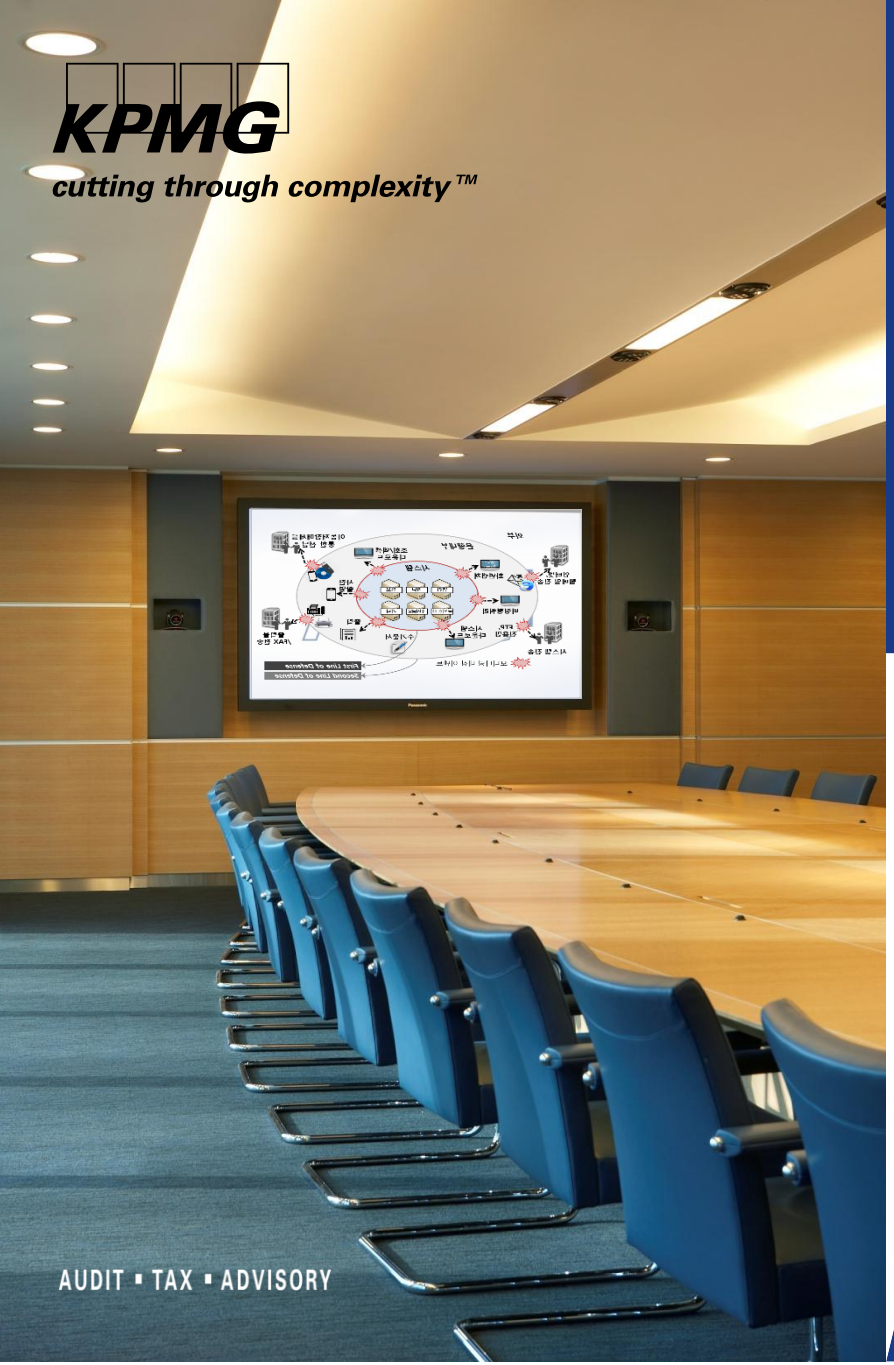


금융기관의 개인정보보호 통합관리 고도화 방안

Dec. 10th 2015

주제발표자 : KPMG삼정회계법인 허은석 이사

KPMG
cutting through complexity™

발표순서

I. 대내외 환경 변화

II. 금융기관의 주요 현황

III. 통합관리 강화 방안

IV. 통합관리시스템 구성안

I. 대내외 환경 변화

1. 정부의 지속적인 유출방지 대책

2. 신기술 도입 및 자율보안체계 강화

I.1 정부의 지속적인 유출방지 대책

개인정보 사고의 근본적 재발방지대책 마련을 위한 정부의 지속적인 유출 방지 대책 발표 및 개인정보보호 유관 법령 제/개정이 진행중이며 이에 대한 신속하고 효과적인 대응이 필요합니다.

정부의 유출방지 대책

3.10 금융분야 개인정보 유출방지 종합대책 2014.03.10 발표	금융회사 책임 강화
개인정보보호법 주민번호 처리금지 2014.08.07 시행	주민등록번호 처리 금지
전자금융거래법 개정	규제개혁 및 보안 강화
신용정보보호법 개정	신용정보 처리 사업자의 책임 강화 및 정보주체 권리 개선

금융기관 대응 현황

현재까지 정부의 유출방지 대책 및 법령 시행에 따른 긴급한 대응으로 체계적인 적용은 미흡한 실정

주요 과제

- 수집항목 최소화
- 법령 근거없는 주민등록번호 처리 금지
- 주민등록번호 암호화 보관
- 정부 가이드라인에 따른 동의서 개정
- 2단계 파기 구축

I.2 신기술 도입 및 자율보안체계 강화

Fintech 활성화, Outdoor Sales 강화, 빅데이터 활성화, 클라우드 발전법, IoT 등 신기술 및 New Trend의 금융권 확산 적용으로 이에 대한 보안 대책 마련이 필요합니다.

Trend	주요 내용
핀테크 활성화	• 보다 간편한 서비스 Needs로 사후 보안 및 모니터링 강화 • 감독기관의 사전규제 완화 및 사후책임 강화로 PCI-DSS 등 글로벌 인증제 도입 및 자율적 보안역량 강화 필요
Outdoor Sales 강화	• ODS(Outdoor Sales), 옴니채널 등 채널 간 융합 서비스 및 스마트 워크 환경 강화 • 모바일 업무처리환경에서의 정보보안 강화 필요
데이터분석 기반 내부통제 강화	• 다양한 내부 취급자의 행위분석을 위한 정형/비정형 원천데이터의 빅데이터 기반 실시간 분석을 통한 내부통제 및 모니터링 강화
클라우드 발전법 시행	• 범정부 차원의 클라우드컴퓨팅 육성 지원 및 클라우드 이용 규제 완화 • 안전한 클라우드 이용 환경 조성을 위한 관련 정보보호 및 이용자 보호 근거 마련
IoT 활성화	• 금융권 비즈니스 부가가치 창출 및 고객 편의성 증대를 위한 다양한 사물인터넷 적용 서비스 증가 • 사물인터넷 취약성을 이용한 금융 사고 및 보안 위협의 확산

정보보호 동향

사전 규제 완화 , 사후보안 강화 및 무한책임

기존의 금융권에 요구되었던 보안 수준의 한 단계 업그레이드 필요

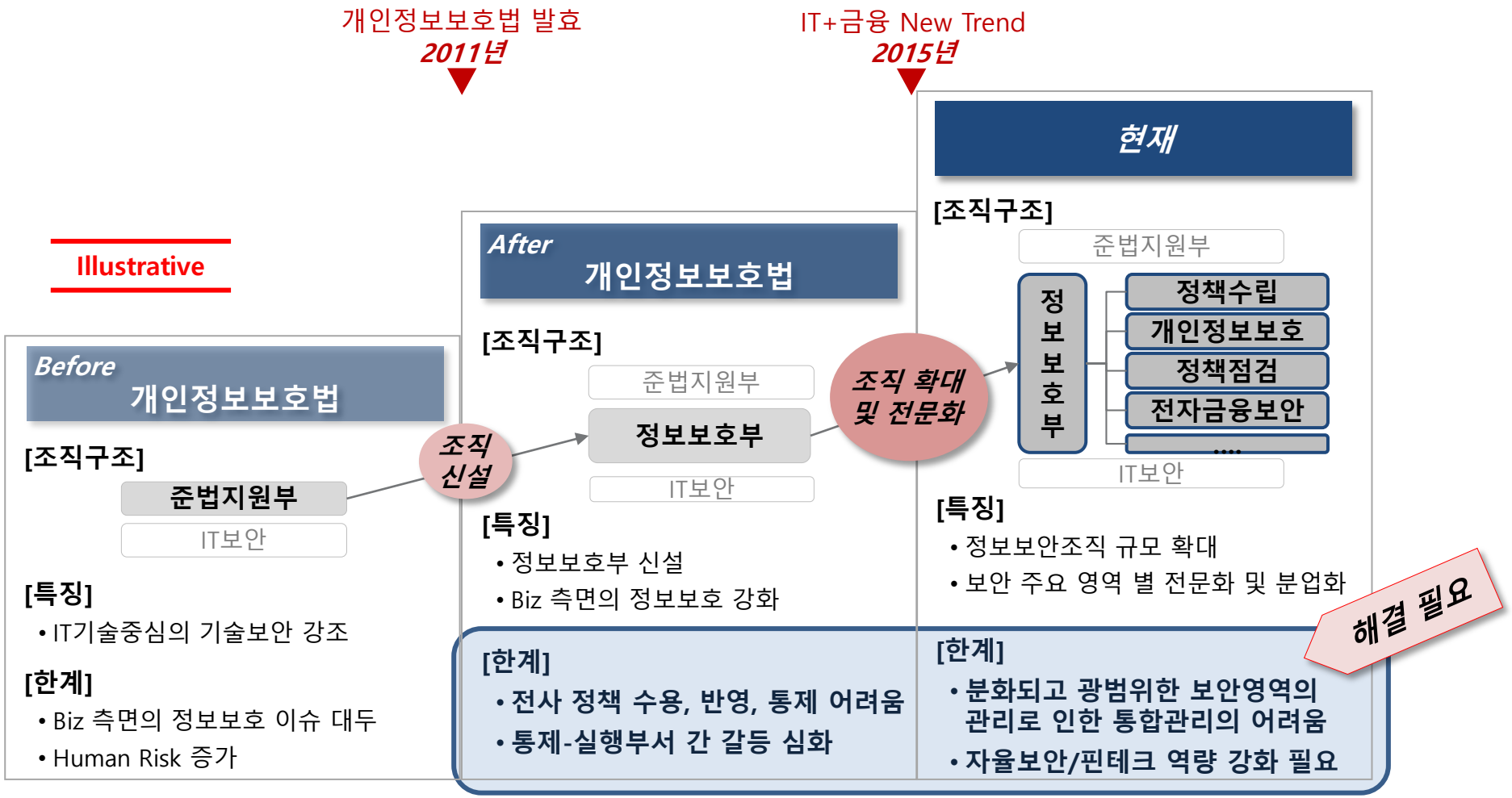
II. 금융기관의 주요 현황

1. 정보보호조직의 대응 현황

2. 통합관리 측면 주요 개선요인

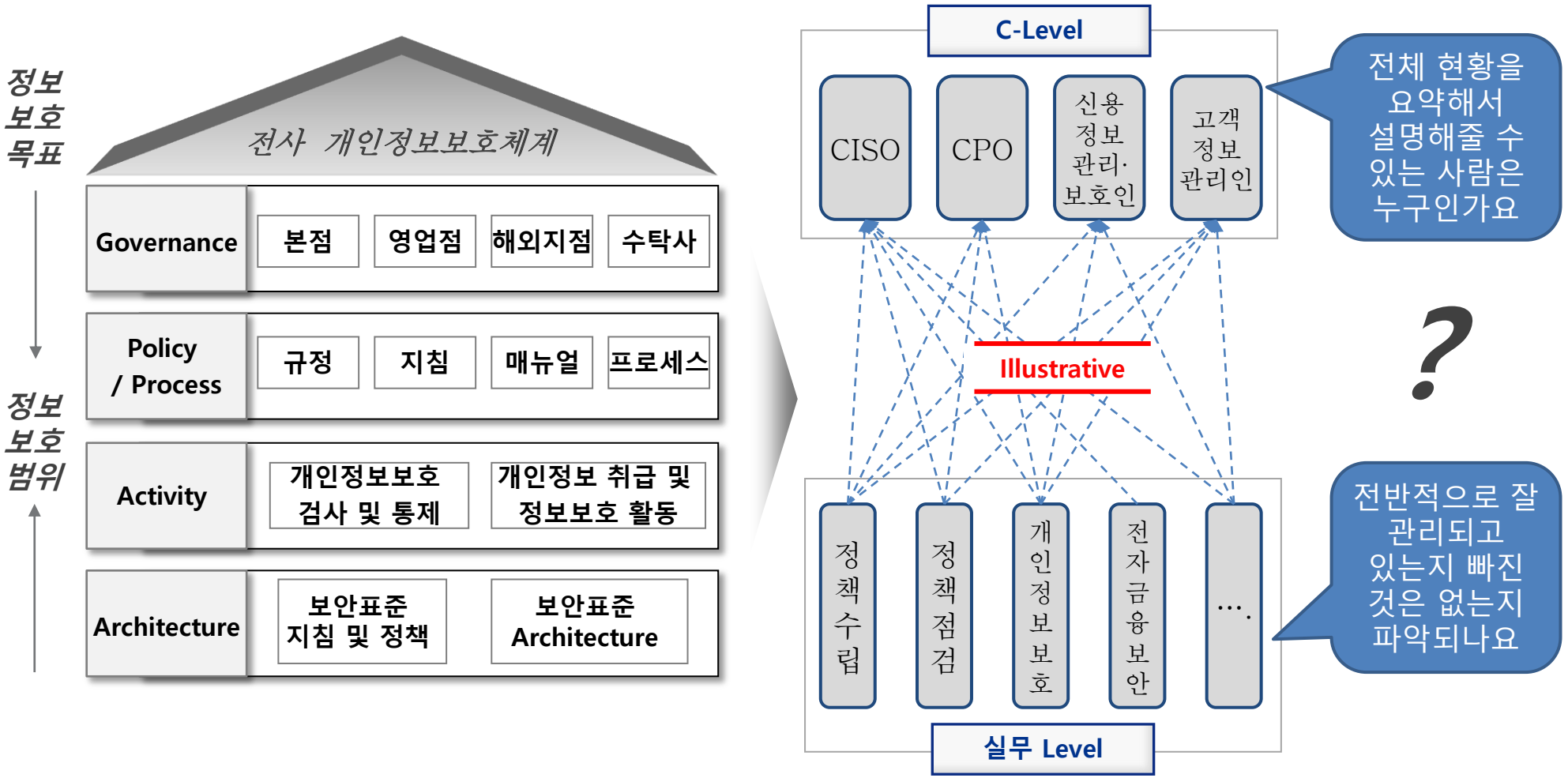
II.1 정보보호조직의 대응 현황

개인정보보호 관련 법률의 강화 및 금융환경의 변화로 인해 각 금융기관 정보보호 조직은 새로운 구조로 변화하고 있으며 보다 분화된 조직구조로 전문화되고 있습니다.



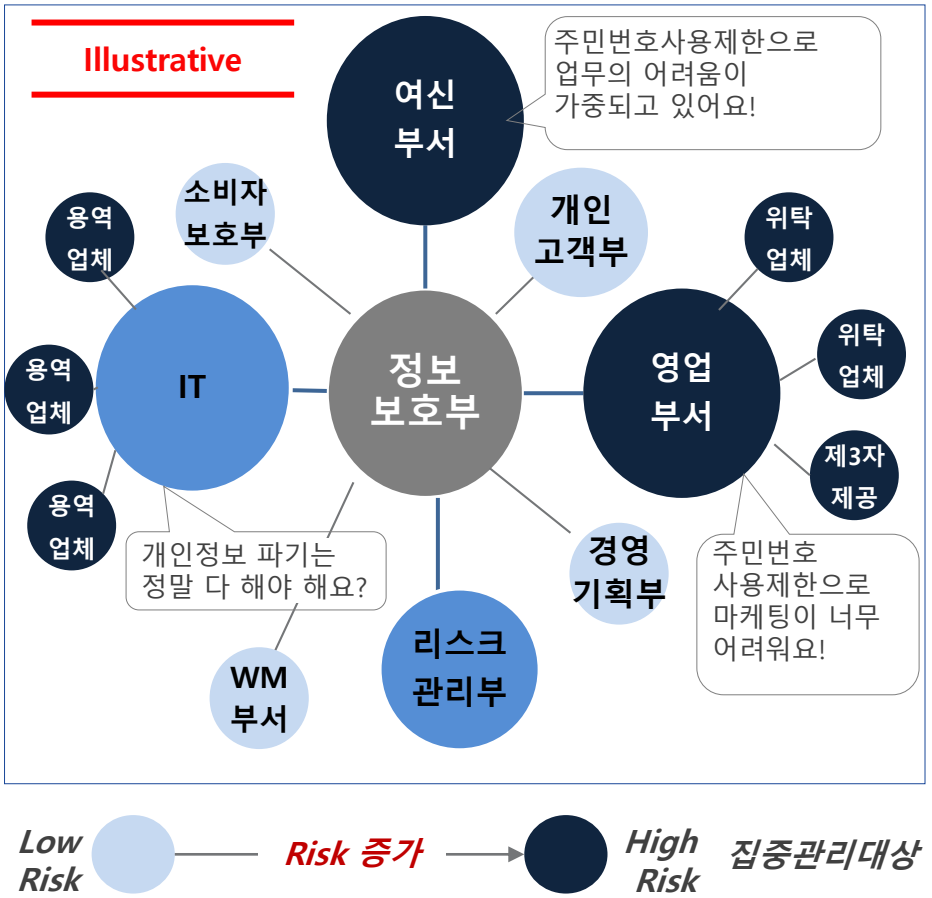
II.1 정보보호조직의 대응 현황, 계속

전사 개인정보보호체계는 개인정보보호 조직 뿐만 아니라 정보보안 전반의 이해와 여러 유관 법률 및 IT보안 영역과 밀접한 관계가 있으나 전체적인 통합관리 측면의 역할이 모호할 수 있습니다.



II.2 통합관리 측면 주요 개선요인

개인정보보호 정책을 수립/점검하는 통제부서와 개인정보를 취급하는 실행부서 간의 불균형 및 업무 수행의 비효율성으로 인해 새로운 통제 패러다임이 요구되고 있습니다.



시사점

☑ **개인정보보호 정책이 현장(본부부서, 영업점, 외주직원 등)에 미치는 한계 존재**

- 각 부서 별 정책 실행 현황 파악 어려움
- 통제를 효율적으로 지원하는 시스템 부재
- 전사 차원 정책 실행 현황 파악 및 효율적 통제를 위한 실직적인 모니터링 방안 필요

실질적, 효율적 통제를 위한 관리 체계 개선 및 시스템 측면 지원이 필요함

III. 통합관리 강화 방안

1. 통합관리 강화 방안 요약
2. 비즈니스 측면 개선방안
3. 시스템 측면 개선방안

III.1 통합관리 강화 방안 요약

개인정보보호 활동에 대한 통합관리 측면 고려가 부족한 것이 현실이며 이 부분에 대한 비즈니스 측면과 시스템 측면 개선이 필요합니다.

통합관리 주요 현황 요약

주요 개선방안

1 비즈니스 측면

- ***정보보호 기능의 분산 및 통합 관리 역량 부재***
  - 정보보호 활동을 위한 명확한 R&R 수립 필요
  - 원활한 정보보호 활동을 위한 소통체계 필요
- **다양한 내/외부 위험에 대한 단편적인 대응**
  - 체계적 관리를 위한 사전 위험 식별 및 통제 정의 필요
  - 단위부서가 아닌 전사 차원의 점검 및 일관된 대응 필요
- **정부가이드에 따른 수동적인 대응 체계**
  - 다양한 정보보호 관련 법령 요구사항 통합 관리 필요
  - 지속적 운영 가능한 자율보안체계 수립 필요

- 각종 위협 및 정부의 가이드에 원활한 대응을 위한 **유기적인 정보보호 관리모델 필요**

2 시스템 측면

- ***세분화된 시스템에 의한 개인정보보호 관리***
  - 다양한 기능별 개별 시스템 및 솔루션에 의한 관리
  - 시스템 간 연관성에 대한 고려가 부족함
- **시스템 중심의 보안 관리**
  - 시스템 기반의 보안 관리
  - 업무 프로세스 상의 개인정보 취약성 고려 부족

- 개인정보 오남용 및 유출위험 방지를 위한 **통합 관리 데이터베이스 구축** 필요
- **비즈니스 기반의 Rule 도출**을 통한 개인정보 이상징후 검출

III.2 비즈니스 측면 개선방안

지속적이고 체계적인 방법을 통해 정보보호 내/외부 현황을 진단하고, 다양한 위협으로부터 조직을 보호하기 위한 정보보호 통합관리 모델의 수립이 필요합니다.

Governance 수립 측면

- **조직 전반에 걸친 정보보호 목표를 달성하기 위해 '정책 및 전략을 통한 지시'와 '성과 모니터링을 통한 통제'를 수행하기 위한 거버넌스의 구성이 필요**
- **개선방안**
  - 분산된 역할 및 책임의 통합 관리
  - 전사 개인정보보호 통합 관리를 위한 커뮤니케이션 채널 마련

Risk 관리 측면

- **리스크 유형별 시나리오를 도출하고 이를 기반으로 정보보호 대책을 구현함**

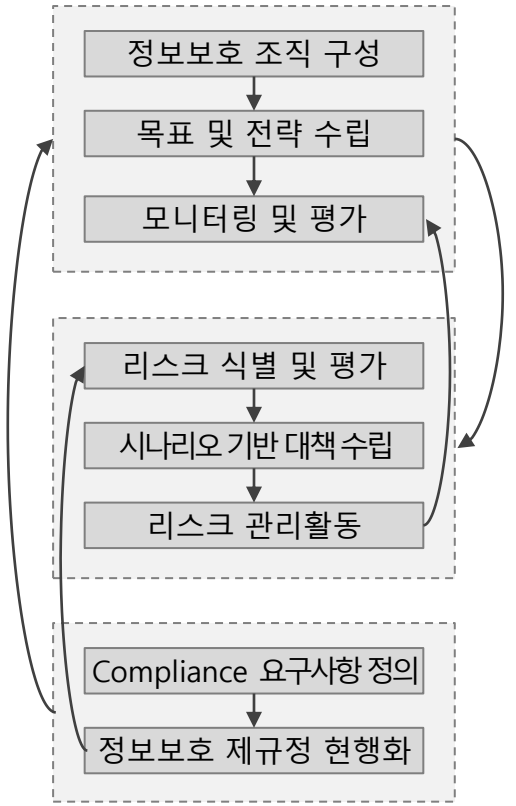
  정보 침해 | 정보 유출 | 정보 오남용 | 신기술 위협

- **개선방안**
  - 정보자산 기반의 대책수립 → Risk 시나리오 기반 대책수립

Compliance 대응 측면

- **정보보호 관련 법령 요구사항의 통합 정의 및 감독기관 규제의 신속 대응체계 마련**
- **개선방안**
  - Compliance 관리 시스템 구축
  - 자율보안체계 역량 확보

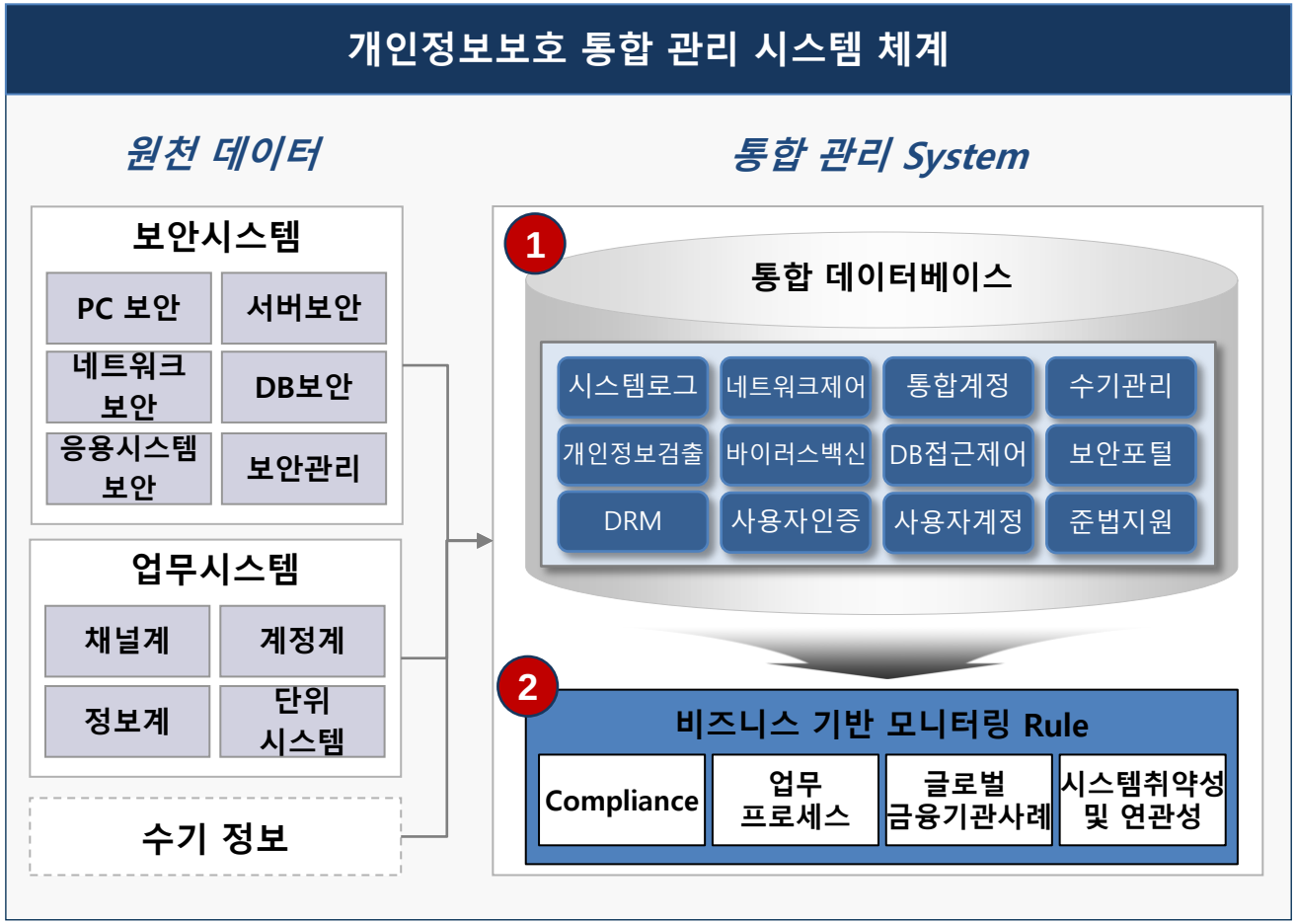
Governance, Risk, Compliance를 아우르는 정보보호 통합관리



KPMG

III.3 시스템 측면 개선방안

통합 데이터베이스 구축 및 비즈니스 기반 모니터링 Rule 도출을 통해 개인정보보호 통합관리 개선이 가능합니다.



1 통합 데이터베이스 구축

- 금융기관 내에 개별적으로 관리되고 있는 보안시스템, 업무시스템 및 수기 관리 되고 있는 정보를 통합한 통합 DB 구축

2 비즈니스 기반 모니터링 Rule 도출

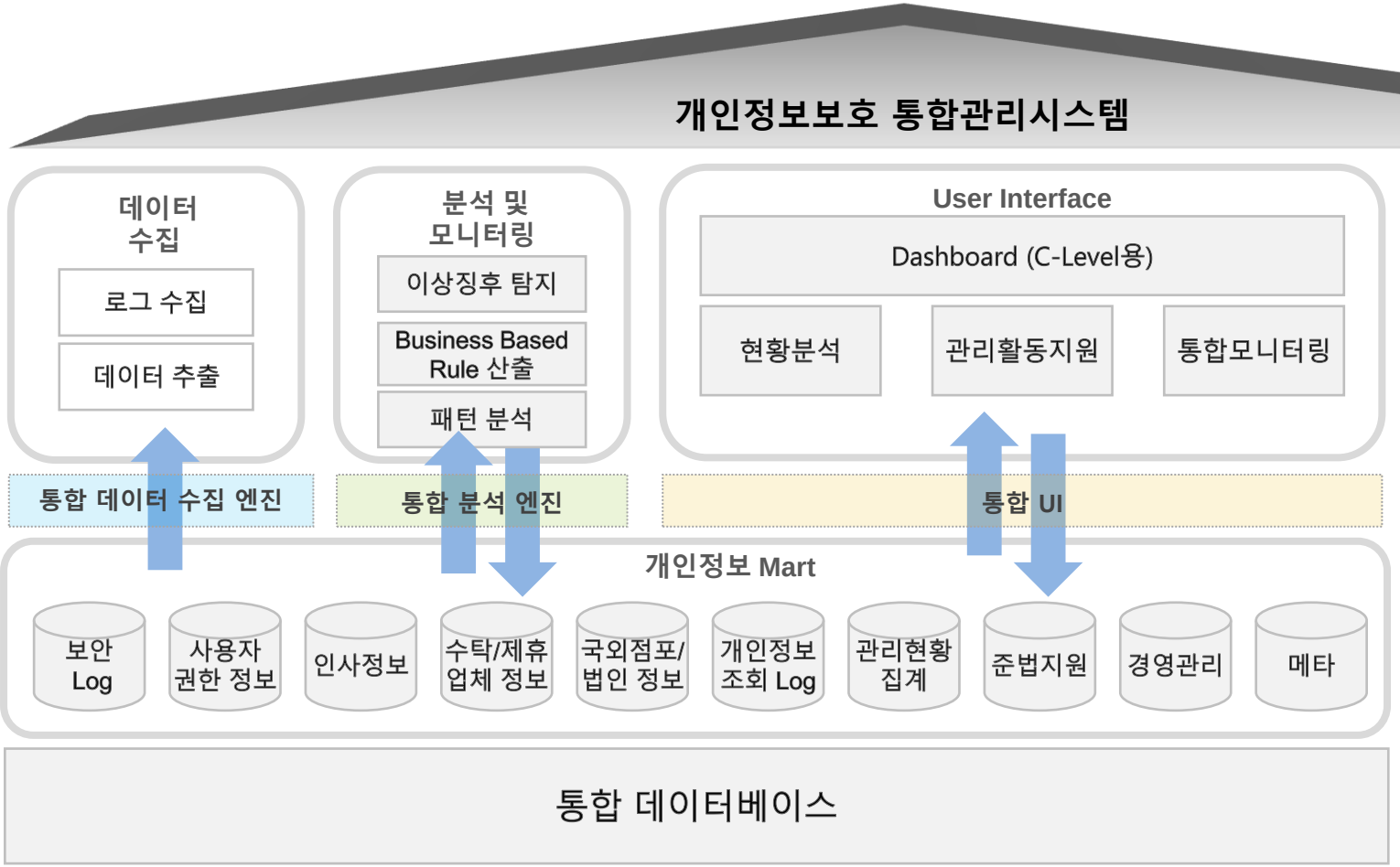
- 비즈니스 기반 모니터링 Rule 도출을 위해 Compliance, 업무 프로세스, 글로벌 금융기관 사례, 시스템 간 취약성 및 연관성 분석을 실시함
- 모니터링 Rule을 통해 개인정보 오남용 및 유출위험의 패턴을 분석하고 이상징후를 포착함

IV. 개인정보보호 통합관리 시스템 구성안

1. 시스템 구성(안)
2. 시스템 기능 예시
3. 화면 구성 예시

IV.1 시스템 구성(안)

개인정보보호 통합관리시스템은 산재되어 있는 다양한 개인정보 보호활동 및 처리로그를 통합 데이터베이스에 수집, 저장하고 비즈니스기반의 룰 정의, 패턴 분석을 통한 모니터링 및 지속적인 개인정보보호 관리활동을 지원하도록 구성할 수 있습니다.



데이터 수집

- 업무서버 로그, 보안서버 로그, 개인PC 로그 등의 관련 정보 수집

분석 및 모니터링

- 비즈니스 기반 룰로 이상징후 산출 및 패턴 분석

User Interface

- Dashboard
- 개인정보보호 현황 분석 및 관리활동 지원
- 통합 모니터링탐지 /분석

IV.1 시스템 구성(안), 계속

개인정보보호 통합관리시스템은 산재되어 있는 전사 시스템 내부 및 외부의 시스템 들을 효율적으로 통합 구성하여 실질적인 개인정보보호 인프라 완성을 목표로 합니다.

개인정보보호 통합관리시스템 흐름도

시스템 구성 주요 특징

- 각 회사 별 기능 별 다양한 원천시스템의 통합을 위한 **유연한 시스템 구성 필요**
- **업무 및 시스템 환경에 적합한 솔루션 및 장비의 도입** (예: 빅데이터 분석 시스템, 데이터 수집 엔진 등)
- 향후 **확장 가능한 시스템 구조 구성**

IV.2 시스템 기능 예시

개인정보보호 통합관리시스템은 개인정보보호 관리활동과 주요 현황관리, 개인정보보호 통합 모니터링, Dash Board 등으로 구성할 수 있습니다.

개인정보보호 통합관리시스템

Illustrative

Dash Board

현황분석 및 관리활동

- 리스크 스코어
- 수탁/제휴사 관리
- 국외점포 관리
- 개인정보보호 교육
- 개인정보보호 점검
- 정보주체 권리 보장
- 고객정보 이용/제공 현황
- 고객정보 관리 현황
- …

통합 모니터링

- 개인(신용)정보 권한 과다 모니터링
- 개인(신용)정보 오남용 모니터링
- 업무목적 외 거래 모니터링
- 외주직원 모니터링
- 개인정보 유출 위험 거래 모니터링
- 빅데이터 기반 모니터링
- …

시스템 관리

- 공통 정보 관리
- 권한 정보 관리
- Rule 정보 관리
- 이상패턴 분석 관리
- 기준 정보 관리 (공통코드 등)
- …

기능 구성 시 고려사항

- **개인정보보호 관리활동의 시스템 측면 통합**
- **개인정보 오남용 및 유출방지를 위한 통합 모니터링 기능 구현**
- **개인정보 처리 현황의 관리대상 정의**
- **C-Level 사용자를 고려한 전사 통합 View (대시보드) 구현**

IV.3 화면 구성 예시 (1/2)

개 요	• 전사 부점 별 개인정보보호 관리 현황을 분석하고 부점 별 관리 위험점수를 산출 및 제공하는 화면

User 개인정보보호 담당/관리자

화면요건

- 전사 부점별 개인정보보호 관리 수준 분석
- 본부/영업점/국외점포/ 업체별 통합 관리 점수 및 내역 산출
- 부점별 개인정보보호 관리활동 상세 내역 제공

전사 리스크 스코어

Illustrative

기준일자 [ ] 조회

전사 개인정보보호 관리 점수 경계 (77)

본부부서 양호 (95)		영업점 경계 (65)		국외점포 양호 (98)		수탁/제휴업체 위험 (45)	
보안서약	100	보안서약	100	보안서약	100	보안서약	100
정보보호 교육	90	정보보호 교육	90	정보보호 교육	90	정보보호 교육	90
개인정보활동 점검	85	개인정보활동 점검	85	개인정보활동 점검	85	개인정보활동 점검	85
고객정보 보유	7	고객정보 보유	7	고객정보 보유	7	고객정보 보유	7

부점별 개인정보보호 관리활동 상세 내역

관리 등급	관리 점수	구분	부점	보안서약		정보보호교육		개인정보보호 점검			고객정보 보유		
				서약 결과 등록	서약 완료 율	교육 결과 등록	교육 이수 율	미 점검	조치 필요	조치 기한 경과	미 삭제 건수	미 삭제 일수	보유 고객 건수
위험	45	본부부서	IT기획부	Y	60%	N	0%	3			10	30	천만

KPMG

IV.3 화면 구성 예시 (2/2)

개 요	• 전사 모니터링 탐지 및 대응 현황을 요약 확인할 수 있는 화면

전사 모니터링 대시보드

Illustrative

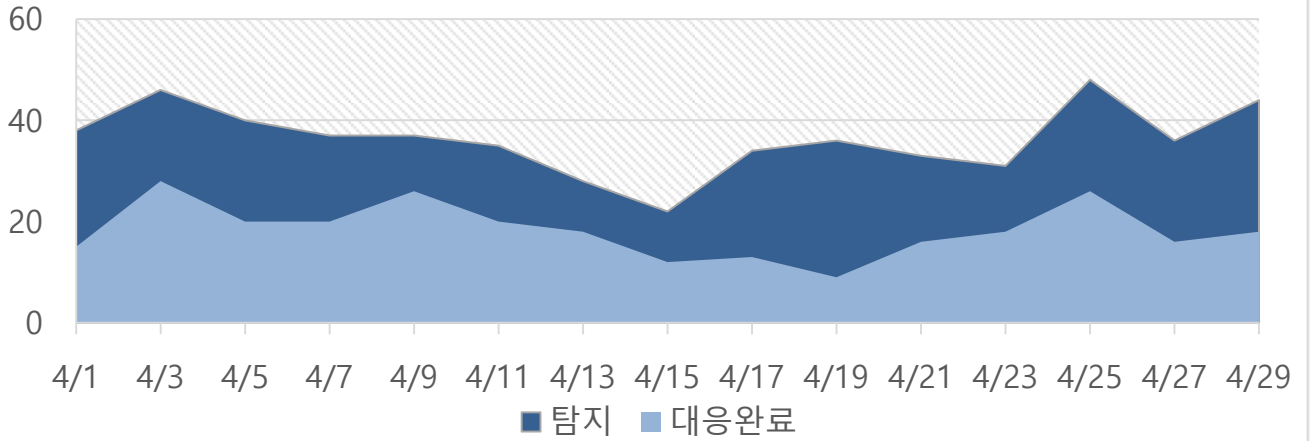
2016.04.30 | 임직원 | 조회

탐지	44
소명 대상	32
소명 비대상	12

대응	32
소명 완료	18
소명 미완료	14

고위험 탐지 부점		대응 미완료 부점	
리스크관리부	10	리스크관리부	7
여신관리부	8	업무지원부	6
업무지원부	7	여신관리부	5
...		...	

탐지 대응 추이



User 개인정보보호 담당/관리자

화면요건

- 일자별 전사 모니터링 탐지 및 대응 현황 조회
- 탐지 건수 및 대응 미완료 건이 많은 부점 Display
- 전사 모니터링 탐지 및 대응 완료 추이 Display

맺음말

맺음말

금융기관 대내외 환경 변화에 따른 개인정보보호를 위해 정보보호에 위협이 되는 전반적인 리스크 요인을 식별하고 이에 대응하기 위한 개인정보보호 통합관리체계 수립이 필요합니다.

대내외 환경변화

정보유출 사고 후 정보보호 강화 활동

정부의 유출방지 대책 및 규제 강화

신기술 도입에 따른 신생 위협 대두

금융기관 대응 과제

- 대내외 환경변화에 따른 주요 리스크 영역 자체 식별 및 통제 방안 수립
- 개인정보보호에 대한 통합 관리를 기반으로 관리 역량 고도화

KPMG

cutting through complexity™

감사합니다.

KPMG

박용수 전무

Tel. (02)2112-0421
H.P. 010-2290-4874
yongsoopark@kr.kpmg.com

이응도 상무

Tel. (02)2112-0156
H.P. 010-3805-5699
eungdolee@kr.kpmg.com

문철호 상무

Tel. (02)2112-0869
H.P. 010-3378-7086
cmoon@kr.kpmg.com

허은석 이사

Tel. (02)2112-0652
H.P. 010-3327-7311
ehuh@kr.kpmg.com