แนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยี
สารสนเทศระดับองค์กรที่ดี (IT Governance Practice)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

พฤศจิกายน 2562

สารบัญ

1. **หลักการและเหตุผล** 1

1.1 วัตถุประสงค์ 2

1.2 การจัดทำแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีของ ก.ล.ต. 2

1.3 บทนิยาม 4

2. **บทบาทหน้าที่ โครงสร้างองค์กร และการบริหารจัดการบุคลากรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี** 5

2.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ 5

2.2 โครงสร้างการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี 5

2.3 การบริหารจัดการบุคลากร 6

3. **แนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี** 8

3.1 การกำหนดกรอบการกำกับดูแลและบริหารจัดการ (Governance Framework Setting and Maintenance) 8

3.2 การจัดการความเสี่ยงที่เหมาะสม (Risk Optimization) 10

3.3 การส่งมอบผลประโยชน์ (Benefit Delivery) และการใช้ทรัพยากรสารสนเทศให้ได้ประโยชน์สูงสุด (Resource Optimization) 14

3.4 ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency) 16

ภาคผนวก ตัวอย่างดัชนีวัดผลที่สำคัญที่เกี่ยวข้องกับแผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศหรือแผนทางด้านเทคโนโลยีสารสนเทศ และงบประมาณทางด้านเทคโนโลยีสารสนเทศ 17

1. หลักการและเหตุผล

เนื่องด้วยระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ และถือเป็นหนึ่งในระบบงานหลักที่หากมีเหตุขัดข้องหรือสถานการณ์ฉุกเฉินเกิดขึ้น จะส่งผลกระทบต่อการดำเนินงานของผู้ประกอบธุรกิจ ผู้ลงทุน และความเชื่อมั่นต่อตลาดทุนโดยรวมได้ ผู้บริหารระดับสูงจึงมีบทบาทสำคัญในการบริหารจัดการในการนำเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจ รวมถึงมีหน้าที่ในการส่งทอดเป้าหมายทางธุรกิจตามภารกิจ กลยุทธ์ นโยบาย และแผนงานระดับองค์กร ไปสู่เป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอยู่ภายใต้การกำกับดูแลของคณะกรรมการบริษัท เพื่อทำให้มั่นใจได้ว่าการนำเทคโนโลยีสารสนเทศดังกล่าวมาใช้ในการประกอบธุรกิจ จะช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุเป้าหมายได้ตามที่กำหนดไว้โดยมีการใช้ทรัพยากรอย่างเหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม ให้สอดคล้องกับการกำกับดูลกิจการที่ดี (Corporate Governance)

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี หมายถึง การจัดการโครงสร้างองค์กรและสาธารณูปโภคพื้นฐานทางด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนกลยุทธ์และเป้าหมายขององค์กร รวมทั้งสนับสนุนการดำเนินงานทางด้านสารสนเทศอย่างมีประสิทธิภาพและประสิทธิผล โดยเป็นที่ยอมรับในระดับสากลว่าการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี เป็นกระบวนการที่สำคัญที่ช่วยผู้ประกอบธุรกิจในเรื่อง

- การจัดสรรทรัพยากรสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล สอดคล้องกับเป้าหมาย พันธกิจ และวัตถุประสงค์ขององค์กร
- การบริหารความเสี่ยงในกิจกรรมด้านเทคโนโลยีสารสนเทศ ในด้านของผลตอบแทนเปรียบเทียบกับความเสี่ยงและการจัดการกับความเสี่ยงอย่างเหมาะสม
- การสร้างความมั่นใจถึงคุณภาพของเทคโนโลยีสารสนเทศเพื่อใช้ในการตัดสินใจในทุกระดับ ทั้งการตัดสินใจในเชิงกลยุทธ์ ไปจนถึงการตัดสินใจเพื่อบริหารจัดการในการดำเนินธุรกิจ
- การสร้างความมั่นใจในความน่าเชื่อถือของระบบสารสนเทศ
- การพิจารณาความคุ้มค่าของต้นทุนของการให้บริการ และผลตอบแทนที่ได้รับอย่างมีประสิทธิภาพและมีประสิทธิผล
- ความมั่นใจในการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ หรือมาตรฐานอุตสาหกรรมที่เกี่ยวข้อง

การจัดทำแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี เป็นส่วนหนึ่งของนโยบายสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน”) ที่ต้องการผลักดันให้มีการนำหลักการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีมาปฏิบัติ เพื่อให้ได้ผลอย่างจริงจังและเป็นรูปธรรมภายในองค์กร ซึ่งนอกจากจะช่วยสนับสนุนให้การดำเนินงานทางด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจบรรลุตามวัตถุประสงค์ในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีข้างต้นแล้ว ยังสามารถสร้างความเชื่อมั่นต่อมาตรฐานทางด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจในตลาดทุนไทยให้เป็นที่ยอมรับในระดับสากล

1.1 วัตถุประสงค์

แนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีได้จัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ โดยคำนึงถึงความต้องการของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ในการสร้างคุณค่า (Value creation) จากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ ซึ่งหมายถึงการได้รับผลประโยชน์ด้วยต้นทุนทรัพยากรที่ให้ประโยชน์สูงสุดและความเสี่ยงที่เหมาะสมที่สุด โดยการสร้างคุณค่าดังกล่าวจะส่งผลสะท้อนถึงเป้าหมายระดับองค์กรในภาพรวม

1.2 การจัดทำแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีของ ก.ล.ต.

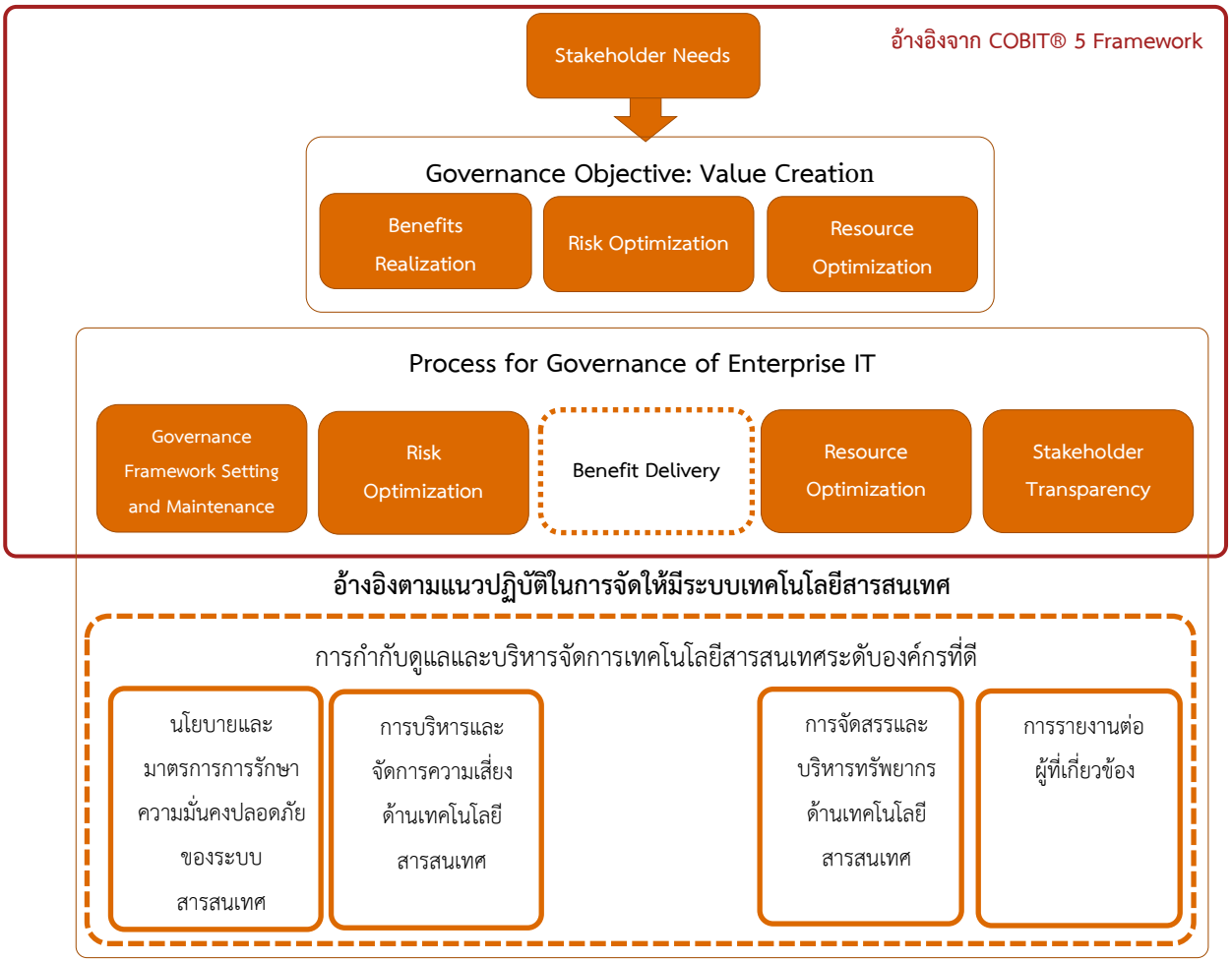
สำนักงานได้จัดทำแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีโดยอ้างอิงกรอบของ COBIT[1] ซึ่งเป็นกรอบการควบคุมและกำกับดูแลเทคโนโลยีสารสนเทศที่เป็นที่ยอมรับในระดับสากล โดยมีความต้องการของผู้มีส่วนได้ส่วนเสียในกิจกรรมที่เกี่ยวกับการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศเป็นแรงผลักดันให้เกิดการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ในเอกสารฉบับนี้มุ่งเน้นในกระบวนการการกำกับดูแลด้านเทคโนโลยีสารสนเทศตามกรอบมาตรฐานของ COBIT ซึ่งประกอบไปด้วย 5 กระบวนการหลัก อันได้แก่

1. การกำหนดกรอบการกำกับดูแลและบริหารจัดการ (Governance Framework Setting and Maintenance)
2. การจัดการความเสี่ยงที่เหมาะสม (Risk Optimization)
3. การส่งมอบผลประโยชน์ (Benefit Delivery)
4. การใช้ทรัพยากรสารสนเทศให้ได้ประโยชน์สูงสุด (Resource Optimization)
5. ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency)

โดยสามารถเทียบเคียงกับหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ ดังแสดงในภาพประกอบที่ 1

[1] ผู้ประกอบธุรกิจสามารถอ้างอิงข้อมูลเกี่ยวกับแนวทางและกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศตามกรอบของ COBIT ได้จาก Information System Audit and Control Association (www.isaca.org) นอกจากนี้ ผู้ประกอบธุรกิจยังสามารถอ้างอิงแนวทางและกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอื่น ๆ เพิ่มเติม เช่น ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (www.iso.org), IT Governance Institute (www.itgovernance.co.uk) และ Information Security Forum (www.securityforum.org)

ภาพประกอบที่ 1



1.3 บทนิยาม

ผู้ประกอบธุรกิจ	หมายถึง	ผู้ประกอบธุรกิจภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ หรือ ธุรกิจสัญญาซื้อขายล่วงหน้าตามที่ระบุไว้ในหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ
บุคลากรของผู้ประกอบธุรกิจ	หมายถึง	คณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง พนักงานชั่วคราว ลูกจ้างชั่วคราว รวมถึงผู้ให้บริการภายนอก ที่เกี่ยวข้องหรือมีหน้าที่ในการดำเนินงานของผู้ประกอบธุรกิจ
ทรัพย์สินสารสนเทศ	หมายถึง	1. ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3. ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
ทรัพยากรสารสนเทศ	หมายถึง	ทรัพยากรสารสนเทศ ประกอบด้วย ทรัพย์สินสารสนเทศ (ระบบ อุปกรณ์ และข้อมูล) บุคลากรทางด้านเทคโนโลยีสารสนเทศ ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศ งบประมาณ
ผู้รับผิดชอบ	หมายถึง	Accountable person หรือ ผู้ที่มีหน้าที่รับผิดชอบในผลสำเร็จหรือผลลัพธ์ของการดำเนินงานตามขอบเขตงานที่กำหนด โดยผู้รับผิดชอบมีหน้าที่วางกรอบหรือแนวทางการดำเนินงาน อนุมัติและบังคับใช้ รวมถึงติดตามผลการดำเนินงานตามกรอบที่ได้วางไว้ โดยตัวอย่างของผู้รับผิดชอบในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ได้แก่ คณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ
ผู้ทำหน้าที่	หมายถึง	Responsible person หรือ ผู้ที่มีหน้าที่ในการดำเนินงานตามกรอบการปฏิบัติงานที่กำหนดโดยผู้รับผิดชอบ โดยตัวอย่างของผู้ทำหน้าที่ในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ได้แก่ ผู้บริหารและบุคลากรที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ และผู้ใช้ระบบเทคโนโลยีสารสนเทศ

2. บทบาทหน้าที่ โครงสร้างองค์กร และการบริหารจัดการบุคลากรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

2.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

คณะกรรมการของผู้ประกอบธุรกิจ (Board of Directors) มีหน้าที่รับผิดชอบกำกับดูแลองค์กรและจัดสรรและควบคุมทรัพยากรขององค์กรโดยรวม โดยคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ มีบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับ

- การกำหนดขอบเขตและวางกรอบกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ และระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
- การอนุมัตินโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี และจัดให้มีการกำหนดขั้นตอน วิธีปฏิบัติงานและกระบวนการที่เกี่ยวข้องให้เป็นไปตามนโยบายดังกล่าว
- การสื่อสารนโยบายการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ รวมทั้งขั้นตอน วิธีการปฏิบัติงานและกระบวนการที่เกี่ยวข้อง ให้บุคลากรของผู้ประกอบธุรกิจที่เกี่ยวข้องรับทราบ และสนับสนุนให้มีการปฏิบัติตามนโยบายดังกล่าว
- การดูแลและติดตามเพื่อให้มั่นใจว่า กิจกรรมในการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศมีการดำเนินการอย่างมีประสิทธิภาพและมีประสิทธิผล เช่น จัดให้มีการออกแบบการควบคุมภายในที่เพียงพอเหมาะสม มีการดำเนินงานตามการควบคุมที่ได้ออกแบบไว้ มีการตรวจสอบโดยหน่วยงานที่เป็นอิสระ มีการรายงานผลการดำเนินการต่อคณะกรรมการของผู้ประกอบธุรกิจอย่างเพียงพอ ทันเวลาและต่อเนื่อง รวมทั้งมีการติดตามผลการปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ให้อยู่ในระดับที่ยอมรับได้
- ทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี อย่างน้อยปีละหนึ่งครั้ง และทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และจัดให้มีการปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

คณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ควรมีความรู้ ความเข้าใจเกี่ยวกับเทคโนโลยีสารสนเทศและพัฒนาการทางด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป รวมทั้งความเสี่ยงที่เกี่ยวข้องและความเสี่ยงอันสืบเนื่องมาจากการใช้งานเทคโนโลยีสมัยใหม่ เช่น ความเสี่ยงทางด้านไซเบอร์ เพื่อให้สามารถกำหนดทิศทางและกำกับดูแลให้องค์กรมีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจขององค์กร และสามารถกำกับดูแลการบริหารจัดการเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ นอกจากนี้ คณะกรรมการควรได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศที่เกี่ยวข้องอย่างเพียงพอตามระยะเวลาที่เหมาะสม

2.2 โครงสร้างการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

โครงสร้างองค์กรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ควรมีผู้รับผิดชอบ (Accountable person) คือ คณะกรรมการของผู้ประกอบธุรกิจ โดยผู้ประกอบธุรกิจควรจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่เหมาะสมและสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defence) โดยคณะกรรมการของผู้ประกอบธุรกิจอาจพิจารณาแต่งตั้งมอบหมายคณะกรรมการเพื่อทำหน้าที่ที่เกี่ยวข้องต่าง ๆ เช่น คณะกรรมการเพื่อทำหน้าที่ในการกำกับดูแลการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศ (IT Steering Committee), คณะกรรมการเพื่อทำหน้าที่ในการกำกับดูแลการบริหารจัดการความเสี่ยงหรือความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk Management Committee) และคณะกรรมการ

เพื่อทำหน้าที่ในการกำกับดูแลให้มีการตรวจสอบทางด้านเทคโนโลยีสารสนเทศ (IT Audit Committee) ตามความเหมาะสมกับลักษณะการดำเนินงานของผู้ประกอบธุรกิจ

ทั้งนี้ โครงสร้างองค์กรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ควรพิจารณาตามหลักการถ่วงดุลอำนาจอย่างอิสระ (Check and Balance) และการแบ่งแยกหน้าที่อย่างเหมาะสม (Segregation of Duties) ตามระดับของ Three Lines of Defence อันได้แก่ หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (First Line of Defence), หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Second Line of Defence) และหน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (Third Line of Defence)

2.2.1 ระดับที่ 1: หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (First Line of Defence)

หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หมายถึง บุคลากรหรือหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ (เช่น หน่วยงานด้านเทคโนโลยีสารสนเทศ) หรือเป็นผู้ใช้ระบบเทคโนโลยีสารสนเทศ บุคลากรหรือหน่วยงานในกลุ่มนี้จัดเป็นผู้ทำหน้าที่ (Responsible person) ในการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ ซึ่งมีหน้าที่ในการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศในขอบเขตงานที่รับผิดชอบ และปฏิบัติตามแนวทางการควบคุม

2.2.2 ระดับที่ 2: หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Second Line of Defence)

หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หมายถึง บุคลากรหรือหน่วยงานที่มีหน้าที่ในการกำกับดูแลให้มีการปฏิบัติตามกฎและหลักเกณฑ์ต่าง ๆ โดยบทบาทหน้าที่อาจรวมถึงการกำหนดกรอบการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ สื่อสารปัญหาหรือความเสี่ยงใหม่ ๆ ที่เกิดขึ้น ติดตามและสนับสนุนกระบวนการกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปในทิศทางที่เหมาะสม รวมทั้งติดตามความเพียงพอเหมาะสมของการควบคุมและการปฏิบัติตามกฎระเบียบต่าง ๆ ขององค์กร บุคลากรหรือหน่วยงานในกลุ่มนี้อาจประกอบด้วย หน่วยงานด้านบริหารความเสี่ยง หน่วยงานด้านบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และหน่วยงานกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ (Compliance)

2.2.3 ระดับที่ 3: หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (Third Line of Defence)

หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ หมายถึง บุคลากรหรือหน่วยงานที่มีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานปฏิบัติงานและหน่วยงานกำกับดูแลการปฏิบัติงาน รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง บุคลากรหรือหน่วยงานในกลุ่มนี้ คือ หน่วยงานตรวจสอบภายใน หรือหน่วยงานตรวจสอบทางด้านเทคโนโลยีสารสนเทศ รวมทั้งผู้ตรวจสอบภายนอกที่เป็นอิสระจากหน่วยงานปฏิบัติงานและหน่วยงานการกำกับดูแลการปฏิบัติงาน

<u>2.3 การบริหารจัดการบุคลากร</u>

เพื่อสนับสนุนโครงสร้างองค์กรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีข้างต้น ผู้ประกอบธุรกิจควรพิจารณาบริหารจัดการบุคลากร โดยดำเนินการดังต่อไปนี้

- มีกระบวนการคัดเลือกบุคลากรที่มีความเหมาะสมทั้งในด้านประสบการณ์และความรู้ความสามารถ ทั้งนี้ อาจพิจารณาจากวุฒิการศึกษา ประสบการณ์การทำงาน รวมทั้งเอกสารรับรองความรู้ความสามารถตามมาตรฐานต่าง ๆ (Certificate) ที่เกี่ยวข้องกับหน้าที่งาน และประวัติการกระทำความผิดที่ผ่านมา
- จัดหาบุคลากรทางด้านสารสนเทศในจำนวนที่เหมาะสมต่อปริมาณการใช้เทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ
- มีมาตรการสร้างและส่งเสริมความตระหนักถึงความสำคัญของความเสี่ยง และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจที่เกี่ยวข้อง เพื่อให้บุคลากรมีการตระหนักถึงบทบาท

หน้าที่และความรับผิดชอบของตน รวมทั้งมีมาตรการดูแลให้บุคลากรปฏิบัติตามหน้าที่และความรับผิดชอบที่กำหนดไว้ เช่น

- จัดให้มีการสื่อสาร อบรม และพัฒนาความรู้ทางด้านเทคโนโลยีสารสนเทศให้แก่คณะกรรมการ ผู้บริหาร และเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้มีความรู้และทักษะที่เพียงพอในการปฏิบัติงาน รวมทั้งการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี โดยเนื้อหาควรครอบคลุมถึงความเสี่ยงและการจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นใหม่ เช่น ความเสี่ยงทางด้านไซเบอร์ นอกจากนี้ ยังอาจรวมถึงกฎหมาย และข้อกำหนดที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ
- มีการกำหนดหน้าที่ความรับผิดชอบของบุคลากรในหัวข้อเรื่องเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยอาจระบุในสัญญาจ้างงาน หรือกฎระเบียบบริษัท เพื่อให้มีการปฏิบัติตามอย่างเคร่งครัด

โดยรายละเอียดบทบาทและหน้าที่ในการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ สำหรับการดำเนินงานในกระบวนการต่าง ๆ มีระบุไว้ในส่วนถัดไป

3. แนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

เพื่อให้เป็นไปตามการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ผู้ประกอบธุรกิจควรพิจารณากำหนดกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร โดยในกรอบการดำเนินการนี้ควรประกอบด้วย การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม การส่งมอบผลประโยชน์และการใช้ทรัพยากรสารสนเทศให้ได้ประโยชน์สูงสุด รวมถึงความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย โดยผู้ประกอบธุรกิจอาจพิจารณาการดำเนินการดังต่อไปนี้

3.1 การกำหนดกรอบการกำกับดูแลและบริหารจัดการ (Governance Framework Setting and Maintenance)

เพื่อให้การกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศมีความสอดคล้องกับวัตถุประสงค์ขององค์กร มีประสิทธิผล มีความโปร่งใส และเป็นไปตามกฎหมายและข้อบังคับต่าง ๆ ผู้ประกอบธุรกิจควรมีการกำหนดและจัดทำนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี เพื่อกำหนดกรอบการกำกับดูแลระบบและกระบวนการทางด้านเทคโนโลยีสารสนเทศ โดยนโยบายดังกล่าวควรประกอบด้วยหัวข้อ ดังนี้ (1) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (2) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรให้ได้เพียงพอตามที่กำหนดไว้ และ (3) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ ขั้นตอนในการจัดทำนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี อาจดำเนินการดังนี้

- วิเคราะห์และระบุถึงปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กร ทั้งด้านกฎหมาย ระเบียบข้อบังคับและภาระผูกพันของสัญญาต่าง ๆ รวมทั้งแนวโน้มทางธุรกิจที่อาจมีผลต่อการออกแบบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี
- พิจารณาระดับความสำคัญของเทคโนโลยีสารสนเทศ รวมทั้งบทบาทของเทคโนโลยีสารสนเทศต่อการดำเนินธุรกิจขององค์กร
- พิจารณาการนำเทคโนโลยีสารสนเทศมาใช้และประเมินผลกระทบจากการดำเนินการดังกล่าวที่มีต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกขององค์กร รวมทั้งความสอดคล้องกับเป้าหมาย และวัตถุประสงค์โดยรวมขององค์กร
- พิจารณานัยสำคัญของสภาพแวดล้อมของการควบคุมโดยทั่วไปของผู้ประกอบธุรกิจที่มีต่อเทคโนโลยีสารสนเทศ
- กำหนดหลักการสำคัญที่จะใช้เป็นแนวทางสำหรับการออกแบบการกำกับดูแลและการตัดสินใจที่สำคัญเกี่ยวกับเทคโนโลยีสารสนเทศ รวมทั้งทำความเข้าใจเกี่ยวกับวัฒนธรรมขององค์กรในการตัดสินใจและพิจารณากำหนดรูปแบบการตัดสินใจเกี่ยวกับเทคโนโลยีสารสนเทศที่เหมาะสมสำหรับองค์กร (Optimal Decision-Making Model) อันอาจมีรูปแบบปัจจัยและลำดับความสำคัญในการพิจารณาและตัดสินใจที่แตกต่างกันไปในแต่ละองค์กร เช่น ปัจจัยด้านผลประโยชน์ตอบแทน ปัจจัยด้านผลกระทบต่อบุคลากร ปัจจัยด้านการปฏิบัติตามข้อกำหนดทางกฎหมาย เป็นต้น
- กำหนดระดับการมอบหมายอำนาจอนุมัติ รวมทั้งข้อกำหนดที่เกี่ยวข้องสำหรับการตัดสินใจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่เหมาะสม

ภาพประกอบที่ 2 – กรอบการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ

โดยเนื้อหาที่เกี่ยวข้องของนโยบายแต่ละด้านอาจประกอบด้วย

(1) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

(3) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ทั้งนี้ เพื่อให้นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีมีผลบังคับใช้ทั่วทั้งองค์กร ควรมีการกำหนดบทบาทของบุคลากรที่เกี่ยวข้อง และแนวทางการสื่อสารที่เหมาะสม อันได้แก่

- มีช่องทางที่เหมาะสมในการสื่อสารนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีไปยังบุคลากรที่เกี่ยวข้อง รวมทั้งมีกระบวนการการสื่อสารเพื่อให้บุคลากรที่มีหน้าที่เกี่ยวข้องรับทราบข้อมูลที่เพียงพอในการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี
- ผู้ที่ได้รับการสื่อสารเกี่ยวกับนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีนี้ควรรวมถึงพนักงานและลูกจ้างของผู้ประกอบธุรกิจ รวมถึงผู้ให้บริการภายนอกที่มีการเข้าถึงระบบสารสนเทศขององค์กร

- นอกเหนือจากการสื่อสารข้างต้น ผู้ประกอบธุรกิจอาจมีการบังคับใช้และสนับสนุนให้มีการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีภายในองค์กร ตัวอย่างเช่น
    - มีการกำหนดบทลงโทษในกรณีที่เกิดการกระทำที่ขัดต่อจริยธรรม หรือการฝ่าฝืนนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี
    - มีการพิจารณาผลประโยชน์ตอบแทน เช่น การประกาศเกียรติคุณ การประเมินผลงาน หรือรางวัลพิเศษอื่น ๆ เมื่อมีบุคลากรหรือหน่วยงานปฏิบัติเป็นแบบอย่างที่ดีตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

เพื่อเป็นการวัดผลการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ผู้ประกอบการควรกำหนดกระบวนการประเมินผลการปฏิบัติตามนโยบายดังกล่าว ซึ่งอาจประกอบด้วย

- การกำหนดรอบระยะเวลาที่ชัดเจนในการประเมินผลการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี และรายงานต่อคณะกรรมการของผู้ประกอบธุรกิจ อย่างน้อยปีละ 1 ครั้ง โดยการประเมินผลการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรอาจประกอบด้วย
    - รายงานจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ซึ่งเนื้อหาการรายงานควรครอบคลุมถึง ผลการปฏิบัติงานด้านการบริหารความเสี่ยง และการจัดการทรัพยากร ความคืบหน้าของโครงการและการดำเนินงานที่สำคัญ การปฏิบัติตามกฎระเบียบข้อบังคับหรือข้อตกลงต่าง ๆ ประสิทธิภาพและประสิทธิผลในการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน รวมถึงปัญหาและอุปสรรคที่เกิดขึ้น
    - รายงานจากหน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยการรายงานอาจรวมถึงการรายงานแผนการตรวจสอบตามความเสี่ยงทั้งในส่วนของแผนการตรวจสอบระยะสั้นและระยะยาว ผลการตรวจสอบตามแผนการตรวจสอบที่ได้วางไว้ และการติดตามการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบ
- ในกรณีที่พบว่า มีข้อบกพร่องในการออกแบบกระบวนการ หรือการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ควรรายงานต่อคณะกรรมการโดยไม่ชักช้า รวมทั้งมีการกำหนดผู้มีหน้าที่รับผิดชอบและวิธีการแก้ไขข้อบกพร่องนั้น ๆ

<u>3.2 การจัดการความเสี่ยงที่เหมาะสม (Risk Optimization)</u>

เพื่อให้ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอยู่ในระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Appetite) และลดความผิดพลาดที่อาจเกิดขึ้นจากการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ ผู้ประกอบธุรกิจควรมีกระบวนการดังนี้

3.2.1 การจัดทำนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีส่วนร่วมอยู่ในทุกด้านของความเสี่ยงขององค์กร โดยเฉพาะอย่างยิ่งในองค์กรที่มีการใช้งานเทคโนโลยีสารสนเทศเป็นตัวผลักดันในการดำเนินธุรกิจ ดังนั้น เพื่อให้การบริหารและจัดการความเสี่ยงขององค์กรมีการดำเนินการอย่างมีประสิทธิภาพ เป็นไปในแนวทางเดียวกันและสามารถเชื่อมโยงเป็นภาพเดียวกันได้ทั้งหมด กระบวนการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงควรสอดคล้องและเป็นไปในแนวทางเดียวกันกับนโยบายและการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ และมีการสื่อสารไปยังผู้ที่เกี่ยวข้อง รวมทั้งต้องมีการทบทวนและปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และต้องทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ

ซึ่งอาจส่งผลกระทบต่อการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ โดยควรระบุระเบียบวิธีปฏิบัติและกระบวนการที่สอดคล้องกับนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่วางไว้ ทั้งนี้ นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีเนื้อหาครอบคลุมกระบวนการบริหารความเสี่ยงตามข้อ 3.2.2 – 3.2.7

3.2.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ผู้ประกอบธุรกิจอาจพิจารณาปรับใช้กระบวนการในการเก็บข้อมูลที่เกี่ยวข้อง เพื่อนำมาพิจารณาประกอบในการระบุความเสี่ยงที่เป็นไปได้ทั้งหมด การกำหนดสถานการณ์ความเสี่ยง และการกำหนดปัจจัยความเสี่ยงที่เหมาะสม โดยควรมีขั้นตอนดังนี้

- กำหนดกระบวนการในการเก็บข้อมูล แยกหมวดหมู่ และวิเคราะห์ข้อมูลเกี่ยวกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ โดยอาจจัดแบ่งตามประเภทของเหตุการณ์ ประเภทของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และปัจจัยความเสี่ยงต่าง ๆ ทั้งนี้ ควรพิจารณารวมถึงความเสี่ยงทางด้านเทคโนโลยีที่เกิดขึ้นใหม่ เช่น ความเสี่ยงทางด้านไซเบอร์
- รวบรวมและวิเคราะห์ข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจมีผลต่อการดำเนินงานและความสำเร็จของแผนกลยุทธ์ทางธุรกิจขององค์กร รวมทั้งแผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ
- มีการบันทึกข้อมูลสภาพแวดล้อมการดำเนินงานทั้งภายในและภายนอกเพื่อใช้ประกอบในการประเมินความเสี่ยง โดยสภาพแวดล้อมการดำเนินงานภายในอาจประกอบด้วย แผนกลยุทธ์และนโยบายทางด้านเทคโนโลยีสารสนเทศ โครงสร้างองค์กรทางด้านเทคโนโลยีสารสนเทศ และทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ ในขณะที่สภาพแวดล้อมการดำเนินงานภายนอกอาจประกอบด้วยกฎระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้อง และแนวโน้มทางด้านเทคโนโลยีสารสนเทศในกลุ่มธุรกิจ
- สำรวจและวิเคราะห์ข้อมูลความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งผลกระทบหรือความเสียหายในอดีต โดยอาจมีการรวบรวมข้อมูลมาจากภายนอก ข้อมูลแนวโน้มธุรกิจ ข้อมูลของบริษัทอื่น ๆ ในธุรกิจเดียวกัน หรือมีการแบ่งปันข้อมูลกันระหว่างธุรกิจ
- บันทึกข้อมูลเหตุการณ์ความเสี่ยงที่ส่งผลหรืออาจส่งผลต่อการใช้เทคโนโลยีสารสนเทศ การส่งมอบระบบงานหรือโครงการทางด้านเทคโนโลยีสารสนเทศ รวมทั้งการปฏิบัติงานและให้บริการทางด้านเทคโนโลยีสารสนเทศ ทั้งนี้อาจรวมถึงข้อจำกัด ประเด็นปัญหา และการติดตามการแก้ไขปัญหาด้วย
- มีการจัดการและจำแนกประเภทของข้อมูลเหตุการณ์ความเสี่ยง รวมถึงมีการระบุถึงปัจจัยที่ส่งผลต่อเหตุการณ์นั้น
- พิจารณาเงื่อนไขที่มีผลต่อเหตุการณ์ความเสี่ยงจากเหตุการณ์ที่เคยเกิดขึ้นแล้ว รวมทั้งความเชื่อมโยงของเงื่อนไขต่อโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง
- วิเคราะห์และทบทวนเหตุการณ์ความเสี่ยงและปัจจัยความเสี่ยงอย่างสม่ำเสมอเพื่อระบุประเด็นความเสี่ยงใหม่ ๆ เพิ่มเติม ซึ่งจะช่วยให้มีความเข้าใจเกี่ยวกับภาพความเสี่ยงขององค์กรได้ดีขึ้น

ภาพประกอบที่ 3 – การระบุความเสี่ยง

3.2.3 การกำหนดความเสี่ยงที่สามารถยอมรับได้

จากความเสี่ยงที่ได้รวบรวมในขั้นตอนข้างต้น ผู้ประกอบธุรกิจควรพิจารณาถึงระดับความเสี่ยงที่องค์กรสามารถยอมรับได้เมื่อมีความเสี่ยงนั้น ๆ เกิดขึ้น โดยควรมีการกำหนดระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) โดยอาจพิจารณาจากระดับความเสี่ยงที่ผู้ประกอบธุรกิจสามารถยอมรับได้ รวมถึงวัฒนธรรมองค์กร หรือระดับการยอมรับความเสี่ยงของคณะกรรมการบริษัท

3.2.4 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เมื่อผู้ประกอบธุรกิจระบุความเสี่ยงที่เป็นไปได้ทั้งหมดกำหนดสถานการณ์ความเสี่ยง และกำหนดปัจจัยความเสี่ยงที่เหมาะสม รวมทั้งกำหนดความเสี่ยงที่สามารถยอมรับได้แล้ว จึงประเมินถึงโอกาสเกิดและผลกระทบของเหตุการณ์ความเสี่ยงที่กำหนดไว้ โดยอาจจัดทำในรูปแบบของแผนภาพความเสี่ยง (Risk Map) เพื่อนำเสนอระดับของโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง และทะเบียนความเสี่ยง (Risk Register) เพื่อบรรยายข้อมูลรายละเอียดของความเสี่ยง จากนั้นจึงจัดทำโครงร่างของความเสี่ยง (Risk Profile) เพื่อรวบรวมความเสี่ยงที่เกี่ยวข้องทั้งหมด โดยโครงร่าง

ของความเสี่ยงนี้ยังช่วยผู้ประกอบธุรกิจเปรียบเทียบโอกาสเกิด และผลกระทบของแต่ละความเสี่ยง และใช้ในการจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

3.2.5 การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

เพื่อให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปตามระดับความสำคัญ และตอบสนองต่อเป้าหมายขององค์กร ผู้ประกอบธุรกิจควรมีกระบวนการในการบริหารและจัดการต่อความเสี่ยง ดังนี้

- ควรนำระดับความเสี่ยงที่สามารถยอมรับได้มาเปรียบเทียบกับผลการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ได้ดำเนินการไว้ข้างต้น ซึ่งในกระบวนการนี้ ผู้ประกอบธุรกิจอาจประเมินการควบคุมและความเสี่ยงที่ยังหลงเหลืออยู่ โดยในกรณีที่ความเสี่ยงที่หลงเหลืออยู่เกินกว่าระดับที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงนั้น
- การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (Risk Response) อาจพิจารณาจากระดับความสำคัญของความเสี่ยง ประสิทธิภาพและประสิทธิผลของการจัดการความเสี่ยง และความสามารถของผู้ประกอบธุรกิจในการดำเนินกิจกรรมเพื่อจัดการความเสี่ยง โดยการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงสามารถดำเนินการได้ใน 4 ลักษณะ อันได้แก่ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance), การยอมรับความเสี่ยง (Risk Acceptance), การร่วมรับความเสี่ยง/ถ่ายโอน (Risk Sharing/Transfer) และการลดความเสี่ยง (Risk Mitigation)

3.2.6 การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) และจัดให้มีการติดตามรายงานผลตัวชี้วัดดังกล่าว

- ผู้ประกอบธุรกิจควรกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) เพื่อสามารถชี้วัดและติดตามความเสี่ยงได้อย่างรวดเร็ว รวมทั้งสามารถติดตามแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น
- ควรมีการรายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไปประกอบการตัดสินใจได้ รวมถึงรายงานผลการบริหารจัดการความเสี่ยง ประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบจากรายการความเสี่ยง

3.2.7 การกำหนดหน้าที่และความรับผิดชอบของบุคลากรผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- คณะกรรมการของผู้ประกอบธุรกิจควรเป็นผู้รับผิดชอบ (Accountable person) ในการให้แนวทางและอนุมัติ เห็นชอบในนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งติดตามผลการปฏิบัติตามนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ
- ผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยง อาทิ หัวหน้าสายงานบริหารความเสี่ยง และหัวหน้าสายงานบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นผู้ทำหน้าที่ (Responsible person) ในการกำหนดกรอบและกระบวนการการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งสนับสนุนให้มีการดำเนินงานดังกล่าว โดยผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยงนี้จะเป็นผู้รับผิดชอบ (Accountable person) ในผลการบริหารจัดการความเสี่ยงทุกรูปแบบทั่วทั้งองค์กร รวมถึงรับผิดชอบให้มีการจัดทำและปรับปรุงรายการความเสี่ยงและกิจกรรมการบริหารความเสี่ยง
- ผู้บริหารหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ อาทิ หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศเป็นผู้ทำหน้าที่ (Responsible person) ในการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

เพื่อเป็นแนวทางในการดำเนินงานทางด้านการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานได้จัดทำเอกสาร “การบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (IT Risk Management Practice)” เพื่อแสดงรายละเอียดเพิ่มเติมของกระบวนการการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

3.3 การส่งมอบผลประโยชน์ (Benefit Delivery) และการใช้ทรัพยากรสารสนเทศให้ได้ประโยชน์สูงสุด (Resource Optimization)

เพื่อให้มีการใช้ทรัพยากรสารสนเทศอย่างคุ้มค่า และตอบสนองต่อความต้องการทางด้านธุรกิจอย่างมีประสิทธิภาพและมีประสิทธิผล โดยมีต้นทุนในระดับที่ยอมรับได้ ผู้ประกอบธุรกิจควรมีการจัดทำแผนกลยุทธ์และนโยบาย ดังนี้

3.3.1 การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ และงบประมาณด้านเทคโนโลยีสารสนเทศ

แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ รวมถึงงบประมาณด้านเทคโนโลยีสารสนเทศ ควรสอดคล้องกับแผนกลยุทธ์โดยรวมขององค์กร โดยปัจจัยและข้อมูลที่เกี่ยวข้องกับการพิจารณาจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ อาจประกอบด้วย

- ความต้องการของผู้มีส่วนได้ส่วนเสีย และประเด็นที่เกี่ยวข้องกับกลยุทธ์ อาทิ ระดับการพึ่งพิงการใช้ระบบสารสนเทศ ความสามารถและความรู้ความเข้าใจในระบบสารสนเทศขององค์กร เพื่อที่จะประเมินระดับความสำคัญของเทคโนโลยีสารสนเทศในปัจจุบันและแนวโน้มที่เป็นไปได้ในอนาคตต่อแผนกลยุทธ์โดยรวมขององค์กร
- ความน่าเชื่อถือ ความปลอดภัย และความคุ้มค่าในการใช้งานทรัพยากรสารสนเทศที่มีอยู่ และการจัดหาทรัพยากรสารสนเทศเพิ่มเติม
- ความสอดคล้องของกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศและกลยุทธ์ขององค์กรในภาพรวม เพื่อที่จะตอบสนองเป้าหมายขององค์กร โดยอาจพิจารณาจากเป้าหมายผลตอบแทนในการลงทุน (Return on investment) หรือความคาดหวังจากการลงทุนทางด้านเทคโนโลยีสารสนเทศ
- ประโยชน์หรือโอกาส รวมทั้งความท้าทายที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบันและเทคโนโลยีที่มีการพัฒนาขึ้นใหม่มาใช้สำหรับการดำเนินงาน
- การพิจารณากำหนดบทบาทหน้าที่ ความรับผิดชอบ และโครงสร้างการตัดสินใจในการดำเนินงานทางด้านเทคโนโลยีสารสนเทศที่เหมาะสม ที่ทำให้การตัดสินใจและการลงทุนทางด้านเทคโนโลยีสารสนเทศสร้างคุณค่าให้แก่องค์กร
- เงื่อนไขในการจัดระดับความสำคัญหรือเงื่อนไขที่ใช้ในการตัดสินใจเกี่ยวกับการดำเนินงานที่สำคัญ หรือการลงทุนที่สำคัญทางด้านเทคโนโลยีสารสนเทศ โดยอาจพิจารณาจากความเสี่ยงที่เกี่ยวข้อง แผนการใช้งานระบบงานใหม่ งบประมาณ รวมถึงผลตอบแทนที่ได้รับ
- ในการจัดทำงบประมาณทางด้านเทคโนโลยีสารสนเทศ ควรพิจารณาครอบคลุมทุกรายการที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น ทรัพย์สินสารสนเทศ การใช้ทรัพยากรส่วนกลางขององค์กร บุคลากรทางด้านสารสนเทศ ผู้ให้บริการภายนอกทางด้านเทคโนโลยีสารสนเทศ ค่าใช้จ่ายในการประกันภัย และค่าลิขสิทธิ์ที่เกี่ยวข้อง
- นอกจากนี้ อาจมีการประเมินต้นทุนทางตรง และต้นทุนทางอ้อมของบริการทางด้านเทคโนโลยีสารสนเทศเพื่อใช้เป็นข้อมูลในการจัดทำงบประมาณทางด้านเทคโนโลยีสารสนเทศ

แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือด้านเทคโนโลยีสารสนเทศ และงบประมาณด้านเทคโนโลยีสารสนเทศ ควรได้รับการอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ และสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ รวมทั้งมีการมอบหมายให้ผู้บริหารนำไปปฏิบัติเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศในภาพรวมสอดคล้องกับแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ ผู้ประกอบธุรกิจควรระบุและสื่อสารเป้าหมายการดำเนินงานของหน่วยงานด้านเทคโนโลยีสารสนเทศ รวมถึงวิธีการติดตามผลการดำเนินงานตามแผนงานและงบประมาณด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ โดยตัวอย่างตัวชี้วัดที่เกี่ยวข้องกับแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ และงบประมาณด้านเทคโนโลยีสารสนเทศ แสดงอยู่ในภาคผนวก

3.3.2 การจัดทำนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ และการจัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศ

ในการจัดทำนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าทรัพยากรเทคโนโลยีสารสนเทศ โดยเฉพาะทรัพยากรบุคคลมีความเพียงพอ รวมทั้งการจัดการความเสี่ยงอันเกี่ยวเนื่องจากการขาดทรัพยากรในการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ ผู้ประกอบธุรกิจอาจพิจารณาถึงเงื่อนไขและการดำเนินงานที่เกี่ยวข้อง ดังนี้

- พิจารณาและกำหนดกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศสำหรับปัจจุบัน และในอนาคต ทางเลือกต่าง ๆ สำหรับการจัดหาทรัพยากรทางด้านเทคโนโลยีสารสนเทศ และการพัฒนาทรัพยากรสารสนเทศให้เพียงพอต่อความต้องการในปัจจุบันและอนาคต รวมทั้งทางเลือกเกี่ยวกับแหล่งที่มาของทรัพยากรสารสนเทศ และกลยุทธ์ในการจัดหาทรัพยากร
- กำหนดหลักเกณฑ์เพื่อใช้เป็นแนวทางในการจัดสรรและบริหารทรัพยากรสารสนเทศ รวมทั้งขีดความสามารถเพื่อให้หน่วยงานเทคโนโลยีสารสนเทศสามารถตอบสนองตามความต้องการขององค์กรตามระดับขีดความสามารถและสมรรถนะที่ต้องการ ระดับความเร่งด่วนในการใช้งาน และข้อจำกัดด้านงบประมาณ
- เพื่อเป็นการวางแผนในการจัดสรรทรัพยากรอย่างคุ้มค่า และลดความเสี่ยงที่อาจเกิดขึ้น ผู้ประกอบธุรกิจอาจพิจารณาจัดทำแผนการจัดสรรทรัพยากรสารสนเทศและการจัดโครงสร้างภายในองค์กร โดยแผนนี้ควรสอดคล้องกับการจัดสรรทรัพยากรขององค์กร รวมทั้งการบริหารทรัพยากรบุคคลโดยรวมขององค์กรด้วย

นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศนี้ ถือเป็นส่วนหนึ่งของนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ซึ่งควรได้รับการพิจารณาอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ และมีการสื่อสารไปยังผู้ที่เกี่ยวข้อง รวมทั้งมีการสอบทานและปรับปรุงอย่างสม่ำเสมอ นอกจากนี้ ผู้ประกอบธุรกิจควรระบุวิธีการติดตาม และประเมินผลการดำเนินงานตามนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ เพื่อให้มั่นใจถึงความเพียงพอของทรัพยากรสารสนเทศ ซึ่งอาจประกอบด้วย

- การกำหนดเป้าหมาย ตัวชี้วัดความสำเร็จ และกระบวนการที่เกี่ยวข้องสำหรับการจัดสรรทรัพยากรสารสนเทศ
- การกำหนดหลักเกณฑ์ในการป้องกันรักษาทรัพยากรสารสนเทศ ทั้งในส่วนของการป้องกันการสูญเสียทรัพยากรบุคคลที่มีความรู้ความสามารถ และการป้องกันความเสียหายต่อทรัพย์สินสารสนเทศ
- การติดตามผลการทำงานของทรัพยากรสารสนเทศโดยเทียบกับเป้าหมายที่วางไว้ อาทิ การติดตามผลการทำงานของบุคลากรทางด้านเทคโนโลยีสารสนเทศ การติดตามผลการทำงานของระบบงาน และอุปกรณ์ด้านเทคโนโลยีสารสนเทศต่าง ๆ โดยถ้ามีการตรวจพบข้อบกพร่องหรือผลการทำงานที่ไม่เป็นไปตามเป้าหมาย ควรมีการตรวจสอบหาสาเหตุและวางแผนการแก้ไขอย่างเหมาะสม

3.4 ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency)

เพื่อให้มั่นใจว่าการรายงานและการสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศกับผู้มีส่วนได้ส่วนเสียมีประสิทธิผลและทันเวลา การดำเนินงานโดยรวมควรมีการพัฒนาอย่างต่อเนื่อง และวัตถุประสงค์รวมทั้งกลยุทธ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนกลยุทธ์ขององค์กร ซึ่งแนวทางปฏิบัติที่ควรพิจารณามีดังนี้

3.4.1 การประเมินความต้องการของผู้มีส่วนได้ส่วนเสียในการรายงานผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศ

- ผู้ประกอบธุรกิจควรพิจารณาข้อกำหนดด้านการรายงานภาคบังคับ (Mandatory Reporting) ทั้งในปัจจุบันและอนาคตที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศภายในองค์กร รวมทั้งขอบเขตและรอบระยะเวลาในการรายงานที่เหมาะสม
- นอกเหนือจากประเด็นข้างต้น การรายงานยังอาจต้องพิจารณาถึงความต้องการด้านการรายงานสำหรับผู้มีส่วนได้ส่วนเสียอื่น ๆ ทั้งในปัจจุบันและอนาคต ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศในองค์กร รวมถึงขอบเขตและเงื่อนไขในการรายงานที่แตกต่างกัน
- ผู้ประกอบธุรกิจควรจัดให้มีหลักเกณฑ์การรายงานต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร รวมทั้งรูปแบบและช่องทางการสื่อสารอย่างเหมาะสม

3.4.2 การสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสม

- ผู้ประกอบธุรกิจควรมีการกำหนดกลยุทธ์ในการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร
- ควรมีการกำหนดวิธีการสอบทานเพื่อให้มั่นใจว่าข้อมูลการรายงานเป็นไปตามหลักเกณฑ์สำหรับข้อกำหนดของการรายงานภาคบังคับของผู้ประกอบธุรกิจทั้งหมด
- ควรมีกระบวนการในการตรวจสอบความถูกต้องและอนุมัติรายงานภาคบังคับ
- มีกระบวนการ และลำดับชั้นการรายงาน

3.4.3 การติดตามการสื่อสารกับผู้มีส่วนได้ส่วนเสีย

- ผู้ประกอบธุรกิจควรมีการประเมินความมีประสิทธิผลของการรายงานผลอย่างสม่ำเสมอ เพื่อให้มั่นใจในความถูกต้องและความน่าเชื่อถือของรายงานภาคบังคับที่จัดทำขึ้น
- ผู้ประกอบธุรกิจควรมีการประเมินความมีประสิทธิผลของวิธีการสื่อสารและผลลัพธ์ของการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร และประเมินว่าการสื่อสารดังกล่าวสามารถตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียที่หลากหลายอย่างครบถ้วน

ภาคผนวก ตัวอย่างดัชนีวัดผลที่สำคัญที่เกี่ยวข้องกับแผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศหรือแผนทางด้านเทคโนโลยีสารสนเทศ และงบประมาณทางด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของดัชนีชี้วัด	ตัวอย่างดัชนีวัดผลที่สำคัญ
เพื่อวัดผลความสอดคล้องระหว่างกลยุทธ์ด้านเทคโนโลยีสารสนเทศ และกลยุทธ์ขององค์กร	● ร้อยละของเป้าหมายกลยุทธ์ขององค์กรที่สนับสนุนโดยเป้าหมายกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ
เพื่อวัดผลการใช้ต้นทุนทางด้านเทคโนโลยีสารสนเทศเพื่อตอบสนองตามเป้าหมายการดำเนินงาน หรือตอบสนองต่อความเสี่ยง	● ร้อยละของการบริการทางด้านเทคโนโลยีสารสนเทศที่มีการระบุและอนุมัติต้นทุนและผลประโยชน์ในการดำเนินงานที่ชัดเจน ร้อยละของบริการหรือการลงทุนทางด้านเทคโนโลยีสารสนเทศที่สามารถดำเนินงานได้ภายในงบประมาณที่กำหนดไว้
เพื่อวัดประโยชน์ที่ได้รับจากการลงทุนทางด้านเทคโนโลยีสารสนเทศ หรือการใช้บริการทางด้านเทคโนโลยีสารสนเทศ	● ร้อยละของบริการหรือการลงทุนทางด้านเทคโนโลยีสารสนเทศที่ได้รับผลประโยชน์ตามที่คาดการณ์ไว้ หรือมากกว่าที่คาดการณ์ไว้ ● ร้อยละของบริการทางด้านเทคโนโลยีสารสนเทศที่สำเร็จลุล่วงตามแผนทางด้านเทคโนโลยีสารสนเทศที่กำหนดไว้ ● ร้อยละของบริการทางด้านเทคโนโลยีสารสนเทศที่สามารถส่งมอบได้ตามมาตรฐานหรือข้อตกลงที่ตั้งไว้
เพื่อวัดผลการส่งมอบงานทางด้านสารสนเทศที่สอดคล้องกับความต้องการทางธุรกิจ	● ร้อยละของผู้บริหารระดับสูงที่พึงพอใจในนวัตกรรม และทิศทางการนำเทคโนโลยีสารสนเทศเข้ามาส่งเสริมการดำเนินงานทางธุรกิจของหน่วยงานเทคโนโลยีสารสนเทศร้อยละของผู้ใช้งานที่พึงพอใจในการให้บริการทางด้านเทคโนโลยีสารสนเทศ