

การพัฒนาซอฟต์แวร์
เทคโนโลยีปัญญาประดิษฐ์
ระบบเครือข่ายคอมพิวเตอร์
และความมั่นคงปลอดภัย



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

SDLC (Software Development Life Cycle)

คือกระบวนการหรือขั้นตอนในการพัฒนาซอฟต์แวร์ให้มีความสมดุล และประสิทธิภาพ

- การวางแผน (Planning): การกำหนดเป้าหมาย รายละเอียดของโครงการ และการศึกษาความเป็นไปได้ รวมถึงการกำหนดระยะเวลาและงบประมาณของโครงการ
- การวิเคราะห์ (Analysis): วิเคราะห์ความต้องการของระบบและผู้ใช้ และกำหนดข้อกำหนดในการพัฒนาซอฟต์แวร์
- การออกแบบ (Design): ออกแบบโครงสร้างระบบ โครงสร้างข้อมูล ประสบการณ์ผู้ใช้ (UX) ส่วนติดต่อผู้ใช้ (UI) และรายงาน (Report)
- การพัฒนา (Implementation): พัฒนาซอฟต์แวร์โดยการเขียนโค้ดตามข้อกำหนดและออกแบบที่กำหนดไว้
- การทดสอบ (Testing): การทดสอบซอฟต์แวร์เพื่อตรวจสอบความถูกต้องและประสิทธิภาพของระบบ
- การติดตั้งระบบ (Deployment): การติดตั้งระบบและการใช้งานจริง
- การดูแลรักษา (Maintenance): การดูแลรักษาระบบให้ใช้งานได้อย่างมีประสิทธิภาพ



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม



SDLC Model

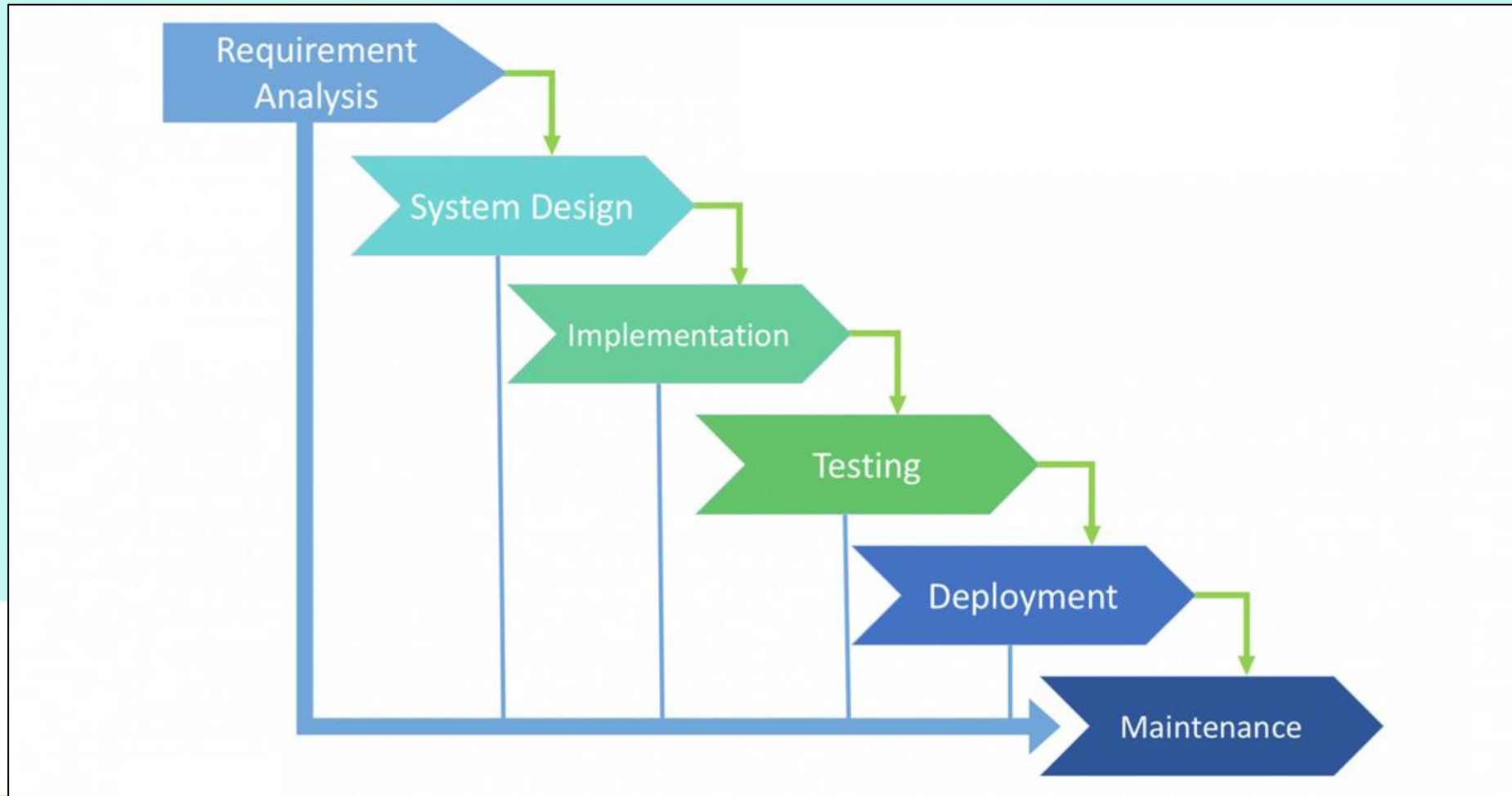
- Waterfall Model
- Agile Model
- Iterative Model
- Spiral Model
- V-Model (Validation and Verification Model)



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Waterfall Model

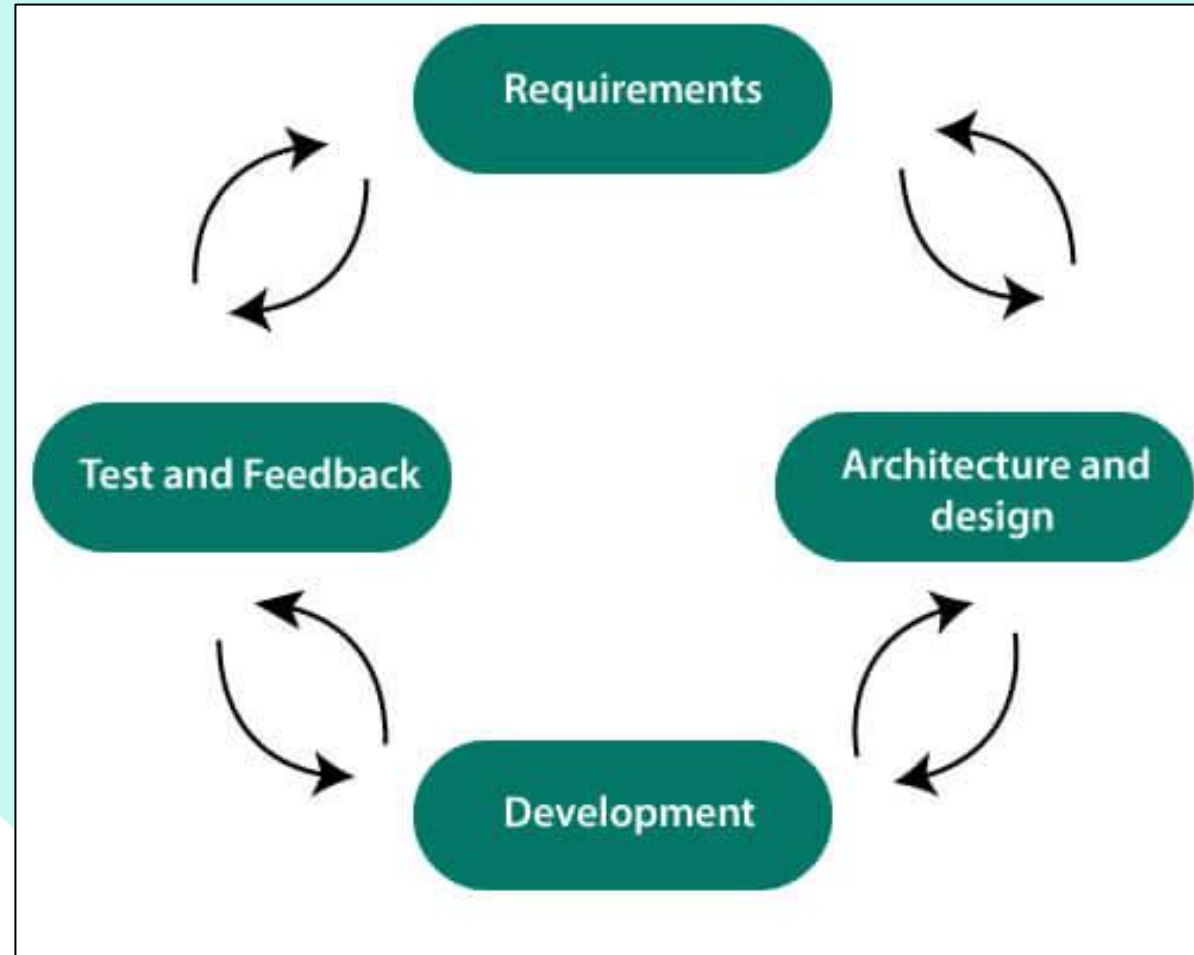
การพัฒนาซอฟต์แวร์ตามลำดับและต่อเนื่อง แต่ละขั้นตอนจะต้องเสร็จสิ้นก่อนที่จะไปยังขั้นตอนถัดไป



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Agile Model

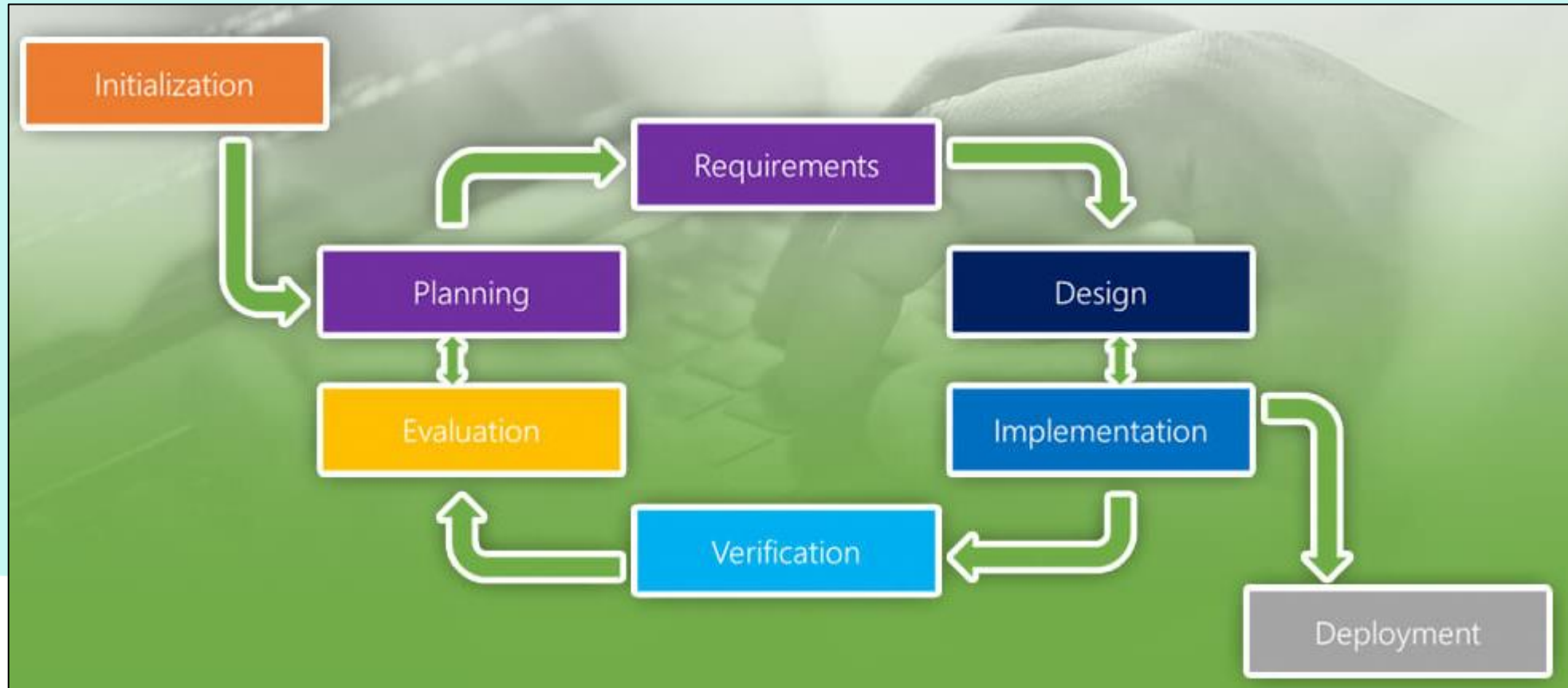
เน้นการทำงานเป็นทีมและการมีส่วนร่วมของลูกค้า มีความยืดหยุ่น โดยแบ่งออกซอฟต์แวร์ออกเป็นส่วนย่อย ๆ พัฒนาและส่งมอบส่วนย่อย ๆ นั้นให้กับลูกค้า และปรับปรุงตามข้อมูลตอบรับของลูกค้า



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Iterative Model

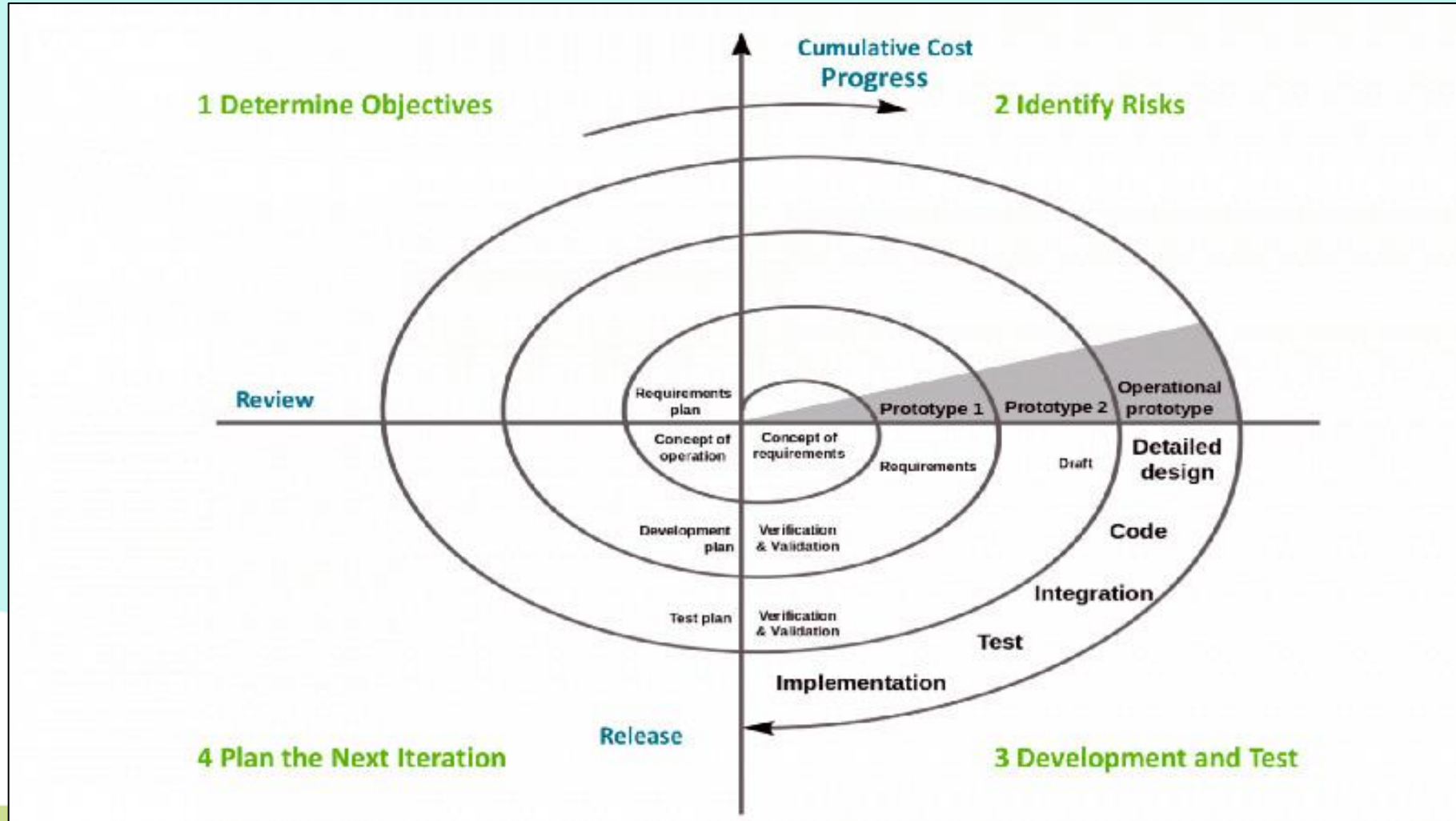
การพัฒนาซอฟต์แวร์ด้วยข้อกำหนดย่อย จากนั้นจึงปรับปรุงเวอร์ชันซ้ำไปเรื่อย ๆ จนกว่าซอฟต์แวร์จะสมบูรณ์



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Spiral Model

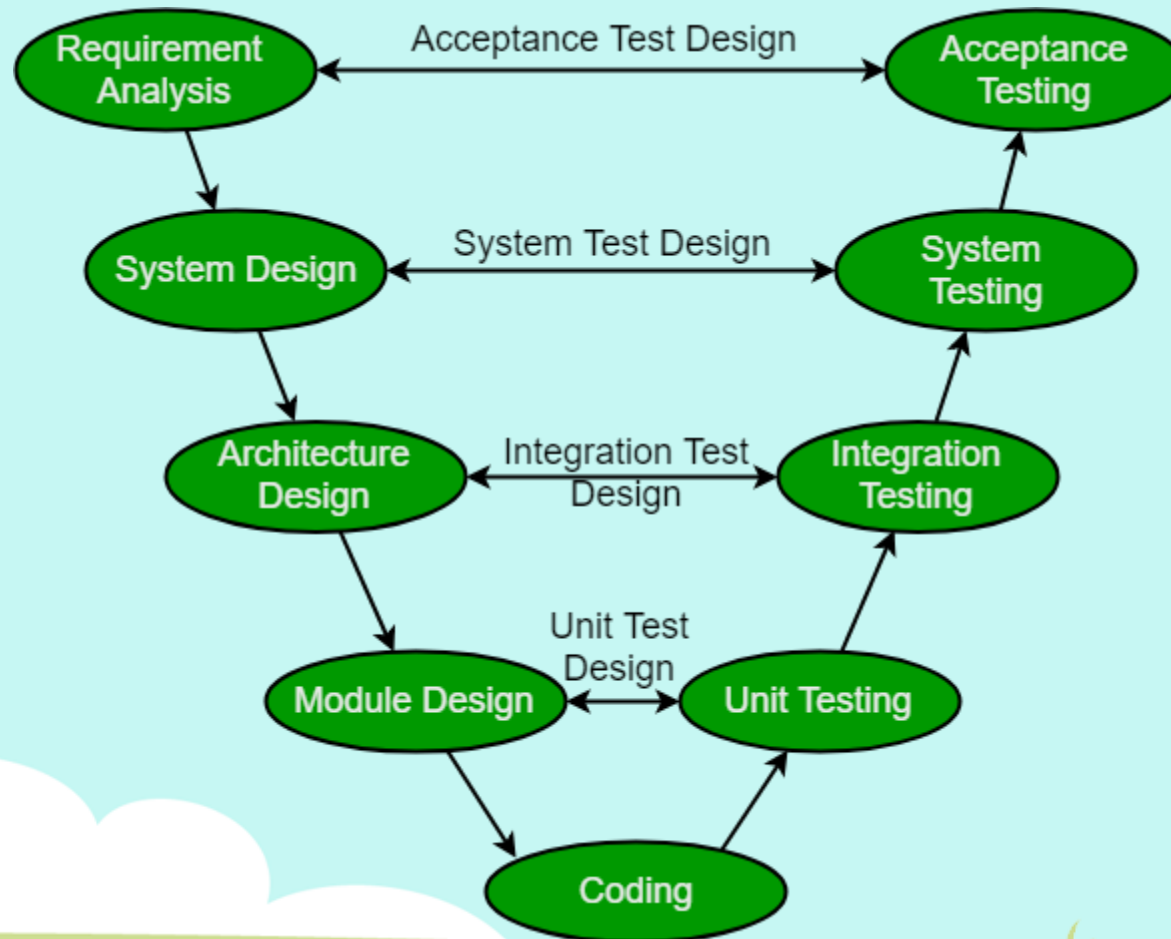
รวมลักษณะทั้งของ Waterfall และ iterative โดยมีการวางแผน การวิเคราะห์ความเสี่ยง การพัฒนา และการทดสอบ ในแต่ละรอบ ใช้กับการพัฒนาโครงการใหญ่ ๆ



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

V-Model

เป็นการขยายจากรูปแบบ Waterfall โดยจับคู่การพัฒนากับการทดสอบในแต่ละขั้นตอน



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

[1] การพัฒนาโปรแกรมเชิงโครงสร้าง (Structured Programming)

คือการพัฒนาซอฟต์แวร์โดยใช้โครงสร้างควบคุม การออกแบบแบบโมดูล จะทำงานจากจากบนลงล่าง

เครื่องมือในการพัฒนา :

- วิเคราะห์ระบบ
 - Context Diagram
 - DFD (Data Flow Diagram)
- ออกแบบระบบ
 - System Flowchart
 - ERD (Entity Relationship Diagram)
 - Data Dictionary
 - UX/UI Design



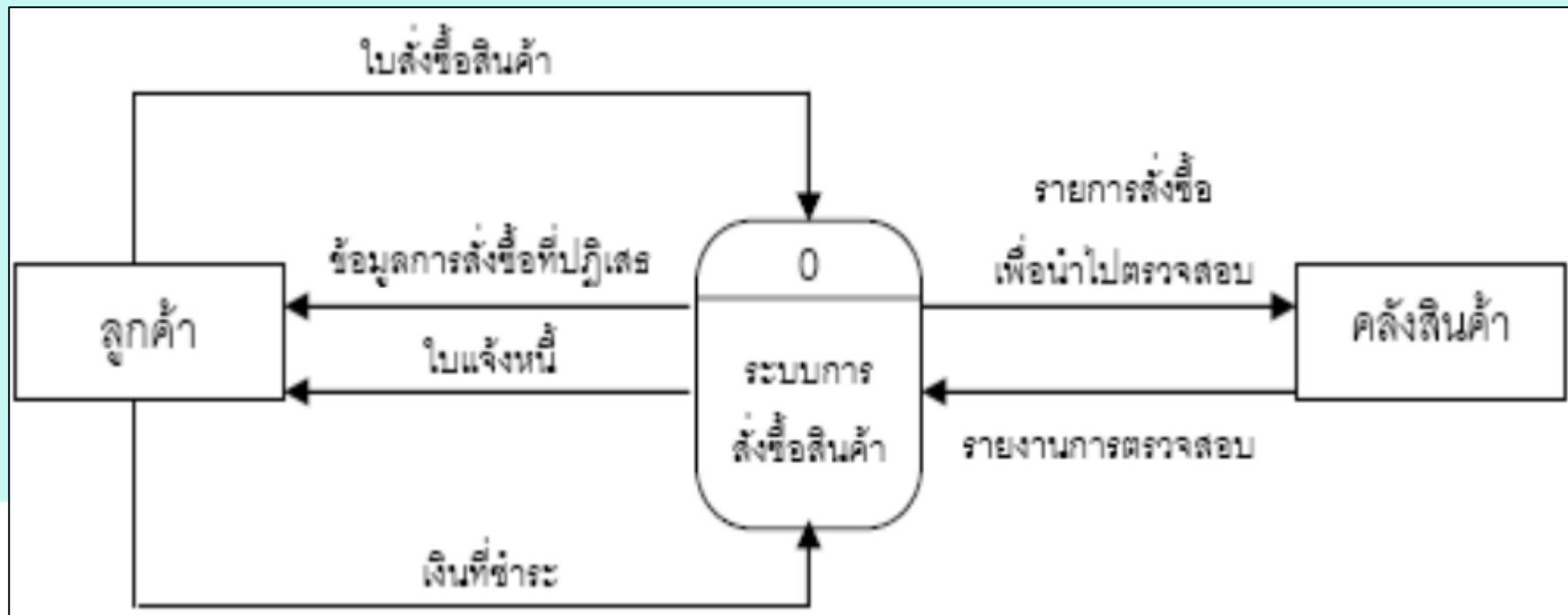
ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

แผนภาพกระแสข้อมูล (Data Flow Diagram: DFD)

เป็นแบบจำลองขั้นตอนการทำงานของระบบ เพื่ออธิบายขั้นตอนการทำงานของระบบ

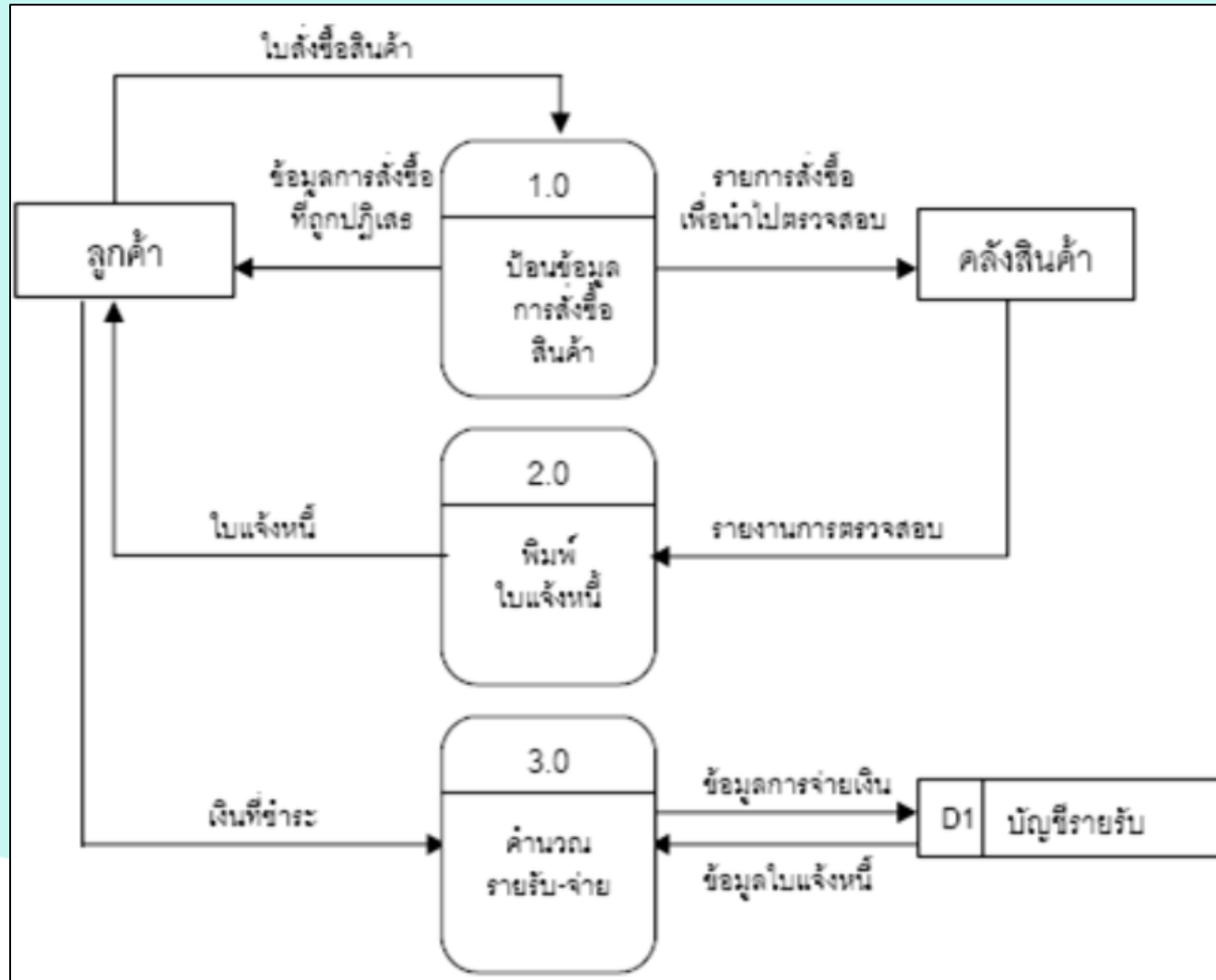
แผนภาพบริบท (Context Diagram / Level-0 Diagram)

Context Diagram คือแผนภาพกระแสข้อมูลระดับบนสุด



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

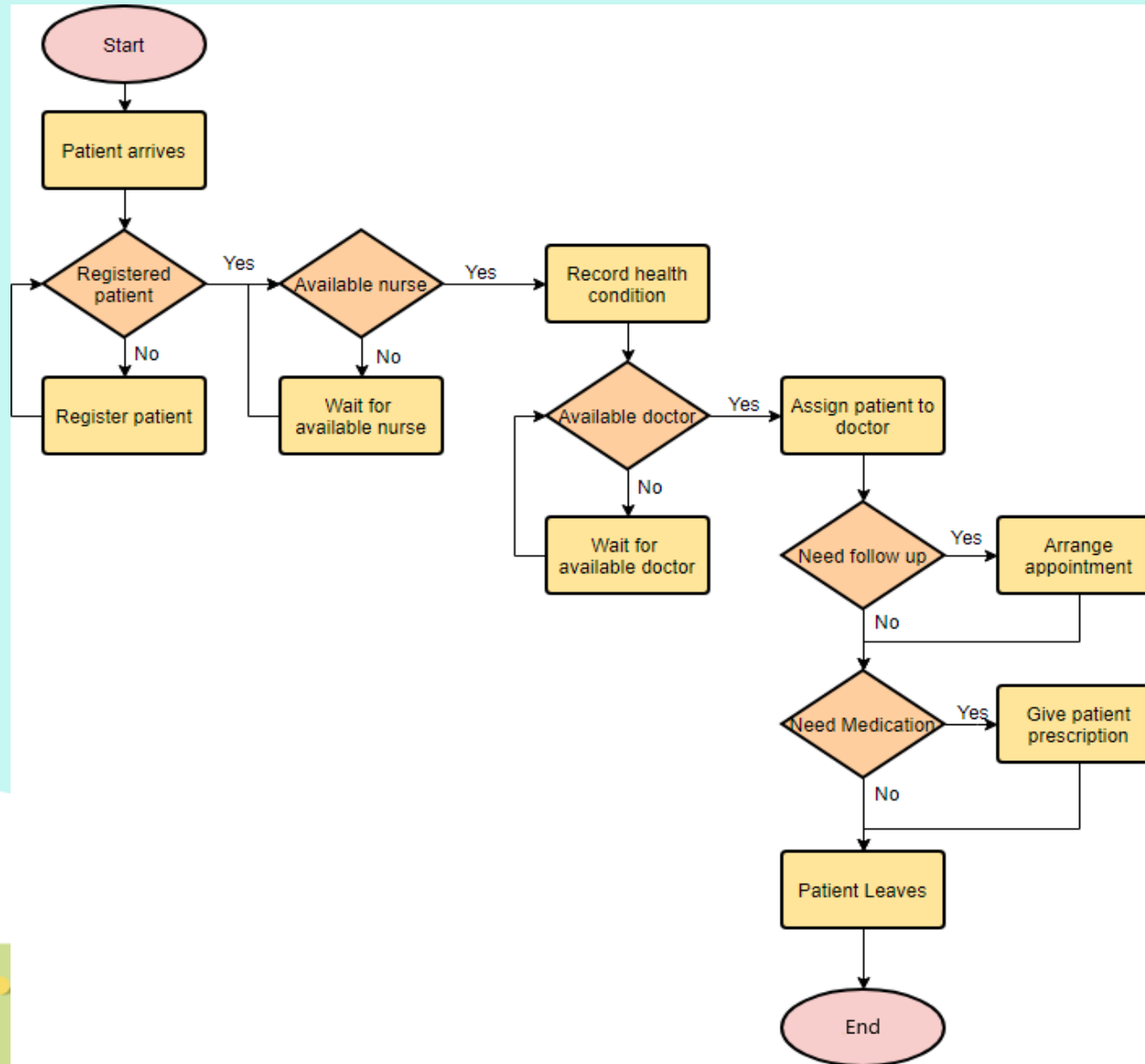
DFD (Data Flow Diagram Level-1)



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

ผังงานระบบ (System Flowchart)

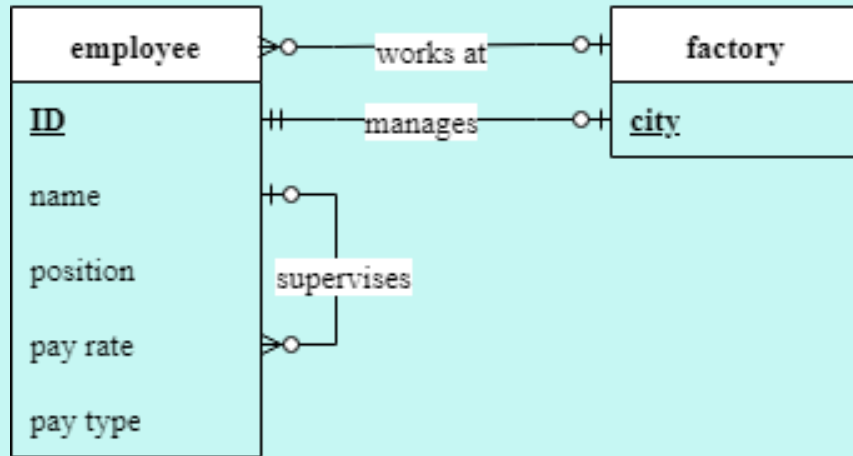
คือ ผังงานที่แสดงขั้นตอนการทำงานในระบบอย่างกว้าง ๆ แต่ไม่เจาะลงในระบบงานย่อย



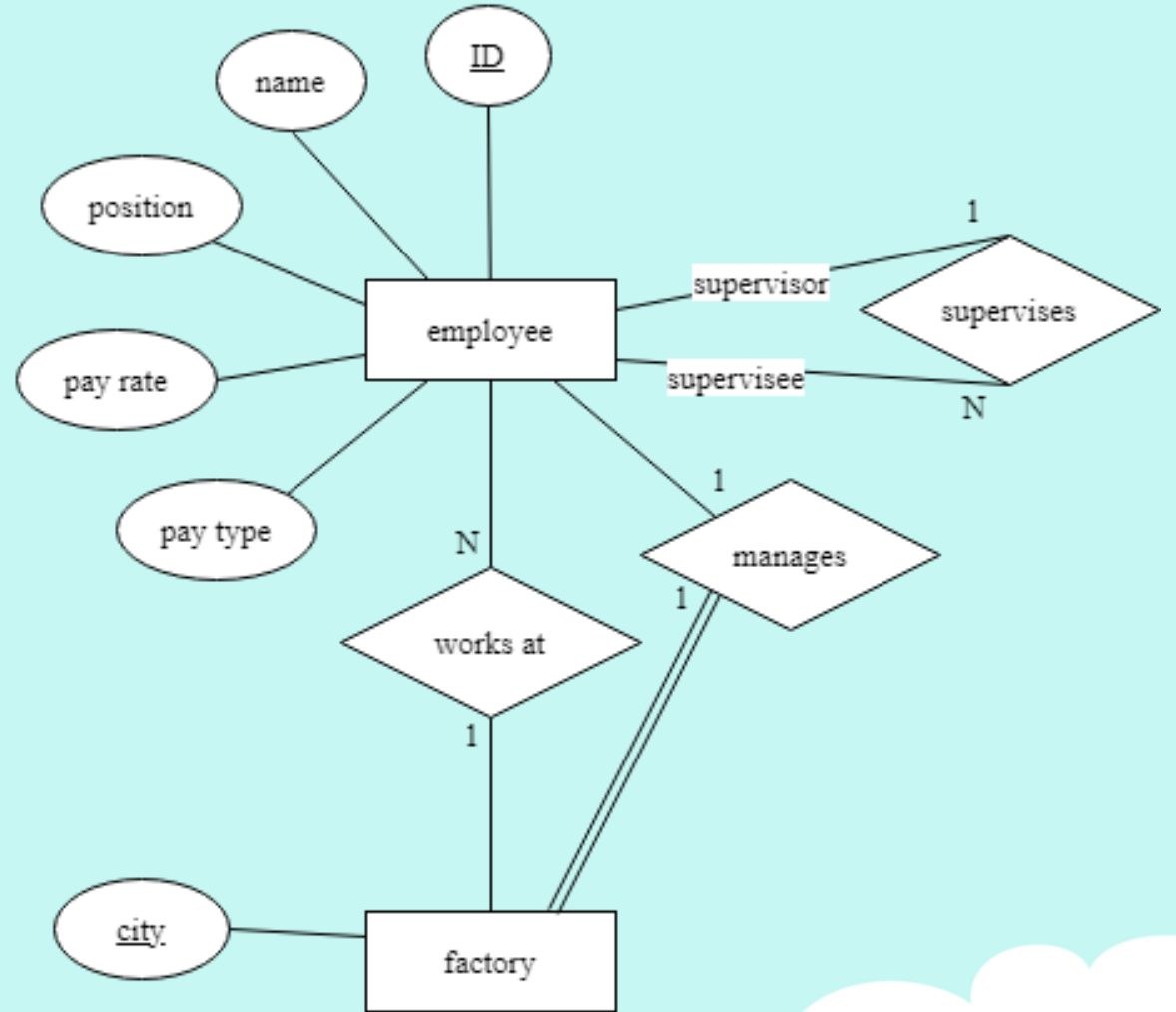
Entity Relationship Diagram (ERD)

คือ แบบจำลองที่ใช้อธิบายโครงสร้างของฐานข้อมูล

Crow's Foot Model



Chen Model



UX/UI Design

- UX (User Experience) หมายถึงประสบการณ์ทั้งหมดที่ผู้ใช้ได้รับเมื่อใช้งานผลิตภัณฑ์หรือบริการใด ๆ ซึ่งรวมถึงความพึงพอใจ ความสะดวกสบาย การเข้าใจ และความสามารถในการใช้งาน รวมถึงความพึงพอใจ
- UI (User Interface) คือการออกแบบส่วนต่างๆ ของหน้าจอให้สวยงามและมีการจัดเรียงองค์ประกอบที่สามารถให้ผู้ใช้ใช้งานได้ง่ายและมีความสวยงาม



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

[2] การพัฒนาโปรแกรมเชิงวัตถุ (Object Oriented Programming)

คือ การพัฒนาซอฟต์แวร์โดยจำลองข้อมูลในการเขียนโปรแกรมที่เน้นมองสิ่งต่างๆ ในระบบให้เป็น Object และมีต้นแบบเป็น Class

เครื่องมือในการพัฒนา : UML (Unified Modeling Language) เป็นภาษาที่ถูกพัฒนาขึ้นเพื่อใช้ในการออกแบบการเขียนโปรแกรมเชิงวัตถุ (OOA และ OOD)

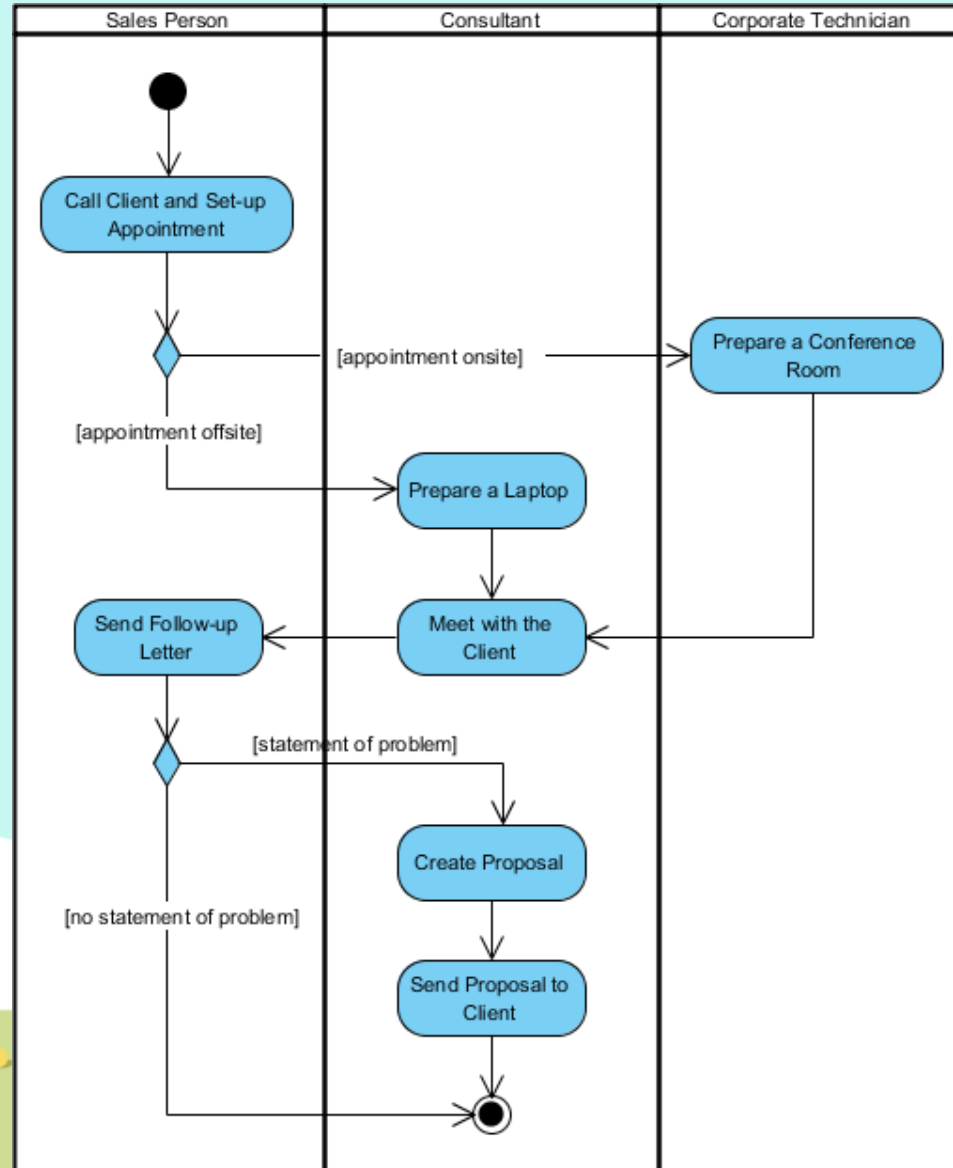
- Activity diagram
- Use case diagram
- Class diagram
- Sequence diagram



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Activity diagram

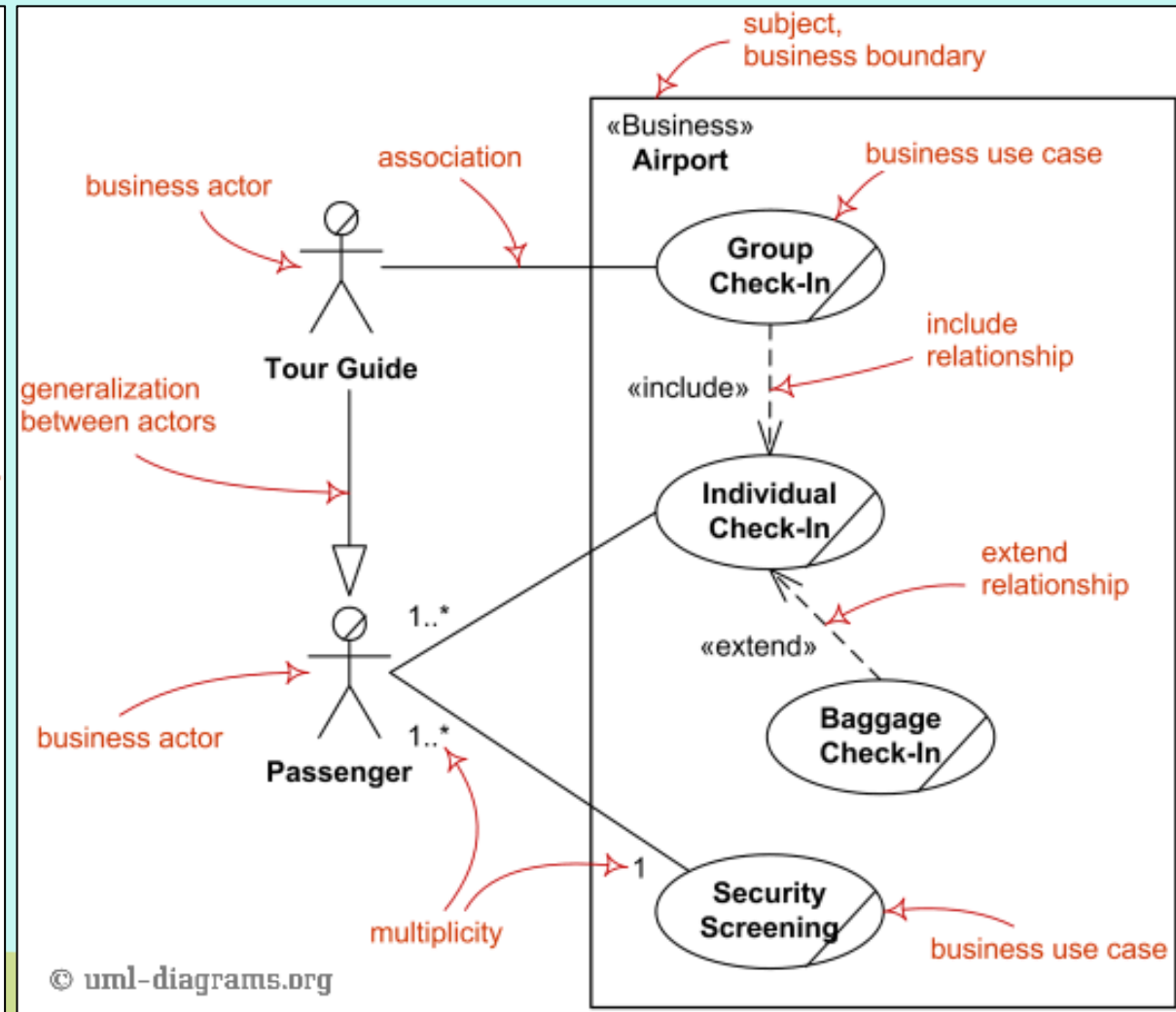
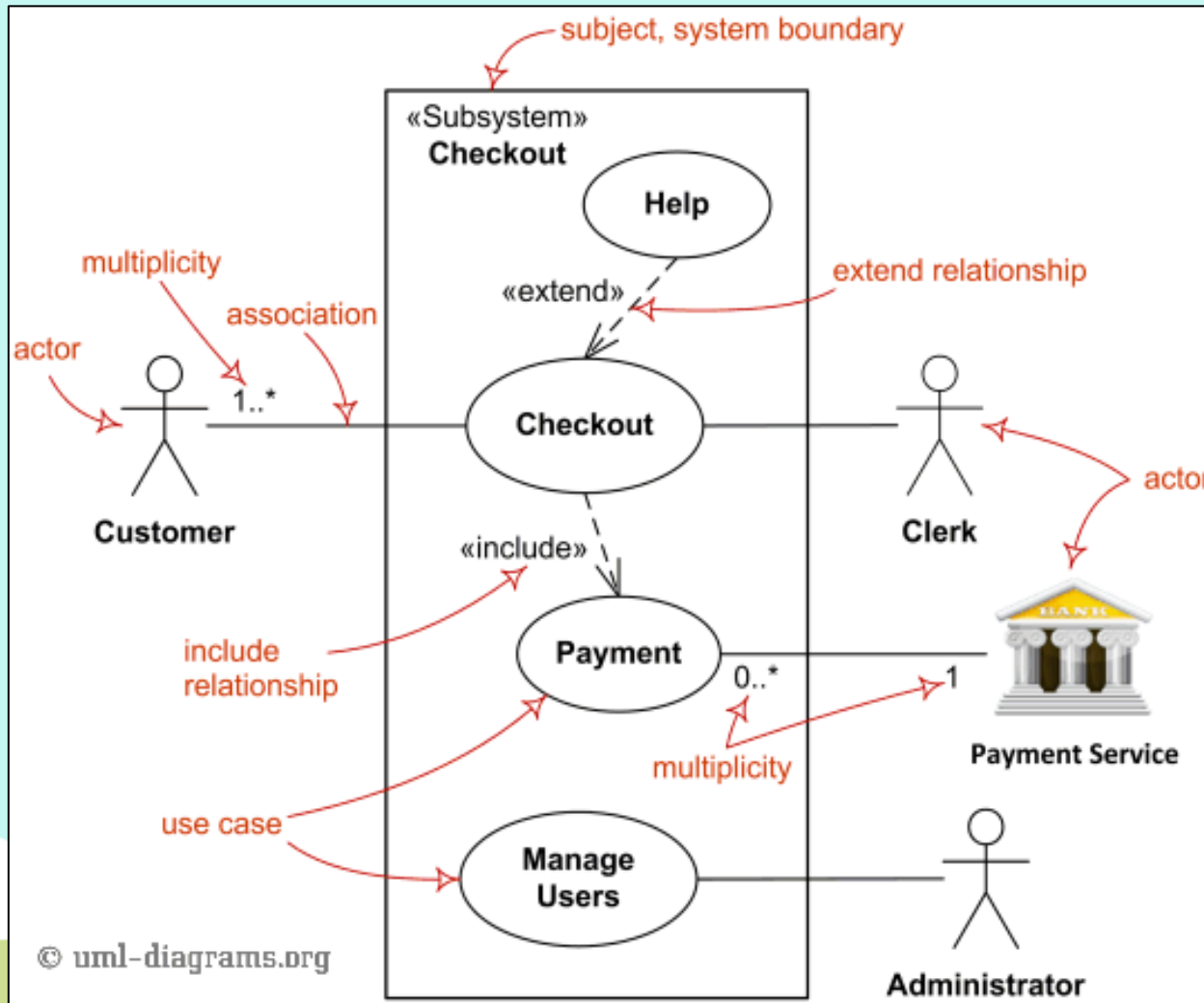
ใช้ในการแสดงและแบบจำลองกระบวนการหรือลำดับของกิจกรรมที่ต้องทำเพื่อให้บ่งชี้ถึงเป้าหมายหรือกระบวนการทางธุรกิจต่าง ๆ ในระบบ หรือแอปพลิเคชัน



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Use case diagram

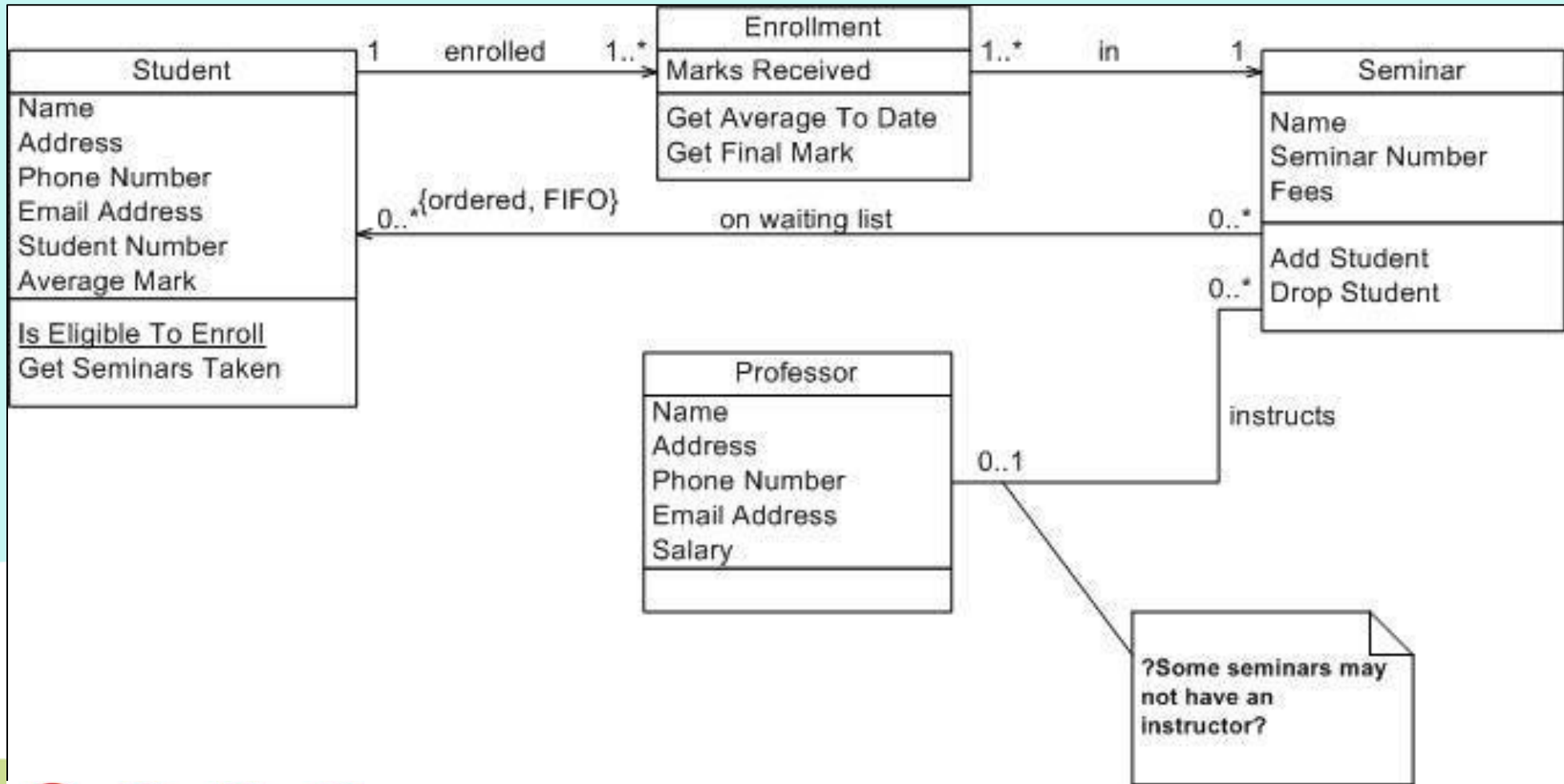
ใช้ในการอธิบายฟังก์ชันหลักของระบบจากมุมมองของผู้ใช้ แสดงการโต้ตอบระหว่างผู้ใช้และระบบ และรายละเอียดของแต่ละ use case หรือฟังก์ชัน



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Class diagram

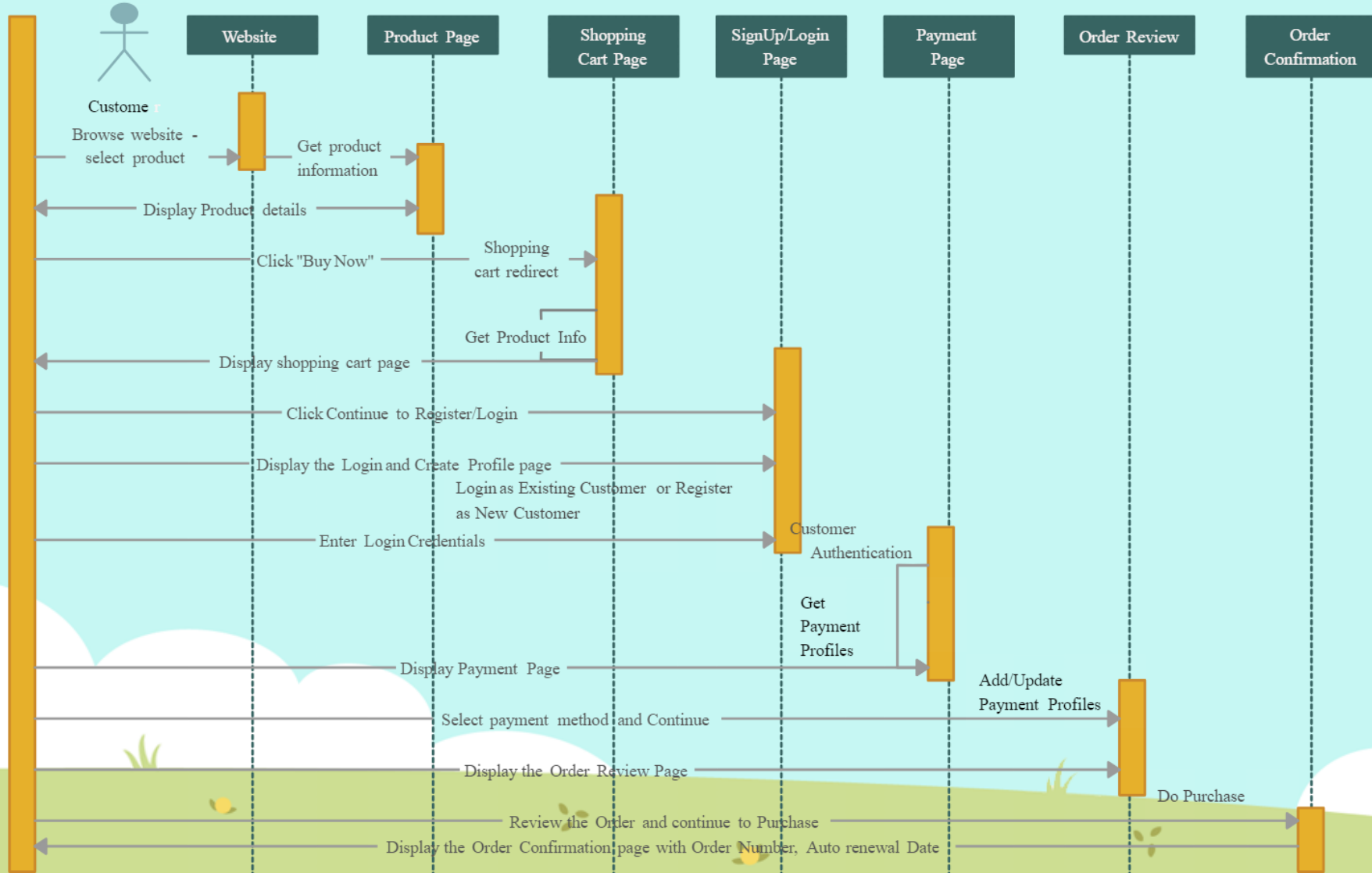
ใช้ในการแสดงโครงสร้างของคลาสและองค์ประกอบของระบบ รวมถึงความสัมพันธ์ระหว่างคลาส โดยแสดงให้เห็นแอตทริบิวต์และเมธอดของแต่ละคลาส



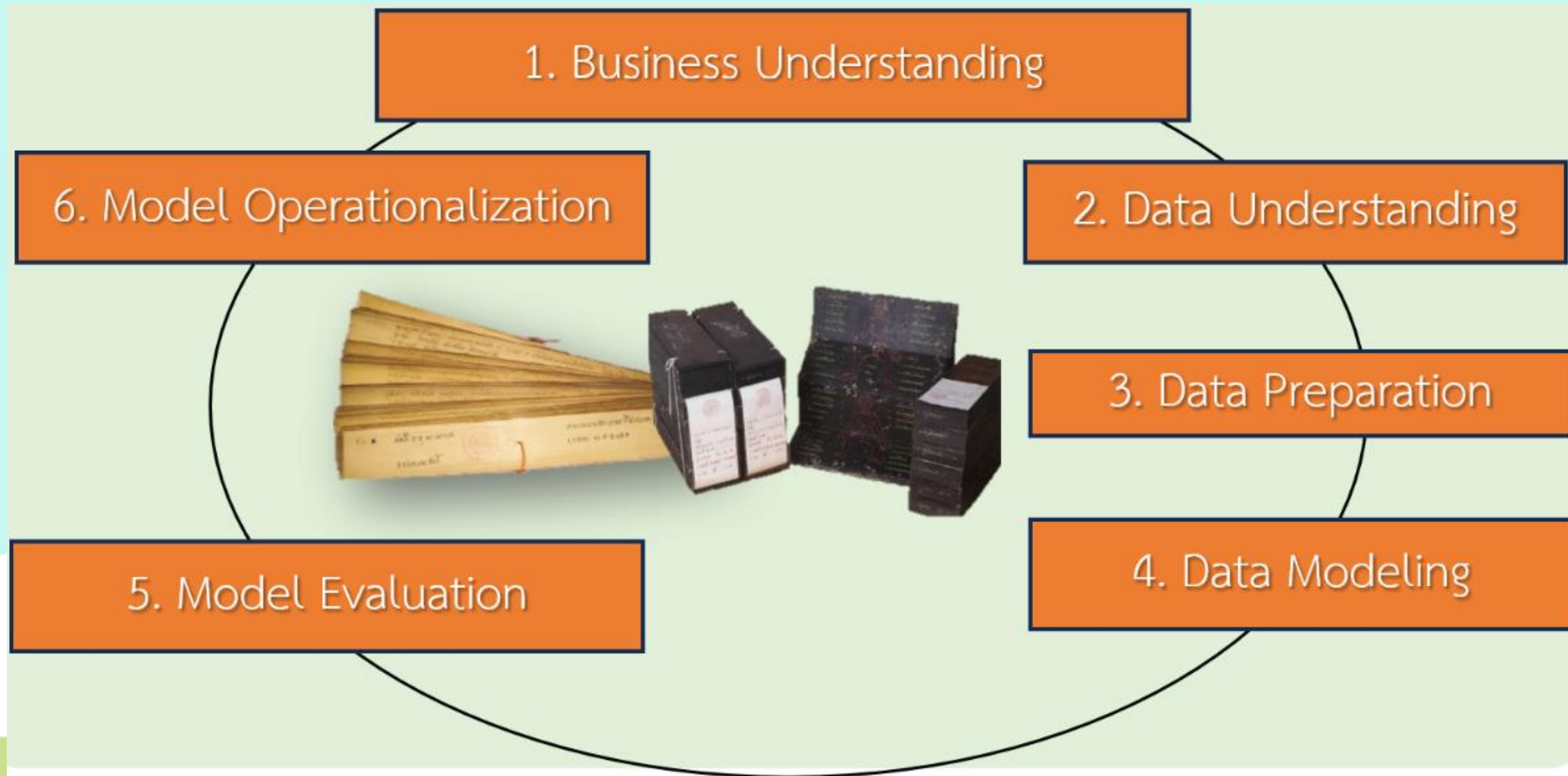
ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

Sequence diagram

ใช้ในการแสดงลำดับของเหตุการณ์ที่เกิดขึ้นในระบบ เราสามารถเห็นความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ และการโต้ตอบระหว่างอ็อบเจ็ค



[3] Artificial Intelligence (AI) Methodology



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

[4] การออกแบบและติดตั้งระบบเครือข่ายคอมพิวเตอร์

PDCA (Plan-Do-Check-Act) เป็นกระบวนการที่ใช้ในการจัดการและปรับปรุงกระบวนการหรือการดำเนินงานต่าง ๆ อย่างเป็นระบบต่อเนื่องเพื่อปรับปรุงคุณภาพและประสิทธิภาพของงานในองค์กร

- Plan (วางแผน) กำหนดเป้าหมายและวางแผนการดำเนินงาน และการกำหนดขอบเขตและระยะเวลา
- Do (ดำเนินการ)
 - การออกแบบระบบเครือข่าย
 - การวิเคราะห์ความต้องการระบบเครือข่าย
 - เครื่องเซิร์ฟเวอร์และแอปพลิเคชันที่ใช้งาน
 - รูปแบบการเชื่อมต่อเครือข่ายระหว่างสาขา
 - รูปแบบผังอาคารสำนักงานและจำนวนพนักงานในแต่ละแผนก
 - ปริมาณผู้ใช้งานเครื่องคอมพิวเตอร์และปริมาณแบนด์วิธ
 - การวิเคราะห์ความต้องการด้านอุปกรณ์เครือข่าย
 - คุณสมบัติอุปกรณ์เครือข่าย Core Switch
 - คุณสมบัติอุปกรณ์เครือข่าย Distribution Switch
 - คุณสมบัติอุปกรณ์เครือข่าย Access Switch
 - คุณสมบัติอุปกรณ์ป้องกันเครือข่าย



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

การออกแบบและติดตั้งระบบเครือข่ายคอมพิวเตอร์ (ต่อ)

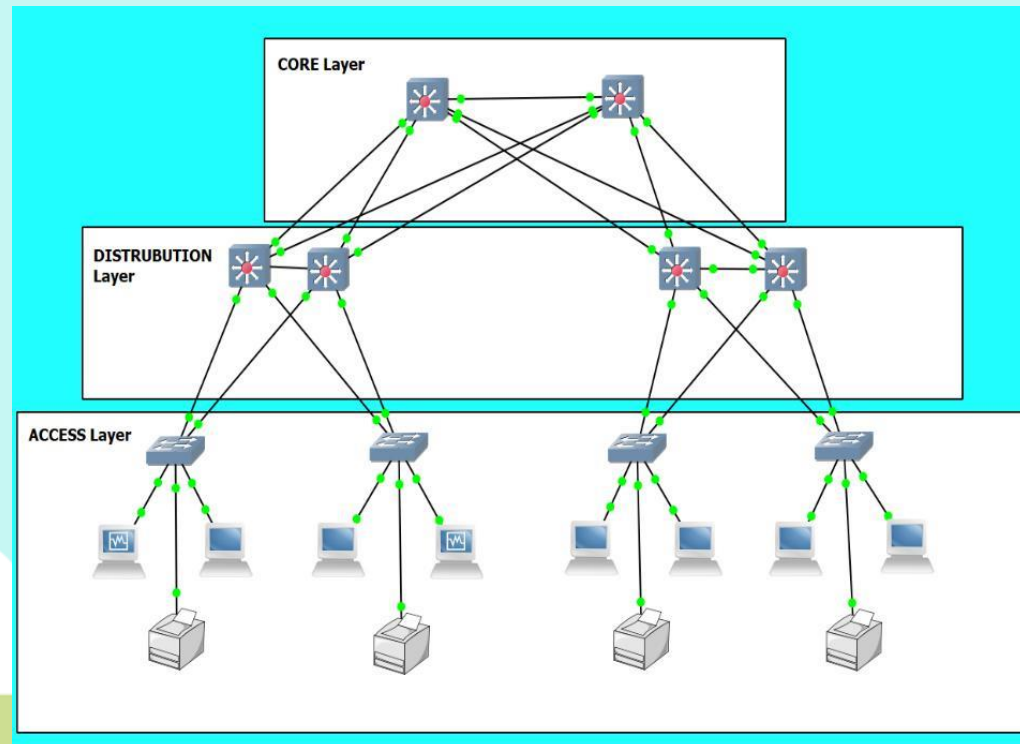
- Do (ดำเนินการ)
 - การออกแบบระบบเครือข่าย (ต่อ)
 - โครงสร้างการออกแบบระบบเครือข่าย
 - รูปแบบระบบเครือข่าย เช่น เป็นลำดับชั้น (Hierarchical Network) หรือ Token Ring
 - การกำหนดหมายเลข IP, VLAN
 - โครงสร้างการเดินสายสัญญาณระหว่างชั้น
 - ภาพรวมผังการออกแบบระบบเครือข่าย
 - รายละเอียดการติดตั้งและการเชื่อมต่อระบบเครือข่าย
 - การติดตั้งระบบเครือข่าย
 - ติดตั้งตู้อุปกรณ์และเครื่องเซิร์ฟเวอร์
 - การเดินสายสัญญาณภายในอาคาร
 - ระบบการสำรองไฟฟ้า
 - ระบบการจ่ายกระแสไฟภายในสำนักงาน
 - การติดตั้งระบบผ่านเข้า-ออกห้องเซิร์ฟเวอร์
 - การตั้งค่าคอนฟิกอุปกรณ์เครือข่าย
 - การติดตั้งระบบสำหรับมอนิเตอร์อุปกรณ์เครือข่าย
 - ระบบความปลอดภัยระบบเครือข่าย



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

การออกแบบและติดตั้งระบบเครือข่ายคอมพิวเตอร์ (ต่อ)

- Check (ตรวจสอบ)
 - การทดสอบระบบตามโครงสร้างระบบเครือข่ายที่ออกแบบ
 - การทดสอบระบบความปลอดภัยระบบเครือข่าย
- Act (ปรับปรุง) สรุปผลการดำเนินงาน และปรับปรุงแก้ไขข้อบกพร่อง



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

[5]



NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPONSE	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Strategy	Protective Technology			
What processes and assets need protection?	What safeguards are available?	What techniques can identify incidents?	What techniques can contain impacts of incidents?	What techniques can restore capabilities?

พ.ร.บ. ไซเบอร์	การระบุความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	มาตรา 13 (4)
----------------	-----------------------------------	--	---	---	---	--------------



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกอบไปด้วย 5 หัวข้อ ดังนี้

1

การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ (Identify)

2

มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

3

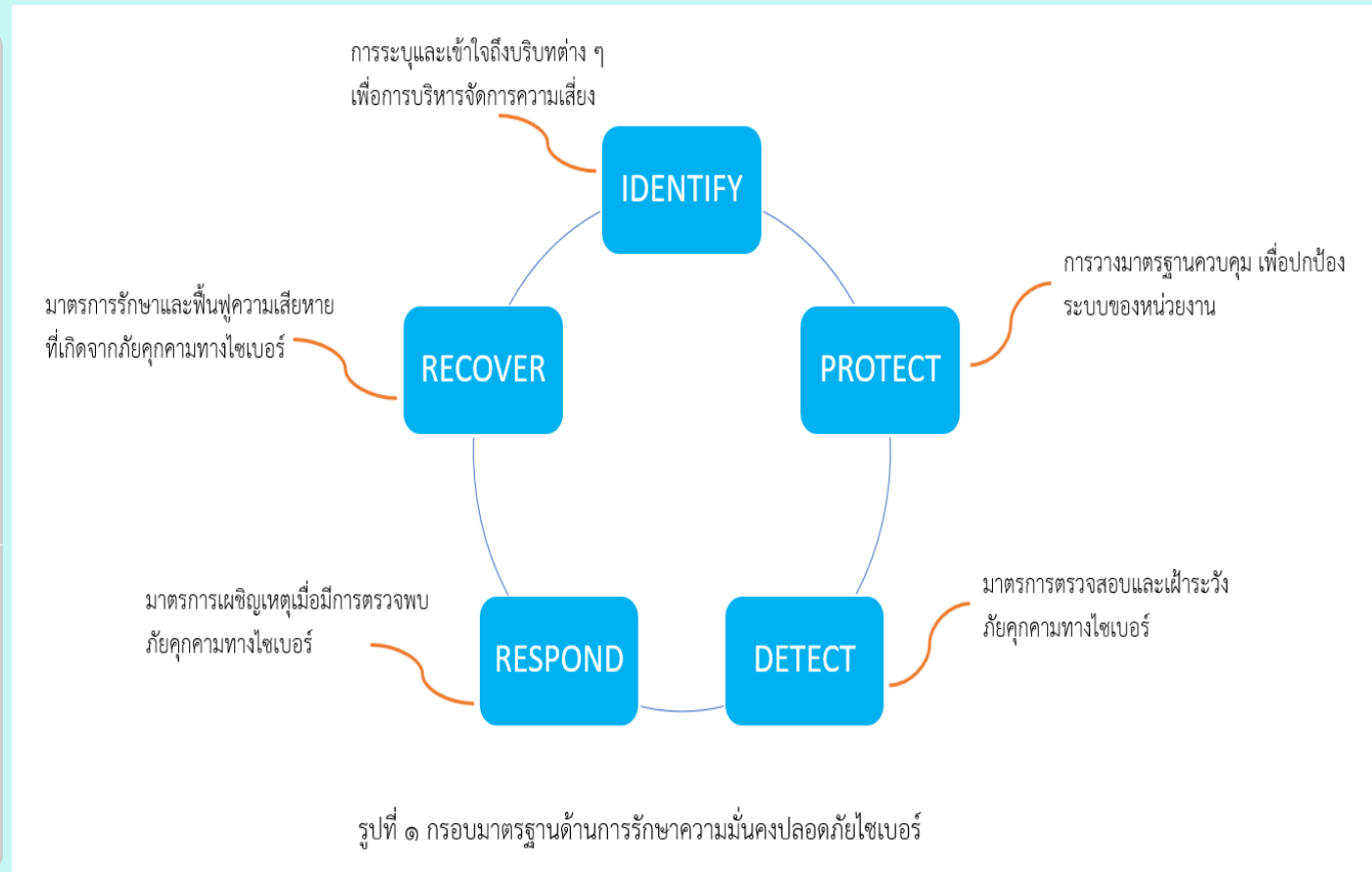
มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

4

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

5

มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)



ห้ามการถ่ายภาพหรือบันทึกเสียง ของการประชุม

