코로나 19 시대
지속경영을 위한
기업 내부리스크 관리 전략

2020.12.11

이병철
한국부정부패방지연구원 원장
경기대학교 명예교수
010-3751-7000
2gyosu@naver.com

한국기업경영학회
Korea Corporation Management Association

말씀드릴 순서

- COVID 19 이후 지속 경영 을 위한 전략 제시 – 전세계 컨설턴트들
- ICT System은 Black Box
- 내부통제 수준이 바로 내부리스크 수준
- 기업이 준비해야 할 7가지 내부리스크 관리전략 : 7 DO strategies

1st DO : 내부리스크 발견 카나리아를 보호하고 칭찬해라 .

2nd DO : 경영자(의사결정자)는 ICT 기술 자체에 대하여 충분히 이해하라.

3rd DO : System은 논리적 설계 후 설계를 100% 따르는 코딩을 하게 하라.

4th DO : System에 내부통제 모듈(embedded internal control module)을 내장하라.

5th DO : System 유지 관리 조직 및 업무에 내부통제구조를 적용하라.

6th DO : 내부 감사계획은 System에 대한 내부통제 진단 결과를 근거로 수립하라.

7th DO : 최신 ICT 기술적 용어에 현혹되지 말고 내부를 들여다보아라.

8th Do : ICT 재난대비계획이 SHOW가 아닌지 점검하라.

COVID 19 이후 지속 경영 을 위한 전략 제시 - 전세계 컨설턴트들

COVID-19: Impacts on Business Strategy | Accenture. www.accenture.com › Accenture Strategy › COVID-19

Accenture shares some our best thinking with CEO's on how to maximize your **business strategy** right now during the time of the **COVID-19** pandemic.

COVID-19: Strategies for the new normal | McKinsey. www.mckinsey.com › business-functions › our-insights

2020. 4. 27. — Two McKinsey experts offer their perspectives on how **businesses** can develop **business strategies** for the new normal after the COVID0-**19** ...

Reset Your Business Strategy in COVID-19 Recovery – Gartner. www.gartner.com › smarterwithgartner › reset-your-bu...

2020. 6. 3. — As the phases of the **COVID-19** pandemic progress, invest your lessons learned back into the enterprise to reset **strategy** and build resilience.

COVID-19: Post crisis strategies for growth | Strategy&. www.strategyand.pwc.com › covid-19

Responding to the **business** impacts of coronavirus (**COVID-19**). How can you prepare your organization to respond?

Business Strategies for COVID-19 and After | ThoughtWorks. www.thoughtworks.com › business-strategies-to-comba...

Re-align your **business strategy** to build resilience and respond effectively to the impact of **COVID-19**. Navigate the crisis with ThoughtWorks Advisory Services.

COVID-19 - Strategy+Business. www.strategy-business.com › covid-19

Dillip Rajakarier, group CEO of Minor International, on why strong cash management, weekly planning, and a focus on local markets have been key to ...

How is COVID-19 reshaping the role of corporate ... – Deloitte. www2.deloitte.com › Deloitte › process-and-operations

services running, it is imperative for **business** leaders, particularly senior **strategy** executives, to reflect on the lasting implications of **COVID-**

기업환경에 대응한 기업 체질 변화 및 전략적 방향을 제시

컨설턴트들이 빈번하게 사용한 단어들

과거에는 이랬는데.....

Innovation, quantum up, reengineering, downsizing, blue ocean

❖ Agile, resilience, change,

- 재택근무, 화상회의, e-commerce, online order, 은행 점포 감소, 등등
- 신제품 도입 속도 증가(2021년 모델을 2020년 6월에 발표, s20 판매 하자 마자 s21 시제품 공개 등)

기업의 환경 적응을 돕기 위하여 수단

ICT 업무 활용을 강제, 가속화

❖ ICT 기술과 기업의 대응이 앞서거니 뒤서거니 하며 변화해 감

- cloud, big data, AI, blockchain, object
- On-line, real-time, mobile,

❖ **COVID 19의 영향**

- 기업의 업무 환경 변화에 대응하기 위한 **ICT 기술 도입 및 활용을 촉진하는 촉진자 역할**
- COVID 19로 인하여 국가, 사회, 기업의 ICT를 활용한 업무 비중이 급속히 증가되고 기업 성과에 미치는 ICT의 중요성이 폭발적으로 증가함.

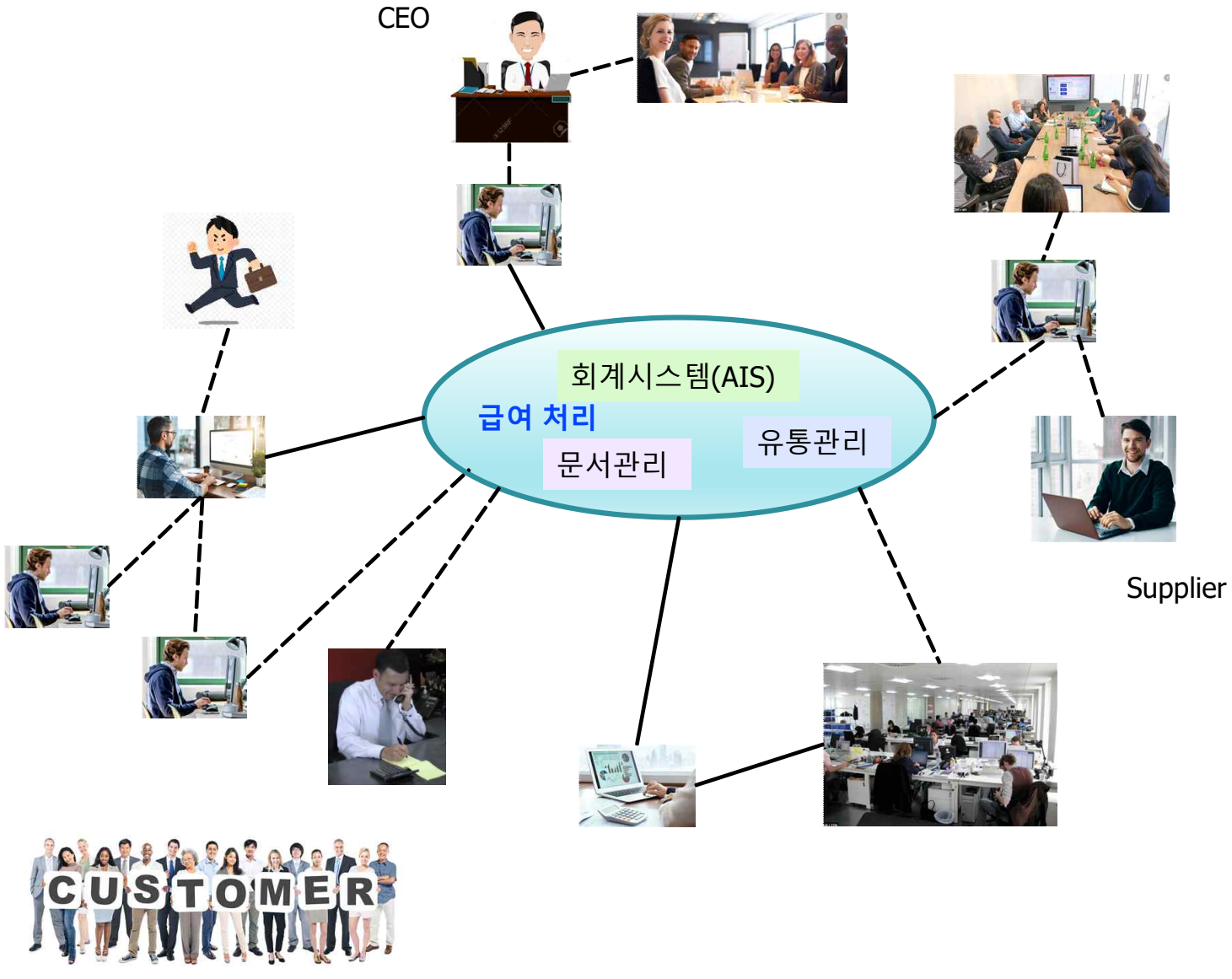
❖ **ICT의 의존도가 높아질수록 ICT로 인한 내부리스크가 증가하고 있음.**

❖ **기업은 외부 침입을 방지하기 위한 보안(security)에 집중하지만 조사에 의하면 부정오류의 90%는 내부에서 발생**

2020년대 ICT System은 Black Box

1960년경 이전의 기업 경영과 업무 처리 모습

1970년-1980년경 기업 정보화 모습



1990년-2010년경 기업정보화 모습

CEO

Management information system

Electronic document approval system

Enterprise resource planning system

Real time processing

Batch processing

CRM

Intra SMS

SCM

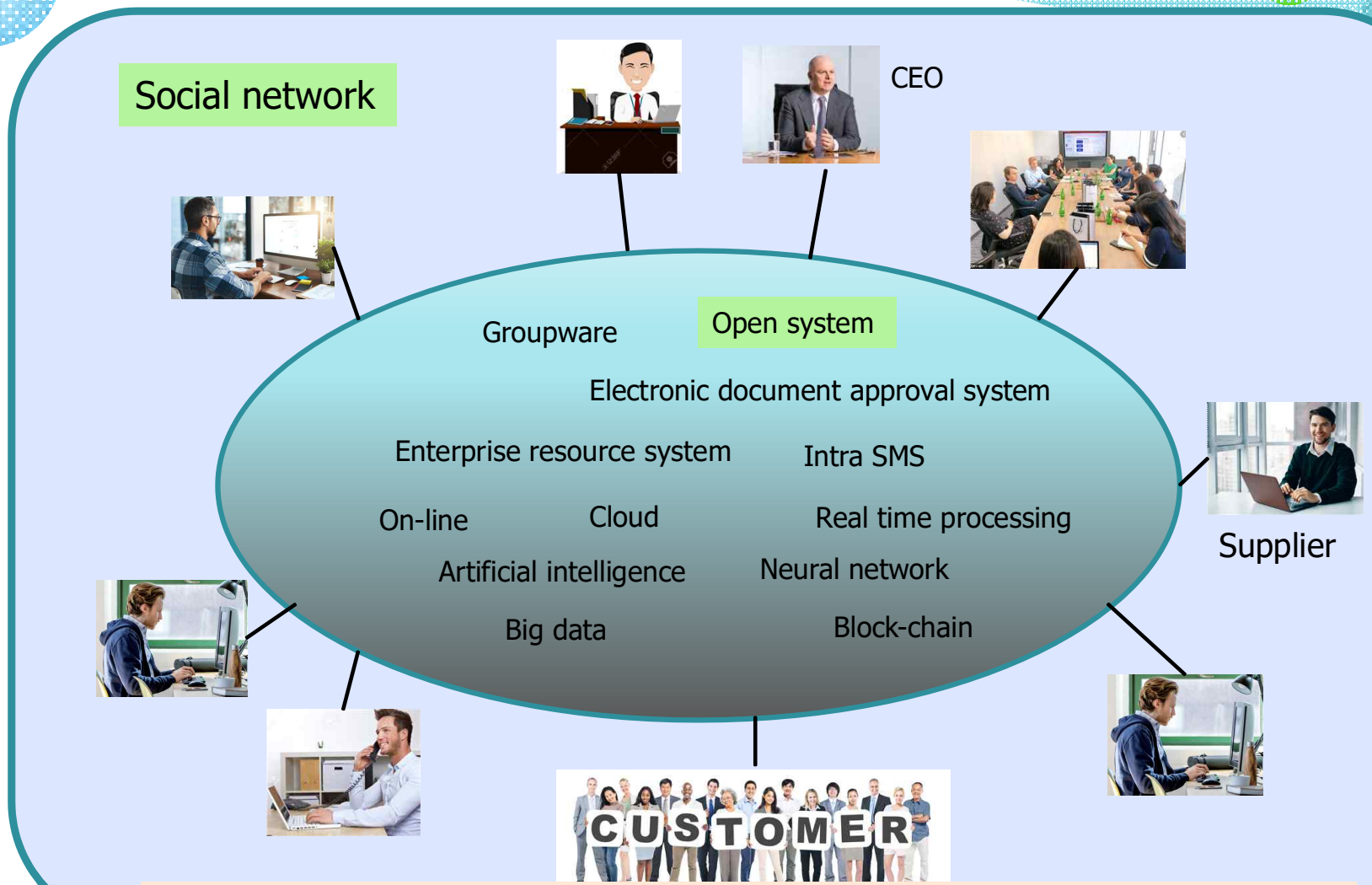
On-line

Data warehouse

Data mart

Supplier

2010년경 이후의 기업 정보화 모습



❖ 기업의 ICT에 의한 업무처리 비중이 점차 늘고 있음

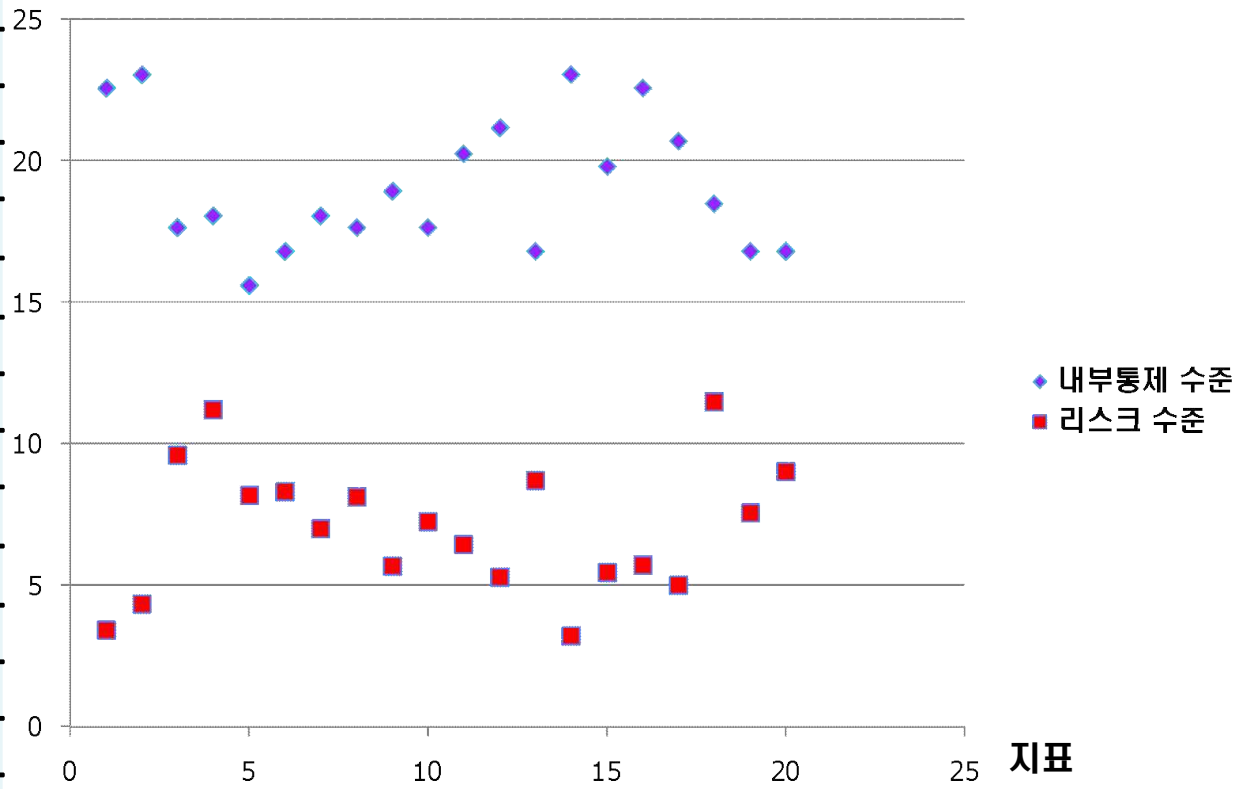
❖ ICT 투자를 늘리고 인력을 감축하는 방향으로 이행

❖ **경영자와 기업 구성원들은 기업의 ICT Black Box에 대하여 어느 정도 파악하고 계십니까 ?**

내부통제 수준과 내부리스크 수준의 관계

(00금융공기업 Blind survey 결과)

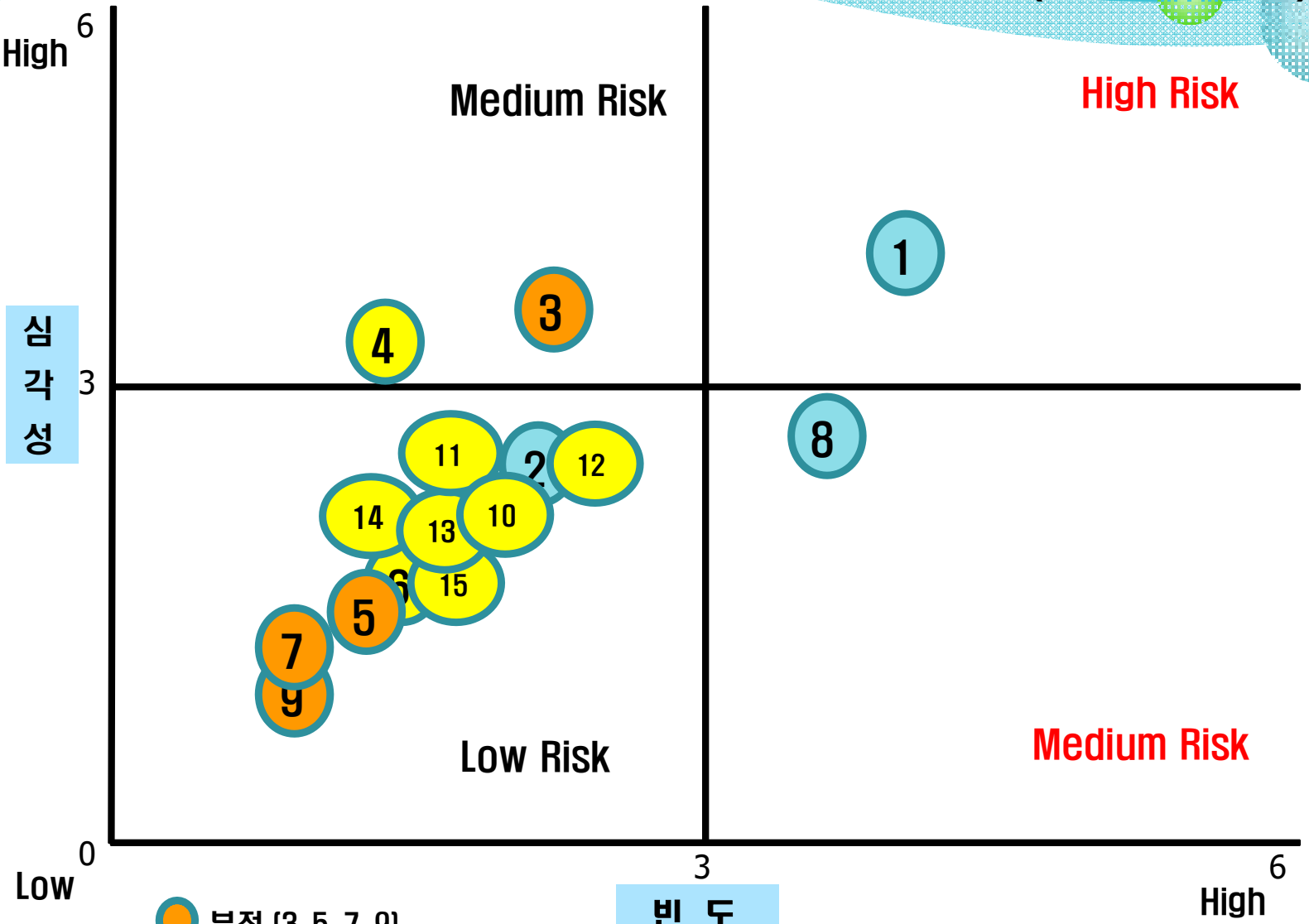
지표	내부통제 수준	내부리스크 수준
1	22.56	3.40
2	23.04	4.32
3	17.64	9.60
4	18.06	11.20
5	15.60	8.16
6	16.81	8.32
7	18.06	7.00
8	17.64	8.10
9	18.92	5.67
10	17.64	7.25
11	20.25	6.44
12	21.16	5.28
13	16.81	8.70
14	23.04	3.20
15	19.80	5.46
16	22.56	5.70
17	20.70	5.00
18	18.49	11.47
19	16.81	7.56
20	16.81	9.00



내부리스크 = 내부통제 취약점

기업의 내부 리스크는 어디에 있는가 ?

(OO금융공기업 사례)



- 부정 (3, 5, 7, 9)
- 재량행위 (1, 2, 8)
- 임무해태, 오류 (4, 6, 10, 11, 12, 13, 14, 15)

❖ ISO 37001 Anti-bribery mgmt. sys. 에 대하여 생각해 볼 점

Post COVID19 정보화 촉진에 대비하여

기업이 준비해야 할 8가지 내부리스크 관리 전략

: 8가지의 DO

1st DO :

내부리스크 발견 카나리아를 보호하고 칭찬해라 .

❖ 대부분 조직 구성원들은 내부리스크 **취약점을 감추기에 급급함**

❖ 부서는 부서의 이익을 위하여, 사장은 자신의 재임을 위하여.

- 00공단의 사례 - 발견 감사실장 즉시 명퇴, 과장 특별 승진 타부서로

❖ **내부고발자 제도는** 내부리스크가 현실로 발생하여 사건이 된 경우에 적용

❖ **리스크를 근본적으로 예방하기 위한 제도나 장치는 없음.**

어느 광역 자치단체 지방세 시스템 관련

❖ 담당자의 고백 : **지방세 합계액이** 이리 이리해서 나온 것, 저리저리해서 나온 것, 요리 요리해서 나온 것 **다 달라요.**

어느 00공단 지급 시스템 관련

❖ 담당자 인터뷰 : 지급 결정 후 내용을 정보지원실 통해 00은행에 이체지시서를 보낸 후 결과를 재무지원실에서 받는데, **지급결정액과 이체금액이 일치하지 않아요.**

네덜란드 소년의 동상

2nd DO :

경영자(의사결정자)는 ICT 기술 자체에 대하여 충분히 이해하라.

❖ ICT 기술을 이해 못하는 경영자는 **바지 사장**

- 기술자는 전사적 목표가 아닌 부문 목표를 위한 의사결정
- 00공립의료원의 사례 - 전산직원이 왜 이렇게 많아야 하지 ??

라. 직원에 관한 사항

전산 **용역 업체** 직원은 포함되지 않은 숫자임

※ 4.( )는 [redacted]병원 파견인력임

① 임.직원 정현원 현황 (단위:명)

구 분			계	① 상임이사	② 의료직	③ 보건직	④ 사무직	⑤ 기술(능)직	⑥ 잡급직
전년도말 인원		정원	1,144	1	776	129	90	148	-
		현원	1,366	1	843	145	102	275	-
기간 중 증감 (1월1일기준)	증	정원	102	-	21	1	2	78	-
		현원	75	-	26	19	6	24	-
	감	정원	-	-	-	-	-	-	-
		현원	2	1	1	-	1	- 1	-
당년도말 인원		정원	1,246	1	797	130	92	226	-
		현원	1,439 (41)	-	868 (29)	164 (3)	107 (7)	300 (2)	-

❖ 자동차 수리의 예

개스켓도 바꾸어야 하고 펌프도 수리해야 겠는데요. 고치지 않으면 큰일나요.

그래요 ? 그럼 수리해주세요.

그런데 개스켓이 뭐지? 펌프는 어디 있는 뭘 말하는 거야?

- ❖ why Oracle DB? why UNIX? why RDB? why standalone Server?
- ❖ 코딩 언어는 어떤 것이어야 하나? java, javascript, ,net, C++, C#, Python 등
- ❖ BPE(Business Process Engineering)과 BPR(Business Process Re-engineering) 차이
- ❖ 어느 금융공기업의 **내부품의서와 지출결의서 작성** 순서 사례
  - ▪ 지출결의서를 작성한 후 내부품의서를 작성 (왜? 시스템이 그렇게 되어 있대요.)

3rd DO :

System은 논리적 설계(문서화) 후 설계를 100% 따르는 코딩을 하게 하라.

❖ **Documentation의 중요성**

- Black Box 보이지 않는 것을 들여다볼 수 있는 것

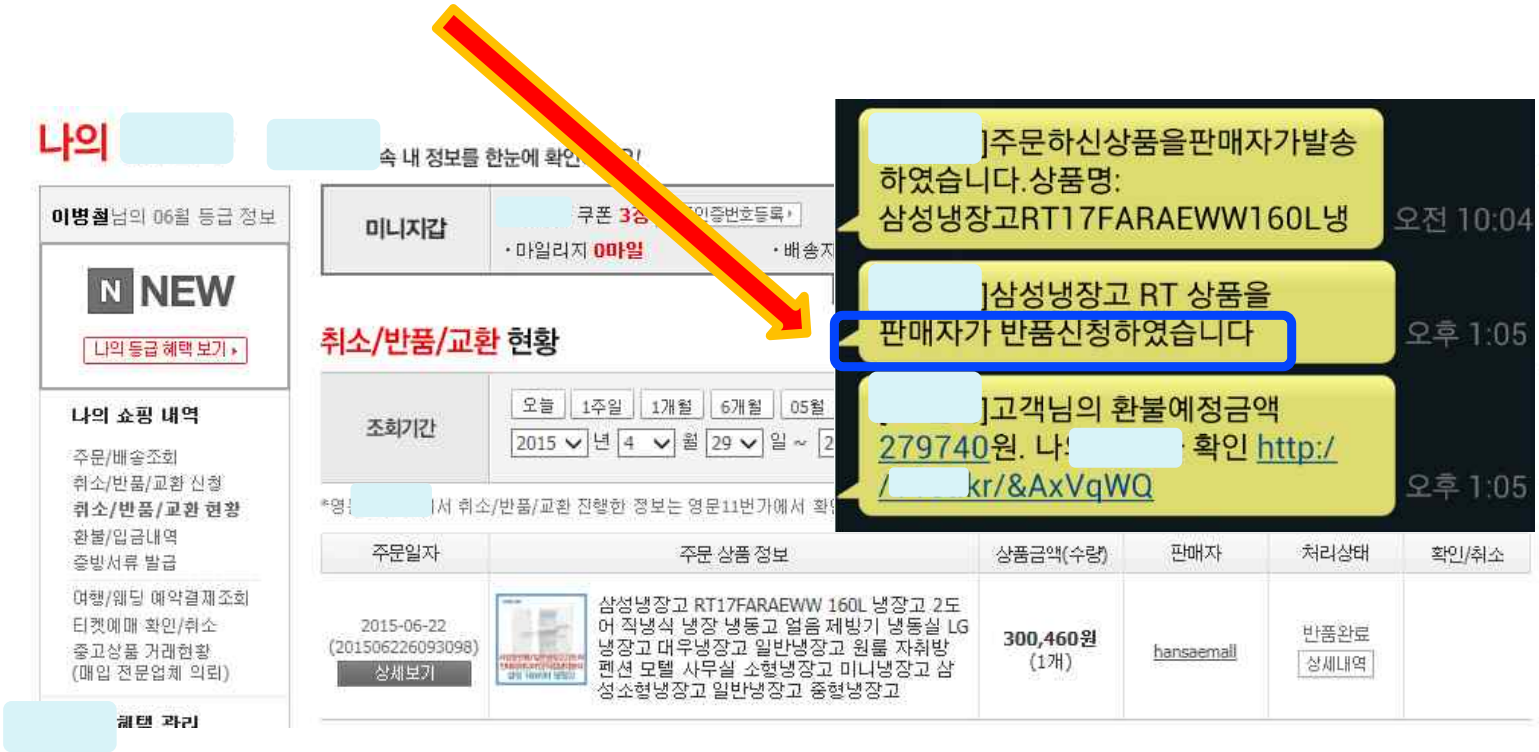
❖ 건물 스케치와 설계도를 이용한 단독 주택과 20층 건물의 건축 비유

이 스케치(조감도)를 보면서 주택(건물)을 지어보라고 ?

작은 주택 정도라면 몰라도, 빌딩을 지으려면 상세 설계가 있어야지

❖ 대한민국은 S/W 개발 후진국

[사례 3-1] 이게 맞는 건가요 ????



- 시스템 설계도에 **반품을 구매자가 아닌 판매자가 하도록** 되어 있었을까요 ?
- 시스템이 왜 설계도대로 코딩되지 않았을까요 ?
- 문제 제기된 후 시스템을 수정하였다면 **설계도부터 수정하고** 그에 따라 코드 수정하였나요?

정보시스템 개발 구축 과정의 현실

정상적 시스템 구축

사용자 요구분석

정보화 계획(ISP) 업무재설계(BPR) → 업무분석 재설계 - 설계도 작성 → 설계도만 보고 Coding → 부정오류 검사목적 현장시험적용 → 보완 후 가동

CASE 도구에 의한 분석 및 설계 ⟹ 프로그램 자동 생성

프로그램 설계도(window layout, data table, job description, specification)와 프로그램 100% 일치

우리나라 시스템 구축 일반적 방법

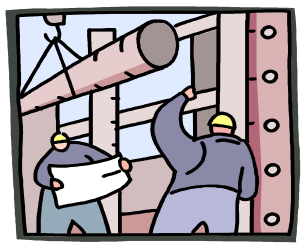
사용자 요구분석

추상적 정보화 계획(AISP) 업무설계(BPE) / 업무 분석 설계 - 시스템 스케치 / 스케치만 보고 원형(Prototype) 방식 Coding → 대폭 수정 위한 현장 시험 적용 → 여러 차례 대폭 수정으로 누더기가 된 후 가동

프로그래머가 일관 수행

고도화 명분 누더기 코드수정

프로그램 설계도 없고 설계 스케치와 프로그램 불일치



대규모 건축물을 현장 시공기사가 스케치만 보고 공사를 진행

- ❖ 설계와 시공(코딩)은 분리되어야 함
- ❖ 설계도는 건축물(프로그램)과 함께 유지되어야 함
- ❖ 반드시 내부통제 전문가 참여

몸에 맞지 않아 뜯어고치기 반복한 누더기 옷에 비유

설계도 없이 코딩 위주로 시스템을 개발할 때 발생하는 문제

- ❖ 시스템 개발 실패보다 무서운 건 **잘못 구축된** ICT 시스템
- ❖ 기업은 **시스템 설계에** 더 많은 정성과 투자가 필요함.

[사례 3-2] 설계가 미흡한 채 코딩 중심으로 개발하여 실패한 것으로 보이는 사례

[아주경제] 00사, 전산시스템 직원들 불만 고조… 'BIT 실패 후유증' 앓는다 (2016.4.7)

- 00 회장이 성공적이라 자평했던 새 영업 전산망 '코스(KOS)'가 최근 시스템 장애를 일으키면서 사내에서 불만의 목소리가 커지고 있다.
- 과거 00 회장 시절 **1조원을 투입해 개발했다가** 00를 적자기업으로 만들었다는 오명을 쓴 'BIT(Business & Information system Transformation)프로젝트'의 악연이 또다시 이번 사태를 통해 00 직원들에게 치명적인 후유증을 입히지 않을까 하는 우려에서다.
- 더구나 지난달 25일 주주총회를 통해 BIT 전산 개발을 총괄했던 00이사가 사외이사 겸 감사위원으로 재선임된 상황이라 BIT 실패를 겪은 00직원들의 볼멘소리가 터져 나온다.

- ▪ 00는 BIT 사업에 인도 프로그래머 투입
- ▪ 기획은 Accenture
- ▪ **설계는 ?**

비교 사례

❖ **40년 전 인터넷이 보급되기 이전 미국의 어느 S/W 개발 업체 사례**

- 설계만하고 설계도를 모듈로 쪼개어 인도 프로그래머에 코딩 위탁
- 코딩 모듈을 조립하여 S/W 완성

❖ 삼성전자의 바다, 타이젠 사례

❖ 현대차 자율주행차 미국에서 개발 중

❖ 한국 10년여 전 **설계와 코딩 분리 발주** 정책 시도의 실패

❖ 대부분의 경영자는 시스템 스케치를 시스템 설계도라 착각

❖ 코딩 중심 구축의 편법 : 구축 후 **고도화 후속사업**(땜질, 보완)

❖ Documentation : logical design -> physical design -> coding -> test

❖ 제대로 된 Documentation은 개발 기간과 투입인력 등 **Cost를 획기적으로 절감**

[사례 3-3] 설계 없이 구축된 시스템 문제 - 업무분장과 접근통제의 현실

00관리시스템의 하위 계약관리 시스템 권한 사례

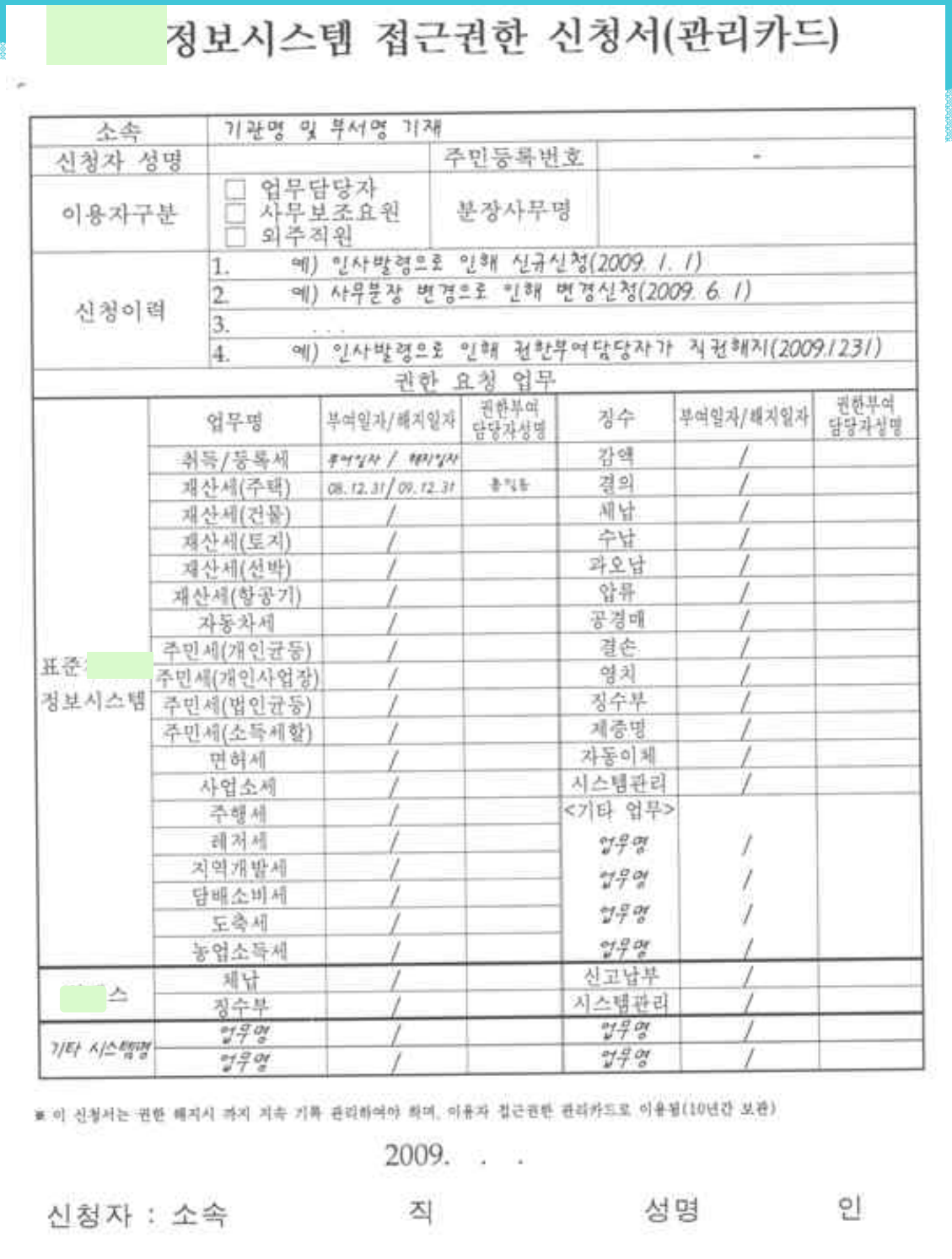
화면구분	화 면 명	계약담당자 (CM002)	계약담당자 (CM003)	검수담당자 (CM004)	계약대장 조회 (CM005)	총괄계약 담당자 (CM999)
계약요청관리	계약요청관리	○	○			
	G2B수신문서조회	○	○			
입찰및낙찰관리	입찰공고 조회	○	○		○	
	최종낙찰자목록	○	○		○	
계약대장관리	계약대장 등록	○	○			
	계약대장 조회	○	○		○	○
	총괄계약대장 등록	○	○			
	총괄계약대장 조회	○	○		○	○
	계약대장 출력	○	○			○
	계약대장 담당자수정	○	○			
	계약담당자위임관리	○	○			
	계약대장 수정	○	○			

❖ 시스템 접근 권한(access control) 설정은 각 담당자, 결재권자 등 시스템에 접근 권한을 가진 모든 사람들이 포함되어야 함

❖ 권한 설정은, read, write, delete 등으로 설정되어야 함.

설계 없이 구축된 시스템 사례 - Access Control 부재

- 말로는 정보가 중요하다고 하지만 정보를 관리하는 방법은 부실하기만 함
- Access Control은 각 담당자의 세부적인 업무(function)을 기준으로 하고 **read(조회), write(생산), restrict(통제)**로 구분되어야 함
- 이와 같이 정보에 대한 Access Control이 제대로 되지 못하는 원인은 시스템 **설계 부실에 있음**
- 아주 쉬운 예로 관리자는 담당자가 작성한 정보를 임의로 수정해서 안됨.
- 우측과 같은 관리카드에 의하면 포괄적이 권한을 받은 자 중 누가 정보에 손을 댓는지 transaction log를 추적하기 전에는 알 수 없음.



정보시스템 접근권한 신청서(관리카드)

소속	기관명 및 부서명 기재		
신청자 성명		주민등록번호	-
이용자구분	☐ 업무담당자 ☐ 사무보조요원 ☐ 외주직원	분장사무명	
신청이력	1. 예) 인사발령으로 인해 신규신청(2009. 1. 1)		
	2. 예) 사무분장 변경으로 인해 변경신청(2009. 6. 1)		
	3.		
	4. 예) 인사발령으로 인해 권한부여담당자가 직권해지(2009.12.31)		

권한 요청 업무

	업무명	부여일자/해지일자	권한부여 담당자성명	징수	부여일자/해지일자	권한부여 담당자성명
표준 정보시스템	취득/등록세	부여일자 / 해지일자		감액	/	
	재산세(주택)	08.12.31/09.12.31	홍길동	결의	/	
	재산세(건물)	/		세납	/	
	재산세(토지)	/		수납	/	
	재산세(선박)	/		과오납	/	
	재산세(항공기)	/		압류	/	
	자동차세	/		공경매	/	
	주민세(개인균등)	/		결손	/	
	주민세(개인사업장)	/		영치	/	
	주민세(법인균등)	/		징수부	/	
	주민세(소득세할)	/		체증명	/	
	면허세	/		자동이체	/	
	사업소세	/		시스템관리	/	
	주행세	/		<기타 업무>		
	레저세	/		업무명	/	
	지역개발세	/		업무명	/	
	담배소비세	/		업무명	/	
	도축세	/		업무명	/	
	농업소득세	/				
[illegible]스	체납	/		신고납부	/	
	징수부	/		시스템관리	/	
기타 시스템명	업무명	/		업무명	/	
	업무명	/		업무명	/	

※ 이 신청서는 권한 해지시 까지 지속 기록 관리하여야 하며, 이용자 접근권한 관리카드로 이용됨(10년간 보관)

2009. . .

신청자 : 소속 직 성명 인

[사례 3-4] 부실한 설계 덕에 기속행위가 재량행위로 둔갑한 평가 사례

○ 입지성(37) > 교통환경(15)

- 지하철 존재여부, 왕복도로 차선에 따라 각각 5점 척도로 평가 후 평균값 적용
- (매우양호) 4점초과~5점이하 (양호) 3점초과~4점이하 (보통) 2점초과~3점이하 (열악) 1점초과~2점이하 (매우열악) 1점

점수	평가	배점	지하철	도로
3	매우양호	15	사업지 반경 500m 이내 지하철역 존재	사업지 반경 1km 이내 6차선 이상 도로
	양호	12	사업지 반경 1Km 이내 지하철역 존재	사업지 반경 1km 이내 4차선 이상 도로
	보통	9	사업지 반경 1.5Km 이내 지하철역 존재	사업지 반경 2km 이내 6차선 이상 도로
	열악	6	사업지 반경 2Km 이내 지하철역 존재	사업지 반경 2km 이내 4차선 이상 도로
	매우열악	3	○ 사업지 반경 2Km 초과 지하철역 존재 지하철이 없는 지역(시군구 단위)	○ 사업지 반경 1km 이내 4차선 미만 도로

※ 택지개발사업지구, 환지방식에 의한 사업지구인 경우에는 만점 적용

❖ **내부통제를 고려하지 않은 시스템 구축**

- **기속행위 임에도 불구하고 재량행위가 되어 버림**

❖ **정보시스템 구축 때 반드시 내부통제 전문가 참여 내부통제 모듈 설계도 작성**

- **시스템 구축 때는 반드시 설계가 선행되어야 함.**

- 평가대상 기업은 반경 1Km 이내에 4차선 자동차 전용도로가 있어 평가점수 12점을 받아야 함.
- 향응을 하지 않았기 때문에 평가 불이익을 당함.
- 근본 원인은 평가와 조사업무를 분리하지 않았기 때문임.
- 조사 결과에 대하여 평가는 자동화(내부통제)되어야 함.

입력 및 평점 산출방식의 개선

- ❖ 담당자는 사실관계만 파악하고 평가에 따른 점수부여는 자동화
- ❖ 평가표가 아닌 조사표 방식 사용
- ❖ 평가는 자동화

평가 업무를 조사 업무로 전환한 사례

입지성 -> 교통환경

(1) 사업장과 직선거리 지하철까지의 거리

1,200 Km 확인자료 ### 스마트폰 사진

사업장과 지하철의 가장 가까운 직선거리로 측정
3Km 이내에 지하철이 없을 경우 "없음"으로 입력

(2) 사업장과 직선거리 6차선 도로까지의 거리

6 차선 도로 1,900 Km 확인자료 ###

사업장과 6차선 도로까지 가장 가까운 직선거리로 측정

사업장과 직선거리 4차선 도로까지의 거리

4 차선 도로 600 Km 확인자료 ###

사업장과 4차선 도로까지 가장 가까운 직선거리로 측정

최근에 문제가 되고 있는 인사부정(채용 비리) 문제도 동일한 관점에서 해결에 도움이 될 수 있음

4th DO :

System에 내부통제 모듈(embedded internal control module)을 내장하라.

- ❖ 대부분 **업무분장, 접근통제를** 사람에게 적용하고 시스템에는 적용 안함
- ❖ 시스템에 접근통제, 업무분장 내부통제 모듈이 존재하지 않아 발생한 부정 사례들

[사례 4-1] OOOO항공사 재무관리부장의 횡령 사건

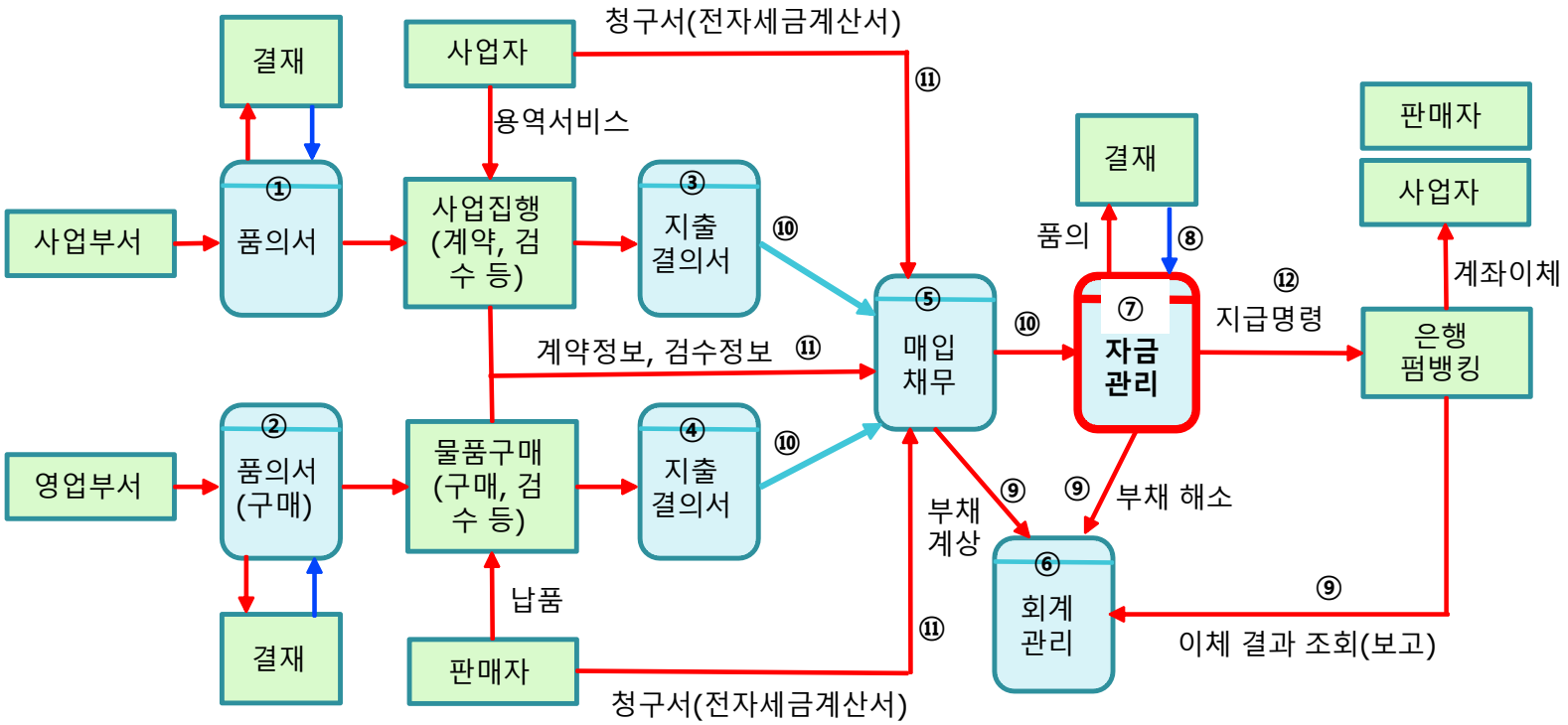
[언론 보도 내용]

6년간 360억 빼돌린 OOOO항공 직원...1심서 "징역 13년" (2019.05.24)

- 김씨는 2005년부터 2012년까지 OOOO항공 한국지사에서 재무관리부장으로 근무했다. OOOO항공은 국내 한 은행과 업무협약을 맺고 자금을 예치했다.
- 이 과정에서 1600만원 미만의 금액은 김씨와 지사장이 서명한 **송금요청서**만 있으면 출금할 수 있도록 했다. 이를 넘는 금액은 본사 임원의 서명이 추가로 있어야 했다.
- 김씨는 이 허점을 이용했다. 지사장의 서명을 위조해 6년간 2481차례에 걸쳐 총 362억여원을 빼돌렸다.

자금관리부서의 자금 지출 결정, 집행 관련 선행 후행 과정 내부통제 모듈 부재

❖ 금액, 계좌번호 등은 선행 process에 권한이 있음. 근거 없이 송금의뢰서 발행 가능



❖ **예산제도, 자금운용계획 process는 생략**

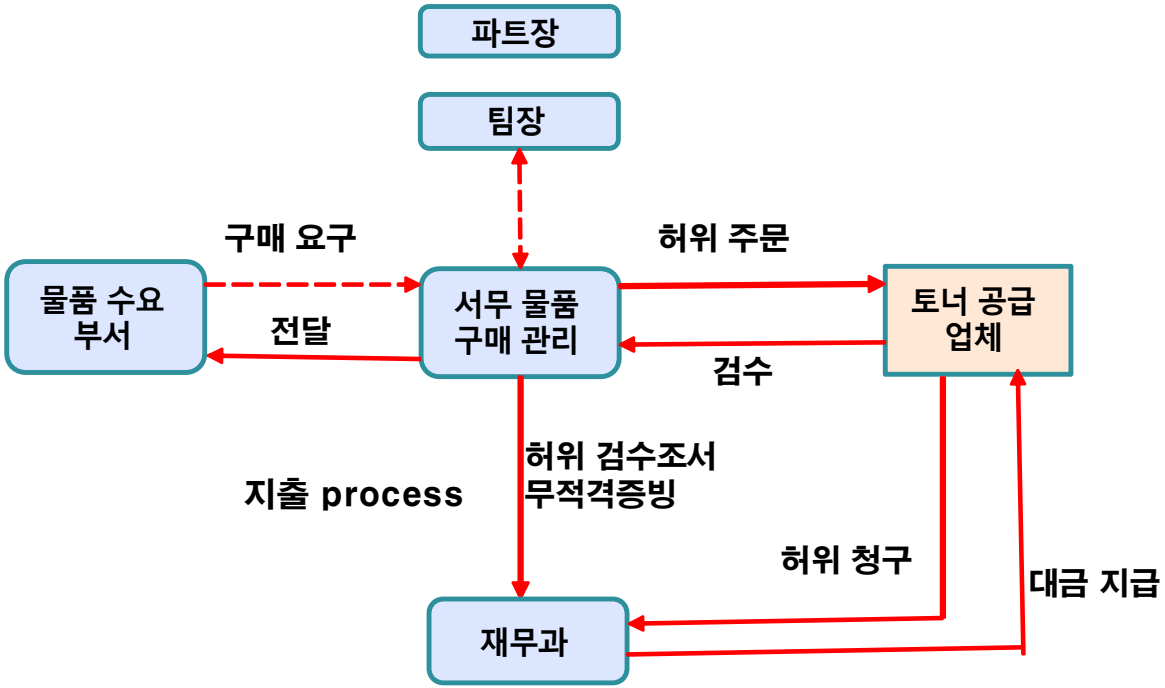
❖ **지사와 본사, 지사와 지사간 자금 유통을** 위한 송금, 수납의 경우에도 ⑤ 채권, 채무 계상 ⑥ 회계처리 등의 process는 존재하여야 함. 송금의 경우에는 ⑤가 타 지사, 본사로부터의 요청 공문을 근거로 ⑦에 송금 요청(⑩)을 하고 그 사실을 ⑥에 전송(⑨). ⑦은 은행에 지급명령을 하고 그 사실을 ⑥에 전송(⑨). **⑥은 이 두 정보를 reconciliation하여 이상이 없을 경우 회계처리**.

[사례 4-2] 직원의 업무분장과 시스템의 업무분장 괴리로 인한 부정사건

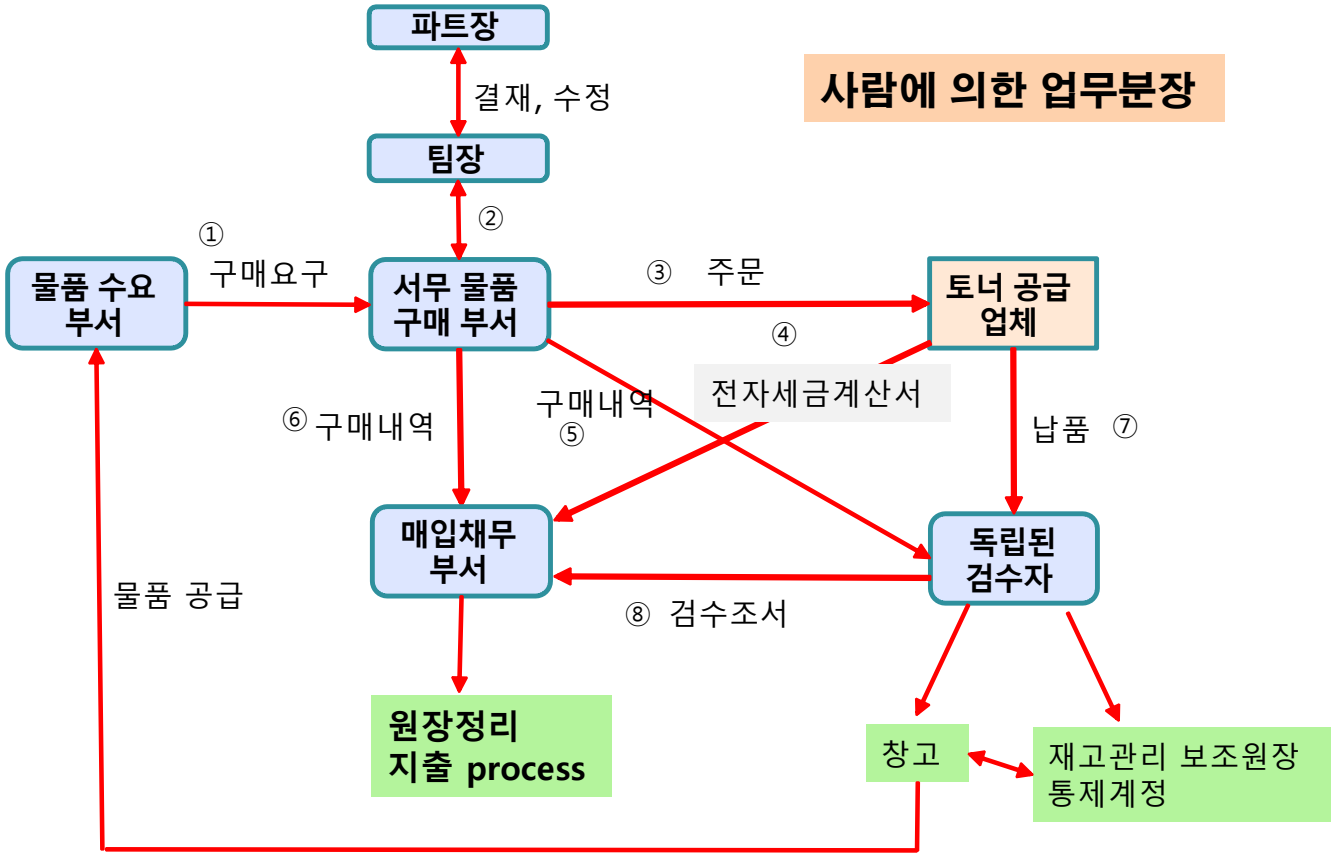
[언론 보도 내용]

프린터토너 구매 허위로 꾸며 1억원 횡령한 병원직원 검거 (2016/09/01 05:55)

- 1994년 서울시내 모 대학병원에 입사해 서무 및 물품관리를 해온 장씨는 지난해 3월부터 올해 3월까지 프린터 토너를 구매하지도 않았으면서 500개 가까이 구매한 것처럼 속여 병원으로부터 1억원을 받아냈다. 장씨가 프린터 토너를 구매한 것으로 가장한 회사는 그의 어머니 명의이나, 실질적으로는 그가 운영했다.

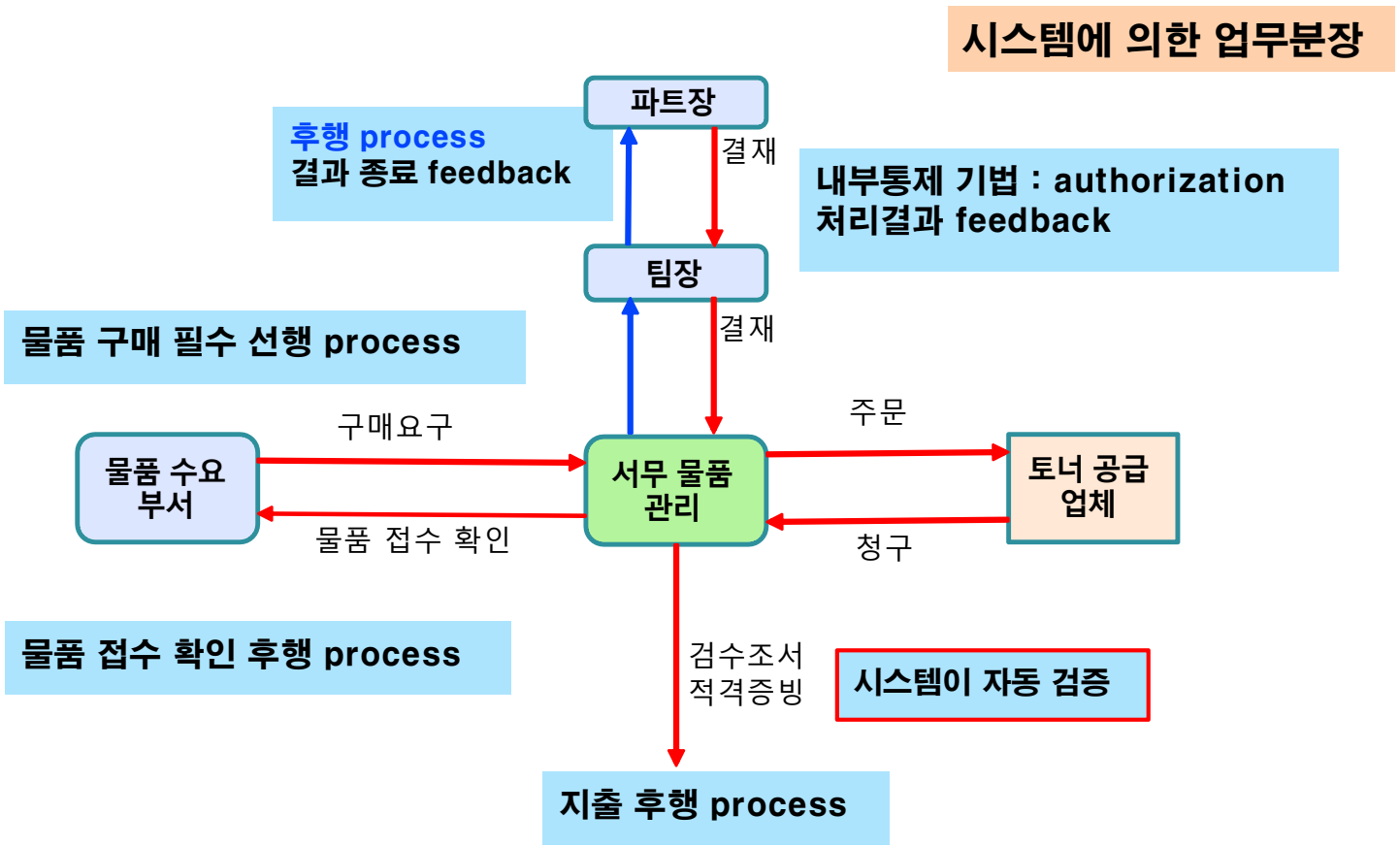


부정을 방지하기 위하여 사람 중심으로 업무를 분장하는 경우



❖ 그럼에도 불구하고 직원이 사용하는 **시스템이 접근통제, 업무분장 되어 있지 않으면** 부정오류가 발생함.

정보시스템에 접근통제, 업무분장 위한 내부통제 모듈을 심은 경우



❖ **직원은 업무분장 안되어 있어도** 부정 오류가 발생하지 못함.

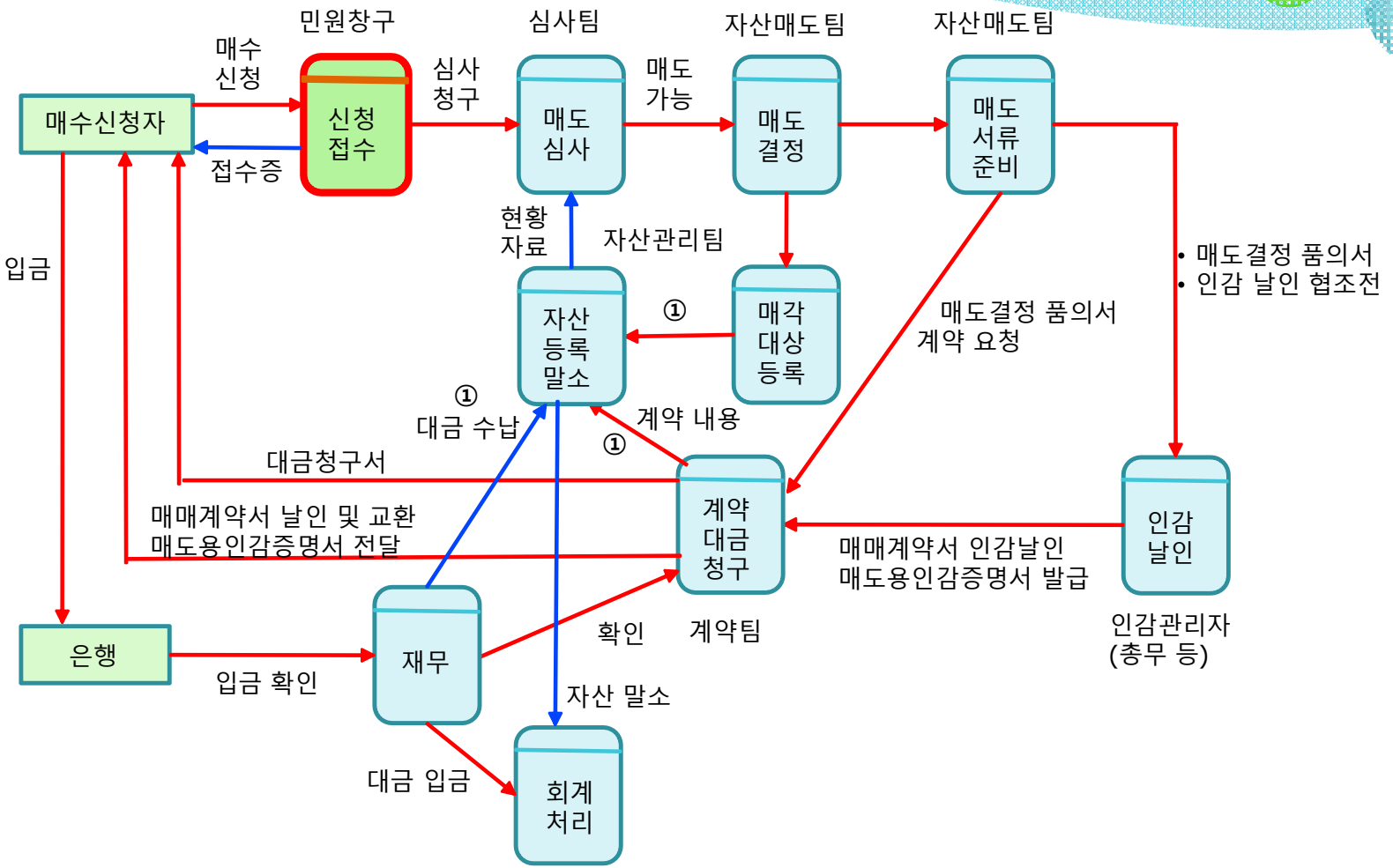
[사례 4-3] 국유지 무단 매매계약을 통한 부정사건

[언론 보도 내용]

국유지 몰래 팔아 횡령 공기업 직원 기소 (2017-09-06 10:51) (2018.08.23 (10:48))

- 국유지를 몰래 팔아넘겨 11억 원의 매각대금을 챙긴 한국OOOO공사 직원이 재판에 넘겨졌습니다. 서울중앙지검은 횡령 혐의로 한국OOOO공사 직원 27살 곽 모 씨를 구속 기소했습니다.
- 곽 씨는 2017년 3월, 법인 인감도장을 이용해 자신이 관리하는 서울 수유동의 국유지 매매계약을 체결하고 매각 대금은 자신이 챙기는 방법으로 1,150만 원을 가로챈 혐의를 받고 있습니다. 곽 씨는 2016년 10월부터 18차례에 걸쳐 서울 강북구 수유동 등에 있는 국유지 24필지를 팔아 18억원 상당의 매매대금을 빼돌린 뒤 개인 용도로 쓴 혐의로 구속 기소됐습니다.
- 검찰 조사 결과 곽씨는 자신이 관리하던 국유지에 대해 매수 신청이 들어오면 상사가 자리를 비운 틈을 타 매매계약서에 법인 인감을 찍고, 매도용 인감증명서 발급 공문을 결재하는 등 매각에 필요한 서류를 위조한 것으로 드러났습니다.
- 곽 씨는 몰래 국유지를 팔아넘긴 사실을 숨기기 위해 사전에 국유지를 분할 신청해 놓고 이를 기록하지 않은 것으로 조사됐습니다.

사람은 업무분장 되어 있으나 시스템에는 내부통제 모듈(업무분장, 접근통제)이 구축되지 않은 경우



- 예산회계 세입처리, 자금운용계획 반영 등 생략
- 결재과정 생략
- 매도용인감증명 발급 및 계약서 인감날인 요청은 계약과 무관한 자산매도팀이 하는 것이 바람직함

[사례 4-4] 허위 매입채무 계상에 의한 부정사건

[언론 보도 내용]

20년 간 회삿돈 500억원 빼돌린 50대 남성 징역 12년

기사입력 2019-11-20 11:40 I 최종수정 2019-11-20 13:19

- 기업의 재무 담당 부서에서 약 20년간 일하며 회삿돈 500억여원을 횡령해 유흥비 등으로 탕진한 50대 남성이 법정에서 중형을 선고받았습니다.

- 1995년 한 광고회사의 재무 담당 부서에서 일하게 된 임 씨는 2000년 2월부터 2019년 5월까지 약 20년간 2천22회에 걸쳐 법인 자금 502억7천여만 원을 빼돌린 혐의로 재판에 넘겨졌습니다.

- 재판부에 따르면 임 씨는 1999년쯤 자금 집행 과정에서 **실수로 거래처에 약속한 액수보다 대금을 많이 지급하게 되자 허위 매입채무를 입력해 위기를 넘긴 뒤 차액은 채워 넣지 않았습니다**. 이런 일이 적발되지 않고 무사히 넘어가자 임 씨는 '이렇게 횡령해도 모르겠구나'는 생각에 범행하기로 마음먹었습니다.

- 앞선 재판에서 **임 씨 측 변호인은** "**피해 회사의 자금 집행 방식과 감사제도가 부실해 범행 발생과 확대에 큰 영향을 미쳤다**"는 취지로 주장했으나, 재판부는 이런 사정이 "양형에 있어 감경 요소에 해당한다고 볼 수 없다"고 판단했습니다.

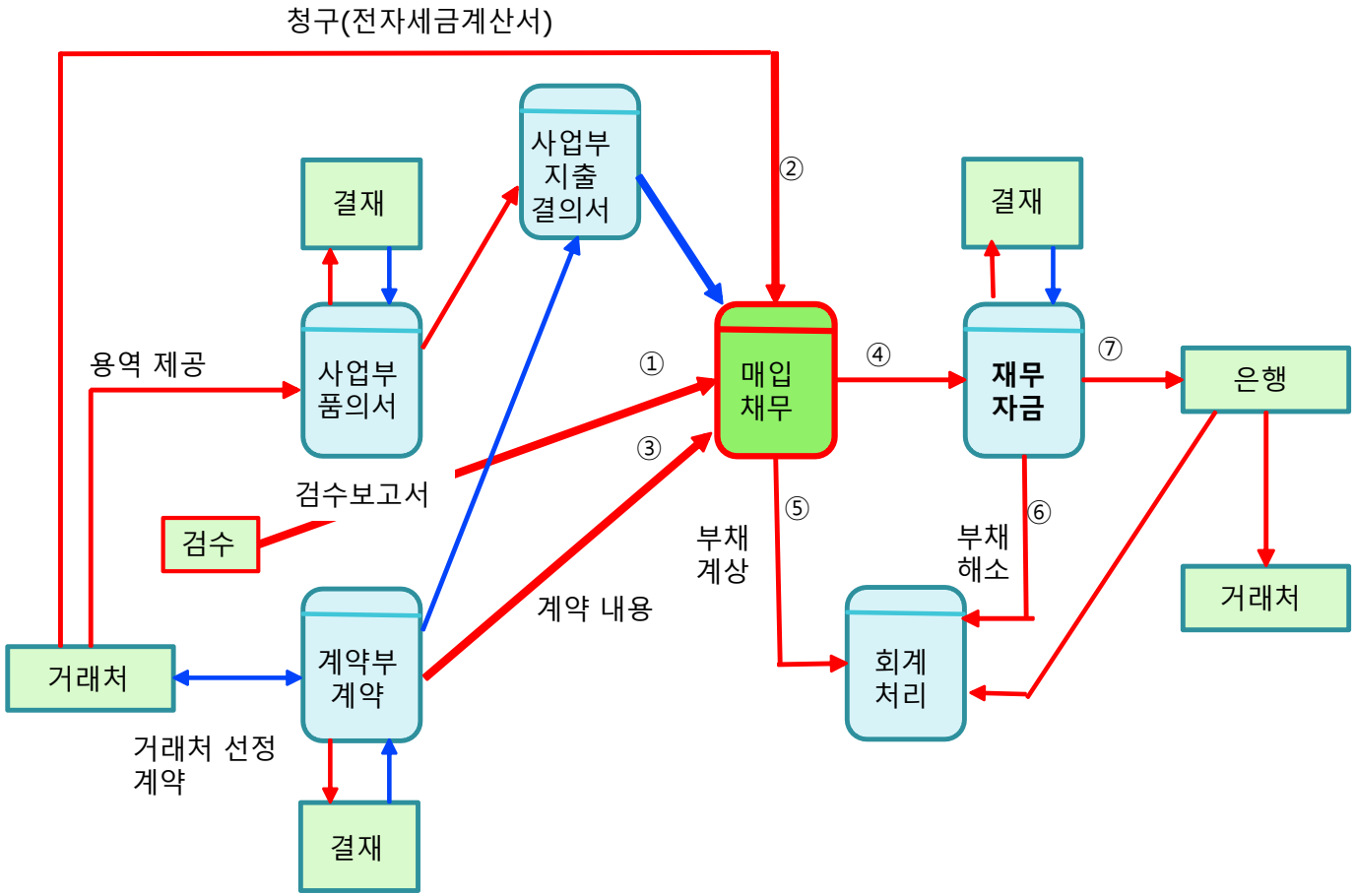
이것도 시스템의 업무분장, 접근통제 모듈 부재에 따른 문제

❖ 부정이 발생하게 된 근본원인은 재무관리부서에서 지출금액을 임의로 생산(수정 포함) 할 수 있었기 때문임.

❖ 선행 process에서 생산된 정보를 임의로 수정하거나 새로 입력 가능한 시스템은 언제든 부정의 위험이 있음.

❖ 정보의 reconciliation 통제가 중요함.

❖ 감사과정에서 한번 생산된 정보를 중복적으로 다시 생산할 수 있도록 되어 있는지 점검할 필요가 있음.



❖ 예산제도(예산배정, 자금배정), 자금운용계획에 따른 자금 통제 process는 별도로 표시하지 않음.

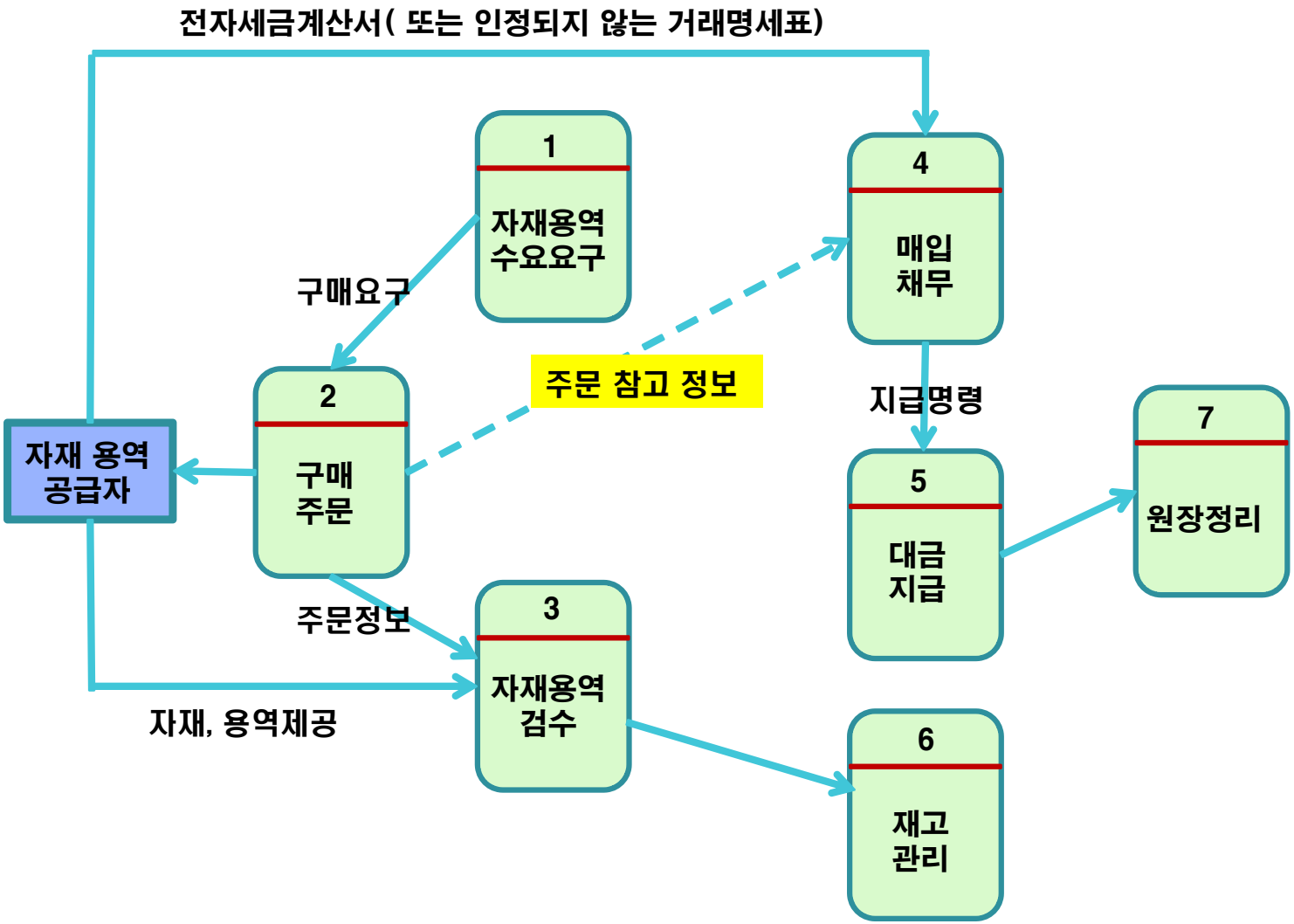
[사례 4-5] 00공사 reconciliation 내부통제 모듈이 없는 부실 시스템 구축 사례

구매오더(EKPO)							입고자재전표(EKBE)			구매송장발행(RSEG)			
구매문서	품목	수량	단위	내역	자재그룹	생성자	자재전표	수량	생성자	송장전표번호	회계연도	금액(SGD)	수량
3900000238	20	2	EA	MC Clock	계측기	MR0001	7000002415	1	RF0001	4805601376	2007	365	2
3900000238	30	2	EA	W Clock	제어기	MR0001	7000002415	1	RG2001	4805601376	2007	90	2

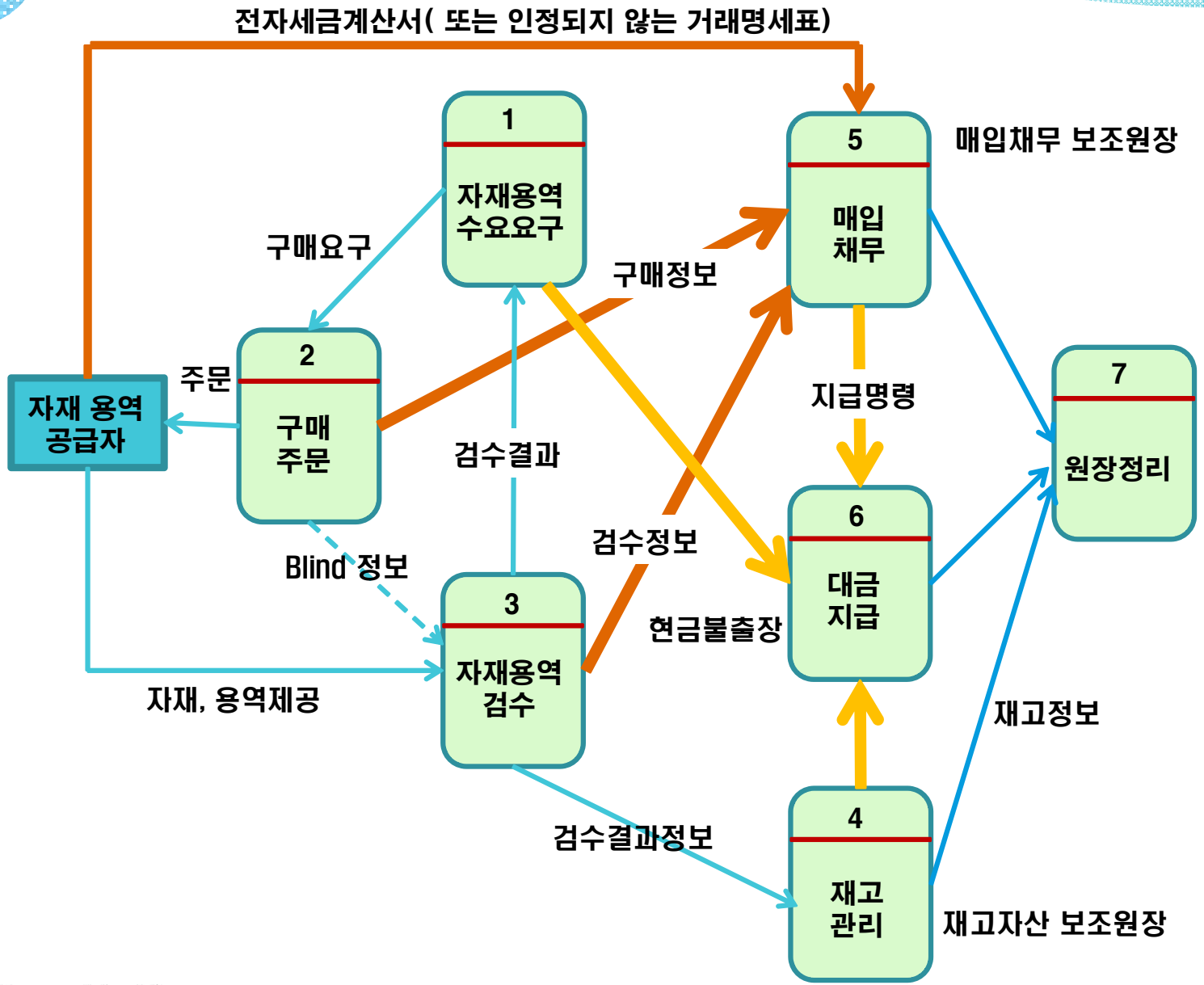
- ✓ 각 process에서 사용하는 용어의 문제
  - 데이터베이스에 저장된 테이블과 호출된 데이터의 제목은 적절한가 ?
- ✓ 구매문서보다 적은 수량이 입고되었음
  - 구매부서는 2개를 주문하였으나 1개만 검수됨(또는 1개는 창고에서 빼돌림).
  - 대금은 2개 값이 지불됨.
- ✓ 우리나라 실정에 맞지 않음
  - 외국은 송장(invoice)을 전달하여 대금 청구를 함.
  - 우리나라 거래명세표와 유사하지만 우리나라는 전자세금계산서가 청구서임.

정보화 이전보다 못한 내부통제 사례

내부통제 장치 설계가 안된 비정상적인 경우 – reconciliation 부재



내부통제 처방 – reconciliation 설정



[사례 4-6] 00증권 시스템 내부통제 모듈 내장 부재로 인한 사건

❖ 내부통제 모듈(limit check, reasonableness check, range check)

- 처리 시간 1 nano second

[서울파이낸스] 딜러 주문 실수로 120억원 손실 (2010.2.10)

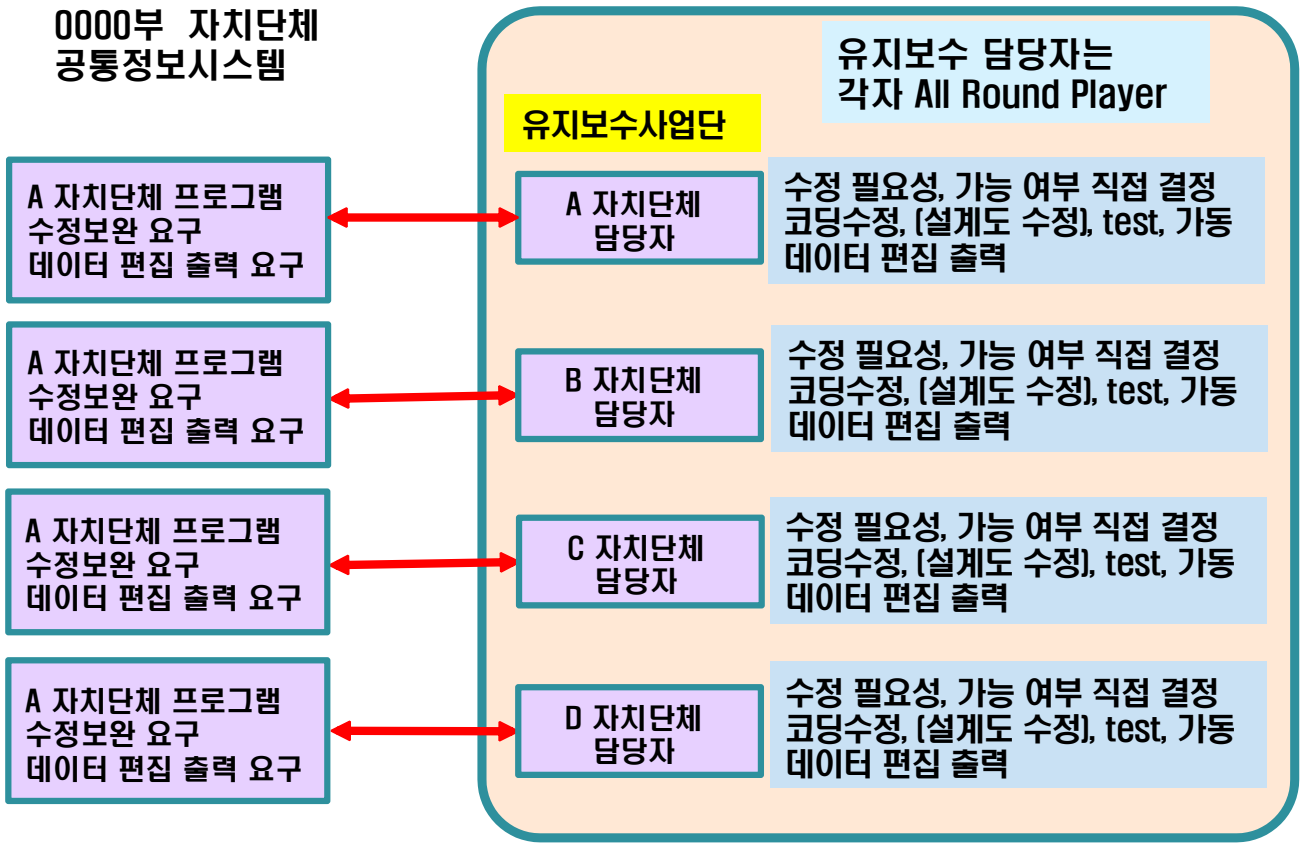
00증권이 달러선물 딜러 실수로 120억원 규모 손실을 입은 것으로 확인됐다. 00증권 관계자는 지난 9일 "담당자가 선물 주문을 잘못 내 손실이 났다"고 전했다. 해당 딜러는 개장 직후 달러선물 스프레드 매수 거래를 80원에 체결했는데 시세를 감안하면 80전(0.80원)을 80원으로 잘못 입력한 것으로 추정된다. 주문이 나온지 15초 만에 1만5000계약이 체결됐으며 거래량은 1만5천계약에 달했다.

달러선물 호가단위 0.10원의 가격변동폭은 1000원이다. 만약, 0.8원 수준에 거래를 했다고 가정한다면 약 118억8000만원의 손실이 발생한 셈이다.

5th DO :

System 유지 관리 조직 및 업무에 내부통제구조를 적용하라.

- 정보시스템 담당자는 **super user**
  - monitoring의 사각 지대
  - 정보시스템 부서는 **유일한 matrix 조직**

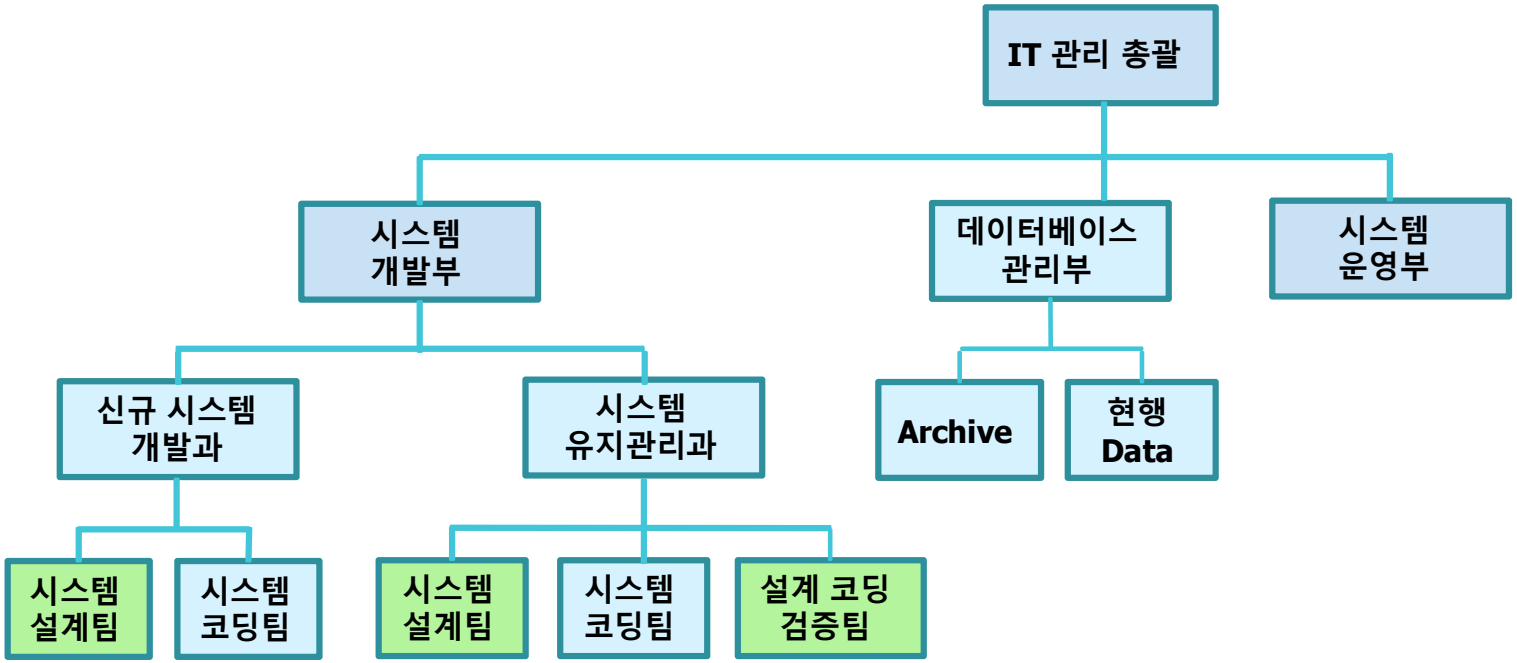


어느 금융공기업 정보지원실의 access control, segregation of duty failure 사례

- 정보지원실 직원은 super user 로 소속과 달리 업무담당 부서의 직원으로 역할 함.
- 해당 부서에서 **데이터 수정 요청이** 있거나 데이터 편집하여 excel 등 출력 요청하면 그 작업을 함.
- 전산 담당 직원은 모든 데이터에 접근하여 입력, 수정, 삭제 등 권한을 가짐
- 프로그래밍 능력은 없어진지 오래고 전산행정직 역할을 함.
- 소속 직원은 전산행정 역할만 수행하고 외부 용역직원이 중요한 주된 역할을 함.
- 매년 유사 명칭의 전산 프로그램 구축예산을 집행하나 그 많은 개발 프로그램이 현재 가동되고 있는지 창고에 처박혀 있는지 의문임.

정보지원실 시스템 개발, 유지관리 업무의 바람직한 업무 분장 사례

- ❖ 설계, 코딩, 운영, data 관리 업무의 분장
- ❖ 감사실의 실시간 monitoring
- ❖ transaction log의 적극 활용
- ❖ 조직도 사례



6th DO :

내부 감사계획은 System 내부통제 진단 결과를 근거로 수립하라.

❖ 가공 후 데이터 또는 문서 중심의 감사

- 업무 담당자 또는 시스템 관리부서가 준비해 준 출력물 중심
- audit around computer vs. audit through computer

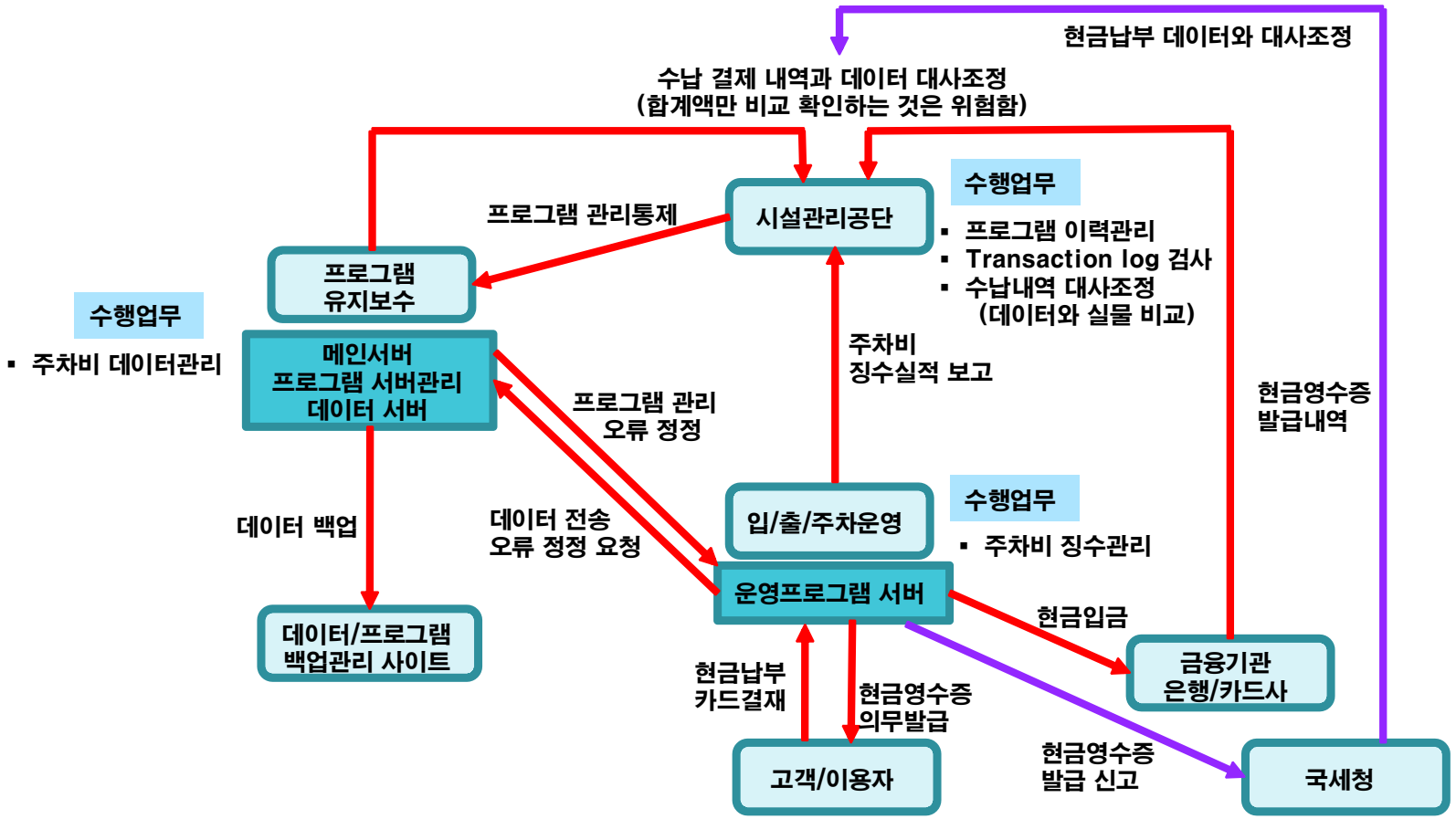
❖ 시스템 설계도와 코딩의 비교 감사

❖ **transaction log 중심 감사**

- 결재 때 첨부문서 사례 – supervising failure
- digital transformation

❖ 사람이 아닌 System에 대한 access control, segregation of duty 등 내부통제 모듈의 내장 여부를 확인

[사례 6-1] 서울시 감사실 내부통제 진단을 이용한 주차관제시스템 감사실행계획 사례



- ✓ 주차장의 입차/출차 관리자는 프로그램에 대한 접근이 통제되어 있음
  - ▪ 프로그램은 오직 유지보수 담당자만 수정가능하므로 감사 방향은 프로그램에 집계된 데이터와 수납된 카드 및 현금액을 대조확인
- ✓ 입차/출차 관리자는 필요한 경우 유지관리 업체 담당자에 연락하여 특정한 차량의 입/출 기록을 삭제해 줄 것을 요청할 수 있음.
  - ▪ 감사방향은 입력된 데이터가 유지보수 담당자에 의하여 수정, 삭제된 것이 있는지를 transaction log를 통하여 확인
- ✓ 프로그램 유지보수 책임자와 입/출차 운영자가 각각 주차 데이터 관리, 주차비 실물관리를 분담하고 있으므로 이들이 공모하기 전에는 큰 부정은 발생 가능하지 않음.
  - ▪ 따라서 감사방향은 이들이 공모하였을 때 발생 가능한 부정위험에 대하여 초점을 두어야 함.
- ✓ 그러한 가능성에 대하여 다음과 같은 감사방법 적용이 필요함.
  - ▪ 현금결재 주차비를 누락할 가능성 : 주차장별(또는 권역별)로 월별 현금결재 비율을 비교 분석
    - • 연간 추세가 균일한지?
    - • 주차장별로 변별적인 차이가 존재하는지?
    - • 3개 제조사(프로그램 유지보수업체)별로 변별적인 차이가 있는지 ?
- ✓ 시설관리공단의 유지보수업체의 데이터와 금융기관의 입금/결제 내역을 대조 확인하여야 함.
  - ▪ 유의할 것은 데이터 상의 합계금액과 금융기관의 입금 합계금액만 대조확인하는 것은 의미가 없음.
  - ▪ 엑셀 등을 이용하여 건별로 대조확인 하여야 함.
  - ▪ 신용카드 결재의 경우 발생일을 기준으로 대조확인하여야 함.
- ✓ 현금 수납 내역의 조작 위험을 감사하기 위하여 국세청으로부터 주차장 발행 현금영수증 정보 조회를 요청하여 시스템의 데이터와 대사조정

[사례 6-2] 시스템 및 업무 처리가 부실한데도 시스템 감사가 없었던 사례

- 2009년 1월~2014년 1월 경기도 김포시 하수도 시설 공사 현장 등에서 근무한 비정규직 현장사무보조원 김00(34)씨는 5년 동안 109억원을 횡령하였다. 본사는 증빙지가 없어도 김씨가 전표를 청구하는 대로 돈을 입금해줬다.

- 김씨가 공사현장 직원 숙소를 임차했다고 허위 전표를 청구하면, 본사는 확인 없이 전도금 통장으로 임차보증금을 보냈다. 현장에서의 전도금 통장 관리도 허술했다. 김씨는 전도금 통장에서 자신과 남편 계좌 등으로 대범하게 이체했다.

- "숙소가 실제 안 생겼는데 신청하니까 입금이 됐다. 웃긴 게 같은 날 2억7000만원, 2억8000만원씩 각각 신청하고 품의서가 없어도 돈이 들어왔다. 한번 해보니 돈이 들어와서 계속했다."(2014년 1월17일 피의자 진술내용)

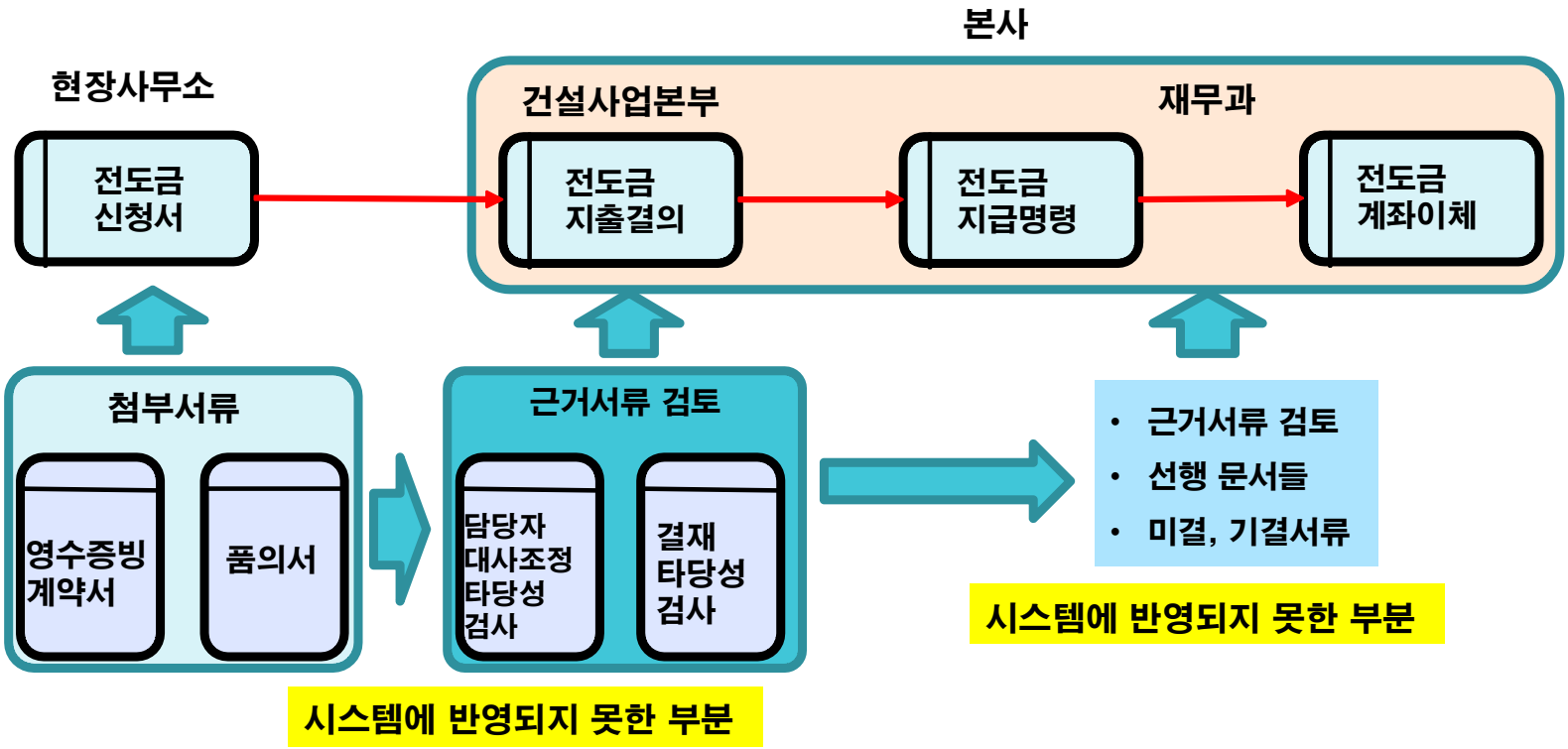
- "품의를 반려한 사람은 재무관리그룹 김○○ 직원 딱 한 명 있었다. 2만2000원짜리 계정이 다르다는 이유로 반려해서 걱정했으나 그 다음 숙소 결제 건인 3억3000만원은 바로 승인해줬다. 월 마감 이후 매월 초 증빙 총괄표를 출력하여 10일까지 증빙지를 재무관리 그룹에 보내야 했으나, 대부분 발송하지 않았다. 재무관리 그룹에서 분기별로 한 번씩 본인에게 독촉이 왔고, 보내겠다고 이야기하면 다시 확인을 하지 않았다."

- 김씨는 "공사가 마무리되면 숙소 임차비를 제외한 원가(경비)에 대해서만 정산을 했다"고 진술했다. 임차 계약 기간이 끝나면 회사로 회수되어야 할 임차보증금은 회계상 미수 채권으로 분류된다. 000건설은 미수 채권인 임차보증금에 대한 결산도, 감사도 하지 않았다.

- 현장소장과 관리팀장도 김씨의 횡령을 막지 못했다. 통상적 절차대로 하자면, 현장 사무보조원은 직원 임차 숙소 관련 전표를 작성하고 현장소장과 관리팀장의 내부 결재를 받아야 한다. 그러나 현장소장과 관리팀장은 모두 바쁘다는 이유로 김씨에게 결재할 수 있는 접속 정보인 아이디와 비밀번호를 주었다. 김씨가 가짜 결재를 하면 본사 재무그룹, 자금그룹 차례로 결재가 이뤄진다. 그러나 본사 회계 담당자들 또한 5년간 검토 한 번 없이 전표를 치는 대로 돈을 입금했다.

00건설 100억대 부정 사건의 근본 원인은 과연 무엇인가?

- 담당자가 업무를 적절히 처리하지 못하여서인가?
- 협조자와 결재자가 근거 증빙자료 대조 확인을 하지 못한 것이 원인임.



- 본사 담당자, 결재자 직원 모두가 누구도 증빙자료 확인을 요구하지 않았음.
- 만일 감사실이 내부통제 진단을 실시하고 그 결과를 바탕으로 검사를 실시하였다면 ....
- 이론으로 배운 COSO 내부통제 5가지 구성요소 중 2번째 Risk Assessment.

[사례 6-3] 00면소재지 종합정비사업 보상금 횡령 사건
시스템 부실한 설계와 시스템 감사가 없었던 것이 근본 원인

공사는 2014.12.2 00시로부터 수탁 받아 2018.12.31 까지 준공계획을 시행

00지사는 위 사업으로 편입되는 토지 및 지장물에 대한 보상비(용지매수비, 지장물, 이주보상비)를 산정, 확정, 지급함.

직원 A는 2014.1.20 부터 2015.1.20까지 00지사 회계업무 담당.

2015.1.21부터 용지매수 보상 및 환지청산금 업무 담당

종합정비사업 보상금 횡령

2016.5.19 지장물보상비 5,353만원 등 총 7,449만원을 지급대상자 B에서 C로 **명의 변경 후 계좌이체**

2017.2.22 동일한 내용으로 다시 결재 받아 C명의로 7,449만원을 이체 지급함.

경지정리사업 환지청산금 횡령

2015.11.30 확정 **명단에 없는 가공의 인물** C를 추가하고 환지청산금 교부통지서, 사용인감, 통장사본 첨부하여 교부금액 2,432만원 지출 위해 ERP 프로그램 이용 재무전표 발행하고 계좌이체

유지관리 전력료 횡령

(1) 정상적인 전표 작성 후 지로대금 납부 않고 출금 : 661,330원

(2) 과거 전표 재활용 지출전표 작성하여 결재 받아 출금 (ERP에는 증빙 미첨부) : 671만원

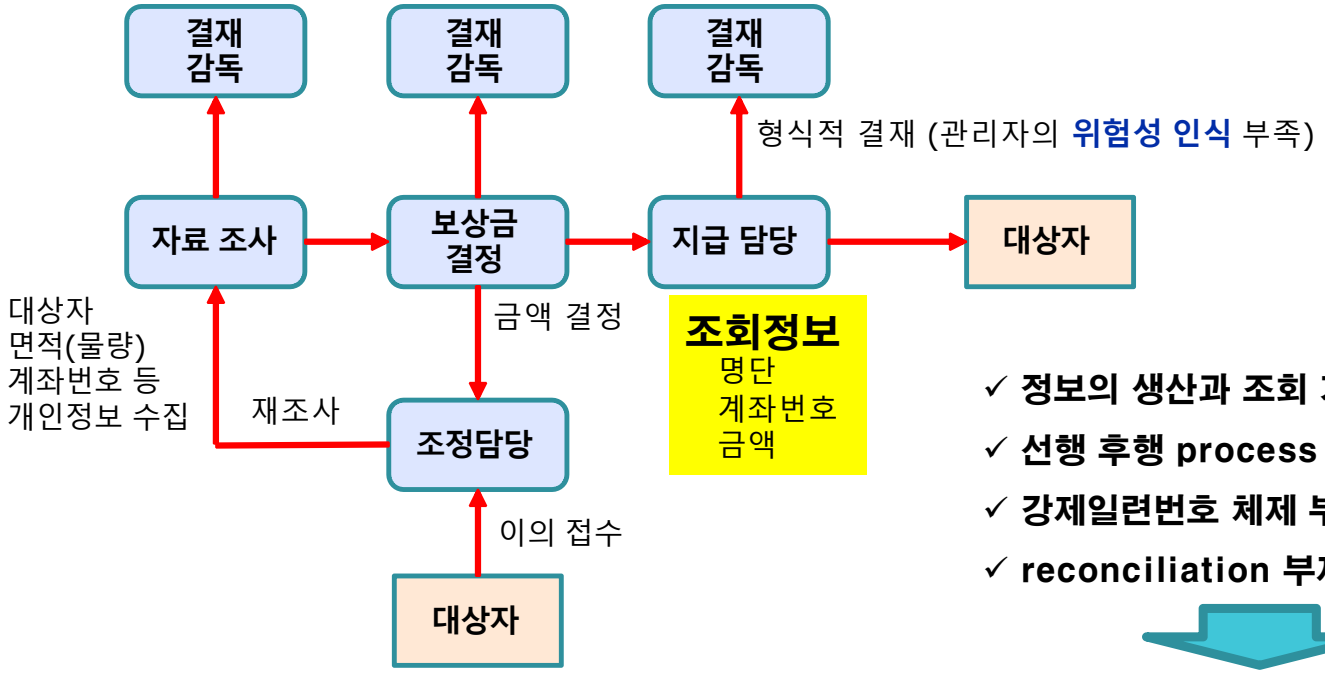
(3) 지급 원인 없는 경우, **지출금액보다 많이 출금 허위 전표 작성**(ERP에 증빙 미첨부) : 780만원

토지매매대금 지급 후 미등기

대금 지급 후 미등기, 제한물권 말소조치 미이행

윤리교육의 문제인가 ? 시스템 부실의 원인인가 ?

예방적 차원 내부통제 진단 결과를 감사계획에 반영하였다면?



- ✓ 정보의 생산과 조회 기능 분장 안됨
- ✓ 선행 후행 process 설계 미흡
- ✓ 강제일련번호 체제 부재
- ✓ reconciliation 부재

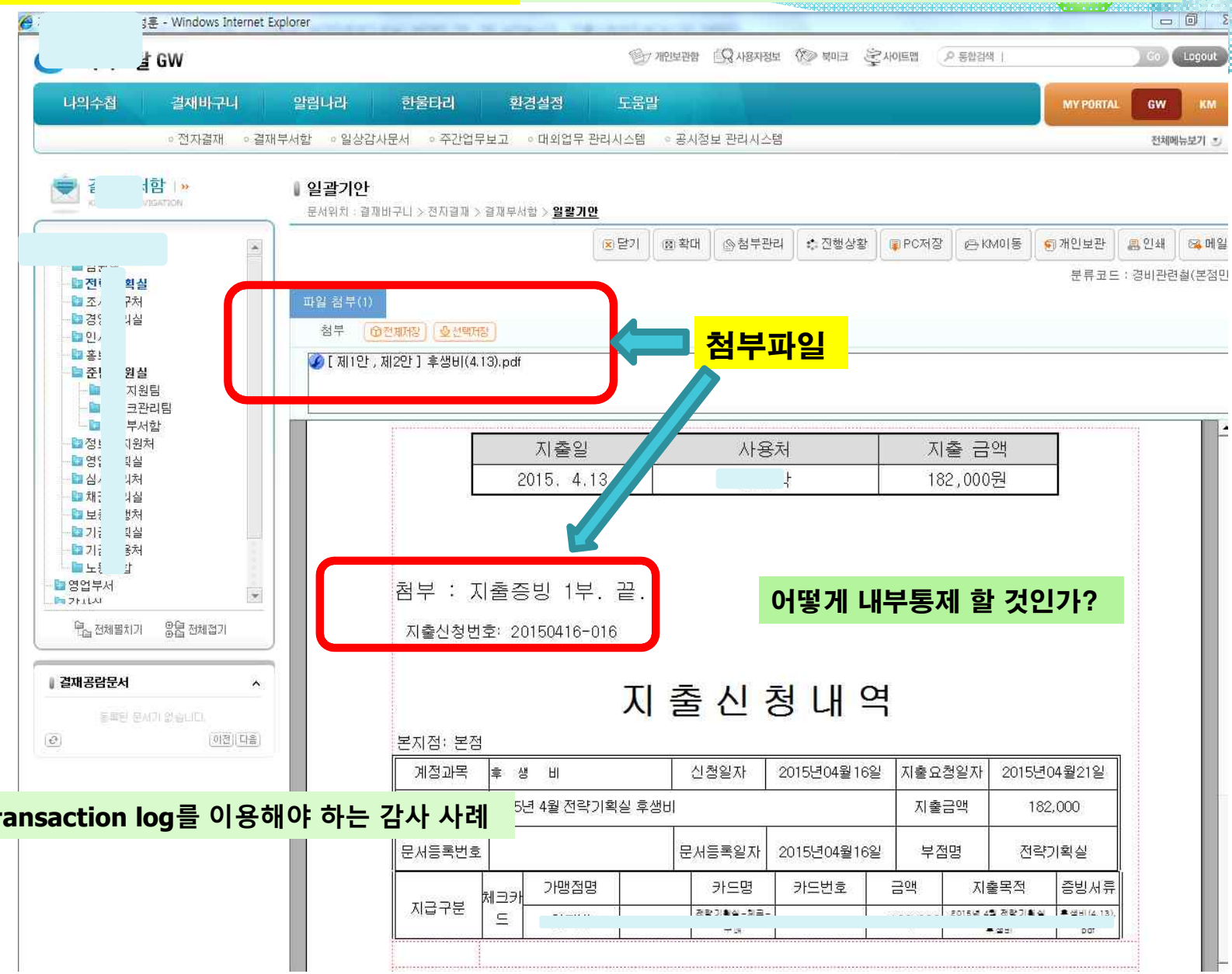
정보시스템 내부통제 진단과 개선 필요

유사한 사례들 : 지방재정정보관리시스템(이호조), 복지시스템, 자산관리공사 등 다수

- ➢ 시스템의 내부통제 진단 및 개선 – 감사실의 역할
- ➢ 소규모 조직의 경우 내부통제 방안 -> 감독 강화가 해답
- ➢ 감독이 부실할 경우 윤리강령에 동일한 책임(연대책임)을 묻도록 규정

[사례 6-4] 전자결재와 시스템 감사 필요성

첨부파일을 열어보지 않아도 결재 가능한 사례



❖ **Transaction log를 이용해야 하는 감사 사례**

[사례 6-5] 우리 통제환경에서 체크리스트는 효과가 있는가?

어린이 집 차량 사고와 내부통제 방안

"동두천 어린이집 차량 사고 막을 기회 3번 있었다"

- 이 원장은 "통원 차량이 어린이집에 들어오면 (1) 일차적으로 차량 인솔 교사가 차에 탄 아이들 인원을 파악하면서 하차시킨다" 면서 "아이들이 모두 내린 후에도 (2) 운전기사가 차 안을 한 번 더 점검하고 내리게 된다" 고 설명했다.
- 이어 (3) "사전 연락 없이 아이가 등원하지 않으면 담임교사가 부모에게 전화를 걸게 돼 있다" 면서 "최소 3번 정도는 사고를 막을 기회가 있었을 텐데 어떻게 이런 일이 발생했는지 이해할 수가 없다" 고 말했다.

우리나라 통제환경에 적합한 내부통제 방안

인천시 : 어린이집 통학차 비상벨 10월부터 설치

경기도 : 10월부터 도내 어린이집 차량 6천여 대에 '잠자는 아이 확인장치' 설치한다

사고 예방을 위하여 어떠한 내부통제가 필요한가 ?

✓ 사고예방을 위한 업무지침, 편람, 체크리스트 ?

✓ 사고예방의 자동화, 제도화?

감사의 초점은 내부통제 체크리스트의 존재가 아니라 내부통제의 자동화에 있음

7th DO :

최신 ICT 기술적 용어에 현혹되지 말고 내부를 들여다보아라.

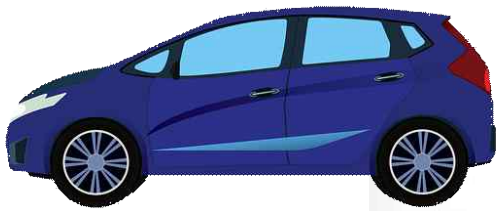
- AI, big data, blockchain, cloud, ERP, open 등
  - 이런 개념들이 포함되지 않은 제안요구서, 제안서, 개발계획서는 무시당함
- 개발 현장에서의 현실적 사례
  - **00국립대 병원의 AI 구축 사례**
    - AI를 이용한 병 진단시스템 발주를 하였는데, 구축된 것은 통계 프로그램이었음
  - 객체 DB 제안요구서 –> RDB로 구축 사례
- AI, big data, blockchain, cloud 등 System 적재 적소에 활용 결정되면 스케치가 아닌 설계를 먼저 하여 구현될 **시스템의 내부를** 들여다보아야 함.
- - 설계 후 설계 내용 검토 과정이 없다면 거짓이거나 부실한 구축에 불과

- **ICT 기술 발전의 추세에 대하여 직접 학습하고 기업의 미래 ICT 방향을 설정하라.**

S/W 개발 환경의 변화의 사례

❖ S/W 개발 세상은 open source, no code를 지향함.

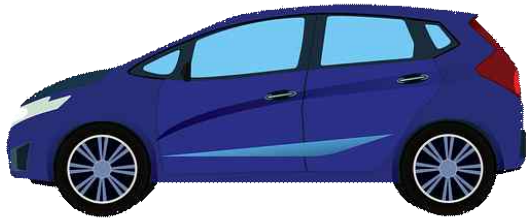
❖ Upper & Lower CASE (Computer Aided Software Engineering)가 나온지 20여년 되었음.



1980년 이전에 S/W(자동차)를 스스로 직접 만들고 싶을 때

➢ 모든 부품을 손수 만들어야

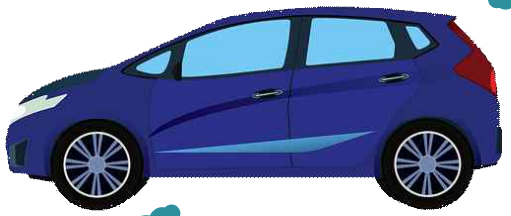
1980년-2010년경 자동차를 직접 제작하려고 하였다면



엔진, 트랜스미션 등 주요 부품을 먼저 선택한 다음 이에 맞추어 자동차를 디자인

현재 시대 자동차(S/W) 를 직접 만들려고 할 때

수만개의 다양한 무료 엔진



우선 자유롭게 자기만의 차를 먼저 디자인하고 그 차에 적합한 엔진 등 부품을 선택하여 조립

수만개의 다양한 무료 트렌스미션

8th DO :

ICT 재난대비계획이 SHOW가 아닌지 점검하라.

❖Disaster Recovery Plan

< 삼성SDS 화재사건 >

- 2014년 4월 20일 낮 12시25분께 경기 과천시에 있는 삼성SDS 데이터센터 3층에서 화재가 발생했다. 이 화재로 삼성카드의 온라인 결제시스템과 홈페이지, 모바일 애플리케이션(앱) 서비스가 중단되었다.
- 삼성SDS 과천센터는 삼성생명, 삼성화재, 삼성증권, 삼성카드 등 삼성그룹의 금융계열사의 시스템을 운영·서비스하고 백업데이터 등을 보관하는 데이터센터로 지상 11개층, 지하 3개층 규모의 건물이다. 삼성카드는 삼성SDS 데이터센터에서 화재가 나자 온라인·모바일 결제와 체크카드, 현금인출 등 거의 모든 서비스가 중단됐고 이를 완전히 복구하는데 8일이 걸렸다.
- 삼성카드 온라인 결제는 **화재가 발생한지 4일째인 23일이 되어서야 제한적으로가 정상화됐다**. 4월 23일 삼성카드는 인터넷쇼핑몰 등 온라인 결제가 정상화됐으며, 카드 결제 시 문자알림서비스를 재개했다고 고객에게 문자로 알렸다. 다만 스마트폰을 이용한 공인인증서 사용과 삼성앱카드 결제 서비스는 복구 중으로 서비스 재개까지는 **시일이 소요될 것이라고 하였다**. 삼성카드 측은 문자알림서비스를 이용하는 회원에게 1개월 요금을 면제하기로 하였다.
- **현행 전자금융감독규정에 따르면** 각 금융사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비해 적정 규모와 인력을 구비한 재해복구센터를 구축해야 하고 **전산센터가 마비돼도 3시간 이내로** 복구해야 한다.

< 노스웨스트 내셔널 은행 화재사건 >

- **1982년** 11월 25일 추수감사절날 미네아폴리스에 있는 노스웨스트 내셔널 은행(Northwest National Bank)에 화재가 발생하여 은행거래기록과 자료처리 시스템을 모두 태워버렸다. 이것은 **미네아폴리스 시 역사상 가장 큰 화재사건**이었다.
- 그러나 **월요일이 되자** 이 은행은 인근 건물에 임시 은행을 열고 정상적으로 예금, 출금, 대출 등 은행 업무를 수행하였다. 이 은행은 다행히도 **재난복구계획을 수립 운용하고 있었다.**
- 재난복구계획에는 화재가 발생할 경우 어느 장소에 얼마의 점포 면적을 확보하고, 컴퓨터 장비와 소모품, 사무용품 등을 어떻게 조달할 것인가에 대한 세밀한 내용이 준비되어 있었다.

< 시에라 은행 화재 사건 >

- **1990년대 초** 어느 날 새벽 캘리포니아 포터빌에 있는 시에라 은행(Bank of the Sierra) 본사에 화재가 발생하였다. 스프링쿨러 시스템과 할론가스 진화장비 등이 마련되어 있었으나 화재로 지붕이 무너져 내려 앉으면서 스프링쿨러 시스템을 파괴하고 할론가스를 분출시켰으며 주전산기를 열기로 녹여버렸다. 은행의 가계 무담보 및 담보 대출, 신용카드 기록, 처리 대기중인 수표 등을 포함하여 데이터베이스는 완전히 파괴되었다.
- 그러나 이 은행은 노스웨스트 내셔널 은행의 150페이지에 달하는 **재난복구계획을 바탕으로** 수립한 계획 덕분에 신속하게 복구팀을 편성하고 핵심적인 임무를 부여하며 필요한 장비를 준비하였다.
- **화재가 발생한지 9시간만인 오전 10시가** 되자 이 은행은 아무 일이 없었던 것처럼 각 지점에서 정상 업무를 시작할 수 있었다.
- 이 은행이 하루에 처리하는 거래 건수는 25,000건 내지 40,000건 정도이나 산 라몬(San Ramon) 시에 마련해 놓은 자료처리 예비시스템(hot site)을 가동하여 자료를 처리하였다.
- 갱신된 파일은 **예비시스템으로부터** 콜로라도 덴버의 한 회사가 마련한 주전산기에 다운로드하여 데이터베이스를 운용하였다. 이 은행은 단 6일 만에 적체된 미처리 거래를 모두 해결하였다.

소방훈련인가 ? 소방 쇼인가 ?

민방위훈련인가 ? 민방위 쇼인가 ?

❖귀 회사의 ICT 재난대비계획은 위와 같지 않다고 확신하시나요 ?

감사합니다.

질의/응답