자본시장 IT 파트너
koscom

내부통제를 위한 효과적인 프로세스 전략

2014.06.24

강사 소개

전자신문

2012년 08월 28일 화요일 014면 경제과학

스마트금융시대 Q&A

〈1〉스텍스넷 공격은 실제 가능한가

제어시스템과 인터넷 분리…현실적 불가능

정보기술(IT)은 은행, 증권, 보험 등 금융산업에서 고객 편의와 보호를 위해 인체의 핏줄과도 같은 역할을 하고 있다. IT가 날로 복잡해지고 전문화된 영역으로 발달하면서 관련 트렌드 조차 따라잡기 어렵게 됐다. 앞으로 10회에 걸쳐 자본시장 IT지킴이 역할을 하고 있는 코스콤 IT 전문가들과 문답형식으로 궁금증을 풀어본다.

Q:최근 TV드라마 '유령'에는 사이버수사대 김우현(소지섭 분) 팀장이 대한전력을 상대로 외부 해커의 스텍스넷 공격을 막는 장면에서, 전력시스템이 인터넷과 연결되지 않았는데도 해커로부터 조종·파괴당할 수 있나.

A:결론부터 말해 현실적으로 불가능하다. 스텍스넷은 발전소, 공항, 철도 등 기간시설(SCADA 시스템)을 파괴할 목적으로 제작된 컴퓨터 바이러스 또는 악성코드를 의미한다. 그런데 기간시설을 제어하는 시스템이 인터넷과 분리돼 있고, 해당 시스템을 관리하는 PC 조차 무선랜이나 별도의 우회 접속경로가 없다면 해킹은 어렵다. 드라마 내용처럼 USB를 통한 스텍스넷 유입은 가능하나 좀비 PC 또는 원격으로 추가 명령 실행 등을 조정할 수는 없다.

그러나 만약 SCADA 시스템을 잘 아는 개발자가 의도적으로 악성코드를 개발해 이를 USB에 담아서 유입시킨다면 사전에 조작된 제어시스템으로 파괴나 오작동을 일으킬 수는 있다. 드라마 내용처럼 해커가 해킹을 시도하면 무방비로 당할 수밖에 없는 것일까. 이에 대한 대답은 '노(No)'다. 통합보안관제라는 기능을 통해 사전에 사이버 테러를 방지할 수 있다.

통합보안관제시스템은 증권·선물회사나 증권유관기관 등을 대상으로 해킹, DDoS공격 등 사이버 침해사고 발생 시 국가사이버안전센터 등과 연계해 대응을 강화하고, 상황에 따라 피해 확산 방지를 위한 보안정보를 수집·분석해 증권사와 관계기관에 신속하게 전파하는 예방 체계다. 또 이 시스템을 통해 증권·선물회사와 한국거래소(KRX)를 연결하는 사이버 트레이딩 구간 등의 침해에 대비해 24시간 365일 모니터링을 실시하는 한편, 침해 대응 능력 향상을 위해 모의훈련도 함께 수행하고 있다.

이주호
코스콤 정보보호센터 차장

전자신문

2012년 08월 30일 목요일
012면 경제과학

스마트금융시대 Q&A

〈2〉PC 해킹

원격제어 SW 이용하면 손쉬워 PC 모든 개인정보 유출돼 '위험'

Q:드라마 '유령'에서 '대한전선 스텍스넷 공격'과 관련해 또 다른 논란 장면은 신효정(이솜 분)이 트위터에 유서를 남기고 자살한 장면에서 해커 하디스(최다니엘 분)가 신효정의 트위터 계정을 해킹해 동영상을 손에 넣는 것이었다. 해커 하디스가 신효정 PC를 해킹해 동영상을 갖게 되는 게 실제로 가능한가.

A:원격제어 프로그램을 통해 얼마든지 가능하다. 원격제어 프로그램은 주로 특정 제품이나 서비스에 문제가 있을 때 직접 방문하지 않고도 문제를 해결할 수 있도록 도와주는 프로그램이다. 이를 이용하면 상대방 PC에서 내 PC 상태가 동일하게 보이기 때문에 상대방이 내 PC를 조작할 수 있다. 이러한 원격제어 프로그램이 실행 중인 가운데 내 PC에 카메라까지 설치돼 있다면 사용자 모르게 파일 검색·전달은 물론이고 동영상 촬영까지도 가능하다.

중요한 것은 원격제어 프로그램은 이메일이나 인터넷 게시판 등을 통해 불법적으로 유포될 수 있다는 점이다. 악의적으로 생성된 원격제어 프로그램을 다운로드해 실행하면 내 PC는 해커들에게 그대로 노출될 수 있다. 그렇게 되면 로그인 비밀번호 설정, 프로그램 패치 미실시 등 PC 해킹이 가능하다. PC에 저장돼 있는 모든 정보는 해커 손에 넘어가게 된다.

드라마 유령에서 보여주듯 인터넷에 연결된 PC는 악성코드에 의한 해킹이 가능하기 때문에 금융권에서는 인터넷용과 업무용으로 PC를 나누는 망분리 작업이 한창이다. 만일 인터넷용 PC가 내부시스템과 연결돼 있을 경우 PC 내의 정보뿐 아니라 내부시스템의 DB, 개인정보 등도 유출될 수 있기 때문이다.

따라서 이와 같은 사고를 예방하기 위해서는 인터넷용 PC와 내부시스템 연결용 PC를 물리적으로 망분리하는 것이 최선의 방법이다.

이주호
코스콤 정보보호센터 차장

강사 소개

아주경제

2013년 01월 31일 목요일
018면 증권

■ 코스콤 정보보호센터부 이주호 차장

"정보보호 업무프로세스 마련 한계 개인들 정보보호 의식 성숙해져야"

"IT기술이 발전함에 따라 정보보호에 대한 중요성이 강조되면서 보안 수준을 끌어올리기 위해 각종 대책들을 강구해 힘쓰고 있습니다. 다만 보안 사고를 최소화하기 위해서는 우선적으로 정보보호 의식에 대한 성숙이 절대적으로 필요합니다."

코스콤 정보보호센터부 이주호 차장(사진)은 30일 아주경제와의 인터뷰에서 정보보호에 대한 중요성을 강조하며 이같이 말했다. 대부분의 금융투자업무는 정보기술(IT) 시스템을 통해 이뤄지고 있다. 특히 스마트폰을 이용한 모바일트레이딩시스템이 최근 발전하면서 PC환경에서 일어났던 각종 보안사고가 모바일로도 옮겨갈 것으로 보고 있다.

이에 따라 코스콤은 지난해부터 각 분야의 IT전문가로 구성된 '스페셜리스트 그룹'을 만들어 IT지식 알리기에 나섰다. 이 차장 역시 그 가운데 한 명으로 지난해부터 금융 정보공유분석센터(ISAC) 취약점분석평가 컨설팅을 총괄하고 있으며 사내 정보보호 정책을 수립하고 있다.

금융ISAC은 전 증권사의 사이버트레이딩시스템을 모니터링해 사이버테러나 해킹 등에 관한 정보를 수집하고 이를 분석, 제공하는 조직이다.

금융ISAC을 운영하고 있는 코스콤은 '철통방어'를 위해 지난해부터 네트워크 인프라와 정보보호 기능을 통합 운영하고 있다. 이에 따라 종전까지 분리돼 있던 네트워크 트래픽 관리와 정보보호 대응장비 관리 기능이 합쳐지면서 디도스 등 사이버 테러에 대한 공동 모니터링을 실시해 신속한 정보 공유와 빈틈없는 유기적 침해대응이 가능할 것으로 보인다.

이 차장은 "금융투자업계는 각종 IT업무를 안전하게 서비스하기 위해 각고의 노력을 기울이고 있다"며 "금융당국 또한 안전한 금융거래를 위해 각종 대책을 수립하고 있다"고 말했다. 이에 관심 분야로는 정보보호거버넌스, 디지털 포렌식(디지털 범죄수사) 기타 정보보호신기술을 꼽았다.

정보보호거버넌스는 최고경영층이 직접 정보보호를 챙길 수 있도록 하고 정보보호의 효과와 영향을 보고할 수 있도록 체계를 구축하는 것을 의미 한다.

디지털 포렌식은 해킹, 개인정보 유출 등 디지털적인 사고가 났을 때 디지털적인 정보를 분석해 사고에 대한 사실 유무를 확인하는 것으로 소송의 증거자료로 유용하다. 그러나 이 차장은 "금융투자업계가 정보보호 업무프로세스를 마련하는데 있어서 한계가 있다"면서 "가장 먼저 보안에 대한 개인의 의식부터 성숙해져야 된다"고 판단했다.

또 이 차장은 "보안토큰과 같이 편의성 등의 문제로 보안 수준이 낮은 상태로 방치해 두는 경우가 빈번하다"며 "이에 대한 결과는 결국 개인의 책임이기 때문에 정보보호 의식이 성숙해야 되는 단계"라고 전했다. .

박정수 기자 wjdtn0227@

디지털타임스

2013년 06월 18일 화요일
009면 정보통신

시스템 계획부터 정보보호책 마련

굿모닝 금융 IT ▮ ICT 보안성 검토프로세스

요즘 국내 스마트폰 회사들의 광고 경쟁이 흥미롭다. '당신의 곁에서 당신과 교감하다(Life companion)', '보지 않으면 멈추고 바라보면 재생되는 눈동자 인식', '카메라보다 스마트폰으로 찍는 사진이 더 많다' 등 광고 카피마다 스마트폰이 우리 삶과 밀접하게 연결돼 있는 점을 강조한다.

이같은 정보통신기술(ICT)은 이미 현대인의 삶 속에 깊숙이 스며들어 많은 변화를 일으키고 있다.

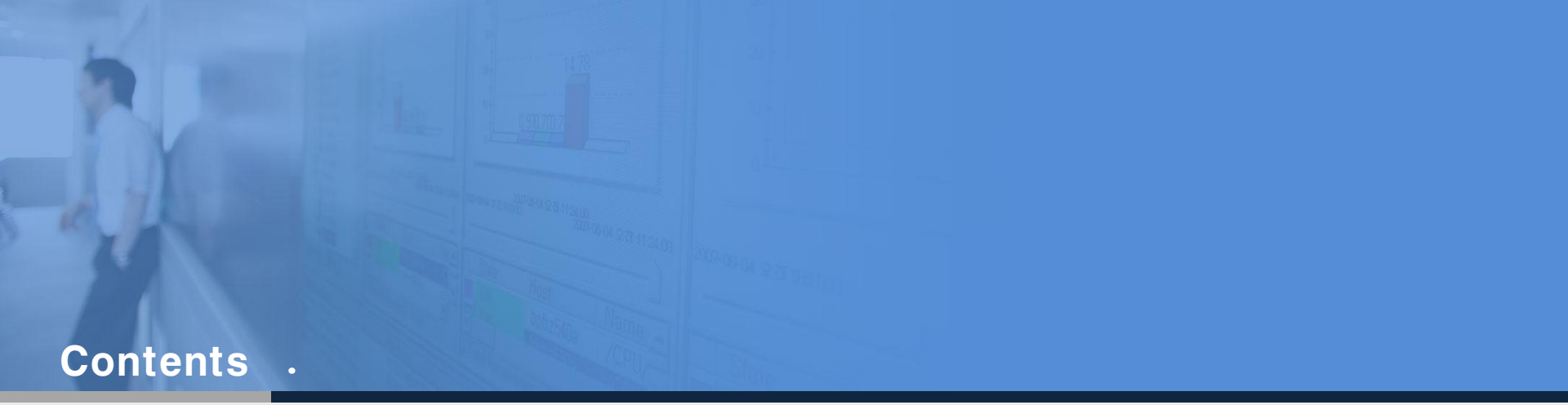
지난 5일 정부가 발표한 '창조경제 실현계획'은 이러한 맥락을 반영한 것으로 보인다. 과학기술과 ICT를 활용해 신산업·신시장을 개척하고 창조적인 경제문화를 조성한다는 것이 주요 골자다. 전 산업분야에서 창의적 아이디어와 기술융합을 통해 포스트 스마트폰 같은 혁신적인 발전을 이루고자하는 로드맵을 제시하고 있다.

중요한 것은 ICT의 양면성이다. ICT는 실생활을 편리하게 할 수 있는 반면 위·변조, 복사, 파괴가 가능한 근본적인 약점이 있다. 해킹 및 사이버테러를 완벽하게 차단할 수 없는 것은 이 때문이다. 올해 3월20일 방송사와 일부 금융회사의 PC 및 시스템이 동시에 파괴되는 사태가 발생했다. 그 원인은 장기간 지속적으로 정보를 수집해 만들어진 악성코드인 지능형 지속 위협(APT) 공격방식으로 밝혀진 바 있다. 우리 삶에 편리함을 더해주는 ICT의 양면성을 체감할 수 있는 사건이었다.

ICT 보안성 검토 프로세스는 ICT 시스템 계획 단계부터 정보보호대책을 수립하고, 프로그램 개발 시 시큐어 코딩, 서비스 이행 전에 취약점 점검 등 대책을 확인하는 일련의 과정이다.

창조경제를 실현하고자하는 이 시점에서 'Life companion'과 같은 편리함을 마음껏 누리는 이면에 해킹, 시스템 파괴 등 ICT의 칼날을 예방하기 위해 정부 및 기업에서 ICT 보안성 검토 프로세스의 요구와 점검 수준을 점차 강화해야 할 것이다.

이 주 호
코스콤
정보보호센터부 차장



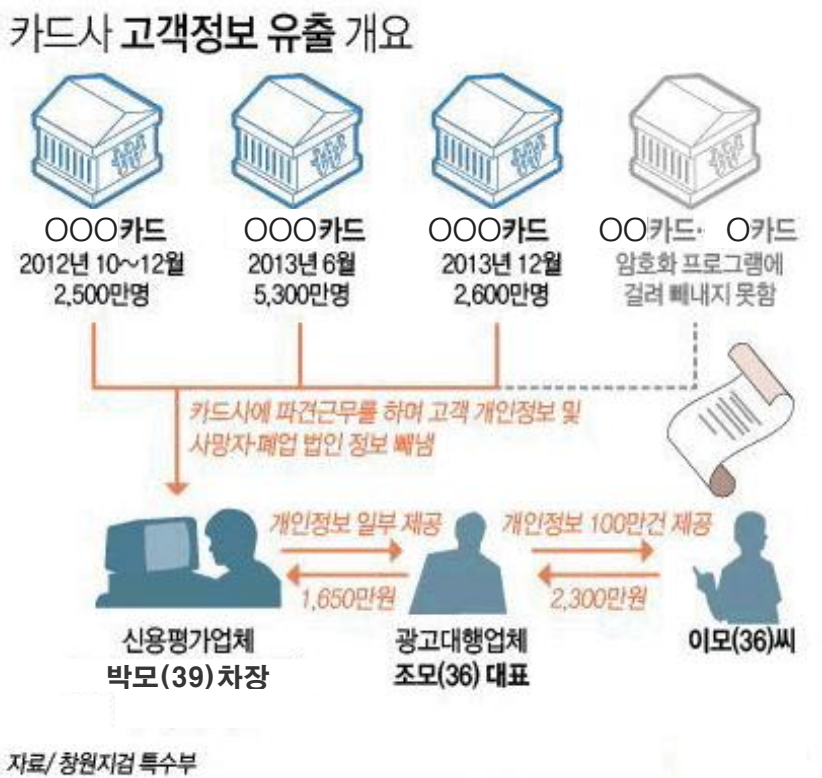
Contents .

미안합니다 … 잊지 않겠습니다.

미안합니다 … 잊지 않겠습니다.

다른 사건은…

- **카드 3사의 고객정보 약 1억 400만건 유출('14.1)**
  - 유출 정보 : 성명, 주민번호, 휴대전화번호, 직장명, 주소, 카드번호, 유효기간 등

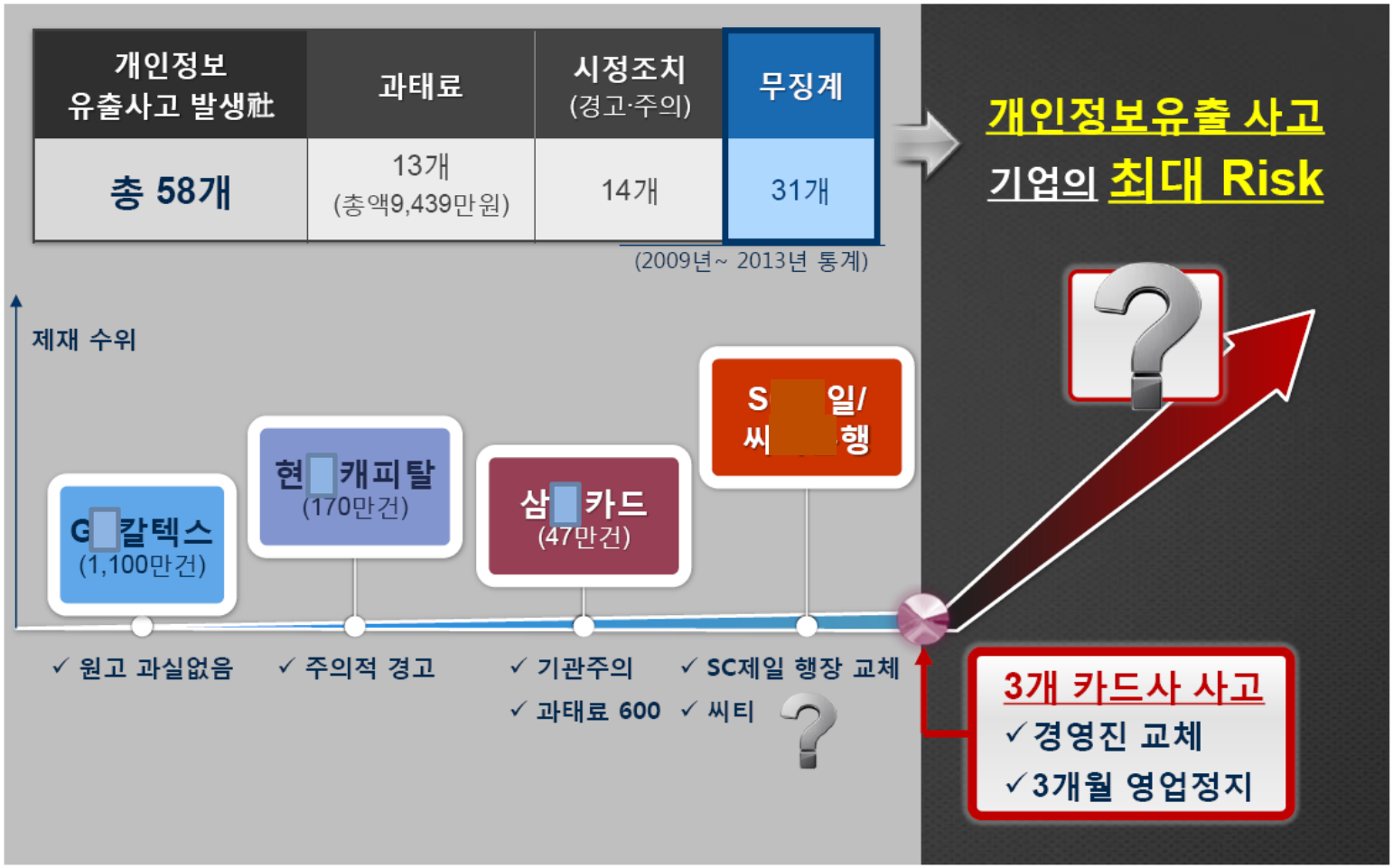


다른 사건은…

발생 일시	사고 제목	사고 내역	사고 영향(임직원 사퇴 및 징계)
2014년 1월	**L사,K사, N카드 개인정보유출**	약 1억건	◆ **K행장, 카드사장 포함 경영진 27명 사퇴** ◆ **L카드 사장 포함 경영진 9명 사퇴** ◆ **N카드 카드부분 부행장 1명 사퇴** ◆ **3개월간 영업정지**
2013년 12월	**C 은행, S 은행 개인정보유출**	C : 3만여건 S : 10만여건	◆ **CEO에 문책경고 예고** ◆ **은행에 기관경고 예고**
2013년 3월	**3.20 방송사, 은행전산망 사이버테러**		◆ **5개 금융회사 기관주의 조치** ◆ **관련 임직원 총 23명 제재 조치('13. 12)**
2012년 10월	**S은행,C 은행, S은행 등 8개사 고객정보 부당조회**	지난 3년간 고객정보 1.5만건	◆ **262명 제재** ◆ **7개 은행 ~600만 과태로** ◆ **S은행:20명 직원 문책 및 감봉** ◆ **W은행:기관경고,3320만 과징금, 51명문책** ◆ **C은행:1억 6300만 과징금, 44명 문책**

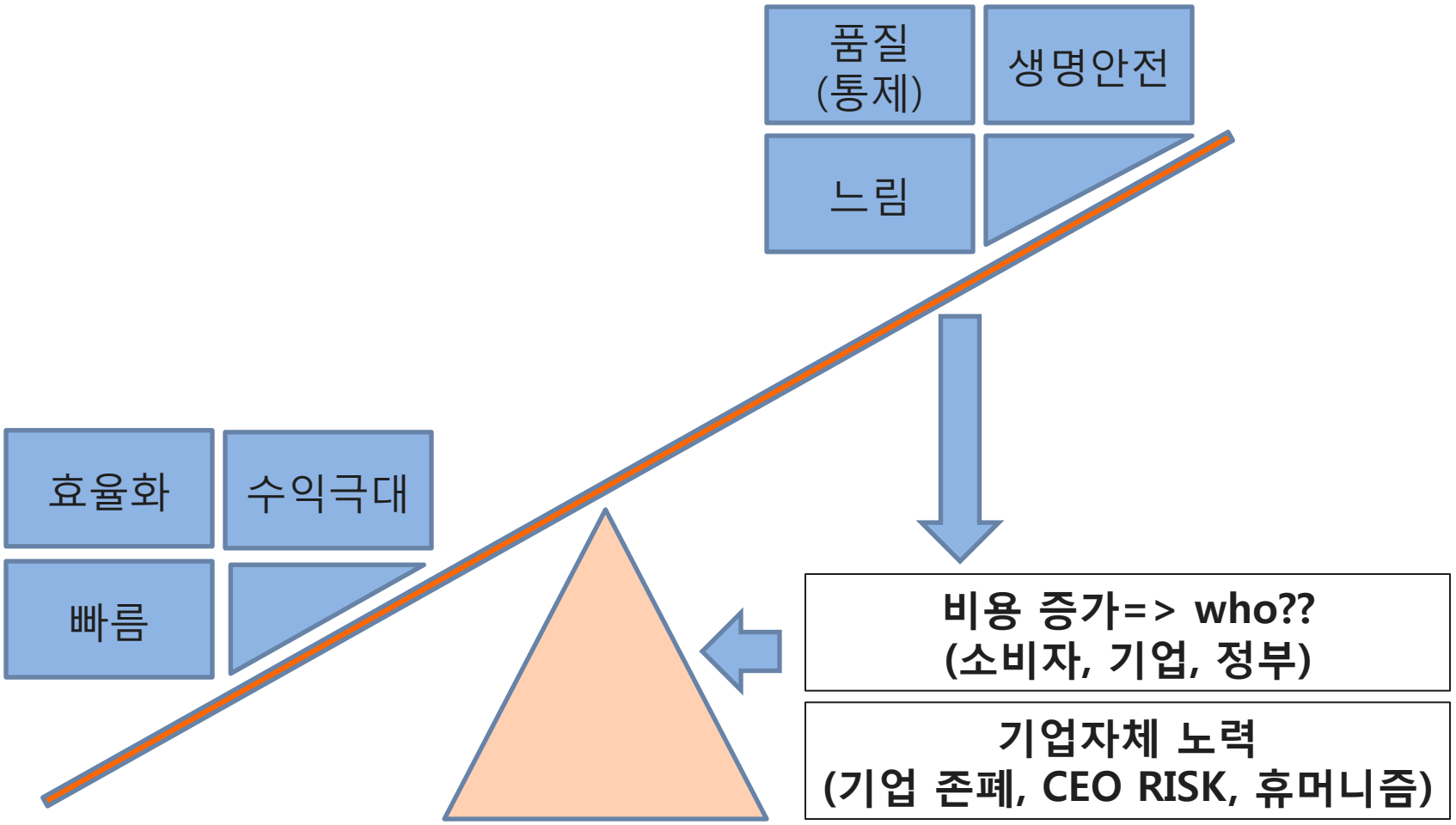
다른 사건은…

금융 'IT사고'_기업의 최대 Risk

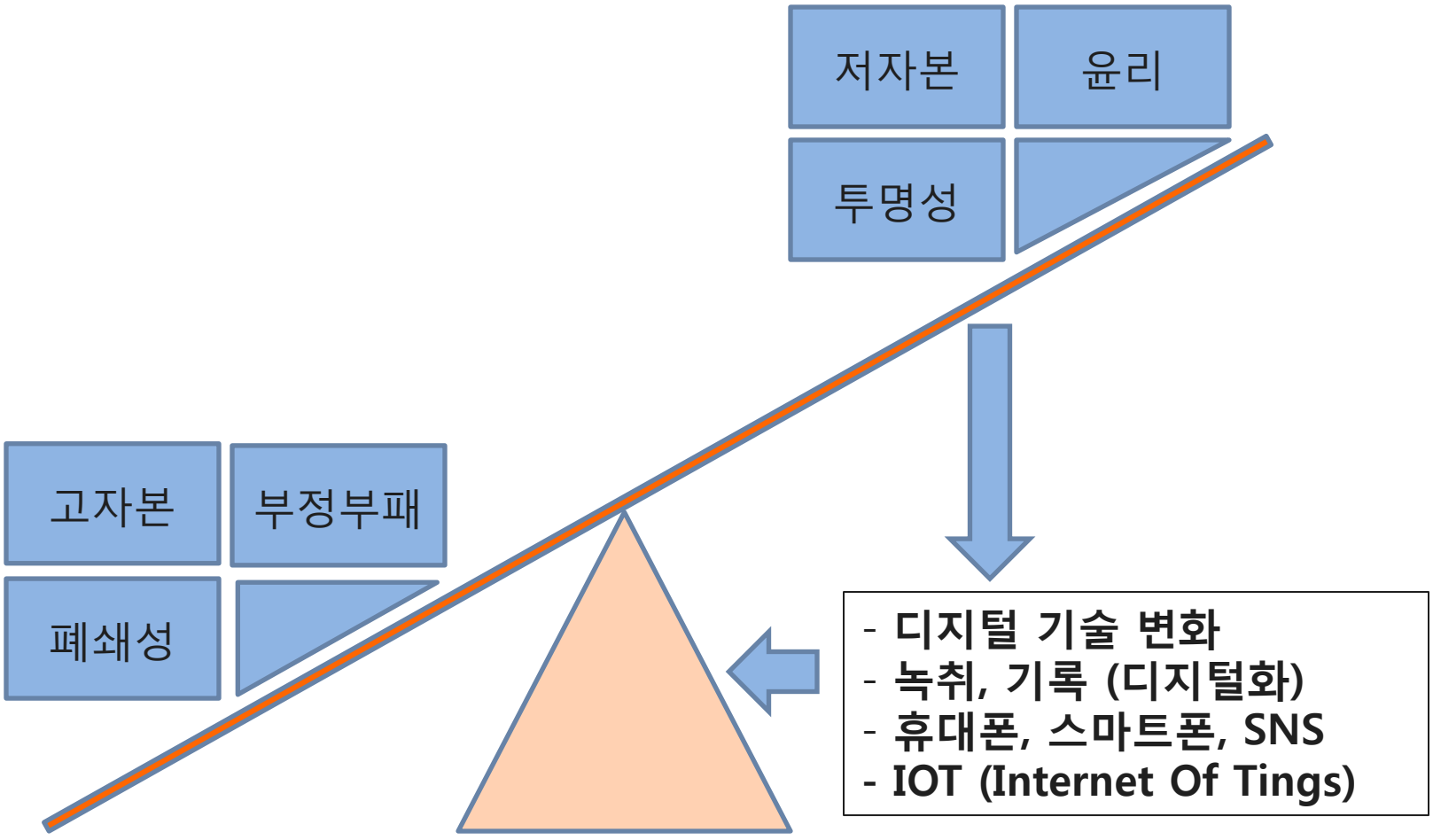


* 출처 : 율촌법무법인

패러다임의 변화


품질
(통제)
생명안전
느림
효율화
수익극대
빠름
비용 증가=> who??
(소비자, 기업, 정부)
기업자체 노력
(기업 존폐, CEO RISK, 휴머니즘)

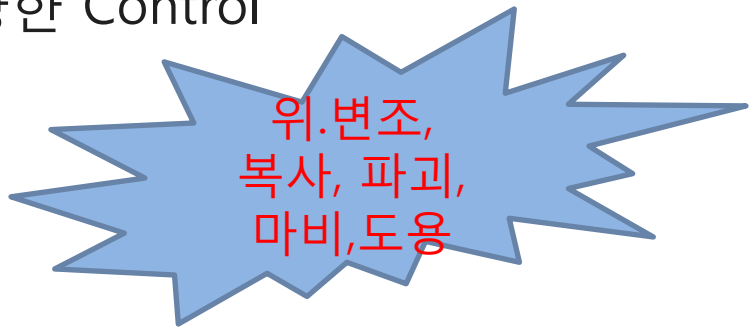
패러다임의 변화


저자본
윤리
투명성
고자본
부정부패
폐쇄성
- 디지털 기술 변화
- 녹취, 기록 (디지털화)
- 휴대폰, 스마트폰, SNS
- IOT (Internet Of Tings)

IT, Digital 의 양면성

Efficiency ↑ V.S. Threat ↑

⇒ 적절한 조치가… 다양한 Control



내부 통제

내부 통제?

갑자기 이 시점에

왠 내부 통제...

준법 감시 v.s. 내부통제

- 은행법, 보험업법, 자본시장법, 금융지주회사법 등

- 내부통제 기준 : 법령을 준수하고 경영을 건전하게 하며 주주 및 예금자 등을 보호하기 위하여 그 은행의 임직원이 직무를 수행할 때 따라야 할 기본적인 절차와 기준 (이하 "내부통제기준" 이라 한다) 을 정해야 한다.

- "내부통제기준" 의 준수여부를 점검하고, 내부통제기준을 위반하는 경우 이를 조사하여 감사위원회에 보고하는자 (이하 "준법감시인" 이라 한다)를 1명 이상 두어야 한다.... 중략...

내부통제기준 (은행법 예)

- 은행법 시행령 제17조의 2(내부통제 기준)

  - 업무의 분장 및 조직구조에 관한 사항
  - 자산의 운용 및 업무의 수행과정에서 발생하는 위험의 관리에 관한 사항
  - 임직원이 업무를 수행할 때 반드시 준수하여야 하는 절차에 관한 사항
  - 경영의사결정에 필요한 정보가 효율적으로 전달될 수 있는 체제의 구축에 관한 사항
  - 임직원의 내부통제기준 준수 여부를 확인하는 절차 방법 및 내부통제 기준을 위반한 임직원의 처리에 관한 사항
  - 임직원의 금융자자상품 거래내용의 보고 등 불공정거래행위를 방지하기 위한 절차나 기준에 관한 사항 등

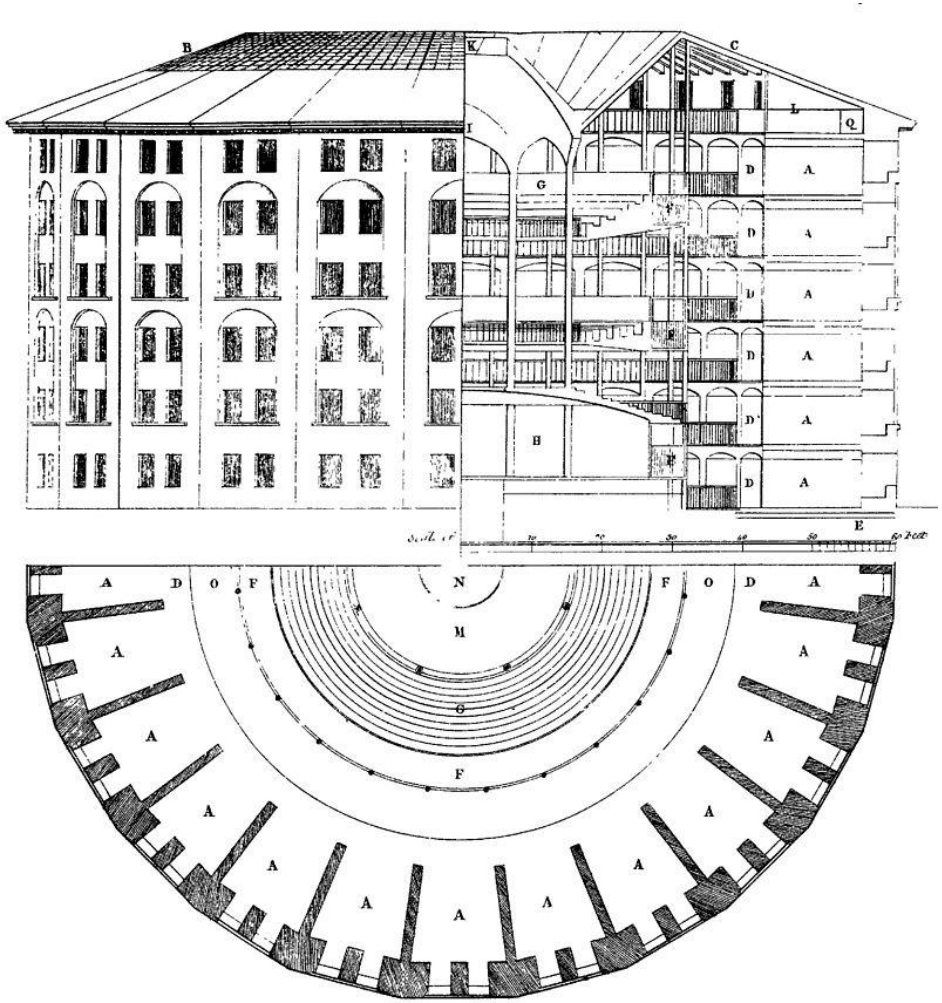
내부 통제

- 내부통제 : 기준 OR 적용
- 준법감시 : 점검 및 조사 행위
  (= Compliance Management)

명확하지는 않지만 통념적,

준법 > 내부통제 ? 감사

내부 통제



파놉티콘을 아십니까?

(pan + opticon)
벤덤
이중 원형건물
감시탑
수용자, 감시자

우리의 내부 통제는?

감사 업무는 뭐고?
Vs.
준법 감시는 뭐지?

내부 통제

아.... 이래서 내부 통제?

금융회사 고객정보 유출 재발방지대책

2014. 1. 22

기획재정부 미래창조과학부 법무부

안전행정부 금융위원회

Ⅲ. 향후 재발방지방안

제도 개선 기본 방향

◈ 개인신용정보 수집·보관·관리 및 유출사고 대응 등 **전반에서 제기되는 문제를 점검**하여 **보다 근본적으로 개인정보유출 재발을 방지**하는 **제도개선 방안**을 마련·추진

① **금융회사**는 "**필요최소한**"**의 정보만 보유**토록 하여, 만일의 정보유출시에 **발생할 수 있는 피해를 최소화**

* 금융회사 정보보유 실태 전면 점검, 과거고객의 정보 별도 관리 및 보존기간의 합리적 설정 등

② **금융회사 정보수집·보관방식을 소비자 관점에서 대폭 개선**

* 제3자 정보제공 동의시 포괄적 동의 제한, 마케팅 목적 제3자 정보활용은 원칙적으로 제한, 금융지주그룹내 고객정보 활용 제한(외부영업활용 제한) 등

③ **불법적인 정보유통의 근본적인 수요측 유인을 제거**

* 불법유출 정보를 활용한 대출모집인 등의 자격박탈 및 영구퇴출, 대출모집인이 불법 유통정보 활용시 전속 금융회사 제재 등

④ 정보보호 관련 **금융회사 및 임원의 책임을 확대**

* 개인신용정보책임자 등의 CEO 및 이사회 주기적 보고 의무화, 정보보호 관련 내부통제 이행에 대한 점검 프로세스 강화 등

⑤ 정보유출관련 **행정제재, 형벌 등 사후제재를 대폭 강화**하고 **징벌적 과징금제도를 도입**

* 개인정보를 유출하거나 불법적으로 활용시 징벌적 과징금 부과, 형벌(징역·벌금) 수준을 대폭 상향조정 등

◈ 향후 이러한 방향으로 **2월초까지** 관계부처 합동 「**금융회사 고객정보보호 정상화 T/F**」에서 **구체적인 세부 실행방안을 확정**

내부 통제

나 내부통제제도 개선 및 외주업체 관리 강화

① 정보보호 내부통제제도 실효성 강화

○ (**현황 및 문제점**) 고객정보 보호를 위한 **내부통제 규정***은 마련되어 있으나 **실행단계에서 제대로 지켜지지 않아** 내·외부 직원에 의한 정보유출사고 발생

* 자료 접근통제, 조회·출력 통제, 인터넷 차단 등(전자금융감독규정§12 및 §13)

○ (**실효성 강화**) 금융회사의 **자체 보안이행 점검 프로세스를 강화***하고, **금감원 검사**시 보안규정 준수여부를 철저히 점검

* (금융회사) 자체 보안규정을 보완·구체화하여 규정 준수여부를 CISO 책임 하에 매월 점검하고('보안점검의 날' 지정), 취약점은 즉시 보완
* (금감원) 보안관련 법규정 준수여부를 철저히 검사하고, 미준수시 엄중 제재

- 내부 보안통제 실효성 강화를 위해 직원의 업무별·직급별 고객정보 접근권한·범위를 명확히 하는 **보안등급제** 추진

- **금감원에 '기동점검반'을 운영**하여 **내부통제상황 및 정보보호 현황 등을 분시에 점검**하여 평소에 이행을 담당

② IT 외주업체 관리 강화

○ (**현황 및 문제점**) 금융의 정보화·전산화 확대로 인해 정보시스템 개발·유지 및 정보처리의 **외부위탁이 불가피하게 증가**

- **외주용역에 대한 통제규정***은 마련되어 있으나 **실행단계에서 실무적 편의를 추구**하다가 규정위반 사례 발생

* 최소작업권한 부여, 전산장비 반출입통제, 테스트시 가상자료 사용 및 종료시 자료삭제, 고객정보유출금지 등(전자금융감독규정 §13 및 §60)

○ (**관리 강화**) 금융회사의 외주용역에 대한 **CEO·CISO의 사전 승인·사후관리 절차**를 명확히 하고

- CISO 책임 하에 **외부저장매체**(노트북, USB 등)의 **반입통제**를 철저히 시행

- **금감원 검사**시 외주용역 통제규정 준수여부를 우선 점검

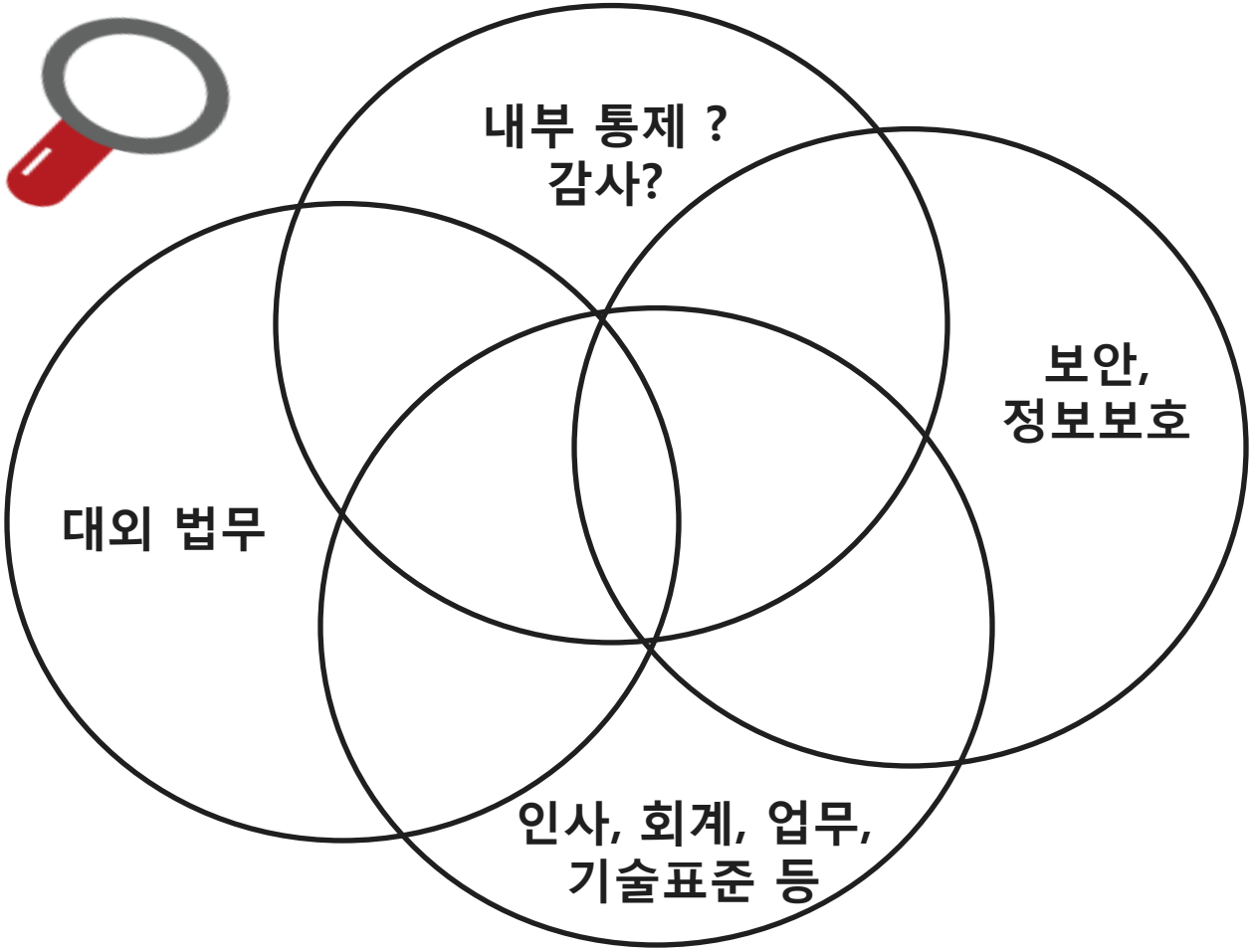
상세내용

정보보호 내부통제제도 실효성 강화

- 금융회사의 자체 보안 이행 점검 프로세스를 강화

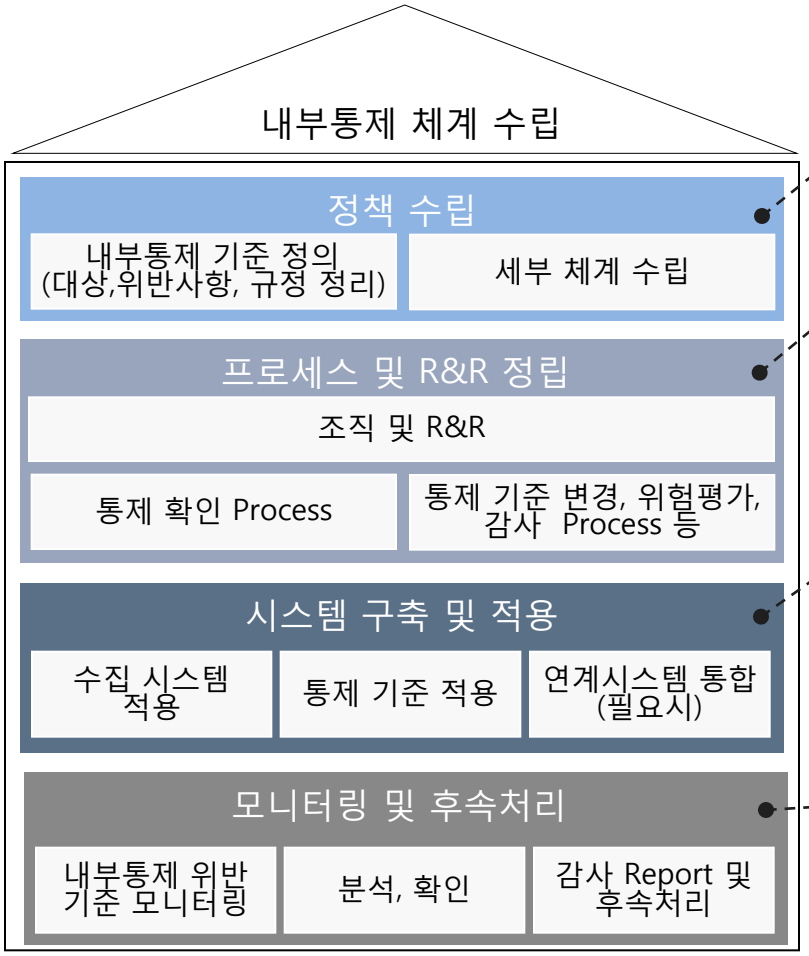
- 금감원은 보안관련 법규정 준수 여부를 철저히 검사, 미준수 시 엄중 제재

우리의 내부 통제는?



효과적인 프로세스? 고려사항은?

내부통제 Framework



내부통제 강화 방안

정책수립(체계정립)

- 내부통제 기준 정의 (내부통제 대상 분류 필요)
- 세부 분류체계 (범위 선정)

프로세스 및 R&R 정립

- 조직, 내부통제 의사결정 협의체 및 R&R 정의
- 통제 확인 Process
- 통제 기준 변경 Process, 위험평가 Process
- 감사 Process 등

시스템 구축 및 적용

- 통제 기준을 수집할 수 있는 시스템 적용
  (필요시 솔루션 도입)
  - 내부 통제 기준에 정의된 사항을 수집할 수 있는 대상
    (자동화 시스템으로 관리로 효율성 증대)
- 다양한 시스템을 통합, 연계 (필요시)

모니터링 및 감사

- 내부통제 위반 기준을 모니터링
- 로그 분석, 위반 사실 확인
- 감사 Report 및 위반 시 처리 규정에 따른 후속 처리

효과적인 프로세스? 고려사항은?

Q1. 내부통제 **범위 및 기준**은?

Q2. 내부통제 **담당 조직**은?

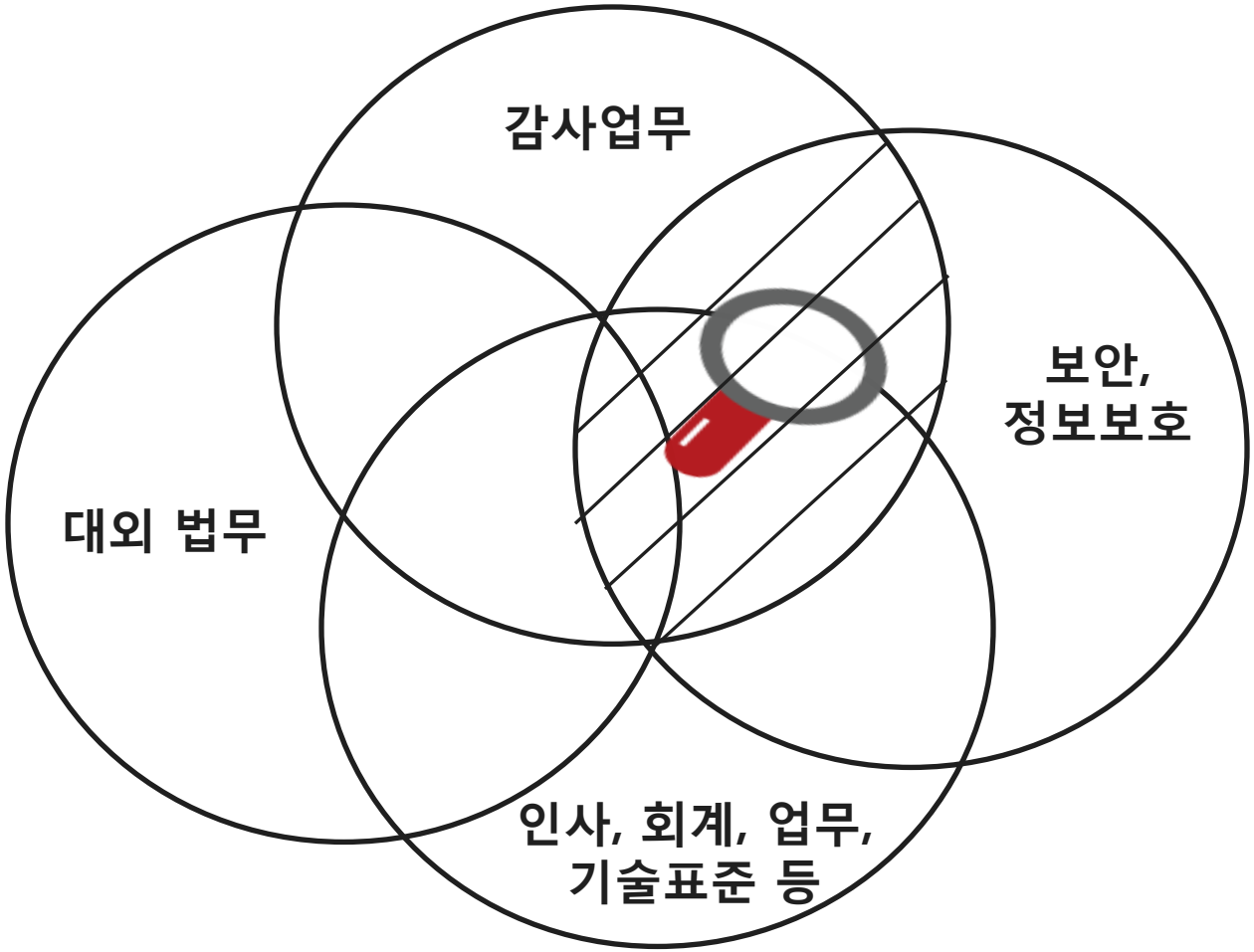
Q3. 내부통제 관련 **정보 수집**은?

Q4. 내부통제 **위반 적발 방법**은?

Q5. 적발 이후 **후속 처리**는?

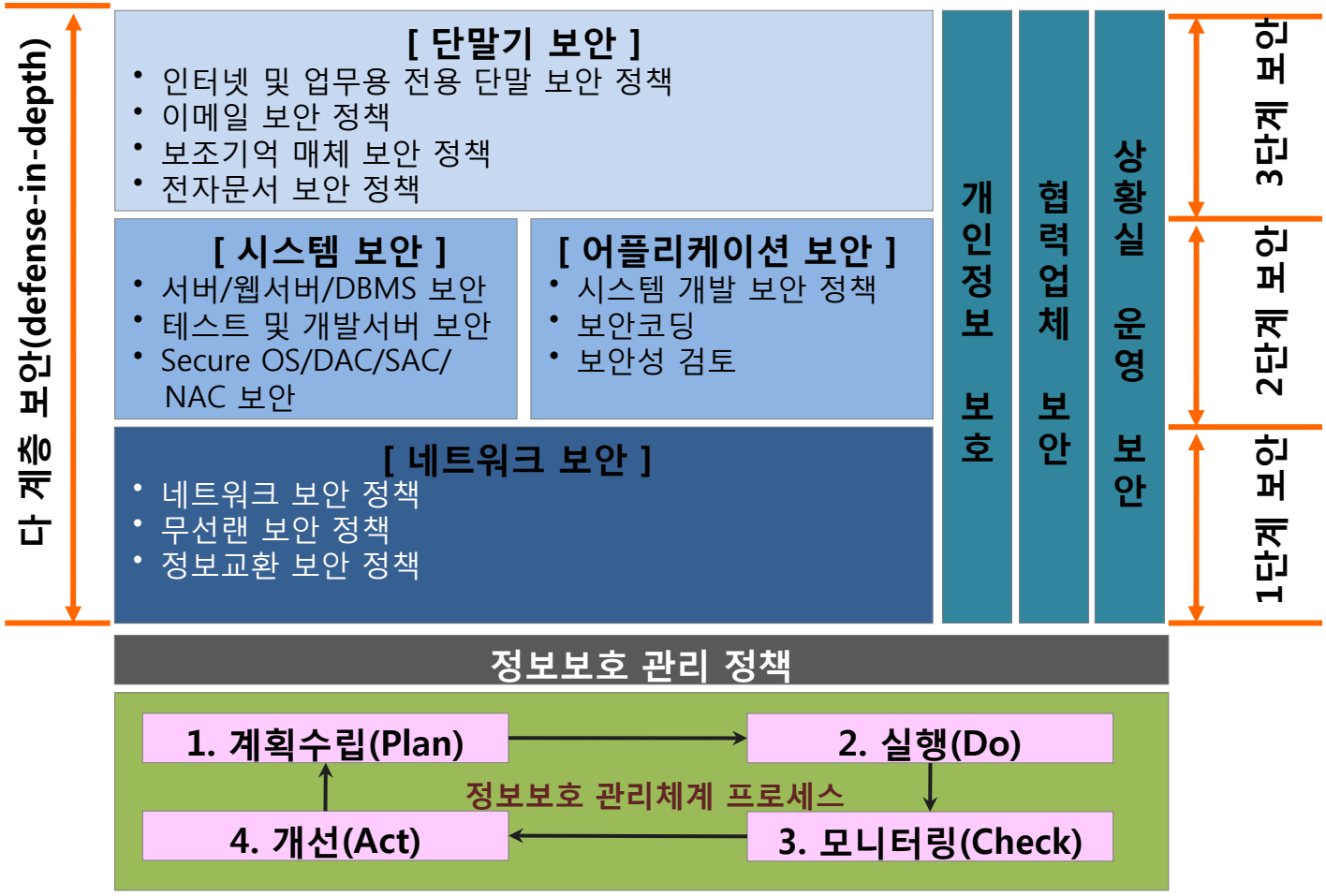
효과적인 프로세스? 고려사항은?

Q1-1. 범위 : 정보보호 관련 통제만



효과적인 프로세스? 고려사항은?

Q1-2. 기준 : 정보보호 정책 => 재수립



정보보호 관점의 내부통제 (안)

Q1-2. 기준 : 정보보호 정책 => 재수립

EXAMPLE

인터넷 PC	o 인터넷PC에 업무 자료 및 개인정보 자료 저장 금지 o 외주 인터넷PC 허용 최소화(업무상 불가피한 경우만 허용) - 현재 546대 허용 ⇒ 약 50대 이하로 제한 (先 차단 後 신청) o 상용 메신저, 웹하드 등 접근 금지	
	* 당사 보안솔루션을 우회하여 접속하는 경우 인터넷 차단	
보안 USB	DRM 권한 통제	o 관리자(팀장) 外 문서담당자 1명 이내 o 해제 후 DRM 再 적용 또는 삭제
	외주직원의 DRM 해제	o 당사 관리자 승인 및 통제 o 도급 직원 → 도급 PL/PM → 당사 관리자 o 도급업체 자체문서는 도급업체 별도 망에서 관리
	외부반출 기간, 파일복사권한 기간	o 日단위로 제한(~24시)
	* DRM 해제 파일복사권한 승인 후 복사된 파일이 꼭 필요한 자료만 보안USB에 저장되었는지 확인(관리자 필수) : 사용 후 삭제 * 보안 USB 보안정책 위반 시 보안 USB 회수 조치	

정보보호 관점의 내부통제 (안)

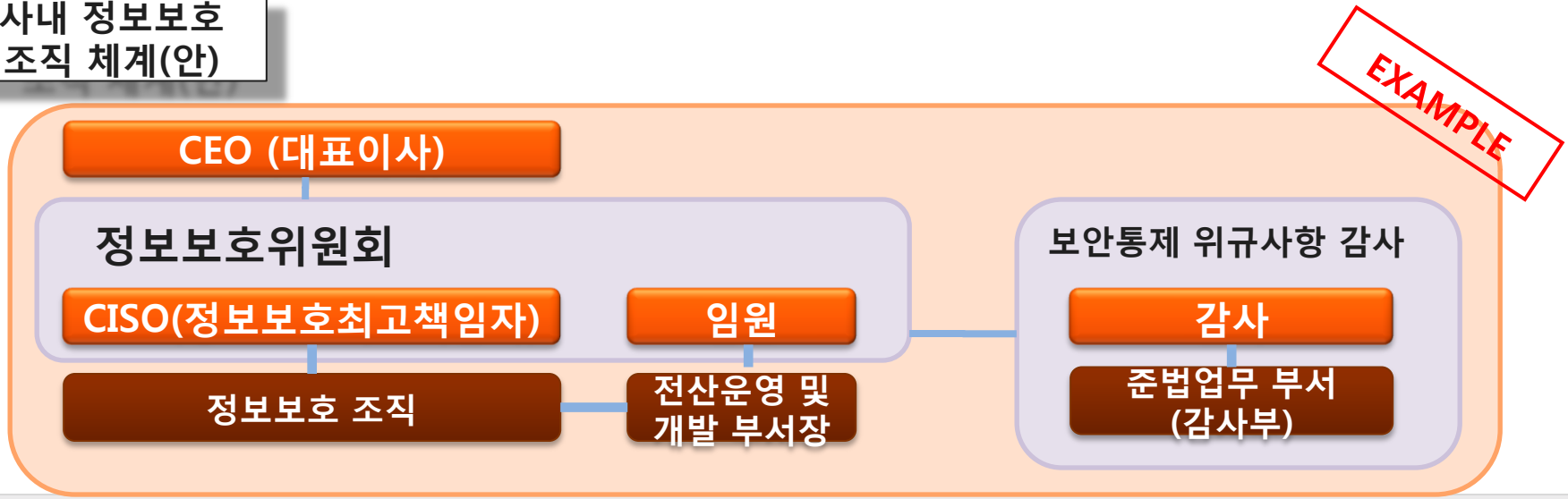
Q2. 조직 : 정보보호 위원회

배경

- **전자금융감독규정 제 8조의 2(정보보호 위원회 운영) 의무화 ('13. 12. 3 개정)** ※ 정보보호위원회 신설 필요
- **금융회사 고객 정보 유출 재발 방지 대책 (금융위, '14. 1. 22)**
  - 고객 정보 관리에 대한 CEO/CISO 역할 및 책임 강화
  - 자체 보안 통제 프로세스 강화 요청
    - . 보안규정 구체화 CEO/CISO 승인, 매월 정기적으로 자체 보안관리실태 점검
    - . 보안관리실태 점검 결과 보고 및 점검결과 이행 계획 CEO 보고
    - . 금감원 검사시 이행실태 점검(금융본부 대상)→**미준수시 엄중 제재**

사내 정보보호 조직 체계(안)

EXAMPLE



정보보호 관점의 내부통제 (안)

Q3. 수집

프로세스화 vs. 시스템화

주요 프로세스

- 보안성 검토 프로세스
- 개발 보안 프로세스
- 퇴직자 보안 대책 프로세스
- 외부관리 보안 프로세스

정보보호 관점의 내부통제 (안)

Q3. 수집

- **정보처리시스템의 안전성 확보는 어떻게…?**

➢ **사후 점검 및 개선도 필요**

EXAMPLE

- 홈페이지 모의해킹
- 취약점 분석 평가
- 개선 조치 및 이행 점검 등

그러나, 근본적으로는 … 건물의 안전성 확보를 설계, 시공 단계부터 안전성을 확보하는 것 처럼

➢ **계획, 설계, 코딩 단계부터 안전성을 확보하여 개발하는 것이 중요 (개발 보안성 검토)**

EXAMPLE

- 개발보안성검토, 개발보안대책 수립
- 「보안 기능 설계 표준(안)」 준수
- 「개발보안 코딩가이드라인」 준수
- 소스코드 보안성 검증 및 개선 … 등등

정보보호 관점의 내부통제 (안)

Q3. 수집 : 프로세스 산출물, 시스템

- 프로세스 결과물
  * 수동 점검 결과
  * 증적자료, 기록물 등

- 시스템 로그

정보보호 관점의 내부통제 (안)

Q3. 수집

시스템 로그 수집 안)

- 단말기 통제시스템 (구축 아이디어)

EXAMPLE

1. 단말기 보안 관련 내부통제를 통합 연계 시스템과 연동, 개발방안 검토
2. 내부 보안 솔루션에서 추출할 수 있는 정보를 이용하여 관리 요건으로 연계 하는 방안을 연구
3. 통합솔루션의 도입 또는 기존 솔루션에이전트의 로그수집 또는 연동을 통한 구현방안 마련
4. 수집 가능성과 개발의 난이도등 고려하여 상, 중, 하로 실현 가능성 타진
5. 우선 '상(上')인 경우에 해당하는 내부통제 솔루션 업체와 상의하여 개발 계획 수립 및 실현 가능한 일부 기능부터 파일럿 구축

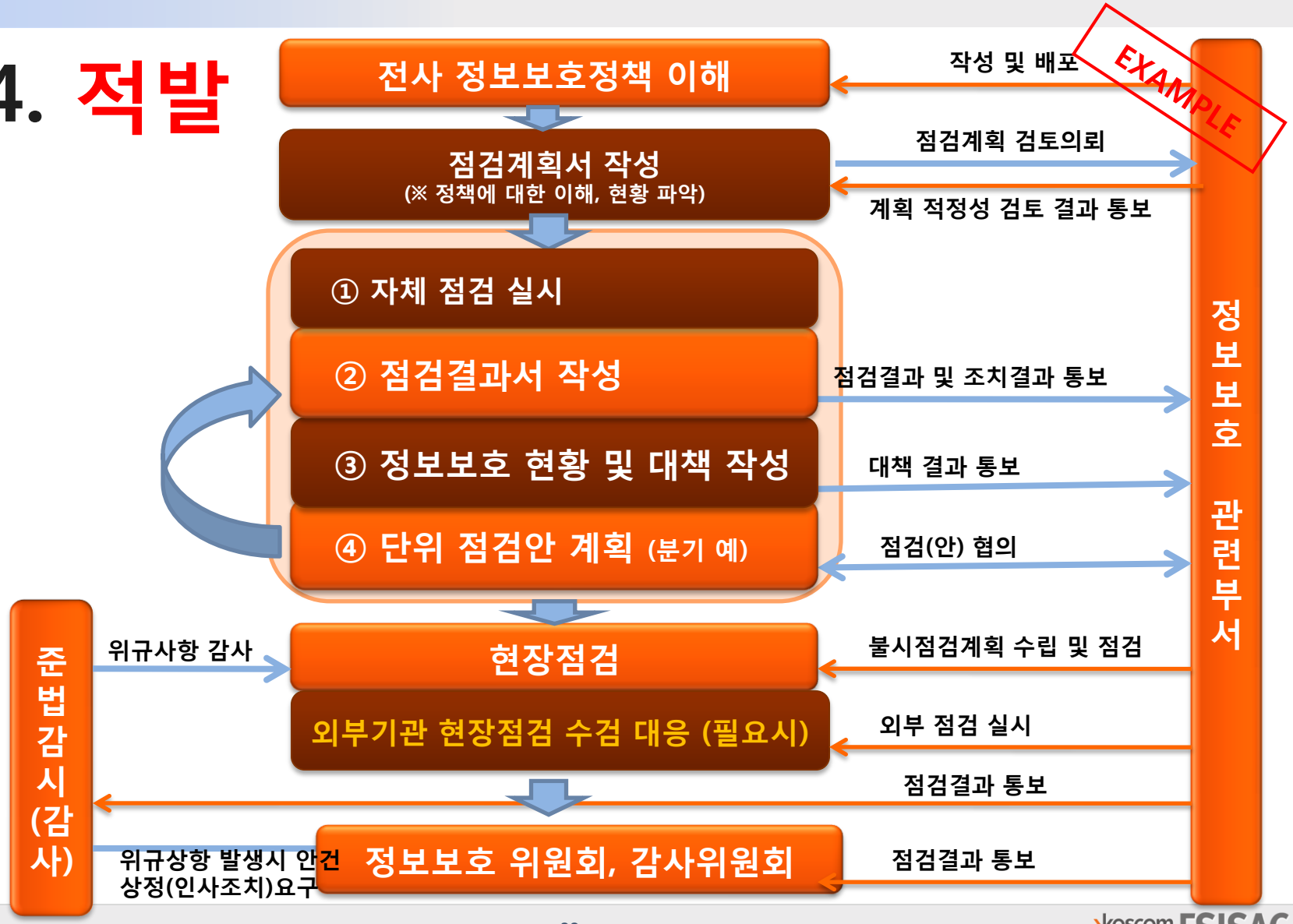
정보보호 관점의 내부통제 (안)

EXAMPLE

내부통제분류	통제 항목	
1.업무PC	1.1	단말기 비밀번호 월1회 변경 여부
	1.2	필수 S/W 설치 여부
	1.3	휴대기기 연결은 보안USB 만 사용하는지의 여부
	1.4	업무 PC 의 인터넷 PC 전환 및 혼용 여부
	1.5	해당 단말기에 비인가된 Network 연결 금지
	1.6	단말기의 원격연결 금지
	1.7	최신 패치 여부
	1.8	퇴직등에 의한 PC사용 종료 시 복구안되도록 물리포맷 여부
	1.9	허가된 폴더 외 공유폴더 금지
2.인터넷PC	2.1	업무관련자료 외 불법자료 금지, 개인자료 저장(소유권자의 허가 없이 취득 금지)
	2.2	USB 사용 후 즉시 분리 하는 지의 여부
	2.3	악성코드, 해킹방지 SW 설치 여부, 비인가 SW 사용 금지
	2.4	업무자료 삭제 시 복구 불가능 하도록 처리 하는 지의 여부
	2.5	불법행위 3회 이상 반복 시 영구 차단
3.회의실 PC	3.1	ADSL 등 외부네트워크망 연결 금지
	3.2	자료보관 금지
	3.3	백신, 보안USB 사용 필수
	3.4	1주 1회이상 업데이트
4.개발용PC	4.1	개발용 PC사용 종료 후 포맷 여부
	4.2	인터넷 금지
	4.3	무선랜 금지
	4.4	운영서버 직접 연결 금지
	4.5	백신, 보안USB 사용 필수
	4.6	주기적 업데이트 여부
	4.7	개인정보 실데이트 취급 금지(저장, 사용 금지)

정보보호 관점에서만 내부통제 (안)

Q4. 적발



정보보호 관점에서만 내부통제 (안)

Q5. 후속처리 : 위원회, 기술적 통제

- 내부 위원회
  * 내부 규정에 따른 규정 위반자 인사 조치
- 기술적 통제
  * 유사 사고가 탐지 될 수 있는 탐지 체계
  * RISK에 따라 시도 자체가 되지 않도록 근본적 기술적 차단
- 교육 : 유사 사고 방지를 위한 교육

고려 사항

←실제 적용된 감옥

디지털 파놉티콘
빅데이터
빅브라더

투명한 사회

시놉티콘은?

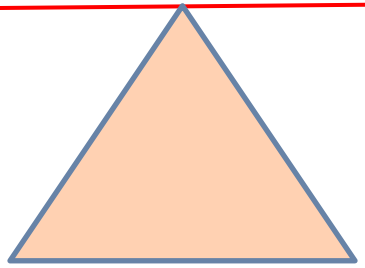
고려사항

범위?

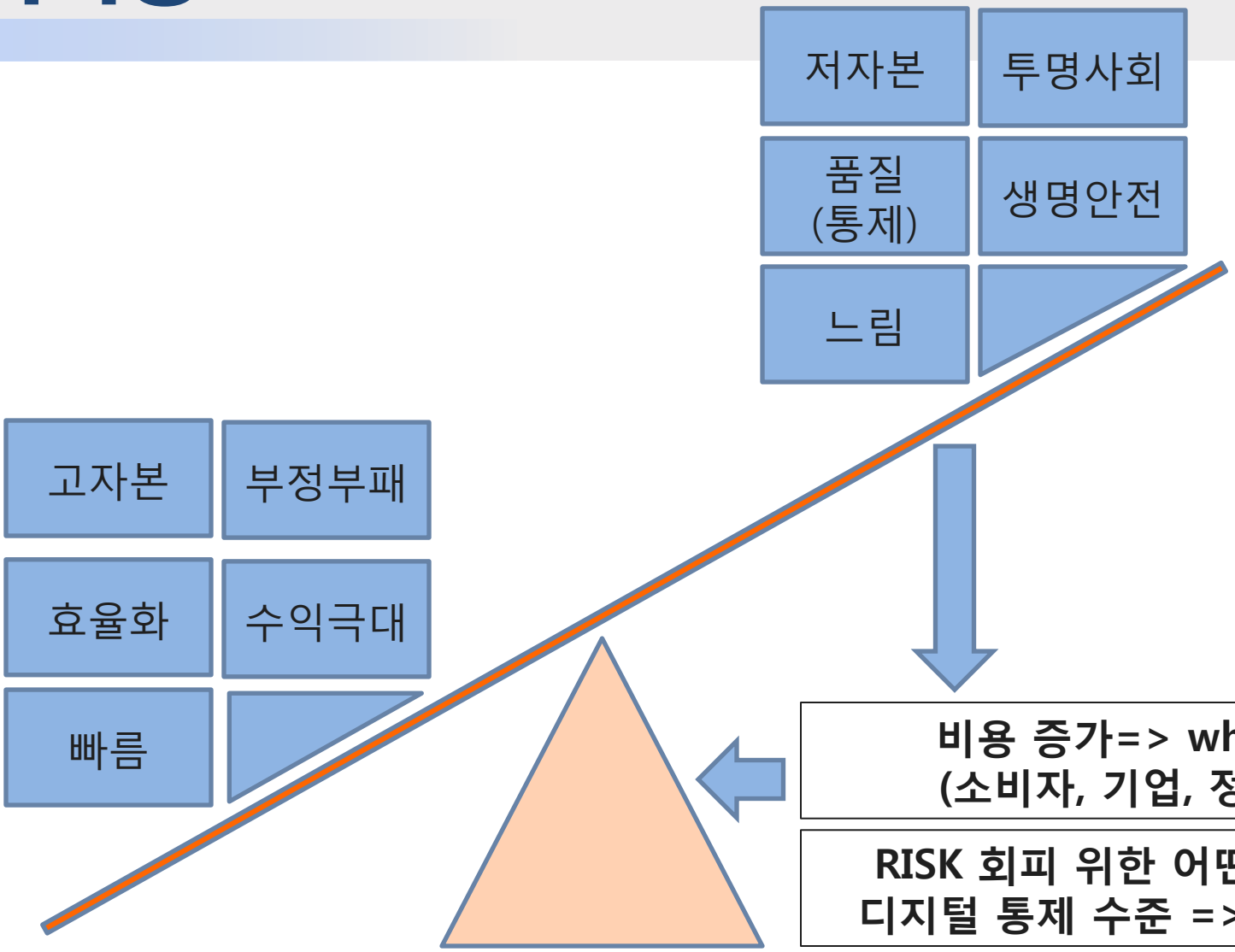
조직?

비용?

경영/기업 철학? 국가정책?



고려사항


저자본
투명사회
품질
(통제)
생명안전
느림
고자본
부정부패
효율화
수익극대
빠름
비용 증가=> who??
(소비자, 기업, 정부)
RISK 회피 위한 어떤 노력?
디지털 통제 수준 => 법규화


작은 움직임이
큰 기적을

감사합니다

자본시장 IT 파트너

koscom