การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 2 : IT Security Governance

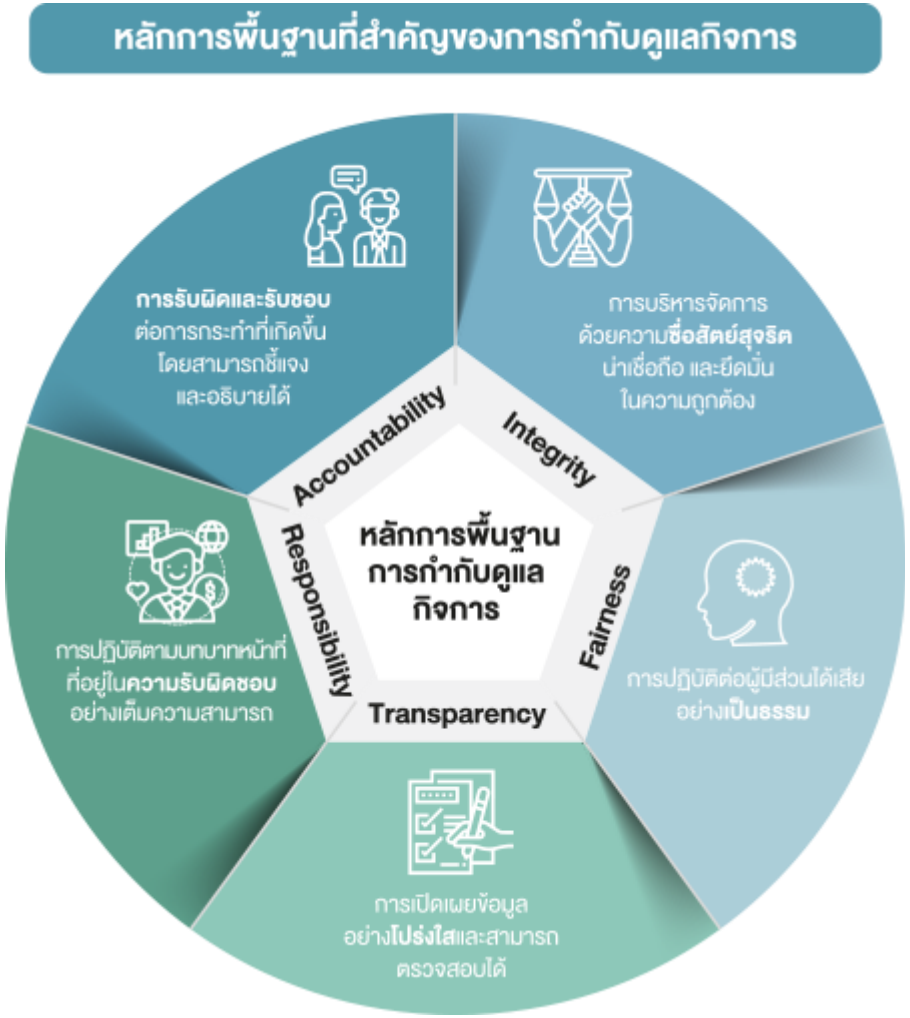
เนื้อหา

- บรรษัทภิบาล (Corporate Governance)
- ไอทีภิบาล (IT Governance)
- มาตราฐานไอทีภิบาล
- นโยบายด้านการรักษาความปลอดภัยข้อมูล (Information Security Policy)
- การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)
- การตรวจสอบ (Audit)

บรรษัทภิบาล (Corporate Governance)

บรรษัทภิบาล หรือการกำกับดูแลกิจการ คือ การบริหารจัดการบริษัทที่มีประสิทธิภาพ โปร่งใส ตรวจสอบได้ และคำนึงถึงผู้มีส่วนได้เสียทุกฝ่าย

ภาครัฐจะใช้คำว่า ธรรมาภิบาล หมายถึง การบริหารของภาครัฐที่มุ่งเน้นความดีงาม และเกิดประโยชน์สูดสุดแก่รัฐและประชาชน



บรรษัทภิบาล (Corporate Governance)

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Cooperation and Development, OECD) พัฒนาหลักบรรษัทภิบาลโดยมีพื้นฐานจากกฎหมายและหลักทางจริยธรรมของชาติตะวันตก โดยจะกล่าวถึงใน 3 ประเด็น คือ

(1) เรื่องการเปิดเผยข้อมูลที่เหมาะสม

(2) ความรับผิดชอบของคณะกรรมการบริหาร

(3) ความเป็นอิสระของผู้บริหาร

หลักบรรษัทภิบาล ตาม OECD

เรื่องการเปิดเผยข้อมูลที่เหมาะสม

การเปิดเผยข้อมูลที่เหมาะสมและโปร่งใสมีผลต่อพฤติกรรมของบริษัท การคุ้มครองผู้ลงทุน และการดึงดูดเงินลงทุน นอกจากนี้ ยังเป็นการรักษาความเชื่อมั่นของบริษัท การเปิดเผยข้อมูลบริษัทที่เหมาะสมโดยคำนึงถึงปัจจัยแวดล้อมของตลาดและมาตรฐานทางจริยธรรมจะช่วยให้สาธารณชนเข้าใจโครงสร้างและการดำเนินการของบริษัทได้ดียิ่งขึ้น

ซึ่งภาครัฐก็มีความพยายามเปิดเผยข้อมูลอย่างเหมาะสมเช่นกัน ในโครงการ Opendata ที่ลิงค์ https://data.go.th

หลักบรรษัทภิบาล ตาม OECD

ความรับผิดชอบของคณะกรรมการบริหาร

คณะกรรมการบริหารของบริษัท (The board of director) คือ ศูนย์กลางของบริษัท และคำสั่งในการบริหารงานของคณะกรรมการบริหารบริษัทถือเป็นที่สุด คณะกรรมการบริหารมีความรับผิดชอบอย่างสูงในการควบคุมดูแลการบริหาร คณะกรรมการบริษัทจะต้องมีประสิทธิภาพในการกำกับดูแลการบริหารงานภายในบริษัท

หลักบรรษัทภิบาล ตาม OECD

ความเป็นอิสระของผู้บริหาร

ความเป็นอิสระที่เพียงพอในการปฏิบัติหน้าที่ของกรรมการบริษัทตามกฎหมายเป็นสิ่งสำคัญ ทั้งนี้ ความเป็นอิสระถือเป็นสิ่งสำคัญสูงสุดที่จะประกันว่ากรรมการบริษัทจะสามารถปฏิบัติตามวัตถุประสงค์ได้อย่างเต็มที่ เสียงส่วนใหญ่ของกรรมการเปรียบเสมือนมติของคณะกรรมการซึ่งต้องอยู่บนพื้นฐานของความเป็นอิสระในการใช้สิทธิออกเสียงของกรรมการแต่ละคน

ไอทีภิบาล (IT Governance)

ไอทีภิบาล (IT Governance) หมายถึง การกำกับดูแลเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กร โดยผู้บริหารทุกภาคส่วนมีบทบาทหน้าที่ในการตัดสินใจ และมีส่วนร่วมกำหนดกระบวนการของกิจกรรม/โครงการที่เกี่ยวข้อง ไอทีภิบาลแบ่งออกเป็น 5 ด้านสำคัญ คือ

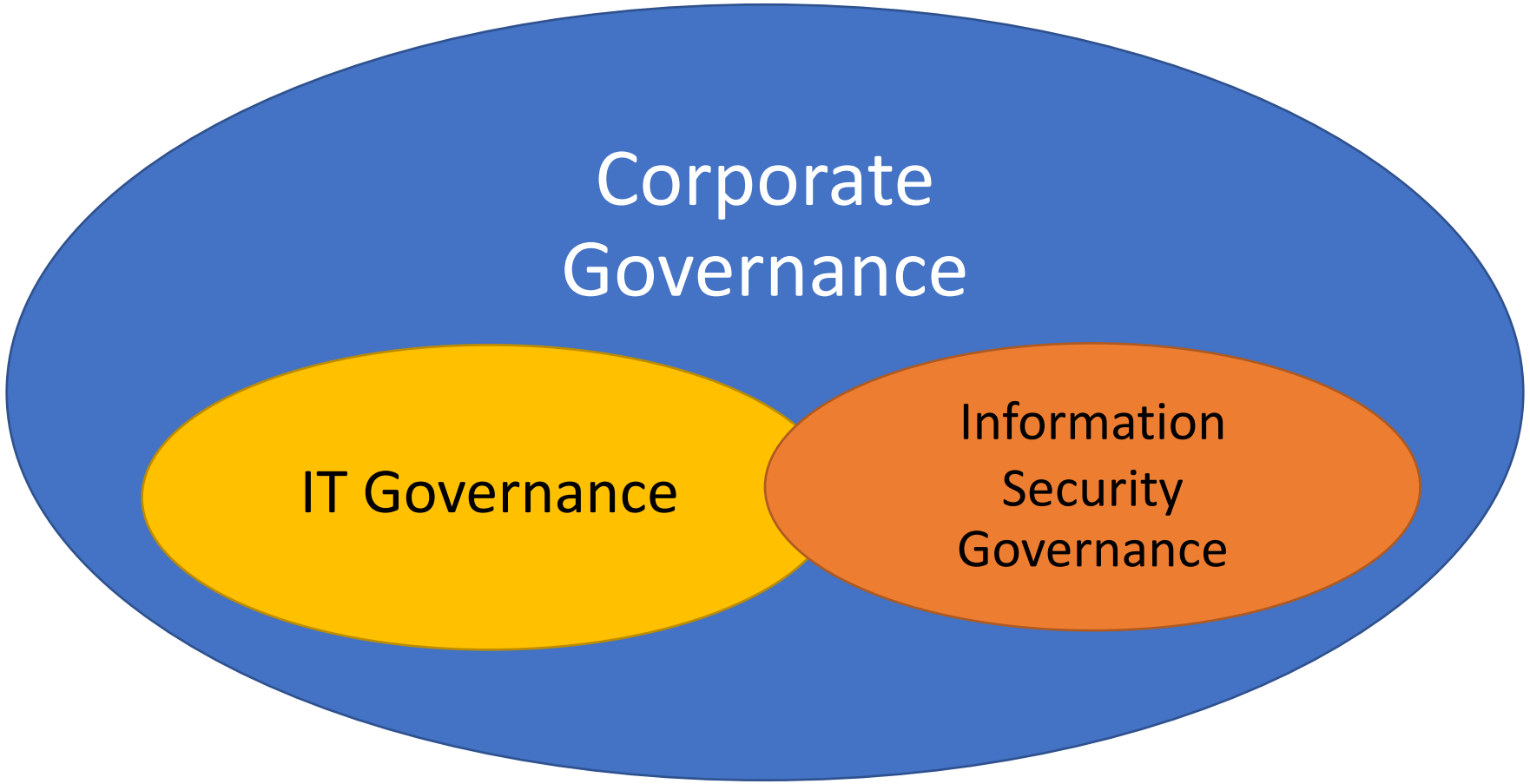
- สอดคล้องกับยุทธศาสตร์ (Strategic Alignment)
- การเพิ่มมูลค่า (Value Delivery)
- การบริหารความเสี่ยง (Risk Management)
- การบริหารทรัพยากร (Resource Management)
- การวัดประสิทธิภาพ (Performance Measurement)

ความสำคัญ IT Governance

1. ความจำเป็นที่ต่องมีการควบคุมการจัดการและการใช้เทคโนโลยีสารสนเทศ เพื่อการบรรลุกลยุทธ์และเป้าหมายขององค์กร

2. ความจำเป็นของการควบคุมและกำกับทางด้านเทคโนโลยีสารสนเทศ ตามกฎหมายที่ยอมรับในระดับสากลกับบริษัทในตลาดหลักทรัพย์ องค์กรต่างๆ จำเป็นต้องให้ความสำคัญกับการควบคุมและการประมวลข้อมูลโดยมีการระบุในกฎหมาย

การอภิบาลรักษาความปลอดภัยข้อมูล (Information Security Governance)



การอภิบาลรักษาความปลอดภัยข้อมูล (Information Security Governance)

ในปัจจุบันมีแนวโน้มการจ้างบริการหรือเอาต์ซอร์ส (Outsource) และคลาวด์คอมพิวติ้ง (Cloud Computing) ทำให้ขอบเขตของการรักษาความปลอดภัยไม่ได้อยู่เฉพาะในองค์กรเท่านั้น หรืออยู่เฉพาะภายในประเทศ ทำให้การบริหารความปลอดภัยข้อมูลต้องปรับเปลี่ยนไปด้วย

มาตรฐานไอทีภิบาล

COBIT®
An ISACA Framework

ITIL®
Foundation V3

ISO
IEC

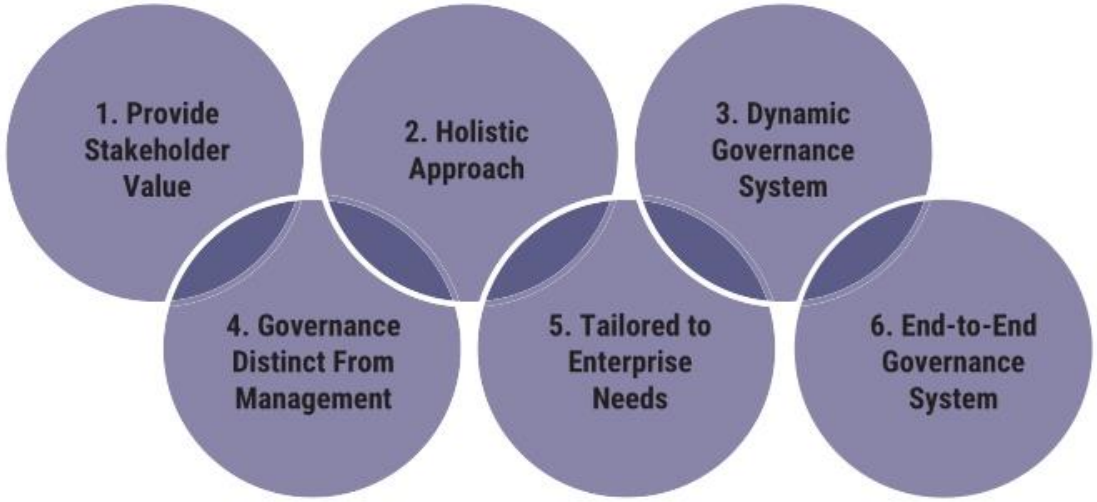
COSO

มาตราฐาน COBIT

Control Objectives for Information and Related Technology (COBIT) กำหนดขึ้นโดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ หรือ ISACA (Information Systems Audit and Control Association) มีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตุประสงค์เชิงธุรกิจขององค์กร

โดยในปัจจุบัน คือ COBIT 2019

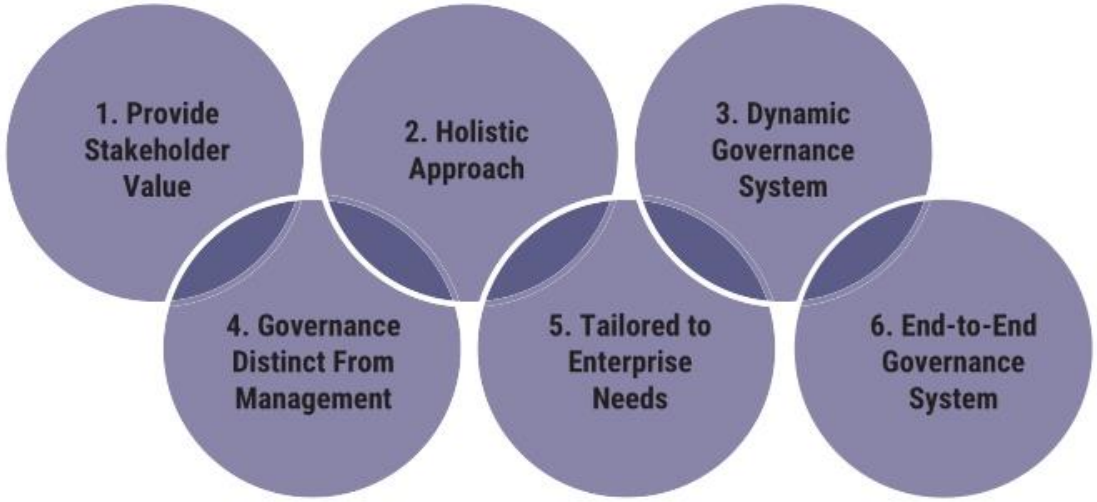
มาตราฐาน COBIT



COBIT 2019 ตั้งอยู่บนหลักการพื้นฐาน 6 ข้อ ได้แก่

1. เป็นหลักการที่ตอบสนองต่อความต้องการของผู้ที่เกี่ยวข้องและก่อให้เกิดคุณค่าจากการนำเทคโนโลยีสารสนเทศมาใช้งาน
2. เป็นหลักการที่นำองค์ประกอบที่สำคัญ 7 องค์ประกอบมาทำงานร่วมกันอย่างสอดประสานกันเป็นหนึ่งเดียว

มาตราฐาน COBIT



COBIT 2019 ตั้งอยู่บนหลักการพื้นฐาน 6 ข้อ ได้แก่

3. ระบบในการกำกับดูแลควรจะสามารถเปลี่ยนแปลงไปตามปัจจัยที่ส่งผลต่อการเปลี่ยนแปลงได้เสมอ

4. เป็นหลักการที่แยกการกำกับดูแลโดย Board หรือหน่วยงานภายนอกออกจากฝ่ายงานต่าง ๆ ภายในองค์กร ทั้งนี้เพื่อให้เกิดความโปร่งใสในการกำกับดูแล

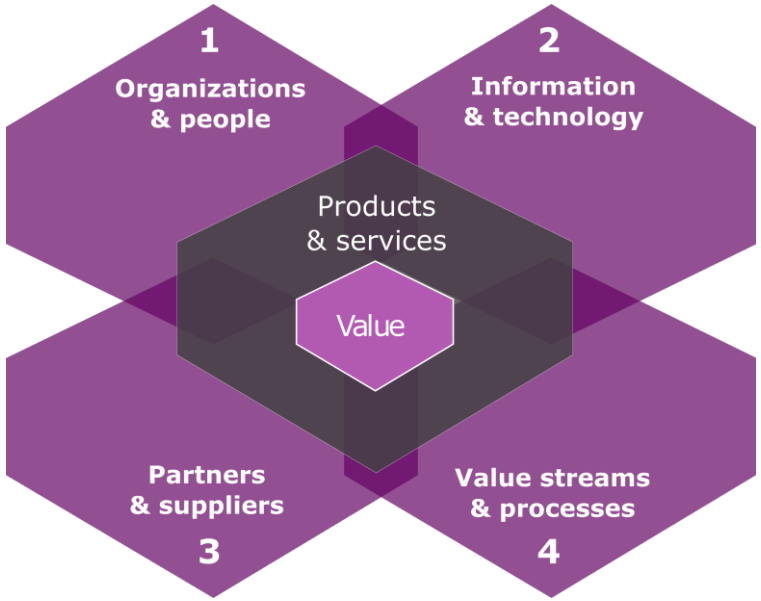
5. เป็นหลักการที่เกี่ยวข้องกับการปรับใช้งานระบบการกำกับดูแลให้เป็นไปตามความต้องการของผู้ที่เกี่ยวข้อง

6. เป็นหลักการของการกำกับดูแลที่ครอบคลุมการดำเนินงานด้านเทคโนโลยีสารสนเทศทั่วทั้งองค์กร

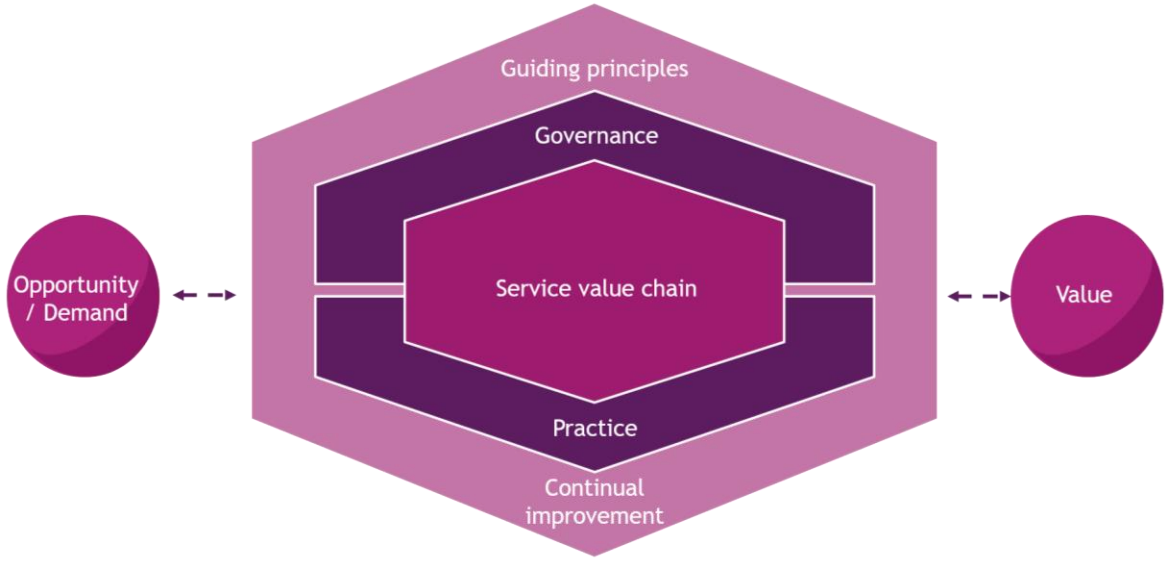
มาตราฐาน ITIL

The Information Technology Infrastructure Library (ITIL) กำหนดขึ้นในประเทศอังกฤษเป็นครั้งแรก โดยความร่วมมือระหว่างภาครัฐและภาคเอกชน

โดยในปัจจุบัน คือ ITIL 4 มีองค์ประกอบหลัก 2 ส่วน คือ



1. Four dimension model

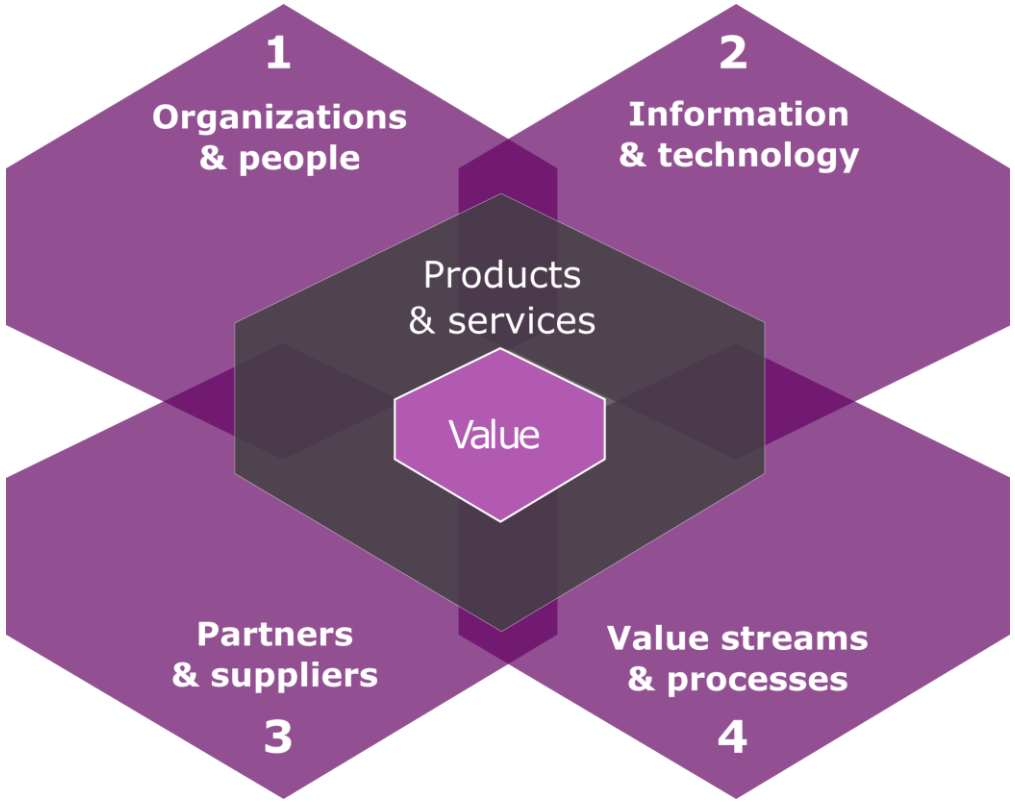


2. ITIL service value system (SVS)

มาตราฐาน ITIL: Four Dimension Model

มองในมุมธุรกิจ และองค์กรทั้ง 4 ด้าน ดังนี้

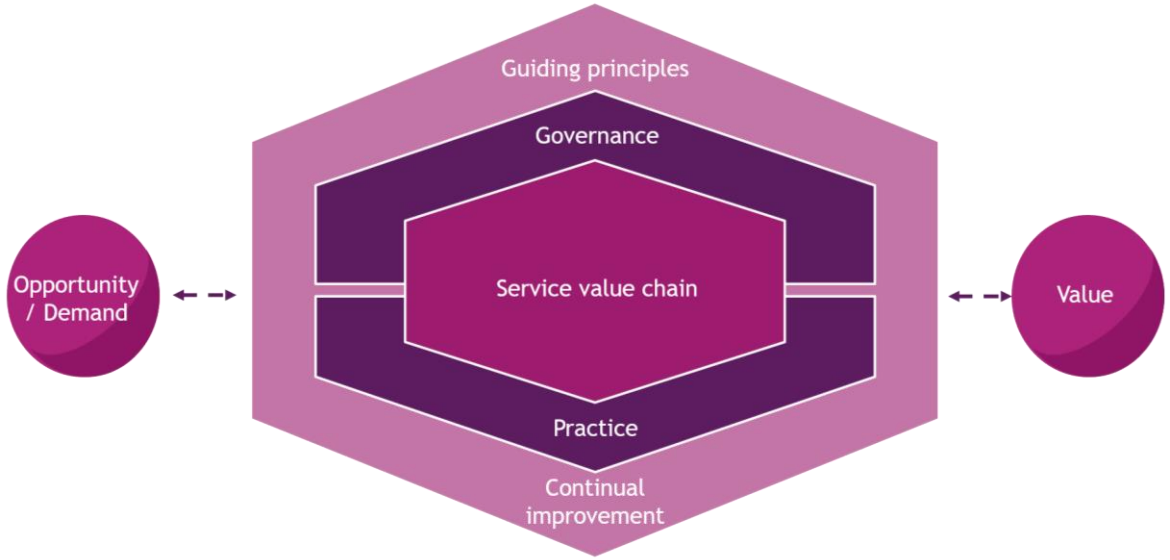
1. องค์กร และคน (Organizations & people)
2. ข้อมูล และเทคโนโลยีที่ใช้สนับสนุนภายในองค์กร (Information & technology)
3. คู่ค้าร่วม และผู้ผลิต (Partners & suppliers)
4. สายน้ำแห่งคุณค่า และกระบวนการทำงาน (Value stream & process)



มาตราฐาน ITIL: ITIL Service Value System (SVS)

องค์ประกอบ และกิจกรรมทั้งหมดขององค์กร ที่ต้องทำงานร่วมกัน เพื่อให้สามารถสร้างคุณค่าได้อย่างไร ประกอบไปด้วย 5 ส่วนดังนี้

1. แนวทางหรือหลักการ (Guiding principles)
2. การบริหารจัดการในองค์กรที่มีรูปแบบชัดเจน, มีตัวชี้วัด หรือวัดผลได้ (Governance)
3. ห่วงโซ่คุณค่าการบริการ (SVC)
4. หลักการและแนวปฏิบัติ
5. ปรับปรุงอย่างต่อเนื่อง



มาตราฐาน ISO/IEC 27001

กำหนดขึ้นโดยสถาบันมาตรฐานนานาชาติ ISO (International Organization for Standardization) และ IEC (The International Electrotechnical Commission) เป็นชุดมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศ

ISO/IEC 27001 เป็นระบบการจัดการความปลอดภัยของข้ำมูลในทั้ง 3 ด้าน คือ

1. **ความลับ** : เพื่อให้แน่ใจว่าข้อมูลต่างๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
2. **ความถูกต้อง** : เพื่อปกป้องให้ข้อมูลมีความถูกต้องและความสมบูรณ์ และแก้ไขได้เฉพาะผู้มีสิทธิ์เท่านั้น
3. **ความพร้อมใช้งาน** : เพื่อแน่ใจว่าผู้มีสิทธิ์ในการเข้าถึงข้อมูล สามารถเข้าถึงได้เมื่อต้องการ

มาตราฐาน ISO/IEC 27001

วัตถุประสงค์และมาตรการควบคุม ประกอบด้วย

Code	Detail
A.5	นโยบายการรักษาความปลอดภัยข้อมูล (Information Security Policy)
A.6	การจัดโครงสร้างของการรักษาความปลอดภัย (Organization of Information Security)
A.7	การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human Resource Security)
A.8	การบริหารทรัพย์สิน (Asset Management)
A.9	การควบคุมการเข้าถึง (Access Controls)
A.10	การเข้ารหัสข้อมูล (Cryptography)
A.11	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

มาตราฐาน ISO/IEC 27001

วัตถุประสงค์และมาตรการควบคุม ประกอบด้วย

Code	Detail
A.12	การรักษาความปลอดภัยในการปฏิบัติงาน (Operation Security)
A.13	การรักษาความปลอดภัยการสื่อสาร (Communications Security)
A.14	การจัดหา พัฒนาและบำรุงรักษาระบบ (System acquisition, development and maintenance)
A.15	ความสัมพันธ์กับซัพพลายเออร์ (Supplier Relationships)
A.16	การจัดการเหตุการณ์ด้านความปลอดภัยข้อมูล (Information security incident management)

มาตราฐาน ISO/IEC 27001

วัตถุประสงค์และมาตรการควบคุม ประกอบด้วย

Code	Detail
A.17	มิติด้านการรักษาความปลอดภัยในการบริหารความต่อเนื่องของธุรกิจ (Information security aspects of business continuity management)
A.18	การปฏิบัติตามระเบียบ (Compliance)

มาตราฐาน COSO

COSO (Committee of Sponsoring Organizations) เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กรอย่างเป็นระบบ ซึ่งออกแบบเพื่อให้เกิดความเชื่อมั่นในการบรรลุวัตถุประสงค์ในเรื่องดังต่อไปนี้

1. ความมีประสิทธิภาพและประสิทธิผลของการดำเนินงาน
2. ความเชื่อถือได้ของข้อมูลและรายงานทางการเงิน
3. การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ

นโยบายด้านการรักษาความปลอดภัยข้อมูล (Information Security Policy)

นโยบาย หมายถึง เอกสารที่กำหนดทิศทางการบริหารงานหรือกรอบแนวปฏิบัติ โดยเป็นสิ่งที่ต้องปฏิบัติตามในทางการรักษาข้อมูล

ถ้าองค์กรยังไม่มีนโยบายใดๆ เลย เราจะเลือกที่กำหนดนโยบายใดก่อน คำตอบคือขึ้นอยู่กับความเสี่ยงขององค์กรในขณะนั้น ถ้าข้อมูลเป็นสิ่งจำเป็น ก็ควรเริ่มพัฒนานโยบายข้อมูลก่อน

แนวทางการจัดทำนโยบายที่สำคัญ

1. ต้องจัดทำนโยบายเป็นลายลักษณ์อักษร โดยผู้บริหาร เจ้าหน้าที่ฝ่ายไอที และผู้ใช้งานทั่วไปต้องมีส่วนร่วมในการจัดทำ
2. ต้องทบทวนและปรับปรุงให้เป็นปัจจุบันเสมอ โดยมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง
3. ต้องระบุวัตถุประสงค์และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุม
4. ต้องประกาศใช้และสื่อสารนโยบายแก่ผู้ที่เกี่ยวข้องอย่างทั่วถึง
5. ต้องมีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด
6. ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่กำหนดไว้

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)

ในการฝึกอบรมให้กับพนักงาน จำเป็นต้องมีเจ้าหน้าที่ถนัดทางด้านนี้ อย่างน้อยที่สุดเจ้าหน้าที่รักษาความปลอดภัยก็ควรต้องเข้ามามีส่วนร่วมในการฝึกอบรม

องค์กรไม่สามารถป้องกันข้อมูลที่สำคัญได้ โดยปราศจากความร่วมมือจากพนักงานทุกคน จึงมีความจำเป็นต้องมีการอบรมกับทุกคนที่อยู่ภายในองค์กร

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)

มุมผู้บริหาร

ถ้าผู้บริหารไม่สนับสนุน ก็จะไม่มีระบบการรักษาความปลอดภัยในองค์กร ดังนั้น ผู้บริหารควรได้รับรายงานสถานภาพและความก้าวหน้าเกี่ยวกับความปลอดภัย ในรายงานควรมีตัวเลขทางสถิติด้วย เช่น

จำนวนช่องโหว่ของแต่ละระบบ

จำนวนครั้งที่มีการฝ่าฝืนนโยบาย

จำนวนความพยายามในการเจาะเข้าระบบ

เพื่อเป็นการเตือนให้ทราบถึงความรับผิดชอบที่มีต่อองค์กร

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)

มุมพนักงานทั่วไป

พนักงานทั่วไปจะต้องฝึกอบรมเพื่อทำความเข้าใจ และทราบว่าการรักษาความปลอดภัยมีความสำคัญอย่างไร การฝึกอบรมนั้นจะช่วยให้พนักงานรับทราบข้อมูลที่ควรทราบ รู้จักจัดการกับรหัสผ่าน และช่วยป้องกันการโดนหลอกจากการโจมตีแบบวิศวกรรมสังคม

การฝึกอบรมนั้นควรเป็นแบบสั้นๆ ใช้เวลาประมาณ 1-2 ชั่วโมง พนักงานใหม่ควรฝึกอบรมนี้กำหนดในส่วนของปฐมนิเทศ ส่วนพนักงานเก่าควรได้รับการฝึกอบรมอย่างน้อย 2 ปี/ครั้ง

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)

มุมผู้ดูแลระบบ

การฝึกอบรมนั้นเป็นสิ่งสำคัญและจำเป็นสำหรับผู้ดูแลระบบ ผู้ดูแลระบบควรปรับความรู้ให้ทันสมัยอยู่เสมอ เช่น เทคนิคการเจาะระบบแบบต่างๆ ภัยที่อาจเกิดขึ้นได้ และการติดตั้งแพตช์เพื่อป้องกันการโจมตีใหม่ๆ

การฝึกอบรมควรจัดให้มีบ่อยๆ ประมาณเดือนละ 1 ครั้ง และควรเชิญผู้เชี่ยวชาญทางด้านนนี้มาฝึกอบรมประเภทนี้

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Security Awareness Training)

มุมนักพัฒนาแอพพลิเคชัน

การฝึกอบรมสำหรับนักพัฒนา ควรเป็นส่วนที่เพิ่มจากการอบรมพนักงานทั่วไป โดยส่วนที่เพิ่มเติมเข้ามาควรเป็นเรื่องเกี่ยวกับเทคนิคการเขียนโปรแกรมอย่างไรให้ปลอดภัย

การตรวจสอบ (Audit)

การตรวจสอบ เป็นขั้นตอนสุดท้ายของกระบวนการรักษาความปลอดภัย หลังจากดำเนินการตามขั้นตอนต่างๆมาแล้ว ท้ายสุดคือ การตรวจสอบว่าได้มีการดำเนินการตามนโยบายและระเบียบปฏิบัติหรือไม่ โดยจะมีการตรวจสอบเกี่ยวกับความปลอดภัย มักจะตรวจสอบ 3 ประเภท ดังนี้

การตรวจสอบ (Audit)

1. การตรวจสอบการปฏิบัติตามนโยบาย
2. การประเมินโครงการใหม่ๆ
3. การทดลองเจาะระบบ (Penetration Test)