

Introduction to BOB



CONTENT



- 01. Introduction**
- 02. Value Chain**
- 03. IT Infrastructure**
- 04. Security Present Condition**



Introduction

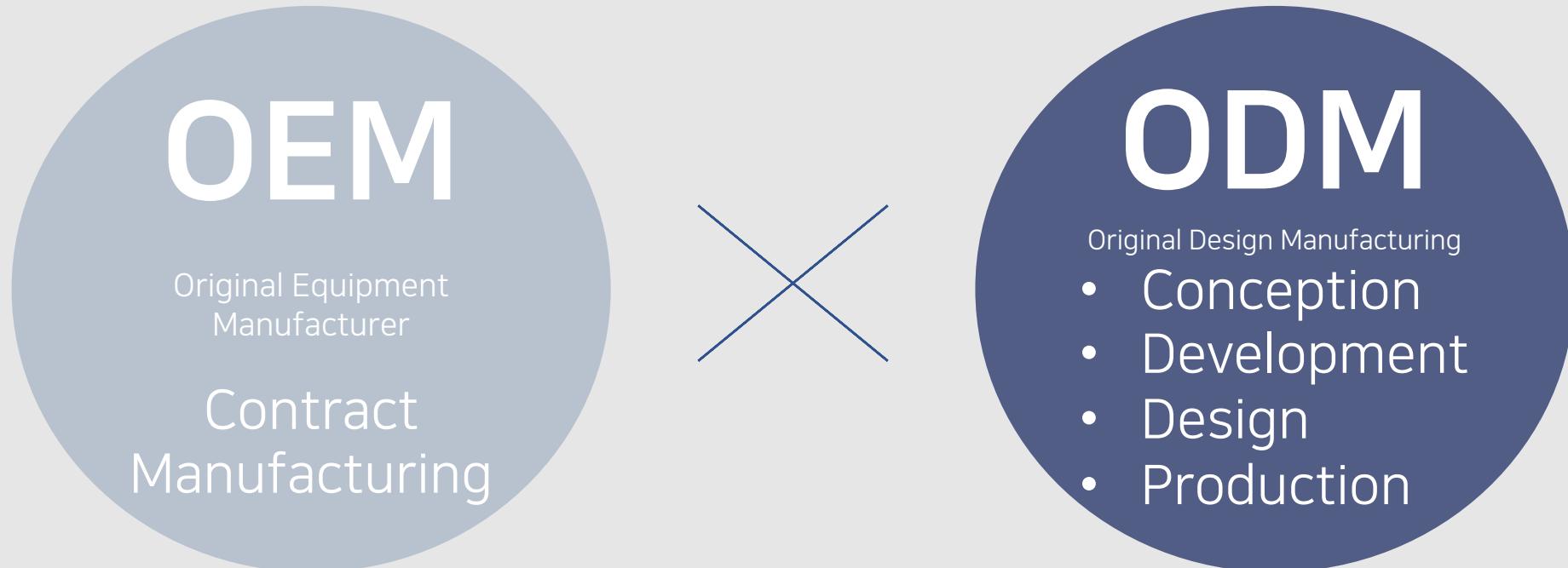
“World First-Class R&D · Manufacturing Company”



BoB Kolmar produces “most loved” **cosmetics** from the customers and is at the center of the fast changing global beauty trends. BoB Kolmar is the **first ODM** in Korea that provides comprehensive end-to-end services from trend identification, product planning, product development, product shipment and to product management.



OEM & ODM



- Similarities: attached trademark of seller, not manufacturer
- Differences **"Has the Manufacturer been involved in product design?"**
 - OEM: Manufacture based on the design of seller; only involved in manufacturing
 - ODM: Manufacturer are responsible for product **development** and production
It has unique technical skills in design and manufacturing and develops research, development and technology accumulation like a company with its own brand.



Total Service From Product Development To Production

- Partner-oriented product development to meet partner's need and for its benefit
- Total marketing service from market research to product & design development by using BoB Kolmar's specialized systems
- Prompt response to risks arisen from changing trends
- Sharing business and technology trends using BoB Kolmar's global network
- Thorough quality control to ensure best quality
- Sharing process know-how from material level to finished product level
- Cost saving through specialized in manufacturing
- Specialty in each technology
- Small quantity batch production



Client companies

Supplies more than 15,000 items annually to about 300 clients in Korea and overseas.

innisfree

Lolita
Lempicka

THEFACESHOP
NATURAL STORY

carverkorea
beauty inventor

LANEIGE

MARY KAY

bareMinerals®
By BARE ESSENTIALS

L' OCCITANE
EN PROVENCE

송염 松鹽

mise
scène
미 장센

L'ORÉAL
PARIS



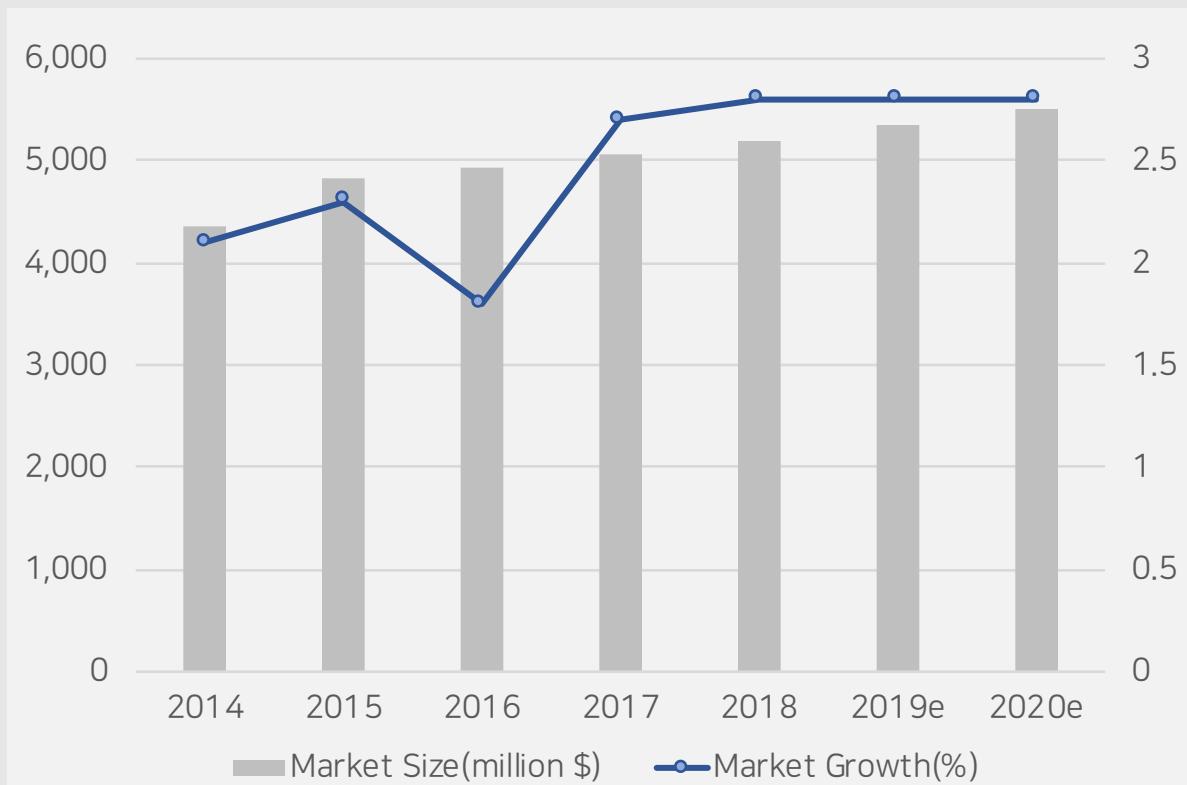
Product List

Type	Detail
Skin care	Toner, lotion, emulsion, cream, essence, pack, mask, cleanser, men's skincare product
Color makeup	BB cream, foundation, skin cover, makeup base, twin cake, powder, lipstick, lip gloss, lip liner, lip care product, blusher, eye shadow, eyebrow product, eye liner
Baby products	Cleanser, bubble bath, soap, shampoo, lotion, cream, oil for baby-use
Hair care	Shampoo, conditioner, 2-in-1 shampoo and conditioner, treatment, tonic, essence, cream, lotion, mousse, spray, temporary hair color, gel, glaze, wax, salon product
Body care	Cleanser, bubble bath, lotion, spray, oil, salon product, hand care product, foot care product, nail product, pedicure product
Perfume	Perfume, eau de perfume, eau de toilette, eau de cologne, shower cologne
Functional cosmetics	Anti-wrinkles, brightening, sunscreen, tanning, complex functional cosmetics
Qusi drug	Hair dye, baby powder, deodorant, acne product, hair removal product, mouth wash, toothpaste Services to offer



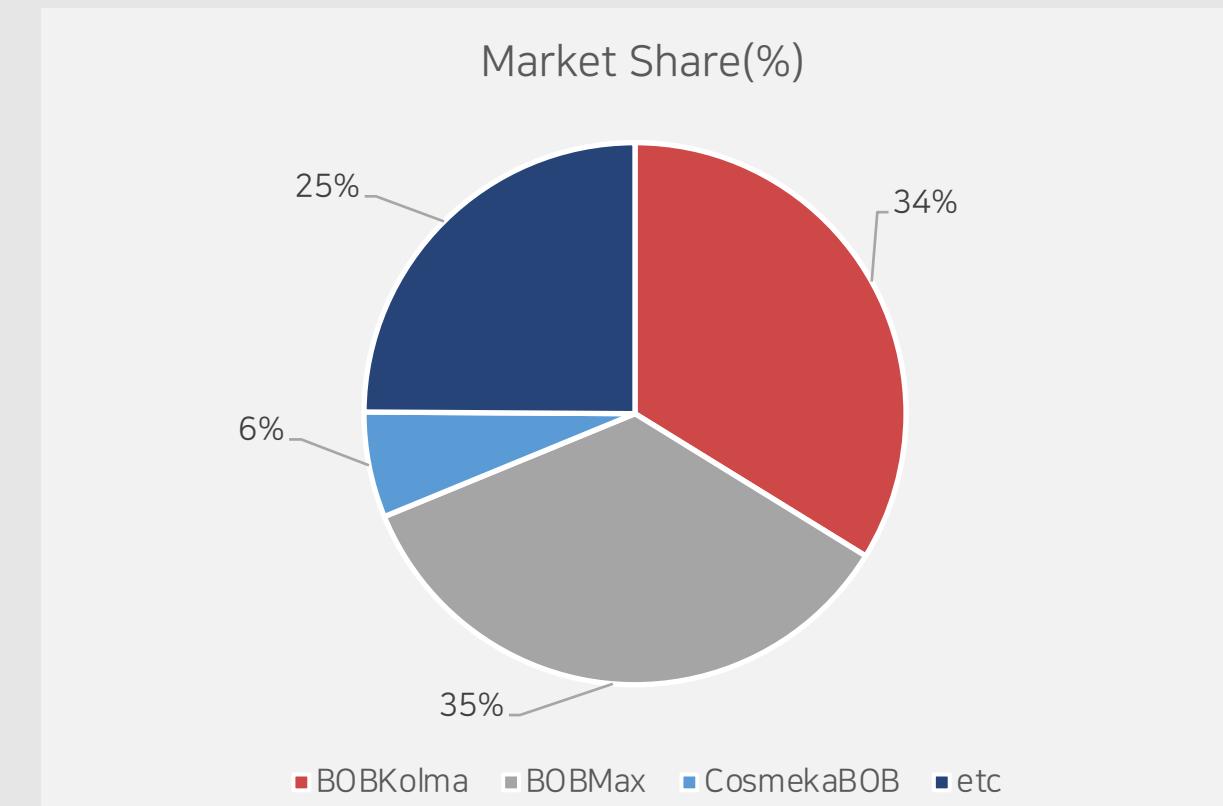
Market Research

1. Global Cosmetic Market Size and Growth Rate



Euromonitor International(2017 Nov)

2. Comparison with 3 Major ODM·OEM



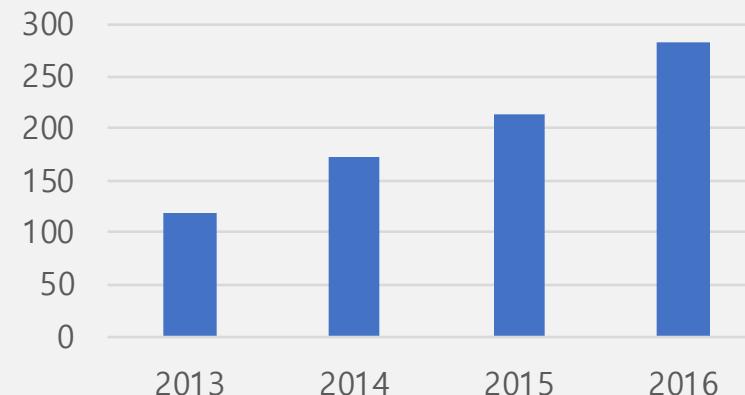
금융감독원(2017)



Business Scale

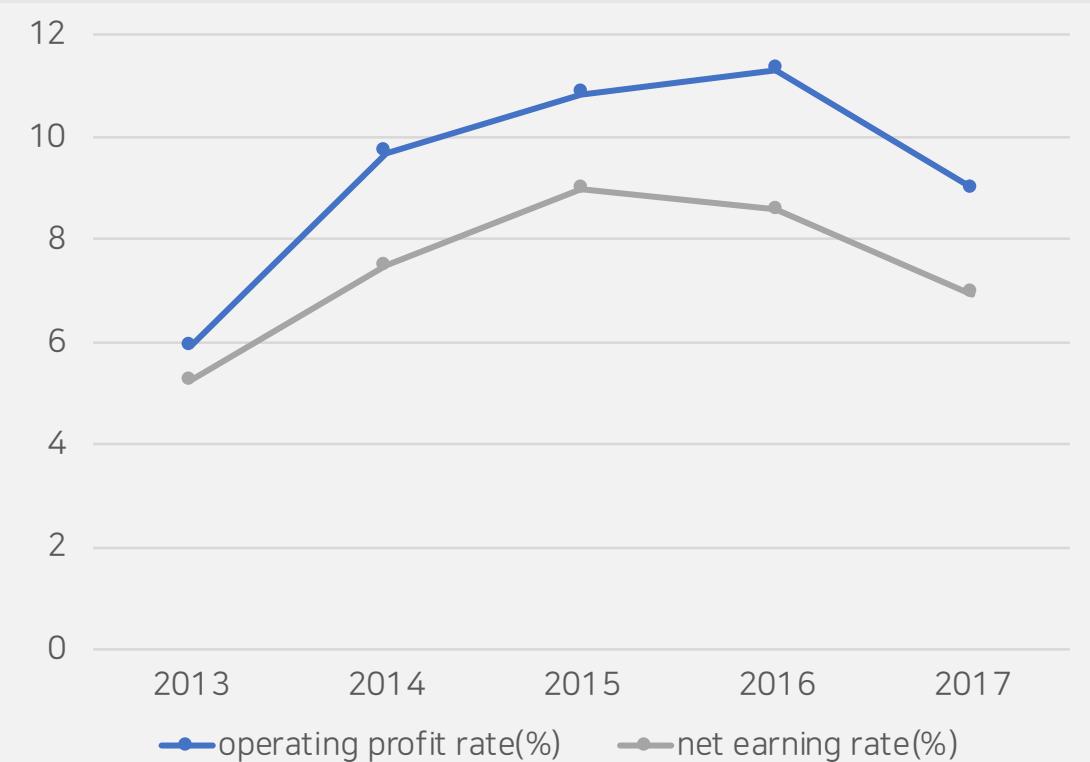
1. Related Information for 2016

- Sales: ₩ 681,624,680,000
- Capital: ₩ 10,552,330,000
- Business profits: ₩ 61,296,270,000
- Change in R&D Investment costs(₩10,000,000)



한국콜마 | 금융감독원, 2016

2. Change in Operating profit rate & Net earning rate

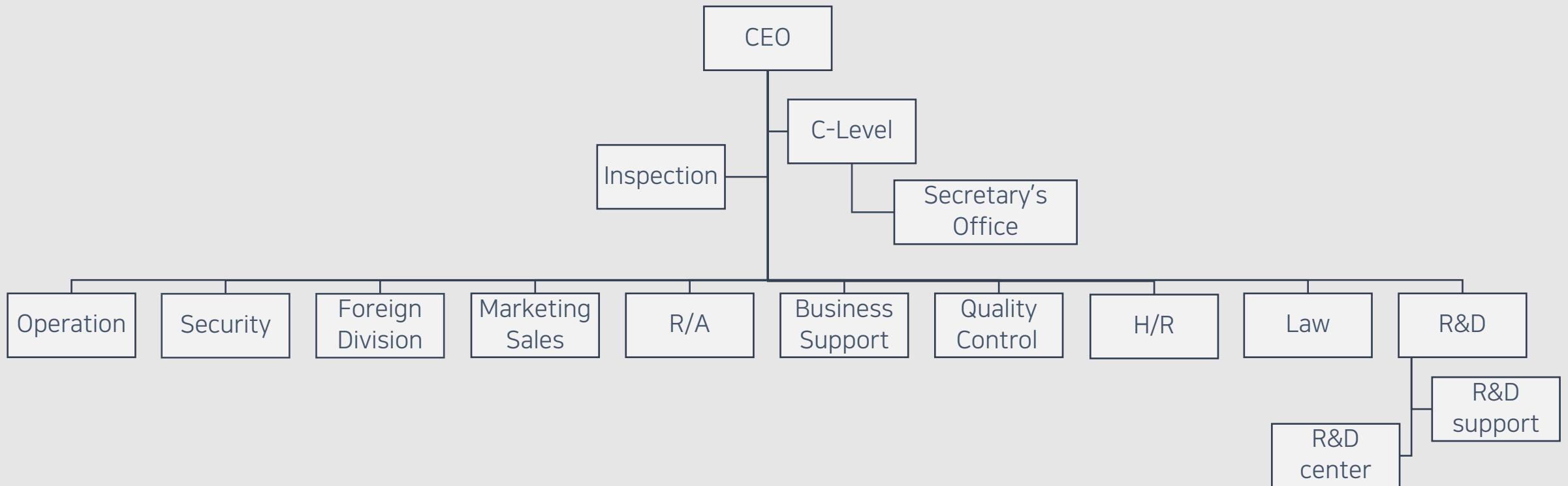


아이투자, 2017



Composition of Organization

Organization Chart



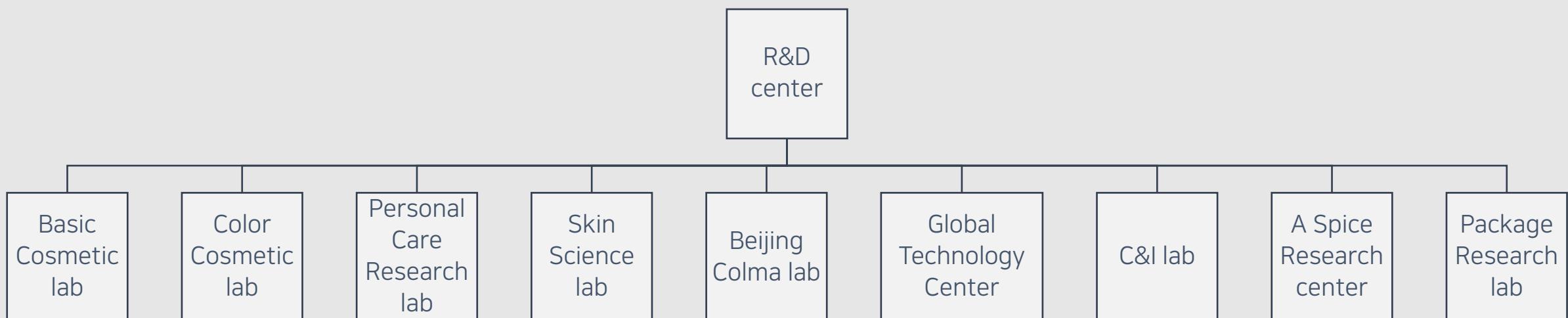
A total of 1,138 employees for 2018



Composition of Organization

R&D Center Organization Chart & Plant List

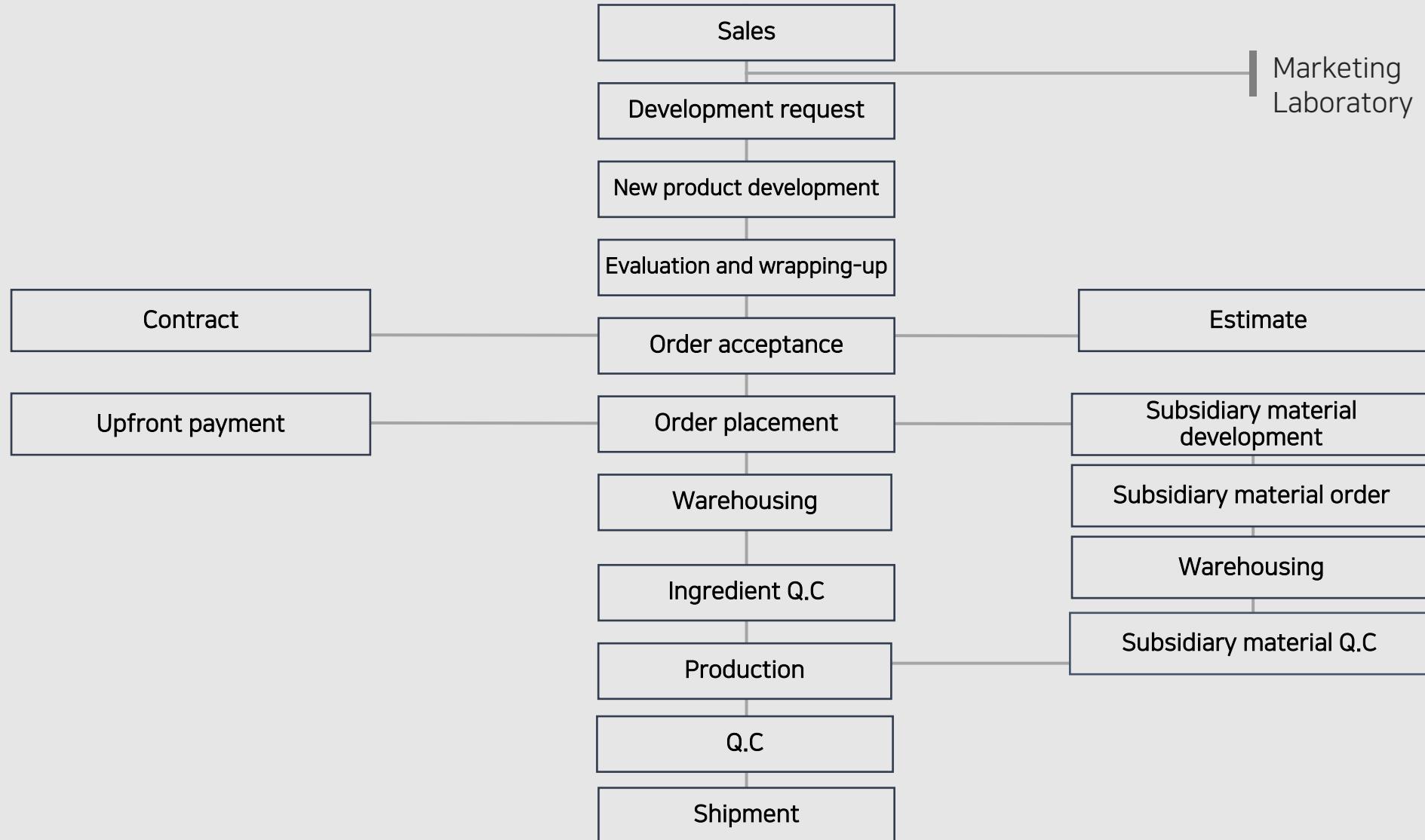
- Skin care manufacturing plant – Sejong, Jeonui, Incheon
- Makeup manufacturing plant – Bucheon, Kyeongin
- Kolmar Cosmetics(Beijing) Limited



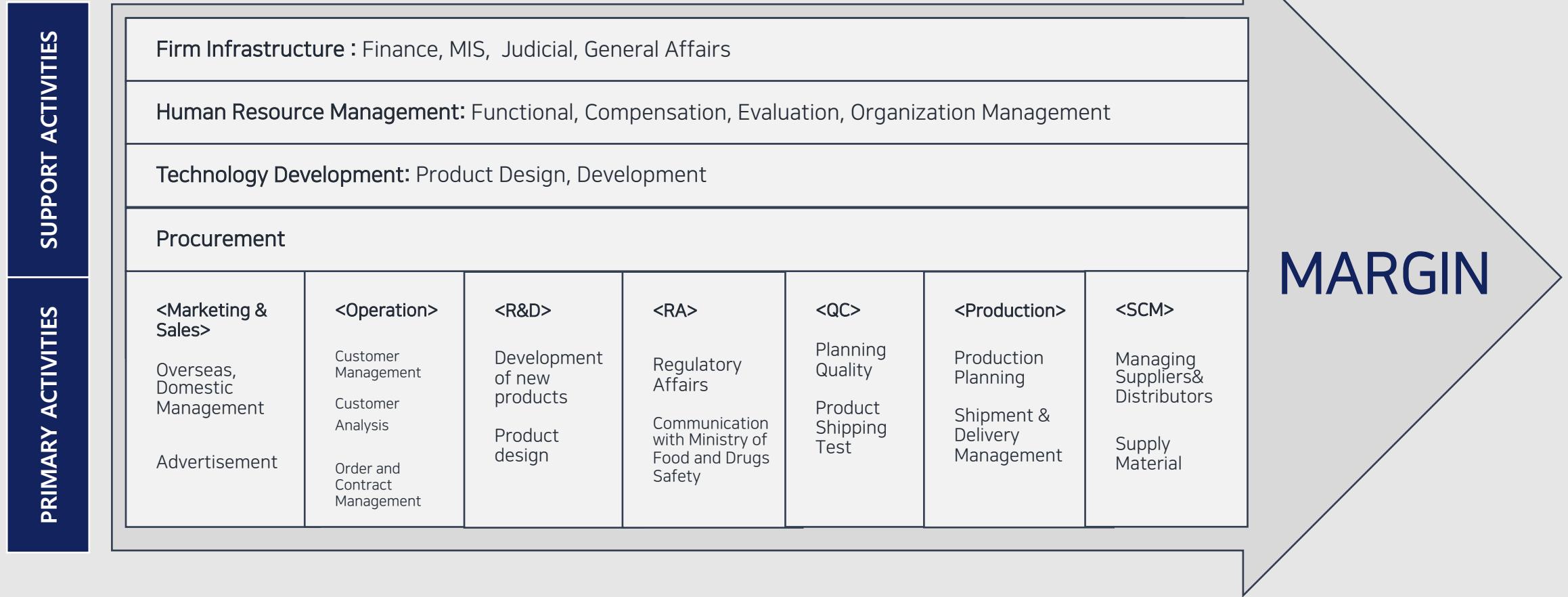
A total of 1,138 employees for 2018



Business Concepts



Value Chain



Classification in SW asset management

NO	Copyright	SW Product Name	Total Number	Period	Contract Date	Expiration Date	Note	Management Number
1	Microsoft	MS Office 2013	793	3 years	17.01.21	20.01.21	Period valid	01-0001 01-0002 01-0003
		Windows Server 2012 R2			17.11.12	20.11.12	Renewal of a contract	
2	Hangul Computer	Hangul 2010	835	-	13.04.06	N/A	Unlimited period	02-0001 02-0002
		Hangul Computer						
3	Adobe	Adobe CS6	1023	-	13.07.08	N/A	Unlimited period	03-0001 03-0002 03-0003
		Adobe CC						
		Adobe Acrobat						
4	Kaspersky	Kaspersky Lab	()	3 years	16.11.01	19.11.01	Period valid / Renewal of a contract	04-0001
5	Avast	Avast Endpoint	30 (Vaccine for servers)	3 years	16.11.01	19.11.01	Period valid / Renewal of a contract	05-0001



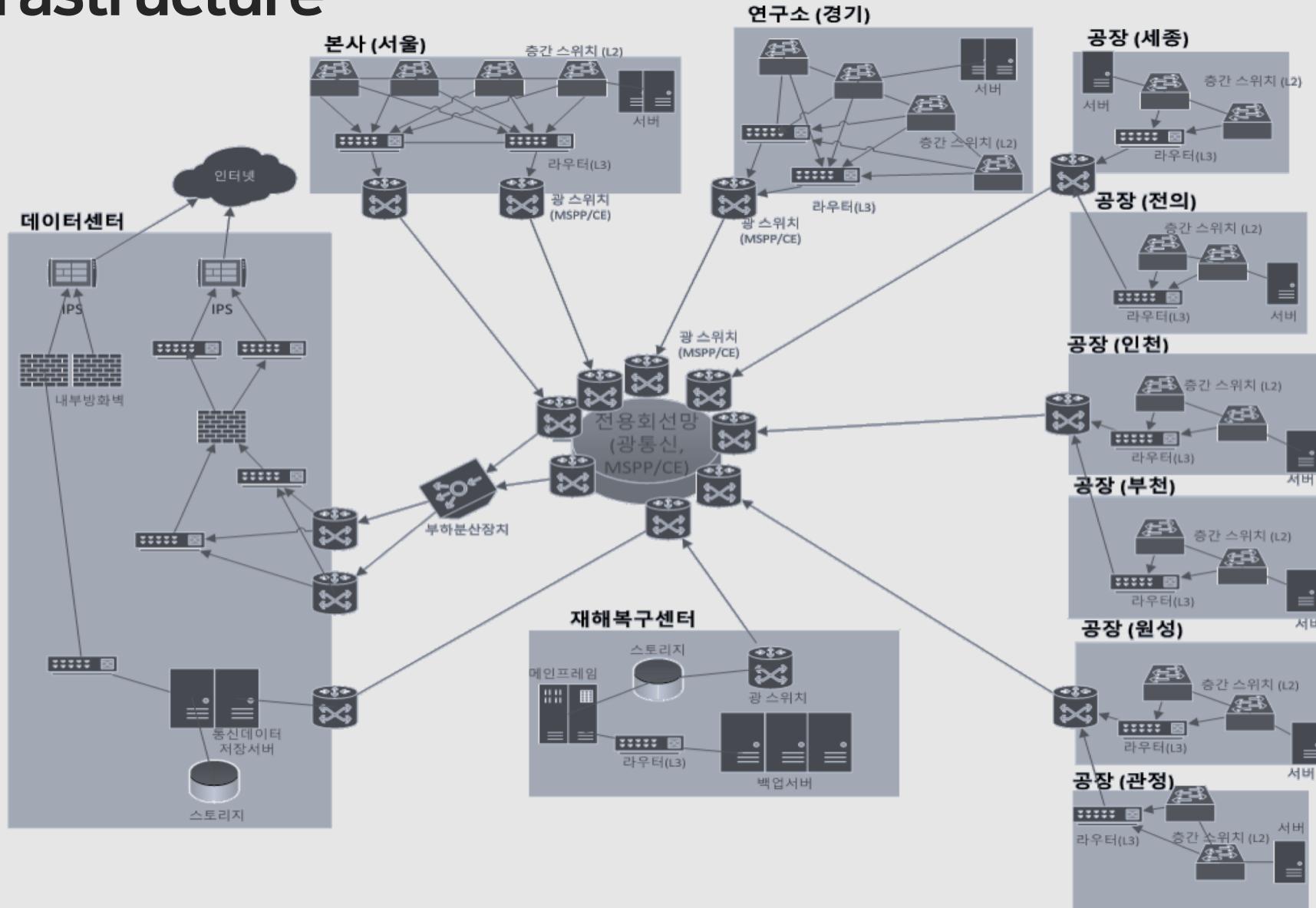
IT Infrastructure

Classification in HW asset management

Category	Detail	Count	Category	Detail	Count
Server	NT	4	Security	Security Device	23
	UNIX	15		VPN	3
	NINUX	3		Security USB	325
	ALX	3		Server Control Device	2
	ASIANLUX	5		DMZ	5
	WINDOWS	6		DB access control device	4
Storage	SAN	6	OA device & PC	DDoS Response Equipment	2
	Storage	3		TMS	3
Backup	Disk	56		Etc.	2
Server Facilities	A thermo-hygrostat	13		Desktop	985
	UPS	8		Monitor	1204
	UPS Battery	12		Laptop	159
	Etc.	3		Printer	104
Network System & Device	Hub	34		Scanner	104
	Gateway	9		Office Machine and PC	96
	Switch	21		OS	982
	Router	28		MS Word	62
	NAC Device	16		MS Excel	23
	Etc.	5		MS Power point	21
Security	Firewall	4	PC Software	Database	8
	Web Firewall	3		Graphics	25
	IDS	3		Video Editor	18



IT Infrastructure





Security Present Condition

Web page for operation team members

The screenshot shows a web browser window with the URL `192.168.2.230/homepage/write.php`. The page has a header with the text "BOB kolmar". On the left, there is a sidebar menu with categories: 공지사항, 영업1팀, 영업2팀, 영업3팀, and 영업4팀. The main content area contains the following form fields:

- Subject: A dropdown menu with three options: 의뢰 현황 (selected), 계약 현황, and 생산 현황.
- Title: A text input field with placeholder text "제목을 입력하시오."
- Author: A text input field containing "bbkolmar".
- Body: A large text area with placeholder text "내용을 입력하시오."
- File Attachment: A file input field with a "파일 선택" button.
- Buttons: A "저장" (Save) button at the bottom left and a footer with links for "쓰기", "삭제", and "로그아웃".

Security Present Condition

List of all related documents

내 드라이브 > BoB 7기 가상기업 4팀 > 관리팀 > 문서 모음	...
이름	▲
■ 1_정보보호조직 구성 및 운영 가이드.pdf	...
■ 2_개인정보처리방침_BoBKolma.pdf	...
■ 3_기술보호_자가진단.pdf	...
■ 4_보안서식.pdf	...
■ 5_보안정책서_BoBKolma.pdf	...
■ 6_보안조직_지침_BoBKolma.pdf	...
■ 7_자산분류_및_평가표.pdf	...
■ 8_재직자용 보안교육 자료책자.pdf	...
■ 9_내부감사지침.pdf	...
■ 10_네트워크 보안 지침.pdf	...
■ 11_물리보안관리지침.pdf	...
■ 12_서버보안지침.pdf	...
■ 13_암호 및 패스워드 관리 정책.pdf	...
■ 14_응용시스템보안지침.pdf	...
■ 15_접근통제지침.pdf	...
■ 16_개인정보처리위탁관련업체점검표.docx	...
■ 17_보안코드.docx	...
■ 18_정보보호교육출석부.pdf	...
■ 19_입사지원서_BoBKolma.docx	...

■ 20_자산도.xlsx	...
■ 21_출입 허가자 명단_BoBKolma.docx	...
■ 22_통제 구역 반출입 관리 대장.docx	...
■ 23_교육평가서.pdf	...
■ 24_이동컴퓨터 보안지침.pdf	...
■ 25_2018 추진계획서.pdf	...
■ 26_인적관리 지침서.pdf	...
■ 27_정보보안 교육계획.pdf	...
■ 28_정보보안위반자 징계지침.pdf	...
■ 29_암호 및 패스워드 관리 정책.docx	...
■ 30_회의록_내부감사지침.docx	...
■ 31_회의록_예산.docx	...
■ 32_회의록_정보보호정책.docx	...
■ 33_회의록_정보보호정책공표.docx	...
■ 34_결재서류_내부감사지침.docx	...
■ 35_결재서류_예산.docx	...
■ 36_결재서류_정보보호정책.docx	...
■ 37_결재서류_정보보호정책공표.docx	...
■ 38_정보보호 관리체계 수립 방법 및 절차.pdf	...

출입허가자 명단					
번호	소속	성명	직위	연락처	사진
1	BoBKolma	허정화	이사	010-1111-1111	
2	BoBKolma	성민석	부장	010-2222-2222	
3	BoBKolma	윤영진	팀장	010-3333-3333	
4	BoBKolma	김만수	사원	010-4444-4444	
5	BoBKolma	임지환	사원	010-5555-5555	

Security Present Condition

List of all related documents

No	증분류	자산 정보				관리자 정보				중요도			보호등급	
		장비명	용도	위치	도입일	관리부서	관리자	담당부서	담당자	유지보수업체	C	I	A	등급
1	방화벽	SonicWall NSA 3500	외부 공격 방어	본사 (서울)	16.03.03	보안 2팀	임지환	서울 지사 전산실	김철수	Dell	2	2	2	나
2	방화벽	SonicWall NSA 3500	외부 공격 방어	연구소 (경기)	16.03.03	보안 2팀	임지환	경기 지사 전산실	김상식	Dell	2	2	2	나
3	방화벽	SonicWall NSA 3500	외부 공격 방어	공장 (세종)	16.03.03	보안 2팀	임지환	세종 지사 전산실	정영준	Dell	2	2	2	나
4	방화벽	SonicWall NSA 3500	외부 공격 방어	공장 (전의)	16.03.03	보안 2팀	임지환	전의 지사 전산실	정만호	Dell	2	2	2	나
5	방화벽	SonicWall NSA 3500	외부 공격 방어	공장 (인천)	16.03.03	보안 2팀	임지환	인천 지사 전산실	김성수	Dell	2	2	2	나
6	방화벽	SonicWall NSA	외부 공격 방어	공장 (부천)	16.03.03	보안 2팀	임지환	부천 지사 전산실	류도현	Dell	2	2	2	나

접근 통제 지침

BOB 풀마

담당자	책임자

접근 통제 지침

201X.XX

BOB kolmar



EH Consulting

Best of Biometrics (BoB)

정보보안 종합 컨설팅 보고

Index

기업 분석



요구사항



프로젝트 착수



진단 결과



위험 분석



결과 보고



01 기업분석

- 기업 개요



- **사업 내용:**

음성 인식을 통한 금융 활동 보조(Alibaba), 지문 인식을 이용한 자동차 개폐 시스템 (Easydoor) 등의 보안기술이 적용된 제품이나 서비스를 제공
생체 인증(Biometrics)을 기반으로 공공부문, 금융부문, 이동 통신부문, 민간부문에
정보보안 및 인증 솔루션을 제공

- **수익모델:**

홍보 및 영업 > 자사 모듈 수주 > 고객 사 맞춤 생체 인증 모듈 & Secure OS 제작
> 제품 발주

02 요구사항

- 관리 보안 요구사항
- 물리 보안 요구사항
- 기술 보안 요구사항

02 요구사항

분야 별 요구사항 내용

기업분석 | 요구사항 | 프로젝트 개요 | 진단 결과 | 위험분석 | 결과보고

관리적 분야

- 관리 책임자 유지
- 보안 서약서 작성 및 유지
- 데이터 분리 저장 및 관리
- 보안 정책서 검토
- 이동식 컴퓨팅 장비 관리
- 접근 통제 관리

물리적 분야

- 출입통제 시스템
- CCTV 관리
- 침입 경보 시스템

기술적 분야

- 침입차단시스템 보안
- 침입탐지시스템 보안
- 침입방지시스템
- 웹 응용프로그램 침입차단 제품(WAF) 보안
- 네트워크 접근통제 제품 보안
- 서버 접근 통제 제품 보안
- 안티바이러스 제품 보안

03 프로젝트 착수

- 프로젝트 내용
- 컨설팅 수행 방법
- 프로젝트 일정

프로젝트 명

- BoB(Best of Biometrics) 정보보안 종합 컨설팅

수행 기간

- 2018년 8월 1일(수) ~ 8월 25일(토)

수행 목적

- BoB(Best of Biometrics)을 대상으로 정보보호 표준을 Issue 사항 파악을 통한 취약점 분석 평가
- BoB(Best of Biometrics)을 대상으로 보안 전반에 대한 가이드 제공을 통한 서비스 신뢰도 확보
- BoB(Best of Biometrics) 웹 어플리케이션 및 웹 서버 취약점 점검을 통한 대응방안 수립

BOSSCM (Business Optimized Security System)

Why?

- EH Consulting에서 자체 개발한 BOSSCM(Business Optimized Security System) 방법론은 ISO27001, Gartner 보안 모델, 정보통신기반 시설, KISA ISMS 모델들의 장점과 EH Consulting의 컨설팅 수행 경험을 토대로 완성
- 주로 적용되는 경우
 - 중견 기업 및 기관 이하 규모로서 보안 전담 인력이 1-2명 이하인 경우
 - 보안 관련하여 일부 투자나 수행이 이루어지고 있으나 보안 전반을 점검해보고 싶은 기업 또는 기관
 - 정보보호 전문 컨설팅은 받아보지 않은 기업으로 보안에 의지가 있는 기업 또는 기관



수행 단계



- | | | | |
|-----------|------------|---------|-------------|
| • 의뢰/회의 | • 웹 취약점 진단 | • 위험 분석 | • 출입통제 시스템 |
| • 일정 수립 | • 네트워크 진단 | | • CCTV 관리 |
| • 기업 분석 | • 물리 보안 진단 | | • 침입 경보 시스템 |
| • 요구사항 분석 | • 정책 진단 | | |
| • 범위 정의 | | | |

03 프로젝트 착수

- 기업분석 | 요구사항 | 프로젝트 개요 | 진단 결과 | 위험분석 | 결과보고

04 진단 결과

- 관리 체계 진단
- 물리 진단
- 웹 서버 진단
- 네트워크 진단

- ✓ 총 42개 체크리스트 진단 항목 중 16개 취약 항목 발견

NO	중항목	진단항목	비고
1		보안 책임자 지정 여부	보안 조직 지침서에 보안 책임자의 역할은 명시되어 있지만 보안책임자 지정관련 항목 부재
2	관리책임자 유지	보안관리자의 지정 여부	보안 조직 지침서에 보안 관리자에 관련 항목 부재
3		보안담당자 지정 여부	보안 조직 지침서에 보안 담당자의 역할은 명시되어 있지만 보안담당자 지정관련 항목 부재
4		시험데이터 관리 절차	
	데이터 분리 저장 및 관리		시험 데이터 관련 정책 부재
5		시험데이터 기술적 보호조치 수립	
6	보안 정책서 검토	임직원 및 관련자의 보안정책서 이해	인터뷰 결과 이해하고 있지 않은 직원 확인

✓ 총 21개 체크리스트 진단 항목 중 9개 취약 항목 발견

NO	진단 항목	비고
1	보호구역 설정	보호구역 설정 보호구역은 제한지역, 제한구역, 통제구역에 따라 보호, 관리하는 정확한 지침이나 방침이 없음
2	사무실 및 설비 공간	사무실 및 설비 공간의 물리적 보호 취약
3	환경 위협	외부 환경 위협으로부터 보호되고 있는 지침/방침이 없고, 재해 시 대비할 장비와 방침이 갖춰지고 있지 않음
4	비상 전원장치 부족	중요 인프라 (연구팀, DMZ 서버실)의 재해 시 비상 전원공급 (UPS) 장치 부족
5	중요 시설 표시	중요 인프라 (서버)에 대한 중요 시설임을 나타내는 표시부족
6	장비 반출입 과정	현재 장비 반 출입 과정에 대한 승인절차 및 방침을 처리하고 있지 않음
7	장비의 폐기 및 재사용	저장매체를 가지고 있는 장비의 폐기 및 재사용 시 점검 부족
8	CCTV 케이블 외부 노출	CCTV 케이블은 외부에서 접근할 수 없도록 천장을 통해 관리하여야 하지만, 특정 구간 외부로 노출
9	케이블 점검 부족 및 접촉불량	네트워크 장비의 물리적 케이블 점검 부족으로 인한 접촉불량

- ✓ 총 26개 체크리스트 진단 항목 중 8개 취약 항목 발견

NO	진단 항목	비고
1	정보 누출	존재하지 않는 주소 입력 뒤 에러문이 출력되는 것을 확인 가능
2	악성 콘텐츠	아이디를 스크립트 문으로 가입한 뒤 검색 기능 시 악성 콘텐츠 실행 가능
3	약한 문자열 강도	Burp Suite를 이용하여 반복적인 로그인 시도에 대한 제한이 없다는 것을 확인, 확인 결과 아이디 값이 코드에 저장되면서 공격 가능
4	XSS	아이디를 스크립트문으로 가입한 후 검색 기능 시 취약점 발현
5	불충분한 세션 만료	로그아웃을 하지 않으면 특정 시간이 지난 뒤에도 해당 세션을 이용하여 접근할 수 있는 것을 확인
6	관리자 페이지 노출	손쉽게 유추 가능한 관리자 페이지가 있는 것을 확인
7	데이터 평문 전송	비밀번호와 같은 민감한 데이터 전송 시에 암호화 되지 않는 것을 확인
8	자동화 공격	회원가입을 자동화 시켜주는 프로그램을 제작 후 실행 시 취약점이 발현 여부 확인

- ✓ 총 31개 체크리스트 진단 항목 중 9개 취약 항목 발견

NO	진단 항목	비고
1	네트워크 망 구조적 문제	전반적 네트워크 망 구조적 문제점
2	방화벽 설정	방화벽이 명시적으로 허용된 서비스를 제외한 모든 서비스를 거부하는 설정 미흡
3	비상 전원공급 문제	중요 인프라 (연구팀, DMZ 서버실)의 재난시 비상 전원공급 (UPS) 장치 부족
4	Ping 공격	중요 인프라 (서버)에 대한 Ping 공격 취약 → 특정 IP만 접근하도록
5	악성 소프트웨어	악성 소프트웨어 (P2P, 백도어, 등) 발견
6	회선 구간 문제	네트워크 내부망 특정 회선 구간 지연
7	중복 IP 문제	동일 Subnet 마스크에서 운영중인 IP 중복 문제로 인한 네트워크 통신 지연
8	Port 개방 문제	불필요한 Port 개방으로 인한 위협 문제
9	케이블 점검 부족 및 접촉불량	네트워크 장비의 물리적 케이블 점검 부족으로 인한 접촉불량

05 위험분석

- 위험도 점수 및 평가 기준
- 점수 별 위험 등급
- 분야 별 자산 중요도
- 분야 별 위험 분석 결과

취약점 점수
(상중하로 구분)

자산 중요도 점수

$$\text{위험도} = \text{자산 중요도} \times \text{취약점 점수} / 10$$

10~7

지체 없이 조치 필요

High

6~4

빠른 시일 내에 조치 필요

Middle

3~2

보안 조치 필요

Low

1

위험 수용

DOA

영향	보안 위협 진단 평가에 대한 기준	점수
최소한의 보안 요구사항 미충족	내,외부자로부터의 심각한 보안사고가 발생할 가능성이 높은 경우	10
	내,외부자로부터의 심각한 보안사고가 발생할 가능성이 있는 경우	9
주요 서비스의 상실 또는 저하 (정보가 유출되지 않은 경우)	회사가 반드시 필요한 서비스가 작동하지 않을 경우	8
	회사가 반드시 필요한 서비스가 비정상적으로 작동 하는 경우	7
보조 서비스의 상실 또는 저하	회사에서 편의를 위해 제공하는 서비스가 작동하지 않는 경우	6
	회사에서 편의를 위해 제공하는 서비스가 비정상적으로 작동하는 경우	5
고객 불편	관련 분야에 고객에 의해 인지되는 경우(> 75%)	4
	관련 분야에 고객에 의해 인지되는 경우(> 50%)	3
	관련 분야에 고객에 의해 인지되는 경우(> 25%)	2
영향 없음	인지할 수 있는 영향 없음	1

NO	자산명	용도	개수	CIA	NO	자산명	용도	개수	CIA
1	x3655 B5 A5-2630V3(32GB)	웹	1	9	19	FQ17V8DWA2	에어컨	2	5
2	x3652 H5 E5-2630J3(32GB)	DB	1	9	20	던게이트	출결/근태	2	5
3	CISCO Firepower 4100 Series	웹 방화벽	4	7	21	XIAOMI-JTYJ	지능형 화재 감지기	2	5
4	CISCO IPS 4520 Sensor	IPS	1	7	22	MP-038-22	보안/안전용 CCTV	10	6
5	CISCO Firepower 9000 Series	웹 방화벽	1	7	23	보안정책서	정책서	1	-
6	CISCO SG220-26-K9-EU	L2 Switch	6	7	24	보안 조직지침	지침서	1	-
7	CISCO SF300-48	L3 Switch	1	5	25	개인 보안지침	지침서	1	-
8	CISCO Linksys E1200	라우터(WiFi)	4	9	26	개인정보처리방침	방침문	1	-
9	CISCO SG220-26-K9-EU	L2 Switch	4	8	27	기술보호자가진단	진단표	1	-
10	CISCO SF300-48	L3 Switch	3	9	28	네트워크 보안지침	지침서	1	-
11	CISCO Linksys E1200	라우터(WiFi)	1	7	29	보안 서약양식	서약서	1	-
12	CISCO SF300-48	L3 Switch	1	7	30	서버 보안지침	지침서	1	-
13	CISCO Firepower 4100 Series	방화벽	4	7	31	응용시스템 보안지침	지침서	1	-
14	CISCO IPS 4520 Sensor	IPS	1	5	32	이동컴퓨터 보안지침	지침서	1	-
15	DLT IR2025	DLT(백업용)	1	9	33	인적관리 지침	지침서	1	-
16	x3650 M5 E5-2630V3(32GB)	연구용 서버	2	9	34	접근통제 지침	지침서	1	-
17	MINI-DC-UPS/24DC/2	UPS	1	6	35	정보보안위반자 징계지침	지침서	1	-
18	ISG7600EX	비상긴급발전기	2	5	36	정보보호 교육수행	지침서	1	-

- 관리체계 취약점 위험 분석 결과

NO	진단 항목
1	관리 책임자 유지
2	보안 서약서 작성 및 유지
3	데이터 분리 저장 및 관리
4	보안정책서 검토
5	이동 컴퓨터 보안지침
6	접근통제점검

- 웹 서버취약점 위험 분석 결과

NO	진단 항목	점수	위험도 등급
1	정보 누출	3	Low
2	악성 콘텐츠	8	High
3	약한 문자열 강도	6	Middle
4	XSS	8	High
5	불충분한 세션 만료	4	Middle
6	관리자 페이지 노출	5	Middle
7	데이터 평문 전송	4	Middle
8	자동화 공격	8	High

• 물리 취약점 위험 분석 결과

NO	진단 항목	점수	위험도 등급
1	보호구역 지정	4	Middle
2	보호설비	5	Middle
3	보호구역 내 작업	4	Middle
4	출입통제	4	Middle
5	모바일기기 반출입	5	Middle
6	케이블 보안	5	Middle
7	시스템 배치 및 관리	1	Low
8	개인업무 환경 보안	2	Low
9	공용업무 환경 보안	4	Middle

• 네트워크 취약점 위험 분석 결과

NO	진단 항목	점수	위험도 등급
1	네트워크 망 구조적 문제	5	Middle
2	방화벽 설정	5	Middle
3	비상 전원공급 문제	5	Middle
4	Ping 공격	6	Middle
5	악성 소프트웨어	9	High
6	회선 구간 문제	2	Low
7	중복 IP 문제	1	Low
8	Port 개방 문제	4	Middle
9	케이블 점검 부족 및 접촉 불량	4	Middle

06 결과 보고

- 관리체계 컨설팅 결과
- 물리보안 컨설팅 결과
- 기술보안 컨설팅 결과

No	진단항목	조치 방법
1	보안관리자가 지정되어 있는가?	기존에 보안책임자가 겸임하였으나, 보안관리자를 지정하도록 조치
2	부서별 보안담당자가 지정되어 있는가?	부서별 팀장이 보안업무를 겸임하였으나, 부서별로 보안담당자를 지정하도록 조치
3	보안관리위원회 구성원은 적절한가?	보안관리위원회 구성원을 각 임원들과 조치된 보안관리자와 보안담당자까지 확장
4	시험 데이터의 관리 절차가 수립되어 있고 이행되는가?	시험 데이터의 관리 절차는 수립되어 있으나, 이행할 수 있도록 별도의 조치방안 제안
5	시험 데이터의 기술적 보호조치가 수립되어 있고 이행되는가?	별도의 시험 데이터의 기술적 보호조치 방안 제안
6	모든 임직원 및 관련자는 보안정책서를 이해하고 있는가?	모든 임직원과 관리자들이 보안정책서를 이해 및 숙지하도록 조치
7	필요한 경우 특정시스템 또는 서비스에 대한 정보보호 정책이 수립되어 있는가?	특정시스템과 서비스에 대한 정보보호 정책을 수립하도록 제안
8	각 장비의 승인을 정상적으로 받은 후 외부 지역에서 사용하는가?	(붙임7)과 같이 “이동 컴퓨팅 장비 사용 및 도입 승인 신청서”를 통하여 장비 승인을 받고 사용하도록 조치

No	진단항목	조치 방법
9	모든 이동 컴퓨팅 장치는 분실, 도난, 훼손에 대비해 적절한 보험에 가입해 두었는가?	이동 컴퓨팅 장치를 사용 시 분실, 도난, 훼손에 대비하기 위해 적절한 보험에 가입하도록 제안
10	장비를 사용하는 장소의 위험을 잘 파악하고 추가적인 보안조치를 취하는가?	장비를 사용할 때 장소의 위험을 파악 후 사용하도록 제안
11	“비밀” 정보 접근 시 승인절차 점검이 잘 이루어지고 있는가?	(붙임 8)과 같이 “비밀” 정보에 접근 하기 위한 사용자 등록 신청서”를 통해서 승인절차를 잘 이행하도록 제안
12	정보 자산을 주어진 기준에 따라 분류하여 철저히 검사를 하고 있는가?	정보 자산을 공개, 대외비, 비밀 등급으로 분류하도록 제시하였고, 각 등급별로 점검절차 마련할 것을 권고
13	각 사용자 별로 필요 권한 외 권한 부여 확인하고 있는가?	각 사용자 별로 자신의 접근권한 외의 권한을 해제하도록 권고
14	모든 사용자 접근 권한은 적어도 6개월에 1회 이상 검토되고 있는가?	6개월에 1회 이상 접근 권한을 점검할 것을 권고
15	변화가 생겼을 경우 관련된 사용자 권한은 즉시 검토되고 있는가?	권한에 대한 변화가 생겼을 경우 사용자 권한을 즉시 점검하고 검토할 것을 권고
16	모든 특권적인 접근 권한은 적어도 매 3개월마다 검토되고 있는가?	3개월마다 특권적인 접근 권한을 점검하도록 권고

개정 목록

- 인적 관리 지침서

신설 목록

- 보안 조직 지침서
- 시험 데이터 지침서
- 조직도
- 사용자 계정 등록 대장
- 정보보호조직원 직무 기술서
- 이동 컴퓨팅 사용 및 도입 승인 신청서
- 사용자 등록 신청서

No.	진단 항목	조치 방법		
		서버	장비	코드
1	정보 누출	Setting.py에서 debug = false로 변경	N/A	<ul style="list-style-type: none"> - 불필요한 주석 제거 - 디버깅 메시지 존재
2	악성 콘텐츠, XSS	N/A	입력 값 중 사용 하지 않는 태그나 스크립트 언어에 대하여 룰셋 지정	<ul style="list-style-type: none"> - 입력 값 중 사용 하지 않는 태그나 스크립트 언어에 대하여 필터링 필요 - 사용자가 입력한 값을 출력 시 검증 필요
3	약한 문자열 강도	N/A	짧은 시간에 같은 기능을 비정상적으로 반복 하는 패킷에 대하여 룰셋 지정	<ul style="list-style-type: none"> - 약한 문자열 강도 공격이 가능한 페이지에 서 횟수 제한 필요 - 회원 가입시 패스워드 길이만 검사 특수문자 , 숫자 , 영어 포함한 8자 이상 필요
4	불충분한 세션 만료	세션 만료 기간 재지정 필요	N/A	<ul style="list-style-type: none"> - 모든 호스트 연결을 허용하고 있음. 허용 IP 지정 필요
5	관리자 페이지 노출	N/A	특정 IP에 대하여 접속을 제한하고 싶다면 관리자 페이지의 접근자에 대한 필터링 필요	<ul style="list-style-type: none"> - 관리자페이지 URL이 ADMIN으로 설정되어 있음
6	데이터 평문 전송	SSL를 적용하는 것을 권고	N/A	<ul style="list-style-type: none"> - 민감한 데이터 전송 시 암호화

No	위험요소	대응책
1	보호구역 설정	보호구역 (제한지역, 제한구역, 통제구역)에 대한 지침이나 방침 설정
2	사무실 및 설비 공간	사무실 및 설비 공간의 물리적 보호 방안 제시
3	환경 위협	외부 환경 위협으로부터 보호되고 있는 지침이나 방침이 없고, 재해 시 대비할 장비와 방침이 갖춰지고 있지 않음 → 재해 설비 구축
4	비상 전원장치 부족	중요 인프라 (연구팀, DMZ 서버실)의 전원 공급량에 맞춰 비상 전원공급 (UPS) 장치 설치
5	중요 시설 표시	중요 인프라 (서버)에 대한 중요 시설임을 나타내는 표시 작성
6	장비 반출입 과정	현재 장비 반 출입 과정에 대한 승인절차 및 방침 제안
7	장비의 폐기 및 재사용	저장매체를 가지고 있는 장비의 폐기 및 재사용 방침 제안
8	CCTV 케이블 외부 노출	외부로 노출된 CCTV 케이블에 대한 배선작업을 수행
9	케이블 점검 부족 및 접촉불량	네트워크 보안 기술적 진단 보고서 하단 부분에 케이블 점검 방법 및 주기 명시

No	위험요소	대응책
1	네트워크 망 구조적 문제	현재 내부망에서만 통신하는 구간에 총 3대의 방화벽이 설치 → 개발, 연구, 지원팀의 방화벽 1개로 통일하고, 망을 합쳐 L3 Switch를 경유하도록 조치
2	방화벽 설정	방화벽이 명시적으로 허용된 서비스를 제외한 모든 서비스를 거부하도록 재 설정
3	비상 전원공급 문제	중요 인프라 (연구팀, DMZ 서버실)의 전원 공급량에 맞춰 비상 전원공급 (UPS) 장치 설치
4	중요 인프라에 대한 Ping 공격	개발팀의 특정 IP만 중요 인프라에 접근하도록 설정, 연구팀 또한 마찬가지
5	악성 소프트웨어	업무 외적인 악성 소프트웨어 (P2P, 백도어, 등) 삭제
6	회선 구간 문제	네트워크 내부망 전체적 케이블 회선 점검 실시
7	중복 IP 문제	Nbtstat 명령어로 중복되는 IP 전부 추적하여 재할당
8	Port 개방 문제	불필요한 Port를 사용하고 있다면, 이는 외부 해킹이나, 트로이목마로 등으로 의심해볼 수 있다. 널 세션 차단, 윈도우 관리목적의 기본 공유 폴더 제거, netbios 관련 서비스 해제
9	케이블 점검 부족 및 접촉불량	네트워크 보안 기술적 진단 보고서 하단 부분에 케이블 점검 방법 및 주기 명시

 03.프로젝트 일정표.xlsx	2018-08-25 오후...	Microsoft Excel ...	17KB
 04.프로젝트 계획서.docx	2018-08-22 오전...	Microsoft Word	531KB
 05.기업 분석서.docx	2018-08-21 오후...	Microsoft Word	654KB
 06.점검 목록별 자산목록 분리 현황.xlsx	2018-08-13 오전...	Microsoft Excel ...	355KB
 07.요구사항 분석서.docx	2018-08-13 오후...	Microsoft Word	37KB
 13.웹 취약점 진단 계획서.docx	2018-08-25 오후...	Microsoft Word	67KB
 13.웹 취약점 진단_체크리스트.docx	2018-08-25 오후...	Microsoft Word	19KB
 14.웹 취약점 점검 보고서.pdf	2018-08-25 오후...	Chrome HTML D...	856KB
 16.네트워크 진단 계획서.docx	2018-08-25 오후...	Microsoft Word	59KB
 16.네트워크 진단_체크리스트.docx	2018-08-25 오후...	Microsoft Word	16KB
 19.풀리보안 진단_체크리스트.docx	2018-08-25 오후...	Microsoft Word	18KB
 19.풀리보안 진단 계획서.docx	2018-08-25 오후...	Microsoft Word	55KB
 20.네트워크 진단 보고서.docx	2018-08-25 오후...	Microsoft Word	731KB
 20.풀리보안 진단 보고서.docx	2018-08-25 오후...	Microsoft Word	30KB
 22.관리체계 진단 계획서.docx	2018-08-25 오후...	Microsoft Word	46KB
 22.관리체계 진단_체크리스트.docx	2018-08-25 오후...	Microsoft Word	24KB
 23.관리체계 진단 보고서.docx	2018-08-25 오후...	Microsoft Word	75KB
 24.위험 분석 계획서.docx	2018-08-25 오후...	Microsoft Word	78KB
 25.위험 분석 및 평가 보고서.docx	2018-08-25 오후...	Microsoft Word	105KB
 27.보안 대책서.docx	2018-08-25 오후...	Microsoft Word	166KB
 사용자등록 신청서.hwp	2018-08-25 오후...	한컴오피스 한글 ...	16KB
 이동 컴퓨팅 장비 사용 및 도입 승인 신...	2018-08-25 오후...	한컴오피스 한글 ...	16KB
 자산평가인정부일지.docx	2018-08-12 오후...	Microsoft Word	18KB

Q&A

THANK YOU FOR LISTENING

THANK YOU