เจาะลึก IT Governance Implementation และ บทวิเคราะห์ CobiT 5.0 “Enterprise Governance of IT Framework” และ IT Governance Implementation Guide ล่าสุดจาก ISACA

Why IT Governance? : The latest update of IT Governance Implementation Guide and Inside the new CobiT 5.0 Design

ปริญญา หอมเอนก, CGEIT, CISSP, CSSLP, SSCP, CISA,

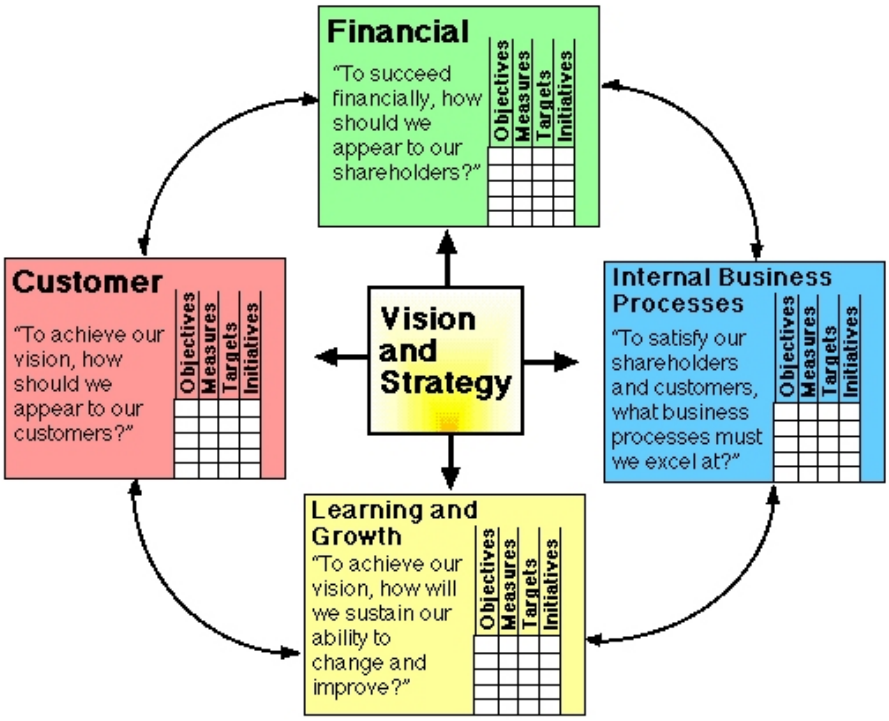
CISM, SANS GIAC GCFW, IRCA Lead Auditor

ACIS Professional Center

http://www.acisonline.net

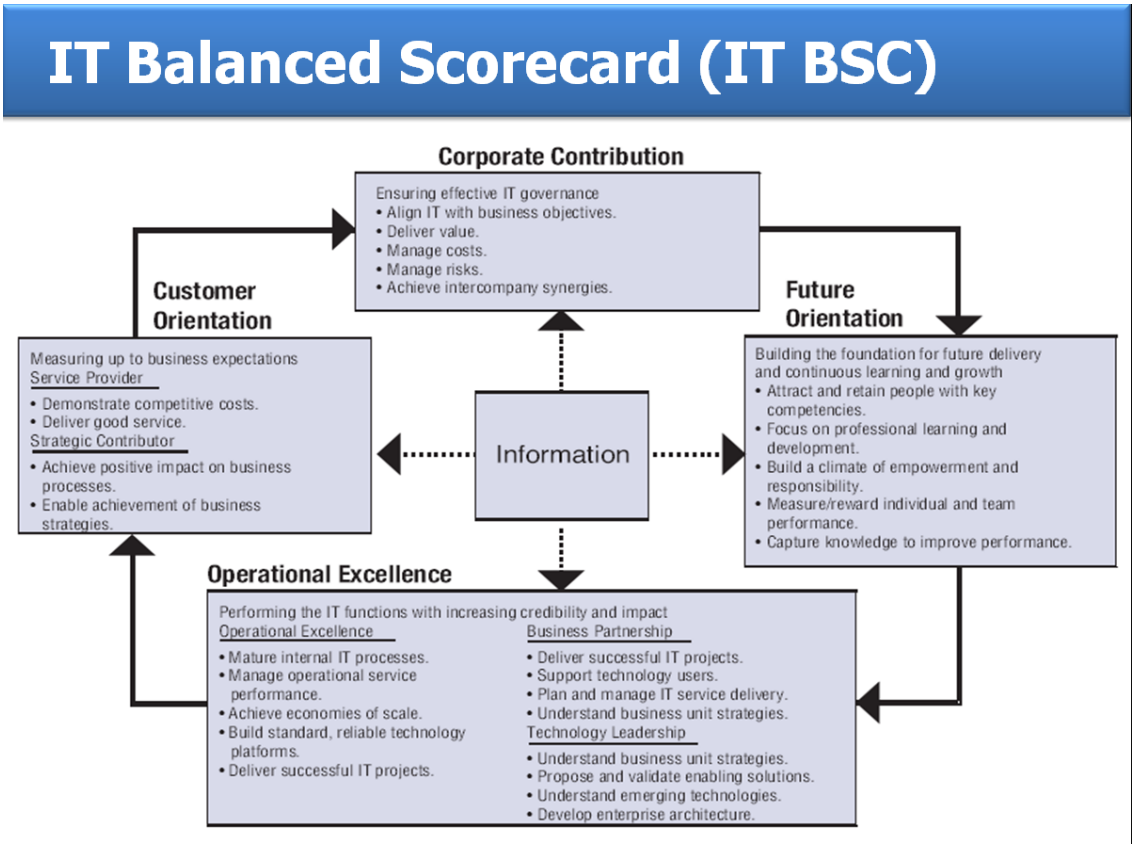
prinya@acisonline.net

ในปัจจุบันคำว่า “IT Governance” และ “Information Security Governance” กำลังเป็นที่กล่าวถึงกันในวงการธุรกิจตลอดจนในวงการไอที ตลอดจนแนวคิดเรื่อง “Green IT” และ “Sustainability” เป็นการมาถึงของยุคที่แนวคิด “Corporate Governance” หรือ “Enterprise Governance” กำลังมาแรงและถูกนำมาประยุกต์ใช้ในองค์กรทั่วโลก อันเนื่องมาจากปัญหาความไม่โปร่งใส และการบริหารงานที่ฉ้อฉล (Fraud) ของผู้บริหารระดับสูง และ การบริหารองค์กรที่ไม่มีประสิทธิภาพของหลายองค์กรใหญ่ๆในเวลานี้ จึงเป็นที่มาของแนวทางในการแก้ปัญหาที่ต้นเหตุ โดยพิจารณาถึงปัญหาที่เกิดจากการบริหารจัดการที่ไม่โปร่งใสของผู้บริหารระดับสูงที่ยังไม่สามารถบริหารจัดการองค์กรให้มีประสิทธิภาพและประสิทธิผลได้ เนื่องจากยังขาดองค์ความรู้หรือแนวทางปฏิบัติที่ดีในการบริหารจัดการตามแนวคิด “Corporate Governance” หรือ “Enterprise Governance” ซึ่งในปัจจุบันการทำธุรกิจธุรกรรมของทุกองค์กรนั้นต้องพึ่งพาการใช้เทคโนโลยีสารสนเทศหรือ “Information Technology (IT)” เป็นสำคัญ ดังนั้น การบริหารจัดการ “IT” จำเป็นต้องสอดคล้อง หรือ “Align” กับการบริหารจัดการองค์กร กล่าวคือ กลยุทธ์ในการบริหารจัดการเทคโนโลยีสารสนเทศ (IT Strategy) ต้องสอดคล้องกับกลยุทธ์ในการบริหารจัดการองค์กร (Business Strategy) เพื่อให้บรรลุเป้าหมายเดียวกัน โดยหลักการที่นิยมในการนำมากำหนดกลยุทธ์ในการบริหารจัดการองค์กรก็คือ Balanced Scorecard (BSC) (ดูรูปที่ 1)



รูปที่ 1 : "Balanced Scorecard"

"BSC" เป็นเทคนิควิธีในการประเมินประสิทธิภาพขององค์กรที่คิดค้นโดย Dr. Robert S. Kaplan และ Dr. David P. Norton แห่งมหาวิทยาลัยฮาร์วาร์ด ซึ่งเมื่อนำมาประยุกต์ใช้กับการบริหารจัดการเทคโนโลยีสารสนเทศที่เรียกว่า "IT BSC" (ดูรูปที่ 2)



รูปที่ 2 : "IT Balanced Scorecard"

โดย BSC จะมีมุมมองใน 4 มุมมองได้แก่ **Financial, Customer, Internal Business Processes และ Learning and Growth** ขณะที่ "IT BSC" มีการปรับ 4 มุมมองของ BSC เป็น 4 มุมมองใหม่ ได้แก่ **Corporate Contribution, Future Orientation, Operational Excellence และ Customer Orientation** โดยการเชื่อม (Link)ระหว่าง เป้าหมายของธุรกิจ "Business Goals" ที่อ้างอิงจาก BSC กับเป้าหมาย จากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร หรือ "IT Goals" นั้นสามารถอ้างอิงได้ จากตารางใน Appendix I ของ CobiT 4.1 (ดูรูปที่ 3) "Linking Business Goals to IT Goals" ทำให้เราสามารถกำหนดกระบวนการทางด้านเทคโนโลยีสารสนเทศ หรือ "IT Processes" ที่สอดคล้องกับ "IT Goals" ดังกล่าว (ดูรูปที่ 4) "Linking IT Goals to IT Processes" ซึ่งใน CobiT Framework ได้กำหนด Business Goals ไว้ทั้งหมด 17 เป้าหมายและ IT Goals ทั้งหมด 28 เป้าหมาย โดยสามารถอ้างอิงถึง 34 กระบวนการหลักในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดีตาม CobiT 4.1 Framework

LINKING BUSINESS GOALS TO IT GOALS

		Business Goals	IT Goals								CobiT Information Criteria: Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24									✔					
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22			✔	✔	✔		
	3	Improve corporate governance and transparency.	2	18													✔
Customer Perspective	4	Improve customer orientation and service.	3	23							✔						
	5	Offer competitive products and services.	5	24							✔	✔					
	6	Establish service continuity and availability.	10	16	22	23					✔				✔		
	7	Create agility in responding to changing business requirements.	1	5	25						✔	✔					
	8	Achieve cost optimisation of service delivery.	7	8	10	24						✔					
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26				✔			✔			✔
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11						✔	✔					
	11	Lower process costs.	7	8	13	15	24					✔					
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27				✔			✔	
	13	Provide compliance with internal policies.	2	13									✔			✔	
	14	Manage business change.	1	5	6	11	28				✔	✔					
	15	Improve and maintain operational and staff productivity.	7	8	11	13					✔	✔					
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28						✔	✔					
	17	Acquire and maintain skilled and motivated people.	9								✔	✔					

รูปที่ 3 : “Linking Business Goals to IT Goals”

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes										CobiT Information Criteria						
												Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4						P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimise the use of information.	PO2	DS11										S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3							P	P		S			
6	Define how business functional and control requirements are translated into effective and efficient automated solutions.	AI1	AI2	AI6								P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5								P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5									S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5									P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2										P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7								P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8						P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9						S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2								P	P	S	S	S	S	S
18	Establish clarity on the business impact of risks to IT objectives and resources.	PO9										S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12									P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5								P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12							P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13							P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6									S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10									P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5									P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4									S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4							P	P					P

รูปที่ 4 : "Linking IT Goals to IT Processes"

ปัญหาที่พบบ่อยจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร (7 IT Challenges)

รูปที่ 5 : "7 IT Challenges"

ปัจจุบันองค์กรทั่วโลกกำลังประสบปัญหาที่คล้าย ๆ กันจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรโดยสามารถแบ่งได้ออกเป็น 7 ปัญหาใหญ่ ๆ (ดูรูปที่ 5) ได้แก่

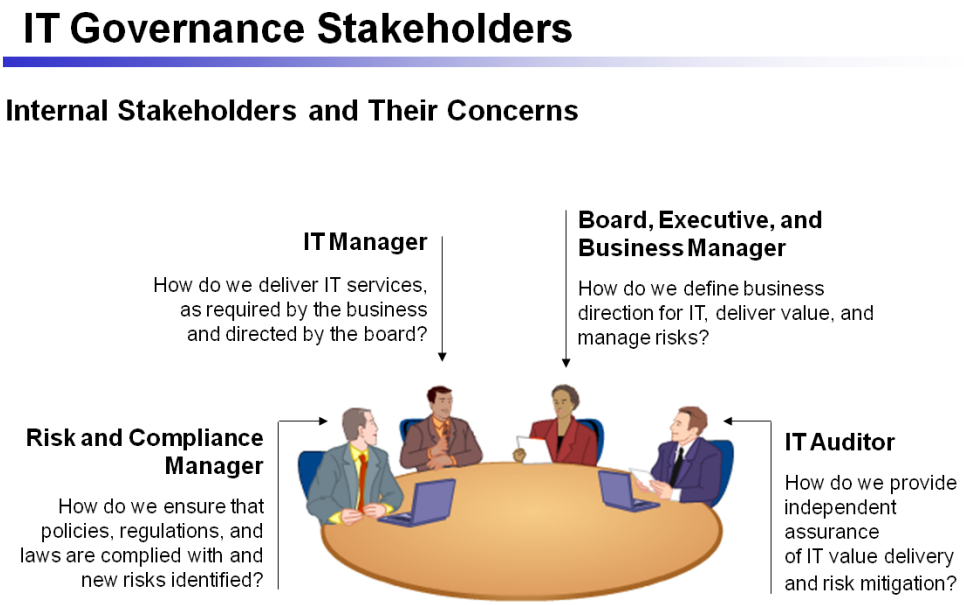
1. **"Keeping IT Running"**

   บางครั้งการให้บริการขององค์กรอาจหยุดชะงักได้ในกรณีที่ระบบสารสนเทศเกิดปัญหา เช่น ระบบล่ม (Unavailability) ทำให้ไม่สามารถให้บริการข้อมูลต่าง ๆ ที่ธุรกิจต้องการจากระบบสารสนเทศที่กำลังเกิดปัญหาอยู่ ดังนั้นองค์กรต้องแน่ใจได้ว่าระบบพร้อมให้บริการในเวลาที่ต้องการ (Availability) และระบบสามารถทำงานและให้บริการอย่างต่อเนื่องได้ (Continuity of IT Service) เวลาที่ระบบหลักเกิดปัญหาฉุกเฉิน เพื่อให้ระบบหลัก (Critical Business System) สามารถกลับมาให้บริการได้อย่างไม่

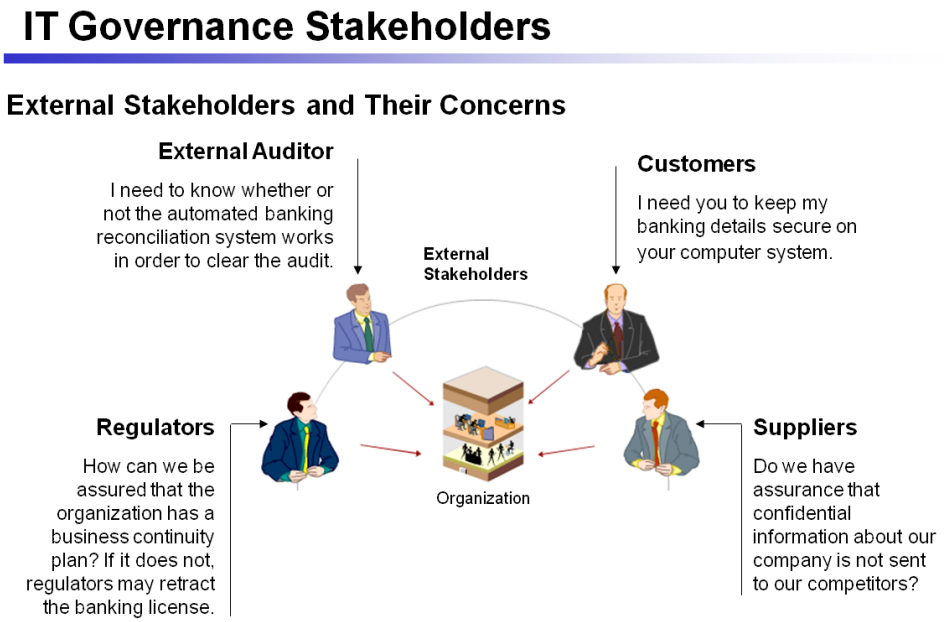
ติดขัด ตามหลักการ BCM (Business Continuity Management) ซึ่งในปัจจุบันอ้างอิงมาตรฐาน BS 25999

2. "Value"

คำว่า "Value" เป็นคำยอดฮิตของวันนี้เช่น การที่องค์กรมุ่งเน้นให้ผลตอบแทนของผู้ถือหุ้นมากที่สุด เรียกว่า "Maximizing Shareholder Value" กำลังเกิดการเปลี่ยนแปลงเป็นการให้ความสำคัญกับผู้ที่เกี่ยวข้องกับองค์กรทั้งหมดที่เรียกว่า "Stakeholder Value" เช่น "Customer Value" และ "Employee Value" คือการทำให้ลูกค้าและพนักงานเกิดความสุขในการใช้บริการและการทำงานในองค์กร ขณะเดียวกันก็ต้องรับผิดชอบต่อสังคมส่วนรวมตามแนวคิด "Corporate social responsibility" หรือ "CSR" ที่เรารู้จักกันดี ตามแนวคิด "IT Governance" นั้น Stakeholder มีสองประเภท ได้แก่ "Internal Stakeholder" (ดูรูปที่ 5) และ "External Stakeholder" (ดูรูปที่ 6)



รูปที่ 6 : Internal Stakeholders and Their Concerns



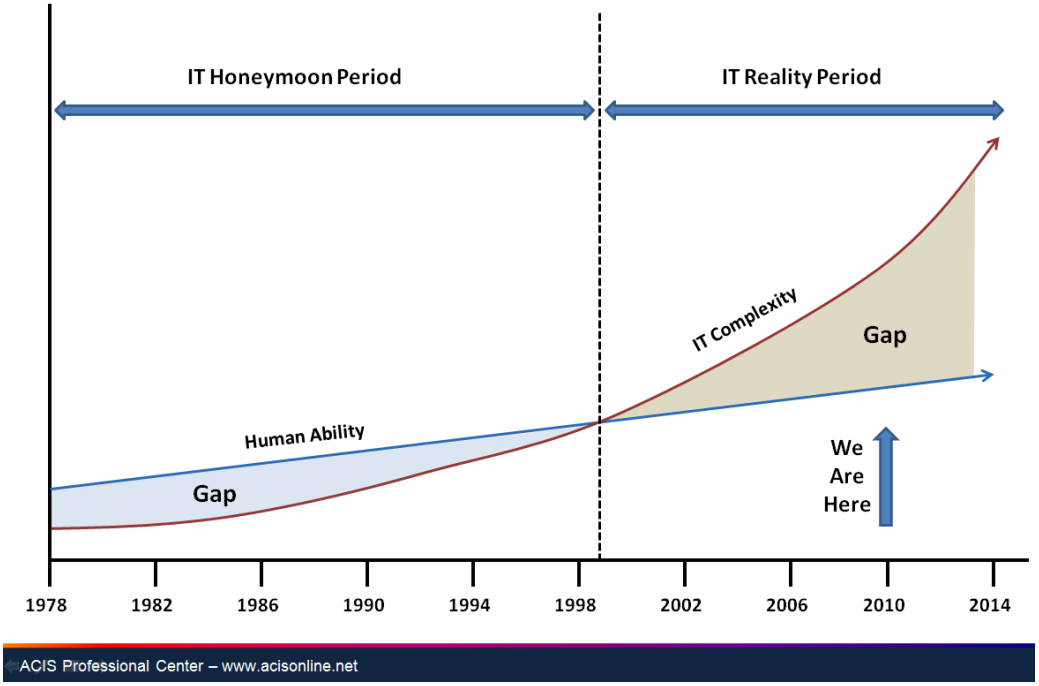
รูปที่ 7 : External Stakeholders and Their Concerns

ดังนั้นการลงทุนทางด้านเทคโนโลยีสารสนเทศขององค์กรที่เรียกว่า “IT Investment” นั้น จึงจำเป็นต้องตอบโจทย์ให้ได้ว่า หลังจากองค์กรลงทุนไปแล้ว **มูลค่าหรือคุณค่า (Value) ที่ได้รับกลับมาจากการลงทุนดังกล่าวนั้น “คุ้มค่า” หรือไม่ ? (IT Value)** ยกตัวอย่าง เช่น ถ้าโครงการที่นำเทคโนโลยีสารสนเทศสามารถตอบโจทย์การให้บริการลูกค้าขององค์กรได้เร็วขึ้น เรียกได้ว่า สามารถทำให้ “IT” มี “Value” ต่อ “Business” ขององค์กร จึงเป็นที่มาของคำว่า “IT Value” (ISACA นำมาเป็นแนวคิดในการพัฒนา Val IT Framework) **ปัญหาก็คือ เราจะสามารถ “วัด” IT Value ได้อย่างไร และ ผู้บริหารจะทราบได้อย่างไรว่าโครงการที่นำเทคโนโลยีสารสนเทศมาใช้สามารถตอบโจทย์ความต้องการทางด้านธุรกิจธุรกรรมต่าง ๆ ขององค์กรได้อย่างมีประสิทธิภาพและมีประสิทธิผล**

3. “Cost”

การควบคุมต้นทุนในการลงทุนเกี่ยวกับเทคโนโลยีสารสนเทศนั้นเป็นอีกปัญหาหนึ่งที่พบเป็นประจำในองค์กร หลายโครงการมักจะมีค่าใช้จ่ายที่สูงเกินกว่าที่คาดประมาณไว้หรืออาจไม่คุ้มค่ากับการลงทุน หลายโครงการล้มเหลวไม่สามารถส่งมอบงานได้ทันเวลาทำให้เกิดค่าใช้จ่ายตามมาอีกมากมาย

จากปัญหาดังกล่าวทำให้องค์กรต้องการมี “กระบวนการ” หรือ “Process” ที่ดี ในการบริหารจัดการค่าใช้จ่ายทางด้านเทคโนโลยีสารสนเทศให้ตอบโจทย์ในมุมมองทั้งด้านประสิทธิภาพ (efficiency) และประสิทธิผล (effective) ในเวลาเดียวกัน ตลอดจนองค์กรควรมีการจัดการด้านการรักษาความสัมพันธ์ที่ดีกับ Vendor หรือ Supplier อีกด้วย (Supplier Management)

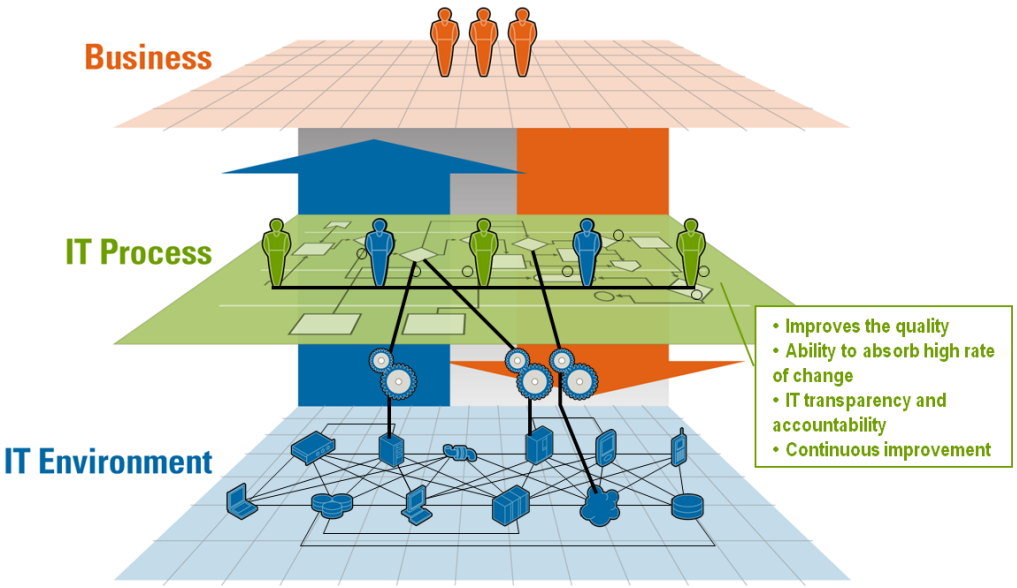


รูปที่ 8 : “Human Ability” vs. “IT Complexity”

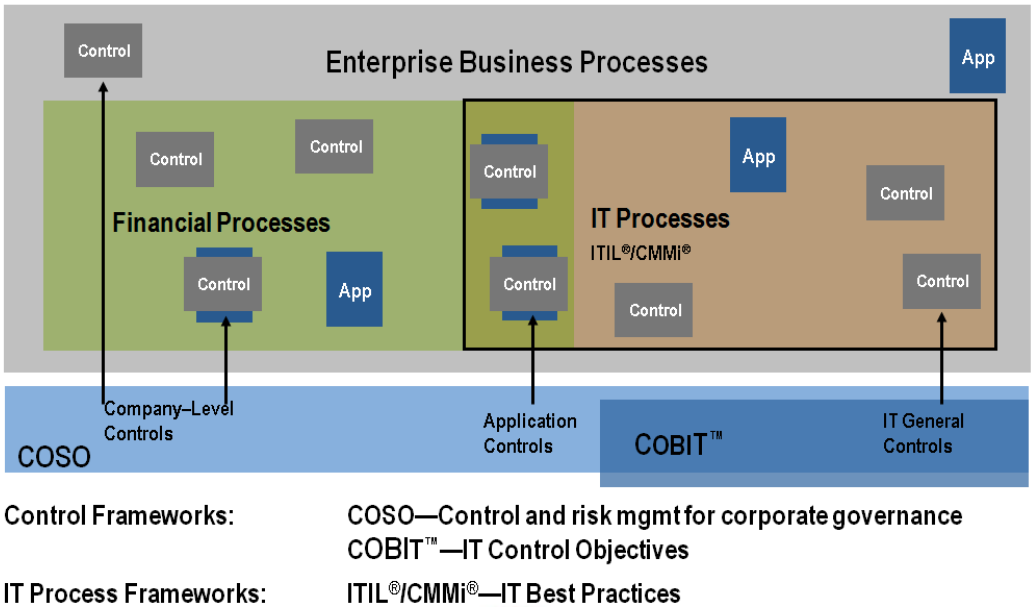
4. “Mastering Complexity”

ในปัจจุบันระบบสารสนเทศและเทคโนโลยีสารสนเทศตลอดจนเทคโนโลยีอินเทอร์เน็ตมีความซับซ้อนมากขึ้นกว่าในอดีตมาก (ดูรูปที่ 8) ความสามารถในการจัดการของมนุษย์ (human ability) เมื่อเปรียบเทียบกับความซับซ้อนของระบบสารสนเทศ (IT complexity) นั้นเริ่มห่างขึ้นเรื่อย ๆ ทำให้เกิดช่องว่าง หรือ “GAP” ส่งผลให้เกิดปัญหาในการควบคุมและบริหารจัดการ (Control and Manage) ระบบสารสนเทศเพิ่มมากขึ้นในระยะยาว ดังนั้น ผู้บริหารระดับสูงขององค์กรที่มีวิสัยทัศน์เล็งเห็นปัญหาดังกล่าว จึงได้พยายามนำ Framework, Standard และ Best Practice ต่าง ๆ ไม่ว่าจะเป็น CobiT, ITIL หรือ ISO27001, ISO 20000 ตลอดจน BCMS มาประยุกต์ใช้ในองค์กรเพื่อปิด GAP ดังกล่าว โดย

เจาะลึกในส่วนของการปรับกระบวนการด้านการบริหารจัดการเทคโนโลยีสารสนเทศภายในองค์กร (Internal IT Process) (ดูรูปที่ 9) ซึ่งเป็นส่วนที่ควรปรับแต่งมากที่สุด ขณะที่การปรับ “IT Process” นั้นก็ควรจะคำนึงถึงกระบวนการในการควบคุม หรือ “IT Control” ไปด้วย เนื่องจากทุกกระบวนการ (Process) จำเป็นต้องมีการควบคุม (Control) เพราะถ้าเราไม่สามารถควบคุมได้ เราก็ไม่สามารถบริหารจัดการได้ (If you cannot control, you cannot manage it : จากหนังสือ ITIL V3 CSI) การนำ CobiT Framework มาใช้นั้น เรานำมาใช้เป็น “Control Framework” ขณะที่การนำ ITIL มาใช้ก็เพื่อใช้เป็น “Process Framework” (ดูรูปที่ 10) ในการบริหารจัดการระบบสารสนเทศให้เกิดประสิทธิภาพ และประสิทธิผลดังที่กล่าวมาแล้วในตอนต้น



รูปที่ 9 : Business, IT process and IT environment Relationship



รูปที่ 10 : Process Framework and Control Framework

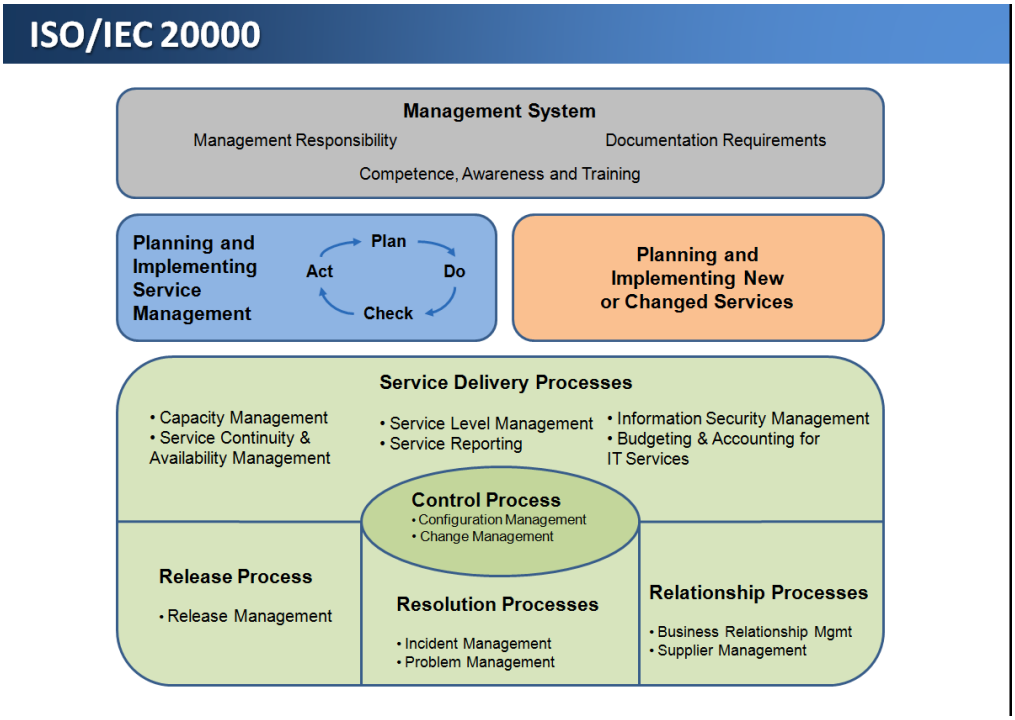
5. "Aligning IT with Business"

เป็นปัญหาใหญ่ระดับองค์กรที่ไม่ควรมองข้าม เพราะถ้าหากการนำเทคโนโลยีสารสนเทศมาใช้แล้วไม่สอดคล้องกับการดำเนินธุรกิจขององค์กรก็ไม่สามารถที่จะตอบโจทย์ของผู้บริหารระดับสูง ผู้ใช้งานระบบสารสนเทศ ตลอดจน ความต้องของลูกค้า และ ผู้ถือหุ้น ได้ ซึ่งโดยปกติแล้ว เราพบว่ามีช่องว่างเกิดขึ้นระหว่างความต้องการของผู้ใช้ระบบสารสนเทศ กับความเข้าใจของคนไอทีอยู่เป็นประจำ ดังนั้น การทำให้ระบบสารสนเทศที่องค์กรนำมาใช้มีความสอดคล้องกับความต้องการทางด้านธุรกิจขององค์กรนั้น จึงมีความสำคัญอย่างยิ่งยวด

6. "Regulatory Compliance"

เป็นอีกปัญหาหนึ่งขององค์กรในปัจจุบันเนื่องจากกระแสของการตรวจสอบ (Audit) และการประเมิน (Assess) ทั้งผู้ตรวจสอบภายใน (Internal Auditor) และผู้ตรวจสอบภายนอก (External Auditor) กำลังเพิ่มขึ้นอย่างต่อเนื่อง โดยปัจจัยที่ทำให้เรื่อง "Regulatory Compliance" มาแรง เนื่องจากการออกกฎหมายและกฎข้อบังคับต่าง ๆ ที่ทยอยออกมาบังคับใช้อย่างต่อเนื่อง อีกทั้งยังเป็นความต้องการของ

องค์กรที่ต้องการยกระดับเข้าสู่มาตรฐานในระดับสากล เช่น ISO/IEC 27001, ISO/IEC 20000 (ดูรูปที่ 11) เพื่อเสริมศักยภาพและภาพลักษณ์ที่ดีให้แก่องค์กรในยุค Globalization โดยกฎข้อบังคับต่าง ๆ ไม่ได้ถูกบังคับเฉพาะสถาบันการเงินเท่านั้น แต่ถูกบังคับสำหรับองค์กรโดยทั่วไป เช่น กฎหมายธุรกรรมอิเล็คโทรนิกส์ และกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์



รูปที่ 11 : ISO/IEC 20000

7. "Security"

ข้อมูล และ สารสนเทศ (Data and Information) จำเป็นต้องรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) หรือ CIA TRIAD ดังนั้นการป้องกันความปลอดภัยของข้อมูลและสารสนเทศขององค์กรจึงมีความสำคัญอย่างมากในยุคที่เราสามารถเข้าถึงข้อมูลและสารสนเทศอย่างรวดเร็ว หรือ **ที่เราเรียกว่ายุค "Pervasive Computing"** ปัญหาทางด้านความปลอดภัยของระบบสารสนเทศจึงเป็น เรื่องใหญ่ที่ผู้บริหารขององค์กรต้องให้ความสำคัญไม่ให้เกิดผลกระทบ หรือ "Impact" ต่อการปฏิบัติงานและการดำเนินธุรกิจขององค์กร

จากปัญหาทั้ง 7 ประเด็นดังกล่าวจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร จึงจำเป็นที่ผู้บริหารระดับสูงต้อง “รับผิดชอบ” (accountability) ในการให้บริการสารสนเทศแก่ผู้ใช้ในองค์กรและลูกค้าให้เกิดความต่อเนื่องและ ต้องรักษาคุณสมบัติที่ดีทั้ง 7 ประการของสารสนเทศไว้ตาม CobiT Information Criteria ได้แก่ Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance และ Reliability เพื่อให้สารสนเทศขององค์กรเป็นสารสนเทศ (Information) ที่มีคุณภาพสามารถนำไปใช้ในการติดสินใจของผู้บริหาร และนำไปใช้ในการดำเนินธุรกิจ, ธุรกรรมต่าง ๆ ขององค์กรได้อย่างมีประสิทธิภาพและประสิทธิผล

ดังนั้นจึงเกิดความจำเป็นในการนำหลักแนวคิด “IT Governance” มาประยุกต์ใช้ในองค์กรโดยนำ CobiT Framework มาเป็นกรอบความคิด และ ปฏิบัติตามหลักแนวคิด IT Governance ที่เราเรียกว่า “IT Governance Implementation” มาทำให้เกิดผลในทางปฏิบัติจริงขององค์กร ซึ่งในปัจจุบันหลายองค์กรได้นำ CobiT Version 4.1 มาใช้เป็น IT Governance Framework และนำเอกสารจาก ISACA ชื่อ “IT Governance Implementation Guide; 2nd Edition” มาเป็นแนวทางในการ Implement และจากการนำ CobiT 4.1 และ IT Governance Implementation Guide มาใช้ในช่วงเวลา 2-3 ปีที่ผ่านมา ทำให้ทาง ISACA ค้นพบจุดบกพร่องของ CobiT 4.1 และ IT Governance Implementation Guide ดังนี้

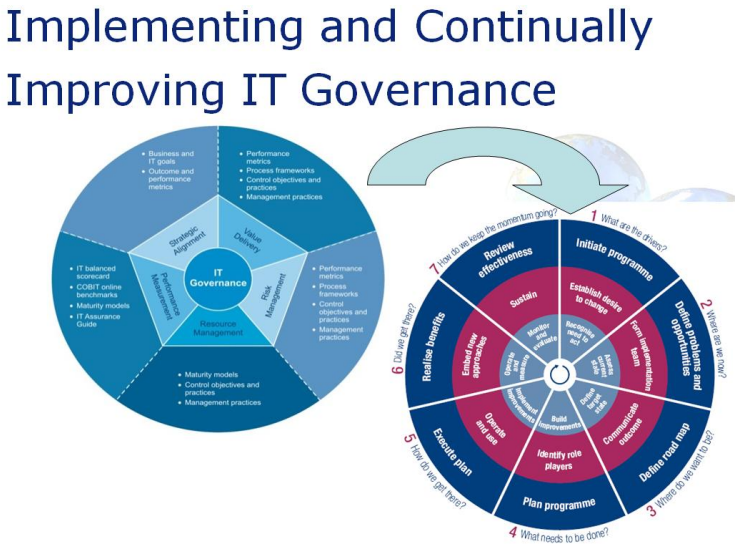
<u>จุดบกพร่องของ CobiT 4.1 (CobiT 4.1 Weaknesses)</u>

- CobiT 4.1 ยังคงเป็น Framework ที่ครอบคลุมเฉพาะเรื่อง IT Governance เท่านั้น แต่ยังไม่ครอบคลุมถึง Enterprise Governance
- CobiT 4.1 ถูกมองว่าเป็น “Tool” ของผู้ตรวจสอบหรือ “IT Auditor” เท่านั้น ซึ่งจริง ๆ แล้ว CobiT ถูกออกแบบมาให้ผู้บริหารระดับสูงและผู้บริหารระบบสารสนเทศตลอดจนผู้ปฏิบัติการด้านสารสนเทศนำมาใช้
- CobiT 4.1 ยังเป็น Framework ที่ยังไม่สมบูรณ์ในตัวเองซึ่งยังต้องอาศัย Framework อื่นมาประกอบในการนำมาใช้งาน เช่น Val IT Framework และ Risk IT Framework
- CobiT 4.1 ยังถูกนำไปใช้ได้ยาก เนื่องจากความยากในการทำความเข้าใจในตัว Framework เอง

<u>จุดบกพร่องของ IT Governance Implementation Guide 2nd Edition (ดูรูปที่ 12)</u>

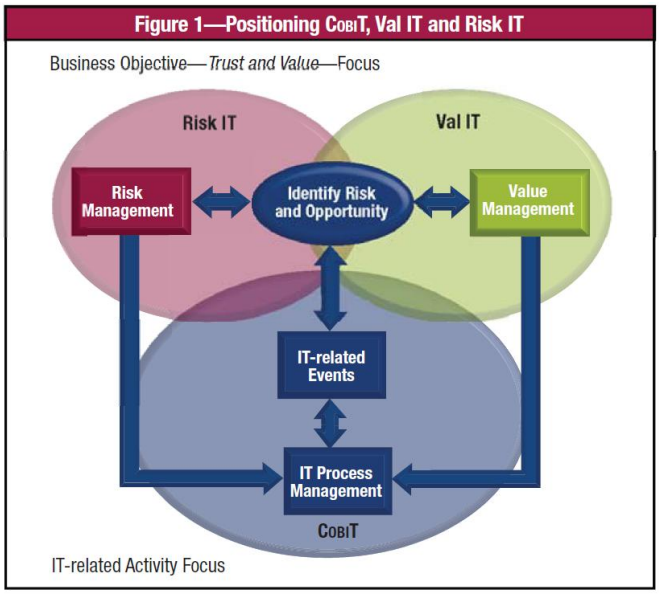
รูปที่ 12 : "IT Governance Implementation Guide 2nd Edition

การ Implement IT Governance ยังเป็นแนวคิดเดิมที่ยังไม่เป็น "Continual Improvement" ทำให้เกิดความเข้าใจผิดว่าเมื่อดำเนินการตามแต่ละขั้นตอนแล้ว เมื่อถึงขั้นตอนสุดท้ายก็แปลว่าจบและไม่ต้องทำต่อ ซึ่งผิดไปจากแนวทางที่ถูกต้องซึ่งจำเป็นต้องทำแบบต่อเนื่อง (Continual) เป็นกระบวนการพัฒนาแบบต่อเนื่อง (Iterative Process) ในลักษณะ "Life Cycle" (ดูรูปที่ 13) และ "IT Governance Implementation Guide 2nd Edition" ยังไม่ได้นำวิธีการของ Best Practice ใหม่ ๆ มาใช้ เช่น ITIL Version 3 ยกตัวอย่างเช่น เรื่อง "Change Enablement" และ "Continual Improvement Life Cycle"



รูปที่ 13 : "The New Life Cycle Model"

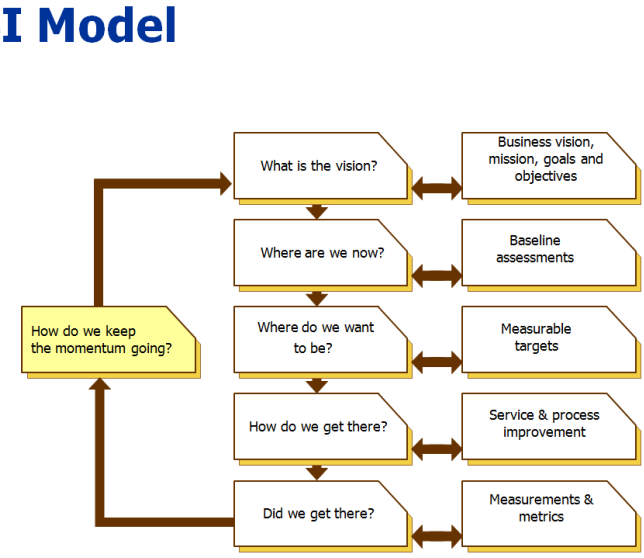
จากข้อบกพร่องดังกล่าว ISACA และ IT Governance Institute จึงมีแนวคิดในการยกเครื่อง CobiT 4.1 ใหม่แบบ "Major Change" เพื่อให้ CobiT เวอร์ชั่นใหม่นั้นครอบคลุมไปถึง "Enterprise Governance" และมีการรวมกันของ Framework ต่าง ๆ ไว้เป็นหนึ่งเดียวโดยจะมีการรวม Val IT Framework และ Risk IT Framework เข้ากับ CobiT 4.1 (ดูรูปที่ 14) เพื่อตอบโจทย์ทั้งมุม "Performance" และ "Conformance" โดยพิจารณา Business Model for Information Security (BMIS) Framework (ขณะที่เขียนต้นฉบับ ยังไม่ออก Final Version) และ A Professional Practices Framework for IT Assurance (ITAF) ร่วมด้วย และได้ให้ชื่อ Framework ใหม่ว่า "CobiT 5" สำหรับเอกสารประกอบอีกสองฉบับได้แก่ ITAF และ IT Governance Implementation Guide ได้มีแผนในการปรับปรุงใหม่ ซึ่งตัวเอกสาร IT Governance Implementation Guide 2nd Edition ได้มีการปัดฝุ่น ปรับปรุงใหม่แบบยกเครื่องเช่นกันและได้ออกมาให้ดาวน์โหลดแล้วในชื่อใหม่ที่เรียกว่า "Implementing and Continually Implementing IT Governance" (ดูรูปที่ 15)



รูปที่ 14 : Positioning CobiT, Val IT and Risk IT Framework

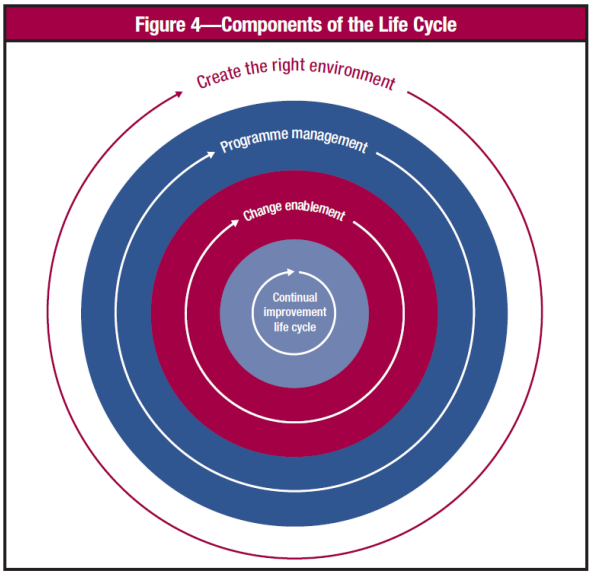
รูปที่ 15 : "Implementing and Continually Implementing IT Governance"

เอกสาร "Implementing and Continually Implementing IT Governance" ได้ถูกปรับปรุงโดยนำแนวความคิดของ ITIL V3 Continual Service Improvement (CSI) มาประยุกต์ใช้ในการ Implement IT Governance ในรูปแบบ "Life cycle Approach" โดยนำหลักการ CSI 6 Steps Model (ดูรูปที่ 16) มาประยุกต์โดยเพิ่มขั้นตอนมาอีกขั้นตอนหนึ่งคือ "What need to be done" (Step 4th) ระหว่าง "Where do we want to be" และ "How do we get there" จาก CSI 6 steps Model โดยใน CobiT 5 จะเน้นในเรื่อง Information Security และ Information Assurance ด้วย



รูปที่ 16 : CSI 6 Steps Model

กระบวนการที่ถูกปรับปรุงเพิ่มขึ้นทั้ง 7 ขั้นตอน มีความสมบูรณ์และพร้อมในการนำไปประยุกต์ใช้องค์กรมากขึ้นกว่าเดิม (ดูรูปที่ 17)

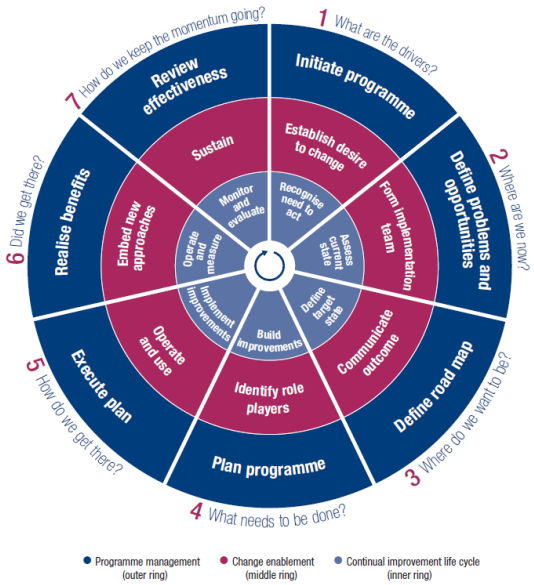


รูปที่ 17 : "4 Components of the life cycle"

เอกสาร "Implementing and Continually Implementing IT Governance" ประกอบด้วย 4 Components ได้แก่

1. Create the right environment
2. Programme Management หรือ Project Management
3. Change Enablement
4. Continual Improvement Life Cycle

ซึ่งรายละเอียดของกระบวนการทั้ง 7 ให้ดูรูปที่ 18



รูปที่ 18 : "Seven Phases of the Implementation Life Cycle"

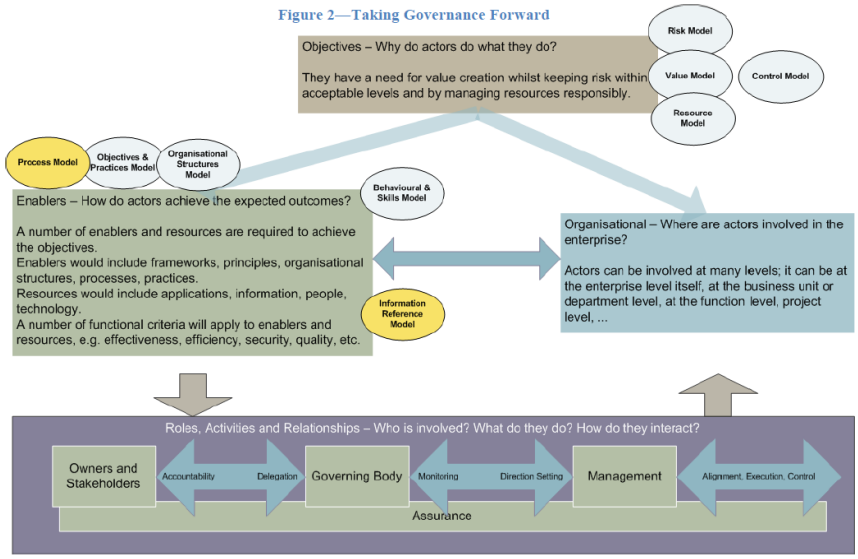
Inside CobiT 5 Design

ปรัชญาในการออกแบบ CobiT 5 นั้นนำมาจาก ISACA Initiative ที่เรียกว่า "TGF" ย่อมาจาก "Taking Governance Forward" ซึ่งตัว CobiT 5 มีวัตถุประสงค์ในการพัฒนาอยู่ 7 ข้อได้แก่

1. ความต้องการในการรวม Framework ต่าง ๆ ได้แก่ Val IT, Risk IT, BMIS และ ITAF เข้าด้วยกันในลักษณะเป็น Framework ใหญ่เพียงหนึ่งเดียว เพื่อไม่ให้เกิดความยุ่งยากสับสนในการใช้งาน Framework ต่าง ๆ
2. ต้องการให้หลักการและให้คำศัพท์ต่าง ๆ เกิดความชัดเจนไม่ซับซ้อน
3. ต้องง่ายในการ "Migrate" จาก CobiT 4.1
4. ต้องมีรายละเอียดเพื่อการค้นหาของผู้ใช้มากขึ้นกว่าใน CobiT 4.1
5. ต้องครอบคลุมเรื่อง Enterprise Architecture (EA) เรื่อง Decision Making เรื่อง People Skill เรื่อง Organization Structure เรื่อง Charge Enablement และ เรื่อง Sustainability
6. ต้องทำให้ชัดเจนในเรื่องของ "Governance Process" และ "Management Process"
7. ต้องง่ายในการ "ทำความเข้าใจ" "การนำมาใช้งาน " สอดคล้องกับ "Standard" และ "Best Practice"

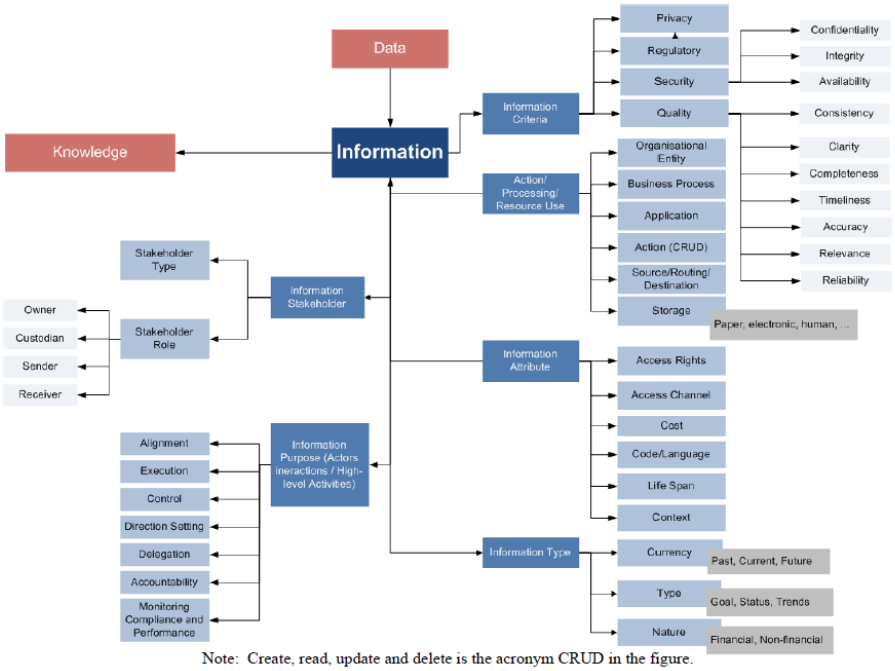
เป็นที่ชัดเจนแล้วว่า การปรับปรุงกระบวนการ “IT Governance” นั้นมีผลทำให้ภาพรวมของการปรับปรุง กระบวนการ “Enterprise Governance” ดีขึ้นด้วย และ การนำ Frameworks, Standards ตลอดจน “Best Practices” ต่าง ๆ มาใช้นั้น จะได้ผลก็ต่อเมื่อถูกนำมา “Adapt” และ “Adopt” อย่างถูกต้อง

CobiT 5 Framework นั้น เรียกได้ว่าเป็น “Enterprise Governance of IT Framework” โดยนำแนวคิด “TGF” (ดูรูปที่ 19) มาใช้ในการออกแบบและพัฒนา โดย CobiT 4.1 จะถูกออกแบบมาตามแนวคิด “Process Model” และเพื่อปรับปรุงในส่วนของ “Information Requirement” โดยใช้โมเดลที่เรียกว่า “Information Reference Model (IRM)” ซึ่งเป็นโมเดลที่เน้นเรื่องการบริหารจัดการกับ “Information” โดยเฉพาะ (ดูรูปที่ 20) โดย “Information” หรือ “สารสนเทศ” จะอยู่ตรงกลางระหว่าง “Data” หรือ ข้อมูล และ “Knowledge” หรือ องค์ความรู้ ซึ่ง “Information” จะถูกมองในมุมของ Information Criteria, Information Stakeholder, Information Purpose, Information Type, Information Attribute ต่างๆ ตลอดจนการนำ Information มาใช้ หรือ “Information Use” เรียกได้ว่าครบทั้ง Information Life Cycle ที่นิยมเรียกว่า “CRUD” (Create, Read, Update และ Delete)



รูปที่ 19 : “Taking Governance Forward” (TGF)

Figure 3—COBIT 5 Information Reference Model



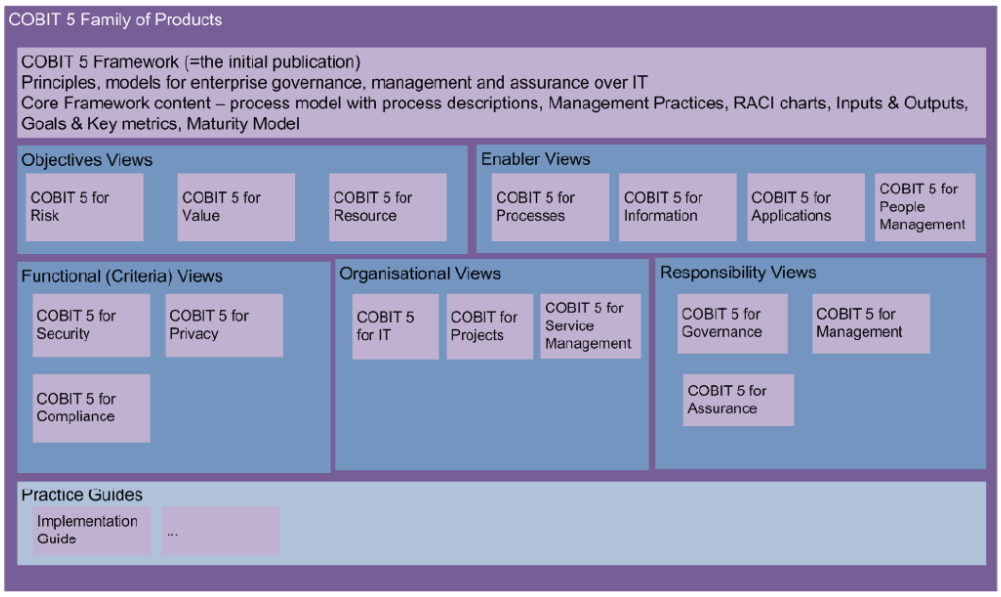
Note: Create, read, update and delete is the acronym CRUD in the figure.

รูปที่ 20 : "Information Reference Model (IRM)"

กลุ่มของผู้ที่มีส่วนเกี่ยวข้องกับการนำ CobiT 5.0 ไปใช้นั้นจะกว้างขึ้นกว่า CobiT 4.1 ทั้ง Internal Stakeholder และ External Stakeholder ทำให้ครอบคลุมผู้ใช้ในวงกว้างมากขึ้นกว่าเก่า

สถาปัตยกรรมของ CobiT 5 ถูกออกแบบให้เหมาะสมกับ Stakeholder ที่แตกต่างกัน ในรูปของ CobiT 5 Family of Products เช่น CobiT 5 for Risk, CobiT 5 for Value หรือ CobiT 5 for Security และ CobiT 5 for Compliance (ดูรูปที่ 22)

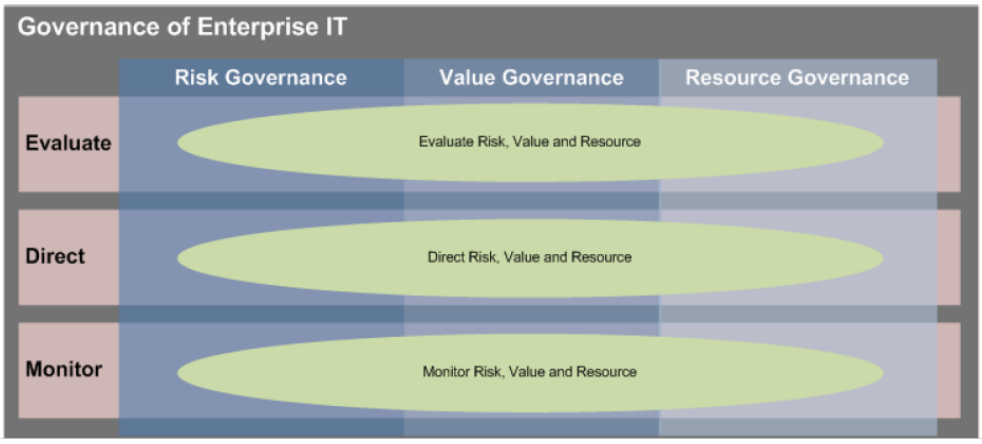
Figure 5—COBIT 5 Product Architecture



รูปที่ 22: “CobiT 5 Product Architecture”

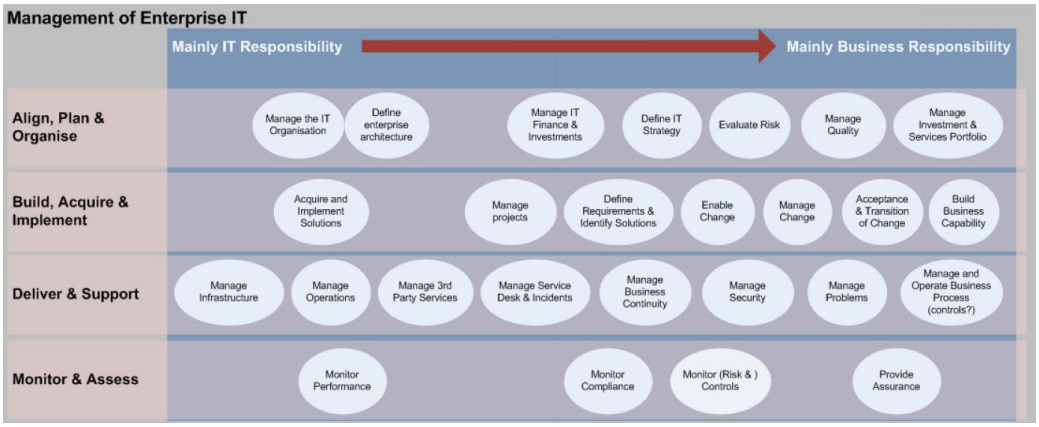
ใน CobiT 5 มีการปรับปรุงในส่วนของ “Process Model” โดยให้สอดคล้องกับมาตรฐาน ISO 38500:2008 “Corporate Governance of Information Technology” (ดูรูปที่ 22) โดยยึดหลัก 3 กระบวนการ ได้แก่ ประเมิน (Evaluate) กำกับ (Direct) และเฝ้าระวัง (Monitor) ซึ่งครอบคลุมใน 3 เรื่อง คือ “Risk Governance”, “Value Governance” และ “Resource Governance” (ดังรูปที่ 23)

Figure 6–COBIT 5 Process Model



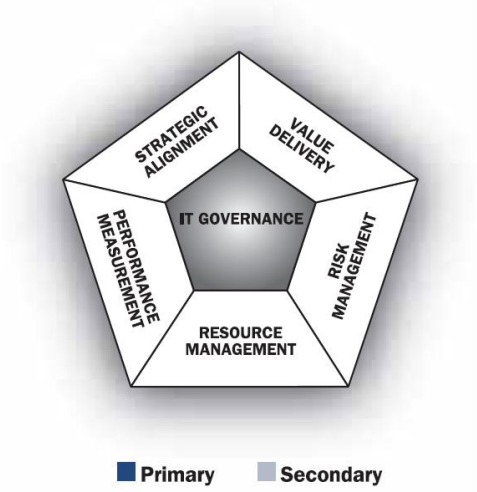
รูปที่ 23 : “Mapping process model with ISO/IEC 38500”

โดยมีการปรับปรุงจาก CobiT 4.1 ซึ่งประกอบด้วย 4 โดเมน ได้แก่ “Plan and Organize”, “Acquire and Implement”, “Deliver and Support” และ “Monitor and Evaluate” มาเป็น “**Align**, Plan and Organize”, “Build, Acquire & Implement”, “Deliver and Support” และ “Monitor & **Assess**” (ดูรูปที่ 24) อีกทั้งใน CobiT 5 ยังมีการนำ Standard และ Best Practice มาใช้อ้างอิงกว่า 60 แหล่ง ยกตัวอย่าง เช่น ITIL V3, ISO 27000 Series, ISO 20000, ISO 38500:2008, TOGAF V9 และ ISO 9000:2008



รูปที่ 24 : CobiT 5 New Design

การนำ CobiT 5 มาใช้ได้ผลดีนั้น ต้องคำนึงถึงวัฒนธรรมขององค์กรด้วย เพราะจะต้องเกิดการเปลี่ยนแปลง หรือ “Change” ทั้งด้าน วัฒนธรรม (Culture) และ พฤติกรรม (Behavior) ของคนในองค์กรอย่างหลีกเลี่ยงไม่ได้ โดย ISACA ได้คำนึงถึงปัญหาใหญ่ในเรื่องนี้จึงได้ทำการปรับแนวทางในการ Implement IT Governance มาเป็น Life Cycle ตามหลักการ CSI 6 Steps Model จาก ITIL V3 มาเป็นแนวทาง 7 Steps ดังที่กล่าวมาแล้วในตอนต้น



รูปที่ 25 : "IT Governance Focus Areas"

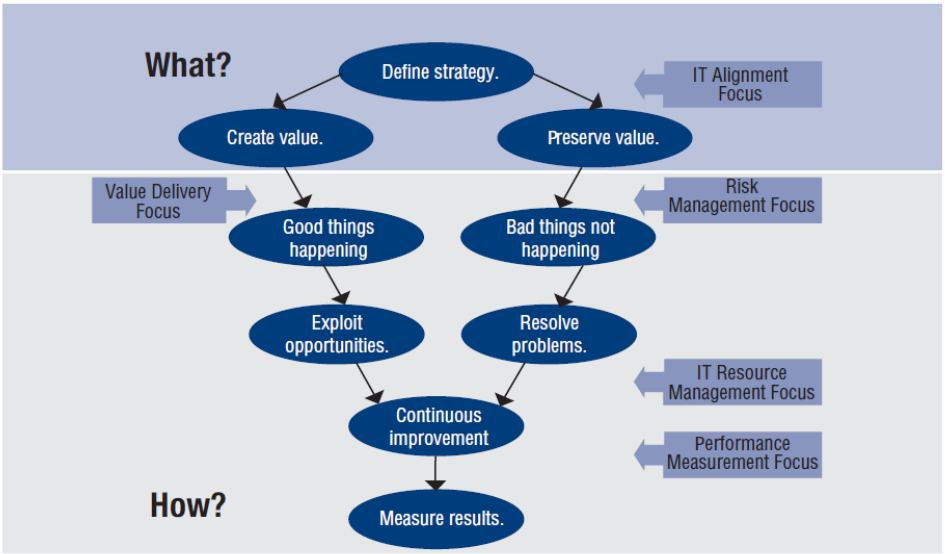
กิจกรรมตามแนวคิด "IT Governance" นั้นสามารถแบ่งได้เป็น 5 กลุ่ม (ดูรูปที่ 25) ได้แก่

1. Strategic Alignment

หมายถึง การทำให้กลยุทธ์ทางด้านการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรนั้น "สอดคล้อง" หรือ "Align" ไปในทิศทางเดียวกับกลยุทธ์ขององค์กร โดยแผนแม่บทด้านสารสนเทศควรสอดคล้องกับแผนแม่บทขององค์กร เพื่อให้การดำเนินการทางด้านสารสนเทศสอดคล้องกับเป้าหมายขององค์กร จะส่งผลให้องค์กรสามารถใช้ทรัพยากรต่าง ๆ ได้อย่างมีประสิทธิภาพ

2. Value Delivery หรือ Value Creation

หมายถึง การนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรต้องตอบโจทย์ความต้องการทางด้านธุรกิจขององค์กรให้ชัดเจนในมุมมองของ "ความคุ้มค่า" ที่สามารถรับรู้ได้โดยผู้ใช้ระบบสารสนเทศตลอดจน ผู้บริหารระดับสูงขององค์กรและลูกค้าที่มีส่วนเกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศเพื่อทำให้การให้บริการขององค์กรดีขึ้น เช่น ให้บริการได้เร็วขึ้น, ทำให้ลูกค้าเกิดความพึงพอใจมากขึ้นจากการที่องค์กรนำระบบสารสนเทศมาใช้ เรียกได้ว่า "เห็นประโยชน์" จากนำเทคโนโลยีสารสนเทศมาใช้อย่างชัดเจน เป็นรูปธรรม ตลอดจนอยู่ในเวลาและงบประมาณที่กำหนดไว้อีกด้วย (ดูรูปที่ 26)



รูปที่ 26 : Two Views of Control

3. Risk Management หรือ Value Preservation

ขณะที่ “Value Delivery” มุ่งเน้นไปที่การสร้างคุณค่า (Value Creation) แต่สำหรับ Risk Management หรือ การบริหารความเสี่ยงนั้น มุ่งเน้นไปที่กระบวนการรักษาคุณค่าหรือ (Value Preservation) โดยการบริหารความเสี่ยงควรเป็นกระบวนการที่กระทำอย่างต่อเนื่องตามหลักการด้านการบริหารความเสี่ยงแบบสากล ได้แก่ การประเมิน (Assess) การวิเคราะห์ (Analysis) และการตัดสินใจ(Treatment) ว่าจะยอมรับความเสี่ยง หรือ ไม่ยอมรับความเสี่ยงในลักษณะใด (Risk Reduction, Risk Retention, Risk Avoidance หรือ Risk Transfer) โดยอ้างอิงจาก Risk Acceptance Criteria (ISO 27005:2008)

โดยการบริหารจัดการความเสี่ยงที่ดีนั้นควรให้ผู้บริหารระดับสูงได้รับรู้ และ ตระหนัก (Risk Aware) ในผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น และ ได้ทำการกำหนดระดับความเสี่ยงที่ยอมรับได้ “Risk Appetite” หรือ Risk Acceptance Level” เพื่อนำไปใช้ในการประเมินความเสี่ยงซึ่งหน้าที่ในการกำหนดระดับความเสี่ยงดังกล่าวนี้จะเป็นใครไปเสียไม่ได้นอกจาก “ผู้บริหารระดับสูง” ที่ต้องรับผิดชอบในเรื่องนี้ เพื่อให้สอดคล้องกับแนวทาง IT Governance และแนวคิด Governance, Risk Management and Compliance (GRC)

เนื่องจากการนำสารสนเทศมาใช้ทำให้เกิดความเสี่ยงที่เรียกว่า “IT Risk” ซึ่งส่งผลโดยตรงต่อการดำเนินงานขององค์กร ทำให้เกิด “Business Risk” หรือความเสี่ยงในเชิงธุรกิจขององค์กร จากการนำเทคโนโลยีสารสนเทศมาใช้อย่างไม่ปลอดภัย และไม่รัดกุมพอ เรียกได้ว่า “IT Risk ก็คือ “Business Risk” ดี ๆ นี่เอง”

4. Performance Management

การวัดประสิทธิภาพและประสิทธิผล ของกระบวนการด้านการบริหารจัดการเทคโนโลยีสารสนเทศนั้น กำลังเป็นประเด็นร้อนที่มีการกล่าวถึงอย่างมากทั่วโลกในขณะนี้ เรื่องของ “IT KPI” “IT Metric” ตลอดจน “IT Performance Management” ต่าง ๆ กำลังเป็นที่เรื่องที่ผู้บริหารระบบสารสนเทศต้องนำมาใช้ในการประเมินการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ ดังนั้นจึงมีความจำเป็นที่ผู้บริหารระบบสารสนเทศต้องกำหนด “ค่าชี้วัด” หรือ “Metric” ในการประเมินที่ได้รับการยอมรับโดยผู้เกี่ยวข้อง หรือ Stakeholder ซึ่งอาจวัดในรูปของ Performance Scorecard, Dashboard หรือ Benchmarking

ความสำคัญของการวัด หรือ “Measurement” นั้น ส่งผลต่อความสามารถในการบริหารจัดการหรือ “Manage” ดังคำกล่าวที่ว่า **“If you cannot measure it, you cannot manage it”** ดังนั้นการวัดประสิทธิผลและวัดประสิทธิภาพนั้นจึงเป็นกระบวนการที่มีความสำคัญอย่างมากซึ่งจะถูกมองข้ามเสียไม่ได้ ผู้ตรวจสอบจาก Certification Body (CB) เวลามาตรวจสอบองค์กรตามมาตรฐาน ISO/IEC 27001 จะเน้นเรื่องการวัดประสิทธิผล (Effectiveness) ของกระบวนการด้านการบริหารจัดการความปลอดภัยสารสนเทศ โดยถ้ามีการปฏิบัติตามกระบวนการตามหลัก ISMS แล้วแต่ไม่มีการประเมินผลก็ถือว่า ยังไม่ตรงตามหลักการของ ISO/IEC 27001

5. Resource Management

หมายถึง การบริหารจัดการทรัพยากรต่าง ๆ ทั้ง 4 กลุ่มได้แก่

1. บุคลากร (People)
2. โครงสร้างพื้นฐาน (Infrastructure)
3. โปรแกรมประยุกต์ (Application)
4. สารสนเทศ (Information)

เป็นการนำทรัพยากรมาใช้อย่างมีประสิทธิภาพ เพียงพอกับความต้องการและคุ้มค่าการลงทุน โดยการบริหารทรัพยากรบุคคล หรือ “Human Resource Management” นั้นเป็นเรื่องสำคัญเพราะบุคลากรถือเป็นทรัพยากรที่สำคัญที่สุดขององค์กรจึงต้องมีการฝึกอบรมให้ความรู้ตลอดจนมีการพัฒนาบุคลากรให้มีความรู้ความสามารถเป็น “Knowledge Worker” ที่สามารถปฏิบัติต่าง ๆ ขององค์กรได้ตามเป้าหมายที่กำหนดไว้ในแผนกลยุทธ์ทางด้านสารสนเทศและแผนกลยุทธธุรกิจในภาพรวมขององค์กรในที่สุด

บทสรุปของการนำ CobiT Framework และ IT Governance Implementation Guide มาใช้นั้นสรุปความได้ว่า ทั้ง CobiT และ IT Governance Implementation Guide นั้นไม่ใช่ “Solution” แต่เป็น “Method” ดังคำกล่าวของ “Luc Kordel” ที่ว่า “It’s a method, not the solution!” ดังนั้นองค์กรต้องนำ Framework มา “Adopt” และ “Adapt” ปรับให้เข้ากับ Corporate Culture, Style และ People Skill