화 진행 중 / 보안 수준???

1. DB보안 현황

1.2 DB보안 인증(DQC-S) 취득 현황

인식 부족 / 예산 부족 / 내재화 수준???

1. DB보안 현황

1.3 보안 신뢰도 (1/2)

[Rethinking Personal Data: **A New Lens** for Strengthening Trust]

1. DB보안 현황

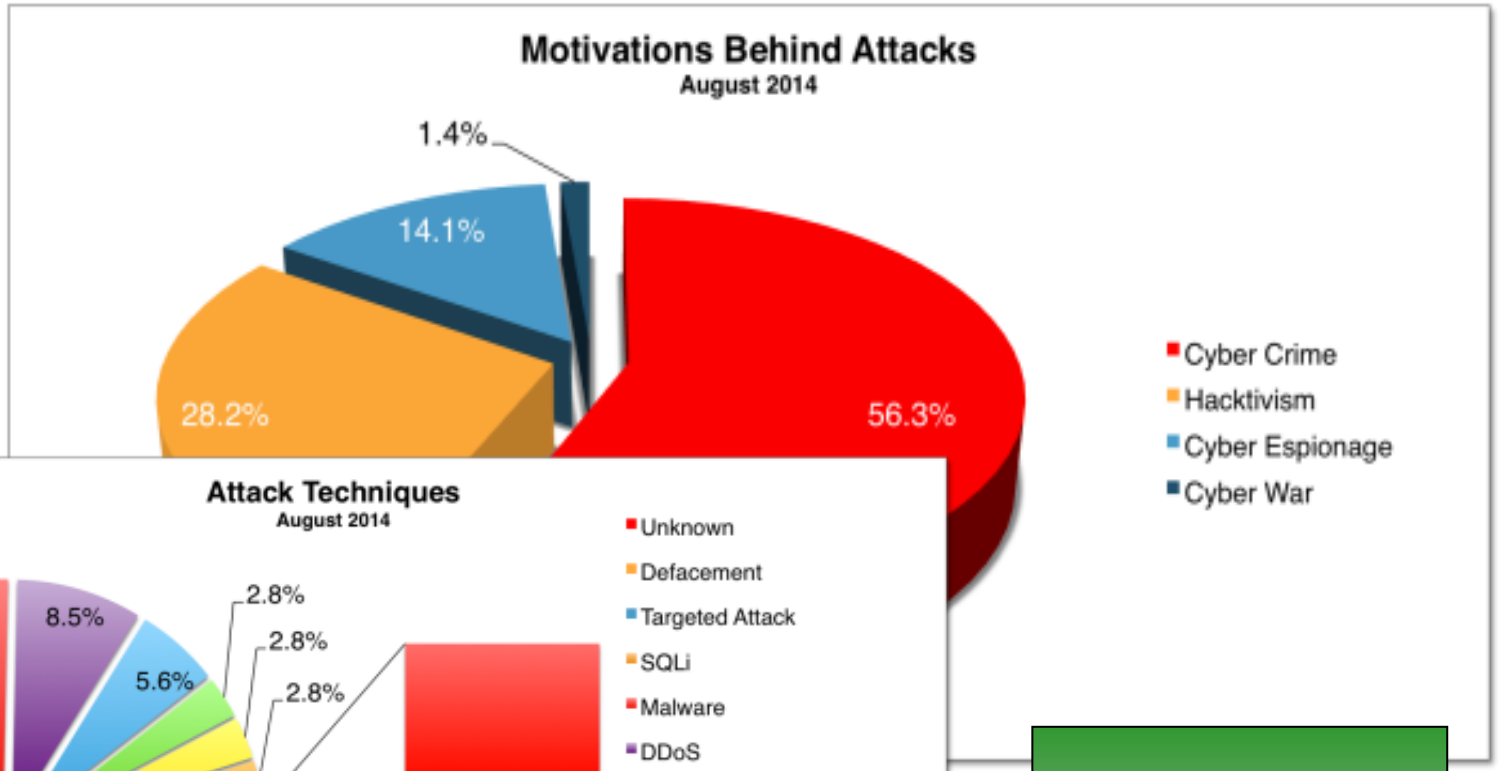
1.3 보안 신뢰도 (2/2)

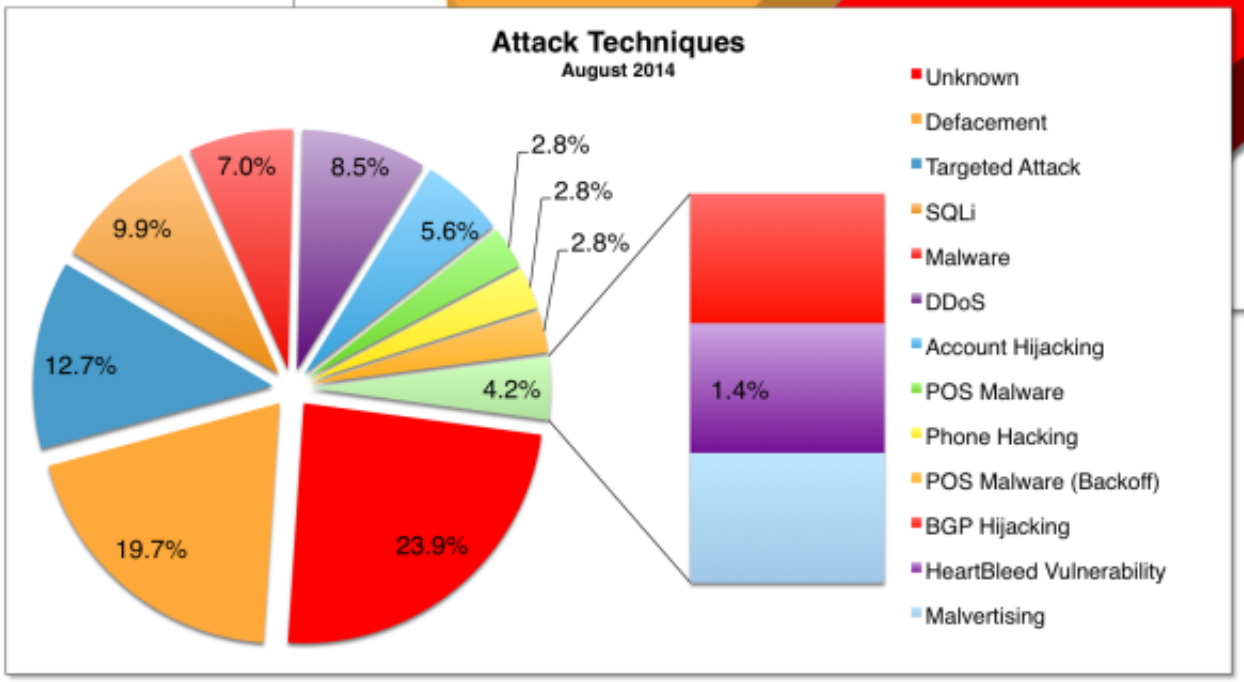
발생일	대상기관	피해사례	보안위협
2011년 4월	H캐피탈	보조서버를 통해 175만 명의 개인정보, 13,000명의 신용등급 정보 등 유출	-내부 통제 취약성 공격 -내부정보 유출 위협
2011년 4월	N은행	외주 직원 노트북에 악성코드를 심은 후, 감염된 노트북을 농협 서버에 연결하면 악성코드를 삽입하고 , 서버 데이터 삭제	-APT -내부 통제 취약성 공격 -서비스 방해 위협
2011년 5월	L투자증권	홈페이지 관리 서버의 개인정보 데이터베이스 관리 소홀로 인해 약 13,000 건의 개인정보가 유출되어 협박 이메일을 받음	-웹 서버 취약점 공격 -저장정보 유출 위협
2011년 9월	S카드	내부 감사 과정에서 내부 직원에 의해 200,000 명의 고객정보가 유출된 것을 확인	-내부정보 유출 위협
2011년 9월	H카드	내부 직원을 통해 가입자 50,000 여 명의 고객 정보가 유출	-내부정보 유출 위협
2012년 1월	(이용자)	대형 마트의 포스 단말기의 보안 문제로 인해 카드 정보가 유출되어 해외에서 복제카드가 무단 사용	-카드 복제 위협 -저장정보 유출 위협
2012년 12월 (ISP 해킹)	K카드 B카드	이용자 PC에서 ISP 정보를 유출 시켜 30만 원 미만의 소액결제를 통해 부정사용하여 190명이 피해	-입력정보 유출 위협 -저장정보 유출 위협 -제휴사업자 정보유출 위협
2013년 1월	(이용자)	이용자 PC가 악성코드에 감염되어 공인인증서 700여 개가 탈취되었으며, 만료된 300여 개를 제외한 약 400여 개의 공인인증서를 폐기	-역공학 공격 -입력정보 유출 위협 -저장정보 유출 위협
2013년 3월 (3.20 사건)	N은행 S은행 J은행 등	내부 컴퓨터가 악성코드에 감염된 후 사내 업데이트 서버 취약점을 이용하여 악성코드를 내부에 유포하여 내부 PC 및 ATM 데이터 삭제	-APT -내부 통제 취약성 공격 -서비스 방해 위협

[금융권 보안사고 사례 및 보안 위협]

1. DB보안 현황

1.4 내/외부 위협의 다양성 증가





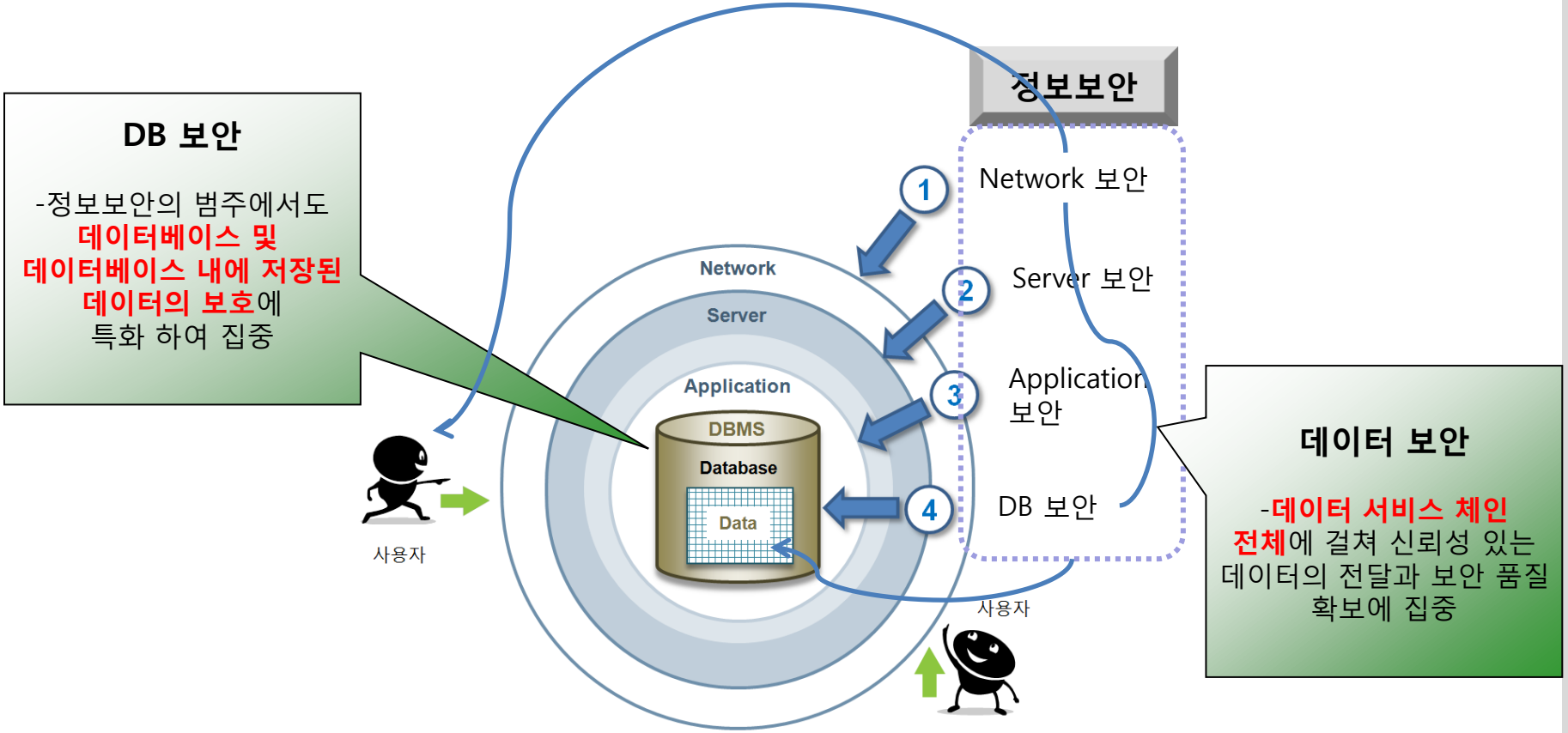
Data의 생성부터 서비스까지의 전방위 보안 필요

[hackmageddon.com: August 2014 Cyber Attacks Statistics]

2. Data보안 정의

2.1 Data보안 개요

데이터 및 정보 자산의 접근, 활용에 대한 적절한 인증과 권한의 감사를 위하여 보안 정책 및 절차를 기획, 구축, 실행하는 것

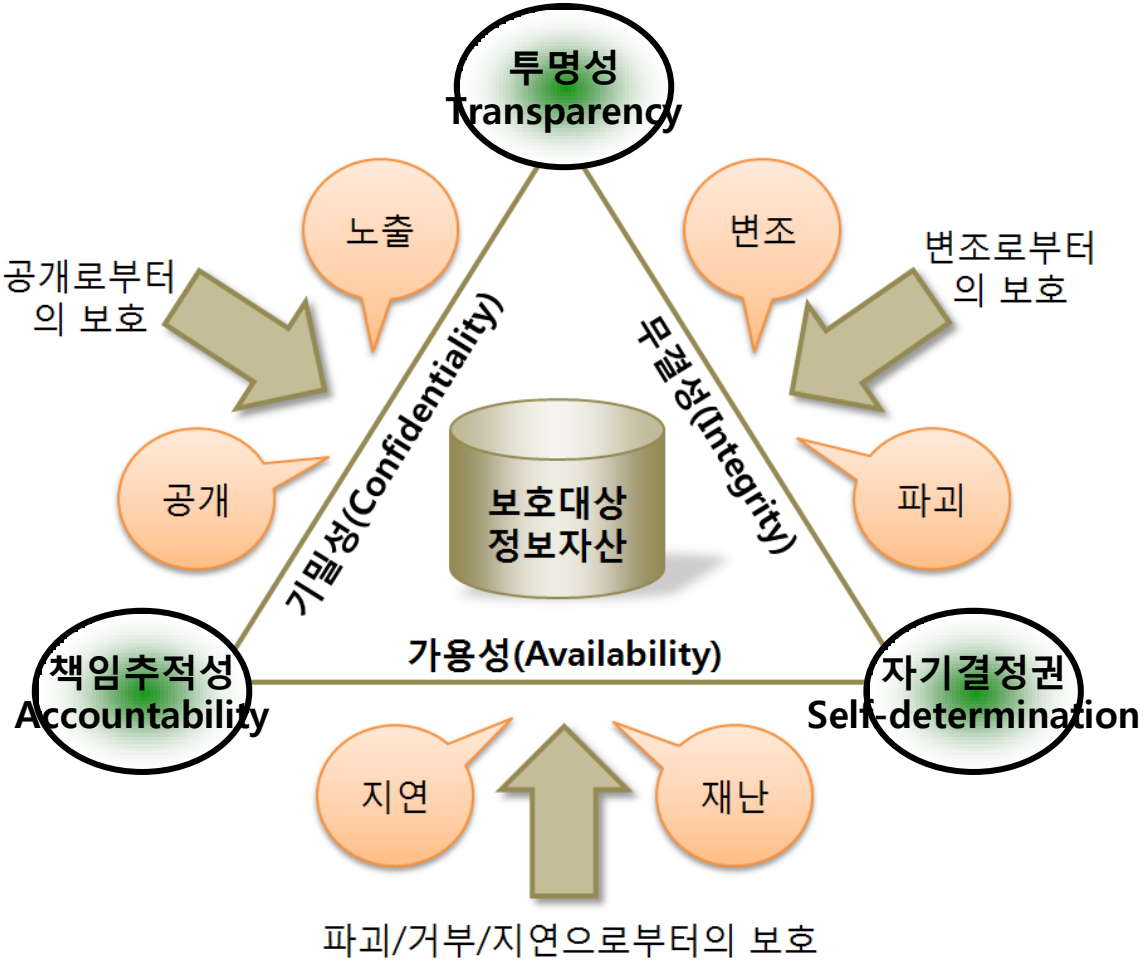


[정보보안 vs. DB 보안]

2. Data보안 정의

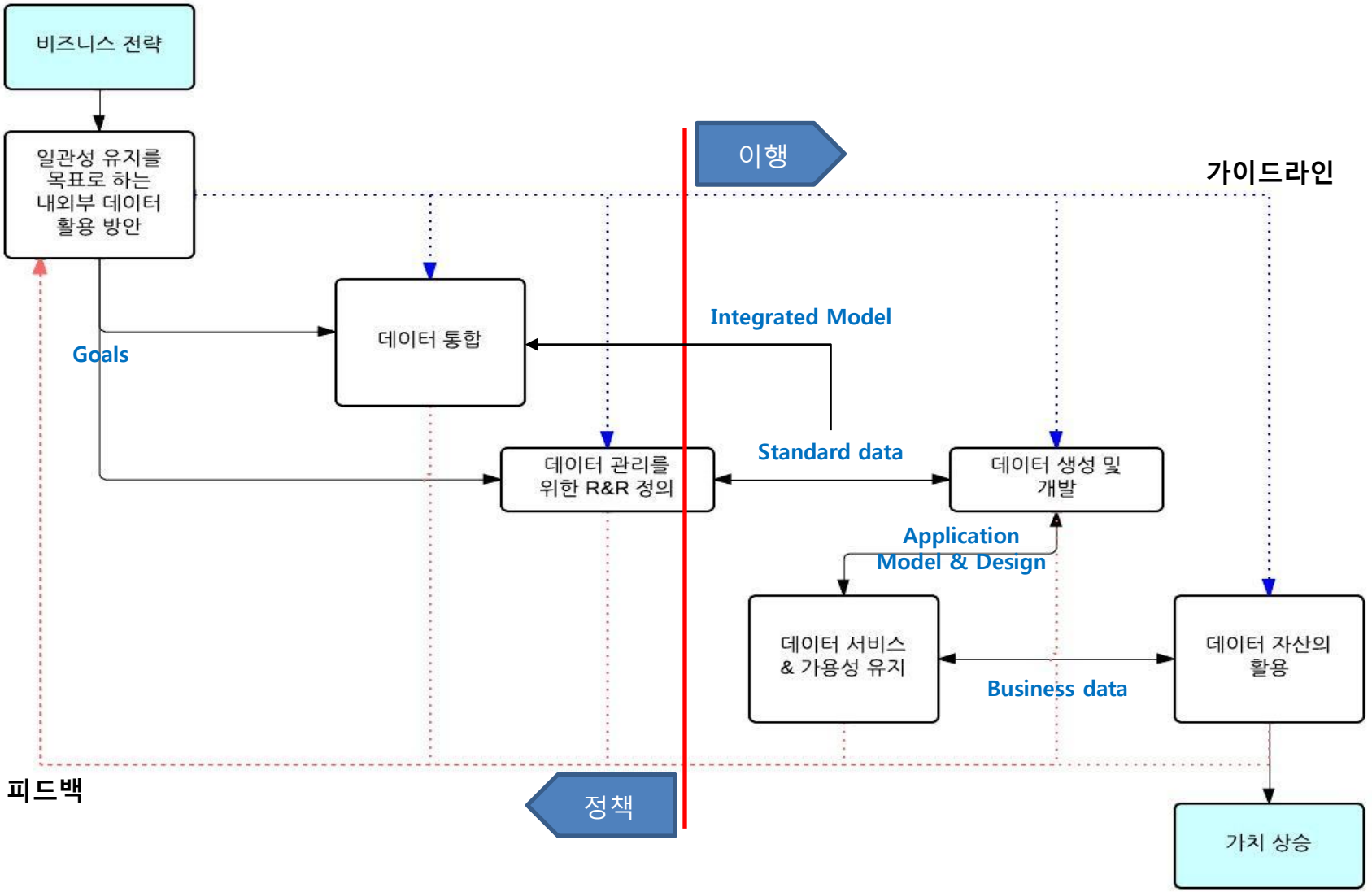
2.2 Data보안 목적

DB 내 데이터를 공개, 노출, 변조, 파괴, 훼손, 지체, 재난 등의 위협으로부터 보호하여 데이터의 생명 주기 동안 데이터 서비스 체인의 전체에 걸쳐 기밀성, 무결성, 가용성을 유지하고 투명성, 책임추적성을 확보하며 자기결정권의 행사에 대응 가능하도록 하는 것



3. Data보안 Role & Rule

3.1 Data 생성 및 활용 주요 단계별 보안 포인트 (1/2)

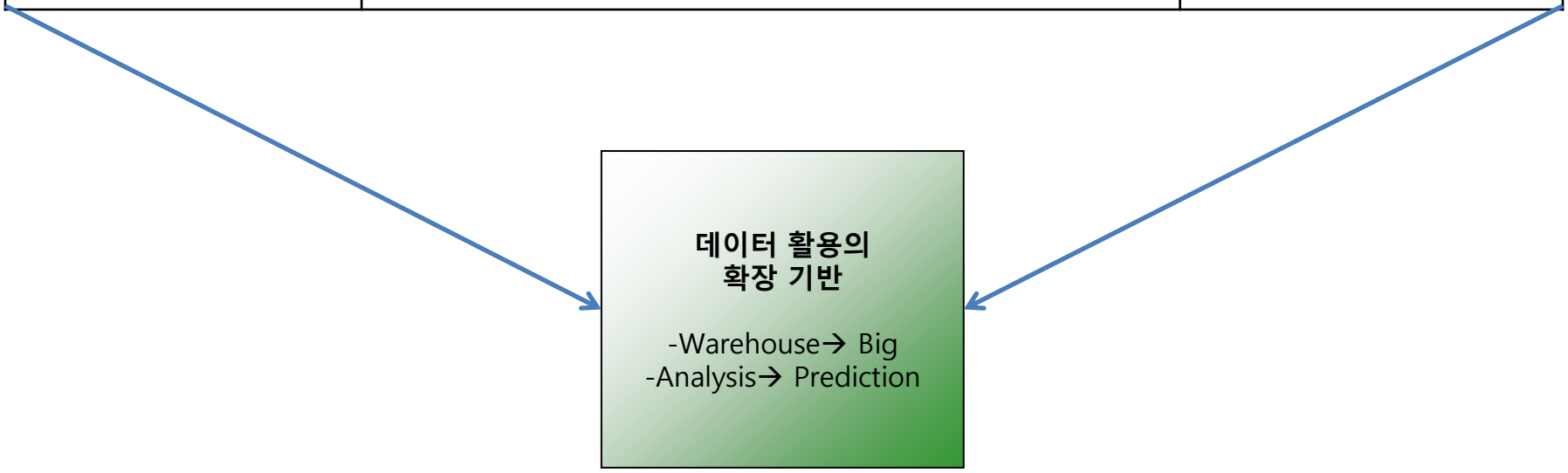


[Published by DAMA International]

3. Data보안 Role & Rule

3.1 데이터 생성 및 활용 주요 단계별 보안 포인트 (2/2)

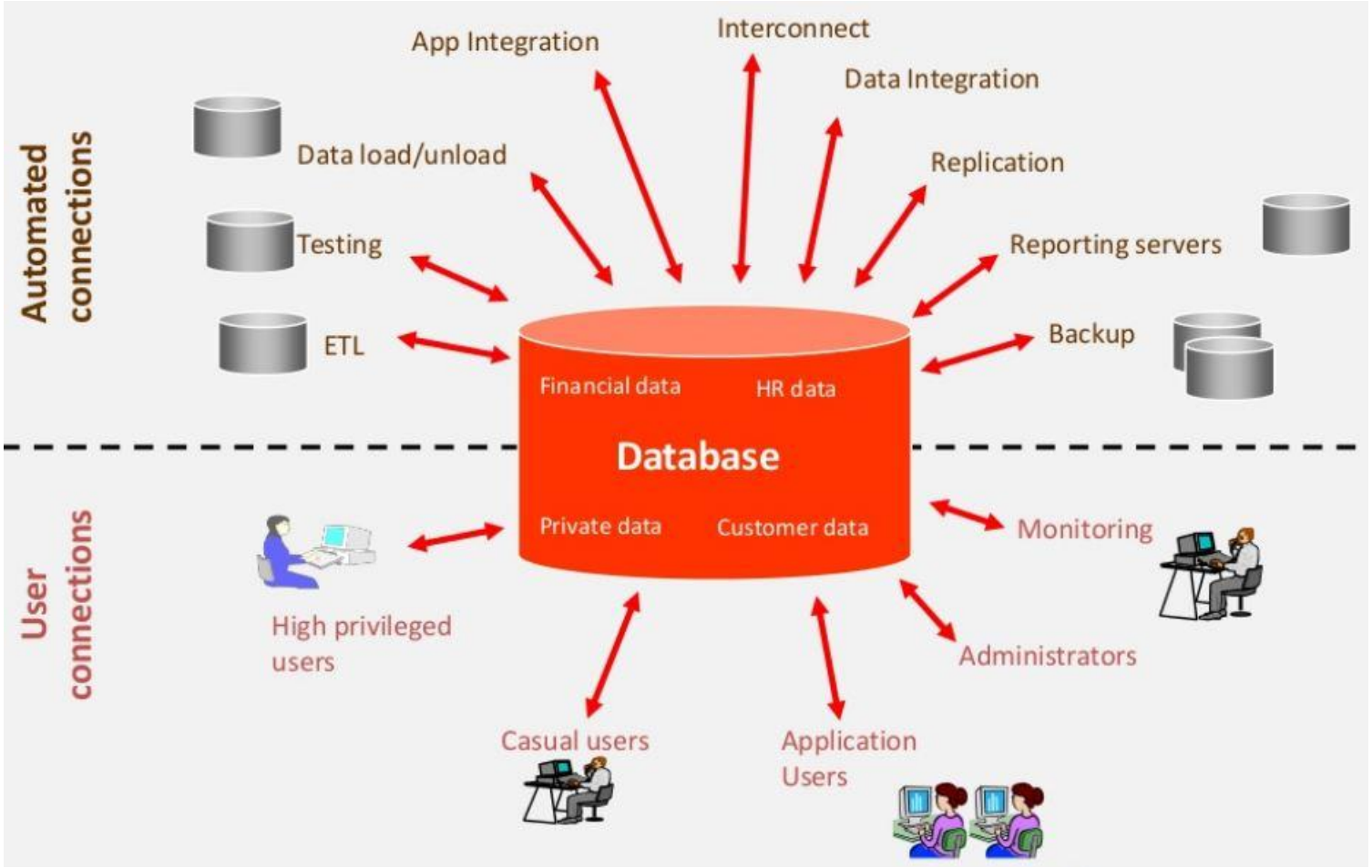
관리 영역	역할	주안점
내/외부 데이터 활용 방안 수립	-전략, 정책, 계획, 자원 상황 및 진행 상황에 대한 모니터링 등의 정의	**데이터의 일관성 유지**
데이터 통합	-필요 요소의 식별 및 조정, 필요 서비스를 위한 설계	**데이터 공유**
데이터 관리를 위한 R&R 정의	-데이터 생성 및 사용의 각 단계별 역할 자의 R&R 정의	**데이터에 대한 책임 할당**
데이터 생성 및 개발	-조직 전체 및 각 역할 자의 요구 데이터의 생성 및 개발	**데이터 공급 시스템 구축**
데이터 서비스 & 가용성 유지	-조직 전체의 활동에 맞게 데이터 서비스의 효율 및 가용성 확보를 위한 유지보수 활동	**데이터 가용성 유지**



3. Data보안 Role & Rule

3.2 Data 자산의 활용에 따른 보안 포인트

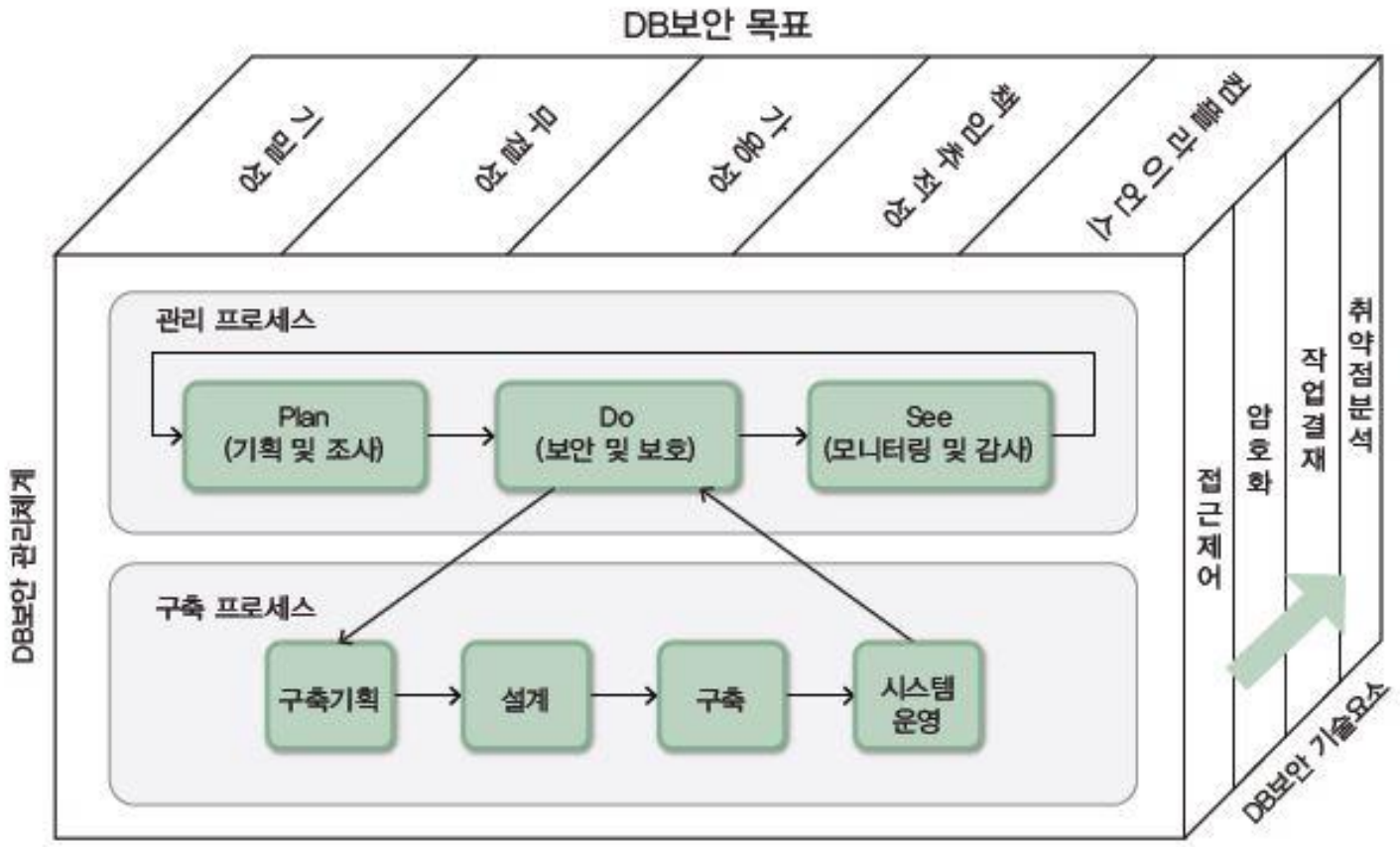
개발/생성된 데이터 및 정보 자산은 목적과 목표에 맞춰 다양한 형태로 사용, 재가공됨으로 표준에 맞춘 활동과 정규화된 관리 체계가 더욱 필요 함



4. Data보안 관리

4.1 Data보안 관리를 위한 DB 보안 프레임워크

DB보안 프레임워크는 효과적인 DB 및 데이터 보안 관리 체계를 구축하고 그 수준을 유지할 수 있도록 하는 제어 틀로서 DB및 데이터 보안 관리 체계의 구축, 운영 및 개선을 위한 프로세스와 활동, 도구 및 가이드를 제공 하는 것

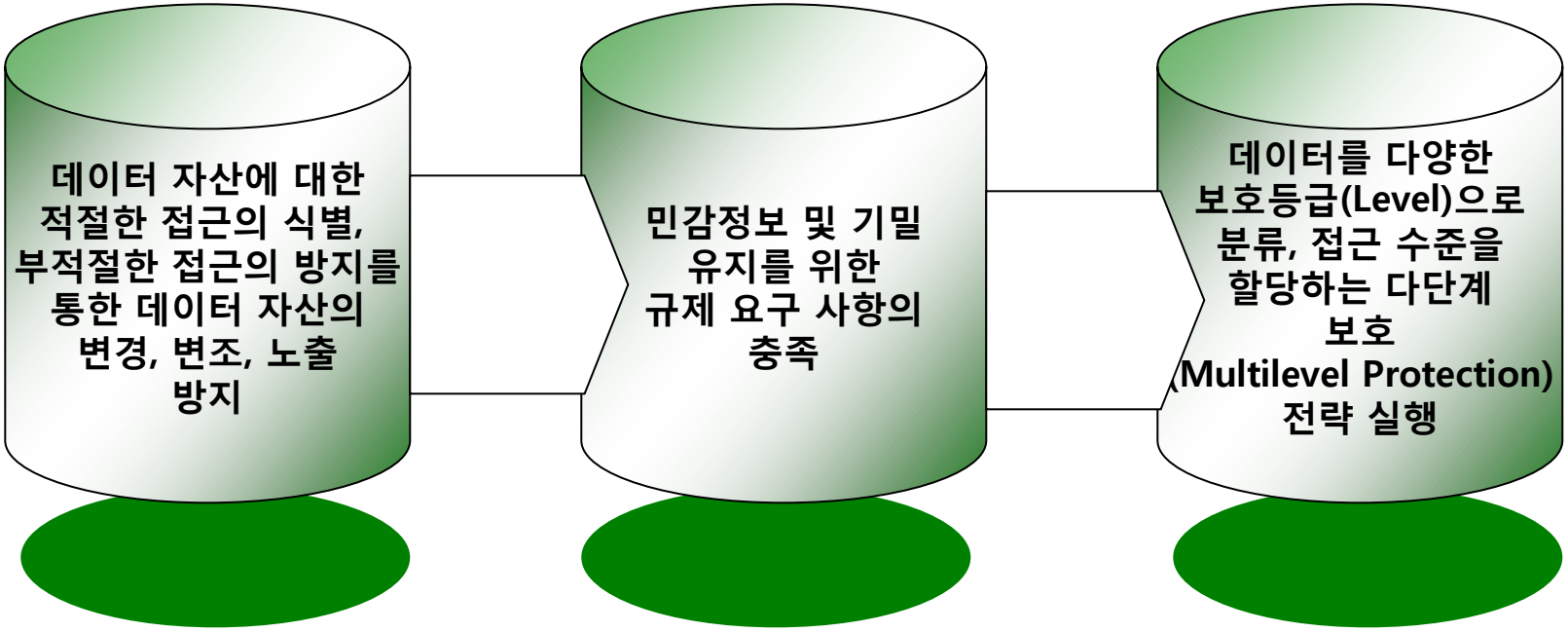


[DB보안가이드라인 2014 개정: DB보안 프레임워크]

4. Data보안 관리

4.2 목표와 원칙

보안을 위해 관리 할 모든 범위를 100% 충족할 수 있는 기술적 대안은 없다는 가정 하에 목표를 현실화하고 보안의 기술적 부분에 관리적인 부분을 더하여 보안 계층을 구성하고 위협 요소의 식별→분석→통제의 과정이 내재화 될 수 있도록 함

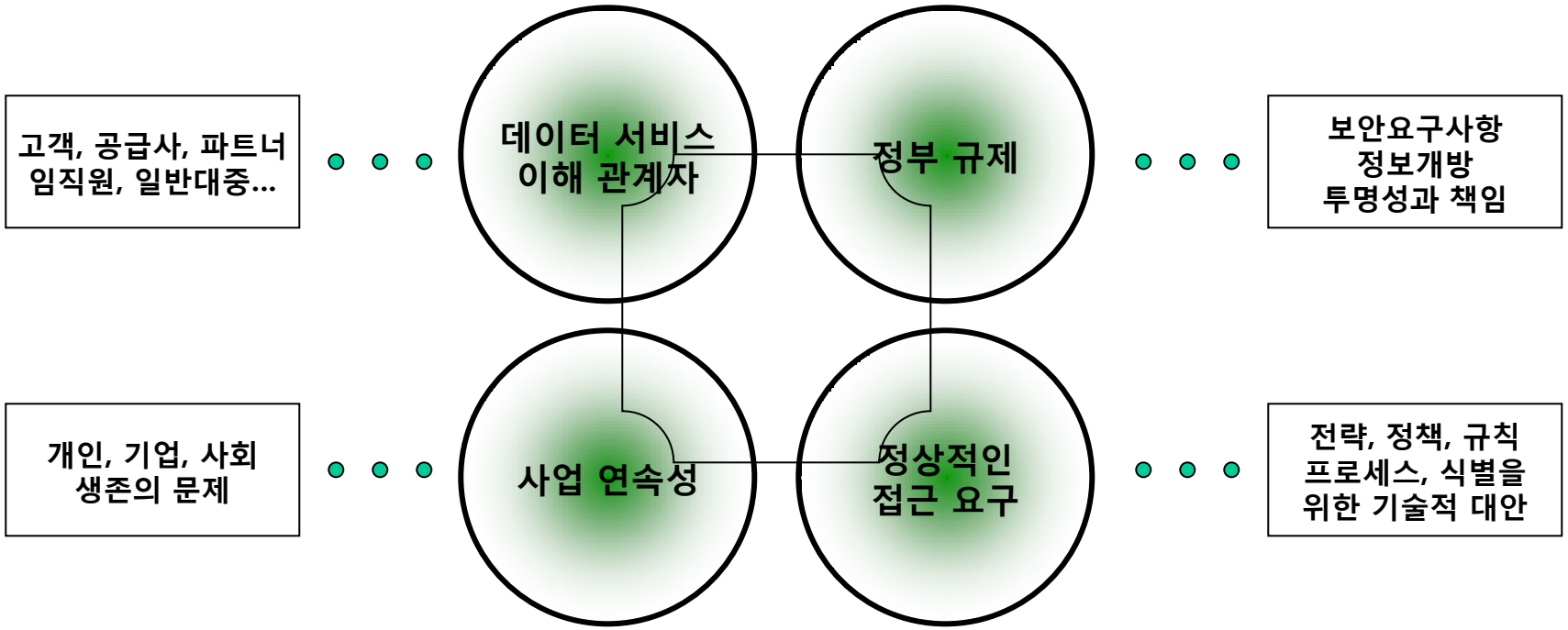


[데이터 보안의 3원칙]

4. Data보안 관리

4.3 정책적 고려 사항

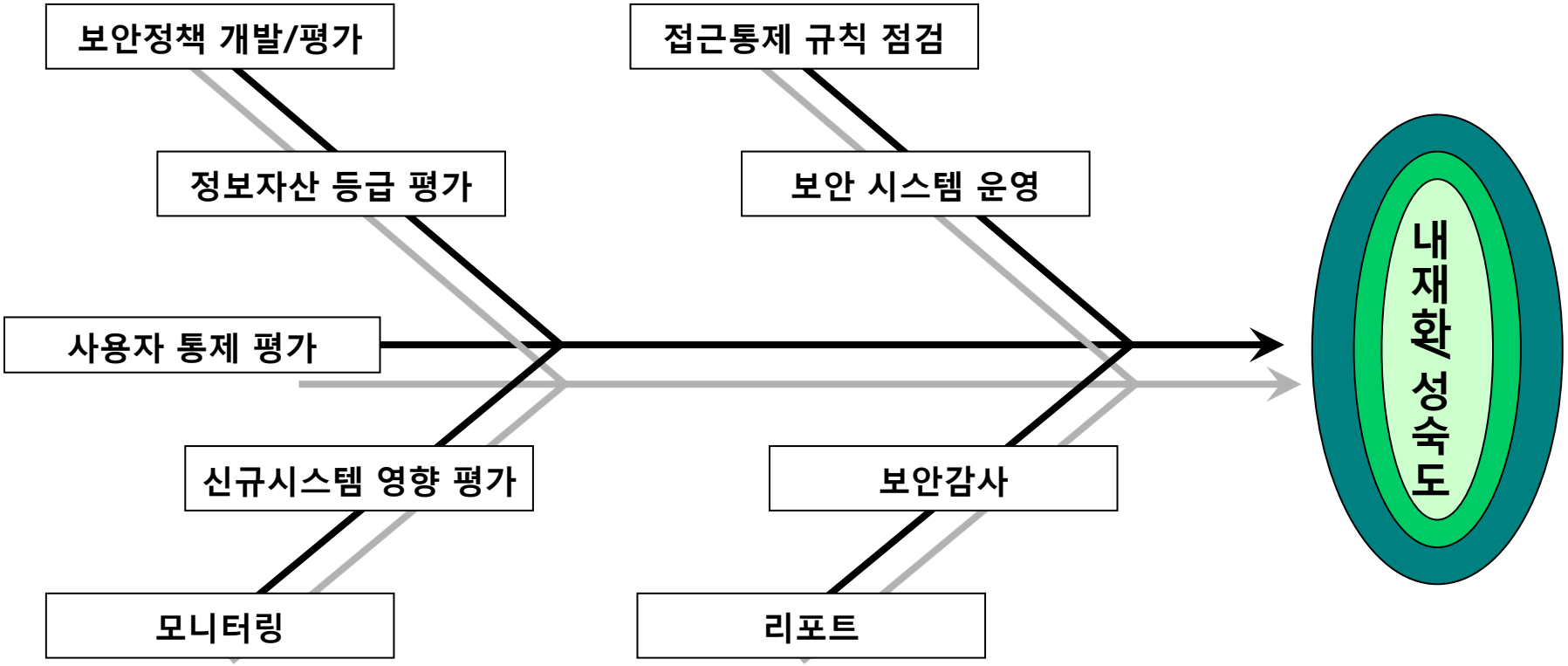
보안 정책은 데이터 자산의 정당한 사용을 위하여 '마땅히 있어야 할 것', '당연히 바람직한 것' 을 찾아 구현 하려는 의도이며 보안 목적의 달성을 위해 '당연히 지켜야 할 것', '당연히 해야 할 것' 등의 규정 및 지침을 주는 것으로 정부 규제, 사람, 사람의 활동, 사업의 연속성 등을 고려해야 함



4. Data보안 관리

4.4 관리 활동

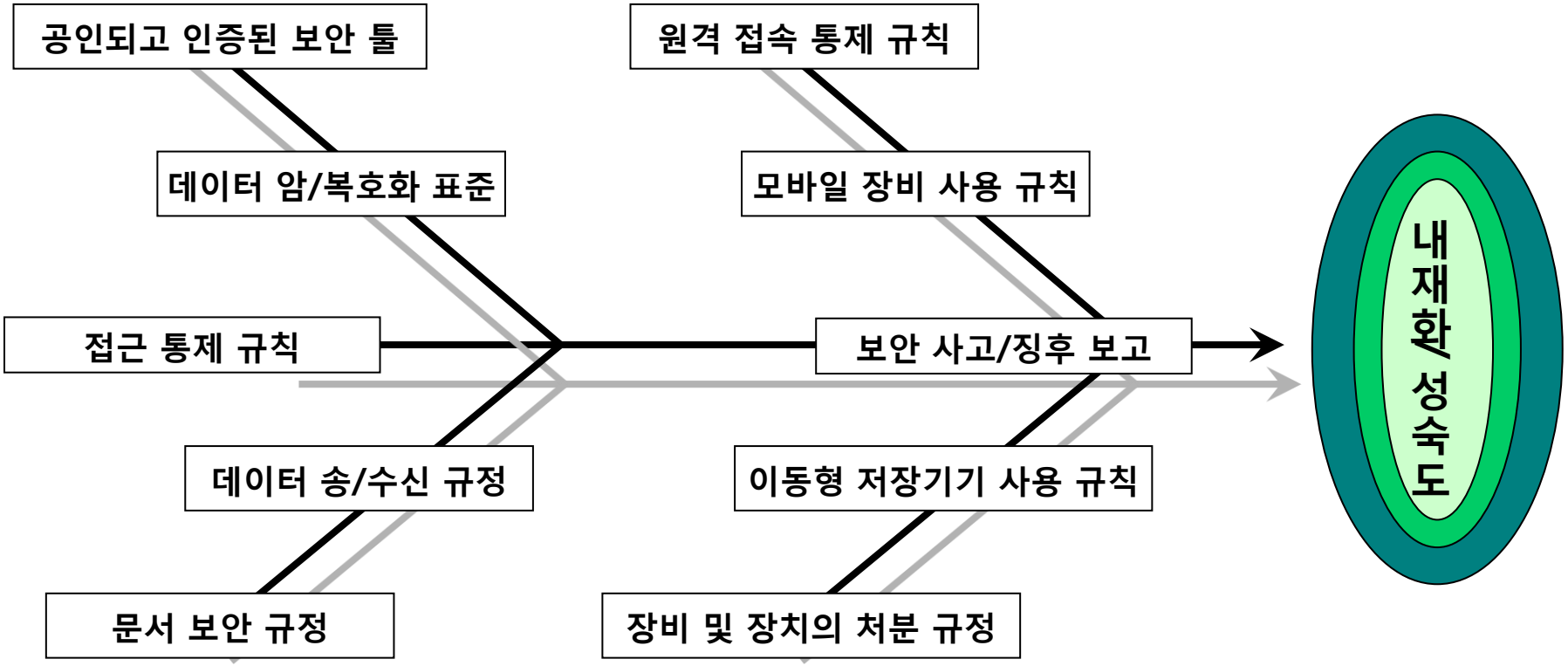
관리 활동은 비즈니스 요구사항, 규제의 보안 요구사항 등에 대한 이해를 바탕으로 해야 하며, 조직 내 모든 보안 관련 활동의 내재화와 성숙도 향상을 목표로 하여야 함



4. Data보안 관리

4.5 관리 활동의 주요 표준

데이터 자산을 활용하는 이해 관계자들의 보안 활동이 내재화 및 성숙 될 수 있도록 '당연히 지켜야 할 것', '당연히 해야 할 것'에 대한 기준을 명확히 제시하여야 함



4. Data보안 관리

4.6 관리 활동 모델 예시 (1/2)

[Published by DAMA International]

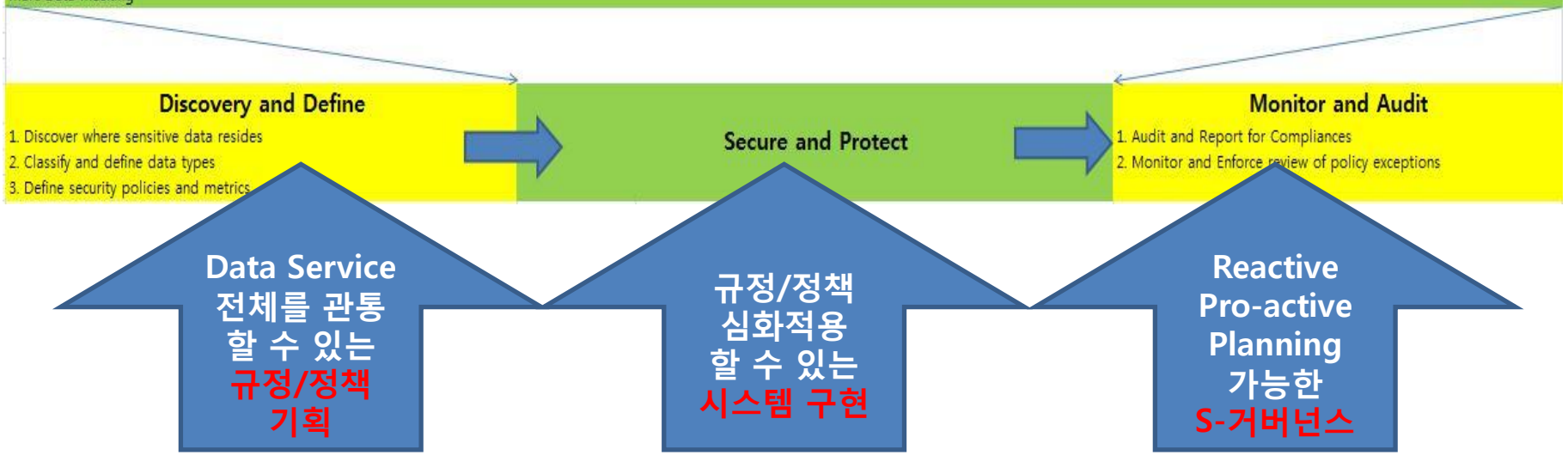
4. Data보안 관리

4.6 관리 활동 모델 예시 (2/2)

	Role Type					DQC-S
	Privileged Users	End Users	Developers, System Analysts and System Administrators	IT Operations	Malicious Users	
Access to, deletion of, or changes to data:	M	NA	NA	NA	NA	DAP
Access using inappropriate or nonapproved channels:	M	NA	NA	NA	NA	DAP, VA
Schema modifications:	M	NA	NA	NA	NA	DAP
Unauthorized addition of user accounts or modification of existing accounts:	M	NA	NA	NA	NA	DAP, VA
Access to excessive amounts of data or data not needed for legitimate work:	NA	M	NA	NA	NA	DAP, WF
Access to data outside standard working hours:	NA	M	NA	NA	NA	DAP, WF
Access to Sensitive Data	NA	M	NA	NA	NA	ENC
Access to live production systems:	NA	NA	M	NA	NA	DAP, MSK
Unapproved changes to databases or applications that access the database:	NA	NA	NA	M	NA	DAP
Out-of-cycle patching of production systems:	NA	NA	NA	M	NA	Operatoinal Management Policy

M: Monitoring and Blocking
NA: Not Allowed
DAP: Database Audit and Protection
ENC: Encryption
WF: Workflow
VA: Vulnerability Assessment
MSK: Data Masking

Privileged Users: DBA
End Users: Groupware, Applications
Developers, System Analysts and System Administrators: Including Outsource Engineers
IT Operations: Including Outsource Engineers



[DQC-S Database Security 참조 모델]

DQC-S

데이터보안 인증

1. Data보안 인증

1.1 DQC-S 개요

DQC-S(데이터 보안 인증, Database Quality Certification-Security)

2012.04.30 "데이터베이스품질인증제도"로부터 출발

2010.11.22 한국데이터베이스진흥원, "데이터베이스품질인증기관지정"으로 인증심사 시행

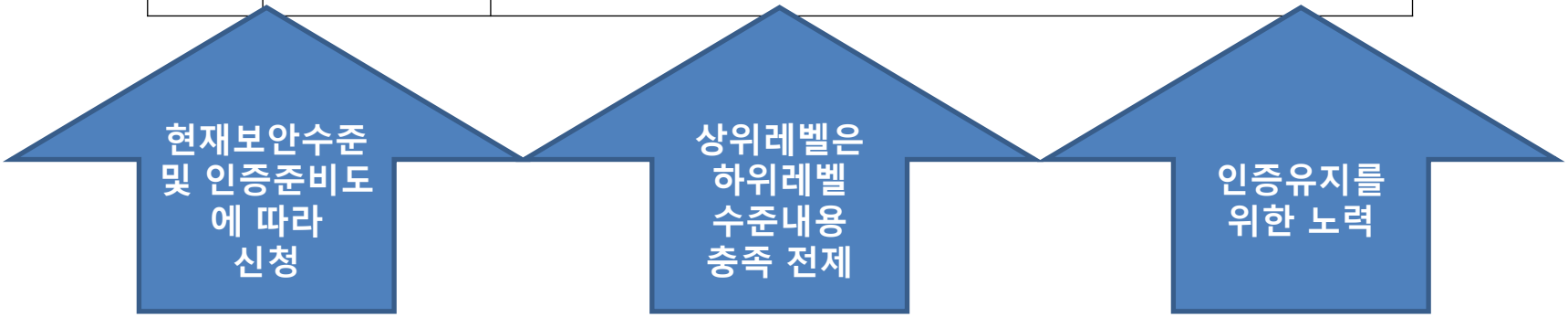
DQC-S 인증모델은

DB보안의 핵심 기술로 **"접근제어, 암호화, 작업결재, 취약점분석"** 등을 선정, 공공·민간에서 구축·활용 중인 **데이터베이스를 대상으로 위의 핵심 기술 전반을 심사, 인증** 하는 것

1. Data보안 인증

1.2 DQC-S 인증 레벨

구분		수준 내용
4레벨	**취약점분석**	DB의 취약점을 다각적으로 분석하여 선재적으로 보완하는 단계
3레벨	**작업결재**	DB작업의 정당성을 확보하기 위해 기술적 수단과 관리적 수단을 복합 수행하는 단계
2레벨	**암호화**	중요 정보를 암호화하여 정보 유출에 대비하는 단계
1레벨	**접근제어**	DB로의 접근 행위 및 DB내에서의 행위를 제어, 관리, 기록하는 단계



1. Data보안 인증

1.3 DQC-S 인증 기준 및 배점 (1/2)

구분	통제영역	통제목표	통제항목
보안기획 (100)	1. 기획 및 조사 (40)	1.1 DB보안 정책의 수립 (20)	NA
		1.2 위험평가 (10)	
		1.3 DB보안 요구사항 정의 (10)	
	2. 보안 및 보호 (20)	2.1 DB보안 구축 (6)	
		2.2 DB보안 교육 (14)	
	3. 모니터링 및 감사 (40)	3.1 DB보안 모니터링 (20)	
		3.3 DB보안 감사 (20)	
접근제어 (100)	4. 구축기획 (10)	4.1 DB보안 구축계획 수립 (2)	
		4.2 DB보안솔루션 도입 (3)	
		4.3 운영 정책의 수립 (5)	
	5. 설계 (10)	5.1 DB보안설계 (6)	
		5.2 DB보안 시험계획 수립 (4)	
	6. 구축 (10)	6.1 DB보안 규칙 적용 (4)	
		6.2 DB보안 시험 (6)	
	7. 시스템 운영 (70)	7.1 DB보안 시스템 운영 (70)	
암호화 (100)	4. 구축기획 (10)	4.1 DB보안 구축계획 수립 (2)	
		4.2 DB보안솔루션 도입 (3)	
		4.3 운영 정책의 수립 (5)	
	5. 설계 (10)	5.1 DB보안설계 (6)	
		5.2 DB보안 시험계획 수립 (4)	
	6. 구축 (10)	6.1 DB보안 규칙 적용 (4)	
		6.2 DB보안 시험 (6)	
	7. 시스템 운영 (70)	7.1 DB보안 시스템 운영 (70)	

1. Data보안 인증

1.3 DQC-S 인증 기준 및 배점 (1/2)

구분	통제영역	통제목표	통제항목
작업결재 (100)	4. 구축기획 (10)	4.1 DB보안 구축계획 수립 (2)	NA
		4.2 DB보안솔루션 도입 (3)	
		4.3 운영 정책의 수립 (5)	
	5. 설계 (10)	5.1 DB보안설계 (6)	
		5.2 DB보안 시험계획 수립 (4)	
	6. 구축 (10)	6.1 DB보안 규칙 적용 (4)	
		6.2 DB보안 시험 (6)	
	7. 시스템 운영 (70)	7.1 DB보안 시스템 운영 (70)	
취약점분석 (100)	4. 구축기획 (10)	4.1 DB보안 구축계획 수립 (2)	
		4.2 DB보안솔루션 도입 (3)	
		4.3 운영 정책의 수립 (5)	
	5. 설계 (10)	5.1 DB보안설계 (6)	
		5.2 DB보안 시험계획 수립 (4)	
	6. 구축 (10)	6.1 DB보안 규칙 적용 (4)	
		6.2 DB보안 시험 (6)	
	7. 시스템 운영 (70)	7.1 DB보안 시스템 운영 (70)	

1. Data보안 인증

1.4 주요 보안 인증 제도와의 비교

구분	DQC-S	ISO27001	KISA ISMS	KISA PIMS	PIPL
범위	특정 업무 DB	전사	전사 또는 특정 서비스	전사	전사 또는 특정 서비스(업무)
대상	민간/공공	민간	민간/공공	민간	공공기관/대기업/중소기업/소상공인
평가 항목	현재 공통영역 29개, 접근제어 30개, 암호화 39개, 작업결재 19개, 취약점분석 33개의 총 150개 심사항목으로 구성	11개 도메인, 113개 통제 항목으로 구성	관리과정 5단계 12개 요구사항과 정보보호대책 13개 통제분야에 대해 92개 통제사항으로 구성	개인정보관리과정, 개인정보보호대책 및 개인정보생명주기 3개 분야의 118개 통제 항목, 325개의 세부점검 사항으로 구성	개인정보보호 관리체계와 개인정보보호대책 구현 9개 심사영역 65개 심사항목 으로 구성
인증 기관	한국데이터베이스진흥원	BSI코리아,DNV,SGS등 국내 인증기관	한국인터넷진흥원	한국인터넷진흥원	한국정보화진흥원

2. 보안 가이드라인

2.1 가이드라인의 구성 (1/3)

구분	주제영역	적용영역
DB보안의 이해	DB보안 개요	DB보안 정의
		DB보안 목적 및 필요성
		DB보안 범위
		IT보안과의 연계
	DB보안 절차 및 기술요소	DB보안 프레임워크
		DB보안 FW ver 2.0 구성 요소
		DB보안 구축시 고려사항
		타 인증제도와의 비교
DB보안 기획	DB보안 기획 개요	DB보안 기획의 정의
		DB보안 기획의 범위
		DB보안 기획의 필요성
		DB보안 기획 고려사항
	DB보안 정책 수립	DB보안 정책 정의
		DB보안 정책 필요성
		DB보안 정책 구성
	DB보안 위협 및 대응	DB보안 대상 식별
		위협 분석
		대응방안 수립

2. 보안 가이드라인

2.1 가이드라인의 구성 (2/3)

구분	주제영역	적용영역
DB보안 실무	DB 접근제어	개요
		설계
		구축
	DB 암호화	개요
		설계
		구축
	DB 작업결재	개요
		설계
		구축
	DB 취약점 분석	개요
		설계
		구축
		주요 DB별 취약점 점검 리스트

2. 보안 가이드라인

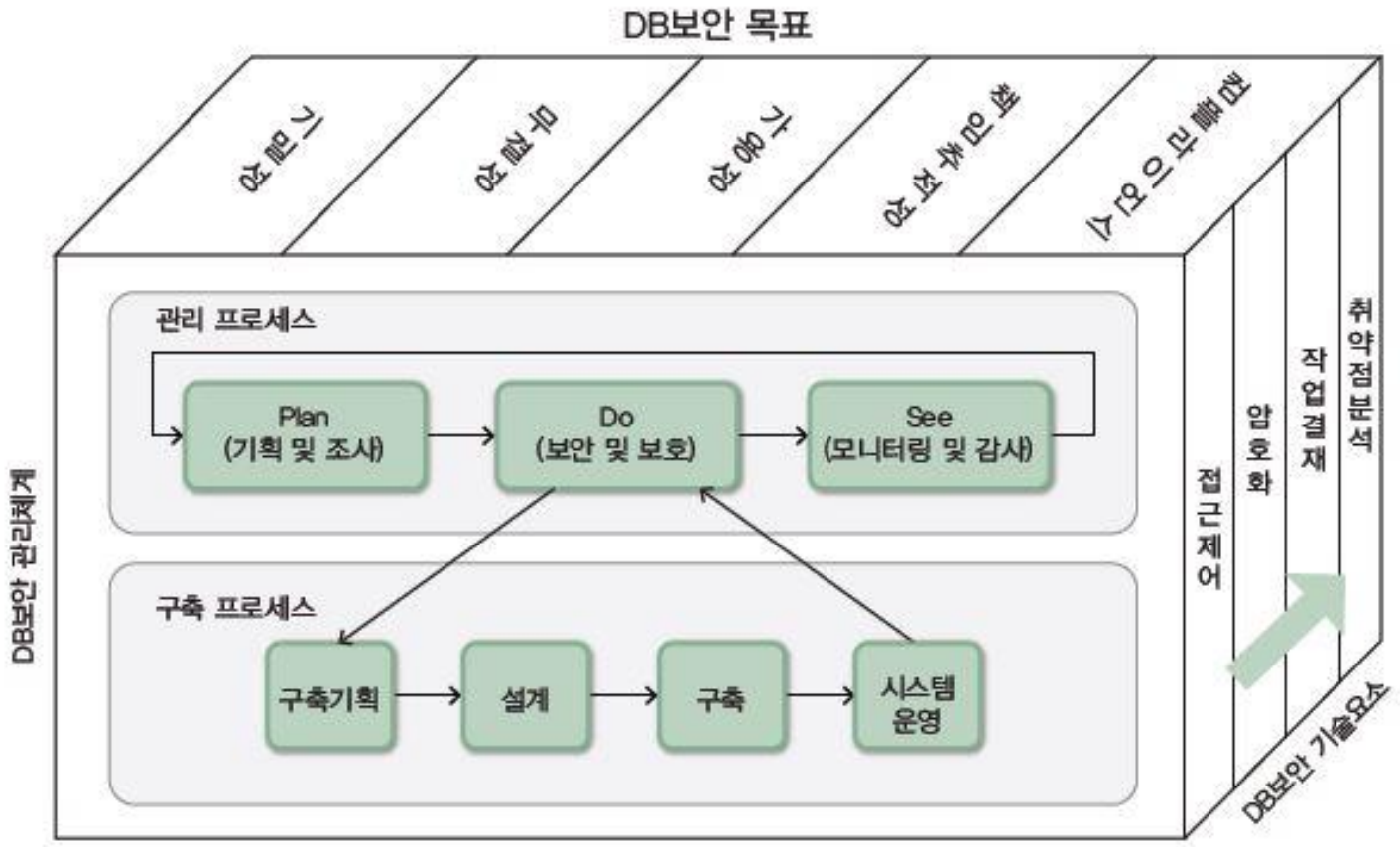
2.1 가이드라인의 구성 (3/3)

구분	주제영역	적용영역
DB보안 운영	감사 및 모니터링	보안정책의 평가
		신규 시스템 도입 대응
		모니터링
	변경 관리	변경관리 개요
		변경관리 정책 및 통제 절차
		변경의 역할 및 책임
	운영 현황 보고	접근제어
		암호화
		작업결제
		취약점 분석
	컴플라이언스 대응	컴플라이언스 개요
		DB보안시스템별 점검

3. 보안 가이드라인 주요 내용

3.1 DB보안 프레임워크 구조

DB보안 프레임워크는 전면의 DB보안 관리체계가 중심이 되어 윗면의 DB보안 목표와 측면의 DB보안 기술요소들을 연결하는 육면체로 구성되어 있다.



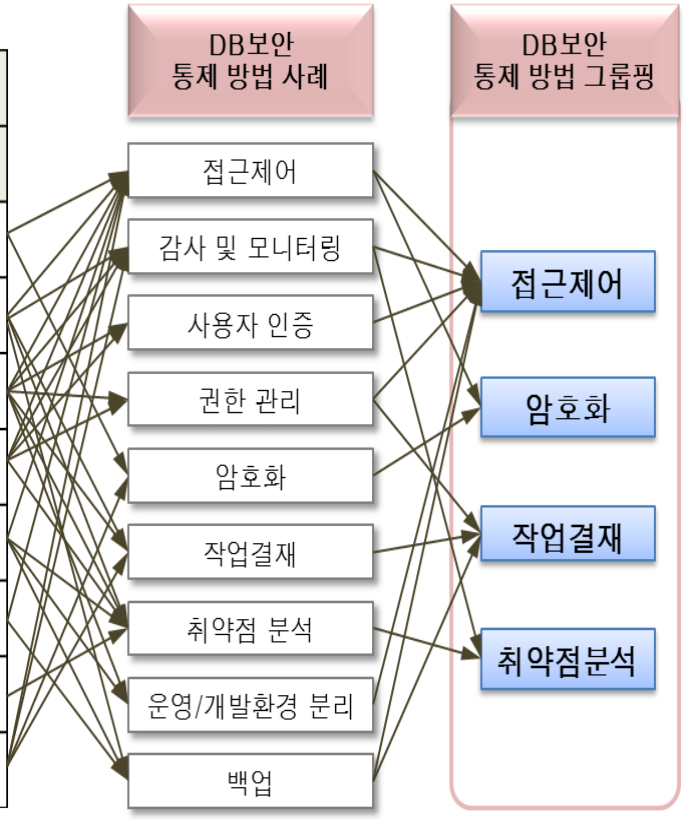
[DB보안가이드라인 2014 개정: DB보안 프레임워크]

3. 보안 가이드라인 주요 내용

3.1 DB보안 프레임워크 구조: DB보안 기술요소 도출

여기서 제시된 기술요소들을 모두 도입해야 하거나 일시에 도입해야 하는 것은 아니며 보호대상 DB자산에 대한 위험평가 결과 및 조직의 역량을 감안하여 부분적 또는 단계적으로 도입할 수 있다. 다만, 각 기술요소들이 상호보완적으로 작용하므로 가짓수가 많을수록 보안수준은 올라간다.

DB보안 위협요소	DB보안 3요소		
	기밀성	무결성	가용성
데이터 노출・유출	○		
부적절한 변경	○	○	○
부적절한 접근	○		○
정당한 접근의 차단/거부			○
DB서비스 실패			○
DB의 물리적인 손상		○	○
보안 취약점 노출	○	○	○
개인정보보호 등 법적요건준수	○	○	○

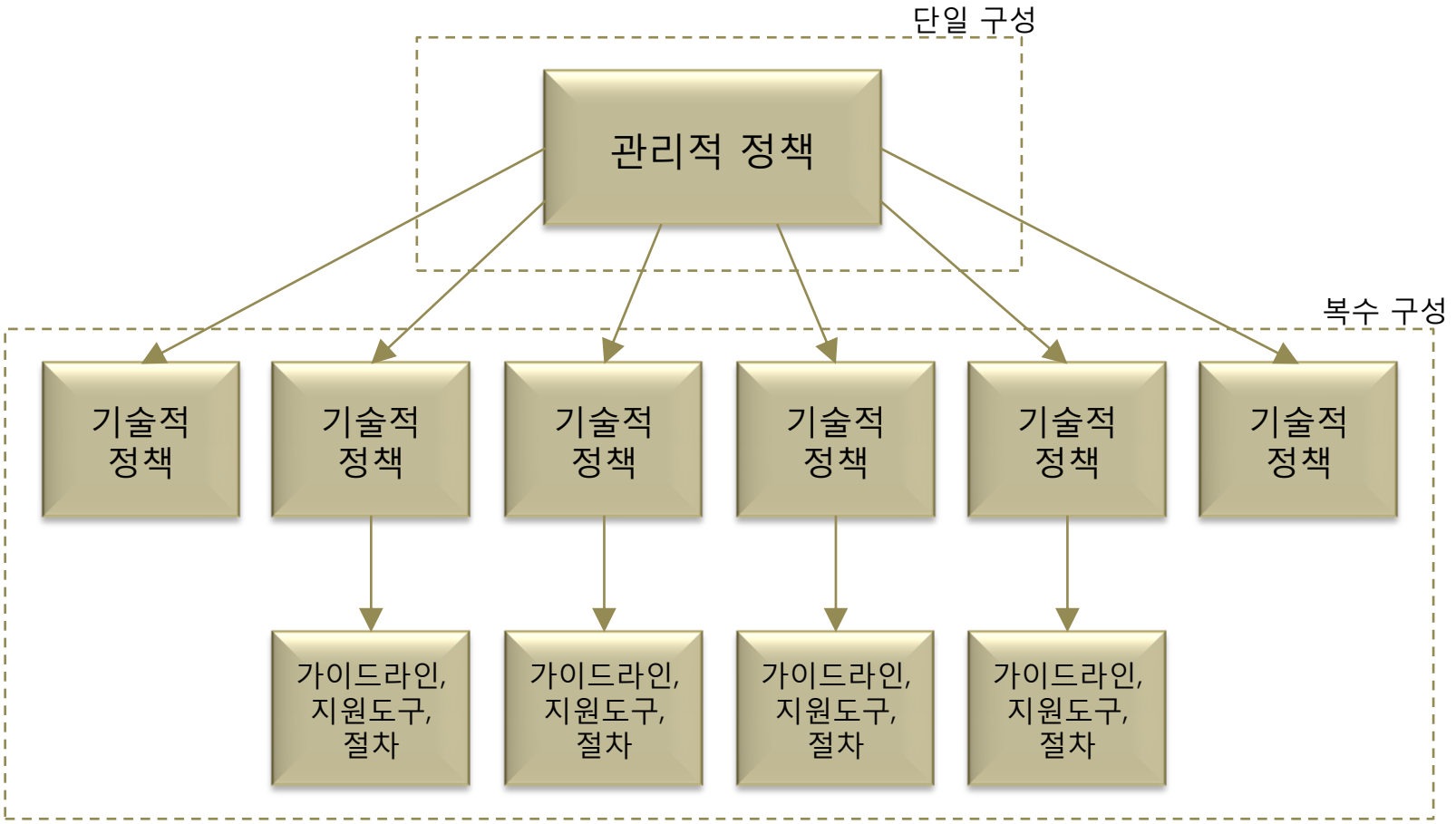


[DB보안가이드라인 2014 개정: DB보안 기술요소의 도출]

3. 보안 가이드라인 주요 내용

3.2 DB보안 정책 구성

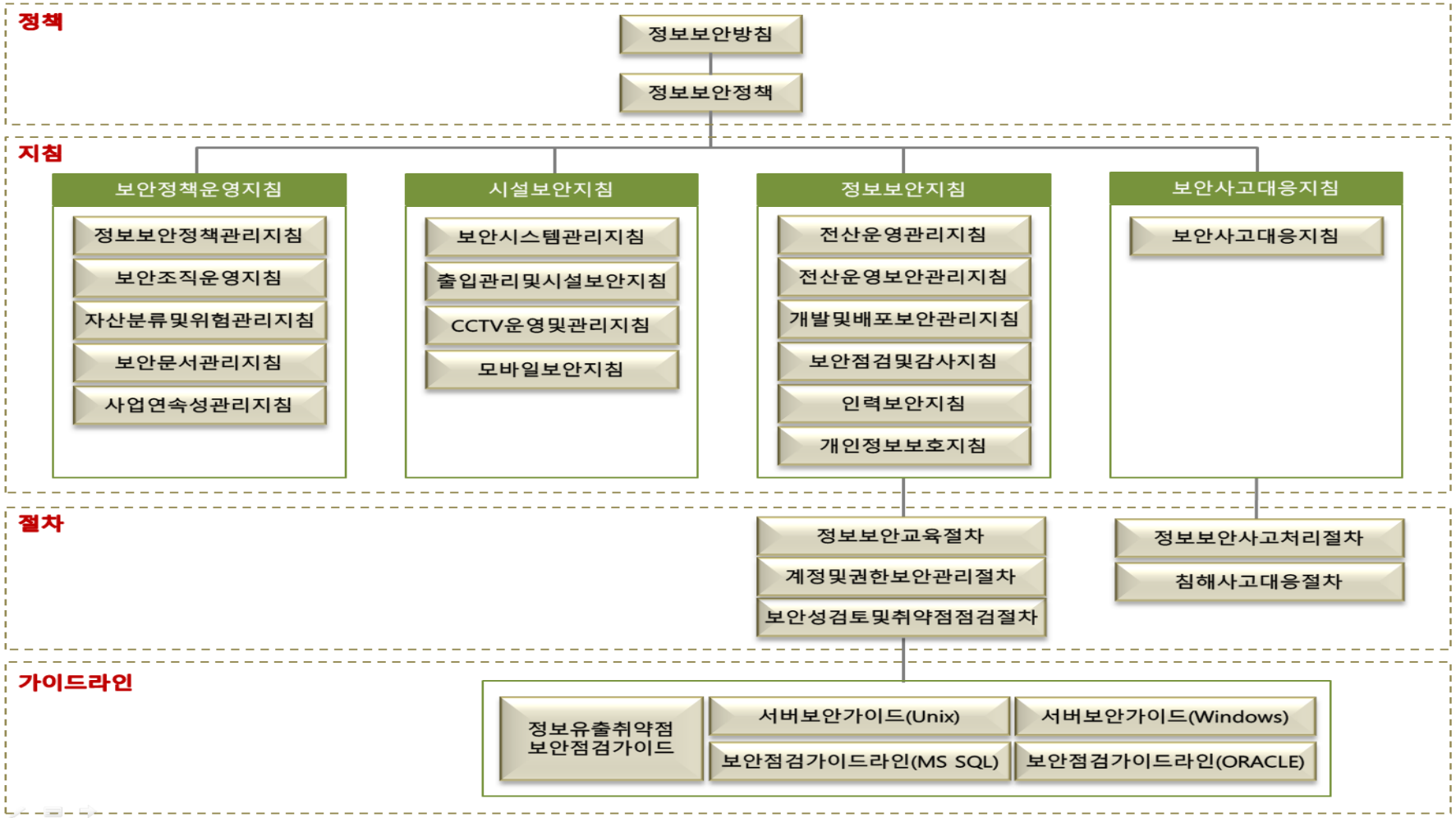
보안정책의 구성은 그 성격이나 위상에 따라 관리적 정책, 기술적 정책, 상세 가이드라인의 3계층으로 나누어지며 각 단계별 문서 세트로 구성된다.



[DB보안가이드라인 2014 개정: DB보안 정책의 계층적 구성]

3. 보안 가이드라인 주요 내용

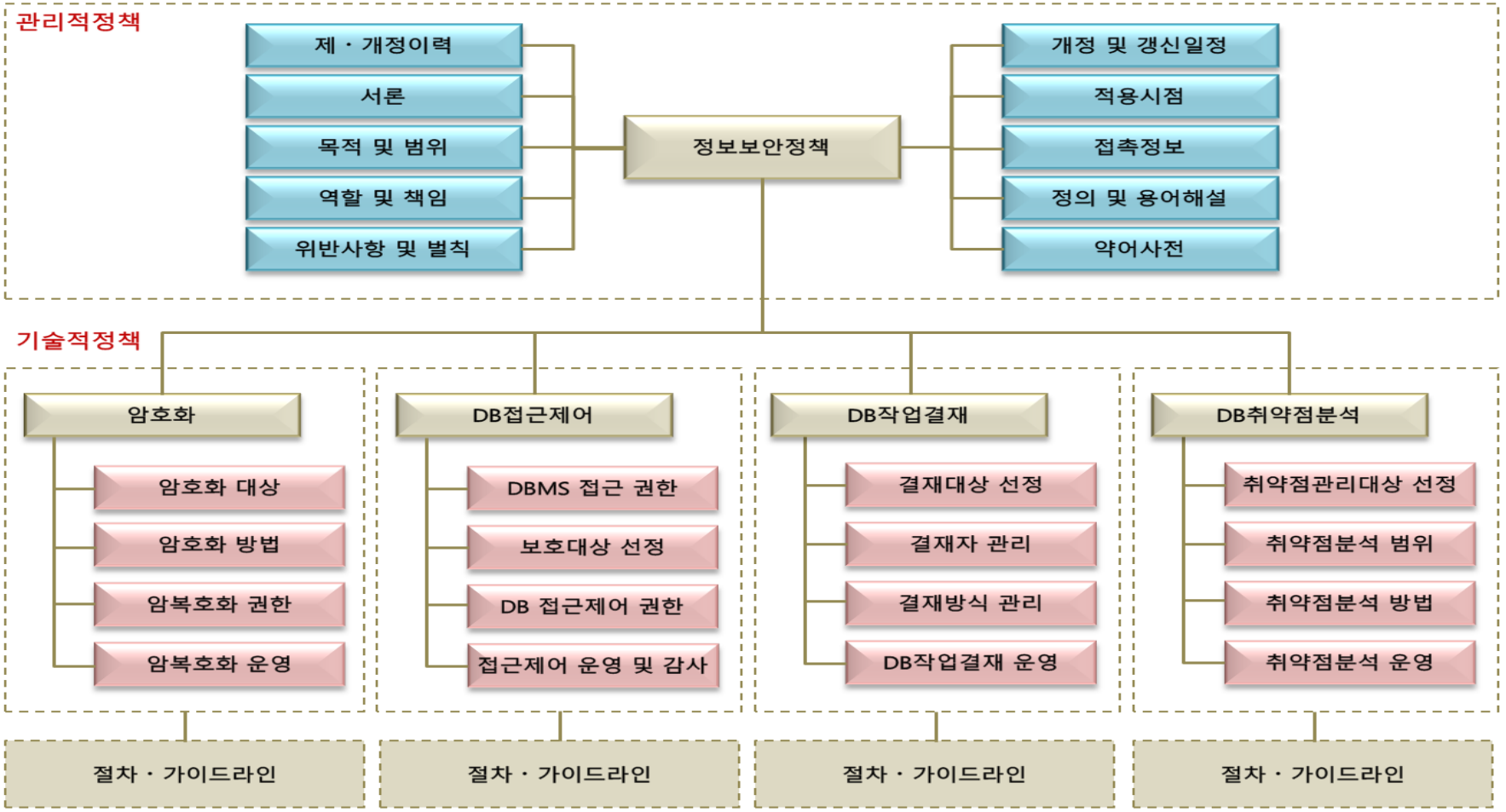
3.2 DB보안 정책 구성: 사례



[DB보안가이드라인 2014 개정: DB보안 정책의 계층적 구성 사례]

3. 보안 가이드라인 주요 내용

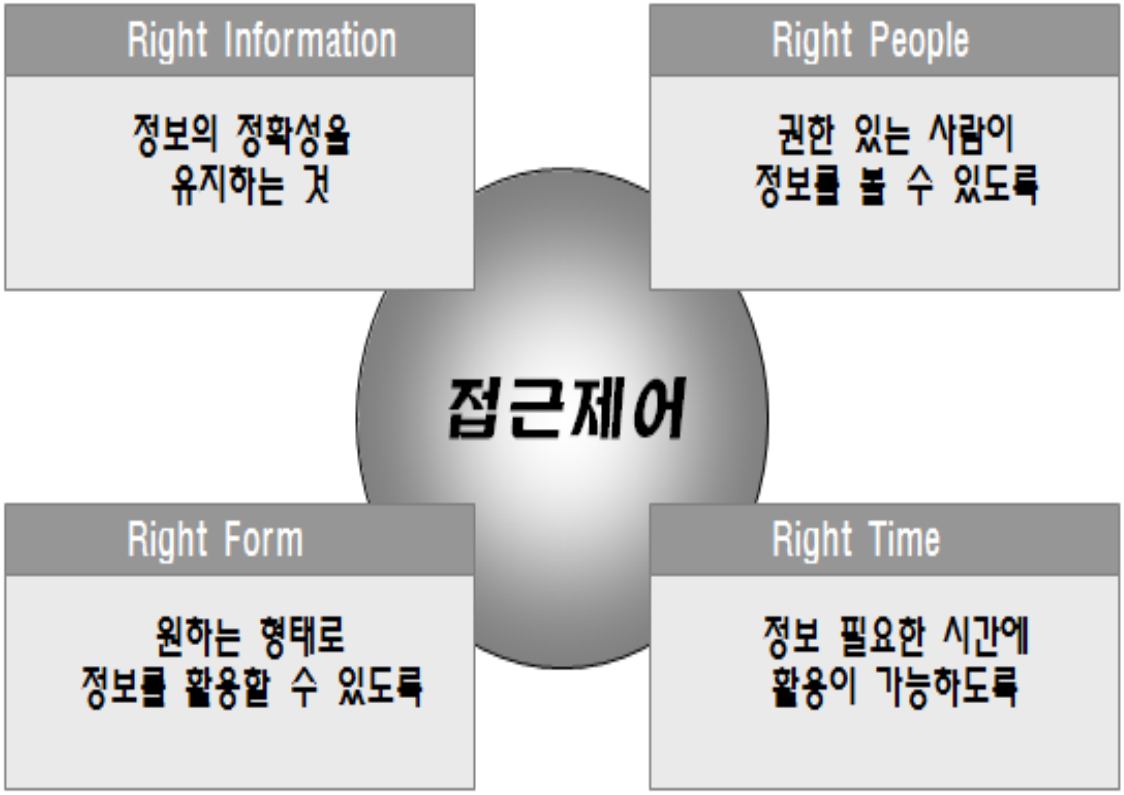
3.2 DB보안 정책 구성: 案



[DB보안가이드라인 2014 개정: DB보안 정책 구성안]

3. 보안 가이드라인 주요 내용

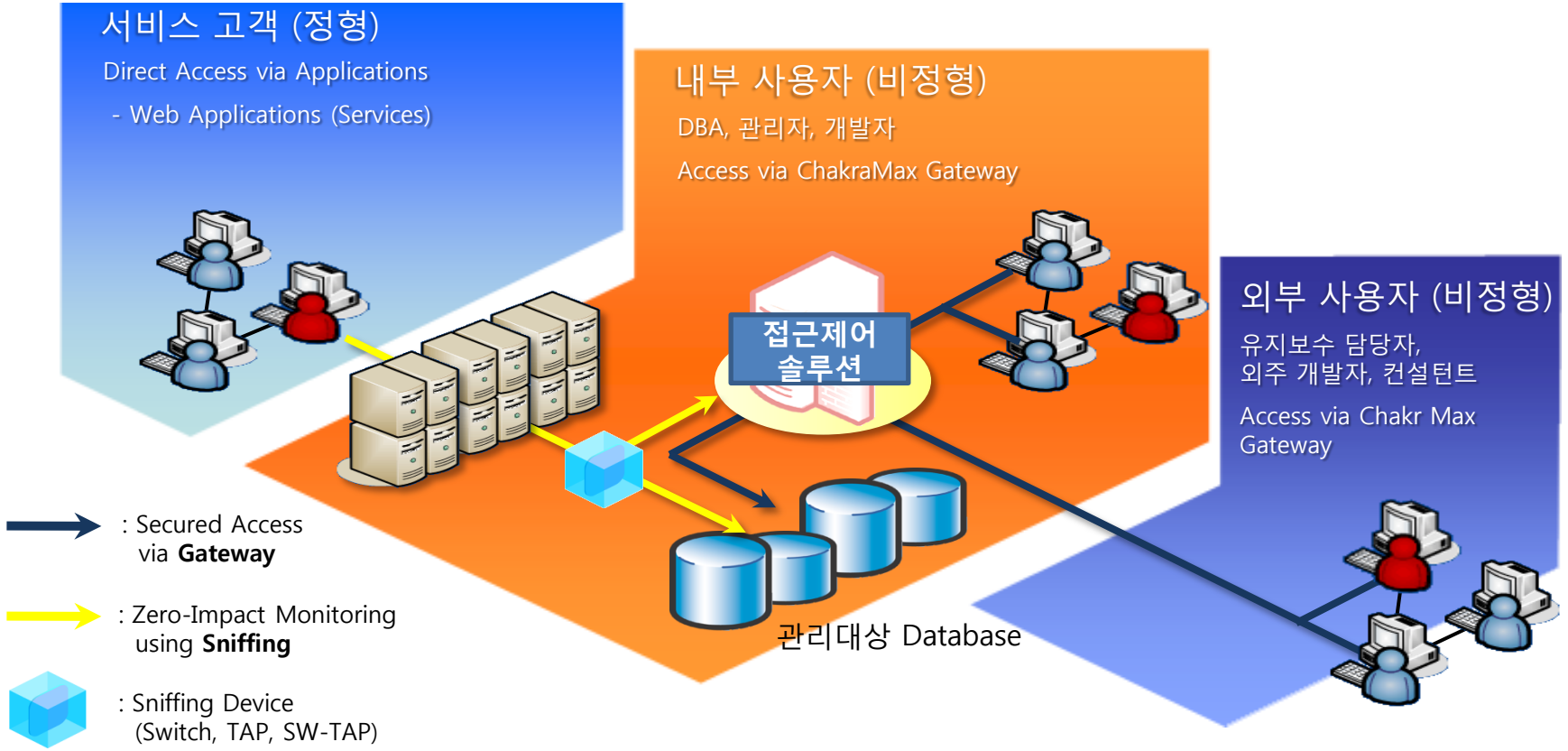
3.3 접근제어: 구성요소



[DB보안가이드라인 2014 개정: 접근제어 구성요소]

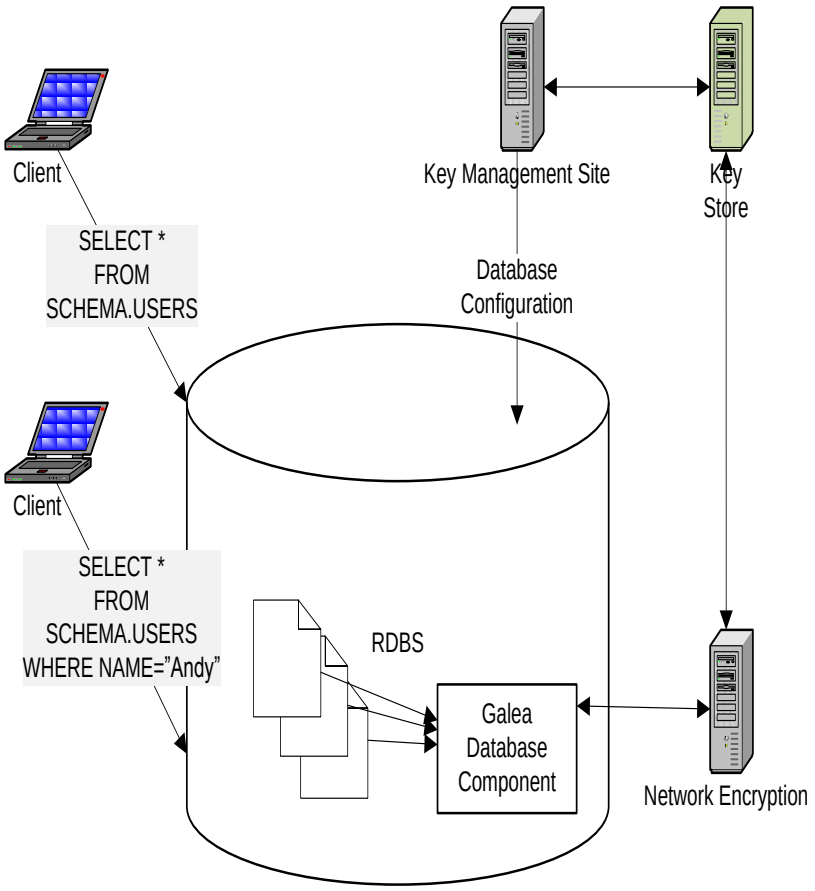
3. 보안 가이드라인 주요 내용

3.3 접근제어: 구성 가이드라인



3. 보안 가이드라인 주요 내용

3.4 암호화: 구성요소



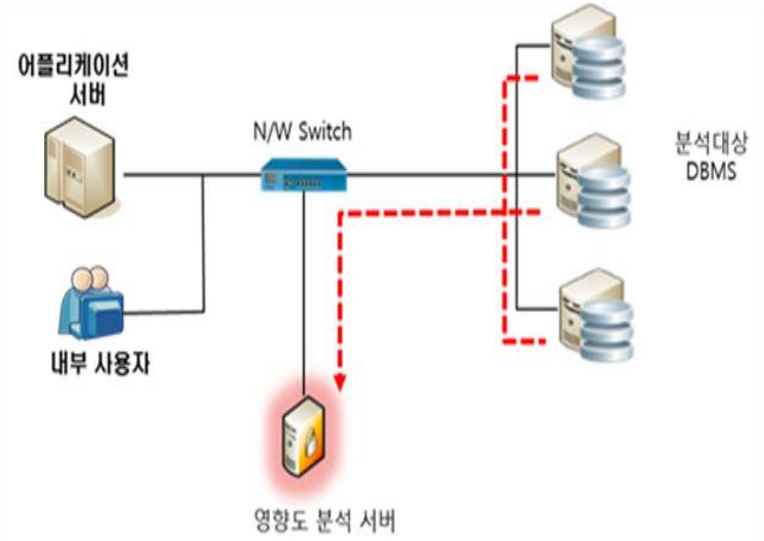
구성요소	주요기능
관리자 콘솔	운영 콘솔
	암호화 대상 Database-Table-Column 설정
	암호화 진행 요청 / 복호화 진행 요청
	Key Server의 운영 구성 설정
	접근제어 정책 설정 및 리포팅
암복호화 엔진	암복호화 수행
	암복호화 시 Key Server와 연계하여 암호화 알고리즘 및 키 적용
Key Server	암복호화 키 저장 서버
	보안 및 정책 설정 값/ 암복호화 모델을 저장 운영 관리

[DB보안가이드라인 2014 개정: 암호화 구성요소]

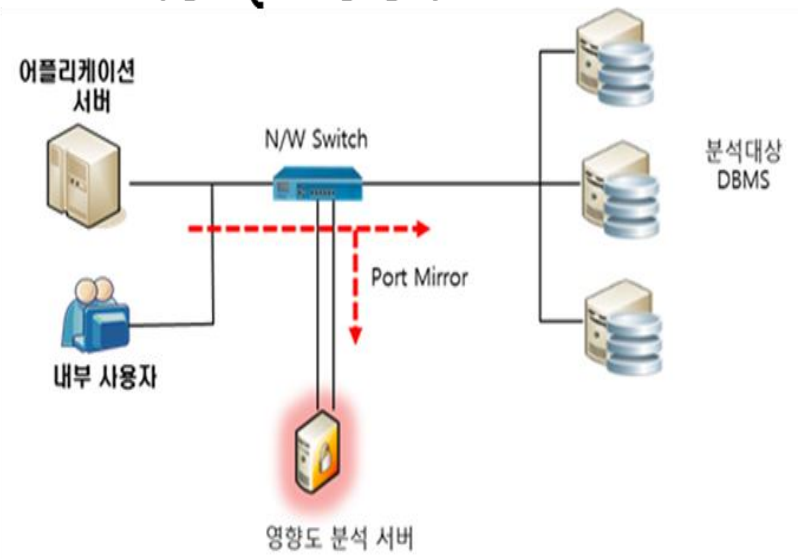
3. 보안 가이드라인 주요 내용

3.4 암호화: 영향도 분석

- DBMS 딕셔너리 수집 방식



- 스니핑 SQL 로깅 방식



[DB보안가이드라인 2014 개정: 영향도 분석용 SQL 수집 방식]

3. 보안 가이드라인 주요 내용

3.4 암호화: 구축 가이드라인(설계 WBS)

				2012년		2013년 1월				2013년 2월				2013년 3월				2013년 4월																		
ID	작업	담당자	산출물	11월	12월	1	2	3	4	1	2	3	4	1	2	3	4	3/30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
01	프로젝트 준비		사업수행계획서																																		
01.01	영향도분석 로그 수집																																				
02	분석																																				
02.01	암호화 대상 선정		최종암호화 리스트																																		
02.02	Database 및 Was 환경 분석		암호화 환경 분석																																		
02.03	영향도분석		영향도 분석보고서																																		
02.03.01	1차 영향도 분석																																				
02.03.02	2차 영향도 분석																																				
03	설계																																				
03.01	암호화 환경 결정	Si	팀																																		
03.02	암호화 교육																																				
03.02.01	PLUGIN & API 암호화 교육		암호화 개발자 가이드																																		
03.02.02	암호화 운영자 교육		운영메뉴얼																																		
03.03	고객사 AP 암호화 설정																																				
03.03.01	개발 Was 암호화 Setting																																				
03.03.02	고객사 연동 Batch 서버 Setting																																				
03.03.03	고객사 개발팀 암호화 관련 개발 지원																																				

[DB보안가이드라인 2014 개정: 암호화 WBS 예시]

3. 보안 가이드라인 주요 내용

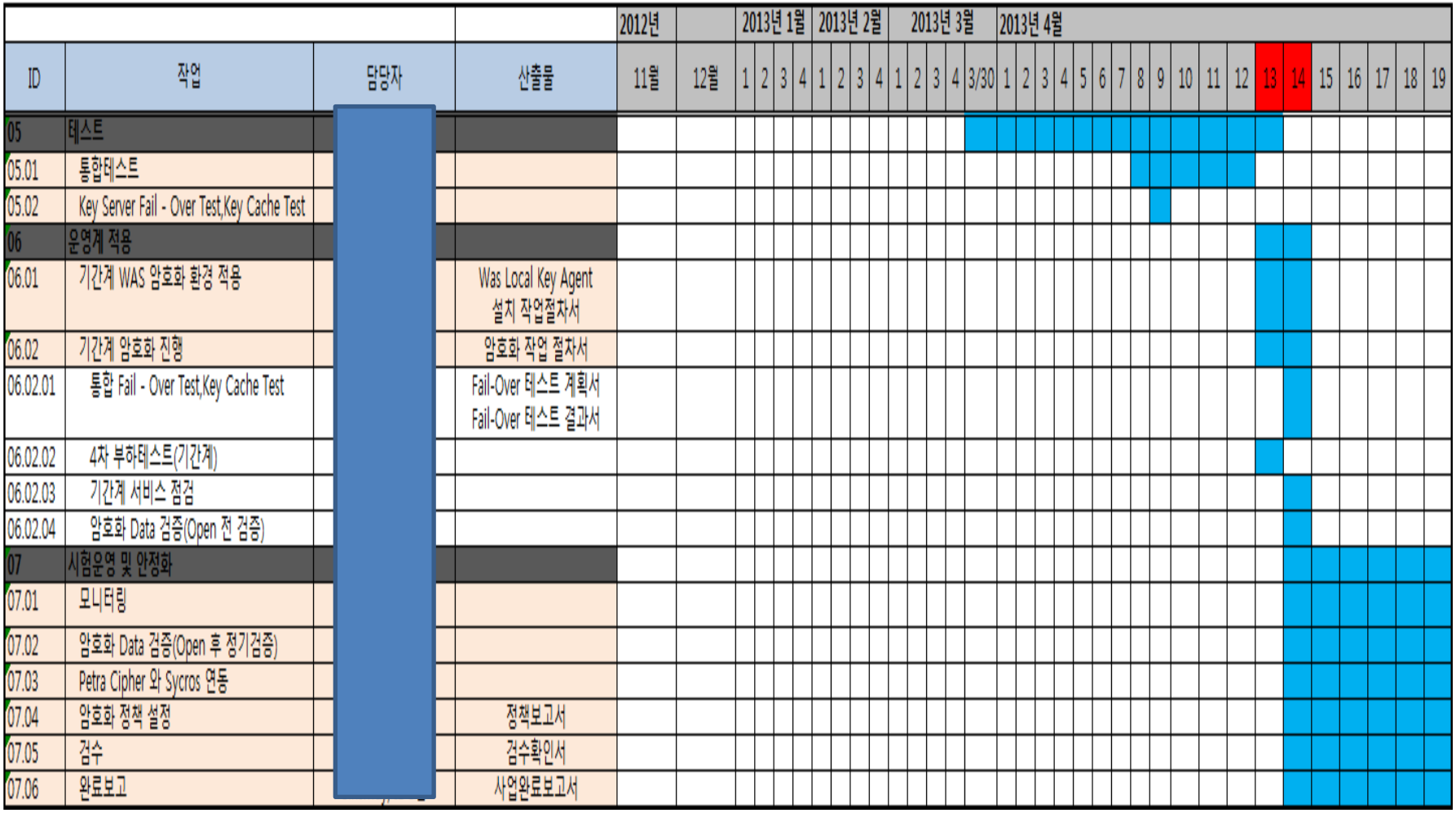
3.4 암호화: 구축 가이드라인(구축 WBS)

ID	작업	담당자	산출물	2012년 11월	12월	2013년 1월 1	2	3	4	2013년 2월 1	2	3	4	2013년 3월 1	2	3	4	3/30	2013년 4월 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
04	구축																																			
04.01	요금계 암호화		암호화 작업 절차서																																	
04.01.01	요금계 1차 암호화																																			
04.01.02	요금계 2차 암호화																																			
04.02	아카이빙																																			
04.02.01	데이터아카이빙																																			
04.02.02	프로그램개발																																			
04.02.03	시스템 적용																																			
04.02.04	데이터 삭제																																			
04.03	WAS 암호화 설정		Was Local Key Agent 설치 작업절차서																																	
04.03.01	프로그램 개발																																			
04.01.03	요금계 3차 암호화																																			
04.01.04	요금계 4차 암호화																																			
04.03.02	1차 테스트																																			
04.03.03	암호화 대상 검증 및 보완																																			
04.03.04	2차 테스트																																			
04.03.05	1차 부하테스트																																			
04.03.06	2차 부하테스트																																			
04.04	기간계 DB, 정보계 DB 암호화 환경 적용		암호화 작업 절차서																																	
04.04.01	기간계 암호화 환경 적용																																			
04.04.02	요금계 5차 암호화																																			
04.04.03	Data 검증용 Trigger 적용																																			
04.04.04	3차 부하테스트(부하걸린 대상 재수정후																																			
04.05	Key Server 도입 및 셋팅		Key Server 설치 작업절차서																																	
04.05.01	OS 설치 및 Network 설정 및 환경설정																																			
04.05.02	암호화 Key Server 설치																																			

[DB보안가이드라인 2014 개정: 암호화 WBS 예시]

3. 보안 가이드라인 주요 내용

3.4 암호화: 구축 가이드라인(테스트 & 적용 WBS)



ID	작업	담당자	산출물
05	테스트		
05.01	통합테스트		
05.02	Key Server Fail - Over Test,Key Cache Test		
06	운영계 적용		
06.01	기간계 WAS 암호화 환경 적용		Was Local Key Agent 설치 작업절차서
06.02	기간계 암호화 진행		암호화 작업 절차서
06.02.01	통합 Fail - Over Test,Key Cache Test		Fail-Over 테스트 계획서 Fail-Over 테스트 결과서
06.02.02	4차 부하테스트(기간계)		
06.02.03	기간계 서비스 점검		
06.02.04	암호화 Data 검증(Open 전 검증)		
07	시험운영 및 안정화		
07.01	모니터링		
07.02	암호화 Data 검증(Open 후 정기검증)		
07.03	Petra Cipher 와 Sycros 연동		
07.04	암호화 정책 설정		정책보고서
07.05	검수		검수확인서
07.06	완료보고		사업완료보고서

[DB보안가이드라인 2014 개정: 암호화 WBS 예시]

3. 보안 가이드라인 주요 내용

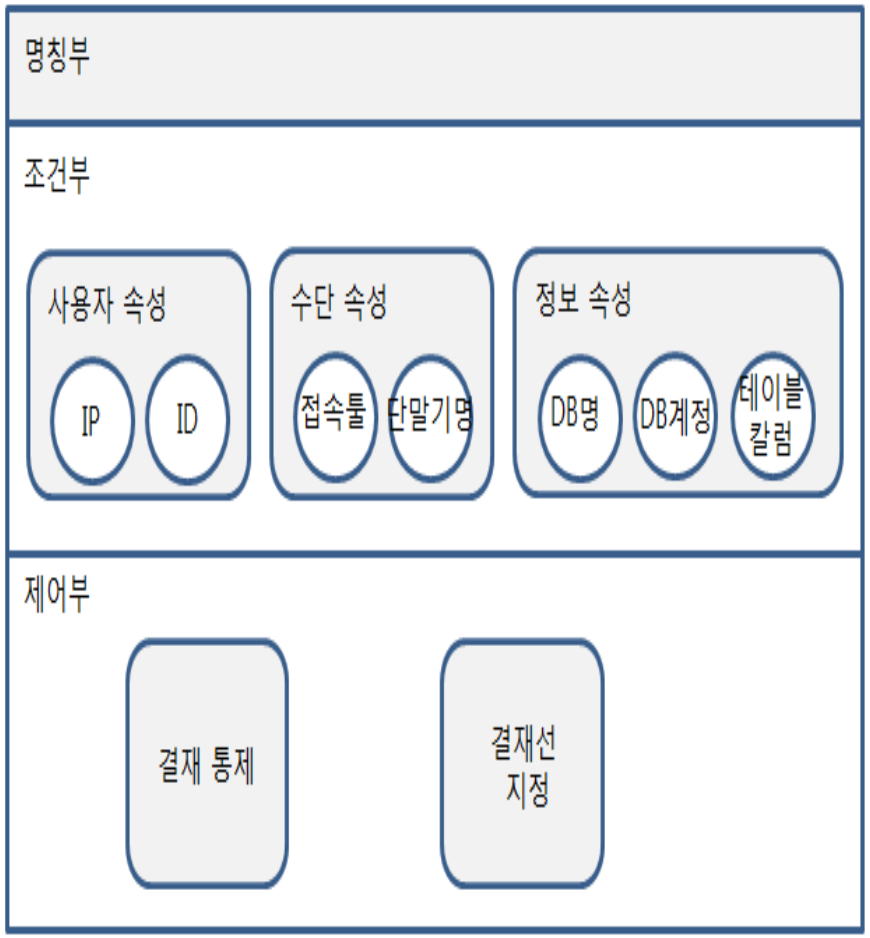
3.4 암호화: 구축 가이드라인(원상복귀 WBS)

				2012년		2013년 1월				2013년 2월				2013년 3월				2013년 4월																		
ID	작업	담당자		11월	12월	1	2	3	4	1	2	3	4	1	2	3	4	3/30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
01	기간계 암호화 원복																																			
01.01	기간계 AP 다운																																			
01.02	기간계 AP 소스 원복(공통 모듈)																																			
01.03	대상 테이블/인덱스 Rename 처리 (암호화																																			
01.04	원본 백업 테이블/인덱스 Rename																																			
02	기간계 아카이빙 대상 암호화 테이블 원복																																			
02.01	대상 테이블/인덱스 Rename 처리 (암호화																																			
02.02	원본 백업 테이블/인덱스 Rename																																			
02.03	연관 Object 삭제																																			
02.04	연관 Object 변경 (원복)																																			
02.05	기간계 AP 기동																																			
02.06	서비스 점검																																			

[DB보안가이드라인 2014 개정: 암호화 WBS 예시]

3. 보안 가이드라인 주요 내용

3.5 작업결재: 구성요소

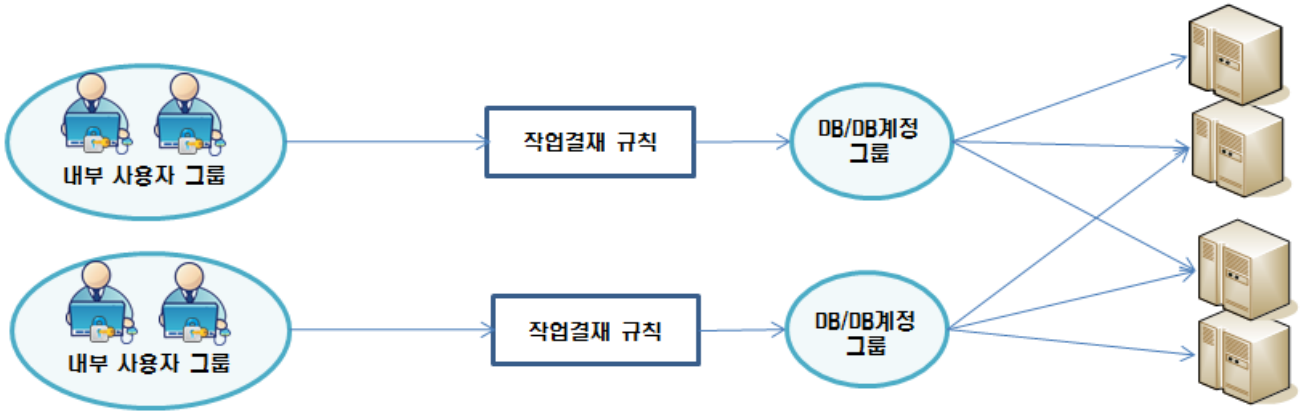


구성 요소	설명
DB 사용자 정보	DB에 접근할 수 있는 사용자들에 대한 IP, ID, 성명, 조직, 연락처 등에 관한 정보
결재자 정보	결재자, 결재선 구성에 대한 정보
DB 정보	사용자가 접속할 수 있는 DB에 대한 정보
통제 규칙	작업결재 규칙 정보
딕셔너리 정보	테이블, 컬럼 단위로 설정을 위해 목표 DBMS의 딕셔너리에서 가져오거나, SQL을 Parsing 하여 저장하는 정보로서, DB계정, 테이블, 컬럼 정보 등으로 구성된다.

[DB보안가이드라인 2014 개정: 결재규칙의 구성요소]

3. 보안 가이드라인 주요 내용

3.5 작업결재: 규칙구성 가이드라인



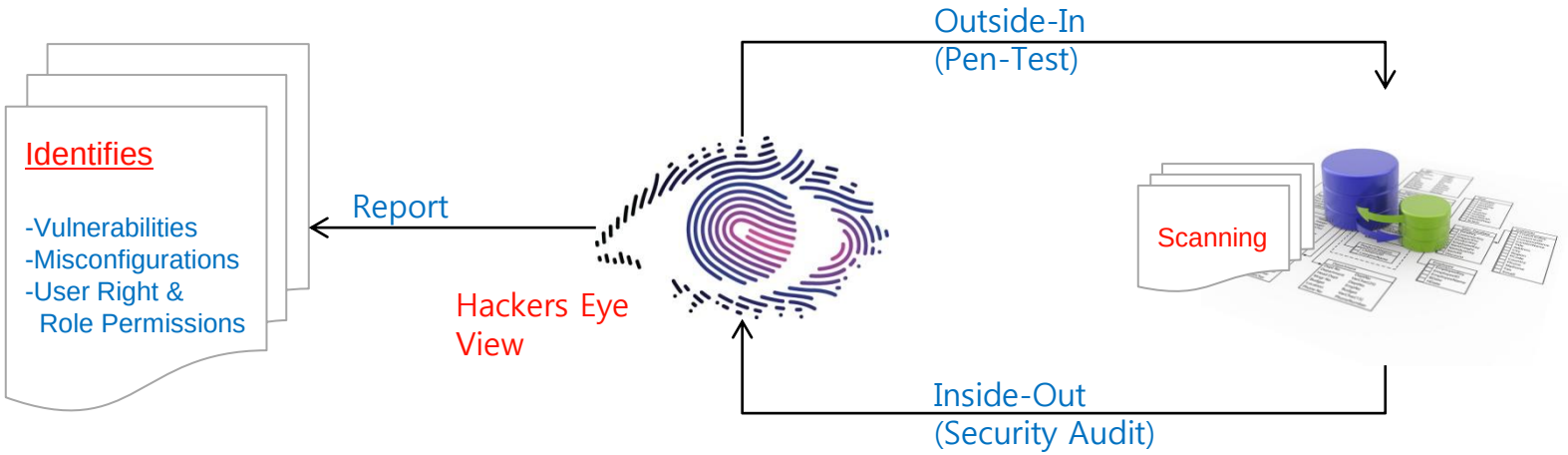
구분	통제방안	접근제어 정책	동작 방식	제어 범위	정책 분류
작업결재	주요 Table 조회 시 통보	주요 Table 조회 시 사전(업무시간)/ 사후(업무 외 시간) 결재	GW	테이블	결재
	DB Data 변경 방지	운영 DB DML/PLSQL 작업 시 사전 (업무시간)/사후(업무 외 시간) 결재	GW	테이블	결재
	DB 구조 변경 통제	운영 DB DDL 작업 시 사전 결재/개 발 DB DDL 작업 시 사후 결재	GW	DB전체	결재
	사용자 통제	주요 Data Return row 값 Export 차단	GW	DB전체	결재

[DB보안가이드라인 2014 개정: 결재규칙 관리]

3. 보안 가이드라인 주요 내용

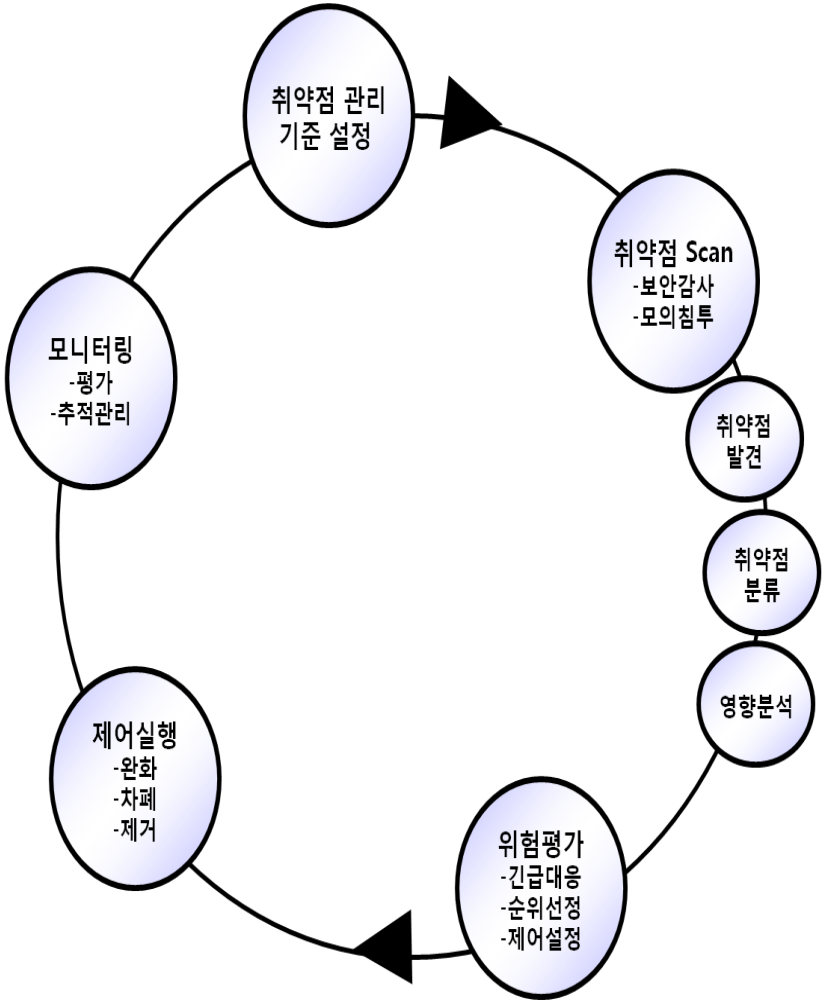
3.6 취약점 분석: 정의

DBMS내에 내재된 보안 취약점들이 악용되기 전에 발견하여 평가(Assessment), 차폐(Shielding), 완화(Mitigation), 추적관리(Monitoring) 등을 수행하는 보안 프로세스 상의 핵심 활동.



3. 보안 가이드라인 주요 내용

3.6 취약점 분석: 라이프 사이클

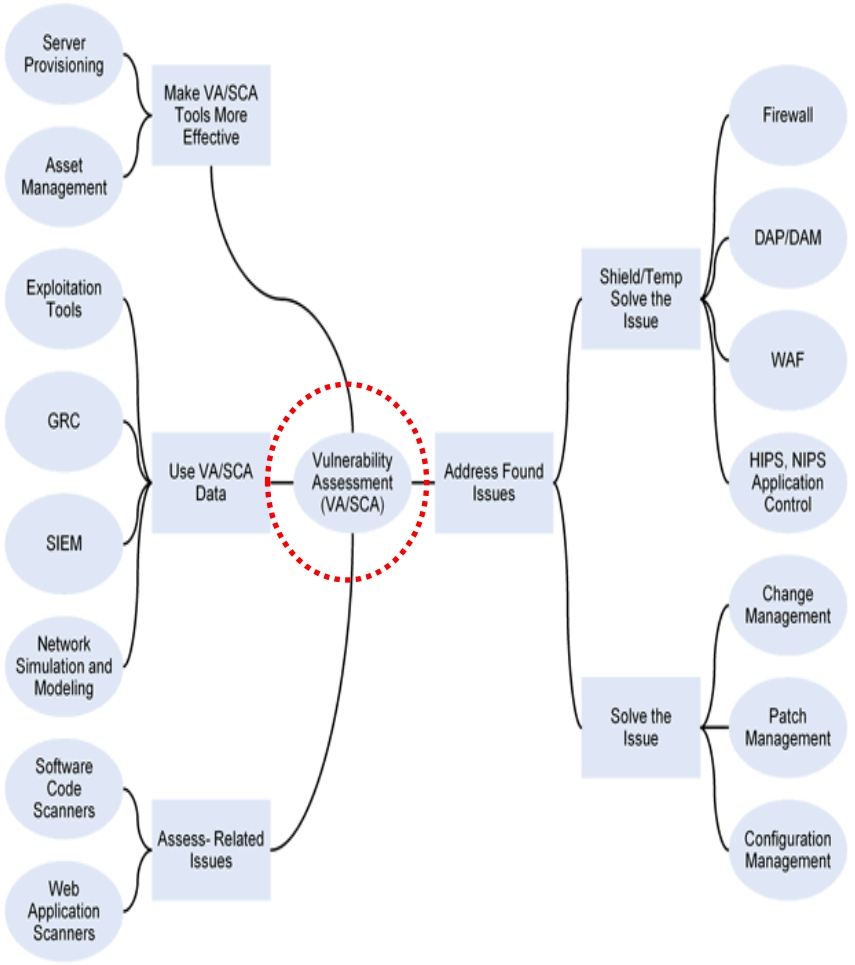


단계	활동 내용
취약점 관리 기준 설정	DB 취약점 관리 전략 수립 및 정책 설정, 대응 지침, 위험 평가 기준, R&R 등의 기준 수립
취약점 Scan	관리 대상 DBMS의 취약점을 검출, 분석하는 단계로서 DBMS 자체의 보안 감사(Security Audit), 모의 침투(Penetration Test) 방식 적용
위험 평가	검출 된 취약점 자체의 위험도 및 연관 위험도 평가하여 각 취약점의 대응 방안 설정
제어 실행	대응 방식 및 우선 순위에 따라 분류 된 취약점의 제어 및 제거
모니터링	각 취약점 및 제어가 실행된 내역의 추적 관리, 제어 실행 내용의 보안 평가, 취약점 관리 기준 개정의 기초 데이터로 활용

[DB보안가이드라인 2014 개정: 취약점 관리 라이프 사이클]

3. 보안 가이드라인 주요 내용

3.6 취약점 분석: 보안 인프라의 연계



데이터의 활용	대응 연계	연계 분석
GRC 대응	**임시 대응, 차폐, 완화를 위한 연계** -Firewall, 접근제어(DAP/DAM) -WAF, HIPS, NIPS	-Software code 취약점 분석 -Web application 취약점 분석 -Network 취약점 분석 -Server 취약점 분석
SIEM 운영 효율 향상	**제거를 위한 연계** -Change Management -Patch Management -Configuration Management	
네트워크 경로 모델링 및 테스트	**관리 효율 증진을 위한 연계** -Server Provisioning -Asset Management	
취약점 검출 툴 개발		

[DB보안가이드라인 2014 개정: 취약점 관리와 보안 인프라의 연계]

3. 보안 가이드라인 주요 내용

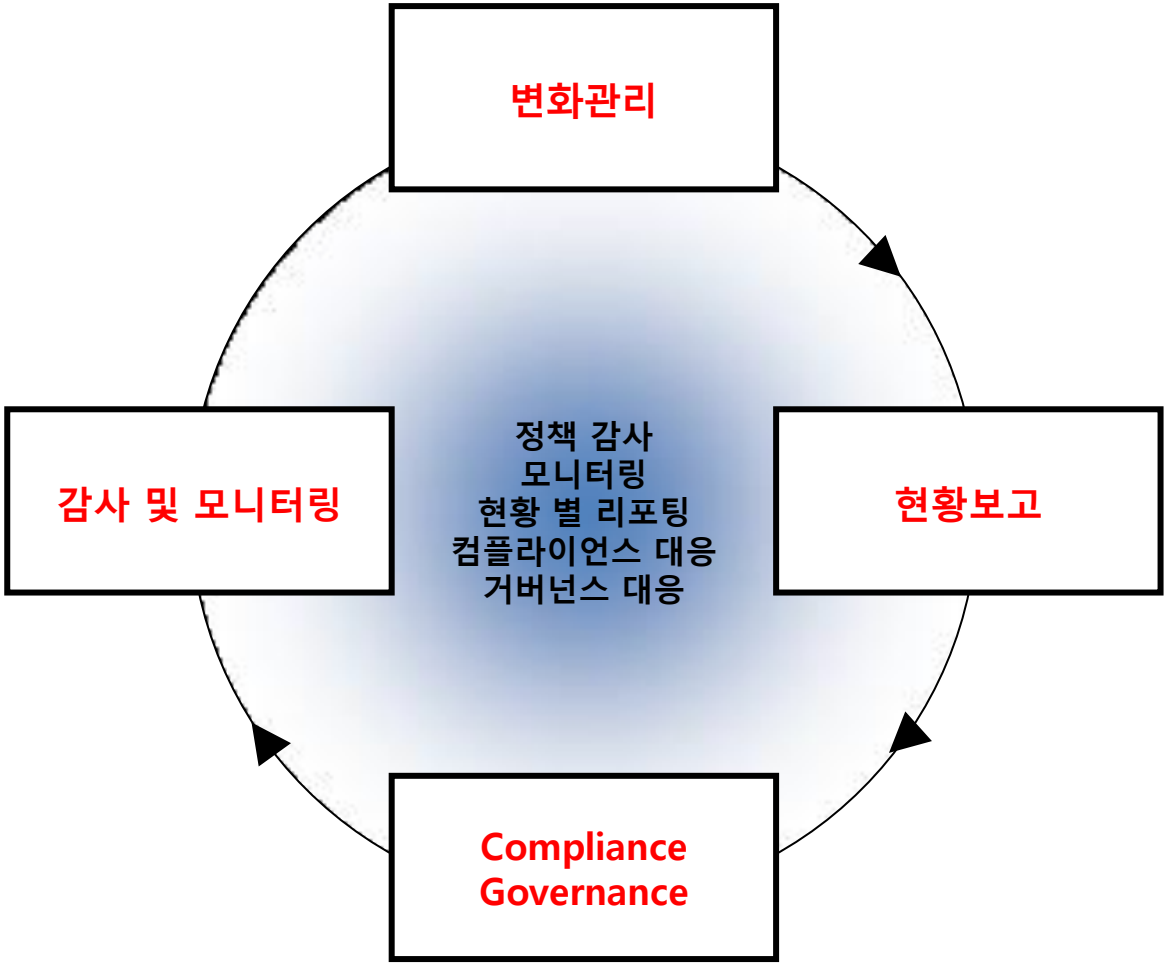
3.6 취약점 분석: 분석 유의점

항목	보안 감사	모의 침투
Scan 범위	대상 시스템의 모든 잠재적 취약점 검사	실제로 악용될 수 있는지 확인 및 결정
취약점 검출	이론적이며 표준화된 정보를 바탕으로 취약점 분류	대상 시스템 자원 및 대상 시스템 경로에 대한 취약점 분류
결과의 유용성	오탐(false positives)의 가능성이 있음	대상 시스템 자원의 실제 악용 가능성이 있는 취약점 리포트
Scan 방식	대상 시스템 중심 Auditing (Inside-out)	대상 DBMS를 향한 실제 공격 경로 중심 Attack (Outside-in)
대응 권고 수준	취약점에 대한 설명, 위험 평가, 권고, Patch 알림, 수정 Script 정보 제공	취약점에 대한 설명, 위험 평가, 권고, Patch 알림, 수정 Script 정보 제공
위험 평가	표준 기반의 위험 측정	실제 악용 가능성 기반의 위험 측정

[DB보안가이드라인 2014 개정: 취약점 관리와 보안 인프라의 연계]

3. 보안 가이드라인 주요 내용

3.7 보안운영



Thank you