법무법인(유) 율촌

Legal Risk 최소화를 위한

정보보호 컴플라이언스와 내부통제

2014. 3. 19.

손도일 변호사

YULCHON 律村 YULCHON
법무법인(유) 율촌

목 차

내부통제 및 컴플라이언스의 중요성

YULCHON 律村 YULCHON
법무법인(유) 율촌

내부통제 사고와 회사의 존립위기 사례

Compliance Risk?

노출된
리스크

잠재된
리스크

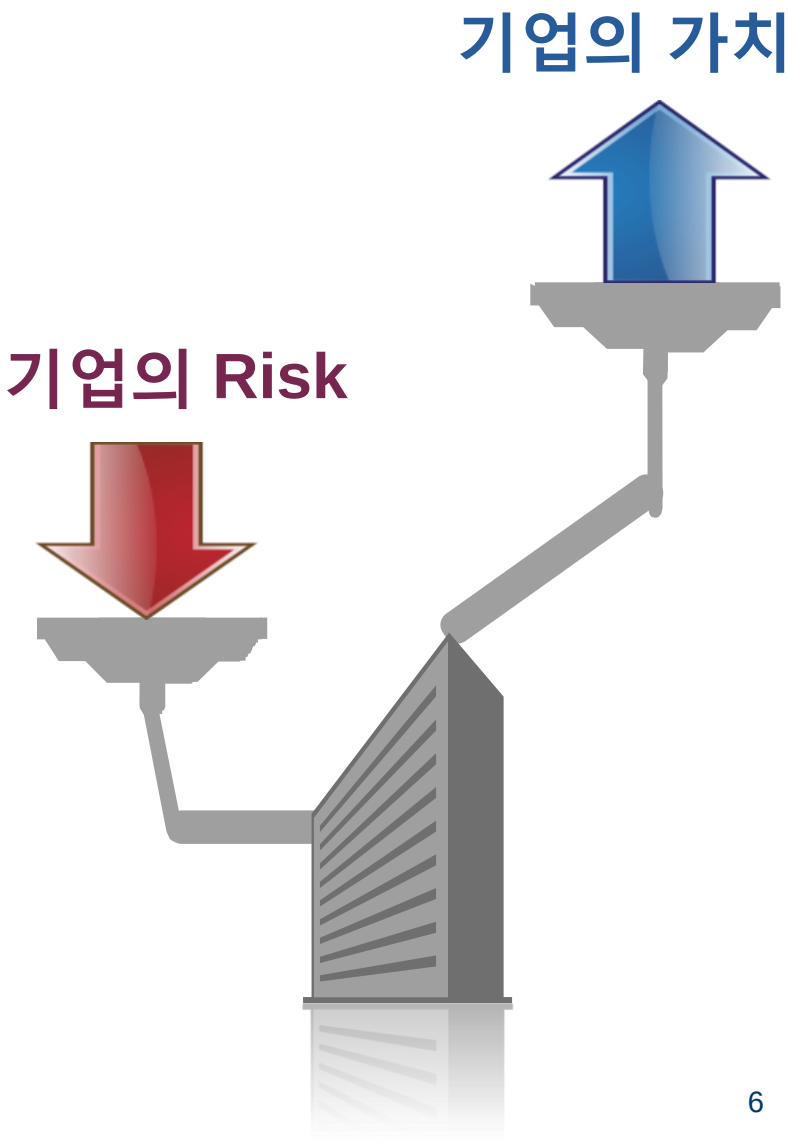
Compliance Risk

- 업무 관련 법규를 위반하거나 해석상의 차이로 인해,
- 법률적 문제로 비화될 가능성이 있는 모든 행위나 절차

Compliance Risk 관리의 필요성

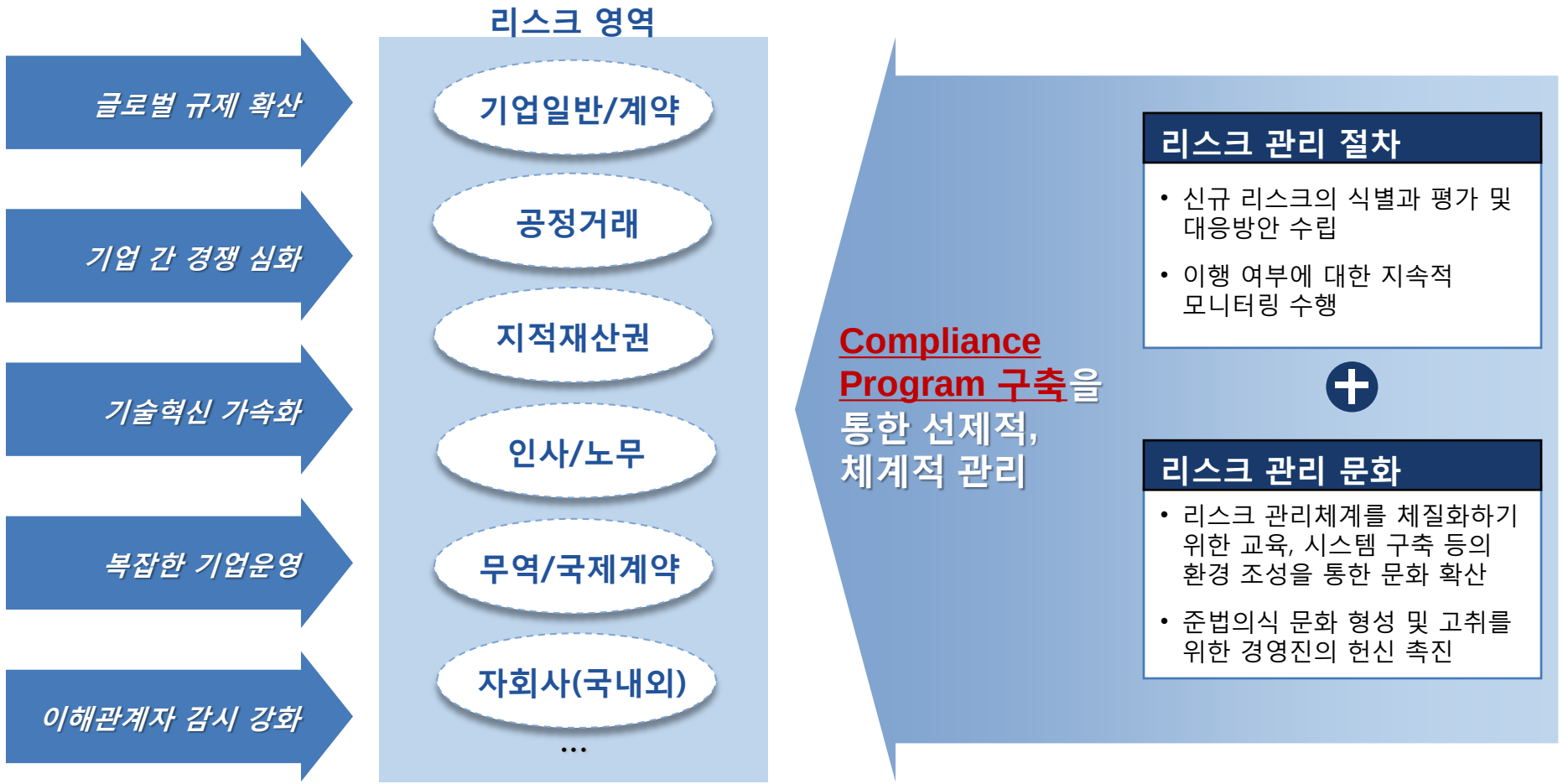
Compliance Risk Management

- 업무 수행 과정에서 발생할 가능성이 있는 Compliance Risk를 사전에 **식별**하고,
- 일정 기준에 따라 **평가**하여 서열化 한 후,
- 발생가능성과 영향도를 최소화하기 위한 **개선안**을 **수립**하고 실행하는 과정



Compliance Risk 관리의 필요성

규제 환경의 변화 및 경쟁 심화로 인해 기업은 더 많은 준법 리스크(Compliance Risk)에 노출되어 있으며 사후적 대응 체계에서 **사전적 대응 체계로의 전환**이 요구됨



'정보보안사고' – 기업의 최대 Risk

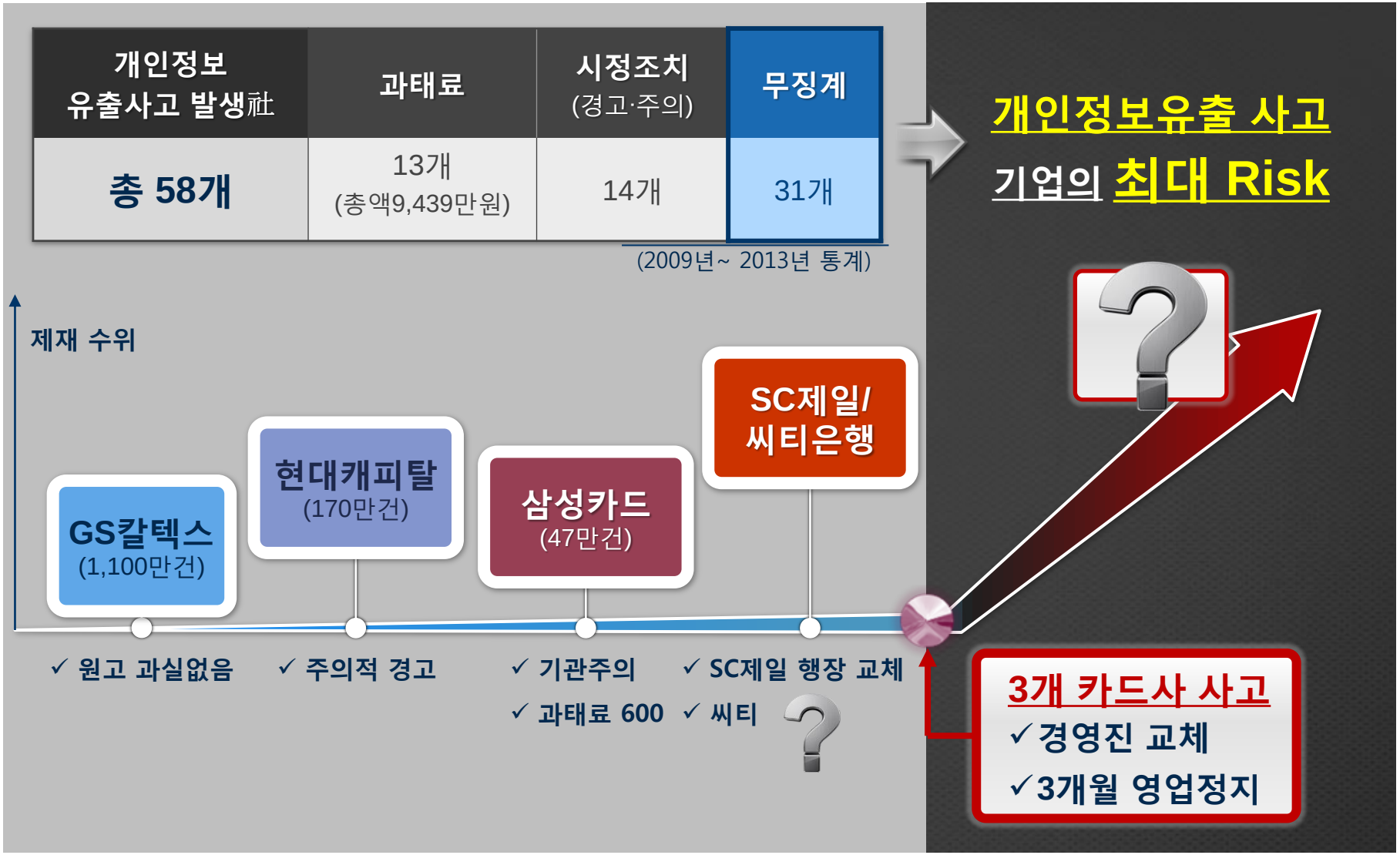
YULCHON 律村 YULCHON
법무법인(유) 율촌

금융 '정보보안 사고'

개인정보 유출사고 발생社	과태료	시정조치 (경고·주의)	무징계
총 58개	13개 (총액9,439만원)	14개	31개

(2009년~ 2013년 통계)

개인정보유출 사고
기업의 **최대 Risk**



경제

금융사 개인정보 불법활용 땐 과징금 최대 3000억

김영진

발행일 : 2014.03.13 / 경제 B2 면 (chosunbiz)

▲ 종이신문보기

금융회사가 불법적으로 개인정보를 활용하다가 적발되면 최대 3000억원의 과징금을 물게 된다.

금융위원회는 12일 '금융분야 개인정보보호 대책 설명 자료'를 내고 과징금 산정기준을 안내했다. 금융위는 최근 개인정보를 불법 활용하다 적발되면 관련 매출액의 3%를 징벌적 과징금으로 부과하겠다고 발표했다.

이날 금융위는 수백만 건의 개인정보를 불법 활용하는 금융회사는 개인을 대상으로 한 영업에 포괄적으로 사용된 것으로 간주해 개인영업 부문 매출 대부분을 과징금 산정 기준이 되는 매출액으로 계산한다고 설명했다.

예를 들어 대형 카드사들은 개인영업 부문 매출액이 1조~4조원이다. 따라서 불법 정보 활용으로 3%의 과징금을 부과하면 최소 300억원에서 최대 1200억원까지 매길 수 있다. 대형 은행은 개인영업 부문의 매출액이 10조원 수준이기 때문에 3%를 부과하면 최대 3000억원에 달하는 과징금이 부과된다.

금융위 관계자는 "불법 정보를 유출하거나 활용하는 금융회사에 대해서는 징벌적 과징금은 물론 최대 6개월 영업정지 조치를 취할 예정이기 때문에 사실상 문을 닫을 정도의 부담을 지게 된다"고 말했다.

향후 입법추진 동향

2014. 2. 국회

국회에 계류 중인 정보 보호 관련 법안 자료: 국회

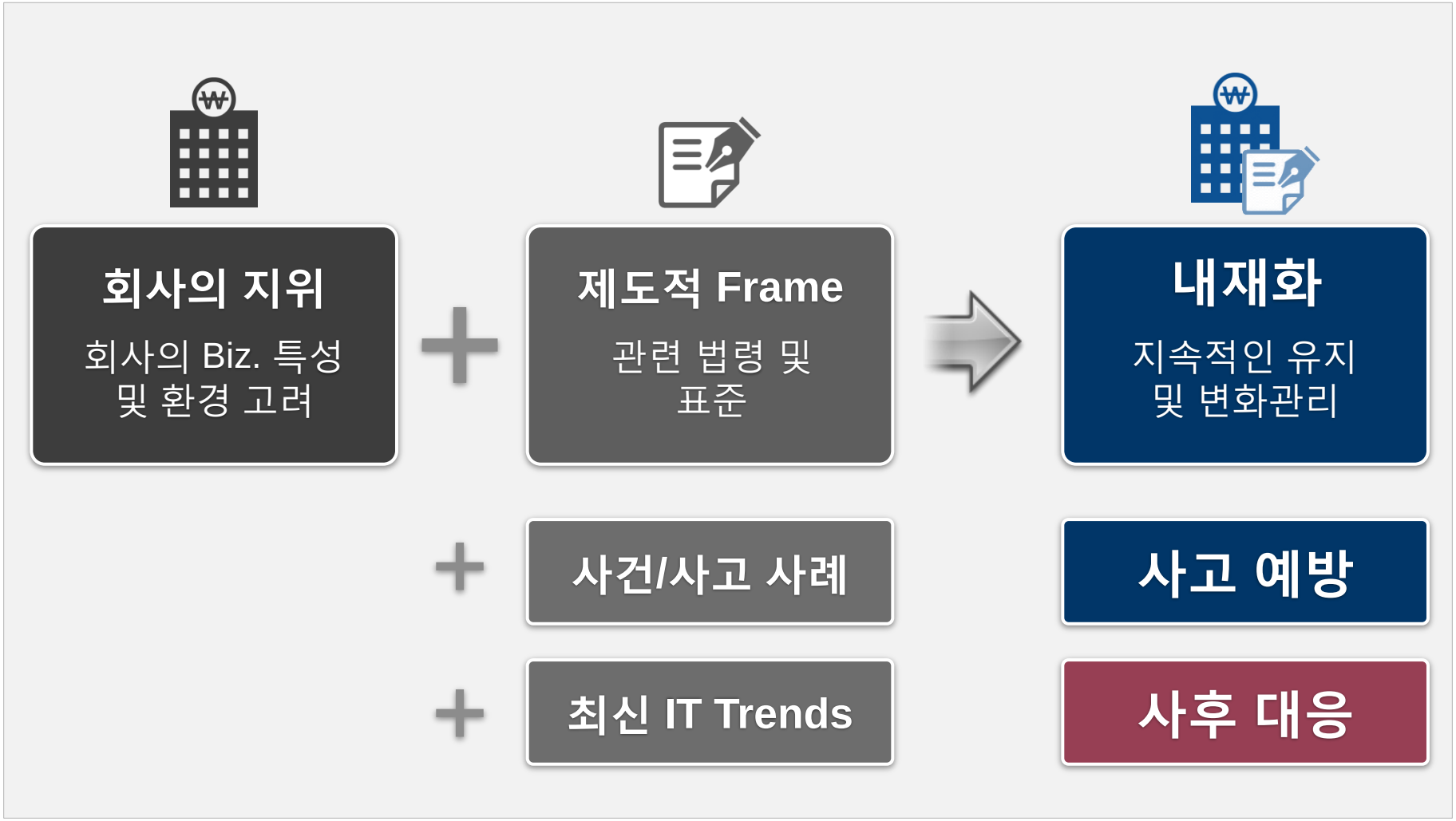
법안	주요 내용	대표 발의
개인정보보호법 개정안	개인 정보 파기 시 해당 정보가 복구·재생되지 않게 함	새누리당 강은희
〃	개인 정보 1건이라도 누출되면 안행부 장관에 신고하게 함	민주당 최민희
〃	소비자 단체가 개인 정보 유출 관련 소송을 신속하게 제기할 수 있게 함	민주당 이상민
〃	주민번호·여권번호·운전면허번호 등 수집할 때 반드시 암호화하게 함	민주당 이찬열
정보통신망법 개정안	정보 유출 사고 발생 후 24시간 내 이용자 및 관계 기관에 통지·신고	민주당 최재천
신용정보법 개정안	보안 대책 부족한 금융기관에 대한 과태료를 3000만원으로 인상	새누리당 박성호

출처: 2014. 1. 21. 조선닷컴

정보보호 Compliance란?

YULCHON 律村 YULCHON
법무법인(유) 율촌

'정보보호 Compliance'란?



‘정보보호 Compliance’_관련 법령

정보통신서비스 제공자

✓ 정보통신망법

전자상거래 사업자

✓ 전자상거래법

개인정보처리자

✓ 개인정보보호법

신용정보 제공·이용자

✓ 신용정보법

전자문서 및 전자거래 기본법

+

전자금융거래법

금융회사의 경우 (예)

금융기관	**전자금융거래법의 적용대상**(법 제2조 제3호 나목/법 제2조 제3호 가목, 금융위원회의 설치 등에 관한 법률 제38조 제3호) **/ 금융실명거래법의 적용대상** (시행령 제2조 제2호/법제2조 제1호 타목)
신용정보제공·이용자	**고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자** (신용정보법 제2조 제7호)
정보통신서비스 제공자	**영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자** (정보통신망법 제2조 제3호)
개인정보처리자	**업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인** (개인정보보호법 제2조 제5호)

법의 적용대상 및 범위 비교

	전자금융거래법	신용정보법	정보통신망법	개인정보보호법	금융실명거래법
보호 대상	전자금융거래의 안정성·신뢰성 및 이용자 법익	신용정보/ 개인식별정보	개인정보	개인정보/ 개인정보파일 (개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 **집합물**) *** 서면 정보 포함**	거래정보등 (금융거래의 내용에 대한 정보 또는 자료)
수범 주체	금융기관/ 전자금융업자/ 전자금융보조업자	신용정보제공·이용자	정보통신서비스제공자	개인정보처리자	금융회사등에 종사하는 자 (4조①전단)
보호 주체	전자금융거래 이용자	신용정보주체	정보통신서비스 이용자	정보주체	금융거래자

『전자금융거래법, 신용정보법, 금융실명거래법』은 특별법으로 개인정보보호법에 우선하나 금융거래 고객의 정보에 국한됨/『개인정보보호법』은 일반법으로 금융거래가 없는 잠재 고객의 정보 등 모든 형태의 개인정보에 적용되며, 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보보호법이 적용됨 (금감원, 금융분야 개인정보보호 체계 및 추진방향 2013. 5.)

금융권에 대한 규제강화

YULCHON 律村 YULCHON
법무법인(유) 율촌

규제의 강화

- ’11.10月 **5.5.7 규정** (전자금융감독규정)
- ’13.05月 **CEO 확인 및 서명** (전자금융거래법 개정)
- ’13.07月 **금융전산 내부통제 및 CEO 책임 강화** (금융전산 보안강화 종합대책)
- ’13.08月 **CEO 또는 임원 징계 권고** (개인정보보호법 개정)
- ’13.11月 **매출액 1% 이하 과징금 부과** (정보통신망법 개정안 입법예고)
- ’14.01月 **금융회사 정보관리 및 CEO 책임 강화** (금융회사 고객정보 유출 재발방지 대책 ’14.1月)
- ’14.03月 **금융회사 및 CEO 및 임원 책임 강화** (금융분야 개인정보 유출 재발방지 종합대책 ’14.3月)

2013. 7. 11. 금융전산 보안강화 종합대책

1 CISO 역할 및 독립성 강화

2 금융전산 **내부통제 강화**

3 **금융전산부문 감독 및 검사 강화**

4 금융보안 전문인력 양성 및 교육 강화

5 금융보안 관리체계 인증제도 도입 및 금융전산 망분리 의무화

2014. 1. 20. 금융회사 고객정보 유출 재발방지 대책

1 CISO 역할 및 독립성 강화

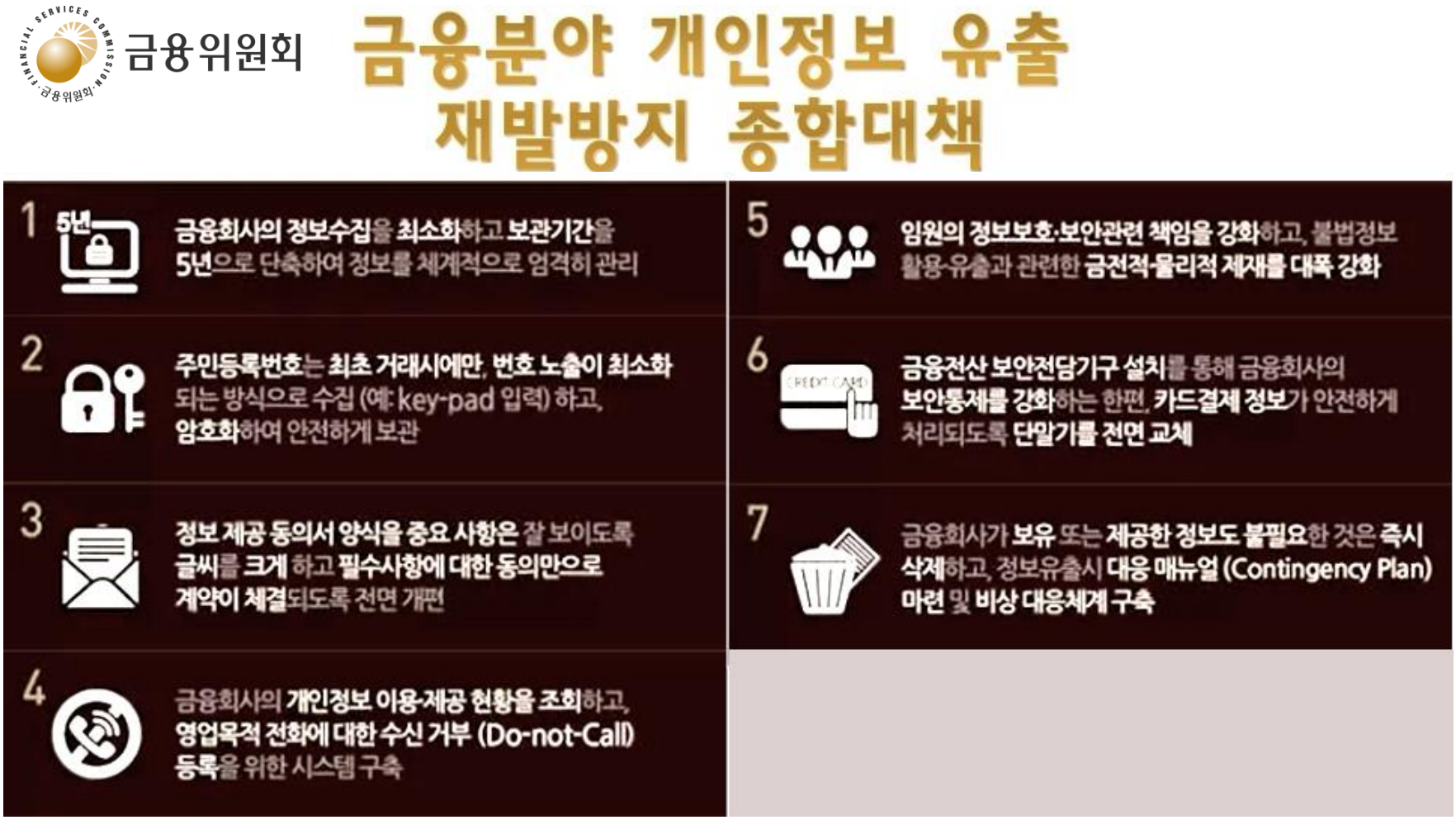
2 금융전산 **내부통제 강화**

3 **금융전산부문 감독 및 검사 강화**

4 금융보안 전문인력 양성 및 교육 강화

5 금융보안 관리체계 인증제도 도입 및 금융전산 망분리 의무화

2014. 3. 10. 금융분야 개인정보 유출 재발방지 종합대책



'정보보호 Compliance' 민·형사·행정상 Risk

YULCHON 律村 YULCHON
법무법인(유) 율촌

‘정보보호 Compliance’_손해배상책임

원칙적
무과실

입증책임
전환

사용자 책임

'정보보호 Compliance'_손해배상책임

회사	법원의 판단	배상액	現 경과
A 은행 (2006. 5.)	• 정신적 손해배상 인정	• 10만~20만원 → (X 1024名 = **1~2억**)	• 2007. 11. 항소심 확정
B 전자 (2006. 9.)	• 입사지원서 정보의 보호가치 인정	• 70만원 → (X 32名=**2,240만**) • 30만원 → (X 258名=**7,740만**)	• 2008. 11. 확정
C (전자상거래) (2008. 2.)	• 개인정보 관리 상의 과실 부정	• 50~300만원 청구 → **원고 패소**	• 대법원 계류 중
D (정보통신) (2013. 2.)	• 관리 책임 인정	• 20만원 → (X 2,900名=**5.8억**) • **(3,500만名 배상 시 7조원)**	• 항소심 계속 중

'정보보호 Compliance'_경영진의 책임

제3자에 대한 책임

✓ 이사가 고의 또는 중대한 과실로 인하여 그 임무를 게을리한 때에는 그 이사는 제3자에 대하여 연대하여 손해를 배상할 책임이 있음 (상법 제401조)

이사들의 감시의무

- 대규모의 회사에서 **각자의 전문 분야를 전담하여 처리하는 것이 불가피한 경우라 할지라도** 그러한 사정만으로 다른 이사들의 업무집행에 관한 **감시의무를 면할 수는 없음**

회사에 대한 책임

✓ 고의 또는 과실로 법령 또는 정관에 위반한 행위를 하거나 그 임무를 게을리한 경우에는 그 이사는 회사에 대하여 연대하여 손해를 배상할 책임이 있음(상법 제399조)

"법령"의 범위

- 이사로서 임무를 수행함에 있어서 준수하여야 할 의무를 개별적으로 규정하고 있는 상법 등의 제 규정과 **회사가 기업활동을 함에 있어서 준수하여야 할 제 규정을 위반한 경우도 포함**

'정보보호 Compliance'_경영진의 책임

현행법	개정법(2014. 8. 7. 시행)
(제65조②,③)안전행정부장관 또는 관계 중앙행정기관의 장은 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 **책임 있는 자를 징계할 것**을 **그 소속기관단체 등의 장**에게 권고할 수 있음. 이 경우 권고를 받은 사람은 이를 존중하여야 하고 그 결과를 안전행정부장관 또는 관계 중앙행정기관의 장에게 통보하여야 함.	(제65조②,③)안전행정부장관 또는 관계 중앙행정기관의 장은 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 **책임 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것**을 **해당 개인정보처리자**에게 권고할 수 있음. 이 경우 권고를 받은 사람은 이를 존중하여야 하고 그 결과를 안전행정부장관 또는 관계 중앙행정기관의 장에게 통보하여야 함.

개정 개인정보보호법상 대표자 및 책임 있는 임원에 대한 징계 권고의 근거를 명시적으로 마련

'정보보호 Compliance'_형사 책임

양벌 규정: 상당한 주의와 감독의무

형사 책임	**2년 이하의 징역 또는 1천만원 이하의 벌금**	**2년 이하의 징역 또는 1천만원 이하의 벌금**
위반 행위	• 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자	• 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자
관련 근거	✓ 정보통신망법	✓ 개인정보보호법

'정보보호 Compliance'_행정 조치

✓ 매출액 1% 이하 과징금 부과

[정보통신망법 개정안 입법예고 (’13.11月)]

- 기업 개인정보 보호조치 의무 위반 시 1억원 이하 정액 과징금을 관련 **매출액의 1%이하**로 변경하기 위한 입법안 논의 中

✓ 징벌적 과징금제도 도입

[금융회사 고객정보 유출 재발방지 대책(’14.1月)]

- 정보유출관련 행정제재, 형벌 등 사후제재 대폭 강화 및 **징벌적 과징금제도 도입**
- 자체 보안이행 점검 프로세스 강화 및 금감원 검사 시 보안규정 준수여부 철저히 점검

금융 '정보보호 컴플라이언스'_금융위 제재 조치

- **금융기관검사및제재에 관한 규정 시행세칙 제46조 제2항**

구 분	사고금액 위반건수 초과(중단)시간	제재양정	
		임·직원	기관
임·직원이 전산자료 또는 프로그램을 조작하여 발생한 중대한 사고 (전자금융거래법 제21조 위반)	-	해임권고(면직)	기관경고 이상
금융회사의 부주의에 의하여 접근매체 위·변조 등에 의한 금전사고 (전자금융거래법 제9조 위반)	50억원 이상	직무정지(정직)이상	기관경고 이상
	10억원 이상	문책경고(감봉)	기관주의
	1억원 이상	주의적경고(견책)	
전산시스템 재해복구 지연 (전자금융감독규정 제23조 제8항 위반, 신용카드사 3시간 이내/보험사는 24시간 이내에 복구 의무)	24시간 이상	직무정지(정직)이상	기관경고 이상
	5시간 이상	문책경고(감봉)	기관주의
	1시간 이상	주의적경고(견책)	
고객정보 유출 (전자금융감독규정 제4절 위반)	**1백만건 이상이고 전체고객수의 10% 이상**	**직무정지(정직) 이상**	**기관경고 이상**
	10만건 이상	문책경고(감봉)	기관주의
	1만건 이상	주의적경고(견책)	
법 제21조(안전성의 확보의무) 위반으로 사고발생 위험이 현저히 높은 경우	-	주의적경고(견책) 이상	기관주의 이상
정보시스템 가동기록을 보존하지 않았거나 기록을 삭제 또는 훼손한 경우(전자금융감독규정 제13조 제1항 제11호 및 제4항 위반)	-	주의적경고(견책) 이상	기관주의 이상

Risk 최소화를 위한
'정보보호 컴플라이언스' 제언(提言)

YULCHON 律村 YULCHON
법무법인(유) 율촌

정보보호 컴플라이언스 대응 필요성

Legal Risk를 최소화하는 최적의 Compliance 개선안 마련

- 관련 법령•판례의 분석을 통해 도출한 **Tool**을 적용한 입체적인 진단
- **축적된 소송 경험과 관련 법령에 관한 자문** 경험을 바탕으로 한 최선의 개선안 제시

선관주의의무를 다하였음을 입증하는 문서보관체계 수립

- **소송 및 분쟁(제재) 대응 시 선관주의 의무 이행 노력을 입증하기 위한** 정보보호 컴플라이언스: 관련 전자문서, 이메일 등을 체계적으로 보관하는 기록 보전 체계 수립
- 現 업무 중심의 문서보관체계 및 프로세스 Remodeling 방안

임•직원들의 정보보안 의식 제고 및 업무 수행 역량 강화

- 경영진들에 대한 **맞춤형 교육** 실시로 보안 책임 의식 제고
- 관련 법령 및 판례에 대한 교육 실시로 **임직원들의 보안 업무 수행 역량 강화**
  → 정보보안사고의 사전적 예방 및 사고 발생 시 신속한 대처 가능

4대 목표 및 기대 효과

금융회사로서의 선관주의 의무 이행 요건 식별 및 이행체계 재정비

- 선관주의 의무 이행을 통한 Legal Risk 최소화
- CEO, CISO, CPO 등 주요 직급별 이행체계
- Legal Risk 분배를 통한 위험전이 방지

내부통제, 정보보호 및 준법감시 체계 등에 대한 정보보호 컴플라이언스 운영 실태 파악

- IT/보안/법률 전문가를 통해 정보보호 컴플라이언스 수준에 대한 객관적 실태 점검

선제적 선관주의 의무 이행 체계 마련

現 정보보호 컴플라이언스 운영 실태 파악

정보보호 컴플라이언스 Governance 체계 기반 정비

Legal Risk 최소화를 위한 사후 대응체계 수립

정보보호 컴플라이언스 Control Tower로써 금융그룹 Governance 체계 마련을 위한 기반 정비

- 그룹사 공통 적용을 위한 통제체계 마련 및 배포
- 정보보호 컴플라이언스 Control Tower역할 정립
- 정보보호 컴플라이언스 Governance 체계 마련

정보보호 컴플라이언스 Legal Risk 식별 및 위험요소 개선을 통한 체계적인 대응체계 수립

- 실태 점검을 통해 도출된 주요 위험요소 개선
- 사후 체계적인 대응을 위한 주요 사고 시나리오 도출 및 대응절차 마련

Legal Risk 최소화_법률 적합성 검토 영역

체계적이고 효과적인 정보보호 컴플라이언스 대응 체계 수립을 위해 다양한 영역에 대한 법률적합성 검토가 필요한 실정임

1. 관련 조직의 정비
2. 내부통제체계의 검토
3. 전산업무 위수탁 현황 검토
4. 고객정보 Life-Cycle 현황 검토
5. 감시체계의 적정성
6. 사고발생시 대응체계 수립
7. 교육 프로그램의 운용

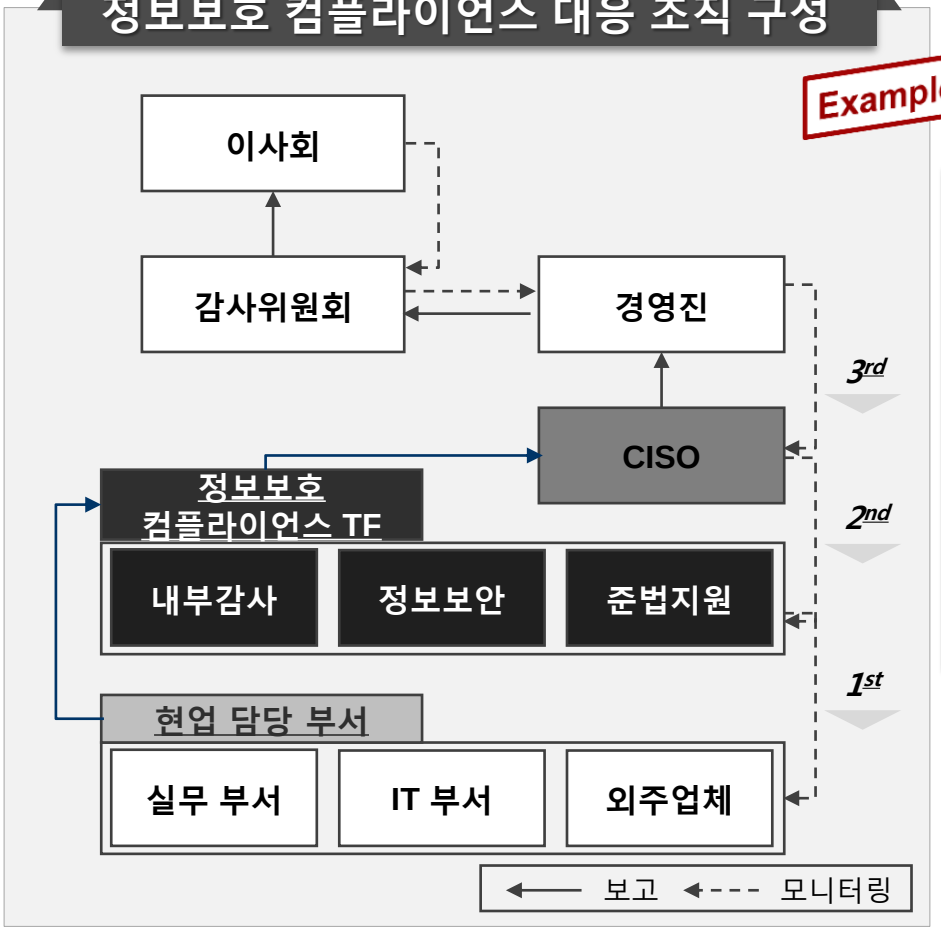
※ 기타 고려사항

1 관련 조직의 정비_내부 정보보호 컴플라이언스 대응 조직 구성

개선과제의 이행 여부 점검 및 주기적인 모니터링 활동이 유지되도록 정보보호 컴플라이언스 이행 조직을 중심으로 명확한 역할과 책임(R&R)을 정의와 보고체계 정비

정보보호 컴플라이언스 대응 조직 구성

Example



Example

조직	책임 및 역할
이사회	• 업무 집행에 관한 의사결정
감사위원회	• 회사의 정보보호 컴플라이언스 집행 이력 감독 및 업무 감시
경영진	• 정보보호 컴플라이언스 계획 수립 및 이행
준법지원	• 규제 환경 변화 모니터링 • 준법 리스크 관리 • 준법지원 교육 프로그램 수립/실행
내부감사	• 내부통제정책 수립 및 내부감사
정보보안	• 정보보호 정책 수립 및 Guide • 정보보호 교육 및 보안통제
현업 담당	• 관련 법규 및 내규 준수 및 이행

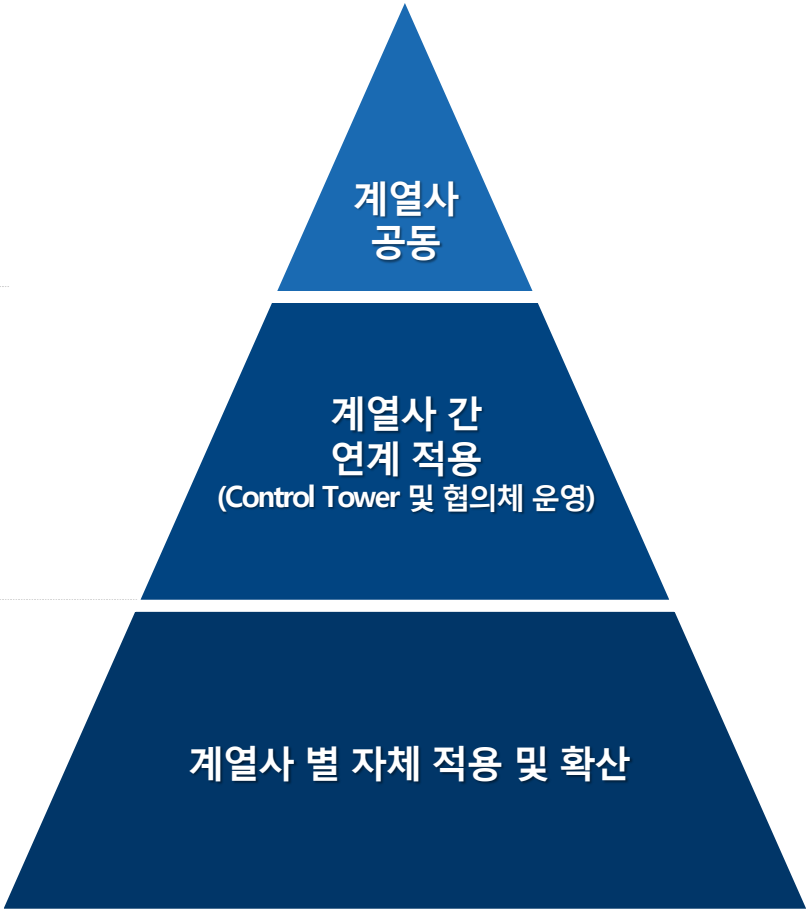
1 관련 조직의 정비_그룹 정보보호 컴플라이언스 대응 조직

그룹 차원의 정보보호 컴플라이언스 대응을 위한 Control Tower 수립 및 비상 시 공동 대응을 위한 업무 협의체 운영

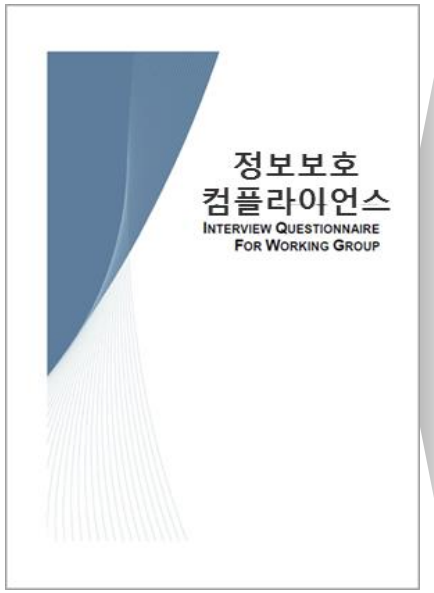
- 정보보호 컴플라이언스 통제항목 및 운영관리 표준 마련 및 배포
- 지주사의 역할 및 특징 반영

- 지주사와 계열사간 정보보호 컴플라이언스 운영관리를 위한 협의체 구성 및 운영

- 계열사 별 업무 특성을 반영한 통제항목 체계 수립, 통제항목 운영 및 관리체계 마련
- 지주사 보고 및 Feedback



2 내부통제 체계 검토



금융회사 고객정보 관리실태 점검 체크리스트

Example

▣ 내부통제 부문

구분	No.	점검 항목	No.	세부 내용	Opt.	관련 법	보호대책
1. 규정 및 절차 수립	1.1	개인신용정보 및 금융거래정보(이하 '고객정보')의 안전한 처리를 위한 내부 관리규정 마련 여부	1.1.1	개인신용정보 제공 및 이용에 관한 사항 등 신용정보의 수집, 처리 및 이용에 관한 세부절차	필수	**신용정보법 제20조** **제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ① 신용정보의 수집·처리 및 이용 등에 대하여 내부관리규정 수립 ② 각 호의 기록을 3년간 보존 1. 주소와 성명 또는 정보제공·교환기관의 주소와 이름, 2. 의뢰받은 업무 내용 및 의뢰받은 날짜 3. 의뢰받은 업무의 처리 내용 또는 제공한 신용정보의 내용과 제공한 날짜 ③ 신용정보관리·보호인을 1명 이상 지정 **신용정보업 감독규정 제22조** **제22조(내부관리규정의 마련)** 각 호의 사항이 포함된 내부관리규정을 구체적이고 상세하게 마련	개인정보처리 내부 프로세스 정립 - 개인정보 수집, 처리, 활용, 승인 절차 마련 - 개인정보의 활용 범위 정의 - 신용정보 제공 사실 및 거절 절차 - 신용정보 위탁 기준
			1.1.2	신용정보집중기관의 경우 집중관리, 활용의 대상이 되는 신용정보의 종류 및 범위	필수		
			1.1.3	기술적·물리적·관리적 보안대책의 수립 및 실행	필수		
			1.1.4	신용정보의 열람 및 정정청구업무 처리절차	필수		
			1.1.5	자신이 제공하는 신용정보를 이용하는 자에 대하여 동 신용정보의 이용이 법, 영, 규칙 이 규정에 적합한지 여부의 점검절차와 위반시 제재	필수		
			1.1.6	신용정보관리·보호인의 지정 및 수행하는 업무	필수		
			1.1.7	신용정보 제공사실 통보업무 처리 절차	필수		
			1.1.8	상거래 거절 근거 신용정보 고지업무 처리절차	필수		
			1.1.9	동의철회권 등의 업무 처리절차	필수		
			1.1.10	신용정보의 정확하고 신속한 등록 및 보유한 정보의 정확성을 상시 점검할 수 있는 시스템	필수		
			1.1.11	신용정보처리 위탁의 기준	필수		
			1.1.12	다음의 기록을 3년간 보존 - 주소와 성명 또는 정보제공·교환기관의 주소와 이름, 의뢰받은 업무 내용, 날짜, 처리내용과 제공한 신용정보의 내용과 제공한 날짜	선택		
			1.1.13	신용정보관리·보호인을 1명 이상 지정	선택		
	1.2	고객정보의 안전한 처리를 위한 내부 관리계획의 수립 및 시행 여부 * 개인정보보호책임자 지정, 안전성 확보에 필요한 조치, 임직원 교육 등	1.2.1	개인정보 보호책임자의 지정에 관한 사항	필수	**개인정보보호법 제29조** **제29조(안전조치의무)** 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. **동법 시행령 제30조** **신용정보업 제19조** **제19조(신용정보전산시스템의 안전보호)** ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을	개인정보 책임자 및 취급자의 선정과 역할 정의 - 개인정보 책임자, 취급자의 선정 - 개인정보 책임자, 취급자의 역할과 책임 정의 - 개인정보 책임자, 취급자의 개인정보 및 정보보호에 대한 필수 교육내용의 정의
			1.2.2	개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	필수		
			1.2.3	개인정보의 안전성 확보에 필요한 조치에 관한 사항	필수		
			1.2.4	개인정보취급자에 대한 교육에 관한 사항	필수		
			1.2.5	개인정보보호 내부관리의 변경이 발생할 경우 즉시 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리	선택		
	1.3	고객정보의 오·남용에 대한 자체 제재기준 마련 여부 및 오·남용 발생시 제재 실시 여부	1.3.1	고객정보 오.남용에 대한 제재 기준 수립 및 이행	필수		고객정보 사용에 대한 기준 및 보안대책 수립 - 고객정보의 오남용기준 수립 - 고객정보 시스템을 통한 고객정보 오남용시 통제방안 수립
			1.3.2	신용정보전산시스템에 대한 기술적·물리적·관리적 보안대책	선택		
			1.3.3	신용정보제공·이용자는 신용정보를 제공하는 경우 신용정보 보안관리 대책을 포함한 계약체결	선택		
2 고객정보 수집 및 제3자 제공	2.1	고객정보 수집시 그 목적에 필요한 최소한의 고객정보만을 수집하는지 여부	2.1.1	개인정보를 수집하는 경우에 그 목적에 필요한 최소한의 개인정보 수집	필수	**개인정보보호법** **제16조(개인정보의 수집 제한)** ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최	개인정보 수집 범위 설정 - 개인정보 수집 목적 정의 - 목적에 다른 최소한의 범위 정의
			2.1.2	개인정보처리자는 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 고지	선택	**개인정보보호법 제21조**	
	2.2	보유기간의 경과, 개인정보의 처리목적 달성 등 불필요하게 된 경우 지체 없이 복구 또는 재생되지 않도록 파기하는	2.2.1	불필요한 고객정보에 대한 영구 삭제, 파쇄, 소각 등의 파기 및 개인정보보호책임자 확인	필수	**제21조(개인정보의 파기)** ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이	개인정보 파기에 대한 기술적 대책 수립 (예 : 데이터 덮어쓰기(오버라이팅), 디가우징)

2 내부통제 체계 검토_실사 및 인터뷰

각 영역별 현황에 대한 이해를 토대로 자료 검토 및 현업부서 담당자 대상 인터뷰 실시

자료 검토

[각종 규정, 문서 등 자료 검토]

- 업무전결규정
- 업무 표준
- 기타 TF가 요청하는 자료

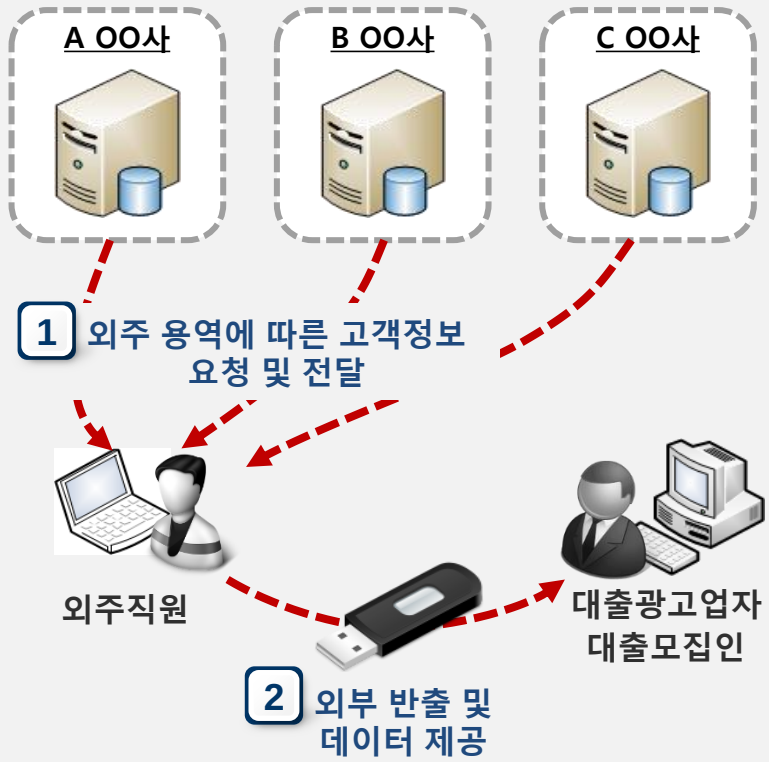
인터뷰

[현업부서 대상 인터뷰]

3 전산업무 위수탁 현황 검토_예시

전산업무 외부 위수탁으로 인한 최근 사건 사례에 비추어 금융지주사 및 계열사의 위수탁 현황 검토 및 이에 대한 현실적인 대응체계 수립

OO사 고객정보 유출 사고 사례



외부주문 프로세스 현황 진단

Example

- ✓ 고객정보 취급에 따른 타당성 및 최소화 검토
- ✓ 고객정보 전달 과정상의 절차 준수
- ✓ 고객정보 전달 이후 보안통제 준수
- ✓ 프로젝트 종료 시 보안성 검토 및 고객정보 파기 확인
- ✓ …

"통제 준수와 업무편의 간 Conflict"

Example

1 Access Control & Encryption

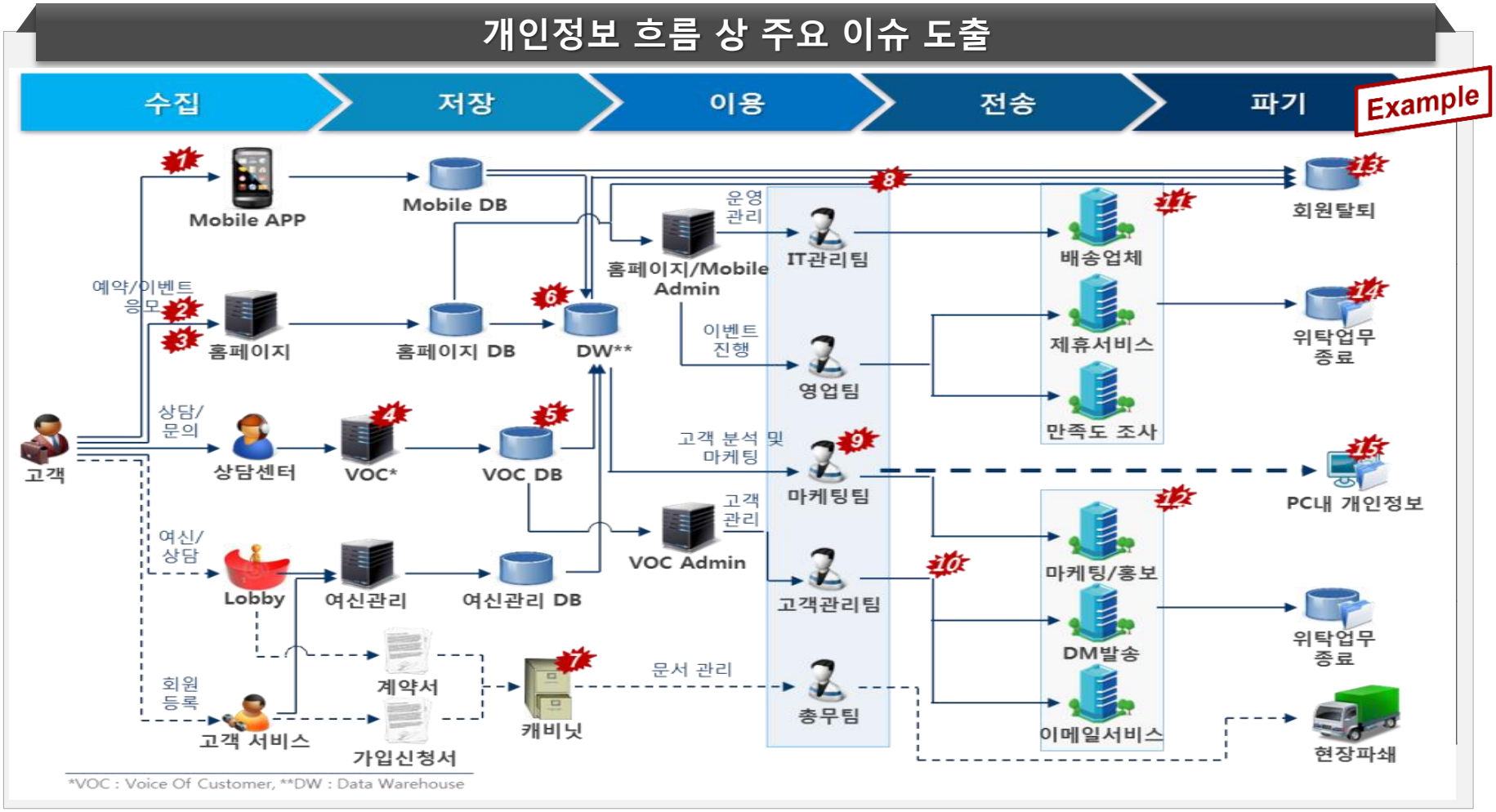
외주직원의 개인정보 접근 통제, 취급 범위 및 처리 절차에 대한 검토와 관련 보완통제 미비

2 System & Physical Security

이동식 저장매체 통제 및 외부 반출과 관련된 통제 포인트가 적절히 설계 · 운영되지 못함

④ 고객정보 Life Cycle 현황 검토

개인정보 제공 현황을 통한 Compliance 이슈 도출 및 개선 대응체계 마련



5 감시 체계의 적정성 검토

진단기준 및 범위

Example

진단 대상	• 퇴사자 계정 관리
감사 범위	• 그룹 공동망을 이용하는 계정 • 계열사 자체망을 이용 하는 계정
감사 기준	• 최근 7일간 로그인 되지 않은 계정 • 그룹 사 재배치에 의해 사용 되지 않는 계정 • 퇴사 등록 기준일 이후 남아 있는 계정
감사 시기	• 상시 감사, 특별 감사

진단 주체 및 방법

Example

그룹사	지주사	외부 감사
IT Compliance 협의체	그룹 IT Compliance 협의체	그룹사/지주사 IT Compliance 감사
점검 체계를 통한 진단 및 그룹사 결과 보고	감사 체계를 통한 처리 결과 감사 및 감사 결과 보고	점검 Process 무결성 검증 및 결과/감사 보고서 감사

5 감시 체계의 적정성 검토_내부 감시 및 보고 체계

수립된 개선방안 이행 여부에 대한 지속적인 점검 등 통제항목 체계 운영 및 관리 사례 공유를 통한 고도화 방안 모색

모니터링 및 보고 체계

Example

경영진 보고 체계

Example

관리 번호	리스크 번호	리스크	리스크 오너	Spon -sor	작성			진척 진척도		
					기준일	작성일	작성자	목표	실제	Status
AP01	R01	증권거래법 관련 공시/신고/보고 의무 위반	홍보팀장	경영지원 본부장	2009. 10.31	2009. 11.03	홍보팀 ○○○	70%	66%	

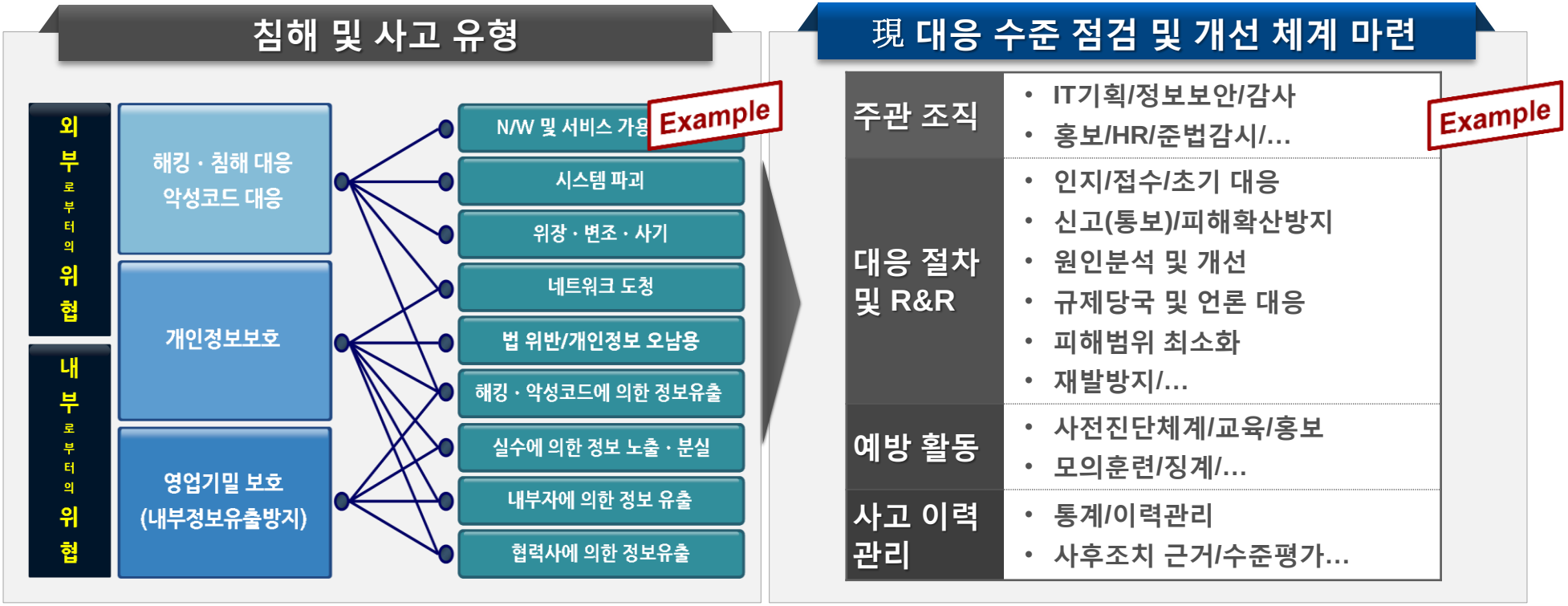
개선과제 이행 Status

개선과제		세부 개선과제		주관부서	진척도			
번호	과제명	번호	과제명		목표	실제	Status	비고
AP01. 01	공정공시에 대한 교육 강화	AP01. 01-1	공정공시 교육 프로그램 작성 - 대상, 주기, 교육 방법, 내용 확정	인재개발팀	50%	10%		담당자의 퇴사, 교육업체 미지정으로 인해 진행이 거의 이루어지지 않음
AP01. 02	공정공시 Awareness강화	AP01. 02-1	포스터 제작 및 부착 - 부착 장소, 위치 선정	홍보팀	100%	90%		포스터 제작 업체의 물량 주문 과다로 납기 예정일의 1주일 후 Delivery 예정
		AP01. 02-2	시스템 메인 화면에 공정공시 준수가 중요하다는 내용 삽입	전산팀	100%	100%		시스템에 문구 삽입 완료
AP01. 03	언론대응지침 작성	AP01. 03-1	언론 대응 지침 작성 - 언론 대응 프로세스 포함	홍보팀	75%	65%		홍보팀에서 대응 지침 마련 중이나 담당자의 업무 과중으로 1명 인력 추가 보강 필요

이슈 번호	과제명	대응 방안
ISO1	공정공시 교육 프로그램 과제 진척 미진	담당자를 재지정하여 교육 업체 선정 신속히 진행
ISO2	언론대응지침 작성을 위한 인원 보강 필요	홍보팀에서 0.5 M/M를 추가 투입하여 신속히 진행

6 사고발생시 대응체계 수립_ 핵심 시나리오 도출

내부 및 외부로부터의 주요 위협 및 발생가능한 사고 유형에 기반한 현 대응 수준 점검 및 개선 체계 마련



6 사고발생시 대응체계 수립_ 핵심 시나리오 도출

CEO, CIO, CISO, 신용정보 관리·보호인 및 정보보호 컴플라이언스 실무자 등 직급별 선관주의의무 이행과 관련한 입증 매뉴얼 작성

CEO	• 취약점 점검결과 및 이행여부 보고받음 • 정보기술부분계획 내용 확인 및 서명	✓ 전자금융거래법
CIO	• CIO - CISO 겸직 금지	✓ 7.11 금융전산 보안강화 종합대책
CISO	• 전임제 도입 및 인사상 불이익 금지 • 취약점분석·평가 자체전담반 운영	✓ 7.11 금융전산 보안강화 종합대책 ✓ 전자금융감독규정
CPO	• 개인정보보호 관리책임자 지정	✓ 개인정보보호법
신용정보 관리·보호인	• "임원"으로 임명, 권한과 의무 강화 • CEO 및 이사회 주기적 보고 의무화	✓ 신용정보법 (개정)
실무자	• 관련법규 및 내규 에 따른 업무 수행	✓ 관련법규

각 직급별 선관주의의무 이행 메뉴얼 마련

6 사고발생시 대응체계 수립_사고대응 절차 및 매뉴얼

예기치 못한 상황으로 인하여 실제 정보보호 컴플라이언스 관련 사고 발생 시, 사고 대응 주체간 구체적인 R&R 정의 및 대정부·언론 대응 매뉴얼 마련

수사기관 대응 메뉴얼

Example

수사기관 압수수색 절차	• 압수수색 준비 및 실시 • 압수수색 후 조치
피압수자 준수사항	• 준수사항: 즉시 통지, 영장 내용 확인 • 금지사항: 수사관 진입 방해, 증거인멸죄
상황별 대처요령	• Reception 도착 시 행동 요령 • 수사관 질문 시, 요구 시 행동 요령

6 사고발생시 대응체계 수립

주요 사고 시나리오 인지 단계

Example

I. 언론 노출	II. 자체 사고인지	III. 규제기관 점검 통보
• 방송 및 지면을 통한 사건 보도 • 인터넷 및 SNS 등을 통한 사고 전파	• 내부통제 활동을 통한 사고 인지 • 제보자를 통한 사고 사실 접수	• 수사당국의 압수영장 제시 • 감독당국의 특별 검사 통보

각 예상 사고 시나리오별 Legal Risk 최소화를 위한 핵심사항 도출

6 사고발생시 대응체계 수립

수사기관	감독기관	각종 소송
내부 관련자 관점	임직원 개인의 징계	단체소송
압수수색 대응방안	제재심의 前/後	행정소송
		형사소송

Example

7 교육 프로그램의 운용_예시(금융기관)

『전자금융감독규정』 정보보호 교육계획의 수립 / 시행

제19조의2(정보보호 교육계획의 수립 시행)

① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다.

1. **임원 : 3시간 이상 (단, 정보보호최고책임자는 6시간 이상)**
2. **일반직원 : 6시간 이상**
3. **정보기술부문업무 담당 직원 : 9시간 이상**
4. **정보보호업무 담당 직원 : 12시간 이상**

② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다.

③ 제1항의 교육프로그램 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.

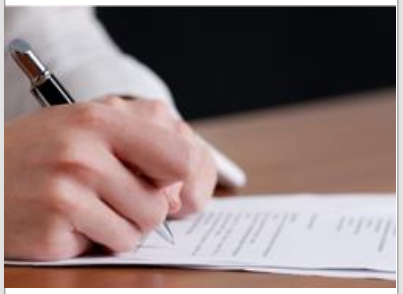
✓회차별 금융정보보호 교육프로그램 기획 및 운영

회차	대상	주요 교육 내용
1회차	임원	- 정보보안 사고로 인한 기업의 손실과 경영진의 손해배상 책임의 경감 방안 - 최근 금융감독당국의 금융 IT 규제 및 감사 동향
2회차	정보보호 업무담당 직원	- 정보보안 담당자의 책임 및 역할
3회차	정보기술 업무담당 직원	- 금감원의 IT감사 및 내부통제 기준 해설
4회차	일반직원	- 금융IT사고 발생 시 민.형사.행정상 책임 소재 감경 방안
5회차	정보보호 업무담당 직원	- 개인정보 Life-Cycle(수집/저장/이용/전송/파기)에 따른 금융정보보호 관리 방안 - 금융회사의 정보처리 위탁 및 제공 시 고려사항
6회차	정보기술 업무담당 직원	- 금융감독당국의 IT 감사 준비 및 사전 대응방안
7회차	일반직원	- 최근 사건 사고 및 판례를 통한 전자금융거래법규 해설
8회차	정보보호 업무담당 직원	- 최근 금융분쟁조정 사례를 통해 본 분쟁 대응 방안
9회차	정보기술 업무담당 직원	- 금융감독규제 준수를 위한 고려대 김인석 교수의 실전 Know-how 전수
10회차	정보보호 업무담당 직원	- 사전 금융정보보호업무 관련 질의 사항에 대한 맞춤형 Q&A

7 교육 프로그램의 운용

Example

CISO/CPO	Legal Team	Audit Team	IT Team

최근 사건사고에 따른 주요 판례	제개정 법규 및 제도 현황	사고 시 내부 통제 및 언론대응 절차	규제 기관 조사 대응 실무 절차
			

※ 특별 고려사항

IT감독국 제재관련 사례 및 감독당국 움직임

금융회사 해외지점에 대한 정보보호 컴플라이언스 관리 방안

금융정보 및 개인정보 역외이전에 대한 고려사항

계열사간 금융정보 공유에 따른 Compliance 이슈

내부통제와 준법감시

YULCHON 律村 YULCHON
법무법인(유) 율촌

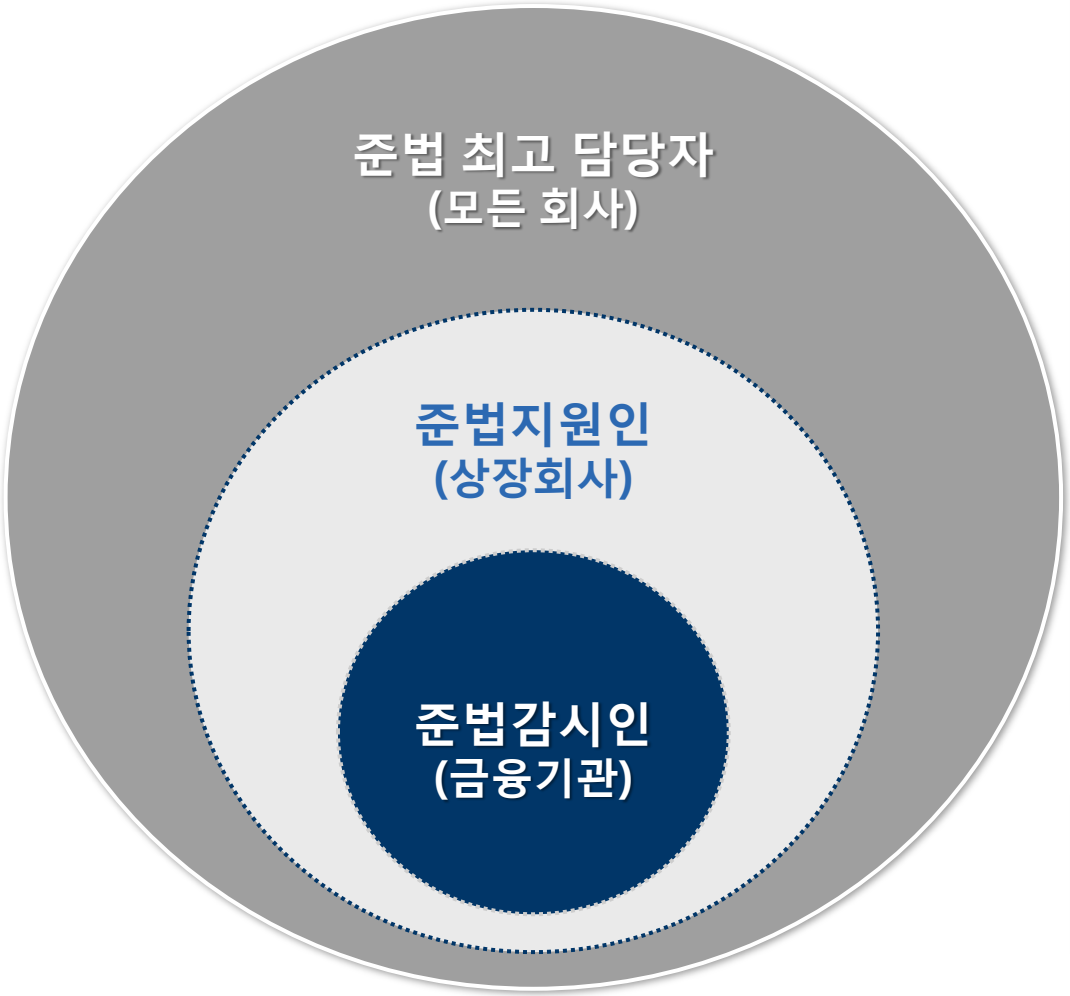
내부통제와 준법감시

내부통제

(광의) 이사회, 대표이사, 감사(위원회) 등에 의해 이루어지는 회사 경영 전반에 대한 감사, 준법감시(통제), 리스크관리, 내부회계 등을 포괄하는 통제행위

(협의) 법규준수차원의 내부통제 → 준법감시

준법지원인과 준법감시인



 # 준법 최고 담당자

- 준법지원, 준법통제 또는 준법감시에 관한 최고책임자
- 일반적인 컴플라이언스 업무 총괄 책임자
- 임의적 시행
  예) 개정상법상 준법지원인제도 신설 이전의 삼성전자 컴플라이언스팀장(부사장급)

 # 준법지원인

- 개정상법에 따라 자산 5천억 원 이상 상장회사에 의무적 시행

 # 준법감시인

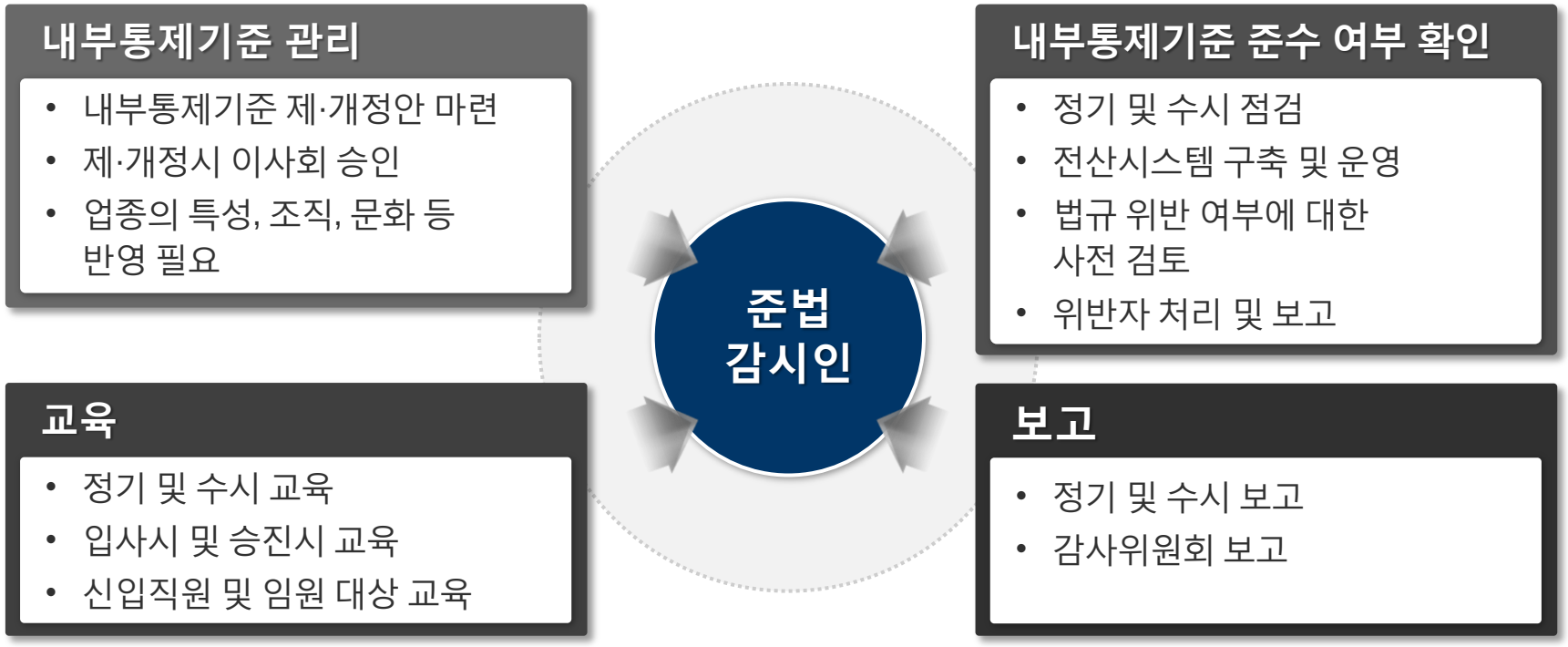
- 금융관련 법에 따라 의무적 시행

준법지원인과 준법감시인

구분	준법감시인	준법지원인
통제기준의 마련	목적: 회사의 건전성 유지, 이해상충 방지, 금융소비자 보호 명칭: **"내부"통제기준** 회사 및 그 임직원이 직무를 수행함에 있어서 준수하여야 할 적절한 기준 및 절차	목적: 법령 준수, 회사경영 적정 명칭: **"준법"통제기준** 임직원이 그 직무를 수행할 때 따라야 할 준법통제에 관한 기준 및 절차
준법 담당자의 설치 및 보고대상	**준법감시인** = 내부통제기준 준수 여부 점검, 내부통제기준 위반시 조사 **감사위원회 보고**	**준법지원인** = 준법통제기준 준수 관련 업무 담당, 준법통제기준 준수여부 점검 및 그 결과 **이사회 보고**

준법감시인의 역할

- **내부통제기준의 준수 여부 점검 + 내부통제기준에 위반시 조사 + 감사위원회 보고**
- **일반적으로 4가지 역할 수행**



준법감시인과 감사위원회(감사) 역할 비교

넓은 의미의 Compliance가 감사 업무를 포함함.

우리나라 현실

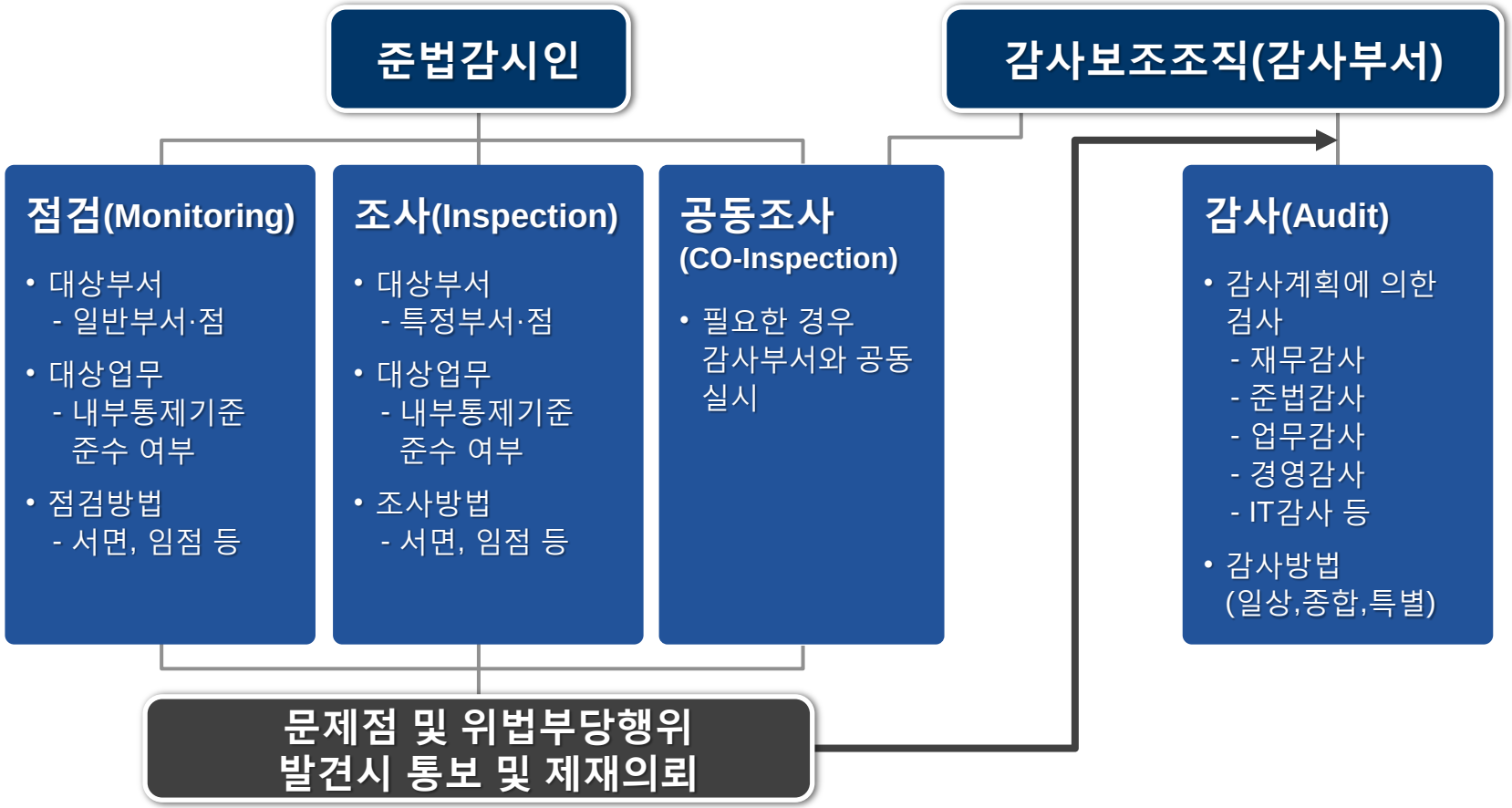
- 감사위원회(감사)는 감시 업무를 상시적으로 수행하는 하부조직을 두고 있지 않은 경우가 대부분
- 대부분 회계 감사 치중

준법감시인

- 상시적인 업무 감사에 종사하는 자
- 회사에서 문제되는 모든 법률적 이슈 검토

준법감시인과 감사위원회(감사) 역할 비교

은행 준법감시인 제도운영 모범규준



기타 사항: 주민등록번호

주민등록번호의 수집 제한

[2012. 8. 18. 시행] 정보통신망법 제23조의 2	[2014. 8. 7. 시행] 개인정보보호법 제24조의 2
① 정보통신서비스제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다. 1. 본인확인기관으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집이용이 불가피한 정보통신서비스제공자로서 방통위가 고시하는 경우	① 제24조 제1항(고유식별정보처리제한–별도 동의)에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우
② 위 제2호 및 제3호에 따라 주민등록번호를 수집·이용하는 **경우에도 대체수단(주민등록번호를 사용하지 아니하고 본인을 확인하는 방법)**을 제공하여야 한다.	② 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 **주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법**을 제공하여야 한다.

개정법에 따르면 오프라인에서도 주민등록번호 수집 원칙적 불가

주민등록번호의 파기

법령	내용
정보통신망법 부칙	• 2012. 8. 18.부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 하나, 주민등록번호수집이 예외적으로 허용되는 경우(제23조의 2 제1항)에는 그렇지 않음
개정 개인정보보호법 부칙	• 2014. 8. 7.부터 2년 이내에 보관 중인 주민등록번호를 파기하여야 하나, 다만 주민등록번호 수집이 예외적으로 허용되는 경우(법 제24조의2 제1항 각호)에는 그렇지 않음.
파기 방법	• 출력물은 파쇄 또는 소각, 전자기적 파일형태의 정보는 복원이 불가능한 기술적 방법으로 영구 삭제

주민등록번호의 파기 프로세스

1 주민등록번호 취급 목적 분석

- 대상 시스템에서 수집/이용하고 있는 주민등록번호의 정보주체 유형 분류 (Table 단위)
- 정보주체 유형 별 주민등록번호 취급 목적 분석

2 관련 근거 및 처리방안 제시

- 주민등록번호 취급 목적에 따른 관련 법규 매핑
- 관련 근거에 따른 보관 기간 또는 파기 등의 처리방안 제시

3 법률적합성 검토

- 관련 법규 법리적 타당성 검토
- 취급 목적 및 관련 근거 간의 conflict 발생 시

Example

시스템	DB 명	Table 명	정보주체				취급 목적	처리 방안		관련 근거					비고
			임직원	고객	협력사	기타		보관	파기	전자금융거래법	부가가치세법	소득세법	…	고용보험법	
AA시스템	인사DB	Master_T	●			●	직업능력개발 훈련 실시	●						●	시행령 제41조, 시행규칙 제60조
							소득지급 및 원천징수	●				●			법 제145조
BB시스템	거래처DB	Co_T		●	●		세금계산서 발행	5년	●		●				법 제 조
	회원DB	Member_T		●		●	온라인 제품 구매이력	5년	●						법 제6조, 제7조, 제16조

결 론

맺음말

✓정부, 개인정보 관리를 최우선 과제로 점검

"개인정보보호 강화는 금년에 정부가 추진하는
비정상의 정상화 과제 중에서도 가장 중요한 과제"

"100-1 = 0" ? (Broken Window Theory)

회사, 경영진 및 정보보호 책임자의 법률 리스크 완화 위한 선제적 방어 체계 (Preemptive Defense) 수립 필요

법무법인(유) 율촌 소개

YULCHON 律村 YULCHON
법무법인(유) 율촌

율촌의 정보보호 컴플라이언스 전문가

- **정보보호 컴플라이언스 주요 구성원 및 업무 경험**

윤희웅 변호사		• **정보보호 대응팀 Leader (율촌 기업법무 부문장. 미래창조과학부 고문변호사)**
고문	**형태근**	• 前 방통위 상임위원(차관급) 및 現 부산시장 정보통신 정책고문
	문재우	• 前 **금감위 상임위원** 및 손해보험협회장
	유흥수	• 前 **금감원 부원장보** 및 LIG투자증권 대표이사
	양성용	• 前 **금감원 부원장보, 기획조정국장**
	박삼철	• 前 **금감원 법무실장** 및 現 금융법학회 부회장
한국 변호사	**손도일**	• **개인정보처리 시스템의 구축 및 보안, 진단 등과 관련한 각종 규제 및 Risk Management 프로젝트 수행**
	임재연	• 前 **금융제재심의위원회 위원** 및 前 금융위원회 금융발전심의회 자본시장분과위원 역임
	김세연	• 개인정보 및 정보보호 침해 민형사 소송 대응 및 자문 수행 (GS Caltex 소송 대응)
	조상욱	• 노동관련법령 해석상 문제에 관한 자문, HR COMPLIANCE PROGRAM, 임직원의 개인정보 처리에 관한 자문
	박재현	• 개인정보보호법 시행령 등 관련 법규 제정에 참여하고, 개인정보분쟁조정위원회 위원으로 활동
	손금주	• 규제기관 및 사업자들을 위하여 방송통신 규제, 개인정보 보호 등과 관련한 자문과 소송업무 수행
	이희중	• 개인정보 및 정보보호 침해 민형사 소송 대응 및 자문 수행(GS Caltex 소송 대응)
	김세진	• 개인정보보호와 관련된 규제 이슈 전반에 관한 법률 자문 제공, 외국계 자동차 제조 및 판매회사 관련 자문
	김현정	• 개인정보 보호 표준지침 제정 작업 등 정보보호 관련 업무 다수 수행
	최재혁	• 기업,금융범죄 등의 수사 전담 검사 출신으로써 개인정보관련 형사 사건 자문 및 소송 업무 수행
	이정환	• 개인정보보호 뿐만 아니라 기업일반, M&A 등 업무에 대한 법률 자문

율촌의 정보보호 컴플라이언스 전문가

- **정보보호 컴플라이언스 주요 구성원 및 업무 경험**

윤희웅 변호사		• **정보보호 대응팀 Leader (미래창조과학부 고문변호사)**
미국 변호사	**이재욱**	• 개인정보에 관한 형사 및 민사 소송 수행, e-Discovery, forensic 및 기업내부조사 등 / 현재 CPO 포럼 위원
	윤용	• 前 방송통신위원회 과장, 개인정보법제 개선반 자문위원 등 방송통신위원회의 부문별 법률 및 정책 자문
전문 위원	**이후록**	• **금융감독원 출신으로 은행검사 및 감독, 보험감독 등** 다양한 유형의 금융 Compliance 자문
	유호범	• **금융감독원 선임조사역 출신으로 기획조정국, 총괄조정국, 은행검사국 등**의 다양한 업무 수행
	고영대	• 개인정보 및 정보보호 관리체계 구축, 이행, 감사/진단 및 컨설팅 관련 보안 자문
	박준일	• 개인정보 및 정보보호 관련 시스템 구축 및 운영, 진단 등 보안 관련 자문
자문 (고려대)	**김인석**	• 現 **고려대학교 정보보호대학원 금융보안연구소 교수** • 戰 금융감독원 IT감독국 부국장 및 한국은행 과장

율촌_주요 사업실적

- **Compliance 수행 실적**

프로젝트명	프로젝트 내용
Compliance System 구축 Project	**A자동차사**의 전반적인 Compliance 구축 및 자문
IP Compliance Project	**B화학소재** 기업의 IP, HR 및 개인정보보호 부문에 특화된 Compliance Program 구축/자문
Compliance Audit Project	**C외국계 의료회사**의 공정거래, 의료제약규제 분야 등의 준법실태 점검을 위한 Audit Project
Compliance Package	**D소비재사**의 준법지원인제도 도입 관련 자문 제공(준법통제기준 제정 / manual 제공)
불법방지 프로그램(LRMS) 개선 프로젝트	**E반도체사**의 불법방지프로그램 개선과 관련된 전반적인 Compliance 자문
기업내부조사 및 Compliance guideline 수립	**외국계 F보안업계**의 기업내부조사 및 내부 Compliance 가이드 라인 수립
공정거래 Compliance project	**외국계 G의료기기사**의 Compliance 매뉴얼, 내부규정, 가이드라인 작성 등 전반적인 자문

프로젝트명	프로젝트 내용
공정거래 Compliance project	**외국계 J제약사**의 기업내부조사와 Compliance manual 작성 및 교육
준법점검 이사회보고 프로젝트	**K중공업**의 준법점검결과에 대한 이사회보고를 위한 제반사항 준비를 위해 필요한 자문
Compliance 프로젝트	**L광학 및 의료기기사**의 준법실태 점검 및 개선방안 수립 관련 자문 제공
컨설턴트 채용 개선 프로젝트	**M중공업**의 영업비밀 유출을 막는 Compliance 프로그램
영업비밀 유출 및 침해 방지를 위한 Compliance 프로젝트	**P제조 그룹**의 영업비밀 유출 및 침해 위험을 경감위한 전반적인 Compliance 프로그램 구축
직무발명 제도 개선 프로젝트	**R 가전 및 전자**의 직무발명 보상과 관련한 소송 리스크를 경감시키는 프로젝트
공정거래 Compliance project	**SI업체 S사**의 IT 업체의 거래구조, 사업특성, 실무 등을 파악하여 Compliance 자문 제공.

율촌_주요 사업실적

- **정보보호, 개인정보보호 및 금감원 제재 대응 실적**

사업자 명	프로젝트 내용
국내 금융기관	초대형 고객정보 유출사건 법무 자문 및 대응 지원
H사(제조사)	개인정보 보호법 등 개인정보 관련 법령의 준수여부를 함께 검토하고 대안 제시
외국계 B사(금융기관)	정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관계 법령 자문
C 카드사	문서보관시스템에 관한 실사 및 개선책 제시
H사(금융기관)	고객과 임직원의 개인정보 처리 프로세스 개선 및 유출 시 대응방안 마련
전국은행연합회	금융기관이 처리해야 하는 개인정보와 관련된 각종 서식 점검 및 compliance 업무 수행
국민은행, 금융감독원, 금융투자협회, 농협손해보험, 롯데캐피탈, 삼성생명, 예탁결제원, 우리금융지주, 중소기업은행 등	개인정보 관련 다수의 자문 업무 수행
A 손보, B 카드, C캐피탈, D, E저축은행, F 대부업 등	IT감독국의 금융회사 검사 제재 자문

Q & A