

Objectives of Chofn IP information security project

Data Type	Example	Definition
Personal info	Employee personal info, cvs, etc.	Data pointing to a natural person; Data one's not willing to open.
Key Asset Info	Source code, consultancy solutions, etc.	Information asset that has great commercial value, that makes the company at competitive advantage, that have great effects on business model and product development.
Business Secret	COntacts, compensations, cost&profits	Unpublished technical and business data that can bring commercial benefits to the right holder, and have practicality and taken confidential measures
Sensitive info	Technical disclosure, unpublished patent applications, etc.	Data that has a material adverse effect on the data owner after unauthorized access, Leakage

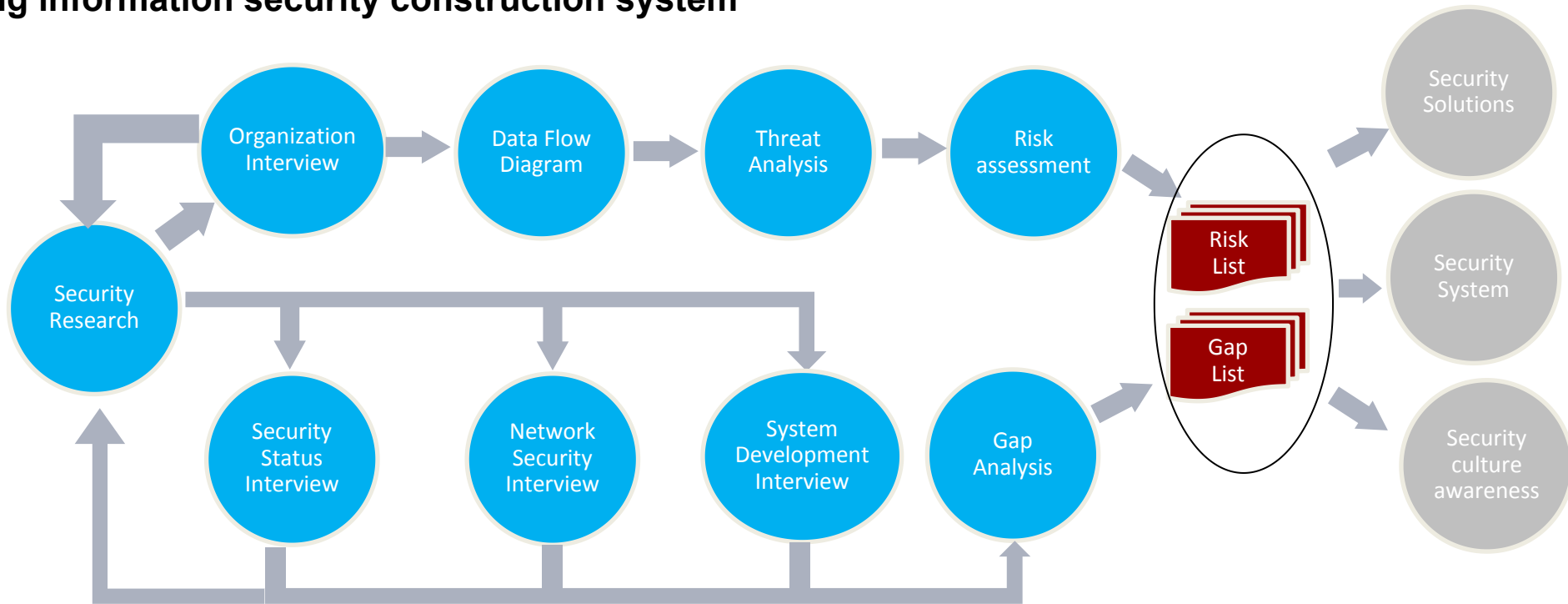
- Different companies pays different attention to data security, different stages of company have different strategy
- To Chofn IP, our management has now understood that given our size, achieving growth is not a problem; The focus should be put on docketing procedure, risk management and sustainability

Overall Objective

To protect client's core technology secrets and trade secrets

Project implementation mind map

Research on the company's current situation, focusing on threat modeling, supplemented by gap analysis, identifying security system design requirements list, matching technology and management tools, and improving information security construction system



- Threat modeling: Business process analysis through data perspective
- Gap identification: Comparing management, network and business system security to best practice, and produce key gap list.
- Technical approach: Network management (VPN or physical isolation), permission management (DLP, business system permissions)

Solution Plan

Building Security Boundaries

- **Seperation of internal and external network**

Protection against external attacks and prevent internal unintentional disclosure

- **Intranet partition management**

Building data security management system and matching security strategy for different business nature

- **Outer net + Physical Media + Email + IM Software DLP control**

Implement different management strategies on each port through the DLP (data loss prevention) tool

Permission Management

- **IAM unified identification**

Centralized management of logins and permissions

- **Authority management**

Through job requirements and responsibilities, setting the data security permissions of the confidential info, landing on DLP

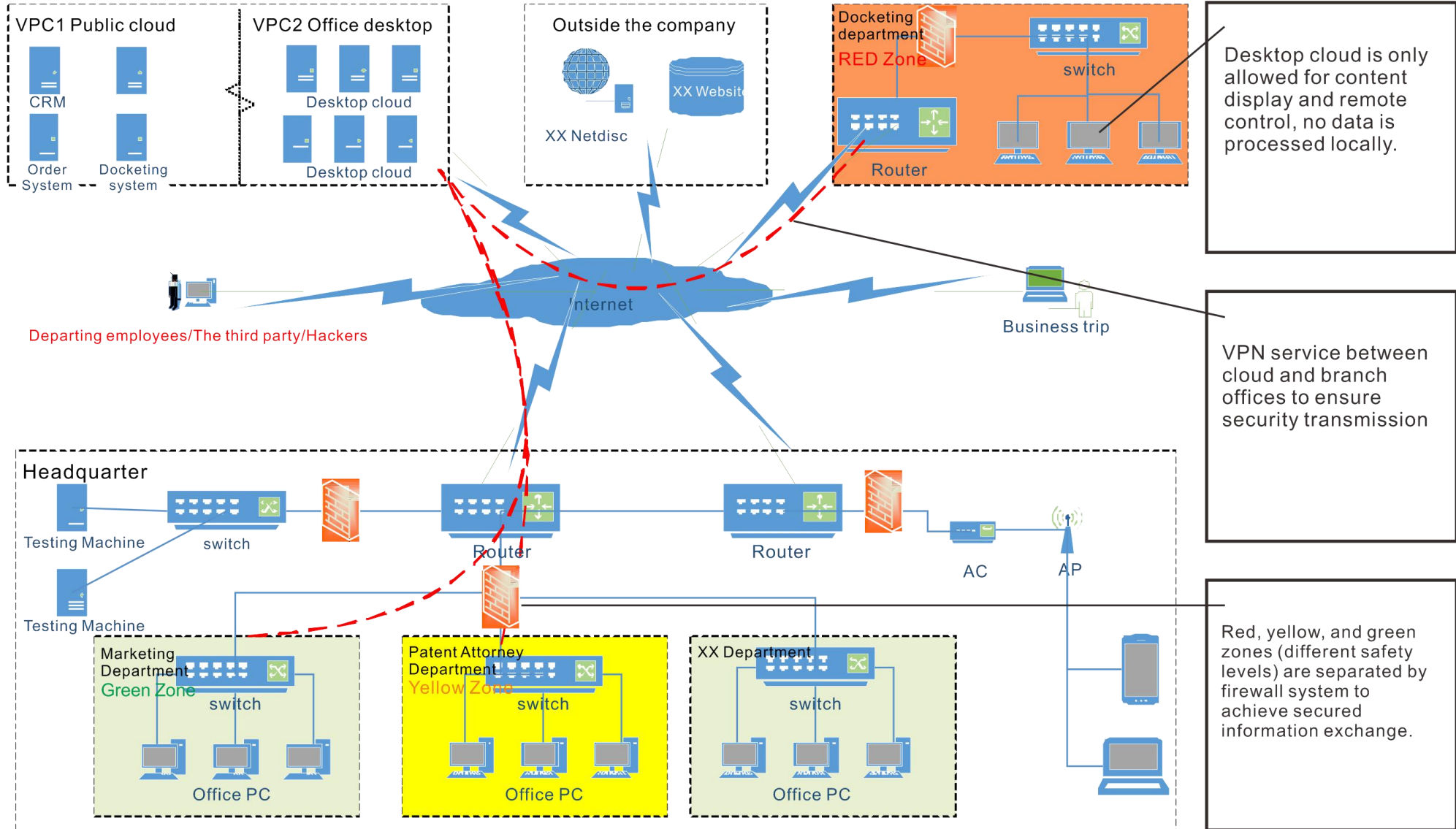
Operation Upgrade - Ernst & Young System and culture

- **Improving management and supervision**

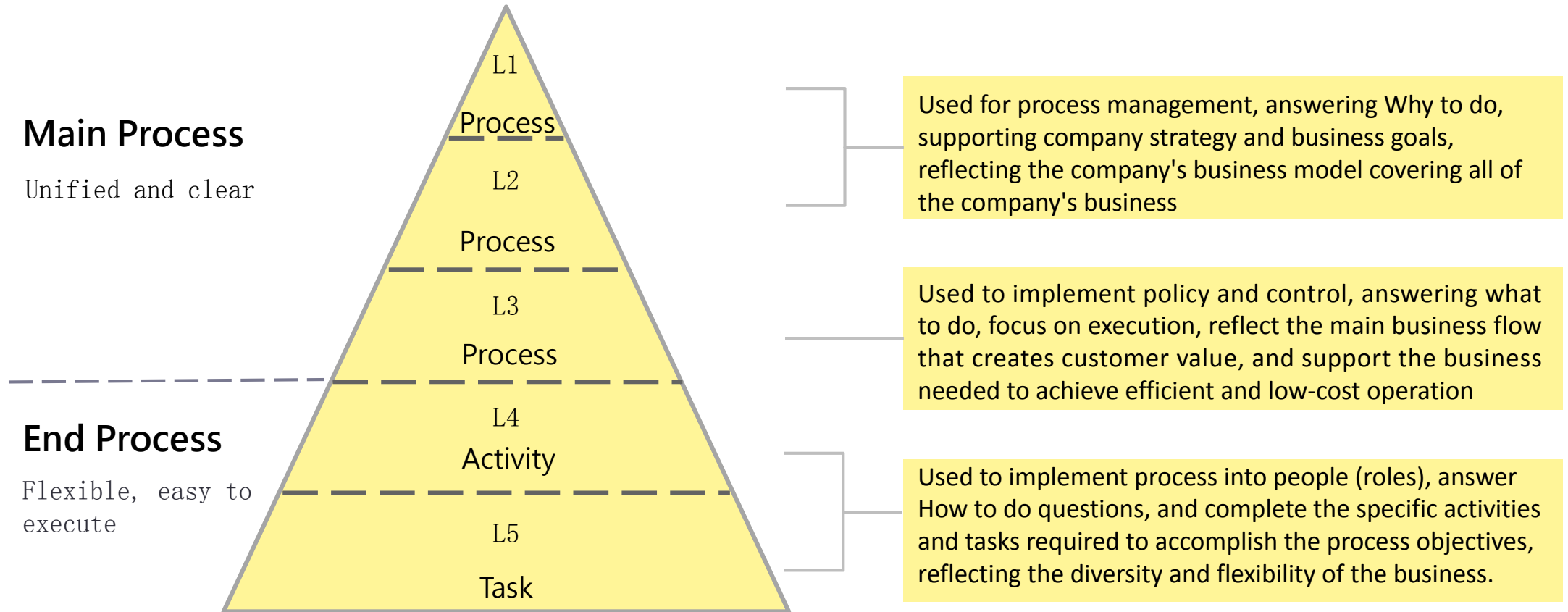
- **Promote information security culture among organization**

Solution proposal :

use firewall/VLAN/policy routing to implement intranet isolation, partition management and restricted interworking; advanced solution, desktop cloud-red area service on cloud, offline only deploy TC (no data storage)



L1 and L3 are the main processes, and L4-L5 is the end process



Example: A well-known enterprise process framework (Level 1 process)

Strategic
management
process

5.0 DSTE (Develop Strategy to Execute)

14.0 MCI (Manage Capital Investment)

Core
Business
Process

1.0 IPD (Idea to Market)

2.0 MTL (Market to Lead)

3.0 LTC (Lead to Cash)

4.0 Issue to Resolution

6.0 MCR (Manage Client Relationships)

7.0 Service Delivery

8.0 ISC

9.0 PRC

15.0 MPAR (Manage Partner and Alliance Relationships)

Management
Supporting
Process

10.0 MHR (Manage HR)

11.0 FIN (Manage Finances)

12.0 MBT&IT (Manage BT&IT)

13.0 MBS (Manage Business Support)

The first level process is the first level department.

This benchmark is limited to the 2.0, 3.0 and 7.0 processes that are extremely relevant.



Chofn IP Related

Example: 7.0 Service Delivery High-Level Process (Level 2 Process, Level 3 Process)

