การบรรยายทางวิชาการ Information Security

(ความปลอดภัยของระบบข้อมูลในระบบสารสนเทศ)

เรื่อง **เวชระเบียนอิเล็กทรอนิกส์** ของโรงพยาบาลชัยนาทนเรนทร

ก้าวแรกสู่ดิจิทัลไทยแลนด์

วันอังคารที่ 12 มีนาคม 2562 เวลา 08:30 - 16:00 น.

ณ ห้องประชุมบุษราคัม ชั้น 6 อาคาร 100 ปี สมเด็จพระศรีนครินทร์

บรรยายโดย

นาวาเอก ดร.บุญเรือง เกิดอรุณเดช

ผู้อำนวยการศูนย์ประสานงานเครือข่ายองค์กรวิจัย (องค์กรเอกชน)

และที่ปรึกษาศูนย์คอมพิวเตอร์ โรงพยาบาลราชวิถี กรมการแพทย์

หัวข้อบรรยาย

- นโยบายดิจิทัลไทยแลนด์ กับ การพัฒนาดิจิทัลด้านการแพทย์และการสาธารณสุข
- องค์ประกอบของเทคโนโลยีดิจิทัลสู่ Digital Hospital->Smart Hospital->Intelligence Hospital
- เวชระเบียนอิเล็กทรอนิกส์ ก้าวแรกสู่การพัฒนาที่ยั่งยืน
- การจัดการเทคโนโลยีที่เกี่ยวข้องกับเวชระเบียนอิเล็กทรอนิกส์
- ความปลอดภัยของเอกสารอิเล็กทรอนิกส์ และ การสร้างความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย
- การบริหารความเสี่ยงด้านสารสนเทศ และ การจัดการข้อมูลดิจิทัลที่เป็นผลพลอยได้จากเวชระเบียนอิเล็กทรอนิกส์

นโยบายดิจิทัลไทยแลนด์ กับ การพัฒนาดิจิทัลด้านการแพทย์และการสาธารณสุข

- **“ไทยแลนด์** 4.0” เป็นวิสัยทัศน์เชิงนโยบายการพัฒนาเศรษฐกิจของประเทศไทย หรือ **โมเดลพัฒนาเศรษฐกิจของรัฐบาล** โดย ดร.สุวิทย์ เมษินทรีย์ รัฐมนตรีช่วยว่าการกระทรวงพาณิชย์ ได้กำหนดแนวคิด และวางระบบเพื่อดำเนินการตามนโยบายของ ฯพณฯ พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.)
- เน้นการขับเคลื่อนปฏิรูปประเทศไทย ให้เป็นไปตามวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” เป็นภารกิจสำคัญที่ต้องปรับแก้จัดระบบ ปรับทิศทาง และ สร้างหนทางพัฒนาประเทศให้เจริญสามารถรับมือกับโอกาสและภัยคุกคามแบบใหม่ๆ ได้

ยุทธศาสตร์ชาติ 20 ปี เพื่อบรรลุวิสัยทัศน์ประเทศไทย

เพื่อให้บรรลุวิสัยทัศน์ **"มั่นคง มั่งคั่ง ยั่งยืน"**

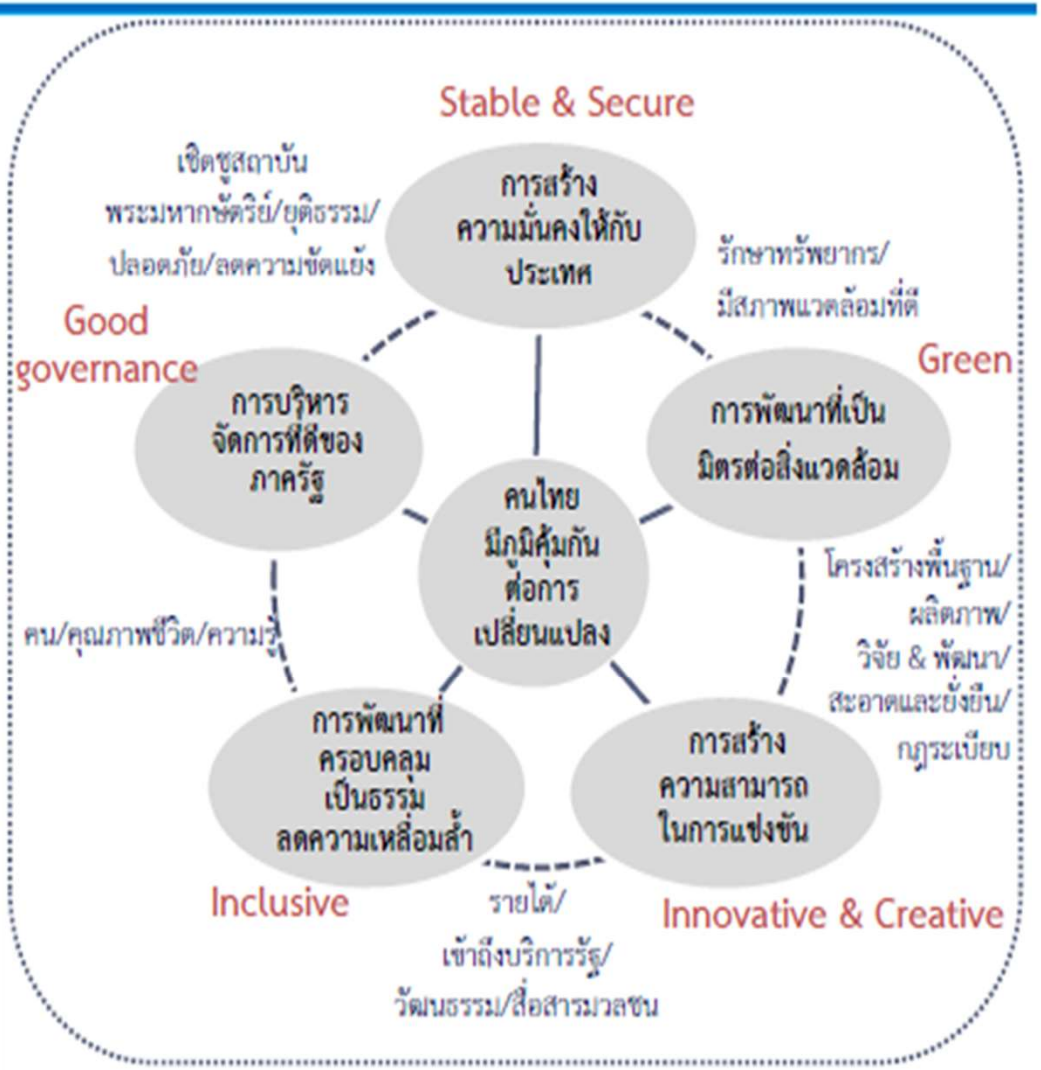
นำไปสู่การพัฒนาให้คนไทยมีความสุขภายใต้หลัก

"ปรัชญาของเศรษฐกิจพอเพียง"

และตอบสนองตอบต่อการบรรลุซึ่งผลประโยชน์แห่งชาติ ในการพัฒนาคุณภาพชีวิต สร้างรายได้ระดับสูงหลุดพ้นจากรายได้ปานกลาง และสร้างความสุขของคนไทย **สังคมมีความมั่นคง เสมอภาค และเป็นธรรม** ประเทศสามารถแข่งขันได้ในระบบเศรษฐกิจ

6 ยุทธศาสตร์หลัก

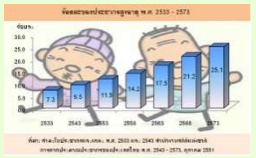
- ยุทธศาสตร์ด้านความมั่นคง
- ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน
- ยุทธศาสตร์การพัฒนาและเสริมสร้างศักยภาพคน
- ยุทธศาสตร์ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม
- ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรต่อสิ่งแวดล้อม
- ยุทธศาสตร์ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

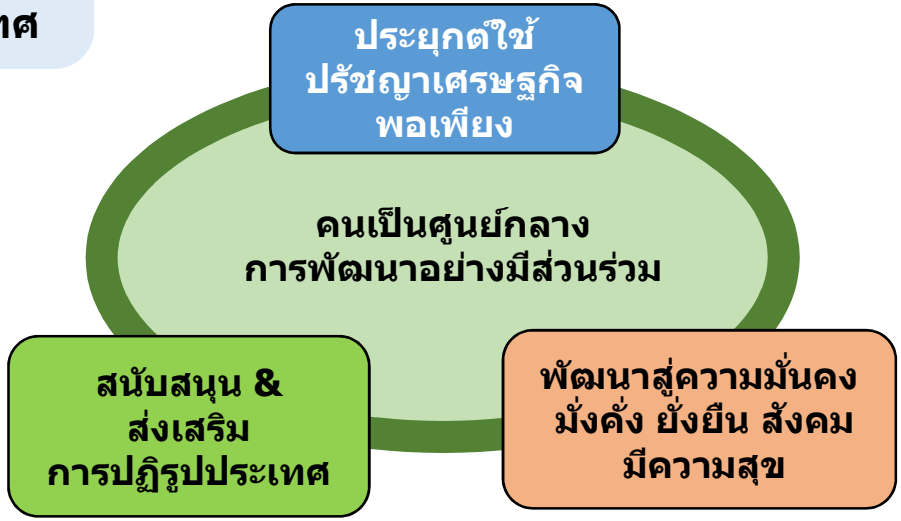


กรอบแนวคิดและหลักการของแผนพัฒนาฯ ฉบับที่ 12

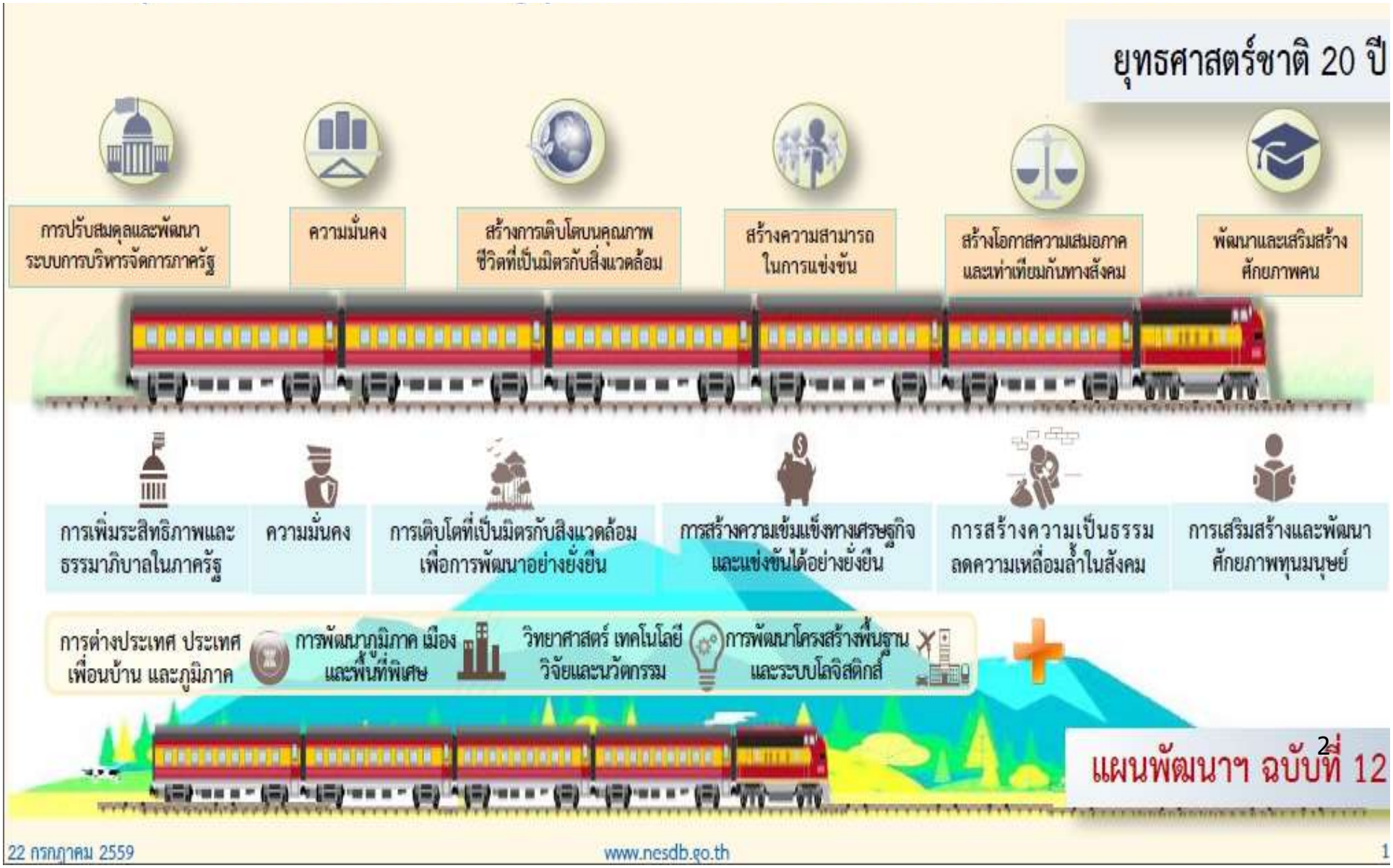
ในช่วงของแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 (พ.ศ. 2560-2564) ประเทศจะยังคงประสบสภาวะแวดล้อมและบริบทของการเปลี่ยนแปลงต่างๆ ที่อาจก่อให้เกิดความเสี่ยงทั้งจากภายในและภายนอกประเทศ

- การเปิดเศรษฐกิจเสรี
- สังคมสูงวัย
- ภัยธรรมชาติที่รุนแรง
- ปัญหาผลิตภาพการผลิต
- ความสามารถในการแข่งขัน
- คุณภาพการศึกษา
- ความเหลื่อมล้ำทางสังคม





ความเชื่อมโยงระหว่างยุทธศาสตร์ชาติ 20 ปี กับ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12



ไทยแลนด์ 4.0 จะพัฒนาเรื่องใดบ้าง?

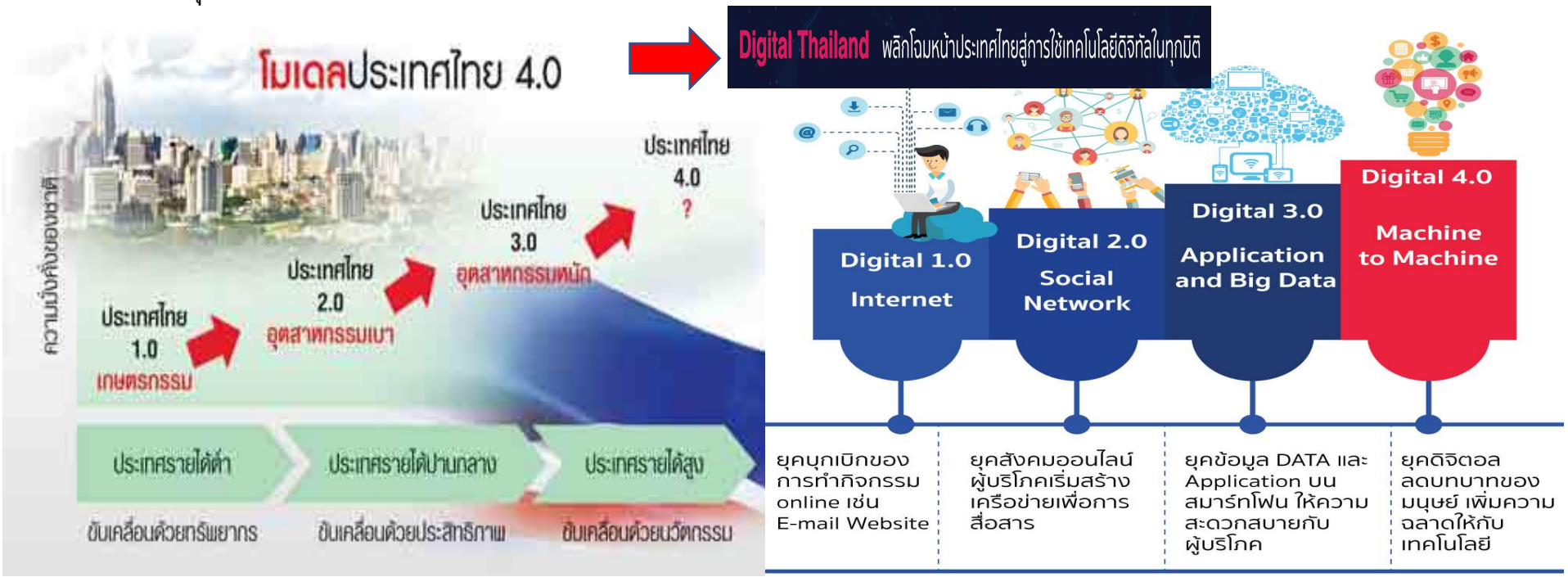
1. กลุ่มอาหาร เกษตร และเทคโนโลยีชีวภาพ เช่น สร้างเส้นทางธุรกิจใหม่ (New Startups) ด้านเทคโนโลยีการเกษตร เทคโนโลยีอาหาร เป็นต้น

2. กลุ่มสาธารณสุข สุขภาพ และเทคโนโลยีทางการแพทย์ เช่น พัฒนาเทคโนโลยีสุขภาพ เทคโนโลยีการแพทย์ สปา เป็นต้น

3. กลุ่มเครื่องมือ อุปกรณ์อัจฉริยะ หุ่นยนต์ และระบบเครื่องกลที่ใช้ระบบอิเล็กทรอนิกส์ควบคุม เช่น เทคโนโลยีหุ่นยนต์ เป็นต้น

4. กลุ่มดิจิตอล เทคโนโลยีอินเตอร์เน็ตที่เชื่อมต่อและบังคับอุปกรณ์ต่างๆ ปัญญาประดิษฐ์และเทคโนโลยีสมองกลฝังตัว เช่น เทคโนโลยีด้านการเงิน อุปกรณ์เชื่อมต่อออนไลน์โดยไม่ต้องใช้คน เทคโนโลยีการศึกษา อี–มาร์เก็ตเพลส อี–คอมเมิร์ซ เป็นต้น

5. กลุ่มอุตสาหกรรมสร้างสรรค์ วัฒนธรรม และบริการที่มีมูลค่าสูง เช่น เทคโนโลยีการออกแบบ ธุรกิจไลฟ์สไตล์ เทคโนโลยีการท่องเที่ยว การเพิ่มประสิทธิภาพการบริการ เป็นต้น



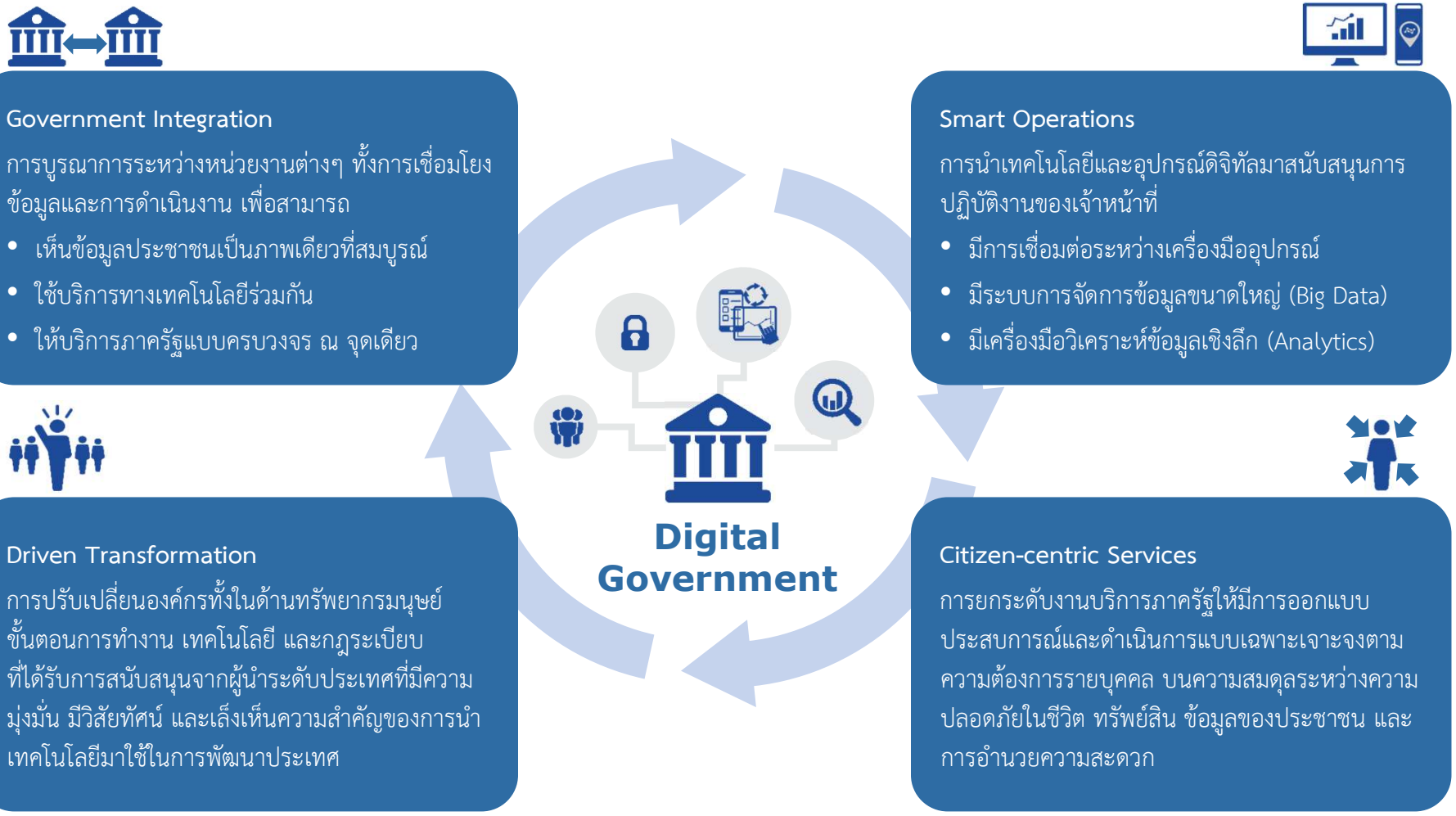
ปฏิรูปประเทศไทยสู่

ดิจิทัลไทยแลนด์

และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างไร

วิสัยทัศน์สู่การพัฒนารัฐบาลดิจิทัล...

“ใน 3 ปีข้างหน้า ภาครัฐไทยจะยกระดับสู่การเป็นรัฐบาลดิจิทัล ที่มีการบูรณาการระหว่างหน่วยงาน มีการดำเนินงานแบบอัจฉริยะ ให้บริการโดยมีประชาชนเป็นศูนย์กลาง และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริง”



ยุทธศาสตร์ที่ 1	• พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ
ยุทธศาสตร์ที่ 2	• ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล
ยุทธศาสตร์ที่ 3	• สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล
ยุทธศาสตร์ที่ 4	• ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล
ยุทธศาสตร์ที่ 5	• พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล
ยุทธศาสตร์ที่ 6	• สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

แผน 20 ปี กสธ.

นโยบายรัฐบาล

ยุทธศาสตร์ชาติระยะ 20 ปี
และปฏิรูปประเทศไทย
ด้านสาธารณสุข

ประเทศไทย 4.0

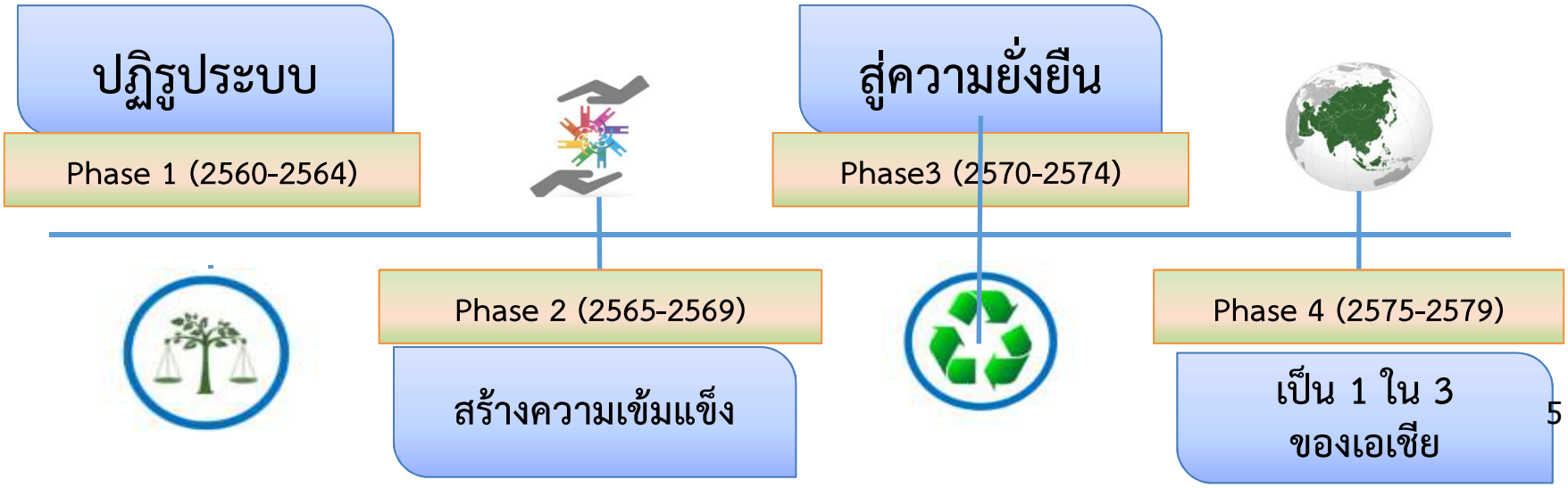
ประชารัฐ

แผนปฏิรูป

แผนพัฒนาเศรษฐกิจ
และสังคมแห่งชาติ
ฉบับที่ 12
(พ.ศ.2560 – 2564)

กรอบแนวคิด

ทิศทางการวางแผน 20 ปี (4 Phase)



Retreat MOPH

ทิศทางกระทรวงสาธารณสุข

เป็นองค์กรหลักด้านสุขภาพ
ที่รวมพลังสังคม
เพื่อประชาชนสุขภาพดี

พัฒนาและอภิบาลระบบสุขภาพ
อย่างมีส่วนร่วมและยั่งยืน

MOPH

M astery

P eople centered approach

O riginality

H umility

เป้าหมาย

ประชาชนสุขภาพดี

เจ้าหน้าที่มีความสุข

ระบบสุขภาพยั่งยืน

3. 4 Excellence Strategies

แผน 20 ปี กสธ.

กระทรวงสาธารณสุข
Ministry of Public Health

4 Excellence Strategies (16 แผนงาน 48 โครงการ) → **8 Corporate Indicators**

P&P Excellence

1. พัฒนาคุณภาพชีวิตคนไทยทุกกลุ่มวัย
2. การป้องกันควบคุมโรคและภัยสุขภาพ
3. การลดปัจจัยเสี่ยงด้านสุขภาพ
4. การบริหารจัดการสิ่งแวดล้อม

Service Excellence

1. การพัฒนาระบบการแพทย์ปฐมภูมิข
2. การพัฒนาระบบบริการสุขภาพ
3. ระบบการแพทย์ฉุกเฉินครบวงจรและการส่งต่อ
4. การพัฒนาคุณภาพหน่วยงานบริการด้านสุขภาพ
5. การพัฒนาตามโครงการพระราชดำริและพื้นที่เฉพาะ
6. ประเทศไทย 4.0 ด้านสาธารณสุข

People Excellence

1. พัฒนาการวางแผนกำลังคนด้านสุขภาพ (HRP)
2. การผลิตและพัฒนากำลังคนสู่ความเป็นมืออาชีพ
3. เพิ่มประสิทธิภาพบริหารจัดการกำลังคนด้านสุขภาพ
4. พัฒนาเครือข่ายกำลังคนด้านสุขภาพ

Governance Excellence

1. พัฒนาระบบธรรมาภิบาลและคุณภาพการบริหารจัดการภาครัฐ
2. พัฒนาระบบข้อมูลสารสนเทศและกฎหมายด้านสุขภาพ
3. การบริหารจัดการด้านการเงินการคลังสุขภาพ
4. การพัฒนางานวิจัยและองค์ความรู้ด้านสุขภาพ
5. การปรับโครงสร้างและพัฒนากฎหมายด้านสุขภาพ

Digital Thailand พลิกโฉมหน้าประเทศไทยสู่การใช้เทคโนโลยีดิจิทัลในทุกมิติ

เข็มมุ่งพ.ศ. 2561 – 2563

- Intelligent Hospital: (IT & Innovation)
- 2 P Safety: (Patient & Personnel)
- Green & Clean Hospital

Intelligence Hospital

IoT, AI, ML, Automonous Easy, Fast, Elastic, Convenience

Smart Hospital

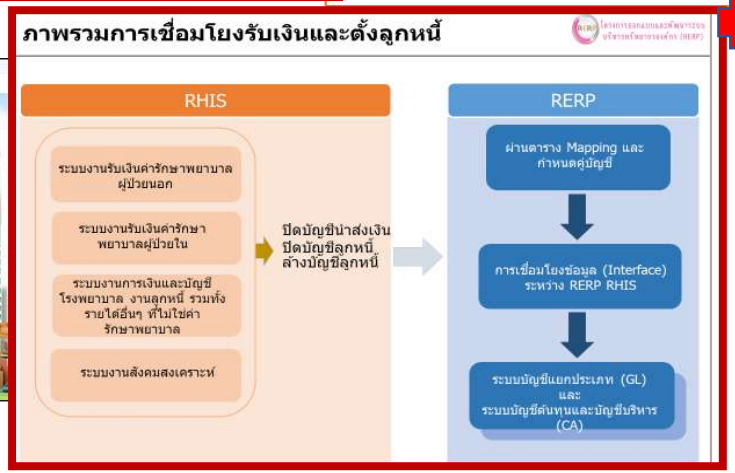
Automatic , Mobile Apps, Medical Device, VDI, Cloud

Digital Hospital

Paperless, Digital Technology, ERP Privacy&Security ISO27001

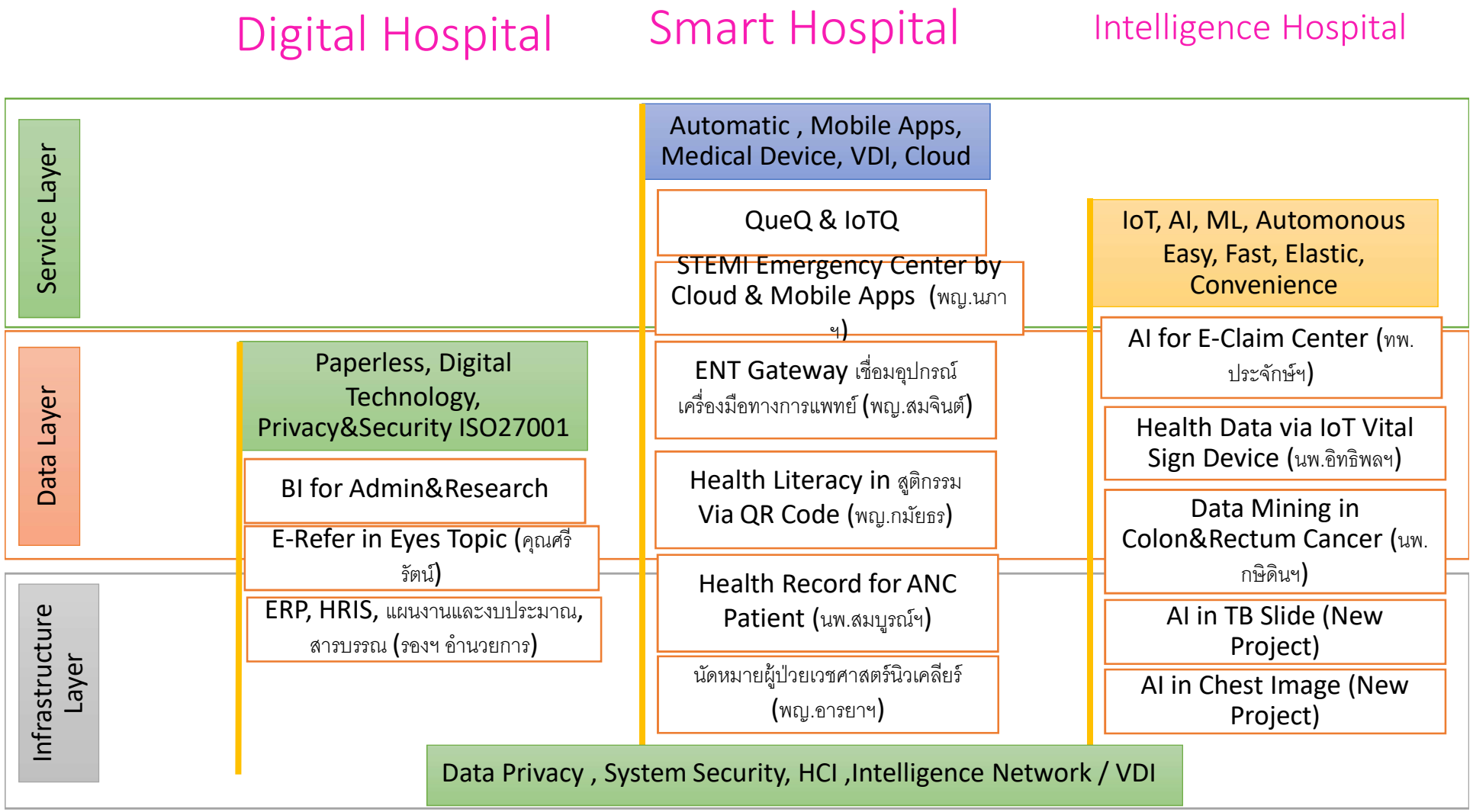
Group	From	To
1	Food, Agriculture and Bio-Tech	Agritech, Foodtech
2	Health, Wellness and Bio-Med	Healthtech, Meditech
3	Smart Devices, Robotics and Mechatronics	Robotech
4	Digital, Internet of Things, Artificial Intelligence and Embedded Technology	Fintech, Internet of Things, Edtech, E–Marketplace and E–Commerce
5	Creative, Culture and High Value Services	Designtech, Lifestyle Business, Traveltech and Service Enhancing

HRIS + แผนงานและงบประมาณ + สารบรรณอิเล็กทรอนิกส์



ERP REFORM TO SMART HOSPITAL

คู่มือการใช้งานระบบบัญชีแยกประเภท (GL)
ระบบการจัดทำและบริหารงบประมาณ (BG)
ระบบการบัญชีต้นทุนและบัญชีบริหาร (CA)
ระบบเงินเดือนและค่าตอบแทน (PC)
ระบบจัดซื้อจัดจ้าง (MM)
ระบบทะเบียนและบัญชีสินทรัพย์ ครุภัณฑ์ (FA)
ระบบเบิกจ่ายและบัญชีเจ้าหนี้ (AP)


Digital Hospital
Smart Hospital
Intelligence Hospital
Service Layer
Data Layer
Infrastructure Layer
Automatic , Mobile Apps, Medical Device, VDI, Cloud
QueQ & IoTQ
STEMI Emergency Center by Cloud & Mobile Apps (พญ.นภาฯ)
ENT Gateway เชื่อมอุปกรณ์เครื่องมือทางการแพทย์ (พญ.สมจินต์)
Health Literacy in สูติกรรม Via QR Code (พญ.กมัยธร)
Health Record for ANC Patient (นพ.สมบูรณ์ฯ)
นัดหมายผู้ป่วยเวชศาสตร์นิวเคลียร์ (พญ.อารยาฯ)
IoT, AI, ML, Automonous Easy, Fast, Elastic, Convenience
AI for E-Claim Center (ทพ.ประจักษ์ฯ)
Health Data via IoT Vital Sign Device (นพ.อิทธิพลฯ)
Data Mining in Colon&Rectum Cancer (นพ.กษิดินฯ)
AI in TB Slide (New Project)
AI in Chest Image (New Project)
Paperless, Digital Technology, Privacy&Security ISO27001
BI for Admin&Research
E-Refer in Eyes Topic (คุณศรีรัตน์)
ERP, HRIS, แผนงานและงบประมาณ, สารบรรณ (รองฯ อำนวยการ)
Data Privacy , System Security, HCI ,Intelligence Network / VDI

Smart Healthcare Consumer Protection System

Healthcare System Standard

- Health Service Across Border
- Healthtech&Meditech
  - Medical Robotic
  - Automated Diagnosis
  - Precision medicine
  - Digital Health & IOT
- Wearable Technology

Smart Services

- QR code
- E-registration
- E-payment
- E-signature
- E-CRM

- Automated Complaints Processing
- Cyber security

Consumer Protection Management

- E-monitoring
- E-surveillance
- Drone Technology
- Fraudulent Behavior Detection

Big Data System

- Blockchain Technology
- Underwriting and Healthcare Consumer Protection Process การนำข้อมูลจาก social media มาใช้เพื่อการพัฒนามาตรการคุ้มครองผู้บริโภคฯ

เสริมสร้างความรอบรู้ นำคนไทยสู่สุขภาพดี ที่ 4.0

แนวคิดการขับเคลื่อน

- เปลี่ยนสังคมผู้สูงอายุ จากผู้พึ่งพิงเป็นผู้มีพลัง
- มุ่งพัฒนานวัตกรรม และเทคโนโลยีสุขภาพ
- ใช้เทคโนโลยีอย่างสร้างสรรค์และใช้นวัตกรรม เป็นตัวขับเคลื่อน
- พลังประชารัฐ ขับเคลื่อนสังคม

ประชาชนดูแลสุขภาพตนเองได้

- มี HL HB ในเกณฑ์ระดับดี เลือกใช้บริการที่เหมาะสมอย่างยั่งยืน
- ประชาชนเข้าถึงบริการสุขภาพได้อย่างเหมาะสม

ผลลัพธ์ทางสุขภาพ
สุขภาวะที่ดี
อัตราการป่วยลดลง
ลดค่าใช้จ่ายด้านสุขภาพ

คนไทย
มั่นคง มั่งคั่ง ยั่งยืน

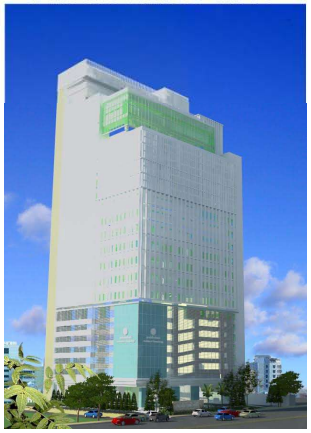
Smart Hospital

Green & Clean Hospital

ปรับปรุงเปลือกอาคารผู้ป่วยนอก
โรงพยาบาลศูนย์ ให้เป็นไปตามเกณฑ์ทางด้านพลังงานของอาคารเขียว (LEED)

จัดทำแบบก่อสร้างอาคารสถานบริการสุขภาพต้นแบบที่ปลอดจากการปล่อยก๊าซคาร์บอนสุทธิ
(Carbon Neutral)

จัดทำต้นแบบสถานบริการ
สุขภาพผู้สูงอายุ
ตามแนวทางอาคาร



Calibration and Testing Medical Equipment Laboratory

พัฒนาการห้องปฏิบัติการทดสอบ/สอบเทียบด้านไฟฟ้า ความดัน อุณหภูมิ ความชื้น อัตราการไหล มวล แสงสว่าง และเสียง ครอบคลุมเครื่องวัดทางการแพทย์ในประเทศไทย

พัฒนาการทดสอบ/สอบเทียบ เพื่อรับรองนวัตกรรมเครื่องวัดทางการแพทย์4.0 (ทั้งก่อนและหลังใช้งาน)

ทดสอบความปลอดภัยทางไฟฟ้าและความเข้ากันได้ทางสนามแม่เหล็กไฟฟ้า (EMC Testing Center) กับเครื่องมือวัดทางการแพทย์ และหุ่นยนต์ทางการแพทย์

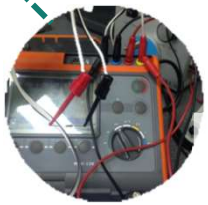
อัตราการไหล

ความดัน

อุณหภูมิ+ความชื้น

มวล

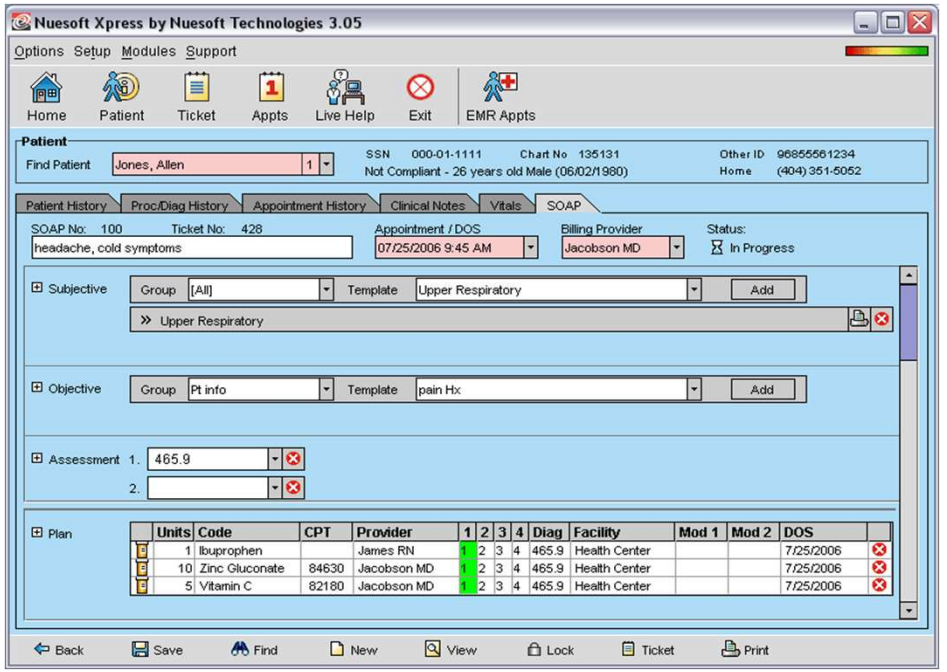
แสงสว่าง+เสียง



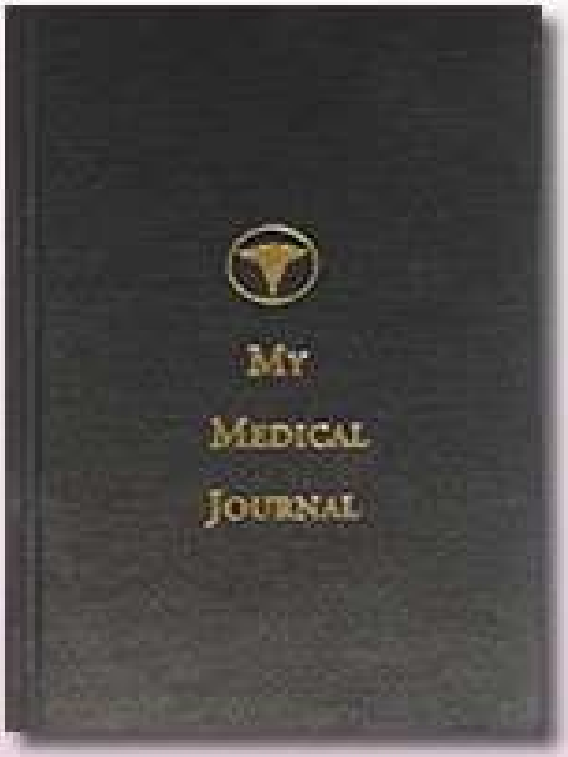
ไฟฟ้า+EMC

เวชระเบียน

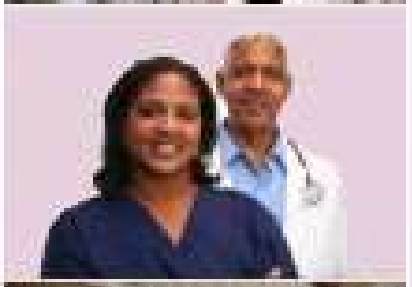
medical record
health record
medical chart



My Medical Journal



- Save time and energy
- Save money
- Improve your health
- Save your life



เวชสารสนเทศ (medical informatics)

- สาขาที่เกิดขึ้นจากการประยุกต์ใช้คอมพิวเตอร์ทางชีววิทยาการแพทย์
- เพื่อเพิ่มประสิทธิผลและประสิทธิภาพของการทำงานโดยอาศัยวิธีการ, เครื่องมือและทรัพยากรการสารสนเทศที่พัฒนาขึ้น
- ระบบบันทึกแบบเดิม (บนกระดาษ) ได้ถูกเปลี่ยนมาอยู่ในรูปอิเล็กทรอนิกส์
- เวชสารสนเทศช่วยให้แพทย์กระทำในสิ่งที่ไม่สามารถกระทำได้ในอดีต
- การใช้เทคโนโลยีสารสนเทศ ในการสืบค้นองค์ความรู้และการตัดสินใจมีความสำคัญต่อชีววิทยาการแพทย์สมัยใหม่

แหล่งข้อมูลที่มี

1- ฐานข้อมูล HR

2- ฐานข้อมูล HIS-1

3- ฐานข้อมูล HIS-2

4- ฐานข้อมูล HIS-3

5- ฐานข้อมูล WEB (เว็บภายนอก)

6- ฐานข้อมูล WEBINTRA (เว็บภายใน)

7- ฐานข้อมูล HIS-4 (ระบบจิตเวช)

8- ฐานข้อมูล HIS-5

9- ฐานข้อมูล Binary (ระบบจัดเก็บไฟล์ภาพสแกนประวัติการรักษาผู้ป่วย)

10 - ฐานข้อมูล LAB (DBF ระบบจุลชีวะ)

11 - ฐานข้อมูล Roche (ฐานข้อมูลLAB)

12 - ฐานข้อมูล Thai-Refer (ระบบส่งต่อของโปรแกรม Thai-Refer)

13 - ฐานข้อมูล referdb (E-refer Local ภายใน รพ. อย่างเดียว ระบบส่งต่อที่ต่อยอดของโปรแกรม Thai-Refer)

14 - ฐานข้อมูล referdw (E- refer รพ อื่นส่งเข้ามาที่โปรแกรม Thai-Refer)

15 - ฐานข้อมูล Pack (ฐานข้อมูลX RAY)

16 - ฐานข้อมูล apponline (ฐานข้อมูลลงทะเบียนออนไลน์)

17 - ฐานข้อมูล web รพ ภายนอก

18 - ฐานข้อมูลฐานข้อมูล p4p Hr

19 - ฐานข้อมูล vacation (ฐานข้อมูล ลาออนไลน์)

20 - ฐานข้อมูล e-learning (ฐานข้อมูลห้องยาเป็นแบบทดสอบห้องยา)

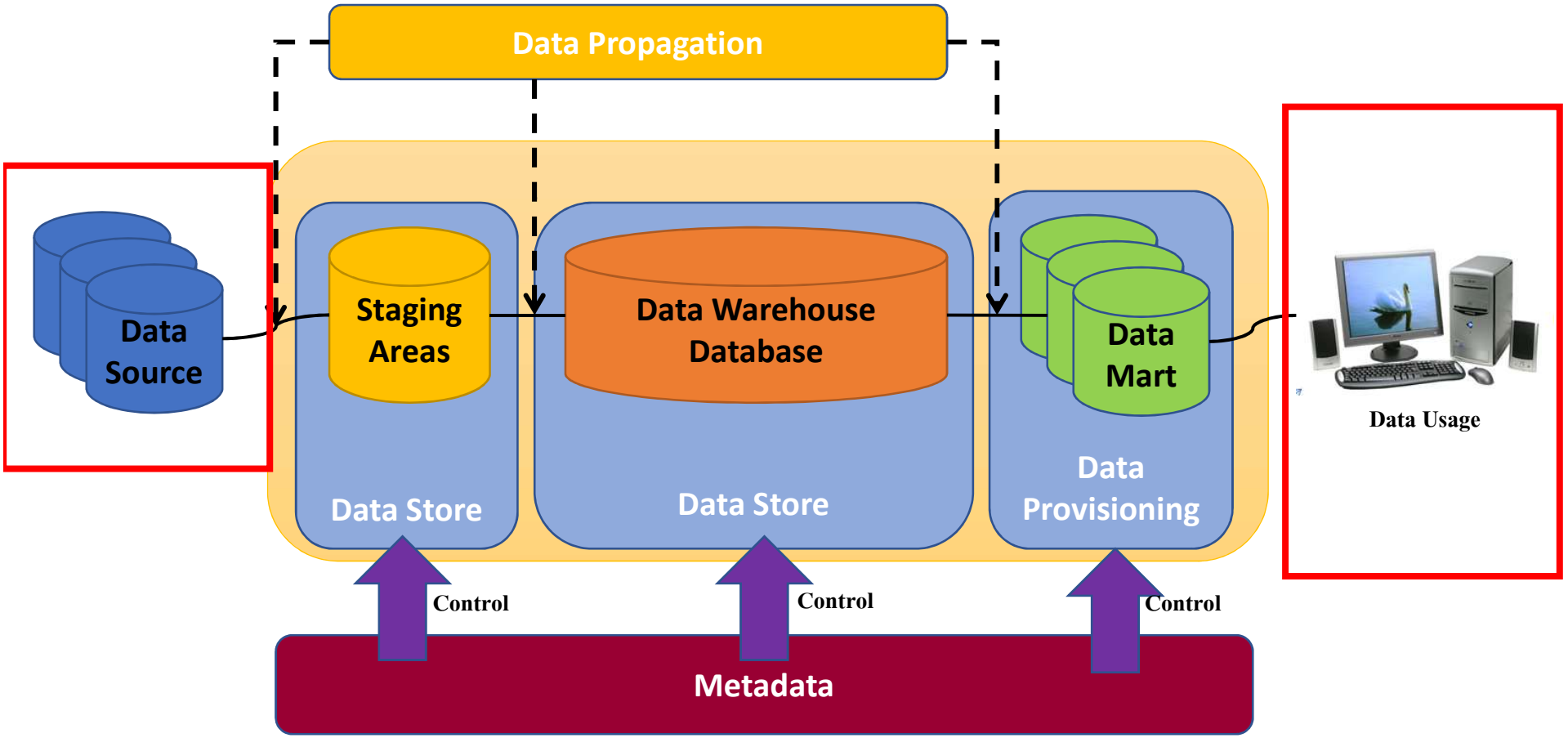
21 - ฐานข้อมูล chemotherapy (ฐานข้อมูล ดาวโหลดเอกสารห้องเคมีบำบัด)

ปัญหาของการนำฐานข้อมูลหลายแบบมารวมกัน

- 1. H/W S/W หลายชนิด
- 2. Data Redundancy เกิดความซ้ำซ้อนของข้อมูล
- 3. Data Inconsistency ข้อมูลไม่สอดคล้องกัน
- 4. Coding System ระบบการให้รหัสเกิดปัญหา มาตรฐานซ้อน (Multiple Standard)

- การพัฒนาระบบแบบยุ้งฉาง (Silo-based System)
  - งานใครงานมัน

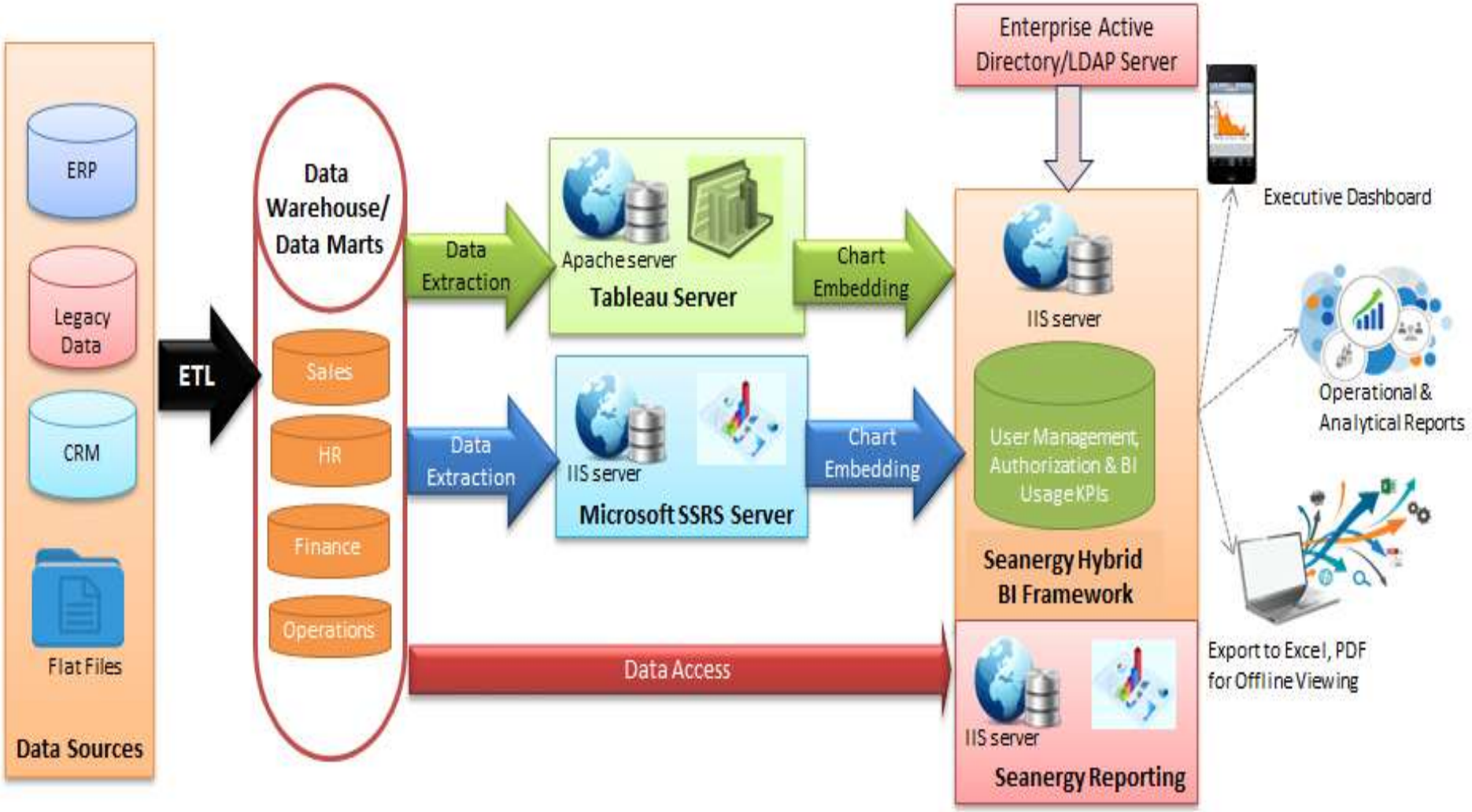
กระบวนการคลังข้อมูล(Data Warehousing)



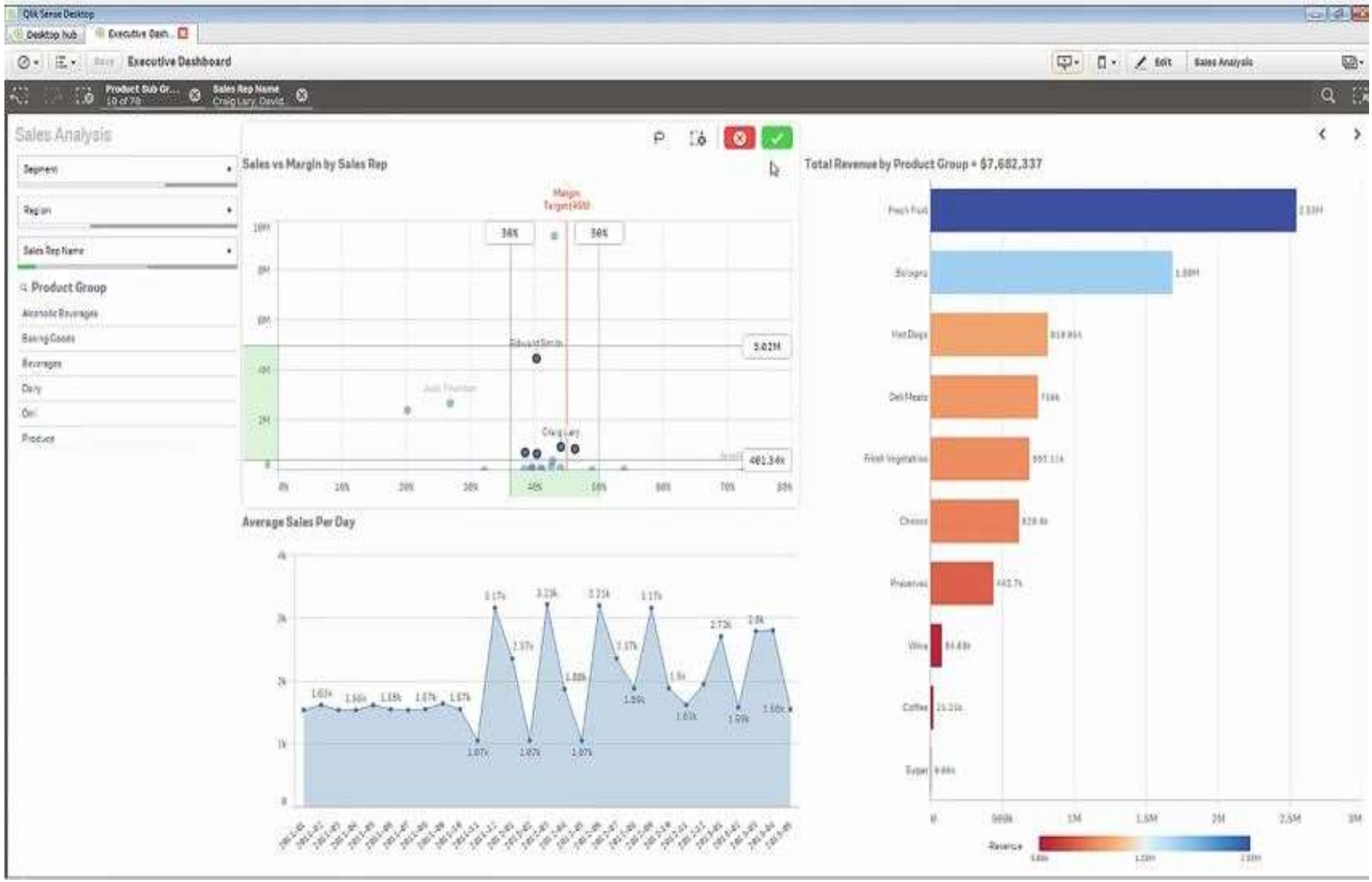
Business Intelligence คืออะไร

- เป็นกลุ่มของ Software และเทคโนโลยีที่รวบรวม จัดเก็บ และวิเคราะห์ รวมถึงวิธีการกำหนดการเข้าถึงข้อมูล เพื่อให้ผู้ใช้ในองค์กรสามารถทำงานได้อย่างมีประสิทธิภาพยิ่งขึ้น
- Software ในกลุ่ม BI จะมีการรวบรวมคุณสมบัติหลายอย่างเช่น DSS (Decision Support System), OLAP (Online Analytical Processing) , การวิเคราะห์เชิงสถิติ รวมถึงการพยากรณ์

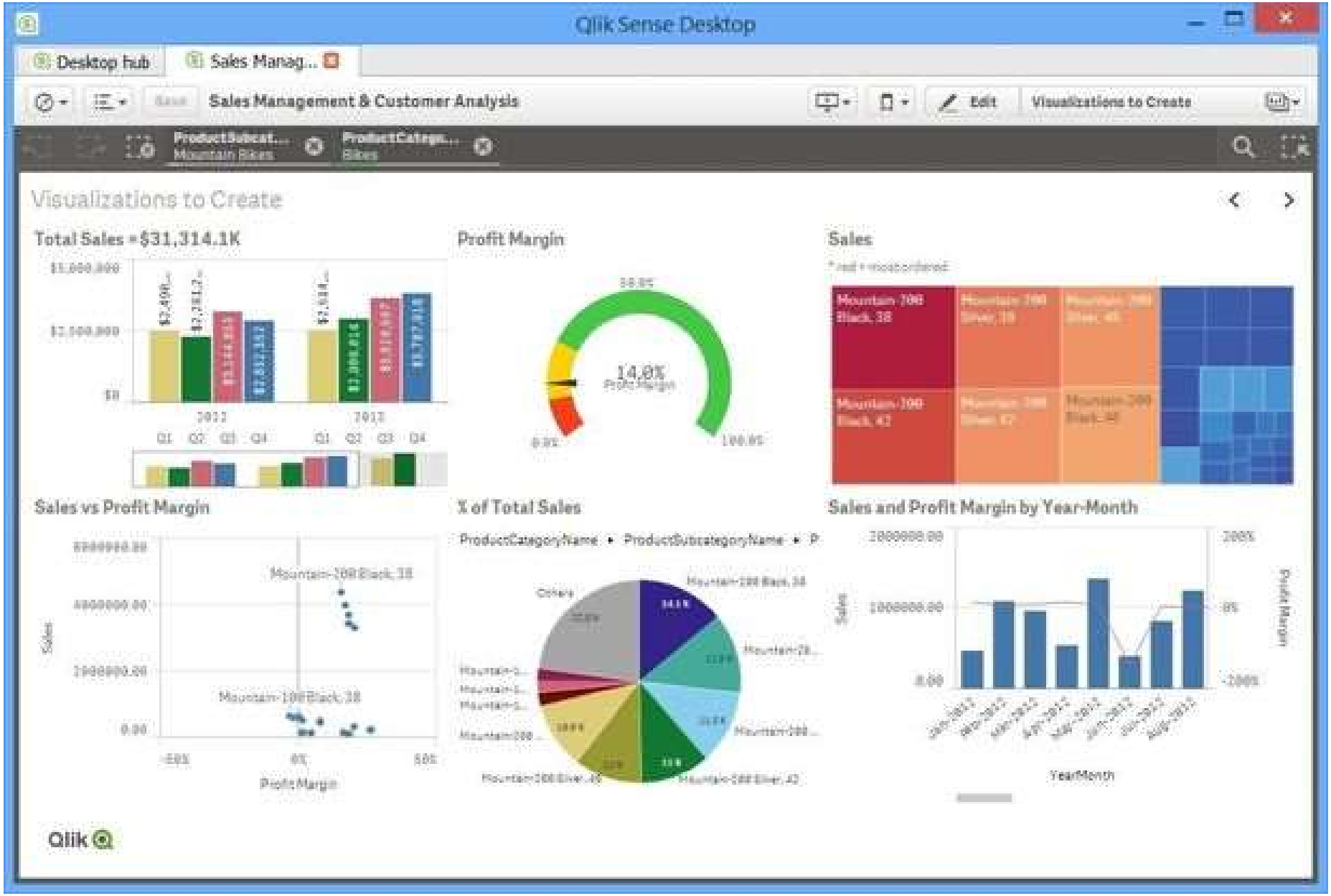
ตัวอย่างแผนภาพ BI Architecture



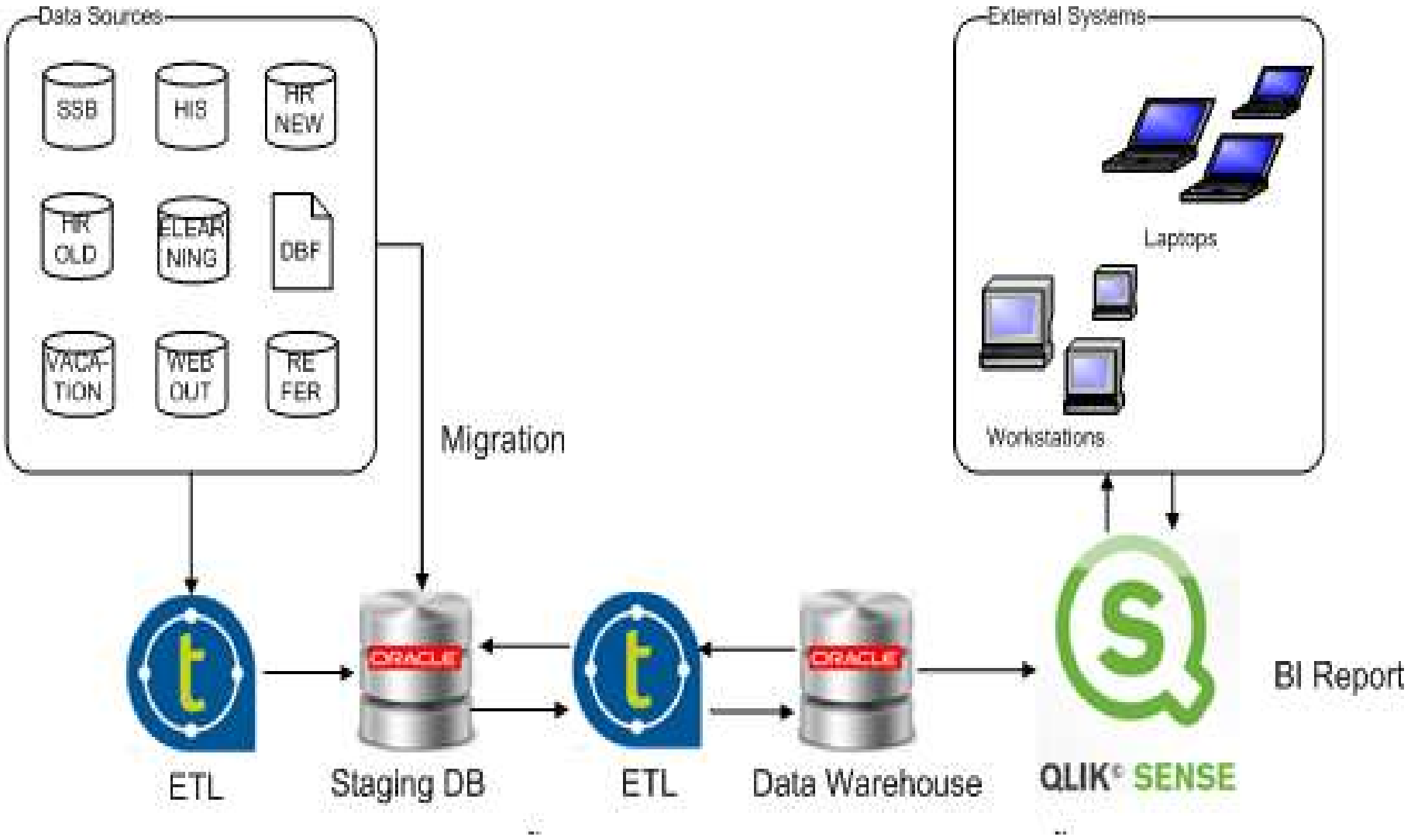
ตัวอย่างรายงาน BI



ตัวอย่างรายงาน BI (2)



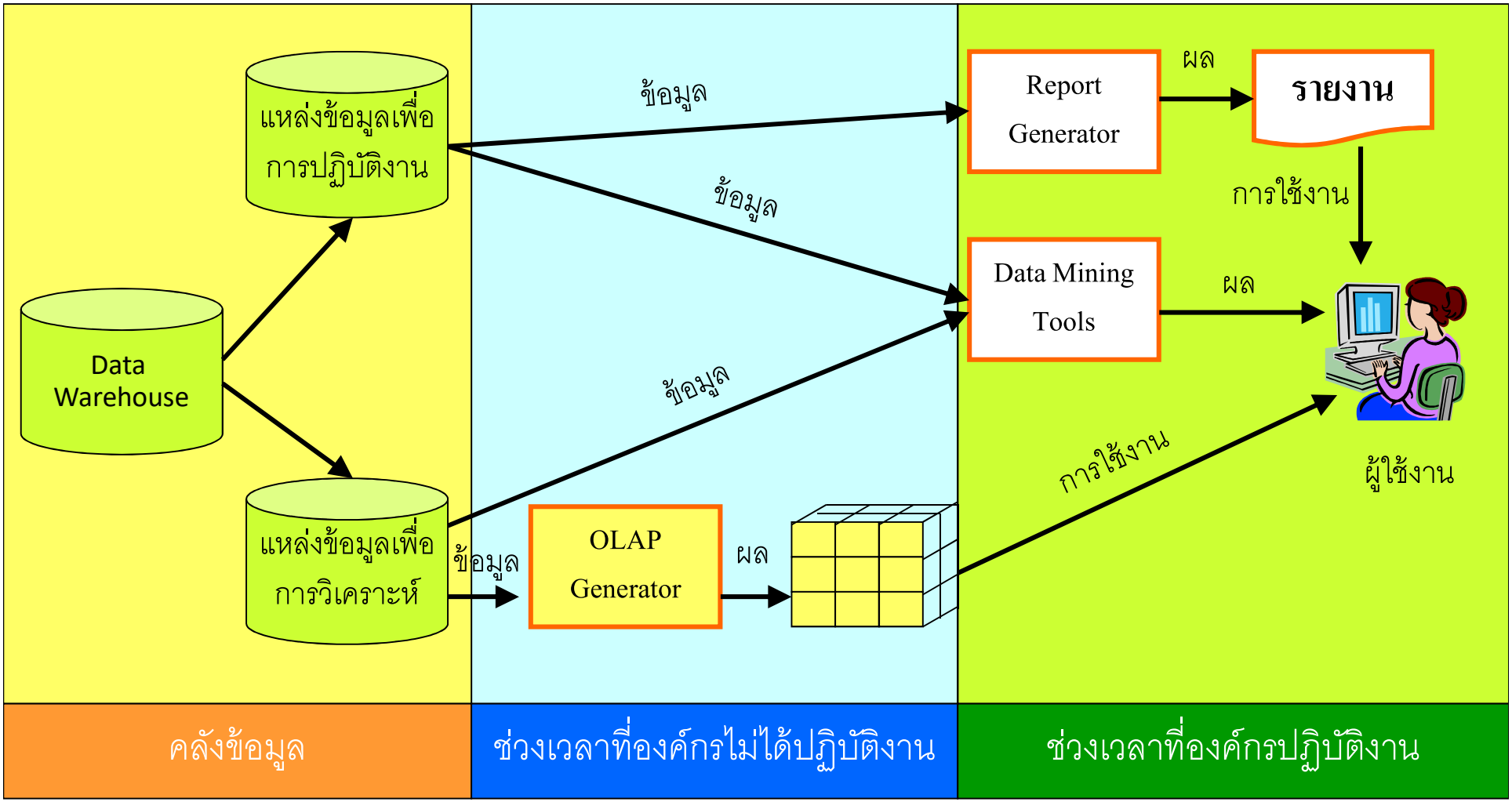
Software Infrastructure



ประโยชน์ที่เด่นชัดของ BI

- Scorecard ให้ภาพขององค์กรโดยรวมแก่ผู้บริหารสรุปอยู่ในมุมมองที่เดียว
- Scorecard ให้ข้อมูลที่เพียงพอในภาพใหญ่ที่แสดงให้เห็นถึงสภาวะของการทำงาน และเป้าหมายขององค์กร
- ข้อมูลที่นำเสนอใน Scorecard เป็นข้อมูลที่ทันสมัยที่สุดเท่าที่เป็นไปได้ เพื่อให้นำข่าวสารนั้นไปใช้กับการดำเนินงานได้อย่างถูกต้อง
- เมื่อทำได้เช่นนี้แล้ว จะเป็นก้าวแรกที่สำคัญสู่ Big Data

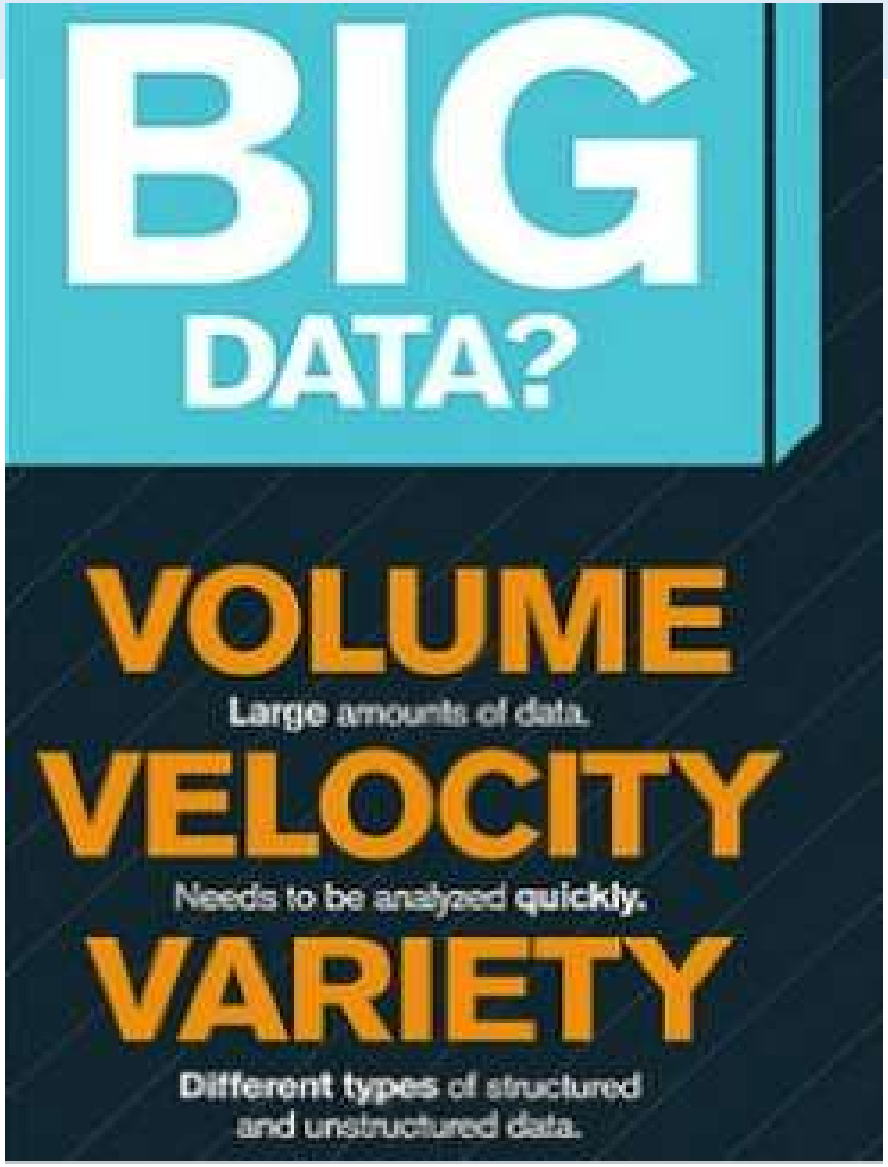
คลังข้อมูล (Data Warehouse) : การวิเคราะห์ข้อมูลในคลังข้อมูล (2/2)



“big data” คืออะไร

- คือ แหล่งข้อมูลขนาดใหญ่ทั้ง
- ด้านปริมาณ high-volume,
- ด้านการเพิ่มขึ้นของข้อมูล high-velocity,
- ด้านความหลากหลายของข้อมูล high-variety
- เป็นทรัพย์สินขององค์กรที่มีคุณค่าช่วยในการตัดสินใจที่ดีและเหมาะสม (Gartner 2012)

Big Data: 3V's


BIG
DATA?
VOLUME
Large amounts of data.
VELOCITY
Needs to be analyzed quickly.
VARIETY
Different types of structured
and unstructured data.

WHY BIGDATA?

VOLUME
DATA SIZE

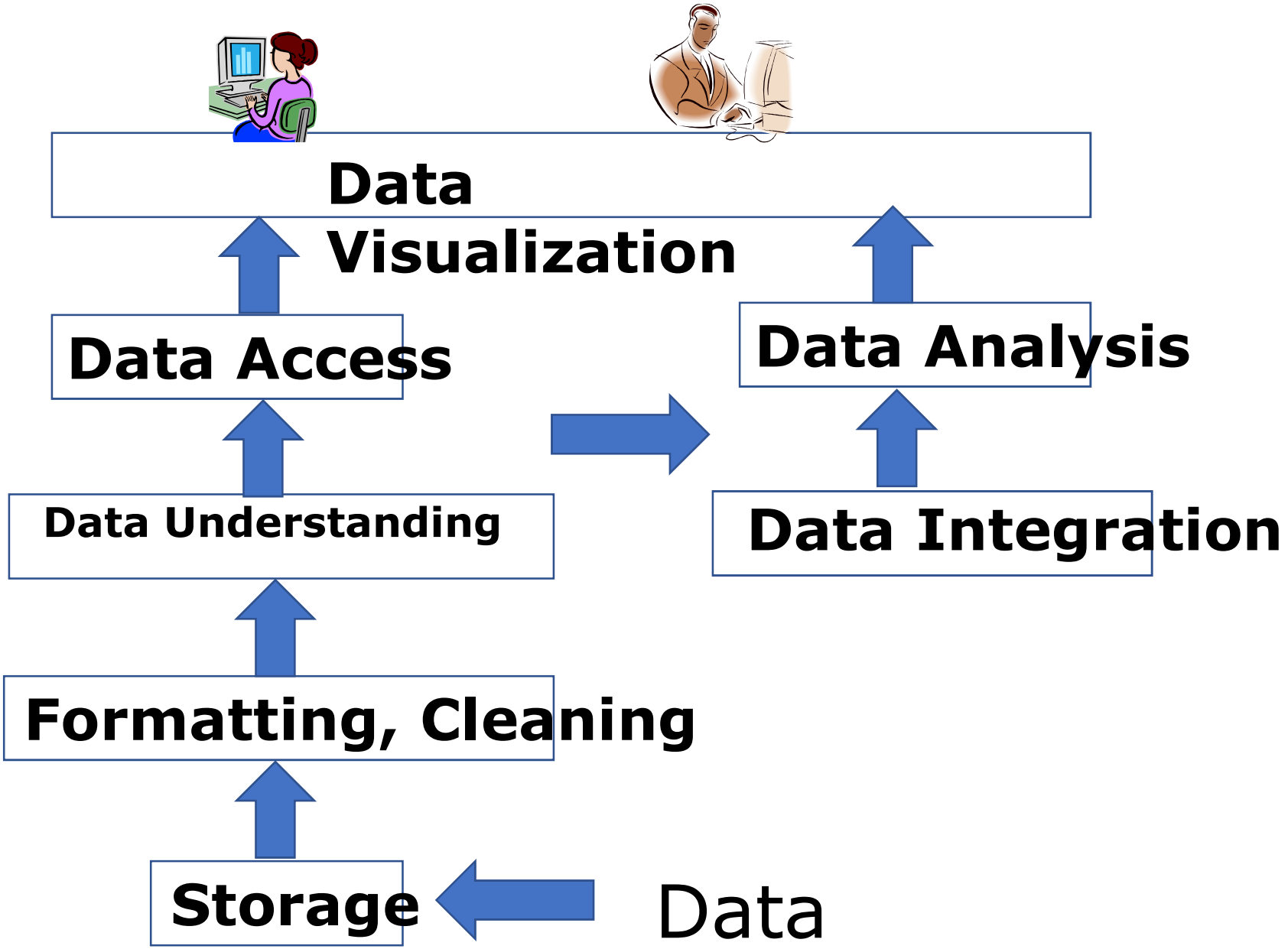
VELOCITY
SPEED OF CHANGE

VARIETY
DIFFERENT FORMS OF DATA SOURCES

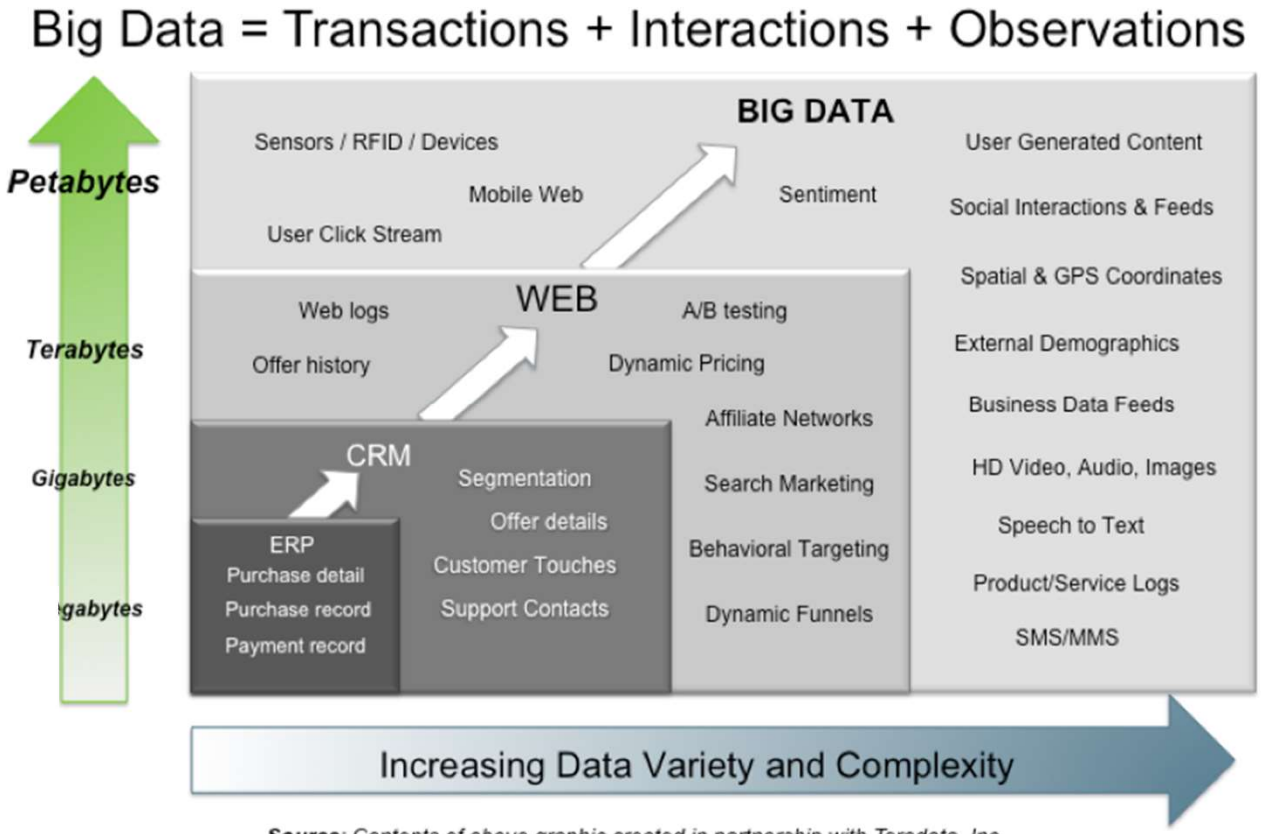
VERACITY
UNCERTAINTY OF DATA

Variability Complexity

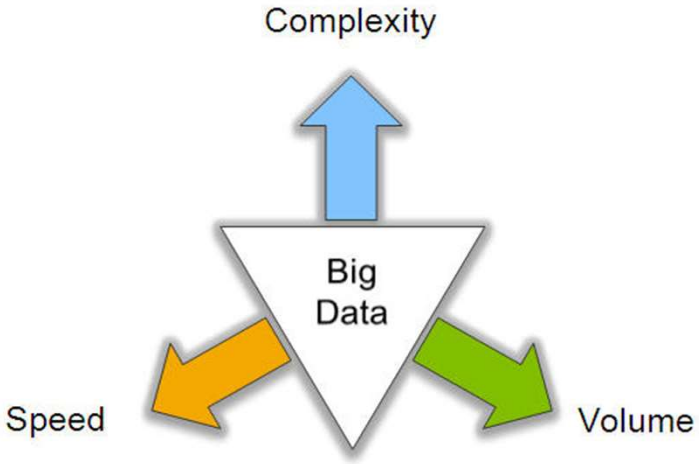
Computational View of Big Data



Big Data: 3V's



Source: Contents of above graphic created in partnership with Teradata, Inc.



Big Data EveryWhere!

- Lots of data is being collected and warehoused
  - Web data, e-commerce
  - purchases at department/ grocery stores
  - Bank/Credit Card transactions
  - Social Network

สรุปผลเกี่ยวกับ Big Data

1. สนับสนุนการใช้ข้อมูลช่วยในการตัดสินใจ

2. ควรเปรียบเทียบผลการได้จากการใช้ BI กับแหล่งข้อมูลอื่นๆ ว่ามีลักษณะคล้อยตาม หรือ ขัดแย้ง แล้วหาเหตุผลอธิบาย

3. เชื่อมโยงข้อมูลหลายลักษณะ หลายแหล่ง เพื่อนำมาใช้ประโยชน์ร่วมกัน

4. ระมัดระวังความผิดพลาดจากการให้ความหมายข้อมูล สารสนเทศ

5. ตระหนักถึงความลับของข้อมูล และ ความมั่นคงปลอดภัยในยุคดิจิทัล

มาตรฐานความปลอดภัยของข้อมูล

ตามมาตรการสำคัญในการควบคุมความปลอดภัยของข้อมูล

กระบวนการเข้าถึงให้ใช้มาตรฐาน 1I 3A

แผนยุทธศาสตร์ชาติระยะ 20 ปี ด้านสาธารณสุข

(พ.ศ.2560-2579)

Identification ระบุตัวตน / กำหนด/ชี้ความเสี่ยงสำคัญ

Authentication ตรวจสอบผู้เข้าใช้ระบบ

Authorization กำหนดผู้มีอำนาจหน้าที่

Access Control ควบคุมการทำงาน/ควบคุมสิทธิในการเข้าถึง

กรณีศึกษาที่ 1ระบบคอมพิวเตอร์ สามารถบันทึกผลการตรวจและส่งคำสั่งการรักษาในระบบ โดยไม่เขียนบันทึกลงบนเอกสาร

- แพทย์เขียนบันทึกผลการตรวจและคำสั่งรักษาลงบน OPD Card จากนั้นจึงลอกคำสั่งรักษาลงบนใบสั่งยา พร้อมทั้งลงลายมือชื่อแพทย์ผู้สั่ง ส่งให้เจ้าหน้าที่ไปดำเนินการตามแพทย์สั่ง
- เจ้าหน้าที่บันทึกคำสั่งแพทย์นั้น (รายการยา/เวชภัณฑ์ Lab Xray หัตถการทางการแพทย์)
- เอกสารเวชระเบียน กับ ข้อมูลอิเล็กทรอนิกส์ ถูกต้องตรงกันหรือไม่ อย่างไร?

กรณีศึกษาที่ 2 โรงพยาบาลใช้ระบบคอมพิวเตอร์ บันทึกผลการตรวจและคำสั่งแพทย์เป็นข้อมูลอิเล็กทรอนิกส์ โดยไม่ได้เขียนเอกสารเวชระเบียน

- ข้อมูลอิเล็กทรอนิกส์เหล่านี้**มีความคงตัว ไม่เปลี่ยนแปลง และ ยืนยันตัวผู้สร้างข้อมูล**
- การรับรองข้อมูลอิเล็กทรอนิกส์ เป็นเรื่องยุ่งยากและลำบากใจสำหรับผู้สร้าง/แก้ไขข้อมูล อันเนื่องจากความไม่ไว้วางใจในระบบคอมพิวเตอร์ ทำอย่างไรจึงจะสร้างความไว้วางใจขึ้นได้
- ร้องขอให้แพทย์ต้องรับรองข้อมูลอิเล็กทรอนิกส์ที่ตนเองสร้างขึ้น
- จำเป็นต้องหามาตรการที่สร้างความมั่นคงปลอดภัยของระบบสารสนเทศที่จะยืนยันให้ผู้เกี่ยวข้องทุกฝ่ายมีความเชื่อมั่นในระบบคอมพิวเตอร์และระบบเครือข่าย อันจะนำมาซึ่งความสำเร็จในการใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารอย่างไม่มีเงื่อนไข

Security ของระบบคืออะไร ?

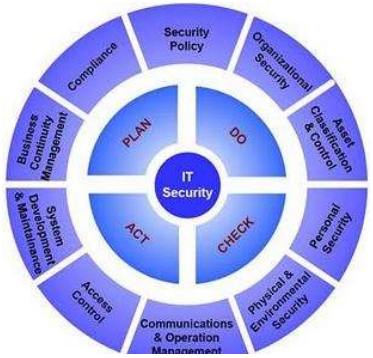
- ความลับของข้อมูล (Confidentiality)
- ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)
- สภาพความพร้อมใช้ของข้อมูล (Availability)

- ผู้ใช้มีตัวตนจริง (Authentication)
- ผู้ใช้มีสิทธิ์ในการจัดทำอะไรบ้าง (Authorization)
- ผู้ใช้ไม่สามารถปฏิเสธการกระทำ (Non repudiation)

การรักษาความมั่นคงปลอดภัย
คอมพิวเตอร์มีองค์ประกอบอะไรบ้าง

T ⟶ **Technology**

P ⟶ **Process**

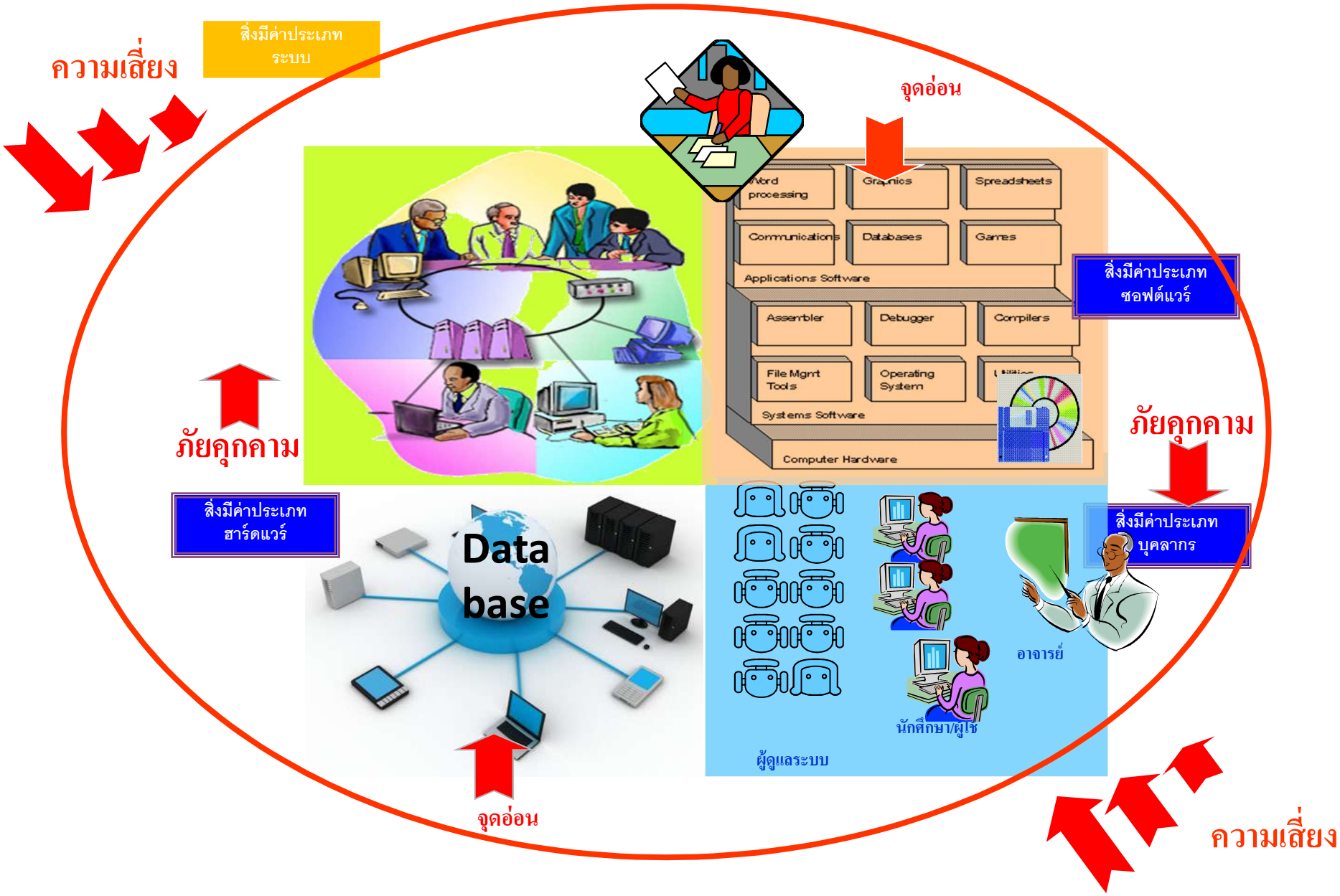


P ⟶ **People**

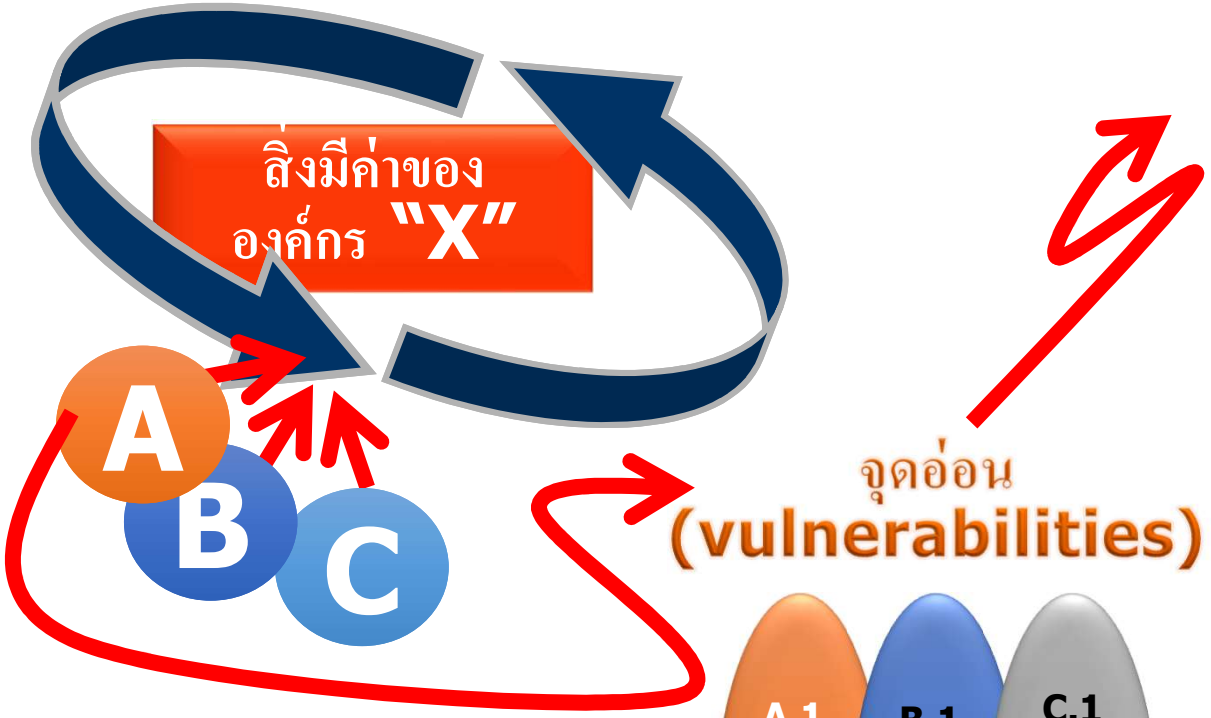
สาเหตุของปัญหาการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์

- เทคโนโลยี
  - การขาดความมั่นคงปลอดภัย
  - Bug, hole, no patch
  - ไม่มีมาตรฐานรับรอง
  - Hard to up-to-date
- กระบวนการ
  - การออกแบบเพื่อความมั่นคงปลอดภัย
  - ไม่มีการมอบหมายหน้าที่ความรับผิดชอบ
  - ไม่มีการตรวจสอบและติดตาม
  - ไม่มีแผนรองรับภัยพิบัติ
  - **Stay up-to-date**
- บุคลากร
  - ขาดความรู้
  - ขาดความมุ่งมั่น
  - ขาดการติดต่อสื่อสารที่ดี
  - **Human error**

ทรัพย์สิน ความเสี่ยง และภัยคุกคาม

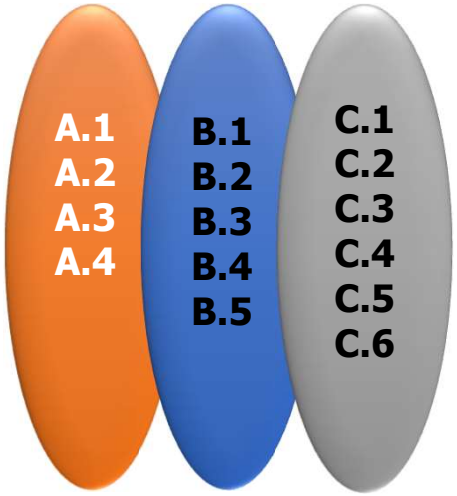


แนวทางการวิเคราะห์ความเสี่ยง ตามประเภทของทรัพย์สิน



ภัยคุกคาม
(threats)

จุดอ่อน
(vulnerabilities)



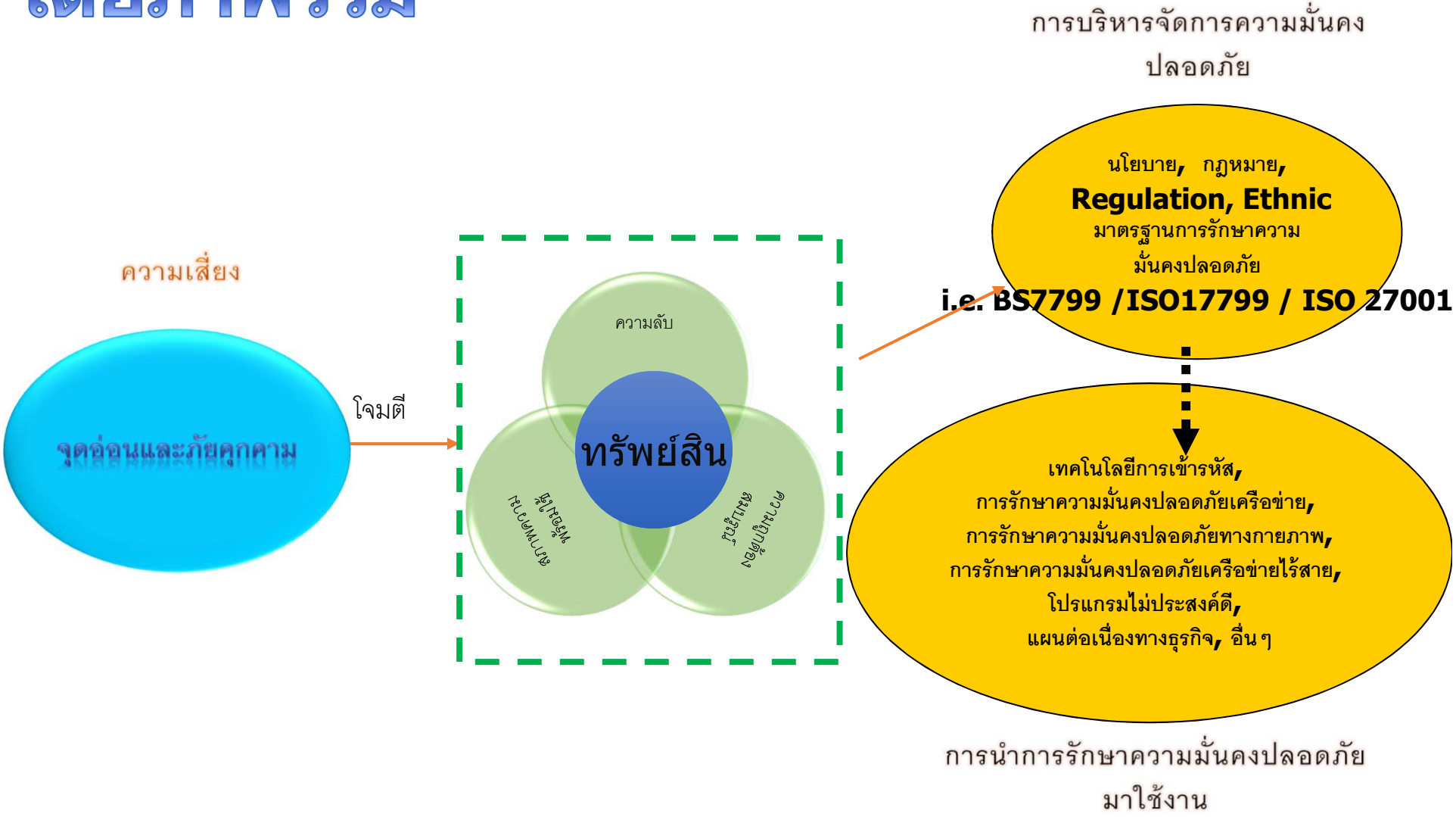
เลือกมาตรการ
(statement of applicable)

A.1.1	B.1.1	C.1.1
A.2.1	B.6.1	C.2.1
A.3.1	B.7.1	C.3.1
A.4.1	B.8.1	C.4.1
A.5.1	B.9.1	C.10.1
A.6.1		C.11.1
A.7.1		C.12.1
A.8.1		
A.9.1		
A.10.1		
A.11.1		
A.12.1		

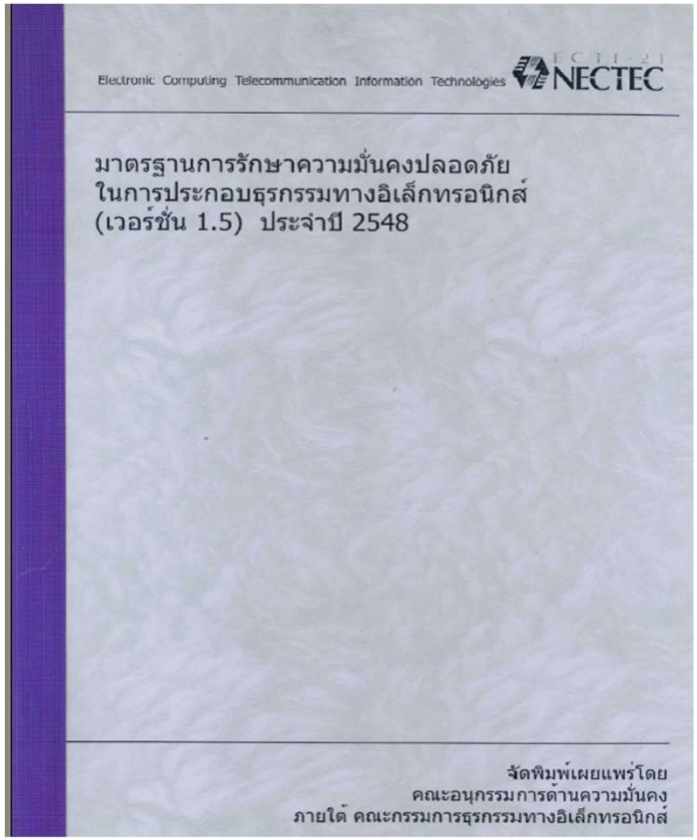
ทรัพย์สินในแต่ละประเภทกับภัยคุกคามและความเสี่ยงที่พบ

สิ่งมีค่า	ภัยคุกคาม	จุดอ่อน	มาตรการที่นำมาแก้ไข
ระบบเซิร์ฟเวอร์ ได้แก่ WWW Server DNS Server SMTP Server Radius Server	**A** ระบบเซิร์ฟเวอร์ถูกละเมิดความปลอดภัย	**A.1** ไม่มีคู่มือในการปฏิบัติงานสำหรับระบบเซิร์ฟเวอร์ จึงทำให้ผู้ดูแลระบบปรับแต่งค่าต่าง ๆ ของเครื่องให้บริการผิดพลาด	**8.1.1** ต้องมีการจัดทำคู่มือในการปฏิบัติงานของผู้ดูแลระบบ
	B ซอฟต์แวร์ไม่ประสงค์ดีทำลายข้อมูล	**B.1** ระบบไม่ได้รับการตรวจสอบไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดีอย่างสม่ำเสมอ	8.3.1 ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอ รวมทั้งตรวจสอบซอฟต์แวร์ที่ไม่ประสงค์
	**C** ระบบไม่สามารถให้บริการได้	**C.1** ขาดการสำรองข้อมูลการปรับแต่งค่าบนเครื่องเซิร์ฟเวอร์	**8.4** ต้องมีการสำรองข้อมูลของไฟล์ระบบของเซิร์ฟเวอร์
		C.2 ไม่มีการทดสอบซอฟต์แวร์ที่ใช้งานบนเครื่องเซิร์ฟเวอร์ก่อนใช้งานจริง	**10.4.1** ต้องมีการทดสอบซอฟต์แวร์ก่อนที่จะใช้งานจริง

การรักษาความมั่นคงปลอดภัยสารสนเทศโดยภาพรวม



มาตรฐาน ISO/IEC 27001,ISO/IEC 17799 (ภาษาไทย)



Electronic Transaction Security Standard (version 1)

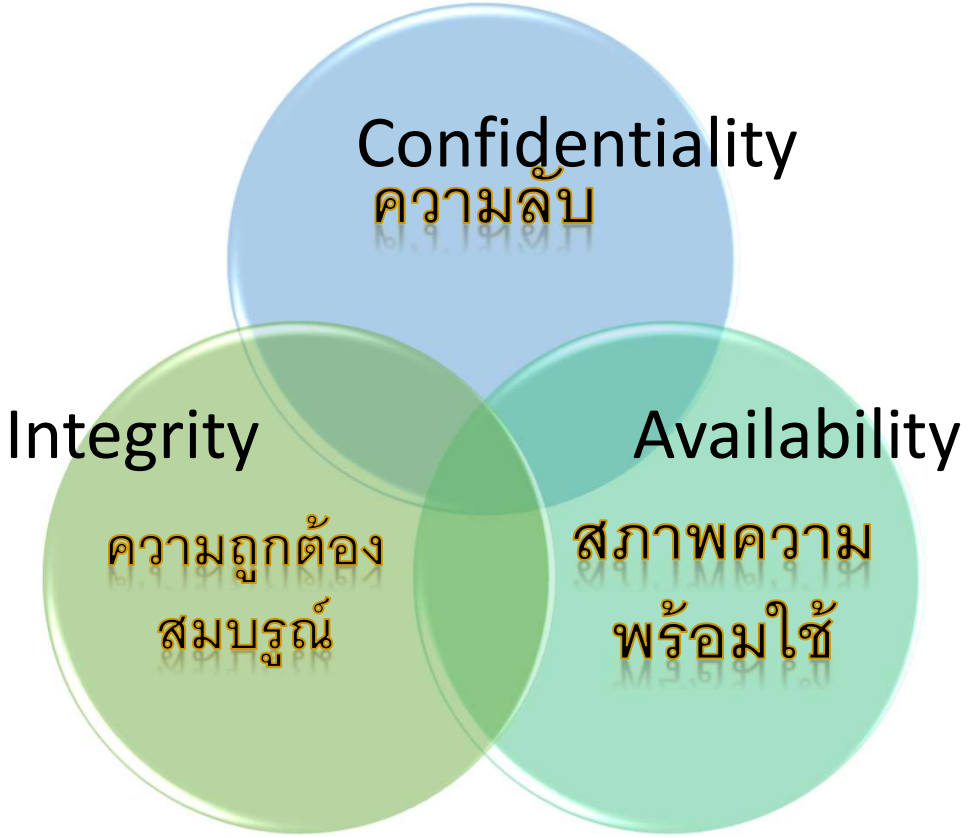
(Draft) Electronic Transaction Security Standard (version 1.5)

ข้อมูลสารสนเทศคืออะไร?

- ข้อมูลสารสนเทศคือทรัพย์สินซึ่งมีความสำคัญเช่นเดียวกับทรัพย์สินที่มีค่า
  ทางธุรกิจขององค์กร ดังนั้นข้อมูลสารสนเทศ
  จึงต้องได้รับการป้องกันอย่างเหมาะสม

ISO/IEC 17799:2005

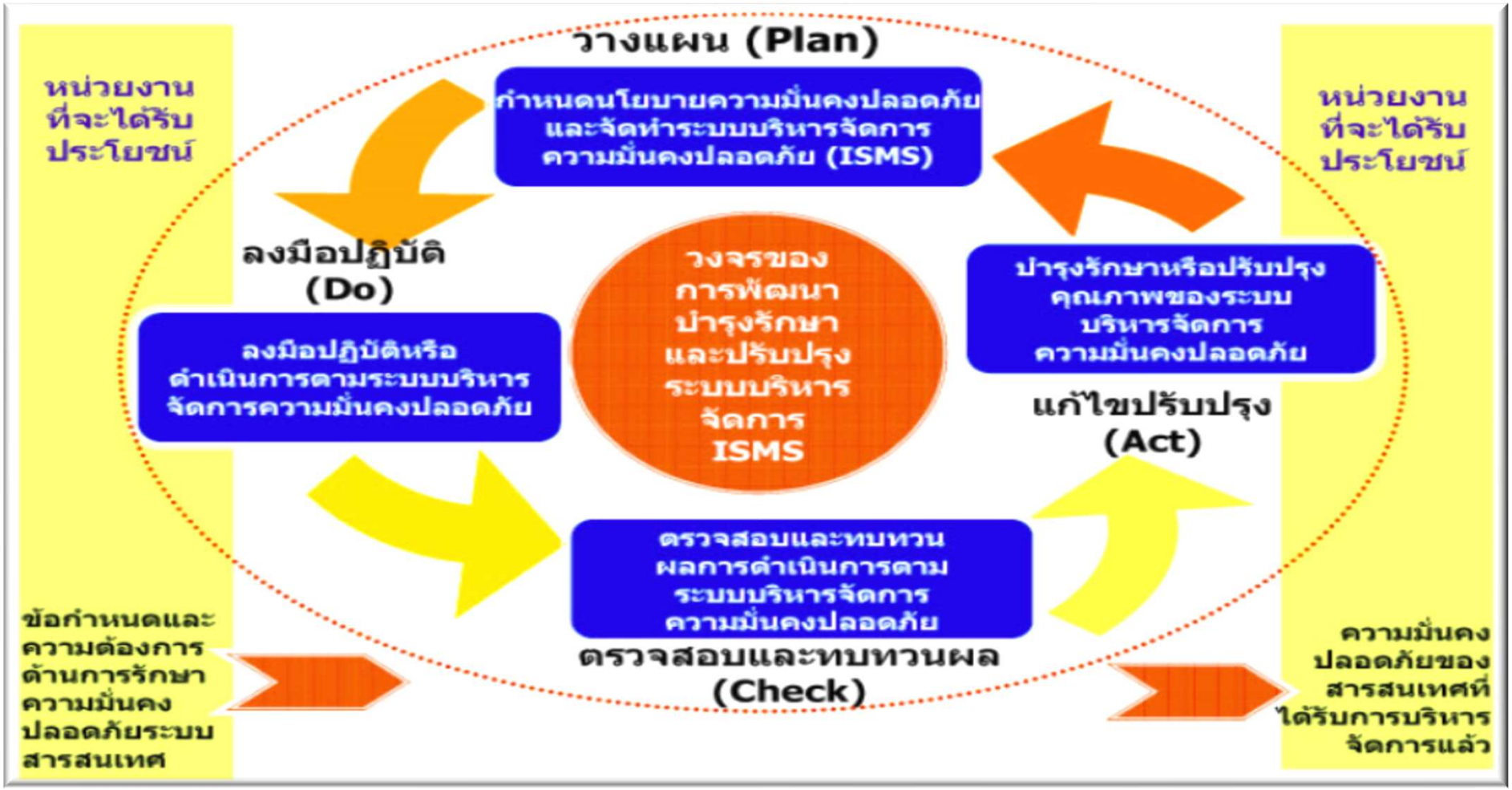
ความมั่นคงปลอดภัยสารสนเทศคืออะไร?



การคงไว้ซึ่ง ความลับ ความถูกต้องสมบูรณ์ และ สภาพความพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่นๆเช่น การพิสูจน์ตัวตน ความรับผิดชอบ การไม่ปฏิเสธความรับผิดชอบ และความน่าเชื่อถือ

ISO/IEC 27001:2005, page 2

แบบจำลอง PDCA ที่นำมาประยุกต์ใช้กับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ



กรอบการทำงานของ ISO/IEC 27001

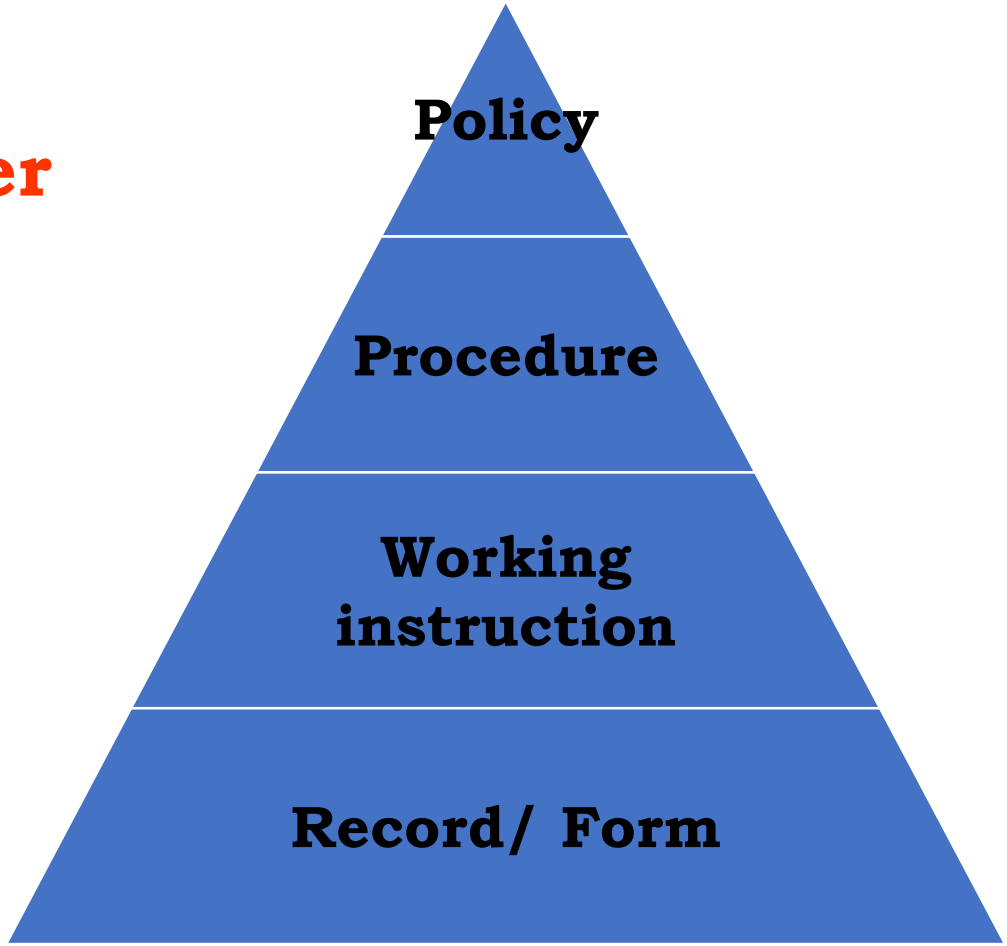
Four layers of documentation structure

1st Layer

2nd Layer

3rd Layer

4th Layer



A.5 นโยบายความมั่นคงปลอดภัย

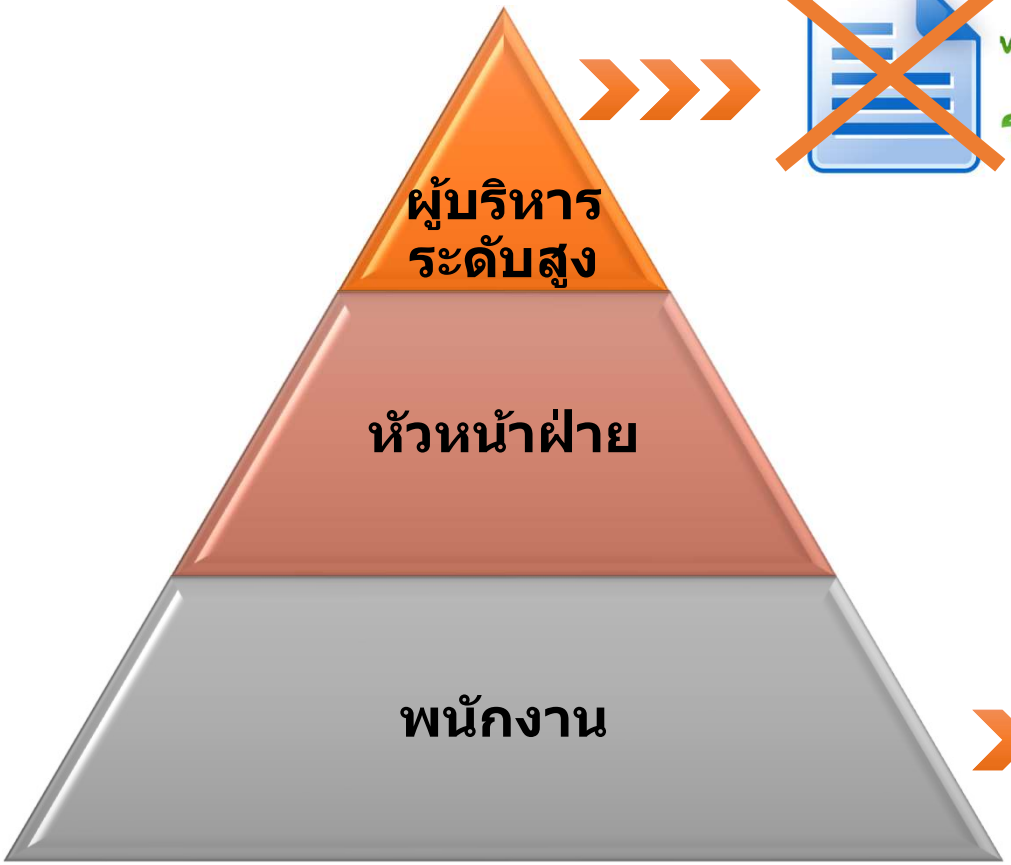
• A.5.1 นโยบายความมั่นคงปลอดภัย (2)

- กำหนดขอบเขตของการรักษาความมั่นคงปลอดภัย
- การแสดงเจตจำนงของผู้บริหารเพื่อให้พนักงานเห็นถึงวามสำคัญของการรักษาความมั่นคงปลอดภัย
- มีการกำหนดหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน
- การให้คำนิยามคำว่า"การรักษาความมั่นคงปลอดภัยสารสนเทศ"
- 1) .....;
- 2) .....;
- มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย

.....

1. เอกสารนโยบายความมั่นคงปลอดภัย
2. ทบทวนเอกสารนโยบายความมั่นคงปลอดภัย

ตัวอย่าง: การขาดนโยบายความมั่นคงปลอดภัยและเอกสารต่างๆ (A.5)



ไม่มีนโยบายความมั่นคงปลอดภัยจากระดับผู้บริหารสู่พนักงานระดับล่าง

ผลจากการไม่มีนโยบายฯ จากผู้บริหารขององค์กร พนักงานขององค์กรไม่มีแนวทางปฏิบัติที่เหมาะสมและอาจทำการละเมิดความปลอดภัยของระบบสารสนเทศในองค์กร

A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

A.6.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (8)

1. การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย
2. การประสานงานความมั่นคงปลอดภัยภายในองค์กร
3. การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย
4. กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ
5. การลงนามไม่ให้เปิดเผยความรับขององค์กร
6. การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่นๆ
7. การมีรายชื่อและข้อมูลสำหรับการติดต่อกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน
8. การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระ

A.6.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก(3)

1. การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก
2. การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร
3. การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร

ตัวอย่าง: การขาดการใช้งานนโยบายความมั่นคงปลอดภัยร่วมกัน(A.6.1.3)

ตัวอย่าง : ขาดการระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร

สัญญาไม่ครอบคลุมพอเพียง

ถูกขโมยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต, อื่นๆ

A.7 การบริหารจัดการทรัพย์สินองค์กร

A.7.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (3)

1. การจัดทำบัญชีทรัพย์สิน
2. การระบุผู้เป็นเจ้าของทรัพย์สิน
3. การใช้งานทรัพย์สินที่เหมาะสม

A.7.2 การจัดหมวดหมู่สารสนเทศ (2)

1. การจัดหมวดหมู่สารสนเทศ
2. การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ

ตัวอย่าง: การขาดการจัดทำบัญชีทรัพย์สิน (A.7.1.1)

Information: Database, File, etc.

Software: software, application, tools, etc.

Hardware: Computer, communication equipment, etc.

Processes and services : Applications etc.

People: IT staff, manager, etc.

Printer Inventory

Printer Types	No. of PC connected	Location	Responsible Person	Other Details
HP LaserJet 4050 Series	3	5th Floor	John	Memory 8 MB, DWS:5.90 I/O Buffering : 100 KB Allocated of 4000 KB Available PS Wait Time-out 300S , Resolution : 1200x1200 dpi
HP LaserJet 1300	3	5th Floor IT Manager Room	Kitti	Memory 16 MB, Resolution 1200 x 1200 dpi PS Wait Time-out 300S 20 ppm black
HP LaserJet 4200 dtn	34	4th Floor	Mary	Model Number : 56057 A Memory 64 MB , 8 MB Flash ROM , Idle Time-out 90 s
HP LaserJet 2200 Series	11	6th Floor 3rd Floor	Jennifer	Resolution 1200 x 1200 dpi , 19 ppm (letter) , 18 ppm (A4) Supports HP PCL 6 , Memory 16 MB
HP Deskjet 1220C	5	2nd Floor	Mike	11 ppm black (600x600 dpi) up to 9.5 ppm colour (2400x1200 dpi)
HP Designjet 500	2	1st Floor	Michale	Model Number : C7770B, 42 inches , RAM 160 MB Ink Use : Black 2 cc, Cyan 1 cc, Magenta 3 cc , Yellow 2 cc Engine F/W : A.02.06

มีชื่อบุคคลที่รับผิดชอบ

ตัวอย่าง: การขาดการจัดหมวดหมู่สารสนเทศ (A.7.2)

เอกสารลับมาก

เอกสารลับที่สุด

เอกสารลับ

เอกสารทั่วไป

A.8 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

A.8.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (3)

1. การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย
2. การตรวจสอบคุณสมบัติผู้สมัคร
3. การกำหนดเงื่อนไขการจ้างงาน

A.8.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (3)

1. หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย
2. การสร้างความตระหนัก การให้ความรู้ และการอบรมความมั่นคงปลอดภัยให้แก่พนักงาน
3. กระบวนการทางวินัยเพื่อลงโทษ

A.8.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (3)

1. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน
2. การคืนทรัพย์สินขององค์กร
3. การถอดถอนสิทธิในการเข้าถึง

ตัวอย่าง: การขาดวิธีการตรวจสอบคุณสมบัติของผู้สมัครงานอย่างเหมาะสม (A.8.1.2)

Before

After

ตัวอย่าง: การขาดการลงนามในสัญญาไม่เปิดเผยความลับ (การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน) (A.8.1.3)

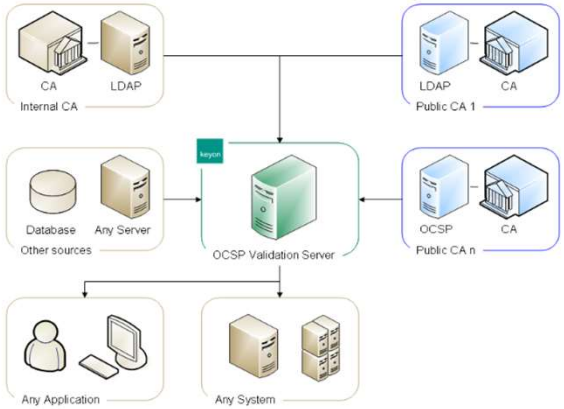
พนักงานใหม่/
ผู้ติดต่อรายใหม่

สองวันผ่านไป

การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (A.8.2)
การขาดการสร้างความตระหนัก การให้ความรู้
และการอบรมด้านวามมั่นคงปลอดภัยให้พนักงาน

ตัวอย่าง: การขาดการถอดถอนสิทธิในการเข้าถึง (A.8.3.3)

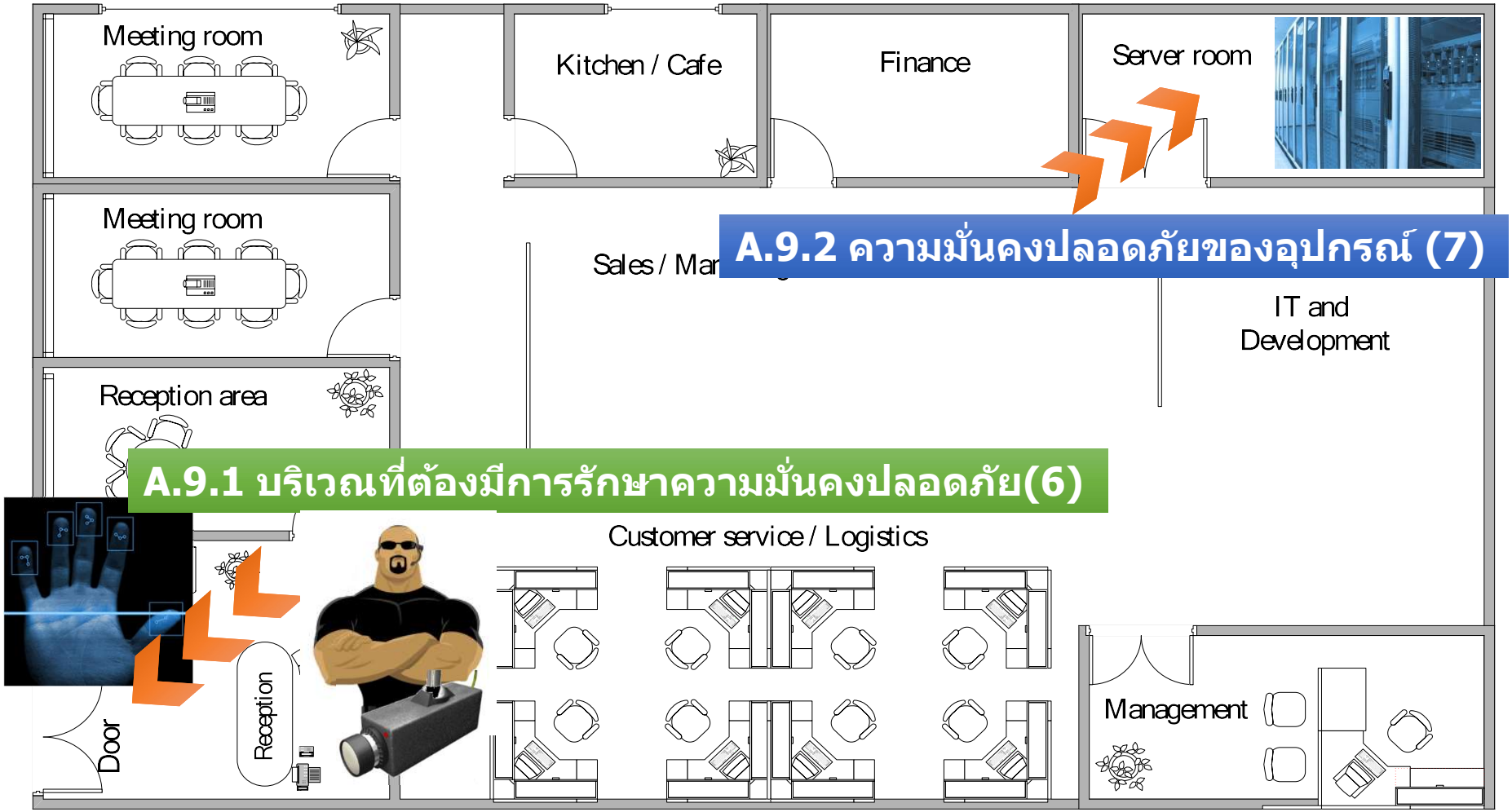
ถอดถอนสิทธิการเข้าถึงระบบหรือเครือข่าย
(Access to System or Network)



Terminated staff

ถอดถอนสิทธิการเข้า-ออกทางกายภาพ
(Access to the sensitive areas)

A.9 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม



ตัวอย่าง: การขาดการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (A.9)

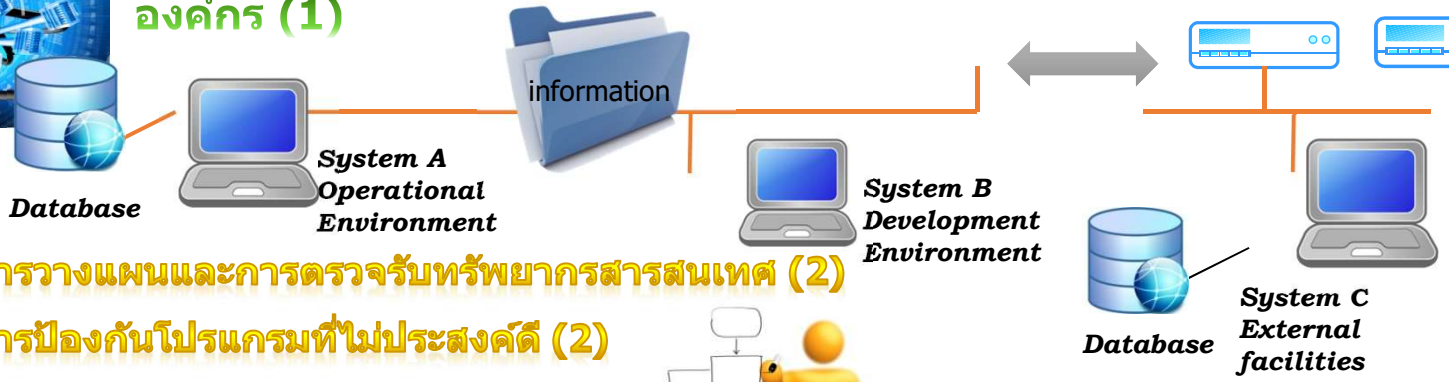
A.10 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

A.10.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (4)

A.10.2 1 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (3)

A.10.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (1)

A.10.8 การแลกเปลี่ยนสารสนเทศ (5)



A.10.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (2)

A.10.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (2)

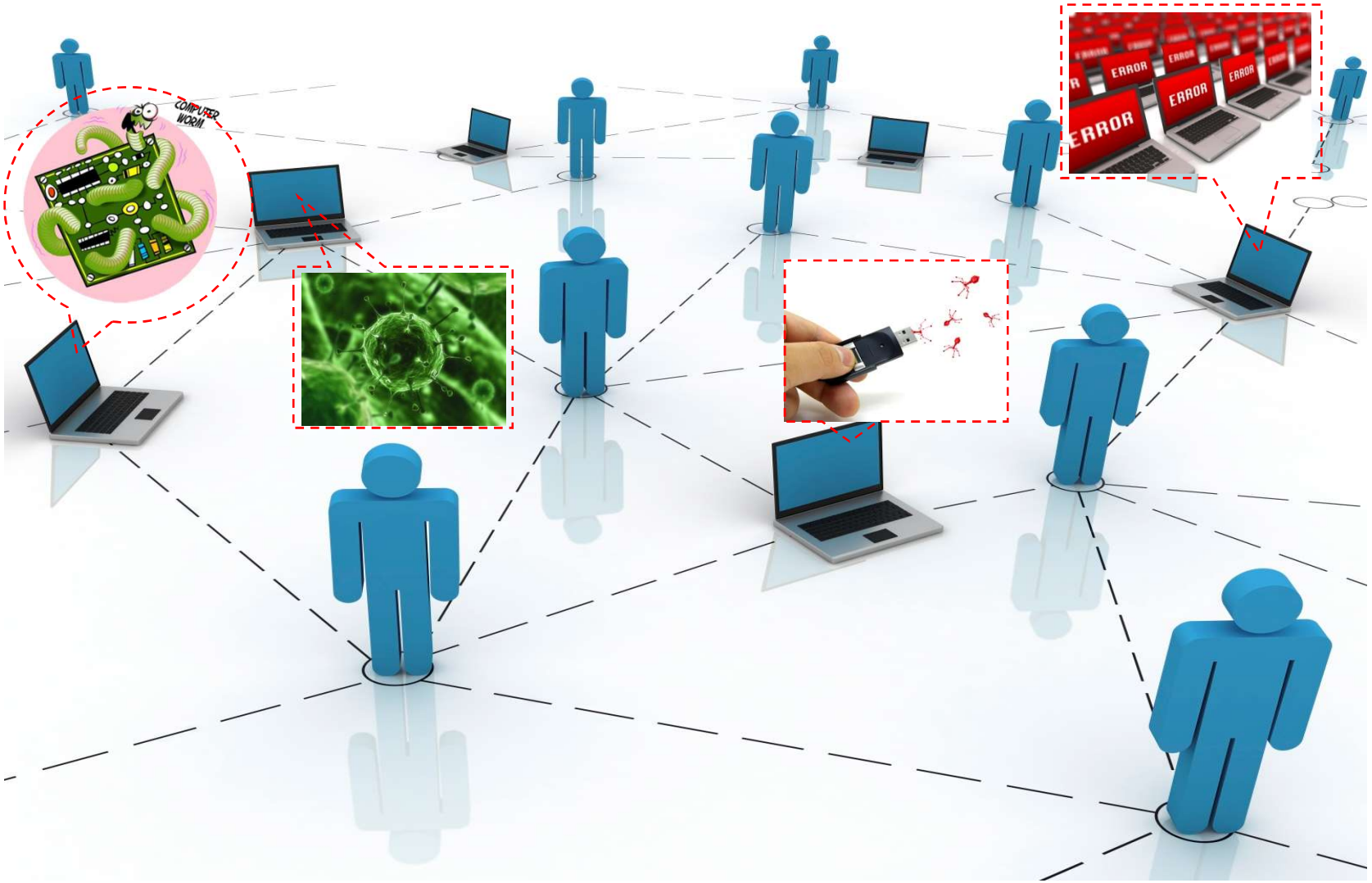
A.10.5 การสำรองข้อมูล (1)

A.10.7 การจัดการสื่อที่ใช้บันทึกข้อมูล (4)

A.10.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (6)

A.10.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (3)

ตัวอย่าง: การขาดการป้องกันโปรแกรมที่ไม่ประสงค์ดี (A.10.4.1)



ตัวอย่าง: การขาดนโยบายการทำลายสื่อบันทึกข้อมูล (A.10.7.2)

To compare a promotion and/or tenure candidate's teaching to other instructors' teaching, departments need to report the comparator group. Many departments do not report the group of instructors or courses that define departmental means, standard deviations, and z-scores. Are the comparators all instructors and all courses, or are evaluations stratified into sub-categories by course level or type? Are courses taught by graduate students and adjuncts separated into their own category or included with those of the tenure-related faculty? Without these facts, the magnitudes of means, and the signs and sizes of z-scores, necessary for comparative analysis, are uninformative.

Many departments also misinterpret z-scores. "Significant" z-scores are only those greater than +2.0 or less than -2.0 (if departments define comparator groups and if certain statistical assumptions are met). Many departments assert "significant" deviations from means when no z-scores exceed the +/-2.0 criterion. Other departments overlook obvious z-score patterns (such as all-negative or all-positive values, or over-time trends) in favor of simple counts of z-scores with large values.

When creating summary tables of quantitative course evaluations, departments should explain their choices and copy the data carefully. It is often illustrative to report certain course types separately (e.g., graduate vs. undergraduate, specialty area vs. non-specialty area, mass classes vs. small classes). When less than half of enrolled students complete course evaluations, the results should be treated as unreliable. Courses with very few students and that involve substantial independent study (such as internship, dissertation, reading and conference) are not appropriate to evaluate. Some departments do not make such distinctions, some exclude certain courses from summary reports for no obvious reason and some make transcription errors when creating summary tables. Such problems potentially mislead peer reviewers and unnecessarily burden FPC.

If quantitative teaching evaluations are to be useful in promotion and tenure evaluations, departments must, at a minimum, identify and report comparator groups, accurately report and interpret z-scores, and explain their summary tables. Better, UO should (1) consider adopting new, improved methods for quantitative teaching evaluation than enables departments to more easily avoid problems like those described above, and (2) consider creating a template summary table for quantitative evaluations to standardize the reporting process. Either improvement will reduce burdens in the peer review process.

Our further suggestions and comments follow:

1. Candidates should prepare their vitas with great care, and vitas should be reviewed at the department level before submission of the case. The department should work with the candidate to assure that the vita is neither over- nor understated (we have seen examples of both). It is important that candidates list publications with full citation, indicate which journal articles have been refereed, provide full employment history, and list all relevant internal and external service.

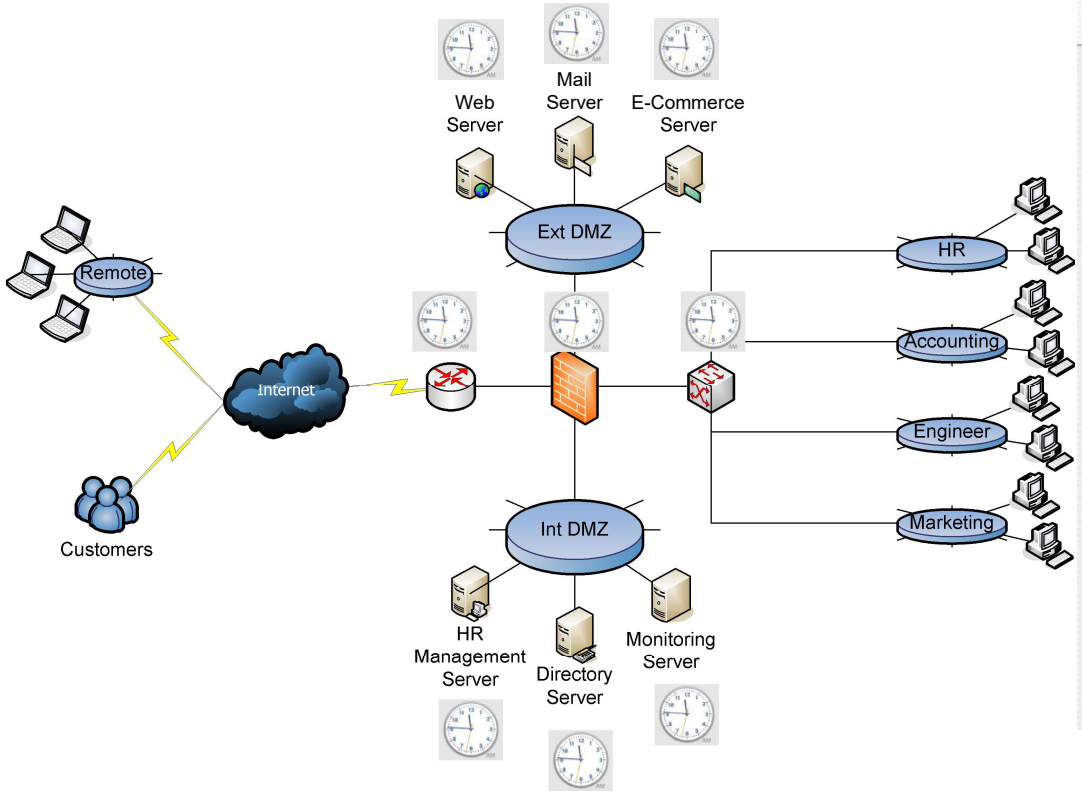
ข้อมูลภายในสื่อบันทึก

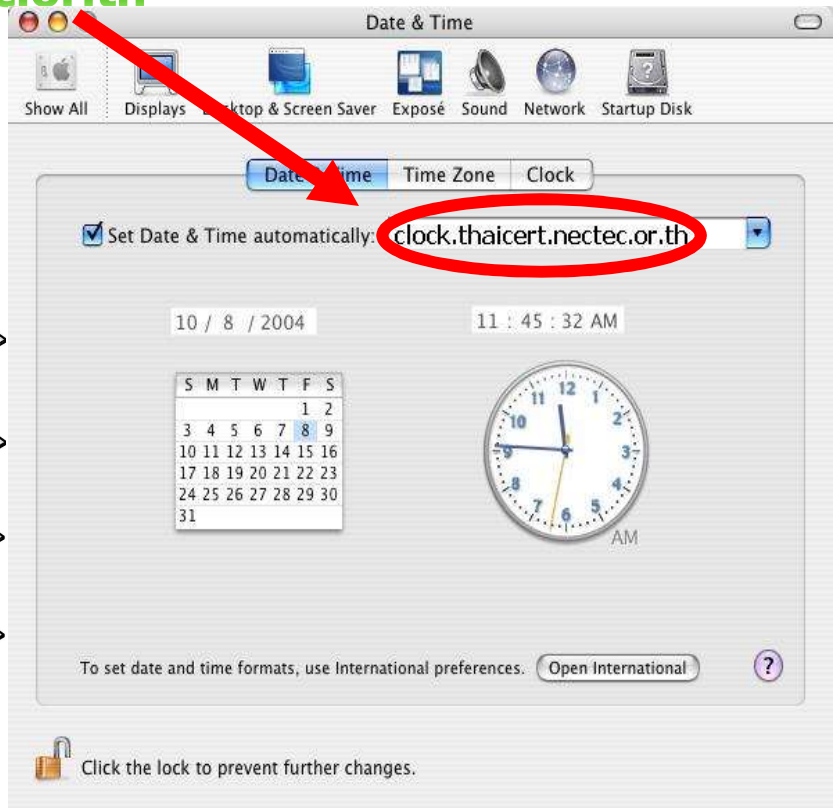
ลบข้อมูล

ข้อมูลถูกทำลายและสามารถกู้คืนได้

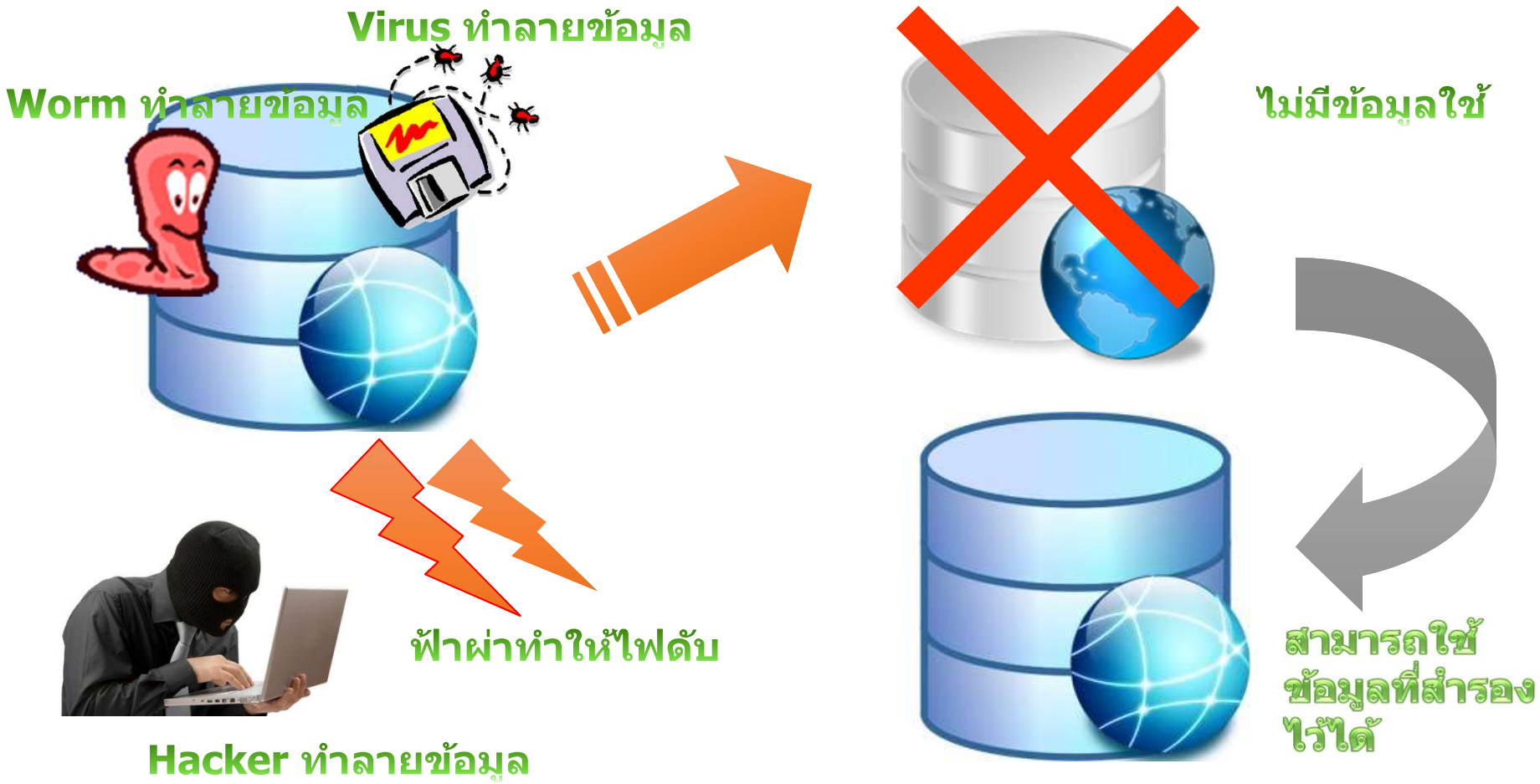
ตัวอย่าง: การขาดการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (A.10.10.6)

สามารถเทียบเวลาได้จาก
clock.thaicert.nectec.or.th





ตัวอย่าง: การขาดขั้นตอนปฏิบัติสำหรับการสำรองข้อมูล (A.10.5)



Procedure name: Backup Procedure
Procedure responsible person: System Admin

1. ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่ดังนี้

ที่	รายการ	สิ่งที่แบคอัพ	ความถี่ในการแบคอัพ
1.1	Mail servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ็อกซ์	1 ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
1.2	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
1.3	Database servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
1.4	Firewall server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
1.5	Server อื่นๆ (สป.ต้องกำหนดเองว่าเซิร์ฟเวอร์อื่นๆ ได้แก่ อะไรบ้าง)	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบนเซิร์ฟเวอร์อื่นๆ	1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
<u>หมายเหตุ</u> ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup			

2. ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่
3. กรณีที่สมบูรณ์ ผู้ดูแลระบบนำสื่อบันทึกข้อมูลแบคอัพไปเก็บไว้นอกสำนักงานในสถานที่ที่ปลอดภัย
4. กรณีที่ไม่สมบูรณ์ ผู้ดูแลระบบต้องแก้ไขให้แบคอัพสมบูรณ์และกลับไปทำตามข้อ 1 ใหม่

A.11 การควบคุมการเข้าถึง

A.11.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (1)

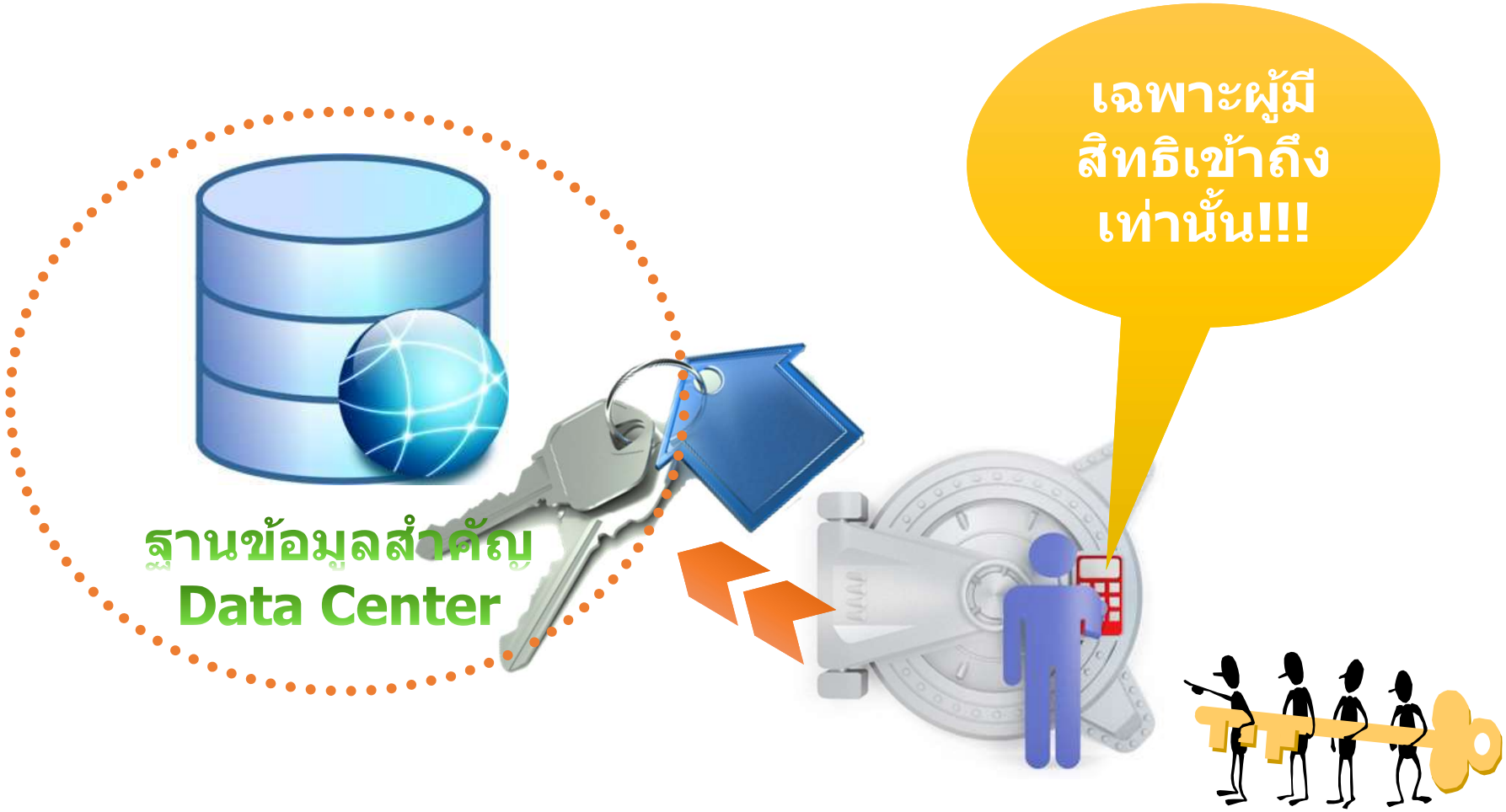
A.11.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (4)

A.11.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (3)

A.11.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (6)

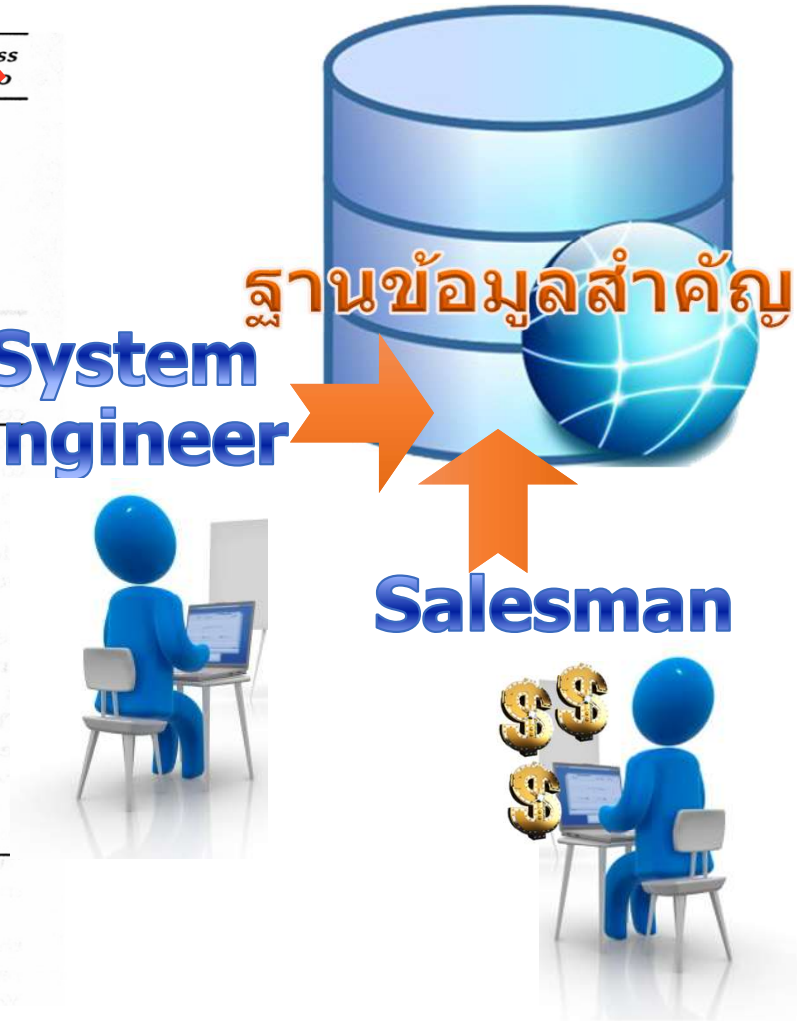
A.11.6 การควบคุมการเข้าถึงแอปพลิชันและสารสนเทศ (2)

ตัวอย่าง: การขาดนโยบายควบคุมการเข้าถึง (A.11.1.1)

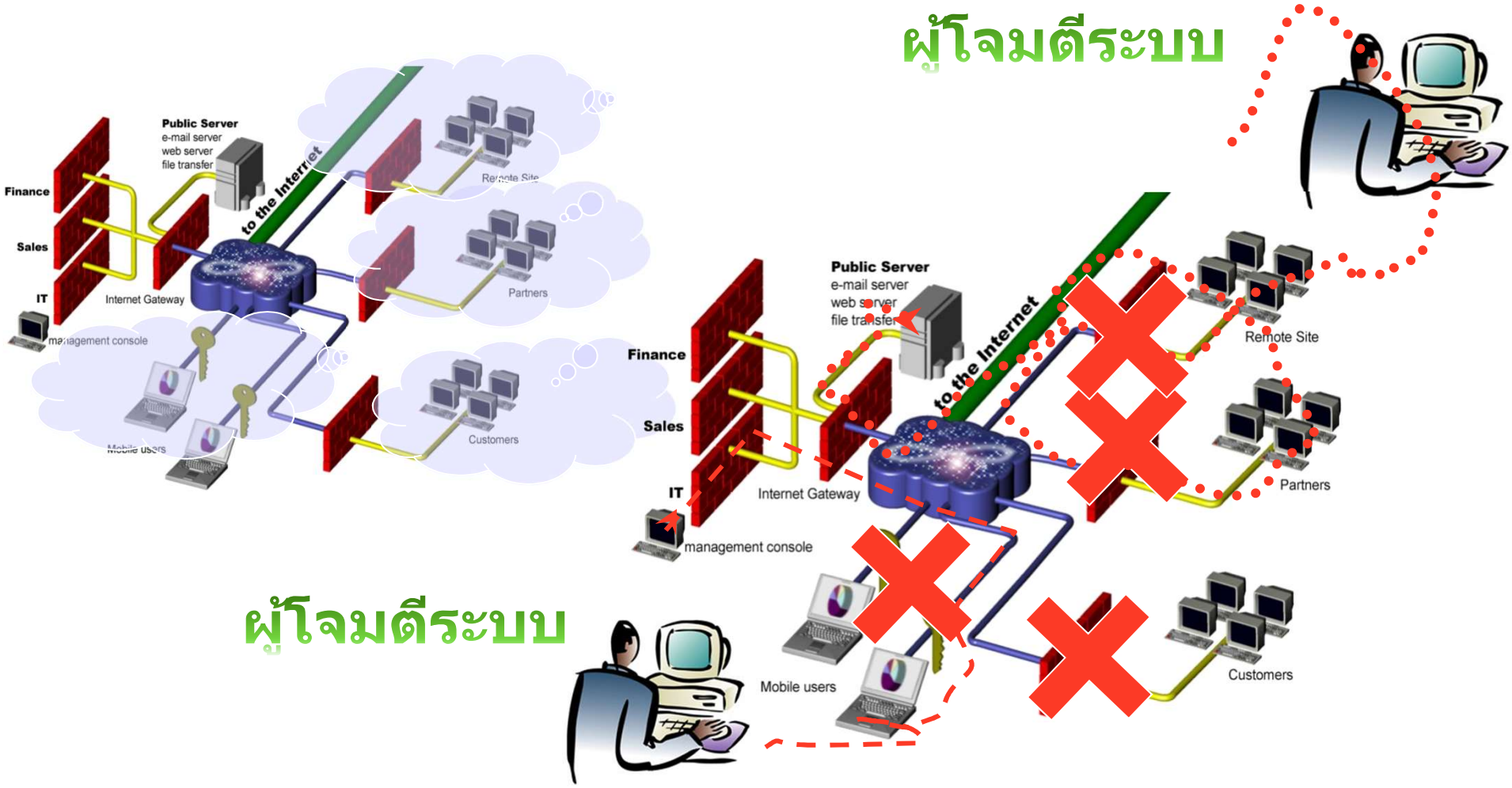


ตัวอย่าง: การขาดการบริหารจัดการสิทธิการใช้ระบบ (A.11.2.2)

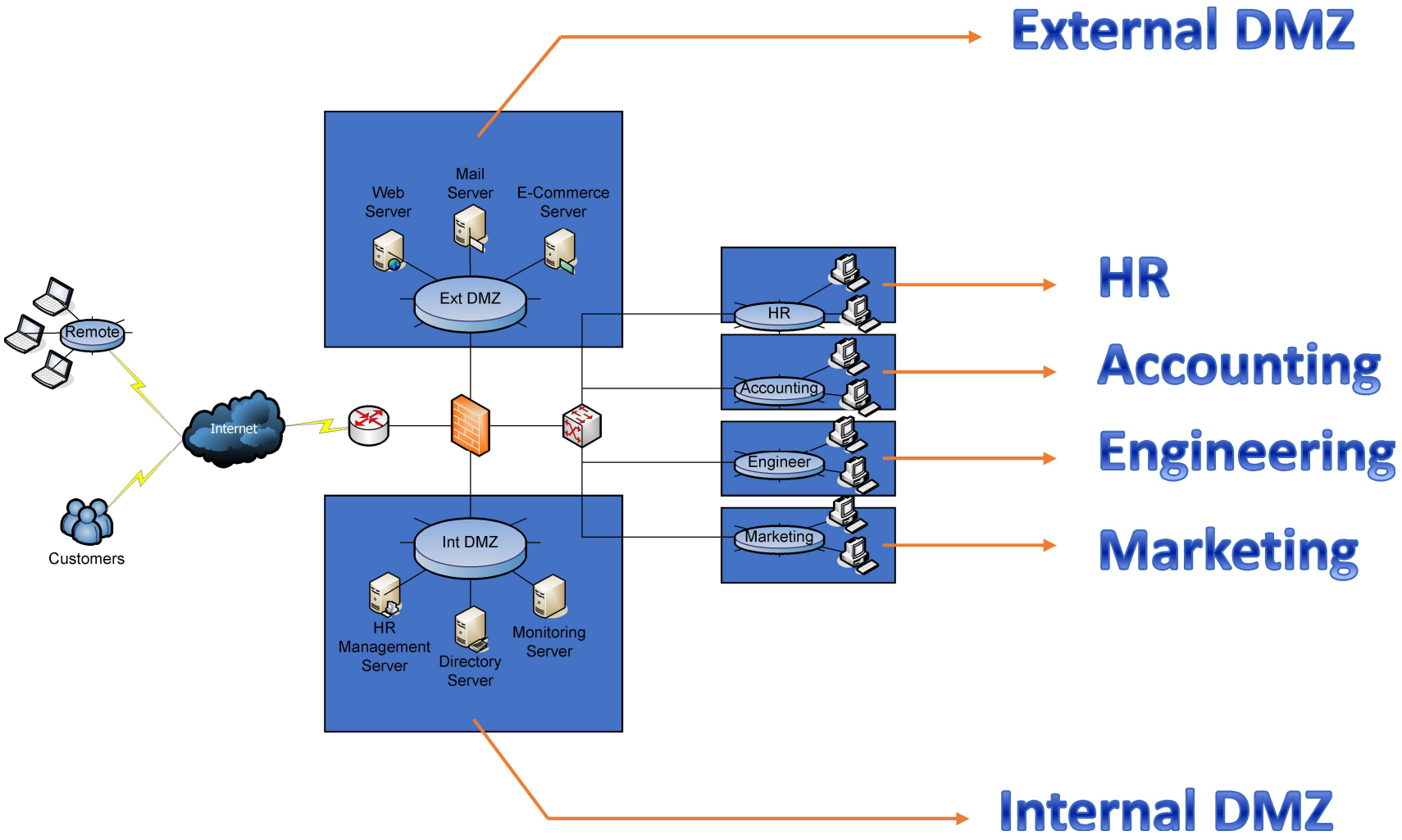
Information Need	*Sales Site*	*System Eng. Site*	*Mfg. Site*	*Geo. Area*	*Global*	*Process Group*
Marketing:						
Customer Information	Y	Y		Y	Y	Y
Pricing and discounts	Y	Y		Y	Y	
Quote	Y	Y		Y	Y	
Forecasting	Y	Y	Y	Y	Y	
Technical Reference	Y	Y		Y	Y	Y
Agreements, Contracts, TC	Y	Y		Y	Y	Y
Sales Goals, Credits	Y					
Pursuit Information	Y			Y	Y	Y
Competitor	Y			Y	Y	Y
Training Course	Y	Y		Y		
Sales Tools (Bulletin Board)	Y	Y		Y	Y	Y
Order:						
Order Information	Y	Y	Y	Y	Y	Y
Project Information	Y	Y	Y	Y	Y	Y
Bookings	Y			Y	Y	
Backlog			Y	Y	Y	
Item and Model Level	Y	Y	Y	Y	Y	
CAD Design Information		Y	Y	Y	Y	
Configurator	Y	Y		Y	Y	
Sales	Y			Y	Y	Y
Distributions Req Plan	Y		Y		Y	
Shipping	Y		Y			
Invoicing					Y	Y
Order Status	Y	Y	Y			
Project History	Y	Y		Y	Y	
Service Level	Y	Y	Y	Y	Y	
Table of Denial	Y					
Project Engineering:						
Project P&L	Y	Y	Y	Y	Y	
Resource Availability		Y		Y	Y	
Project Scheduling		Y		Y		
Resource Skills		Y		Y	Y	



ตัวอย่าง: การขาดกรแบ่งแยกเครือข่าย (A.11.4.5)
การขาดการควบคุมการเชื่อมต่อทางเครือข่าย (A.11.4.6)



ตัวอย่างการแบ่งแยกเครือข่าย (A.11.4.5)



ตัวอย่าง: การขาดการใช้นโยบายการป้องกันอุปกรณ์สื่อสารประเภทพกพา (A.11.7.1)

เอกสารสำคัญมาก
.....
.....

Encrypted

ตัวอย่าง: การขาดขั้นตอนปฏิบัติสำหรับการปฏิบัติงานจากภายนอกสำนักงาน (A.11.7.2)

internet

Tele working

A.12 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

A.12.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (1)

A.12.3 มาตรการการเข้ารหัสข้อมูล (2)
- A.12.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล
- A.12.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล

A.12.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (4)

A.12.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (3)

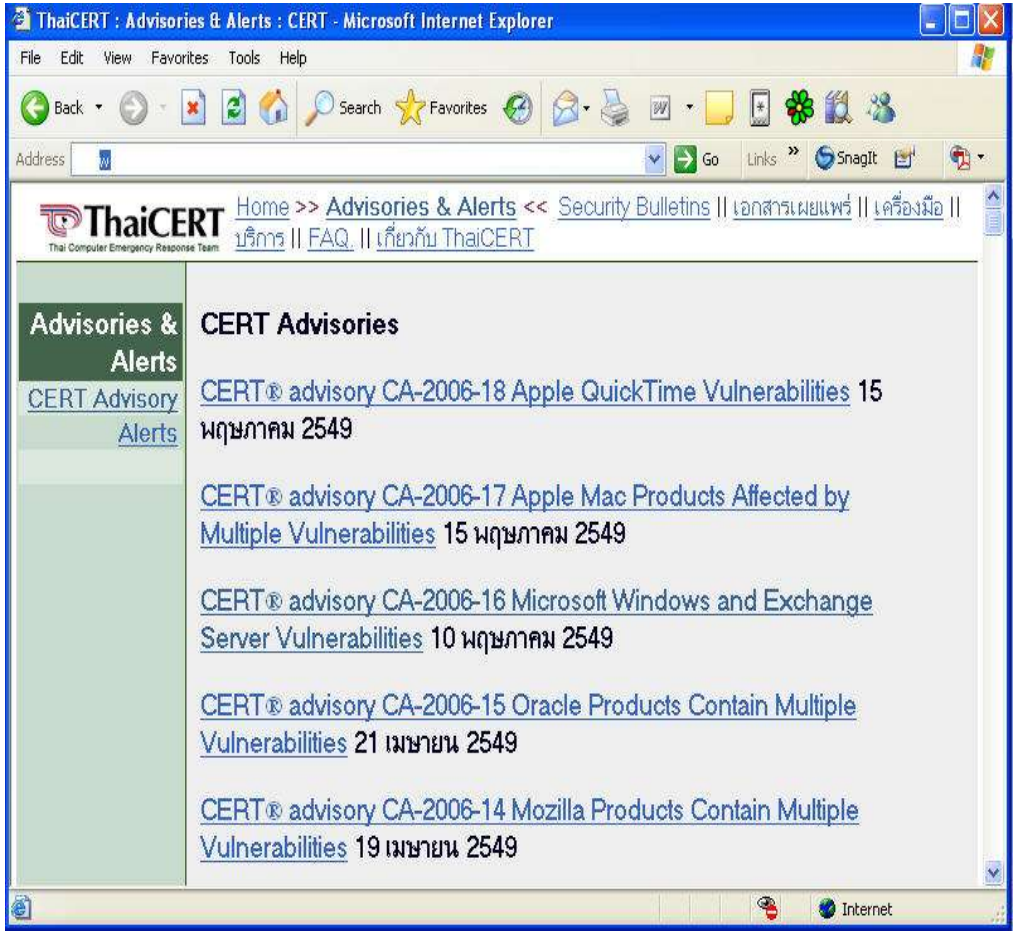
A.12.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (5)

A.12.6 การบริหารจัดการช่องโหว่ (1)

ตัวอย่าง: การขาดการตรวจสอบข้อมูลนำเข้า (A.12.2.1)

Input data validation

Buffer Overflow



Most of vulnerabilities cause Buffer Overflow

ตัวอย่าง: การขาดมาตรการควบคุมช่องโหว่ทางเทคนิค (A.12.6.1)

ระบบที่มีช่องโหว่อาจ<u>ถูกโจมตี</u>
<u>เช่น การขโมยข้อมูลลับ</u>

ระบบที่ได้รับการแก้ไขช่องโหว่
สามารถ<u>ป้องกัน</u>การถูกโจมตีได้

A.13 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

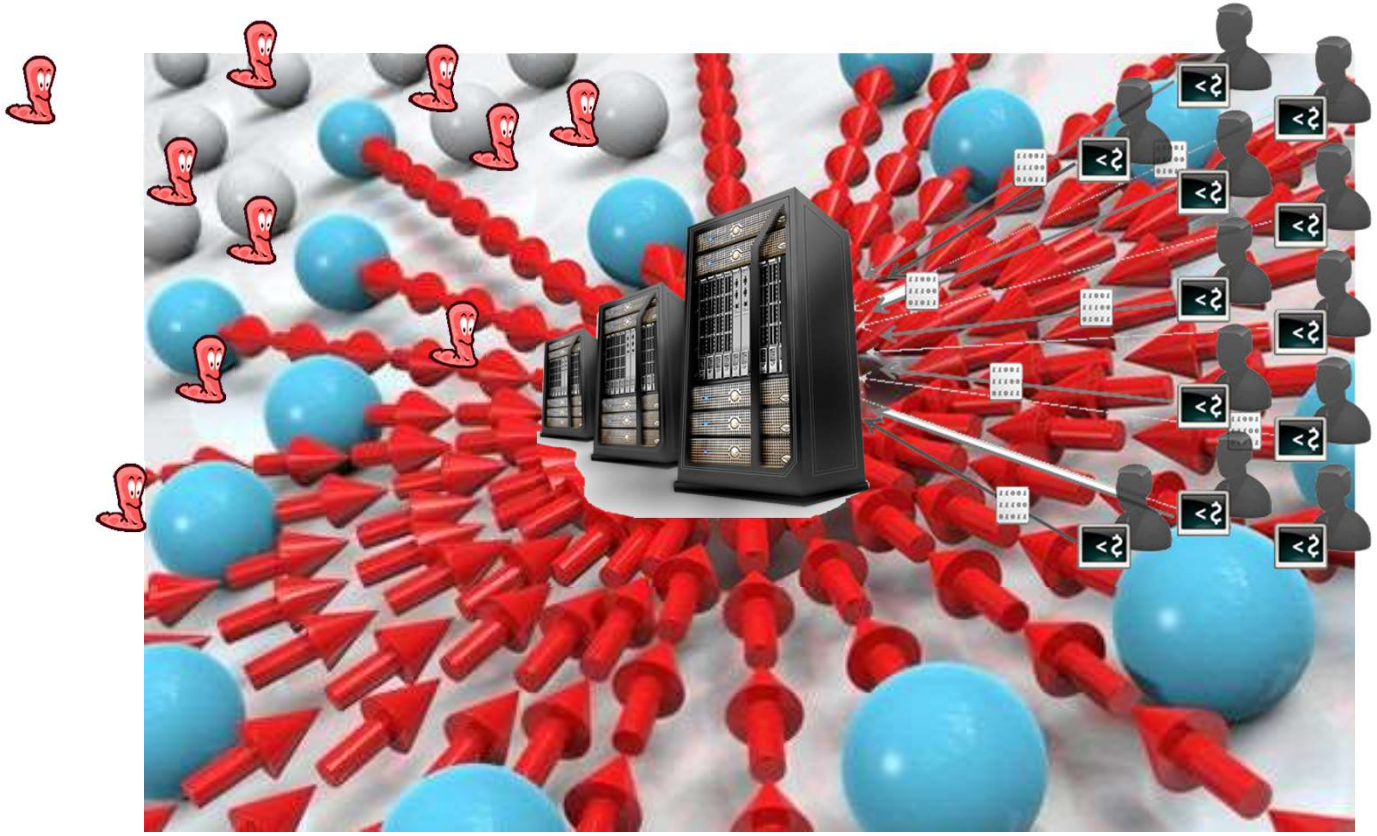
A.13.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย(2)

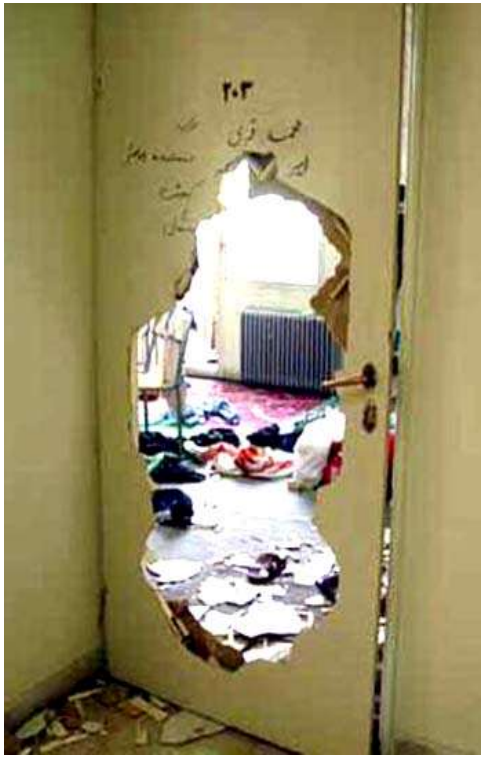
1. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง
2. การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

A.13.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย(3)

1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ
2. การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
3. การเก็บรวบรวมหลักฐาน

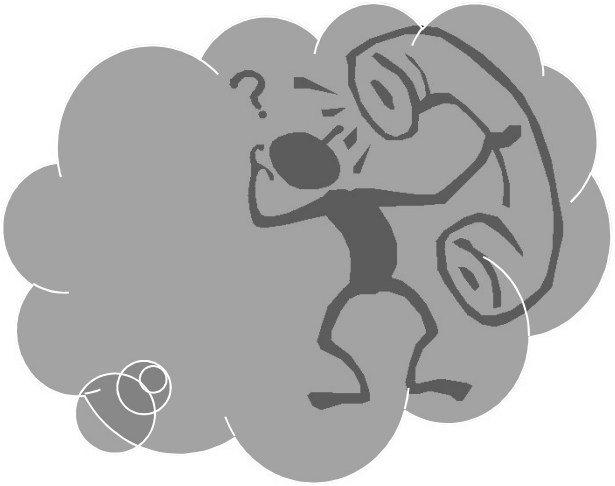
ตัวอย่าง: การขาดการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย(A.13.1)



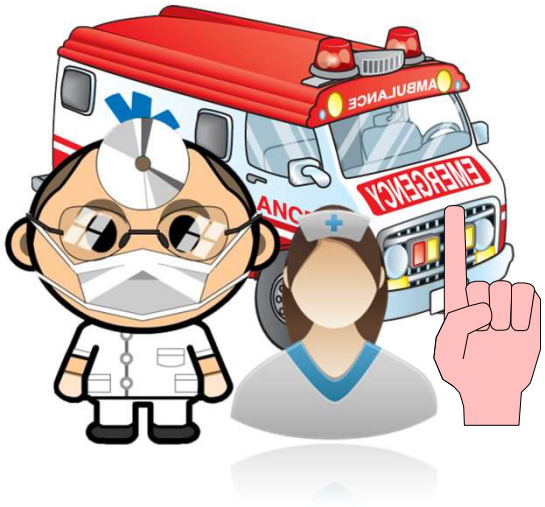


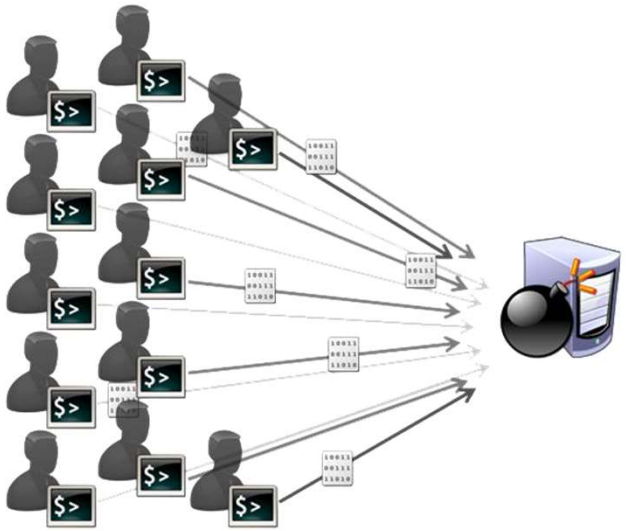
Denial of Service (DoS)

ตัวอย่าง: การขาดการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (A.13.2)



Call Center





A.14 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

A.14.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (5)

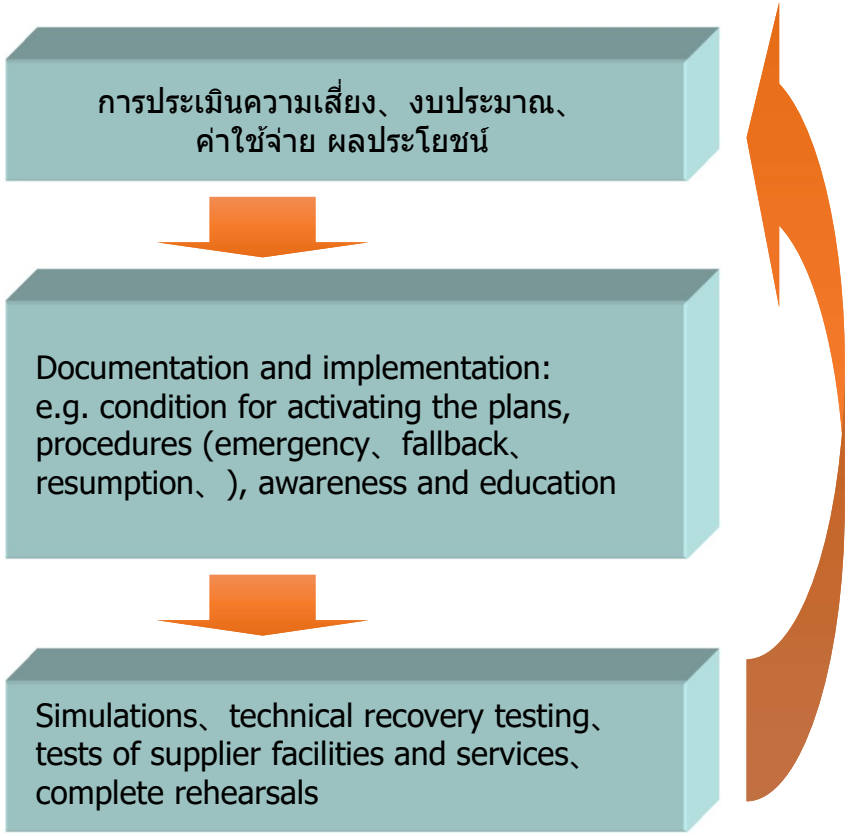
A.14.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ

A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ

A.14.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ

A.14.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ

A.14.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ



ตัวอย่าง: การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

เหตุภัยพิบัติที่ไซต์หลัก

ย้ายไปสู่
ไซต์สำรอง

ไซต์สำรอง

การบริหารความต่อเนื่องในการดำเนินงานขององค์กรที่ไม่สมบรูณ์

- ขาดการกำหนดแอปพลิเคชั่นที่มีความสำคัญในการกู้คืน
- ขาดการกำหนดระยะเวลานานที่สุดที่ต้องทำการกู้คืนกระบวนการทางธุรกิจ
- การสำรองข้อมูลที่ไม่สมบรูณ์
- ขาดความตระหนัก
- ขาดแผนการฝึกซ้อม

A.15 การปฏิบัติตามข้อกำหนด

A.15.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (6)

1. การระบุข้อกำหนดต่างๆที่มีผลทางกฎหมาย
2. การป้องกันสิทธิและทรัพย์สินทางปัญญา(IPR)
3. การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร
4. การป้องกันข้อมูลส่วนตัว
5. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์
6. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด

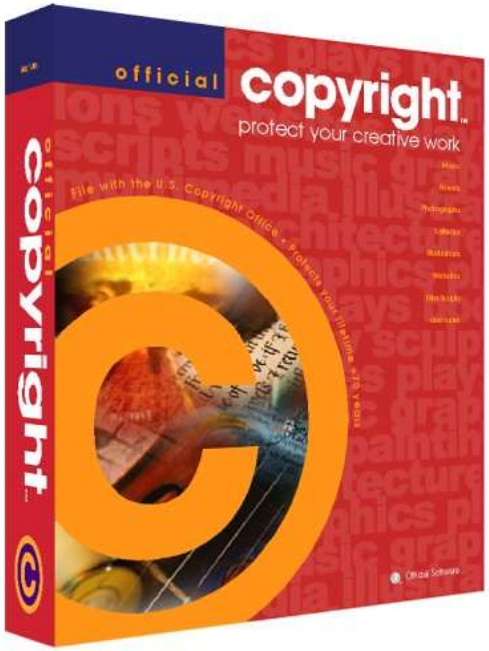
A.15.2 การปฏิบัติตามนโยบายมาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (2)

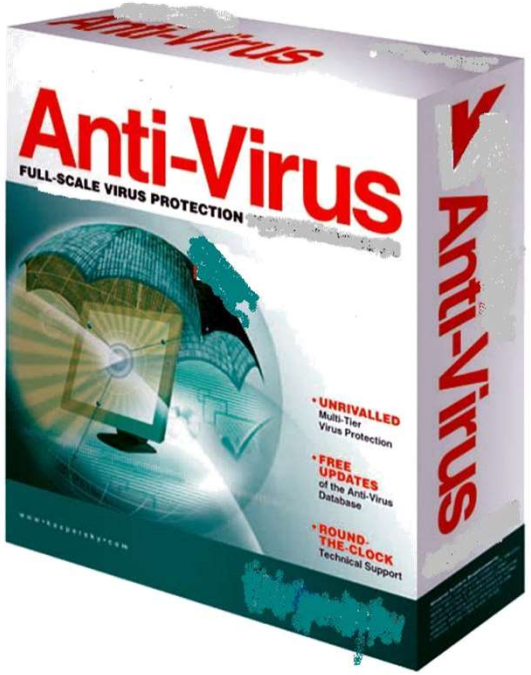
1. การปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัย
2. การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร

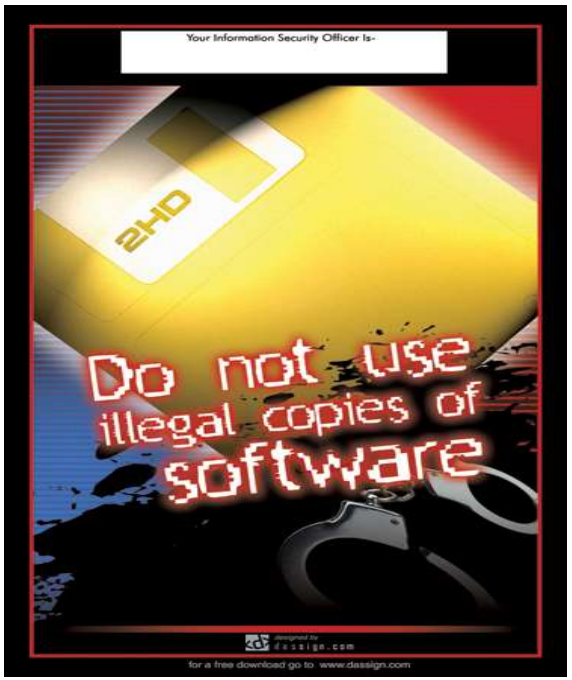
A.15.3 การตรวจประเมินระบบสารสนเทศ(2)

1. มาตรการการตรวจประเมินระบบสารสนเทศ
2. การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ

ตัวอย่าง: การป้องกันสิทธิและทรัพย์สินทางปัญญา (IPR) (A.15.1.2)

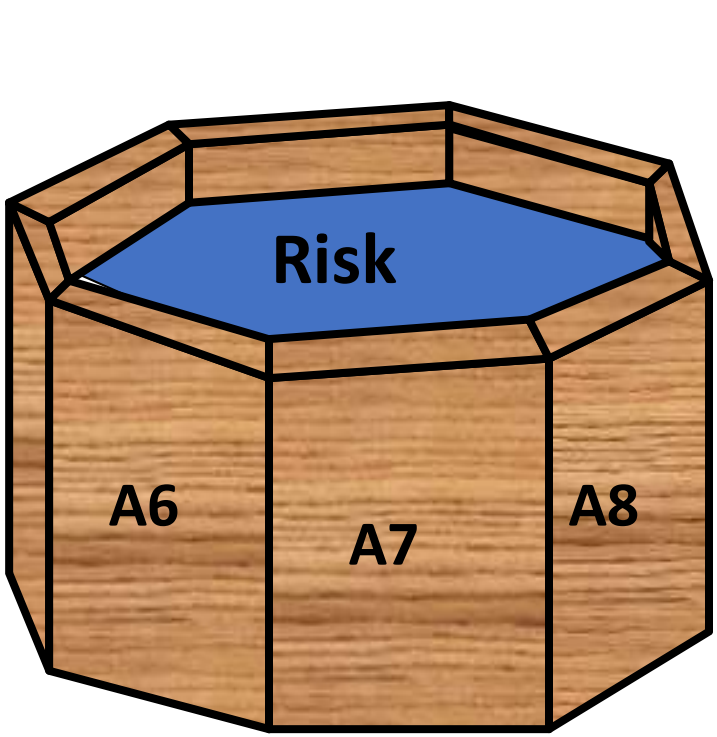


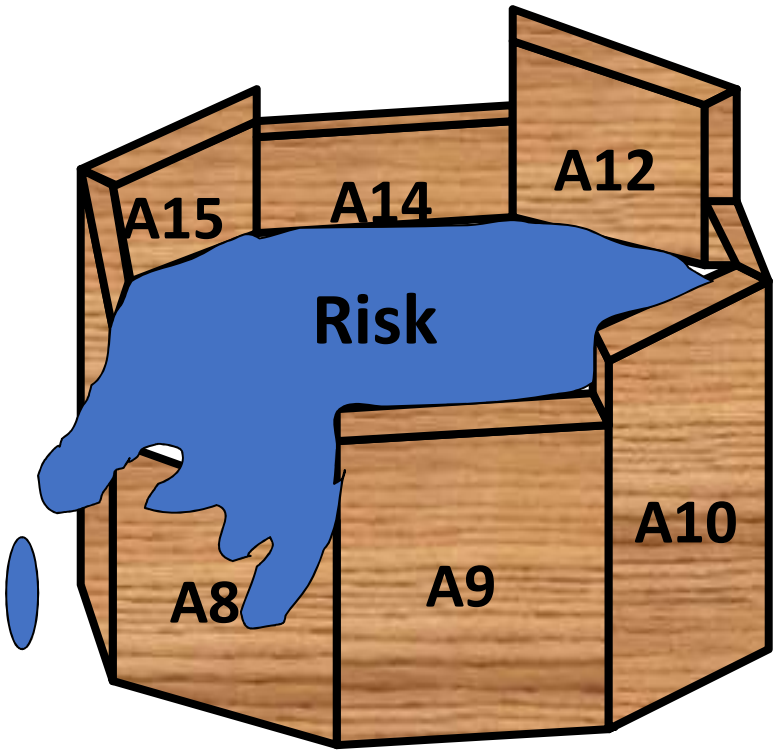


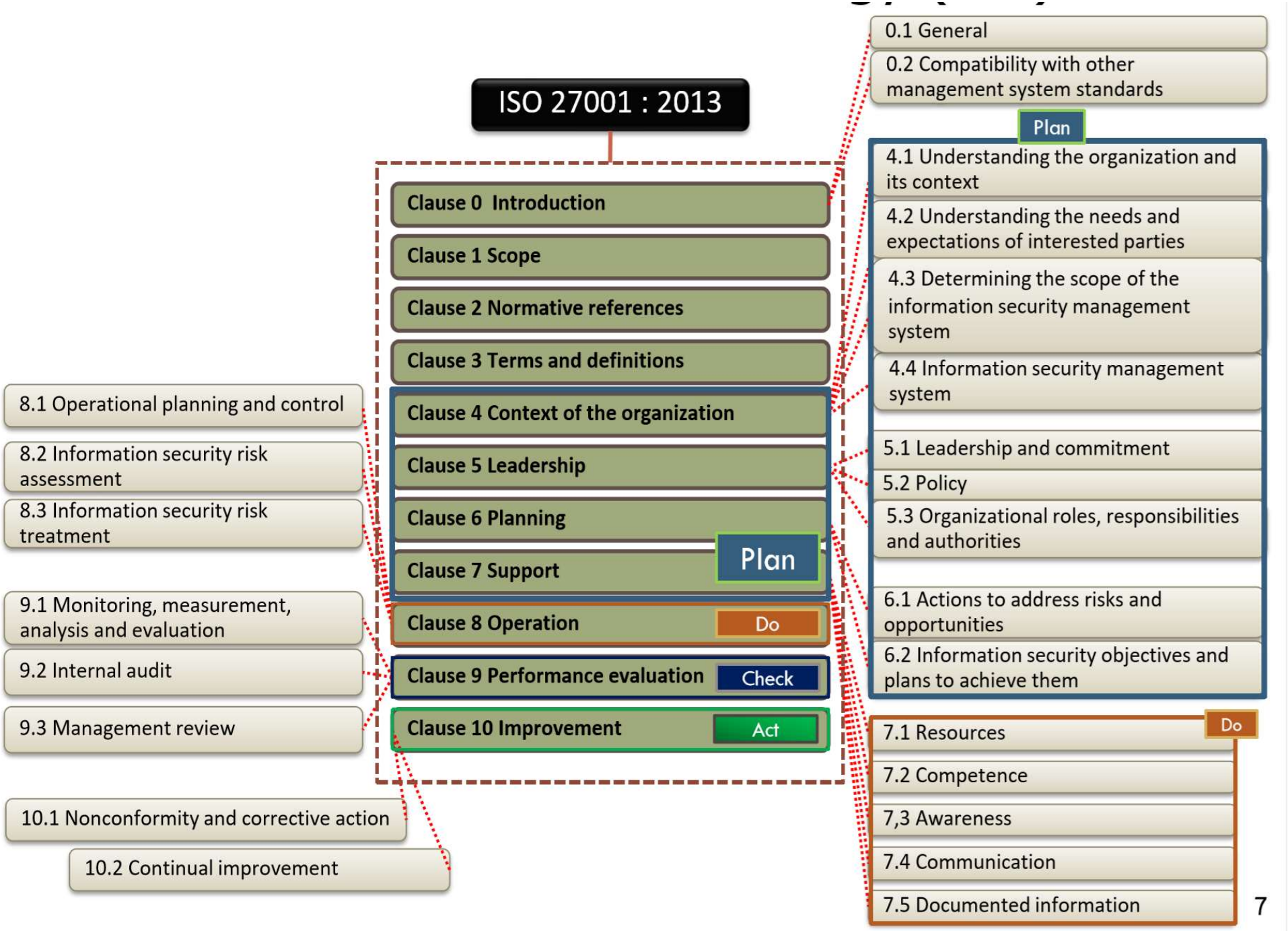


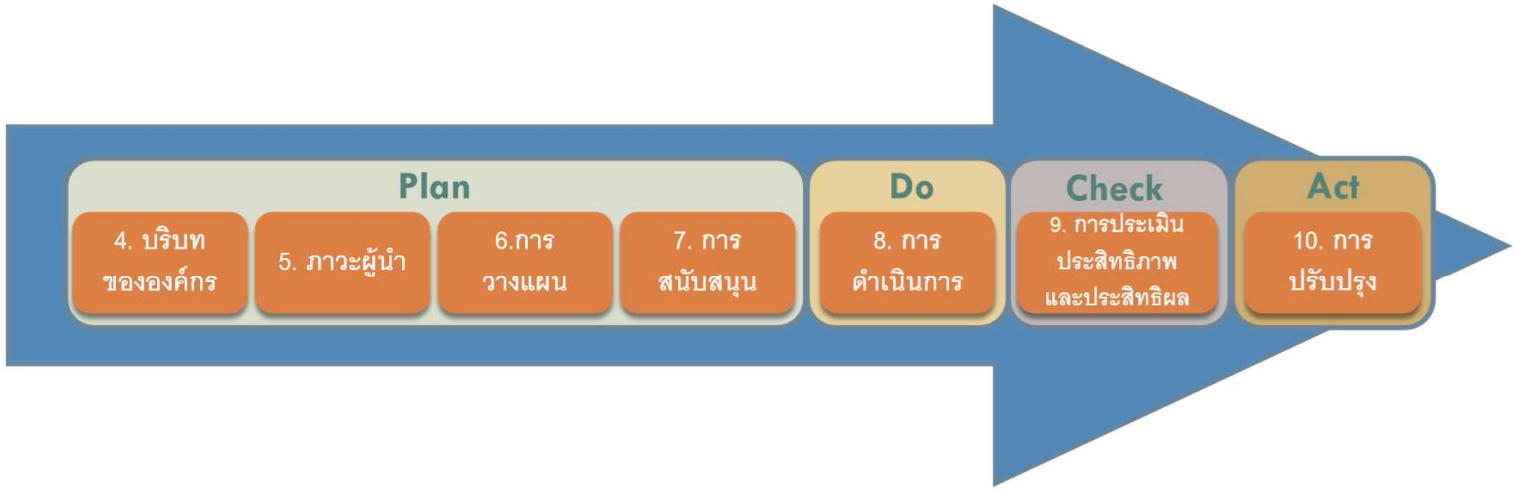
ตัวอย่าง: การขาดการตรวจประเมินระบบสารสนเทศ(A.15.3)

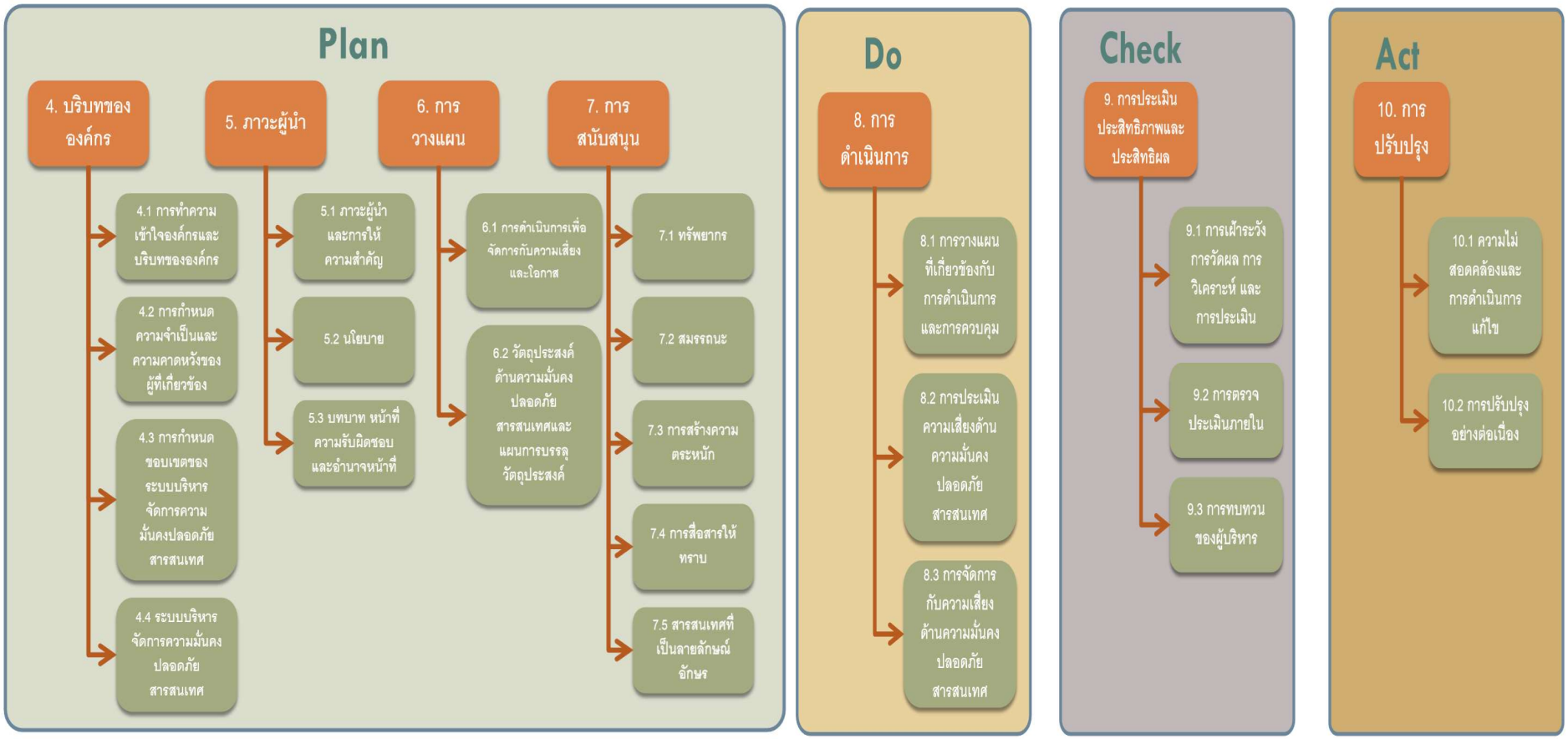
มาตรการควบคุมที่เหมาะสม

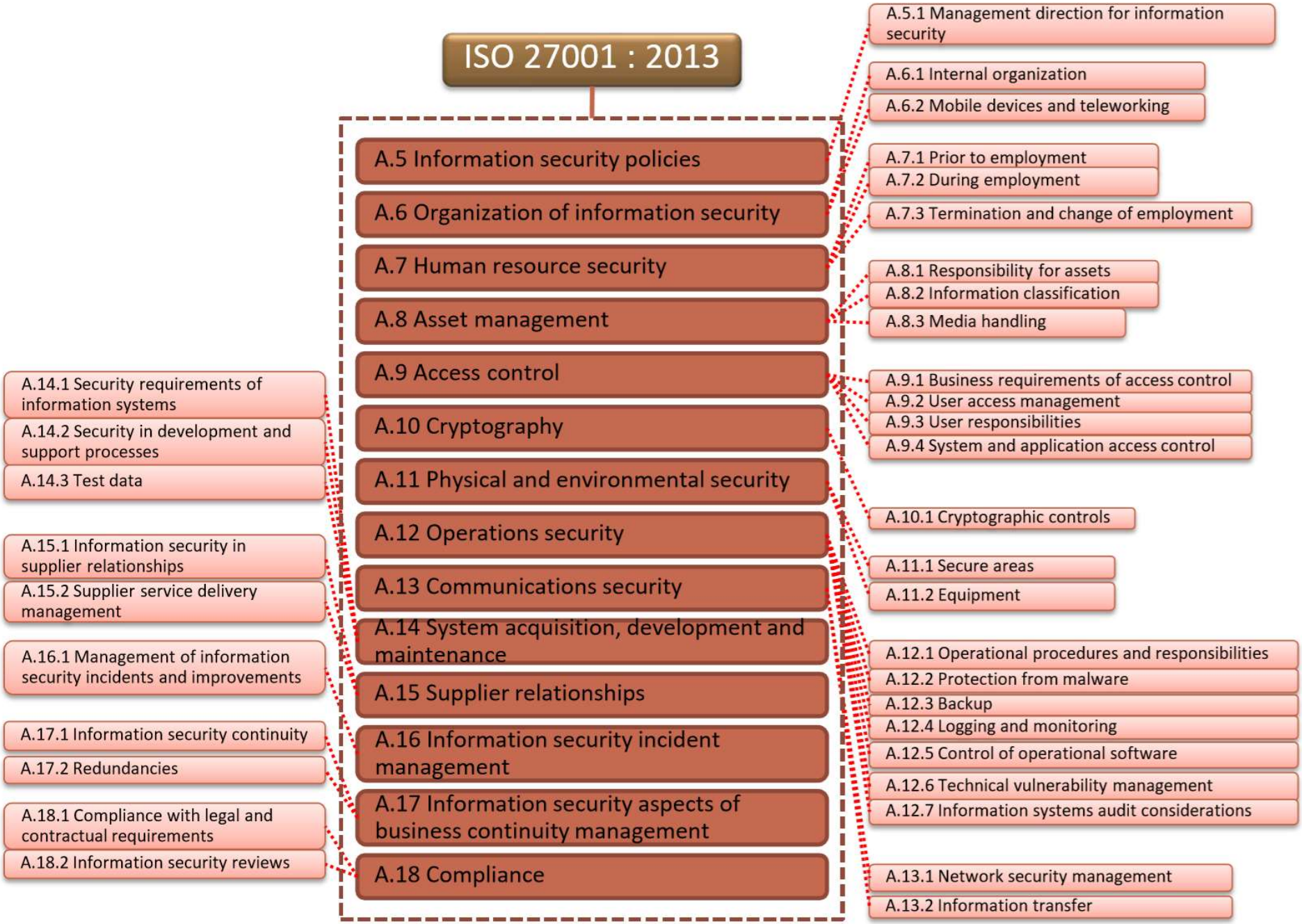




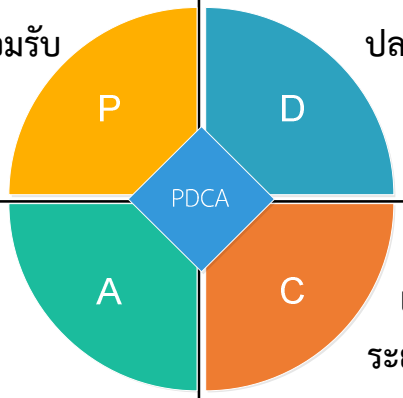

ISO 27001 : 2013
Clause 0 Introduction
Clause 1 Scope
Clause 2 Normative references
Clause 3 Terms and definitions
Clause 4 Context of the organization
Clause 5 Leadership
Clause 6 Planning
Clause 7 Support
Plan
Clause 8 Operation
Do
Clause 9 Performance evaluation
Check
Clause 10 Improvement
Act
0.1 General
0.2 Compatibility with other management system standards
Plan
4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system
4.4 Information security management system
5.1 Leadership and commitment
5.2 Policy
5.3 Organizational roles, responsibilities and authorities
6.1 Actions to address risks and opportunities
6.2 Information security objectives and plans to achieve them
Do
7.1 Resources
7.2 Competence
7,3 Awareness
7.4 Communication
7.5 Documented information
8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review
10.1 Nonconformity and corrective action
10.2 Continual improvement


Plan
4. บริบทขององค์กร
5. ภาวะผู้นำ
6.การวางแผน
7. การสนับสนุน
Do
8. การดำเนินการ
Check
9. การประเมินประสิทธิภาพและประสิทธิผล
Act
10. การปรับปรุง


Plan
4. บริบทขององค์กร
4.1 การทำความเข้าใจองค์กรและบริบทขององค์กร
4.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง
4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
5. ภาวะผู้นำ
5.1 ภาวะผู้นำและการให้ความสำคัญ
5.2 นโยบาย
5.3 บทบาท หน้าที่ความรับผิดชอบและอำนาจหน้าที่
6. การวางแผน
6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส
6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์
7. การสนับสนุน
7.1 ทรัพยากร
7.2 สมรรถนะ
7.3 การสร้างความตระหนัก
7.4 การสื่อสารให้ทราบ
7.5 สารสนเทศที่เป็นลายลักษณ์อักษร
Do
8. การดำเนินการ
8.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม
8.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
8.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
Check
9. การประเมินประสิทธิภาพและประสิทธิผล
9.1 การเฝ้าระวังการวัดผล การวิเคราะห์ และการประเมิน
9.2 การตรวจประเมินภายใน
9.3 การทบทวนของผู้บริหาร
Act
10. การปรับปรุง
10.1 ความไม่สอดคล้องและการดำเนินการแก้ไข
10.2 การปรับปรุงอย่างต่อเนื่อง


ISO 27001 : 2013
A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance
A.5.1 Management direction for information security
A.6.1 Internal organization
A.6.2 Mobile devices and teleworking
A.7.1 Prior to employment
A.7.2 During employment
A.7.3 Termination and change of employment
A.8.1 Responsibility for assets
A.8.2 Information classification
A.8.3 Media handling
A.9.1 Business requirements of access control
A.9.2 User access management
A.9.3 User responsibilities
A.9.4 System and application access control
A.10.1 Cryptographic controls
A.11.1 Secure areas
A.11.2 Equipment
A.12.1 Operational procedures and responsibilities
A.12.2 Protection from malware
A.12.3 Backup
A.12.4 Logging and monitoring
A.12.5 Control of operational software
A.12.6 Technical vulnerability management
A.12.7 Information systems audit considerations
A.13.1 Network security management
A.13.2 Information transfer
A.14.1 Security requirements of information systems
A.14.2 Security in development and support processes
A.14.3 Test data
A.15.1 Information security in supplier relationships
A.15.2 Supplier service delivery management
A.16.1 Management of information security incidents and improvements
A.17.1 Information security continuity
A.17.2 Redundancies
A.18.1 Compliance with legal and contractual requirements
A.18.2 Information security reviews

PLAN	DO
1. กำหนดวัตถุประสงค์ 2. จัดตั้งคณะกรรมการสนับสนุนและทีมทำงานฝึกอบรม 3. กำหนดขอบเขตของการดำเนินงาน 4. กำหดวิธีการประเมินความเสี่ยง (CIA) 5. จัดประเภทและระดับความเสี่ยงที่สามารถยอมรับได้หรือไม่	6. ระบุการควบคุมการปฏิบัติงานของความเสี่ยง (Accept, Transfer, Reduce, Avoid) กำหนดวิธีควบคุม 7. จัดทำนโยบายและขั้นตอนในการปฏิบัติในการควบคุมคม 8. ประชาสัมพันธ์เผยแพร่ข้อมูลข่าวสาร จัดอบรมความปลอดภัย
11. ติดตามผลการดำเนินงาน เพื่อให้เป็นไปตามมาตรฐาน	9. การทำงาน ทบทวน ระบุการดำเนินการแก้ไขหรือป้องกัน จัดทำเอกสาร นำเสนอเป็นระยะ ๆ ต่อคณะกรรมการสนับสนุนพิจารณา 10. คณะกรรมการดำเนินตรวจสอบความถูกต้องของกระบวนการดำเนินเอกสารต่าง ๆ จัดทีมตรวจสอบภายในเพื่อตรวจสอบความถูกต้อง เตรียมการขอการรองรับ ISO 27001 :
ACT	CHECK



Thank you for your attention!