หลักสูตร

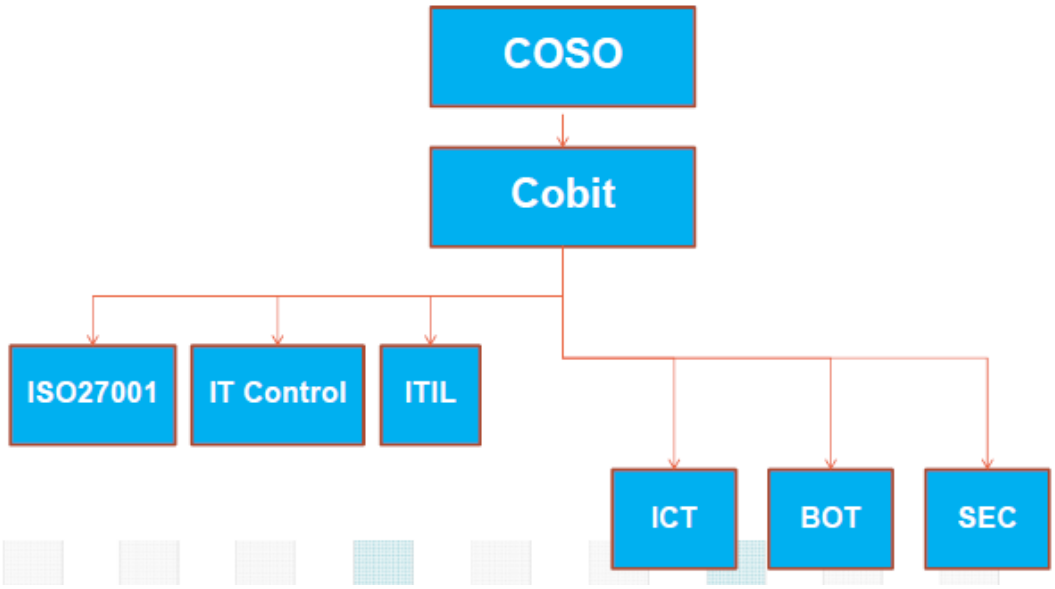
การพัฒนาองค์กรกับมาตรฐานเทคโนโลยี COSO, CobiT, SOX, ITIL, ISO27001:2013 และ ISO22301:2013

จัดโดย สถาบันวิทยาการ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ระหว่างวันที่ 5-9 มิถุนายน 2560

วิทยากร : อาจารย์ขจร สินอภิรมย์สราญ

ความเกี่ยวข้องกันระหว่างมาตรฐาน COSO, CobiT, ISO27001, ITIL, ICT, BOT, SEC



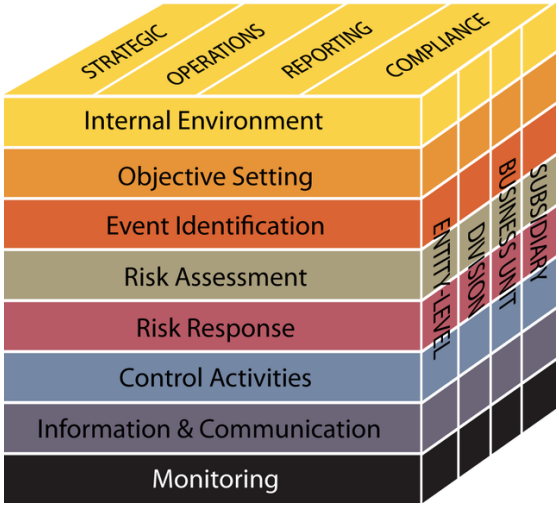
COSO (Committee of Sponsoring Organizations) ก่อตั้งเมื่อปี ค.ศ. 1992 ประกอบด้วยสถาบันวิชาชีพในสหรัฐอเมริกา 5 สถาบัน ได้แก่

1) สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (American Institute of Certified Public Accountants : AICPA)
2) สถาบันผู้ตรวจสอบภายในสากล (Institute of Internal Auditors : IIA)
3) สถาบันผู้บริหารการเงิน (Financial Executives Institute : FEI)
4) สมาคมนักบัญชีแห่งสหรัฐอเมริกา (American Accounting Association : AAA)
5) สถาบันนักบัญชีเพื่อการบริหาร (Institute of Management Accountants : IMA)

การควบคุมภายในตามแนวคิดของ COSO ได้ให้ความหมายและวัตถุประสงค์ของการควบคุมภายในที่สำคัญ คือ กระบวนการซึ่งร่วมกันทำให้บังเกิดผลโดยคณะกรรมการ ผู้บริหารและบุคคลอื่นๆ ขององค์กร ได้รับการออกแบบขึ้นมาเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ 3 ประการ ดังนี้

1) ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน (Effectiveness and Efficiency of Operations)
2) ความเชื่อถือได้ของรายงานทางการเงิน (Reliability of Financial Reporting)
3) การปฏิบัติตามกฎหมายและกฎระเบียบ (Compliance with Applicable Laws and Regulations)

การควบคุมภายใน (Internal Control) ของ COSO ประกอบด้วยองค์ประกอบ 8 ส่วน ดังภาพ



โดยแยกการบริหารความเสี่ยง ออกเป็น 3 มิติ ได้แก่

มิติที่ 1 ประกอบด้วย 8 องค์ประกอบ ได้แก่

1) การวิเคราะห์สภาพแวดล้อมภายในองค์กร (Internal Environment)
2) การกำหนดวัตถุประสงค์ (Objective Setting)
3) การระบุเหตุการณ์ (Event Identification)
4) การค้นหาความเสี่ยง (Risk Assessment)
5) การตอบสนองต่อความเสี่ยง (Risk Response)
6) กิจกรรมการควบคุม (Control Activities)
7) การให้ข้อมูลข่าวสารและการสื่อสาร (Information and Communication)
8) การกำกับติดตาม (Monitoring)

มิติที่ 2 นำไปใช้กับกิจกรรมในทุกระดับขององค์กร ได้แก่

1) ระดับองค์กร (Subsidiary)
2) ระดับหน่วยธุรกิจ (Business Unit)
3) ระดับฝ่าย (Division)
4) ระดับกิจกรรม (Entity Level)

มิติที่ 3 สนับสนุนวัตถุประสงค์ขององค์กร ได้แก่

1) ด้านกลยุทธ์ (Strategic)
2) ด้านการดำเนินงาน (Operations)
3) ด้านการรายงาน (Reporting)
4) ด้านการปฏิบัติตามกฎ/ระเบียบ (Compliance)

ขั้นตอนการประเมินความเสี่ยง

1. การระบุปัจจัยเสี่ยง (Risk Identification) ผู้ประเมินต้องทำความเข้าใจเกี่ยวกับภารกิจในองค์กร และกิจกรรมที่องค์กรทำอยู่ในแต่ละระดับ เพื่อให้สามารถระบุปัจจัยเสี่ยงได้อย่างถูกต้อง

2. การวิเคราะห์ความเสี่ยง (Risk Analysis)

- **โอกาสที่จะเกิด (Likelihood)** หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
- **ระดับของความเสี่ยง (Degree of Risk)** หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง น้อย และน้อยมาก
- **ผลกระทบ (Impact)** หมายถึง ขนาดความรุนแรงของความเสียหายที่มีต่อองค์กร หากเหตุการณ์นั้นเกิดขึ้นจริงผลกระทบอาจพิจารณาความเสียหายทางการเงิน และไม่ใช่ทางการเงิน เช่น ความเชื่อมั่น และชื่อเสียง การประเมินผลกระทบอาจใช้วิธีเชิงคุณภาพ หรืออาจกำหนดเชิงปริมาณโดยพิจารณาจากจำนวนความเสียหายทางการเงิน ซึ่งเหตุการณ์เดียวกันอาจมีผลกระทบแต่ละองค์กรต่างกัน

ระดับค่าความเสี่ยง = ความเป็นไปได้ที่เกิดขึ้น x ผลกระทบของความเสี่ยงนั้น

ระดับความเสี่ยง	ความเป็นไปได้ของความเสี่ยง (Likelihood)				
ผลกระทบ (Consequence)	1	2	3	4	5
5	ความเสี่ยงปานกลาง (5)	ความเสี่ยงสูง (10)	ความเสี่ยงสูง (15)	ความเสี่ยงสูงมาก (20)	ความเสี่ยงสูงมาก (25)
4	ความเสี่ยงปานกลาง (4)	ความเสี่ยงปานกลาง (8)	ความเสี่ยงสูง (12)	ความเสี่ยงสูง (16)	ความเสี่ยงสูงมาก (20)
3	ความเสี่ยงปานกลาง (3)	ความเสี่ยงปานกลาง (6)	ความเสี่ยงสูง (9)	ความเสี่ยงสูง (12)	ความเสี่ยงสูง (15)
2	ความเสี่ยงต่ำ (2)	ความเสี่ยงปานกลาง (4)	ความเสี่ยงปานกลาง (6)	ความเสี่ยงปานกลาง (8)	ความเสี่ยงสูง (10)
1	ความเสี่ยงต่ำ (1)	ความเสี่ยงต่ำ (2)	ความเสี่ยงปานกลาง (3)	ความเสี่ยงปานกลาง (4)	ความเสี่ยงปานกลาง (5)

มีความเสี่ยงสูงมาก คะแนน 17 – 25 คะแนน

มีความเสี่ยงสูง คะแนน 9 – 16 คะแนน

มีความเสี่ยงปานกลาง คะแนน 3 – 8 คะแนน

มีความเสี่ยงต่ำ คะแนน 1 – 2 คะแนน

3. การบริหารความเสี่ยง (Risk Management) ได้แก่

1) การยอมรับความเสี่ยง (Risk Acceptance)

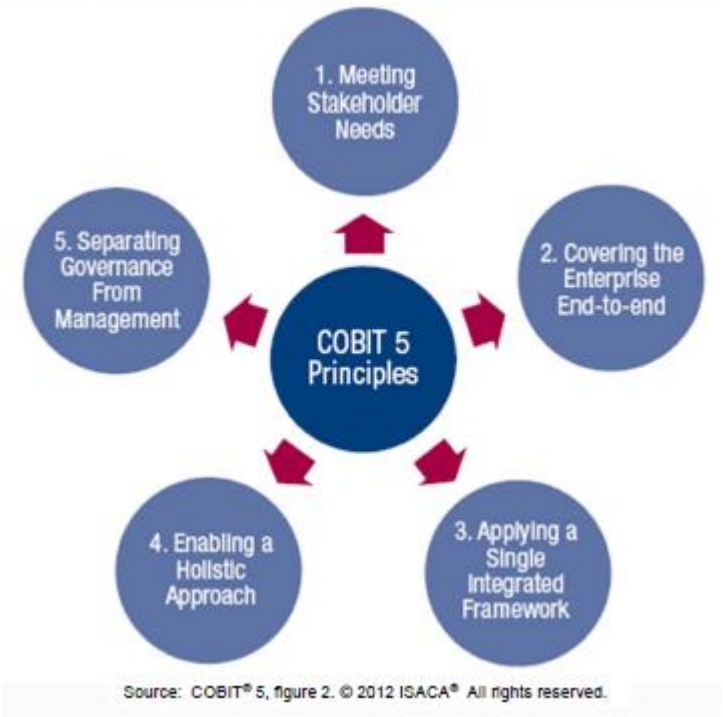
2) การลด/การควบคุมความเสี่ยง (Risk Reduction/Control)

3) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

4) การกระจาย/การโอนความเสี่ยง (Risk Sharing/Spreading)

COBIT® 5 (Control Objectives for Information and Related Technology)

สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ – ภาคพื้นกรุงเทพฯ หรือ ISACA ได้เปิดตัว COBIT®5 อย่างเป็นทางการ เมื่อเดือนเมษายน 2555 โดยตระหนักว่า COBIT®5 เป็นประโยชน์อย่างมากสำหรับองค์กรและผู้ประกอบวิชาชีพที่เกี่ยวข้อง ตลอดจนยังเป็นประโยชน์กับการดำเนินธุรกิจของกิจการต่างๆ ประกอบด้วยหลักการที่สำคัญ 5 ส่วน ได้แก่



1) ตรงตามความต้องการของผู้มีส่วนได้ส่วนเสีย

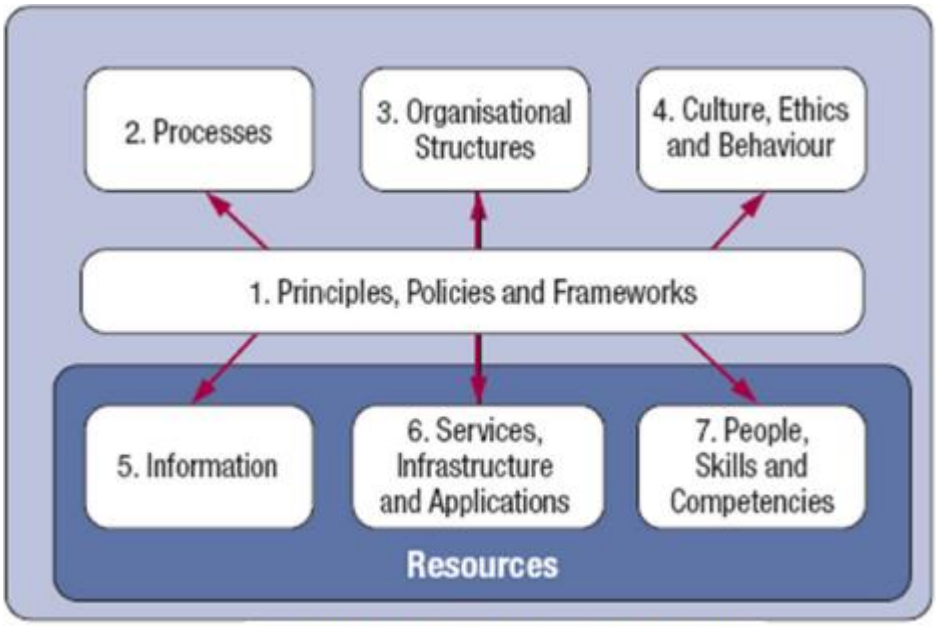
2) ครอบคลุมกระบวนการธุรกิจ (Business process) และ Flow การทำงานทั่วทั้งองค์กร

3) เชื่อมโยงให้เป็นอันหนึ่งอันเดียวกัน

4) เป็นภาพรวมกว้างๆ

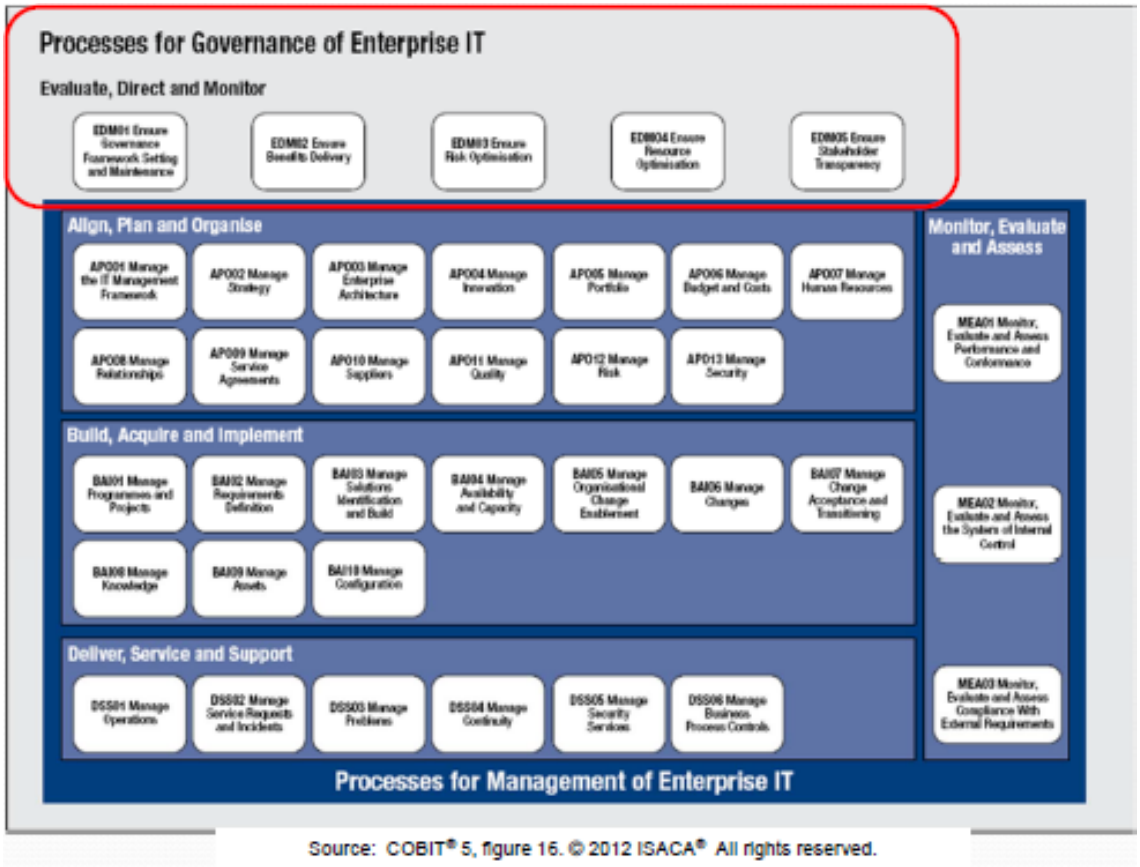
5) แยก Governance ออกจาก Management

โดยต้องดำเนินการ 7 อย่าง ดังนี้



1) มีหลักการ นโยบาย และกรอบการทำงาน
2) มีกระบวนการขั้นตอน
3) มีโครงสร้างองค์กร
4) มีวัฒนธรรมองค์กร จริยธรรม และพฤติกรรม
5) มีข้อมูลข่าวสาร
6) มีบริการ โครงสร้างพื้นฐาน และโปรแกรมประยุกต์
7) มีบุคคลที่มีทักษะและสมรรถนะ

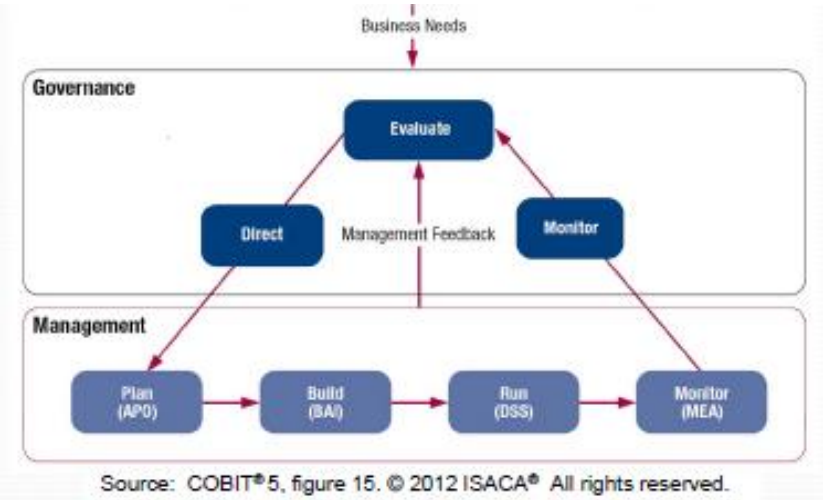
ธรรมาภิบาลของ COBIT®5 ประกอบด้วย 5 โดเมน 37 กระบวนการ ดังภาพ



Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.

- 01 Ensure governance framework setting and maintenance.
- 02 Ensure benefits delivery.
- 03 Ensure risk optimisation.
- 04 Ensure resource optimisation.
- 05 Ensure stakeholder transparency.

ทั้ง 5 โดเมน ต้องครอบคลุมหน้าที่ความรับผิดชอบในเรื่องของการวางแผน (Plan) การสร้าง (Build) การดำเนินงาน (Run) และการติดตาม (Monitor)



Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.

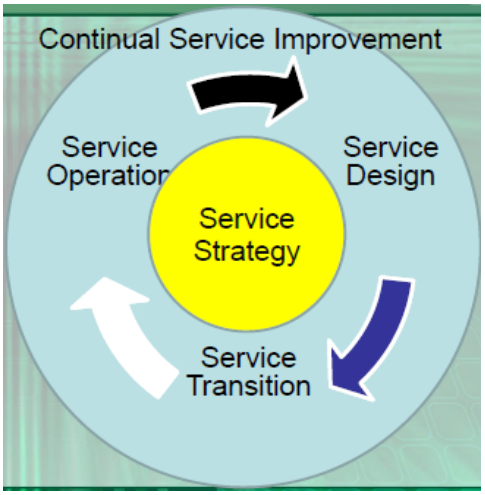
SOX (Sarbanes-Oxley) เป็นมาตรฐานทางด้านกฎหมายและบัญชีขององค์กร เริ่มใช้งานตั้งแต่กรกฎาคม ค.ศ. 2002

มาตรฐาน SOX ที่เกี่ยวข้องกับการควบคุมภายใน คือ SOX Section 404 ซึ่งกำหนดให้องค์กรต้องรายงานสถานะการเงินอย่างมีประสิทธิภาพและโปร่งใส

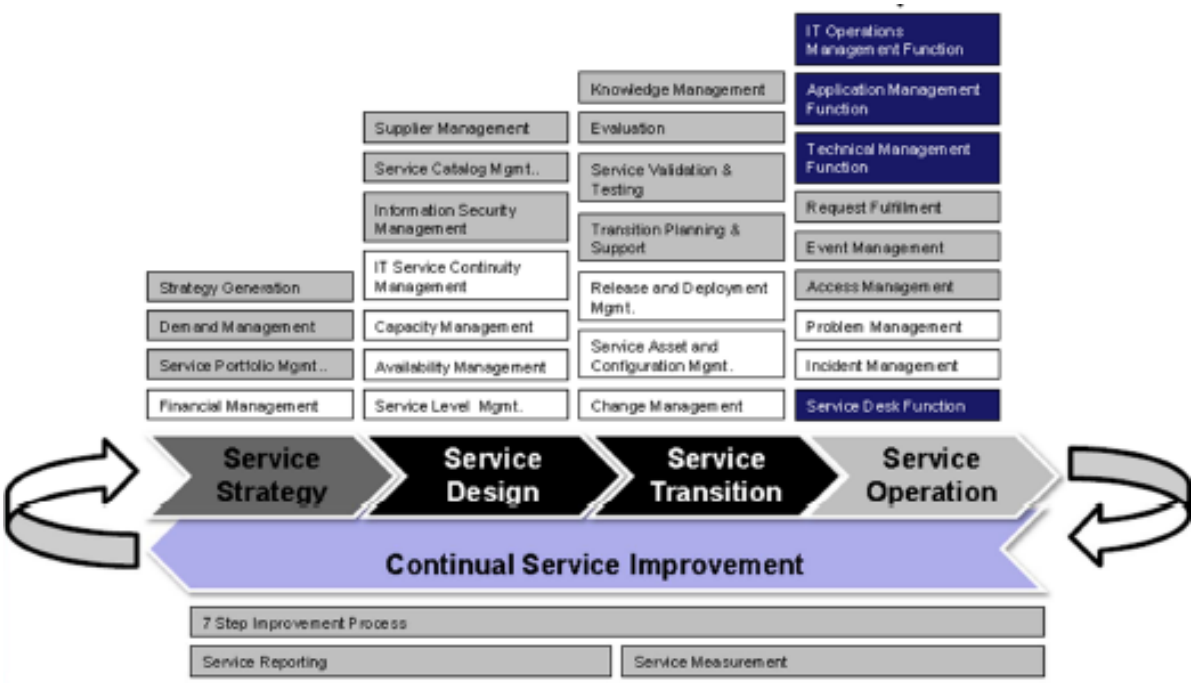
มาตรฐาน SOX มีผลกระทบต่อ IT และ Management ดังนี้

- การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย
  - Areas of Risk
  - Examination of systems
  - Accuracy of Documentation
- สภาพแวดล้อมของการควบคุม (Control Environment) ประกอบด้วย
  - Effectiveness of IC's
  - Tone of Organization
  - Control Environment Factors
- การควบคุมความมั่นคงปลอดภัย (Control Security) คือ ความมั่นคงปลอดภัยของ IT
- การติดตาม (Monitoring) ประกอบด้วย
  - Processes and Schedules
  - Internal Audits
- ข้อมูลข่าวสารและการสื่อสาร (Information and Communication) ประกอบด้วย
  - Timely and Accurate Information
  - Communication to Management

ITIL (Information Technology Infrastructure Library) เป็นมาตรฐานการจัดการบริการด้านเทคโนโลยีสารสนเทศ ของ OGC (Office of Government Commerce) ปัจจุบันใช้ ITIL version 3 ส่วนประกอบของ ITIL version 3 ดังภาพ



กระบวนการ (processes) และหน้าที่งาน (functions) ในวงจรชีวิตของ ITIL version 3 เป็นดังนี้



1. กลยุทธ์การบริการ (Service Strategy) ประกอบด้วย

- Strategy management
- Service Portfolio Management
- Financial Management
- Demand Management
- Business Relationship Management

2. การออกแบบบริการ (Service Design) ประกอบด้วย

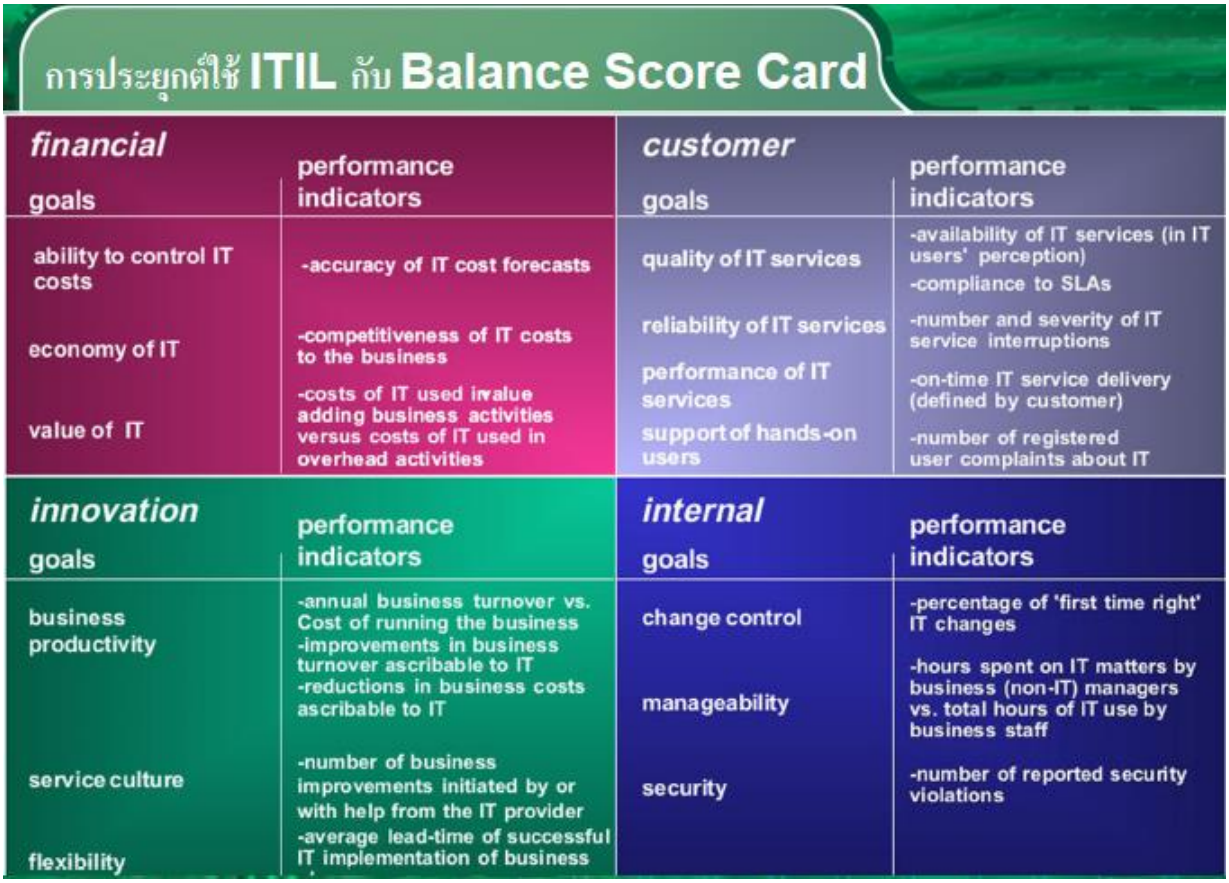
- Design coordination คือ การออกแบบกิจกรรม กระบวนการ ทรัพยากร ให้มีความชัดเจนเกี่ยวกับการเพิ่มบริการใหม่หรือปรับเปลี่ยนบริการเดิม
- Service Catalogue Management เป็นการจัดการสารสนเทศใน Service catalogue เพื่อให้มั่นใจว่าระบบสารสนเทศมีความแม่นยำและเป็นปัจจุบัน
- Service Level Management (SLM)
- Availability Management
- Capacity Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management

3. การส่งต่อบริการ (Service Transition) คือ การส่งมอบสถานะการดำเนินงานในทุกรายการเพื่อให้ระบบปฏิบัติการทำงานอย่างต่อเนื่อง ประกอบด้วย

- การบริหารการเปลี่ยนแปลง (Change Management)
- Service Asset and Configuration Management
- Knowledge Management (S.369)

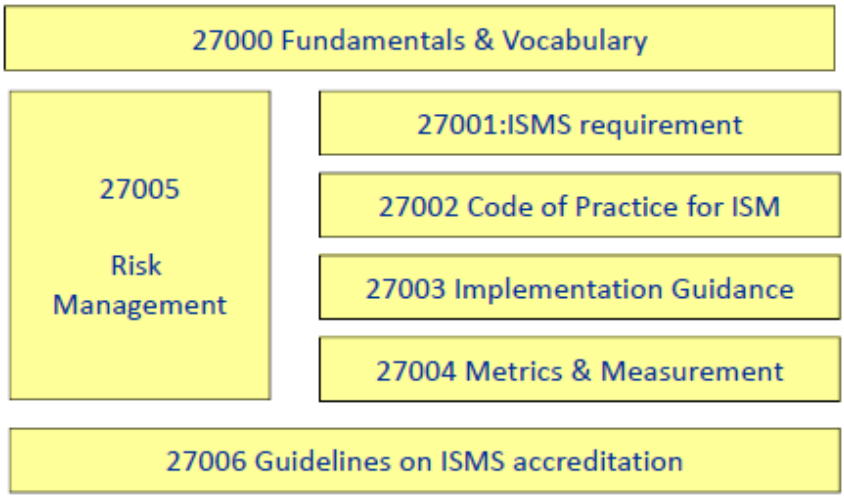
4. การออกแบบบริการ (Service Operation) S.381 ประกอบด้วย

- Event Management
- Request Fulfillment
- Access management
- Service Desk
- Incident Management
- Problem Management


การประยุกต์ใช้ ITIL กับ Balance Score Card
financial
goals
performance indicators
ability to control IT costs
economy of IT
value of IT
-accuracy of IT cost forecasts
-competitiveness of IT costs to the business
-costs of IT used in value adding business activities versus costs of IT used in overhead activities
customer
goals
performance indicators
quality of IT services
reliability of IT services
performance of IT services
support of hands-on users
-availability of IT services (in IT users' perception)
-compliance to SLAs
-number and severity of IT service interruptions
-on-time IT service delivery (defined by customer)
-number of registered user complaints about IT
innovation
goals
performance indicators
business productivity
service culture
flexibility
-annual business turnover vs. Cost of running the business
-improvements in business turnover ascribable to IT
-reductions in business costs ascribable to IT
-number of business improvements initiated by or with help from the IT provider
-average lead-time of successful IT implementation of business
internal
goals
performance indicators
change control
manageability
security
-percentage of 'first time right' IT changes
-hours spent on IT matters by business (non-IT) managers vs. total hours of IT use by business staff
-number of reported security violations

ISO/IEC 27001:2013 (Information Technology Infrastructure Library) เป็นมาตรฐานสำหรับการจัดทำมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ

โครงสร้างของ ISO 27001 เป็นดังนี้



ความมั่นคงปลอดภัยสารสนเทศ (Information Security)

ในเอกสาร ISO 27001:2013 ประกอบด้วย เนื้อหา 14 หัวข้อหลัก มีวัตถุประสงค์ของการควบคุม 35 รายการ และมีการควบคุมทั้งหมด 114 รายการ ดังนี้

ISO 27001:2013 Annex A Controls ISO 27001:2005 Annex A Controls		
Domain	Control Objective	Controls
Clause 1-10 General, Terms, Specifications		
A.5 Information security policies (1, 2)	1	2
A.6 Organisation of information (2, 7)	2	7
A.7 Human resource security (3, 6)	3	6
A.8 Asset Management (3, 10)	3	10
A.9 Access control (4, 14)	4	14
A.10 Cryptography (1, 2)	1	2
A.11 Physical and environmental security (2, 15)	2	15
A.12 Operations security (7, 14)	7	14
A.13 Communications security (2, 7)	2	7
A.14 System acquisition, development and maintenance (3, 13)	3	13
A.15 Supplier relationships (2, 5)	2	5
A.16 Information security incident management (1, 7)	1	7
A.17 Information security aspects of business continuity management (2, 4)	2	4
A.18 Compliance (2, 8)	2	8
Total 14 Domains	35	114

ISO 22301:2012 (Business Continuity Management Systems; BCM) เป็นมาตรฐานสำหรับจัดการความต่อเนื่องในการดำเนินงาน

1. **การวางแผนดำเนินงานอย่างต่อเนื่อง (Business Continuity Planning; BCP)** ประกอบด้วย
   1) กำหนดนโยบาย ขอบเขตการทำงาน และกิจกรรมที่ต้องทำ
   2) กำหนดผู้รับผิดชอบ และการจัดทำเอกสารที่เกี่ยวข้อง
   3) ระบุประโยชน์และวัตถุประสงค์ ประเมินความต้องการ ประเมินความเสี่ยง และตัวบ่งชี้
   4) กำหนดทางเลือกเชิงกลยุทธ์ ทางเลือกของกิจกรรมและลำดับของแหล่งข้อมูล
   5) กำหนดแผนการจัดการ แผนการดำเนินงานอย่างต่อเนื่อง แผนการตอบสนองต่อกิจกรรม
   6) ทดสอบแผน ปรับปรุงและทบทวนแผน
2. **การวางแผนกู้คืนภายหลังจากเกิดภัยพิบัติ (Disaster Recovery Planning; DRP)** ประกอบด้วย
   1) การประเมินความเสี่ยง (Risk Assessment)
   2) การวิเคราะห์ผลกระทบกับการดำเนินงาน
   3) การระบุกลยุทธ์ที่ใช้ในการกู้คืน
   4) การจัดทำแผนกู้คืนภายหลังภัยพิบัติ
   5) กลยุทธ์ในการนำไปใช้
   6) ทดสอบแผน
   6) แผนการบำรุงรักษา