GTAG 7

แนวทางการตรวจสอบเทคโนโลยีในระดับสากล

การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

บทสรุปผู้บริหาร

จุดประสงค์ของแนวทางการตรวจสอบเทคโนโลยีในระดับสากล
“การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก (IT Outsourcing: ITO)”
ก็เพื่อช่วยให้หัวหน้าผู้บริหารงานตรวจสอบภายใน (CAE)
และทีมผู้ตรวจสอบกำหนดขอบเขตของการมีส่วนร่วมของผู้ตรวจสอบภายใน
เมื่อหน่วยงานขององค์กรมีการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกเป็นบางส่วนหรือทั้งหมด
แนวทางฉบับนี้ให้ข้อมูลเกี่ยวกับประเภทและวงจรของการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก
และผู้ตรวจสอบภายในจะวางแนวทางเพื่อเผชิญกับความเสี่ยงที่สัมพันธ์กับการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกอย่างไร

การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกคือ
การจัดจ้างหน่วยงานภายนอกเพื่อทำงานด้านเทคโนโลยีสารสนเทศ
ซึ่งเคยดำเนินการโดยหน่วยงานภายในมาก่อน ด้วยแรงกระตุ้นด้านเศรษฐกิจ
ทำให้มีองค์กรจำนวนมากขึ้นใช้บริการจากหน่วยงานภายนอกในกระบวนการด้านเทคโนโลยีสารสนเทศบางส่วนเพื่อมุ่งเน้นธุรกิจหลัก ในสภาพแวดล้อมขององค์กรภาครัฐ
มีการใช้บริการด้านเทคโนโลยีสารสนเทศจากองค์กรภาครัฐที่ให้บริการร่วมแก่หน่วยงานภาครัฐต่างๆ
บางองค์กรใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกเพียงรายเดียว
บางองค์กรก็ใช้บริการจากหลายราย นั่นคือ
การสร้างและการผสมผสานของธุรกิจและบริการด้านเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายในและภายนอกสามารถร่วมงานกันอย่างลงตัว การใช้บริการจากผู้ให้บริการหลายรายจะเพิ่มความซับซ้อนขึ้น

ประเด็นสำคัญที่ผู้ตรวจสอบภายในควรพิจารณาหาคำตอบให้ได้ในระหว่างการตรวจสอบกิจกรรมการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ได้แก่

- กิจกรรมการควบคุมเทคโนโลยีสารสนเทศที่มีการใช้บริการจากหน่วยงานภายนอกมีความสอดคล้องกับกระบวนการทางธุรกิจอย่างไร
- ผู้ตรวจสอบภายในมีส่วนร่วมอย่างเหมาะสมในขั้นตอนสำคัญของวงจรการใช้บริการจากหน่วยงานภายนอกหรือไม่
- ผู้ตรวจสอบภายในมีความรู้และประสบการณ์ด้านเทคโนโลยีสารสนเทศเพียงพอที่จะพิจารณาความเสี่ยงและให้ข้อมูลที่ถูกต้องเหมาะสมหรือไม่

- ถ้ากิจกรรมการควบคุมด้านเทคโนโลยีสารสนเทศถูกถ่ายโอนไปอยู่กับผู้ให้บริการภายนอก ผู้ให้บริการดังกล่าวเข้าใจบทบาทและความคาดหวังของผู้มีส่วนได้เสียด้านการตรวจสอบภายในหรือไม่ ผู้ตรวจสอบภายในสามารถเห็นถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและให้ข้อเสนอแนะสำหรับกระบวนการต่างๆ ที่ได้ถ่ายโอนไปหรือไม่
- ทีมผู้ตรวจสอบภายในมีบทบาทอะไรในการต่อรองใหม่ การเลิกและการต่อสัญญาการใช้บริการจากหน่วยงานภายนอก

บทนำ

องค์กรอาจใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกด้วยเหตุผลหลายประการ ซึ่งรวมทั้งความเชี่ยวชาญ การปรับโครงสร้างต้นทุน การบริหารขีดความสามารถ และการบริหารความเสี่ยง อย่างไรก็ตาม
ผู้บริหารของหน่วยงานผู้ใช้งานยังคงต้องรับผิดชอบในกิจกรรมการควบคุมและผลการปฏิบัติงาน

บ่อยครั้งที่กระบวนการหลักด้านการเงินและการปฏิบัติการต้องพึ่งพาเทคโนโลยีที่องค์กรใช้บริการจากหน่วยงานภายนอก เมื่อมีการใช้บริการจากหน่วยงานภายนอกในกระบวนการด้านเทคโนโลยีสารสนเทศ เช่น การรักษาความมั่นคงปลอดภัย การบริหารการเปลี่ยนแปลง
และการปฏิบัติงานที่สนับสนุนกระบวนการทางธุรกิจหลัก
ผู้ตรวจสอบภายในอาจต้องพิจารณาผลกระทบต่อกิจกรรมการควบคุมต่างๆ
หน่วยงานผู้ให้บริการภายนอกจะแสดงให้หน่วยงานผู้ใช้งานเห็นว่ามีการดำเนินการควบคุมอย่างต่อเนื่องได้อย่างไร เทคโนโลยีเช่น การประมวลผลแบบกลุ่มเมฆ (cloud computing)
จะช่วยให้หน่วยงานผู้ใช้งานบรรลุกลยุทธ์ที่กำหนดไว้
แต่อาจจำกัดการแสดงให้เห็นถึงประสิทธิผลของกิจกรรมการควบคุมได้

กิจกรรมการตรวจสอบภายในอาจจำเป็นต้องประเมินความเพียงพอและประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศซึ่งดำเนินการโดยผู้ให้บริการภายนอก ทั้งนี้
ขึ้นอยู่กับลักษณะของกระบวนการที่ใช้บริการจากหน่วยงานภายนอก
โดยดำเนินการตามมาตรฐานปฏิบัติงาน Standard 2130. A1: Control ดังนั้น เพื่อให้เกิดความเชื่อมั่น จำเป็นต้องพิจารณาว่า
มีการควบคุมภายในอย่างเพียงพอหรือไม่ในการประมวลผลซึ่งดำเนินการโดยผู้ให้บริการภายนอก เพราะการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของการประเมินความเสี่ยงเกี่ยวกับความน่าเชื่อถือของข้อมูล การปฏิบัติงาน และการปฏิบัติตามกฎระเบียบข้อบังคับ

ความซับซ้อนของหน้าที่งานด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงของเทคโนโลยี และความเชี่ยวชาญ จะผลักดันให้ CAE
ของหน่วยงานผู้ใช้งานต้องประเมินความเสี่ยงต่อธุรกิจและประสิทธิผลของการดำเนินกิจกรรมการควบคุมซึ่งดำเนินการโดยผู้ให้บริการภายนอก

การมีส่วนร่วมของผู้ตรวจสอบภายในจะแตกต่างกันโดยขึ้นอยู่กับ

1. ขีดความสามารถของผู้บริหารและโครงสร้างการกำกับดูแลที่ใช้จัดการกับความเสี่ยงของธุรกิจและเทคโนโลยีสารสนเทศ

2. ประสบการณ์ของผู้บริหารในการใช้บริการจากหน่วยงานภายนอกสำหรับกิจกรรมที่ซับซ้อนและในการบริหารโครงการขนาดใหญ่
3. การมีส่วนร่วมของหน่วยงานอื่นๆ เช่น ฝ่ายบริหารความเสี่ยง
   กลุ่มงานด้านการปฏิบัติตามกฎระเบียบ (compliance groups)
   หรือหน่วยงานตรวจสอบภายในอื่นๆ
4. ลักษณะโดยทั่วไปของกิจกรรมการควบคุมที่ดำเนินการโดยผู้ให้บริการด้านเทคโนโลยีสารสนเทศ
5. ความคาดหวังของผู้มีส่วนได้เสียหลักจากการตรวจสอบภายใน

แนวทางนี้จะ

- ให้เค้าโครงเกี่ยวกับความเสี่ยงทั่วไปของการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เพื่อให้ CAE พิจารณาและกำหนดกลไกในการให้ความเชื่อมั่น
- ให้แนวทางแก่ผู้ตรวจสอบภายในเกี่ยวกับประเภทของการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกที่อาจพบได้บ่อยที่สุด
  และอธิบายวงจรที่มักใช้ในการพิจารณาการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ซึ่งประกอบด้วย 7 ขั้นตอน ดังนี้
  1. การสอดรับกันกับกลยุทธ์และการประเมินการจัดหา
     (Strategic fit and sourcing evaluation)
  2. กระบวนการตัดสินใจและเหตุผลทางธุรกิจ
     (Decision-making process and business case)
  3. กระบวนการประกาศประกวดราคาและการทำสัญญา
     (Tender process and contracting)
  4. การนำไปใช้และการถ่ายโอน
     (Implementation and transition)
  5. การติดตามดูแลและการรายงานผล
     (Monitoring and reporting)
  6. การต่อรองใหม่
     (Renegotiation)
  7. การเปลี่ยนกลับคืน
     (Reversibility)

- ให้แนวทางแก่หน่วยงานผู้ใช้งานเกี่ยวกับการพิจารณาความเสี่ยงและการควบคุมเมื่อต้องตัดสินใจใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก
- ให้แนวทางแก่ผู้ให้บริการภายนอกเกี่ยวกับการพิจารณาความเสี่ยงและการควบคุมในส่วนที่เกี่ยวกับกระบวนการการให้บริการด้านเทคโนโลยีสารสนเทศ

ภาคผนวกจะกล่าวถึงแผนการตรวจสอบวงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกและการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

แนวทางฉบับนี้จะระบุถึงความเสี่ยงและกระบวนการของการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ในขณะที่ธุรกิจต้องพึ่งพากัน
และยังมีความสัมพันธ์กับธุรกิจภายนอกและธุรกิจที่มีการต่อเชื่อมขยายตัวออกไป (“external” and “extended” business relationships) ผู้ตรวจสอบภายในอาจจะใช้ประโยชน์จากแนวปฏิบัติ “การตรวจสอบความสัมพันธ์กับธุรกิจภายนอก” (Practice Guide, Auditing External Business Relationships)

มาตรฐานการปฏิบัติงาน

2130 – การควบคุม (2130 – Control)

กิจกรรมการตรวจสอบภายในต้องช่วยให้องค์กรดำรงไว้ซึ่งการควบคุมที่มีประสิทธิผล โดยการประเมินประสิทธิผลและประสิทธิภาพของการควบคุมและโดยการส่งเสริมให้มีการปรับปรุงการควบคุมอย่างต่อเนื่อง

2130. A1

กิจกรรมการตรวจสอบภายในต้องประเมินความเพียงพอและประสิทธิผลของการควบคุมเพื่อสนองตอบต่อความเสี่ยงในการกำกับดูแล การดำเนินงานและระบบสารสนเทศขององค์กรเกี่ยวกับ

- ความน่าเชื่อถือและความถูกต้องครบถ้วนของข้อมูลสารสนเทศด้านการเงินและการดำเนินงาน
- ประสิทธิผลและประสิทธิภาพการดำเนินงานและแผนงาน
- การปกป้องคุ้มครองสินทรัพย์
- การปฏิบัติตามกฎหมาย กฎระเบียบ นโยบาย ขั้นตอนการปฏิบัติงาน และสัญญา

1 – ประเภทของการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกได้เปลี่ยนจากการใช้บริการในรูปแบบดั้งเดิม เช่น การพัฒนาระบบงานและกิจกรรมของศูนย์ให้ความช่วยเหลือด้านเทคโนโลยีสารสนเทศ (IT help desk) ไปสู่การให้บริการในระดับสูง เช่น การพัฒนาผลิตภัณฑ์ การวิจัยและพัฒนาเฉพาะทาง และการสนับสนุนงานด้านคอมพิวเตอร์แบบกระจายศูนย์ ซึ่งองค์กรต่างๆ ได้มีการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกอย่างต่อเนื่อง เนื่องจากมีเทคโนโลยีใหม่ๆ เกิดขึ้น

ในบางครั้ง คำว่า “การใช้บริการจากหน่วยงานภายนอก (outsourcing)” ก็สับสนกับคำว่า “การดำเนินการในต่างประเทศ (off-shoring)” ซึ่งความแตกต่างคือ

การใช้บริการจากหน่วยงานภายนอก (outsourcing) คือ การทำสัญญากับหน่วยงานผู้ให้บริการภายนอกเกี่ยวกับการปฏิบัติงานทางธุรกิจเฉพาะอย่างหรืองานที่เกี่ยวข้องกับความรู้เฉพาะทาง

การดำเนินการในต่างประเทศ (off-shoring) คือ โยกย้ายกิจกรรมที่เคยดำเนินการภายในประเทศไปยังต่างประเทศ

ขอบเขตของแนวทางฉบับนี้จะเกี่ยวข้องกับการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ไม่ว่าจะอยู่ในประเทศหรือต่างประเทศ อย่างไรก็ตาม ในการจัดทำเหตุผลทางธุรกิจที่จะใช้บริการจากภายนอก ควรพิจารณาความเสี่ยงของผู้ให้บริการในประเทศเปรียบเทียบกับผู้ให้บริการในต่างประเทศ แนวทางฉบับนี้ไม่สามารถประยุกต์ใช้ได้กับกิจกรรมการดำเนินการในต่างประเทศ (off-shoring) แม้ว่าการพิจารณาในหลายประเด็นอาจคล้ายคลึงกัน

การบริการด้านเทคโนโลยีสารสนเทศทั่วๆ ไปจะรวมถึง:

- การพัฒนาและบำรุงรักษาระบบงาน (application development and maintenance)
- การบริหารโครงสร้างพื้นฐาน (infrastructure management)
- ศูนย์บริการให้ความช่วยเหลือ (help desk)
- การทดสอบและการตรวจสอบความถูกต้องสมเหตุสมผลโดยอิสระ (independent testing and validation)
- การบริหารศูนย์คอมพิวเตอร์ (data center management)
- การบูรณาการระบบ (systems integration)
- การวิจัยและพัฒนา (R&D)

- การบริหารการรักษาความมั่นคงปลอดภัย (managed security)
- การประมวลผลแบบกลุ่มเมฆ (cloud computing)

อย่างไรก็ดี
ผู้ให้บริการภายนอกและหน่วยงานผู้ใช้งานอาจเรียกชื่อประเภทของกิจกรรมการใช้บริการจากหน่วยงานภายนอกแตกต่างกัน นอกจากนี้
หน่วยงานผู้ใช้งานอาจใช้บริการจากหน่วยงานภายนอกเพียงบริการเดียวหรือมากกว่านั้น
จากผู้ให้บริการหลายรายก็ได้

การพัฒนาและบำรุงรักษาระบบงาน

เมื่อมีการใช้บริการจากหน่วยงานภายนอก
ในงานพัฒนาซอฟต์แวร์ระบบงานและบางส่วนของซอฟต์แวร์ระบบงานหรือโมดูล
หน่วยงานผู้ใช้งานควรใช้บริการจากบริษัทพัฒนาซอฟต์แวร์ภายนอกที่มีความชำนาญทางเทคนิค
มีความรู้และประสบการณ์ในการพัฒนาระบบงานที่ตรงกับข้อกำหนดคุณลักษณะที่ลูกค้าต้องการ
การเขียนโปรแกรมควรเป็นไปตามระเบียบวิธีในวงจรการพัฒนาซอฟต์แวร์ (software development life cycle: SDLC) อย่างเคร่งครัด
ซึ่งกำหนดขึ้นเป็นส่วนหนึ่งของกระบวนการที่จะทำให้มั่นใจได้ถึงคุณภาพงานที่ได้มาตรฐานของผู้ให้บริการภายนอก ในบางกรณี ขั้นตอนในวงจรการพัฒนาซอฟต์แวร์อาจได้รับการกำหนด ติดตามดูแล
และจัดการโดยหน่วยงานผู้ใช้งานโดยตรง ความต้องการของผู้ใช้บริการหรือรายละเอียดของงาน (work statement) ควรได้รับการระบุอย่างชัดเจนตั้งแต่เริ่มแรกในขั้นตอนการพัฒนา
และพิจารณาการมีส่วนร่วมของผู้ตรวจสอบภายใน ตามที่แนะนำไว้ใน GTAG 12: Auditing IT Project เพื่อ

- ให้คำแนะนำอย่างต่อเนื่องตลอดโครงการเชิงกลยุทธ์
- ระบุความเสี่ยงและปัญหาที่สำคัญแต่เนิ่นๆ

โดยส่วนมาก กระบวนการ SDLC จะเสร็จสิ้นลงด้วยการทดสอบโดยผู้ใช้ จนเป็นที่ยอมรับ (user acceptance testing) ถึงแม้ว่าผู้ให้บริการอาจรับผิดชอบจนถึงเพียงแค่ขั้นตอนการทดสอบในส่วนย่อย (unit testing) เท่านั้น ระบบ การบูรณาการระบบ และขั้นตอนการทดสอบโดยผู้ใช้
เป็นองค์ประกอบที่จำเป็นที่จะทำให้มั่นใจได้ว่าระบบนั้นตอบสนองความต้องการของลูกค้า
การทดสอบอาจดำเนินการโดยทีมลูกค้าหรือโดยลูกค้าและผู้ให้บริการภายนอกร่วมกัน ไม่ว่าจะในกรณีใด ปัญหาหรือประเด็นใดๆ
ก็ตามที่พบในขั้นตอนการทดสอบจะถูกแจ้งกลับไปยังผู้ให้บริการภายนอกเพื่อดำเนินการแก้ไข

การบำรุงรักษาระบบงานที่ใช้อยู่ในปัจจุบันที่ดำเนินการอย่างต่อเนื่อง และการยกระดับระบบงานควรตอบสนองต่อข้อเสนอแนะในการพัฒนาซอฟต์แวร์จากผู้ใช้ในกระบวนการทางธุรกิจและผู้มีส่วนได้เสีย โดยข้อเสนอแนะอาจเป็นการเปลี่ยนแปลงเพียงเล็กน้อย เช่น การสร้างฟิลด์ (field) หรือรายงานใหม่ หรืออาจเป็นการเปลี่ยนแปลงครั้งใหญ่ เช่น การสร้างโมดูลใหม่

การบริหารโครงสร้างพื้นฐาน

การบริการที่เกี่ยวข้องกับการบริหารและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศนั้นถือเป็นการบริหารโครงสร้างพื้นฐานทั้งสิ้น การบริการเหล่านี้รวมถึงการจัดการเครือข่าย การบำรุงรักษาผลการดำเนินงานและสภาพพร้อมใช้งานของระบบโครงสร้างพื้นฐานในภาพรวม กลยุทธ์และขีดความสามารถในการฟื้นตัวจากเหตุภัยพิบัติ การค้นหาสาเหตุเพื่อแก้ไขข้อขัดข้อง การบำรุงรักษาฐานข้อมูล และบริการสำรองข้อมูลและกู้คืน
นอกจากนี้ยังมีการให้บริการประเภทนี้ที่ทันสมัยและมีมูลค่าเพิ่มมากขึ้น ได้แก่ การติดตามดูแลกิจกรรมโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการบริหารขีดความสามารถ การวิเคราะห์การหยุดชะงักของระบบ (downtime) และการรายงานความล้มเหลวที่ร้ายแรงของระบบและผลกระทบที่ตามมา

ศูนย์บริการให้ความช่วยเหลือ

บริการด้านการบำรุงรักษาต่างๆ เช่น การค้นหาสาเหตุเพื่อแก้ไขข้อขัดข้อง การสนับสนุนระบบที่ใช้งานจริง (production support) และการบริหารโครงสร้างพื้นฐาน สามารถจัดเป็นศูนย์บริการให้ความช่วยเหลือประเภทหนึ่ง ภายใต้การจัดการประเภทนี้ บุคลากรของผู้ให้บริการภายนอกจะให้ความช่วยเหลือแก่ลูกค้าเกี่ยวกับปัญหาต่างๆ ด้านเทคโนโลยีสารสนเทศ โดยอาจเป็นการให้ความช่วยเหลือหน้างาน (ได้แก่ ณ สถานที่ทำงานของลูกค้า) หรือนอกสถานที่ (ได้แก่ จากสถานที่ทำงานของผู้ให้บริการเอง) จึงต้องมีการกำหนดระยะเวลานับตั้งแต่เกิดปัญหาจนสามารถแก้ไขและกลับมาใช้งานได้อีก (turn-around time - TAT) (ได้แก่ การตอบสนองและการแก้ไขปัญหา) ไว้สำหรับแต่ละระดับของการบริการ

การปฏิบัติอย่างเคร่งครัดตามระดับการให้บริการประกอบด้วยการบรรลุตามข้อกำหนดระยะเวลานับตั้งแต่เกิดปัญหาจนสามารถแก้ไขและกลับมาใช้งานได้อีกและคุณภาพของการให้บริการ นอกจากนี้ยังมีการกำหนดความคาดหวังของผู้บริหารเพื่อใช้สำหรับขั้นตอนการติดตามดูแลอย่างต่อเนื่อง

ซึ่งจะวัดผลและเปรียบเทียบผลการดำเนินงานจริงกับระดับการให้บริการที่คาดหวังไว้ ในท้ายที่สุดแล้ว ผลการปฏิบัติงาน ข้อบกพร่อง และการแก้ไข
ควรนำมาใช้เป็นเกณฑ์หลักในการประเมินผู้ให้บริการอย่างต่อเนื่อง

การทดสอบและการตรวจสอบความถูกต้องสมเหตุสมผลโดยอิสระ

หลายองค์กรมีการใช้บริการจากหน่วยงานภายนอกในการทดสอบและการตรวจสอบความถูกต้องสมเหตุสมผลของซอฟต์แวร์ที่พัฒนาขึ้นภายในองค์กรหรือโดยบุคคลภายนอก
การทดสอบที่เฉพาะเจาะจงกับระบบที่พัฒนาขึ้นเป็นวิธีการที่ใช้เพื่อการติดตามดูแลผลการดำเนินงานของระบบ ระบุและติดตามข้อผิดพลาดหรือปัญหาของโปรแกรมเพื่อการแก้ไข

การบริหารศูนย์คอมพิวเตอร์

ในขณะที่มีภาคอุตสาหกรรมด้านเทคโนโลยีสารสนเทศ ผู้ขาย
และผู้ให้บริการเข้าสู่ตลาดเพิ่มมากขึ้น
ความคิดเกี่ยวกับการใช้บริการจากหน่วยงานภายนอกก็ได้เปลี่ยนแปลงไป
วัตถุประสงค์ของการใช้บริการจากหน่วยงานภายนอกได้เปลี่ยนจากมุ่งหวังการประหยัดต้นทุนไปสู่การยกระดับประสิทธิภาพการดำเนินงานที่สูงขึ้น ผลิตภัณฑ์เฉพาะทาง และการเติบโตอย่างมีพลวัต
ผู้ให้บริการเริ่มเสนอบริการในลักษณะที่ต้องอาศัยความชำนาญเฉพาะทาง
ที่สามารถนำมาใช้กับลูกค้ามากราย โดยไม่ต้องคำนึงว่าลูกค้าจะอยู่ในภาคอุตสาหกรรมใด
ตัวอย่างหนึ่งของบริการดังกล่าวคือ การใช้การปฏิบัติการด้านศูนย์คอมพิวเตอร์

โดยปกติแล้ว ศูนย์คอมพิวเตอร์ในปัจจุบันให้บริการต่อไปนี้:

- ให้บริการพื้นที่สำหรับติดตั้งเครื่องเมนเฟรมและเครื่องแม่ข่ายแบบกระจาย (distributed servers) และสินทรัพย์ด้านเทคโนโลยีสารสนเทศอื่นๆ
- การวางแผน การกำหนดคุณลักษณะ (specification) การจัดซื้อ การติดตั้ง การกำหนดค่าการทำงาน (configuration) การบำรุงรักษา การยกระดับ (upgrade) และการบริหารจัดการ ด้านฮาร์ดแวร์ ซอฟต์แวร์ และระบบปฏิบัติการ
- การติดตามดูแลผลการทำงานและสถานะการปฏิบัติการของเครื่องแม่ข่ายอย่างต่อเนื่อง
- การบริหารขีดความสามารถของเครื่องแม่ข่ายและเมนเฟรม รวมถึงการวางแผนขีดความสามารถ การบริหารความสมดุลของระบบงาน (load balancing) การปรับแก้ และการปรับค่าการทำงานใหม่

- งานสร้างเครื่องแม่ข่าย (server builds) รวมทั้งการติดตั้งและยกระดับซอฟต์แวร์ระบบงาน ซึ่งเป็นไปตามขั้นตอนการนำออกใช้ (release procedures) ที่ลูกค้าและผู้ให้บริการภายนอกได้ตกลงกันไว้
- การสำรองข้อมูลและการกู้คืน
- การกู้ระบบเครื่องแม่ข่ายเมื่อเกิดภัยพิบัติให้เป็นไปตามระยะเวลาที่กำหนดนับตั้งแต่เกิดปัญหา จนสามารถแก้ไขและกลับมาใช้งานได้อีก

การบูรณาการระบบ

ในสภาพแวดล้อมที่มีลักษณะเป็นแบบกระจายศูนย์ หน้าที่งานต่างๆ อาจได้รับการจัดการโดยใช้ระบบ (systems) และระบบงาน (applications) ที่มากกว่าหนึ่งระบบที่อาจไม่เชื่อมต่อกัน ดังนั้น ในสภาพแวดล้อมแบบกระจายศูนย์ จึงจำเป็นต้องใช้บุคลากรเข้ามาเกี่ยวข้องมากกว่าในการทำให้ระบบและระบบงานเป็นปัจจุบัน หาสาเหตุสำหรับผลแตกต่างที่พบ (clear out-of-balance conditions) นำข้อมูลเข้า (data sources) รวมถึงค้นหาผลลัพธ์ที่ผิดพลาด

การให้บริการเพื่อบูรณาการระบบ (system integration) เป็นเรื่องเกี่ยวกับการพัฒนาสคริปต์ (script) โมดูล เครื่องมือ หรือโปรแกรมต่างๆ เพื่อบูรณาการระบบงานและระบบที่หลากหลาย ซึ่งจะทำให้ระบบงานที่มีอยู่สามารถสื่อสารกับระบบอื่นๆ ได้เสมือนมีการเชื่อมต่อกัน ผลก็คือ เป็นการทำงานรวมเป็นระบบเดียว อย่างไรก็ดี ข้อจำกัดหลักของการบูรณาการระบบคือ การที่ระบบต้องสามารถทำงานร่วมกัน (interoperability) และความถูกต้องเป็นจริงของแหล่งข้อมูล

การวิจัยและพัฒนา

บริษัทจำนวนมากใช้บริการจากหน่วยงานภายนอกในการการวิจัยและพัฒนาเทคโนโลยี วิธีการแก้ปัญหา กระบวนการ และระบบต่างๆ เพื่อปรับตัวและสร้างสรรค์สิ่งใหม่ไว้ตอบสนองความต้องการของตลาด และพร้อมกันนั้นก็เพื่อสร้างและรักษาคลังข้อมูลอัจฉริยะทางธุรกิจ (business intelligence database) นอกจากนี้ การใช้บริการจากหน่วยงานภายนอกด้านการวิจัยยังรวมถึง การใช้บริการจากผู้ให้บริการที่เป็นบุคคลภายนอกในการวิเคราะห์ตลาดซึ่งจะระบุแนวโน้มและการตอบสนองของภาคอุตสาหกรรมหลักสำหรับผลิตภัณฑ์บางประเภท

การบริหารการรักษาความมั่นคงปลอดภัย (Managed Security)

องค์กรจำนวนมากใช้บริการด้านการรักษาความมั่นคงปลอดภัยจากหน่วยงานภายนอก ซึ่งเรียกว่า Managed Security Services: MSS
เนื่องจากเป็นการบริหารข้อกำหนดด้านความมั่นคงปลอดภัยของบุคคลภายนอก MSS หมายถึง การบริการดูแลความมั่นคงปลอดภัยขององค์กรในเรื่องโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศทั้งหมด สินทรัพย์ข้อมูล และกิจกรรมการจัดการด้านผู้ใช้งาน นอกจากนี้ ยังมีศัพท์อื่นๆ ซึ่งใช้เรียกหน้าที่งานนี้ รวมถึง การบริการรักษาความมั่นคงปลอดภัยบนอินเทอร์เน็ต (Internet security services)
การใช้บริการด้านการรักษาความมั่นคงปลอดภัยจากหน่วยงานภายนอก (security outsourcing)
การบริการให้ข้อมูลแบบอัจฉริยะ (intelligence service)
การบริการให้คำปรึกษาด้านการรักษาความมั่นคงปลอดภัย (security consulting services)
การบริการด้านการรักษาความมั่นคงปลอดภัยของเครือข่าย (network security services)
การบริการด้านการจัดการการรักษาความมั่นคงปลอดภัย (security management services)
บริการประเมินความมั่นคงปลอดภัย (security assessment services)
ที่ปรึกษาด้านการรักษาความมั่นคงปลอดภัย (security consulting)
และการบริการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security services) เป็นต้น

เงื่อนไขของสัญญาจะขึ้นอยู่กับความต้องการของลูกค้า
โดยอาจรวมถึงการใช้บริการในการออกแบบและสนับสนุนสถาปัตยกรรมความมั่นคงปลอดภัยตั้งแต่ต้นจนจบ (เช่น การให้คำปรึกษาด้านการออกแบบ การนำไปใช้ การบริหารความมั่นคงปลอดภัย
การบริหารจัดการผู้ใช้ (user provisioning) และการสนับสนุนด้านเทคนิค เป็นต้น)
หรือการจัดการหน้าที่งานเฉพาะด้านความมั่นคงปลอดภัยบนระบบเฉพาะ (เช่น การติดตามดูแลไฟร์วอลล์ การส่งข้อมูล การกลั่นกรองเนื้อหา การป้องกันไวรัส การสืบค้นและการตอบสนองการบุกรุก
การประเมินช่องโหว่ของเครือข่าย เป็นต้น)

การประมวลผลแบบกลุ่มเมฆ (Cloud Computing)

การประมวลผลแบบกลุ่มเมฆจะจัดสรรทรัพยากรที่ใช้ในการประมวลผลซึ่งสามารถเพิ่มหรือลดและมักจะเสมือนจริงเพื่อเติมเต็มความจำเป็นทางธุรกิจเมื่อมีความต้องการ
การประมวลผลแบบกลุ่มเมฆจะจัดสรรให้มีเครื่องแม่ข่าย คลังเก็บข้อมูล และสมรรถนะการประมวลผลในฐานะเป็นบริการมากกว่าจะเป็นผลิตภัณฑ์ ทรัพยากรต่างๆ ซอฟต์แวร์ และข้อมูลสารสนเทศอื่นๆ จะถูกจัดสรรอย่างมีพลวัต เช่นเดียวกับอรรถประโยชน์บนเครือข่าย ซึ่งโดยมากก็คือบนอินเทอร์เน็ต
ประเภทการให้บริการประมวลผลแบบกลุ่มเมฆ ได้รวมถึงการให้บริการประมวลผลแบบกลุ่มเมฆส่วนบุคคล (private cloud) การให้บริการประมวลผลแบบกลุ่มเมฆแบบสาธารณะ (public cloud)
การให้บริการประมวลผลแบบกลุ่มเมฆแบบผสม (hybrid cloud)

หรือการให้บริการประมวลผลแบบกลุ่มเมฆแบบเครือข่ายเฉพาะกลุ่ม (community cloud) หรือบริการใดบริการหนึ่งหรือมากกว่า ดังต่อไปนี้ บริการซอฟต์แวร์ (software-as-a-service: SaaS) บริการโครงสร้างพื้นฐานคอมพิวเตอร์ (infrastructure-as-aservice: IaaS) บริการแพลตฟอร์ม: สภาวะแวดล้อมที่ประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ระบบหนึ่ง (platform-as-a-service: PaaS).

การประมวลผลแบบกลุ่มเมฆเอื้อให้ธุรกิจมีความยืดหยุ่นในการปรับตัวให้เข้ากับตลาดและสร้างสรรค์สิ่งใหม่ หรือโครงการใหม่ๆ
โดยไม่ต้องซื้อและรักษาไว้ซึ่งขีดความสามารถด้านเทคโนโลยีสารสนเทศที่มีราคาแพง
ข้อพิจารณาอีกประการหนึ่งสำหรับการประมวลผลแบบกลุ่มเมฆคือ
ความสามารถที่จะทดแทนการจ่ายซื้อทรัพย์สินเป็นของตนเองโดยใช้เงินจำนวนมากด้วยรูปแบบการจ่ายเมื่อใช้ (pay-for-use model)

2 – วงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก – การพิจารณาความเสี่ยงและการควบคุม

สำหรับหน่วยงานผู้ใช้งาน

ในบทนี้จะกล่าวถึงความเสี่ยงและขั้นตอนที่ผู้บริหารของหน่วยงานผู้ใช้งานจะต้องดำเนินการในการใช้บริการจากหน่วยงานภายนอกในงานหรือหน้าที่งานใดๆ
การใช้บริการจากหน่วยงานภายนอกอาจเป็นผลจากข้อพิจารณาในการวางแผนธุรกิจเชิงกลยุทธ์หรือยุทธวิธี อย่างไรก็ตาม ก่อนทำข้อผูกพันการใช้บริการจากหน่วยงานภายนอก
ฝ่ายบริหารควรกำหนดให้ชัดเจนถึงหน่วยงานที่เป็นเจ้าของงาน เป้าหมายทางธุรกิจ
และความสอดคล้องกับแผนกลยุทธ์
การตัดสินใจใช้บริการจากหน่วยงานภายนอกควรมีเหตุผลทางธุรกิจสนับสนุน
ซึ่งประกอบด้วยการประเมินผลตอบแทนจากการลงทุนและความเสี่ยงพื้นฐานต่อประโยชน์ที่จะได้รับจริง รวมทั้งความเสี่ยงของการนำไปใช้และการดำเนินการถ่ายโอน
บ่อยครั้งที่ความเสี่ยงในการใช้บริการจากหน่วยงานภายนอกไม่ได้รับการพิจารณาอย่างเต็มที่และไม่มีการวัดระดับอย่างโปร่งใส

ในบทนี้จะเน้นวงจรการใช้บริการจากหน่วยงานภายนอก
กระบวนการที่สนับสนุนการตัดสินใจใช้บริการจากหน่วยงานภายนอก
และกิจกรรมหลักในแต่ละระยะของผู้บริหาร โดยระยะต่างๆ ของวงจร รวมถึง

- การพิจารณาถึงการสอดรับกันกับกลยุทธ์และการประเมินการจัดหา
- กระบวนการตัดสินใจและเหตุผลทางธุรกิจ
- กระบวนการประกาศประกวดราคาและการทำสัญญา
- การนำไปใช้และการถ่ายโอน
- การติดตามดูแลและรายงานผล
- การต่อรองใหม่
- การเปลี่ยนกลับคืน

ในตอนท้ายของบทนี้ อ้างถึง ตาราง 1
(วงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก:
ความเสี่ยงและการมีส่วนร่วมของของผู้ตรวจสอบในแต่ละขั้นตอน)
ซึ่งให้รายละเอียดความเสี่ยงที่เกี่ยวข้องในแต่ละขั้นตอนและโอกาสในการมีส่วนร่วมของผู้ตรวจสอบโดยคำนึงถึงความเสี่ยงเหล่านั้น

การสอดรับกันกับกลยุทธ์และการประเมินการจัดหา

เข้าใจบริบทธุรกิจและปัจจัยขับเคลื่อนซึ่งเป็นตัวกำหนดบทบาทของผู้ให้บริการภายนอกให้สอดรับกับกลยุทธ์ขององค์กร

- กลยุทธ์ขององค์กรเป็นปัจจัยขับเคลื่อนหลักของการพิจารณาใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกหรือไม่
  หรือการใช้บริการจากหน่วยงานภายนอกเป็นกลยุทธ์ด้านเทคโนโลยีสารสนเทศที่จะส่งเสริมนวัตกรรมและทำให้ธุรกิจสามารถแก้ปัญหาได้แบบก้าวกระโดด
  โดยอาศัยขีดความสามารถด้านเทคโนโลยีสารสนเทศในตลาด
  ซึ่งหาไม่ได้จากการพัฒนาภายในองค์กรอย่างเดียว โดยปกติแล้ว
  กลยุทธ์การใช้บริการจากหน่วยงานภายนอก
  อาจต้องการการกำกับดูแลและมีผลกระทบต่อการกำหนดและติดตามความรับผิดชอบผลงานตามหน้าที่ที่แตกต่างกัน
  ขึ้นอยู่กับกลยุทธ์ดังกล่าวถูกผลักดันจากความจำเป็นขององค์กรหรือของเทคโนโลยีสารสนเทศ
- เข้าใจปัจจัยขับเคลื่อนหลัก
  - การลดต้นทุนจากความประหยัดเชิงขนาดของผู้ให้บริการ
  - ประสิทธิผลที่เพิ่มขึ้นของกระบวนการโดยอาศัยความเชี่ยวชาญและการลงทุนในบริการของผู้ให้บริการ
  - ความท้าทายด้านบุคลากร/ระดับทักษะ
    เพราะเป็นเรื่องยากที่จะรักษาและบริหารความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศภายในองค์กร
- ทางเลือกใดบ้างที่มีในตลาด
  ระดับขีดความสามารถของหน่วยงานผู้ใช้งาน
  รวมถึงประสบการณ์จริงในอดีตเกี่ยวกับการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก อยู่ในระดับใด
- องค์กรพร้อมที่จะพิสูจน์ว่าแนวคิดนั้นตรงตามวัตถุประสงค์หรือเป็นรายแรกในตลาดหรือไม่
  หรือเป็นการเสี่ยงเกินไป
- จำนวนผู้ให้บริการ หรือ “อัตราความอยู่รอดของผู้ให้บริการ”
  เพียงพอที่จะหลีกเลี่ยงการพึ่งพาผู้ให้บริการรายเดียวหรือไม่

- กระบวนการมีความสำคัญเชิงกลยุทธ์มากเกินไปที่จะใช้บริการจากหน่วยงานภายนอกหรือไม่ กิจกรรมด้านเทคโนโลยีสารสนเทศบางอย่างอาจเป็นข้อได้เปรียบทางการแข่งขันที่สำคัญยิ่งของบางองค์กร
- มีการกำหนดความต้องการตามแบบจำลองและการเชื่อมโยงกับกระบวนการทางธุรกิจเพื่อสร้างเกณฑ์พื้นฐาน กำหนดขอบเขตและเกณฑ์เปรียบเทียบหรือไม่
- ใครควรจะเป็นผู้สนับสนุนการวิเคราะห์ เป็นเจ้าของความสัมพันธ์ และมีส่วนร่วมในการพัฒนาเหตุผลทางธุรกิจ

ข้อพิจารณาในการตรวจสอบภายใน

- ประเมินบริบทเชิงกลยุทธ์และพิจารณาว่าเกณฑ์เปรียบเทียบและข้อมูลสนับสนุนอื่นๆ ทางการตลาดมีความน่าเชื่อถือและสมบูรณ์หรือไม่
- พิจารณาว่ามีกระบวนการกำกับดูแลด้านเทคโนโลยีสารสนเทศเพียงพอที่จะให้แนวทางในการพิจารณาการใช้บริการจากหน่วยงานภายนอกและความสอดคล้องกับเป้าหมายทางธุรกิจในการใช้บริการจากหน่วยงานภายนอกหรือไม่
- ยืนยันว่าการมีส่วนร่วมของผู้มีส่วนได้เสียและเจ้าของกระบวนการมีความชัดเจนและสอดคล้องกันหรือไม่
- พิจารณาฐานลูกค้า ประสบการณ์ และชื่อเสียงในแง่ความน่าเชื่อถือของผู้ให้บริการภายนอก

กระบวนการตัดสินใจ – เหตุผลทางธุรกิจ

การเลือกใช้บริการจากหน่วยงานภายนอกควรมีความสมเหตุสมผลเชิงธุรกิจในระยะยาวและสร้างคุณค่าโดยอยู่บนพื้นฐานของข้อมูลและการคาดการณ์ที่มีความน่าเชื่อถือ (ได้แก่ เข้าใจในความเสี่ยง)

- จัดทำเหตุผลทางธุรกิจที่สมเหตุสมผล มุ่งเน้นถึงประโยชน์และความเสี่ยงหลัก การใช้บริการจากหน่วยงานภายนอกอาจเป็นทางออกในการรับมือกับความเสี่ยงของธุรกิจ หรืออาจก่อให้เกิดความเสี่ยงใหม่ให้ธุรกิจ แต่การประเมินผลควรจะรวมถึงความเสี่ยงในการนำไปใช้และผลกระทบที่อาจเกิดขึ้นถ้าการทำข้อตกลงการใช้บริการจากหน่วยงานภายนอกล้มเหลว
- ทำให้มั่นใจว่า ผู้สนับสนุนและผู้มีส่วนได้เสียหลักได้มีส่วนร่วมและพิจารณาตัดสินใจในขั้นสุดท้าย
- พิจารณาทางเลือกหรือตัวแปรอื่นๆ โดยควรเลือกทางออกที่ได้ประโยชน์สูงสุด คือ มีการตัดสินใจในรายละเอียดมากกว่าแค่เพียงจะใช้หรือไม่ใช้บริการจากหน่วยงานภายนอก

- เคารพในข้อกำหนดการกำกับดูแลภายใน (internal governance mandates)
  โดยระดับความเสี่ยงขั้นสุดท้ายที่ยอมรับได้ควรจะสอดคล้องกับความเสี่ยงที่องค์กรยอมรับได้
- พิจารณาข้อกำหนดในการบริหารการเปลี่ยนแปลง
  มีการสร้างสภาพแวดล้อมภายในองค์กรอย่างไรเพื่อทำให้เกิดสภาพแวดล้อมของการใช้บริการจากภายนอก (เช่น การเปลี่ยนแปลงนโยบายต่างๆ ขั้นตอนการปฏิบัติงาน
  และการสนับสนุนในเรื่องโครงสร้างพื้นฐาน)

ข้อพิจารณาในการตรวจสอบภายใน

- ประเมินว่าข้อมูลในการวิเคราะห์รายละเอียดน่าเชื่อถือหรือไม่และพิจารณาความเสี่ยงเชิงธุรกิจและความเสี่ยงในการนำไปใช้ทั้งหมด
- ยืนยันว่าการกำกับดูแลและกระบวนการอนุมัติโปร่งใส ได้รับการจัดทำเป็นลายลักษณ์อักษรและสมบูรณ์หรือไม่
- พิจารณาว่าผู้ที่เกี่ยวข้องและผู้เชี่ยวชาญที่เหมาะสมได้มีส่วนร่วมในกระบวนการประเมินหรือไม่
- พิจารณาว่าผู้มีส่วนได้เสียหลักอื่นๆ ได้รับทราบข้อมูลอยู่ตลอดเวลาหรือไม่
- ประเมินแผนสำรองฉุกเฉินของผู้บริหาร
  หากการใช้บริการจากหน่วยงานภายนอกล้มเหลวในขั้นตอนต่างๆ
- ประเมินว่าประมาณการความล้มเหลวและผลกระทบ/ค่าใช้จ่ายที่อาจเกิดขึ้นได้รับการพิจารณาในเหตุผลทางธุรกิจ หรือเมื่อเปรียบเทียบทางเลือกต่างๆ ในระหว่างผู้ให้บริการภายนอกหรือไม่
- ประเมินการตอบสนองของค่าใช้จ่าย/ประโยชน์ ต่อ สมมติฐาน
- กำหนดตัวชี้วัดหลักและแหล่งข้อมูล

กระบวนการประกาศประกวดราคาและการทำสัญญา

ดำเนินการเพื่อเชิญชวนให้ยื่นข้อเสนอประกวดราคา คัดเลือกผู้ให้บริการ
และกำหนดเงื่อนไขในสัญญาให้เป็นไปตามเหตุผลทางธุรกิจ

- พัฒนารายละเอียดขอบเขตงานเพื่อให้ผู้ให้บริการสามารถเสนอราคาที่มีรายละเอียดข้อมูลและเสนอจุดเด่นที่สำคัญอื่นๆ ได้
- ประเมินการเสนอราคาตามเกณฑ์ที่เกี่ยวข้องซึ่งใช้กันโดยทั่วไปในเหตุผลทางธุรกิจต่างๆ
  หรือข้อพิจารณาที่เฉพาะเจาะจงตามความจำเป็น
- พิจารณารายละเอียดความเสี่ยงใหม่ๆ ที่เกิดขึ้น หรือความเบี่ยงเบนที่มีนัยสำคัญใดๆ
  จากเหตุผลทางธุรกิจที่ได้รับอนุมัติ

- เลือกผู้ให้บริการตามเกณฑ์และการเสนอราคา/ข้อเสนอที่ได้ยื่นมา
- จัดทีมพนักงานที่มีประสบการณ์เพื่อตรวจสอบความถูกต้องเป็นจริงของประวัติการดำเนินการ (operational due diligence review) และทำให้มั่นใจว่า ตัวชี้วัดหลัก อันได้แก่ ข้อตกลงสำหรับระดับการให้บริการ (SLAs) และข้อตกลงสำหรับระดับการปฏิบัติการ (operational level agreements: OLAs) ได้มีการกำหนดไว้ในสัญญาแล้ว
- ประเมินโอกาสที่จะสูญเสีย ใช้การไม่ได้ และผลลัพธ์ที่ไม่เป็นไปตามที่กำหนด พิจารณาถึงความเสี่ยงสูงสุดที่ยอมรับได้ และสิ่งที่จะเกิดขึ้น [สิทธิไล่เบี้ย (recourse)] เมื่อเกิดเหตุการณ์ต่างจากที่คาดไว้
- ให้ผู้สนับสนุนลงนามรับรอง และแจ้งให้ผู้มีส่วนได้เสียหลักทราบ โดยเน้นย้ำถึงสิ่งที่เบี่ยงเบนไปหรือความเสี่ยงใหม่ๆ รวมทั้งสอบทานการปฏิบัติตามข้อกำหนดด้านกฎหมายและขั้นตอนที่จำเป็นทางกฎหมายเพื่อให้ได้สัญญาที่มีผลผูกพัน (รวมทั้งกลยุทธ์และแผนการออกจากสัญญา ในกรณียกเลิกหรือไม่ต่อสัญญา)

ข้อพิจารณาในการตรวจสอบภายใน

- ประเมินกระบวนการประเมินการเสนอราคา เงื่อนเวลา เกณฑ์ที่ใช้ตัดสิน ความครบถ้วนและความโปร่งใสในการอนุมัติ
- สอบทานข้อกำหนดเพื่อความมั่นใจด้านการควบคุมของผู้บริหาร เช่น รายงานของผู้ตรวจสอบสำหรับการให้บริการ [เช่น Statement on Standards for Attestation Engagements (SSAE) No. 16: Reporting on Controls at a Service Organization ซึ่งออกโดย The American Institute of Certified Public Accountants (AICPA) หรือ International Standard on Assurance Engagements (ISAE) 3402 ซึ่งออกโดย International Accounting and Assurance Standards Board (IAASB) ของ International Federation of Accountants (IFAC)] หรือ การประเมินอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีการยกร่างข้อความที่ระบุสิทธิขององค์กรในการตรวจสอบการให้บริการ (right to audit clause) อย่างมีประสิทธิผล
- ประเมินประสบการณ์และขีดความสามารถของบุคลากรในโครงการ ตลอดจนประเมินว่ามีการจัดการทรัพยากรอย่างเหมาะสมตรงตามความจำเป็นหรือไม่
- ประเมินว่าหน้าที่งานด้านการบริหารความเสี่ยง กฎหมาย ทรัพยากรบุคคล และการเงิน ได้เข้ามามีส่วนร่วมตามความจำเป็นหรือไม่

- ดำเนินการสอบทานความถูกต้องเป็นจริงของประวัติการดำเนินการหรือประเมินการสอบทานการปฏิบัติงานของผู้ให้บริการโดยผู้บริหารของหน่วยงานผู้ใช้บริการ
- พิจารณาการประเมินอย่างต่อเนื่องหรือเป็นระยะๆ โดยผู้ตรวจสอบภายนอกรายอื่น เพื่อเพิ่มความมั่นใจในความมีประสิทธิผลของการควบคุมขีดความสามารถในการดำเนินงาน สอบทานข้อตกลงสำหรับระดับการให้บริการ (SLAs) และข้อตกลงสำหรับระดับการปฏิบัติการ (OLAs) เพื่อให้มั่นใจว่าตัววัดผลการดำเนินงานได้รับการกำหนดไว้และมีความน่าเชื่อถือ การดำเนินการดังกล่าวควรเริ่มจากผู้บริหาร อย่างไรก็ตาม การตรวจสอบภายในสามารถประเมินความน่าเชื่อถือด้วยการเน้นที่ความคาดหวังของผลการดำเนินงานในด้านความเสี่ยงและการควบคุม และการปฏิบัติตามมาตรฐานหลักของผู้ให้บริการหรือความต้องการเฉพาะจากลูกค้าหรือระเบียบข้อบังคับที่นำไปปรับใช้

การนำไปใช้และการถ่ายโอน

พัฒนาแผนการถ่ายโอน จัดหางบประมาณตามที่จำเป็น และจัดให้มีผู้สนับสนุนการบริหารโปรแกรม/โครงการ การสนับสนุน และทรัพยากรอื่นๆ อย่างเป็นทางการ

- กำหนดแผนงานที่เป็นทางการและกำหนดความคาดหวังด้านการกำกับดูแล เมื่อมีการใช้บริการจากหน่วยงานภายนอกในกระบวนการหรือการดำเนินงานที่มีนัยสำคัญ พิจารณารวมตารางเวลาสำหรับการกำกับดูแลไว้ในสัญญา ตั้งงบประมาณส่วนนี้รวมอยู่ในการวิเคราะห์เหตุผลทางธุรกิจ และให้มีการตรวจสอบการปฏิบัติตามข้อกำหนดของสัญญาตามระยะเวลาและวิธีการที่กำหนดไว้
- กำหนดเงื่อนเวลาในเบื้องต้น (fundamental timing) แหล่งเงินทุน วันส่งมอบ การทดสอบและการติดตามดูแลอย่างต่อเนื่อง
- พิจารณาถึงปัญหาทรัพยากรบุคคลและการปรับวัฒนธรรมองค์กรว่าเป็นปัจจัยสู่ความสำเร็จ ทั้งก่อน ในระหว่าง และหลังการถ่ายโอน
- ขอหนังสือรับรองของบุคลากรผู้ให้บริการจากหน่วยงานภายนอก องค์กรจะมั่นใจได้อย่างไรว่าบุคลากรของผู้ให้บริการมีคุณสมบัติเพียงพอที่จะทำงานที่ได้รับมอบหมายและเป็นไปตามเงื่อนไขที่ระบุไว้ในสัญญา
- บริหารการคาดการณ์ เกี่ยวกับความคลาดเคลื่อนและการไม่สามารถส่งมอบงานได้ ทั้งฝ่ายผู้ให้บริการและผู้รับบริการ เพื่อให้ครอบคลุมถึงค่าใช้จ่ายจากการหยุดชะงักซึ่งไม่ได้วางแผนไว้
- จัดทำกระบวนการให้เป็นมาตรฐานก่อนการถ่ายโอน ในการนี้อาจต้องใช้ความพยายามและการลงทุนสูง

- ดำเนินการวิเคราะห์หลังจากเริ่มใช้งานและประเด็นปัญหาที่เกี่ยวข้องในงาน ในขั้นตอนการติดตามดูแลและรายงานผล (หรือประเด็นที่จะพิจารณาในการต่อรองใหม่) เพื่อให้มั่นใจว่าการถ่ายโอนเป็นไปตามข้อตกลงและเหตุผลทางธุรกิจ

ข้อพิจารณาในการตรวจสอบภายใน

- ดำเนินการสอบทานก่อนการนำไปใช้งานเพื่อให้มั่นใจว่า โครงการเป็นไปตามข้อปฏิบัติที่เป็นมาตรฐาน
- สอบทานแผนสำรองฉุกเฉินหากการถ่ายโอนไม่เกิดผลตามที่ต้องการ
- พิจารณาว่ามีการระบุความเสี่ยงและการดำเนินการต่อความเสี่ยงนั้นหรือไม่ รวมทั้งมีการบรรเทาความเสี่ยงและแจ้งต่อผู้มีส่วนได้เสียอย่างเหมาะสมและทันที ในระหว่างกระบวนการนำไปใช้งาน
- ให้มั่นใจว่า การตัดสินใจว่า “ไปต่อ/ไม่ไปต่อ” ได้มีการกำกับดูแลอย่างเหมาะสมและตั้งอยู่บนพื้นฐานของข้อมูลที่เชื่อถือได้หรือไม่
- ประเมินว่าผู้บริหารได้ดำเนินการทดสอบอย่างเหมาะสม ก่อนอนุมัติให้ “ใช้งานจริง” หรือไม่
- พิจารณาว่าผู้มีส่วนได้เสียที่เหมาะสม มีส่วนร่วมและรับทราบหรือไม่
- พิจารณาว่าผู้บริหารโครงการและผู้บริหารระดับอาวุโสมีข้อมูลที่น่าเชื่อถือเพื่อประกอบการตัดสินใจหรือไม่

การติดตามดูแลและรายงานผล

หลังจากการถ่ายโอน
ให้ติดตามดูแลการปฏิบัติงานเพื่อให้มั่นใจว่ามีการส่งมอบงานตามข้อกำหนดทางธุรกิจ ตัวชี้วัดหลัก (KPI) และข้อตกลงสำหรับระดับการให้บริการ (SLA)
ขั้นตอนนี้จะช่วยให้มั่นใจว่าการปฏิบัติงานและการติดตามดูแลผลการดำเนินงานเป็นประโยชน์สูงสุด และเสริมกระบวนการให้ได้ผลดียิ่งขึ้น รวมทั้งเสริมสร้างความสัมพันธ์กับหน่วยงานที่ให้บริการภายนอก

- กำหนดและพัฒนาตัวชี้วัดหลักของผลการดำเนินงาน โดยควรพิจารณาและออกแบบไว้ตั้งแต่ขั้นตอนการทำสัญญาและข้อตกลงสำหรับระดับการให้บริการ (SLA) แม้ว่าจะไม่สามารถระบุไว้ล่วงหน้าได้ทั้งหมด โดยหลักการแล้ว ตัวชี้วัดควรช่วยให้มั่นใจได้ถึงการส่งมอบบริการที่จำเป็นและบ่งชี้ถึงการปฏิบัติตามและการไม่ปฏิบัติตามข้อกำหนดในสัญญา

- ได้รับความเชื่อมั่นอย่างต่อเนื่องจากแหล่งอื่นๆ
  ว่าการปฏิบัติการได้มีการควบคุมและคงไว้ซึ่งความถูกต้องครบถ้วน (ตัวอย่างเช่น SSAE 16 ISAE 3402 การสร้างความเชื่อมั่นในคุณภาพ หรือรายงานการปฏิบัติตามกฎระเบียบในการปฏิบัติการ หรือรายงานจากผู้สอบบัญชีอิสระหรือผู้ตรวจสอบภายใน)
  พิจารณาให้มีการประเมินการปฏิบัติตามสัญญาอย่างต่อเนื่องหรือเป็นระยะ
- ติดตามดูแลลักษณะ สาเหตุ และการตอบสนองของผู้ให้บริการภายนอก
  ต่อประเด็นด้านผลการดำเนินงานและด้านสัญญา
  และทำให้มั่นใจว่าความรู้เหล่านี้ได้มีการถ่ายทอดและนำไปสู่การให้บริการที่ดีขึ้นหรือการต่อรองที่เข้มงวดมากขึ้น
  บริหารความสัมพันธ์ในปัจจุบันและในอนาคตด้วยความรู้ที่ได้รับการพัฒนาขึ้นดังกล่าว
- มองหานวัตกรรมจากผู้ให้บริการภายนอกเพื่อให้มองเห็นความเสี่ยงได้อย่างชัดเจนและเพิ่มศักยภาพในการทำธุรกิจ

ข้อพิจารณาในการตรวจสอบภายใน

- เข้าใจว่าการดำเนินงานของผู้ให้บริการและการปฏิบัติตามข้อกำหนดในสัญญาจะได้รับการประเมินและสอบทานเป็นประจำโดยผู้บริหารอย่างไร
- ประเมินความน่าเชื่อถือของตัวชี้วัดซึ่งได้รับการออกแบบและใช้ในการบริหารความเสี่ยงเกี่ยวกับเทคโนโลยีสารสนเทศด้านการปฏิบัติการ การเปลี่ยนแปลง และการรักษาความมั่นคงปลอดภัย
- ประเมินว่าข้อกังวลและสิ่งที่ควรปรับปรุงจะได้รับการสื่อสารและใช้ประโยชน์ในการปรับปรุงการปฏิบัติการ/สัญญา ทั้งในปัจจุบันและในอนาคตอย่างไร
- ทำให้มั่นใจว่ากิจกรรมการใช้บริการจากหน่วยงานภายนอกเป็นส่วนหนึ่งของงานที่ควรตรวจสอบทั้งหมดและมีการประเมินความเสี่ยงอย่างสม่ำเสมอ
- พิจารณาว่ามีการทำให้ผู้ตรวจสอบภายในรับทราบถึงการเปลี่ยนแปลงความสัมพันธ์ในอนาคตอย่างไร
- ประเมินผลการดำเนินงานกับตัวชี้วัด (KPI) ซึ่งได้กำหนดไว้ตั้งแต่ขั้นตอนการวางแผน

การต่อรองใหม่

เมื่อใกล้กำหนดที่จะหมดสัญญา ควรทำความเข้าใจถึงประโยชน์และปัญหาที่เกิดขึ้นจริง การเปลี่ยนแปลงของตลาดและเกณฑ์เปรียบเทียบ
และค่าใช้จ่ายในการนำกลับมาดำเนินการเองหรือการหาผู้ให้บริการรายใหม่

ซึ่งจะเป็นส่วนหนึ่งของการต่อรองใหม่
ทำให้มั่นใจว่ามีการนำรายงานปัญหาและเหตุการณ์ที่เกิดขึ้นมาใช้อย่างมีประสิทธิผล

- เปรียบเทียบการปฏิบัติการในสภาวะปกติกับที่กำหนดในเหตุผลทางธุรกิจเดิม และปรับสิ่งที่ได้เรียนรู้ให้สมเหตุสมผล
- ใช้เกณฑ์เปรียบเทียบกับผู้ให้บริการภายนอกรายอื่นๆ
- สำรวจทางเลือกอื่นๆ และเปรียบเทียบประโยชน์ในปัจจุบัน ต่อการนำกระบวนการกลับมาดำเนินการเอง
- ประเมินและวิเคราะห์ความเสี่ยงใหม่ๆ ค่าใช้จ่าย และประโยชน์ที่จะได้รับ
- คงไว้ซึ่งเงื่อนไขที่มีประสิทธิผลมากกว่า องค์กรควรมีทางเลือกหลายทางและเข้าใจแต่ละทางเลือกเพื่อรักษาผลประโยชน์ (ดูจากเรื่อง การเปลี่ยนกลับคืน ในหัวข้อถัดไป)

ข้อพิจารณาในการตรวจสอบภายใน

- เข้าใจกลยุทธ์และสารสนเทศที่จำเป็น เพื่อให้มั่นใจถึงการต่อรองใหม่ในอนาคตที่จะได้ประโยชน์สูงสุด
- เข้าใจการเปลี่ยนกลับคืนและการติดตามดูแลหรือผลการดำเนินงาน
- ทำให้มั่นใจว่าผู้เชี่ยวชาญและเจ้าของกระบวนการผลักดันให้เกิดการต่อรองใหม่ที่ดีขึ้น
- ทำให้มั่นใจว่าวันต่างๆ ที่กำหนดให้ผู้ตรวจสอบมีส่วนร่วมได้รับการพิจารณาอยู่ในกระบวนการประเมินความเสี่ยงประจำปี
- ทำให้มั่นใจว่ามีข้อมูลสารสนเทศในอดีตและตัวชี้วัดผลการดำเนินงานที่เพียงพอและถูกต้อง

การเปลี่ยนกลับคืน

เข้าใจว่าในการโยกย้ายการปฏิบัติการ
ไม่ว่าจะย้ายไปให้ผู้ให้บริการรายอื่นดำเนินการหรือนำกลับมาดำเนินการเอง
อาจมีค่าใช้จ่ายและเกิดการหยุดชะงัก

- ประมาณการโอกาสที่โครงการใช้บริการจากหน่วยงานภายนอกจะล้มเหลว โดยพิจารณาจากความล้มเหลวที่เคยเกิดขึ้นในอดีต
- พิจารณาค่าใช้จ่ายทั้งหมดและผลกระทบถ้าต้องนำการปฏิบัติการกลับมาดำเนินการเอง และพิจารณา “ค่าใช้จ่ายที่มีแนวโน้มจะเกิดขึ้น” (โอกาสที่จะเกิด คูณ ค่าใช้จ่าย) ของกรณีนี้ ไม่ว่าในระหว่างหรือเมื่อสัญญาสิ้นสุด

โดยพิจารณาค่าใช้จ่ายดังกล่าวในการวิเคราะห์ผลตอบแทนจากการลงทุน (ROI) ในเหตุผลทางธุรกิจ ตลอดจนในสัญญาเดิม และการต่ออรองใหม่

- เข้าใจทางเลือกอื่นๆ และทางเลือกในการเปลี่ยนกลับคืนการให้บริการบางส่วน
- เตรียมการป้องกันไว้ล่วงหน้าในสัญญาซึ่งป้องกันองค์กรจากการถูกผูกมัดในกรณีที่ผู้ให้บริการคิดค่าบริการเพิ่มขึ้นโดยปราศจากการยินยอม โดยให้ระบุในสัญญาว่าจะคิดค่าใช้จ่ายเท่าใดในขอบเขตที่เป็นไปได้ ในสภาพตลาดและปัจจัยทางเศรษฐกิจ เช่น ภาวะเงินเฟ้อ

ข้อพิจารณาในการตรวจสอบภายใน

- ประเมินความเพียงพอของแผนฉุกเฉินถ้าโครงการใช้บริการจากหน่วยงานภายนอกไม่เป็นผล
- ประเมินว่าผู้บริหารได้ประมาณตัวเลขค่าใช้จ่ายและโอกาสที่จะล้มเหลวหรือไม่
- พิจารณาว่าได้พิจารณาถึงความล้มเหลวในเหตุผลทางธุรกิจและความจำเป็นในผลตอบแทนจากการลงทุนที่ต้องการแล้วหรือไม่
- ถามผู้บริหารว่าได้พิจารณาใช้บริการจากผู้ให้บริการภายนอกรายอื่นอย่างมีประสิทธิผลเพื่อหลีกเลี่ยงการพึ่งพาที่ไม่จำเป็นหรือไม่
- พิจารณาว่าผู้บริหารประเมินอย่างไรว่าผู้ให้บริการภายนอกสามารถให้บริการได้ การตรวจสอบภายในอาจจำเป็นต้องยืนยันหรือประเมินความน่าเชื่อถือของการประเมินนั้น
- ตรวจสอบให้แน่ใจว่าจุดที่จะเริ่มหรือพิจารณาเปลี่ยนผู้ให้บริการภายนอกเป็นที่เข้าใจและได้กำหนดไว้ล่วงหน้าหรือไม่
- พิจารณาความเสี่ยงอื่นๆ ซึ่งอาจนำไปสู่ความจำเป็นที่ต้องนำกระบวนการกลับมาดำเนินการเอง รวมทั้งข้อกังวลในเชิงเศรษฐกิจมหภาค และการเมือง/สภาพภูมิศาสตร์ และพิจารณาว่าสิ่งเหล่านี้ได้มีการประเมินหรือไม่
- พิจารณาว่าผู้ให้บริการภายนอกมีความสามารถในการบริหารแผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) อย่างสมเหตุสมผลและใช้การได้อย่างต่อเนื่องหรือไม่
- พิจารณาว่าในสัญญามีข้อความการสิ้นสุดสัญญา (exit clause) ที่เหมาะสมหรือไม่

ตาราง 1: วงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก:
ความเสี่ยงและการมีส่วนร่วมของผู้ตรวจสอบในแต่ละขั้นตอน

ตารางนี้ให้รายละเอียดเกี่ยวกับความเสี่ยงต่างๆ
ที่ต้องได้รับการพิจารณาในกระบวนการตัดสินใจที่จะใช้บริการจากหน่วยงานภายนอก
หน่วยงานผู้ใช้งานมักเน้นย้ำถึงบทบาทและความรับผิดชอบเพื่อบรรเทาความเสี่ยงและกำหนดการควบคุมที่เกี่ยวข้องและจำเป็น ความเสี่ยงที่เกี่ยวเนื่องกับกิจกรรมหลัก
และประเด็นอื่นใดที่อาจต้องให้ความสนใจจะได้รับการเน้นเป็นพิเศษเพื่อให้ผู้ตรวจสอบภายในพิจารณา
ความเสี่ยงและประเด็นดังกล่าวนี้จะแตกต่างกันอย่างมากขึ้นอยู่กับระดับวุฒิภาวะขององค์กรและผู้บริหาร
(ประสบการณ์การใช้บริการจากหน่วยงานภายนอก) นอกจากนี้
ยังขึ้นอยู่กับการมีส่วนร่วมของฝ่ายบริหารความเสี่ยง สำนักงานบริหารโครงการ (project management

office – PMO) และหน่วยงานสร้างความมั่นใจอื่นๆ ด้วย CAE ควรเข้าใจความคาดหวังของคณะกรรมการ[1] และผู้มีส่วนได้เสียหลัก แต่ไม่ควรมีส่วนร่วมในกระบวนการอนุมัติ
เพื่อคงไว้ซึ่งความเป็นอิสระอย่างต่อเนื่องจากการตัดสินใจของผู้บริหารในเชิงกลยุทธ์/การปฏิบัติการ

ขั้นตอน	จุดประสงค์	กิจกรรมหลัก	บทบาท ผู้บริหาร *[2]	ความเสี่ยง	การมีส่วนร่วมของผู้ตรวจสอบ[3]

1 ตามความหมายที่ระบุไว้ในภาคคำศัพท์ของ *International Standards for the Professional Practice of Internal Audit (Standards)* "คณะกรรมการ หมายถึง คณะบุคคลที่กำกับดูแลองค์กร เช่น คณะกรรมการบริษัท (board of directors) คณะกรรมการอำนวยการ (supervisory board) หัวหน้าหน่วยงานหรือหน่วยงานที่มีอำนาจตามกฎหมาย (head of an agency or legislative body) คณะผู้ว่าการหรือทรัสตีขององค์กรที่ไม่แสวงหากำไร (board of governors or trustees of a nonprofit organization) หรือคณะกรรมการอื่นๆ ขององค์กรที่ได้รับการแต่งตั้ง รวมทั้งคณะกรรมการตรวจสอบซึ่งหัวหน้าผู้บริหารงานตรวจสอบภายในอาจต้องรายงานตามหน้าที่งาน

2 เครื่องหมาย * หมายถึง ความรับผิดชอบหลักและเป็นเจ้าของขั้นตอน

3 การมีส่วนร่วมของผู้ตรวจสอบภายในขึ้นอยู่กับความเสี่ยง ความคาดหวังของผู้มีส่วนได้เสียและของคณะกรรมการ ความสามารถของฝ่ายบริหาร และการมีส่วนร่วมของหน่วยงานสร้างความเชื่อมั่นและผู้เชี่ยวชาญ

A: การสอดรับกันกับกลยุทธ์และการประเมินการจัดหา	ระบุทางเลือกการจัดหาและกำหนดจุดเริ่มต้นของขอบเขตงาน	▪ เชื่อมโยงกับกระบวนการในรูปแบบธุรกิจ ▪ จัดอันดับทางเลือกโดยพิจารณาจากประโยชน์และความเสี่ยง ▪ พัฒนาการวิเคราะห์ตลาดและเกณฑ์เปรียบเทียบ	▪ เจ้าของกระบวนการ* ▪ ผู้เชี่ยวชาญด้านการจัดซื้อจัดจ้าง (ด้านเทคนิค ด้านความเสี่ยง ด้านแผนการดำเนินธุรกิจต่อเนื่อง (BCP) และด้านกลยุทธ์อง	▪ ไม่สอดคล้องกับกลยุทธ์องค์กร ▪ การตัดสินใจผิดพลาด ▪ สูญเสียสินทรัพย์หรือผลตอบแทนการลงทุน (ROI) ลดลง	เข้าใจบริบทเชิงกลยุทธ์และเข้าใจว่าสารสนเทศที่สนับสนุนมีความน่าเชื่อถือและสมบูรณ์ ตามความจำเป็นหรือไม่

			ค์กร) ▪ ผู้บริหารหน่วยธุรกิจ ▪ ผู้สนับสนุนระดับบริหาร		
ขั้นตอน	**จุดประสงค์**	**กิจกรรมหลัก**	**บทบาท** **ผู้บริหาร***[2]	**ความเสี่ยง**	**การมีส่วนร่วมของผู้ตรวจสอบ**[3]

B: กระบวนการตัดสินใจและเหตุผลทางธุรกิจ	จัดทำเหตุผลทางธุรกิจที่น่าเชื่อถือ	▪ วิเคราะห์ความเสี่ยงของธุรกิจและประโยชน์ที่จะได้ในรายละเอียด ▪ พิจารณาถึงความเสี่ยงของการปฏิบัติการและผลกระทบจากความล้มเหลว ▪ เลือกทางเลือกที่ดีที่สุดและให้รายละเอียดเกี่ยวกับค่าใช้จ่าย/ประโยชน์ที่จะได้ ▪ ชี้ให้เห็นถึงความสัมพันธ์ระหว่างกลยุทธ์และการกำกับดูแล	▪ เจ้าของกระบวนการ* ▪ ผู้สนับสนุนระดับบริหาร* ▪ การเงิน ▪ กฎหมาย ▪ ไอที ▪ ทรัพยากรบุคคล ▪ ผู้เชี่ยวชาญอื่นๆ	▪ ไม่ได้เลือกผู้ให้บริการที่ดีที่สุด ▪ สูญเสียสินทรัพย์ ผลตอบแทนจากการลงทุน (ROI) หรือเสียภาพลักษณ์ขององค์กรเพราะคุณภาพบริการอาจลดลง ▪ ผลกระทบเชิงลบต่อการปฏิบัติตามกฎระเบียบ	▪ ประเมินว่าข้อมูลในการวิเคราะห์โดยละเอียดน่าเชื่อถือหรือไม่ และพิจารณาความเสี่ยงเชิงธุรกิจและความเสี่ยงในการนำไปใช้ทั้งหมด ▪ พิจารณาว่าการกำกับดูแลและการอนุมัติเป็นไปอย่างโปร่งใสและน่าเชื่อถือหรือไม่ ▪ พิจารณาว่าการมอบหมายงานตรงกับหน่วยงานและผู้เชี่ยวชาญหรือไม่ รวมทั้งประเมินว่าผู้มีส่วนได้เสียหลักได้รับทราบข้อมูลอยู่ตลอดเวลาหรือไม่

ขั้นตอน	จุดประสงค์	กิจกรรมหลัก	บทบาท ผู้บริหาร *	ความเสี่ยง	การมีส่วนร่วมของผู้ตรวจสอบ
C: กระบวนการประกาศประกวดราคาและการทำสัญญา	เลือกผู้ให้บริการและออกแบบสัญญาที่นำไปสู่ความสำเร็จ	▪ ให้รายละเอียดความต้องการขอบเขตงานและหนังสือเชิญชวนให้ยื่นประกวดราคา (requests for proposals: RFP) ▪ คัดเลือกผู้ให้บริการและตรวจสอบประวัติ ▪ ต่อรองสัญญา	▪ เจ้าของกระบวนการ * ▪ ฝ่ายจัดซื้	▪ ข้อตกลงไม่ได้ให้ประโยชน์สูงสุดแก่องค์กร หรือองค์กรไม่ได้รับการปกป้องจากช่องว่างของความจำเป็นในการส่งมอบงานที่มีคุณภาพอยู่ในสภาพพร้อมใช้งาน และมีความถูกต้อง /การรักษาความลับ ▪ สูญเสียสินทรัพย์ ผลตอบแทนจากการลงทุน (ROI) หรือเสียภาพลักษณ์องค์กร ▪ ผลกระทบต่อความ	▪ พิจารณาว่ามีกระบวนการอนุมัติและการจัดซื้อจัดจ้างที่เหมาะสมหรือไม่ ▪ สอบทานสัญญาและความจำเป็นที่ผู้ให้บริการภายนอกจะต้องทำเพื่อสร้างความมั่นใจด้านการควบคุม (เช่นมาตรฐานSSAE16 หรือรายงานการตรวจสอบจากมาตรฐาน SAS70 จากผู้ให้บริการ) และประเมินว่าได้กำหนดสิทธิที่จะตรวจสอบในร่างสัญญาหรือไม่ ▪ พิจารณาว่าทีมงานของโครงการมีทักษะที่เหมาะสมหรือไม่ สอบถามว่าฝ่ายบริหารความเสี่ยง กฎหมาย ทรัพยากรบุคคลและการเงินได้เข้ามามีส่วนร่วมตามความจำเป็นหรือไม่

* ความรับผิดชอบหลัก และเป็นเจ้าของขั้นตอน

		■ จัดทำแผนการสิ้นสุดสัญญา	อ* ■ ทีมงานของโครงการ ■ ผู้สนับสนุนระดับบริหาร ■ กฎหมาย ■ การเงิน	จำเป็นตามกฎระเบียบ	■ ดำเนินการสอบทานความถูกต้องเป็นจริงของประวัติการดำเนินการหรือประเมินการสอบทานของผู้บริหารที่มีต่อผู้ให้บริการ

ขั้นตอน	จุดประสงค์	กิจกรรมหลัก	บทบาท ผู้บริหาร *	ความเสี่ยง	การมีส่วนร่วมของผู้ตรวจสอบ
D: การนำไปใช้และการถ่ายโอน	ดำเนินการถ่ายโอนตามแผนและเริ่มการปฏิบัติการใหม่	▪ เริ่มใช้แผนการถ่ายโอน ▪ ถ่ายโอน/จัดการทรัพยากรต่างๆ ▪ ปรับเปลี่ยนกระบวนการ	▪ ทีมงานของโครงการ * ▪ เจ้าของกระบวนการ	▪ สูญเสียสินทรัพย์และผลตอบแทนจากการลงทุน (ROI) เนื่องจากแผนงานไม่มีประสิทธิผลและไม่มีการบริหารความเสี่ยง ▪ การบริการหยุดชะงักและส่งผลกระทบต่อลูกค้า ▪ คุณภาพการปฏิบัติการต่ำกว่าที่ตั้งเป้าไว้	▪ สอบทานก่อนการนำไปใช้งานเพื่อพิจารณาว่าโครงการเป็นไปตามข้อปฏิบัติที่เป็นมาตรฐาน ▪ สอบทานแผนสำรองฉุกเฉินถ้าการถ่ายโอนไม่เกิดผลตามที่ต้องการ ▪ พิจารณาว่ามีการระบุความเสี่ยงและการดำเนินการหรือไม่ รวมทั้งมีการบรรเทาความเสี่ยงและแจ้งต่อผู้มีส่วนได้เสียอย่างเหมาะสมซึ่งเป็นส่วนหนึ่งของการกำกับดูแลและการดำเนินโครงการ

* ความรับผิดชอบหลัก และเป็นเจ้าของขั้นตอน

			* ■ ผู้สนับสนุนระดับบริหาร ■ การเงิน ■ ทรัพยากรบุคคล ■ ความเสี่ยง		

ขั้นตอน	จุดประสงค์	กิจกรรมหลัก	บทบาท ผู้บริหาร *	ความเสี่ยง	การมีส่วนร่วมของผู้ตรวจสอบ
E: การติดตามดูแลและรายงานผล	ดูแลและควบคุมการปฏิบัติการที่มีการใช้บริการจากหน่วยงานภายนอก	▪ บริหารความสัมพันธ์ ▪ ประเมินผลลัพธ์และความสามารถในการดำเนินงาน ▪ ออกแบบการรายงานที่ต่อเนื่องและรูปแบบการปรับปรุงกระบวนการ	▪ เจ้าของกระบวนการ* ▪ ทีมงานที่ต้องดำเนินการต่อเนื่อง ▪ ผู้สนับสนุนโครงการ ▪ การเงิน ▪ ทรั	▪ ความสัมพันธ์และการส่งมอบบริการอาจนำไปสู่ความเสียหายต่อลูกค้าและการสูญเสียสินทรัพย์และผลตอบแทนการลงทุน ▪ กระบวนการไม่เสถียรและไม่ได้ให้ประโยชน์ตามที่วางแผนไว้	▪ พิจารณาว่าการดำเนินงานของผู้ให้บริการและการปฏิบัติตามข้อกำหนดในสัญญาจะได้รับการประเมินและสอบทานเป็นประจำโดยผู้บริหารอย่างไร ▪ สอบถามว่าใช้เกณฑ์วัดและดัชนีวัดผลการดำเนินงานอะไร ▪ สอบถามว่าข้อกังวลและสิ่งที่ควรปรับปรุงจะได้รับการสื่อสารและใช้ประโยชน์ในการปรับปรุงการปฏิบัติการ/สัญญาทั้งในปัจจุบันและในอนาคตอย่างไร

* ความรับผิดชอบหลัก และเป็นเจ้าของขั้นตอน

			พยากรบุคคล ▪ ความเสี่ยงและผู้ผู้เชี่ยวชาญอื่นๆ		
ขั้นตอน	**จุดประสงค์**	**กิจกรรมหลัก**	**บทบาท** **ผู้บริหาร ***	**ความเสี่ยง**	**การมีส่วนร่วมของผู้ตรวจสอบ**
F: การต่อรองใหม่	เพื่อให้มั่นใจว่าเมื่อมีการเจรจาต่อรองใหม่ความสัมพันธ์กับหน่วยงานที่ให้บริการภายนอกมีการพัฒนาและปรับปรุง	▪ รวบรวมประเด็นปัญหาทั้งหมดที่เกี่ยวกับการปฏิบัติการค่าใช้จ่าย คุณภาพ และความสัมพันธ์ ▪ กำหนดเกณฑ์เปรียบเทียบและสอบทานผลการศึกษาภาวะตลาดในปัจ	▪ เจ้าของกระบวนการ* ▪ ฝ่ายจัดซื้อ* ▪ ผู้สนับสนุนระดับ	▪ ไม่ได้รับประโยชน์สูงสุด โดยส่งผลให้เกิดการสูญเสียในผลตอบแทนจากการลงทุน (ROI) และคุณภาพการปฏิบัติการในอนาคต ▪ ไม่สามารถหาทางเลือกที่ดีกว่าหรือมีค่าใช้จ่ายเพิ่มขึ้นที่ไม่สมเหตุสมผล	▪ ระบุกลยุทธ์และข้อมูลสารสนเทศที่ใช้ และจำเป็นต้องใช้ เพื่อให้มั่นใจถึงการต่อรองใหม่ในอนาคตที่จะได้ประโยชน์สูงสุด ▪ เข้าใจการเปลี่ยนกลับคืนและการติดตามดูแลหรือผลการดำเนินงาน พิจารณาว่าผู้เชี่ยวชาญและเจ้าของกระบวนการผลักดันให้เกิดการต่อรองใหม่ที่ดีขึ้น

* ความรับผิดชอบหลัก และเป็นเจ้าของขั้นตอน

		จุบัน ▪ กำหนดเป้าหมายใหม่เพื่อปรับปรุงสัญญา	บริหาร ▪ กฎหมาย ▪ การเงิน ▪ ผู้เชี่ยวชาญอื่น ๆ		
ขั้นตอน	**จุดประสงค์**	**กิจกรรมหลัก**	**บทบาท** **ผู้บริหาร ***	**ความเสี่ยง**	**การมีส่วนร่วมของผู้ตรวจสอบ**
G: การเปลี่ยนกลับคืน	เพื่อให้มั่นใจว่าโครงการใช้บริการจากหน่วยงานภายนอกสามารถกลับสู่สภาพเดิมและได้รับการพิจารณาในเหตุผลทางธุรกิจ/กลยุทธ์	▪ ตัดสินใจนำกลับมาดำเนินการเองและระบุผลกระทบของการดำเนินการดังกล่าว ▪ พิจารณาว่าจะเปลี่ยนผู้ให้บริการอย่างไร ▪ ระบุผลกระทบที่มีต่อเหตุผลทางธุรกิจ	▪ เจ้าของกระบวนการ * ▪ ฝ่ายจั	▪ ไม่สามารถตอบสนองต่อสถานการณ์ที่ไม่เป็นผลดีหรือโอกาสที่ดีกว่า ▪ ขาดอำนาจต่อรองในอนาคต ▪ สูญเสียสินทรัพย์และการบริการหยุดชะงักถ้านำกลับมาดำเนินการเองหรือใช้ผู้ให้บริการรายอื่น ▪ ไม่ได้คาดการณ์ถึงค่าใช้จ่ายหากการใช้บริการจากหน่วยงานภายนอกล้มเห	▪ พิจารณาแผนสำรองฉุกเฉินถ้าโครงการไม่เป็นผล นั่นคือ ประมาณการค่าใช้จ่ายและโอกาสที่จะเกิดความล้มเหลว ▪ สอบถามว่าได้พิจารณาถึงค่าใช้จ่ายและโอกาสที่จะเกิดความล้มเหลวในเหตุผลทางธุรกิจและความจำเป็นในผลตอบแทนจากการลงทุน (ROI) ▪ สอบถามว่าสามารถใช้บริการจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพหรือไม่ สอบถามเกี่ยวกับความสามารถในการปฏิบัติงานของผู้ให้บริการ

* ความรับผิดชอบหลัก และเป็นเจ้าของขั้นตอน

			ดซื้อ ▪ ผู้สนับสนุนระดับบริหาร ▪ ความเสี่ยง ▪ แผนการดำเนินธุรกิจต่อเ	ลว	▪ พิจารณาว่าจุดที่จะเริ่มหรือพิจารณาเปลี่ยนผู้ให้บริการเป็นที่เข้าใจและกำหนดไว้ล่วงหน้าหรือไม่ ▪ หาคำตอบว่าได้มีการพิจารณาและประเมินความเสี่ยงอื่นๆซึ่งอาจนำไปสู่ความจำเป็นที่ต้องนำกลับมาดำเนินการเองรวมทั้งข้อกังวลในเชิงเศรษฐกิจมหภาคและการเมือง/สภาพภูมิศาสตร์ ▪ สอบถามว่าผู้ให้บริการมีความสามารถในการบริหารแผนการดำเนินธุรกิจต่อเนื่อง (BCP) หรือไม่ ▪ พิจารณาความพยายามในการดำเนินธุรกิจต่อเนื่องของผู้ให้บริการว่ายังใช้งานได้อย่างต่อเนื่องหรือไม่ ▪ ประเมินว่าสัญญาได้ระบุถึงความจำเป็นในการสิ้นสุดสัญญาอย่างไร

			นื่องBCP) ■ ผู้เชี่ยวชาญอื่นๆ		

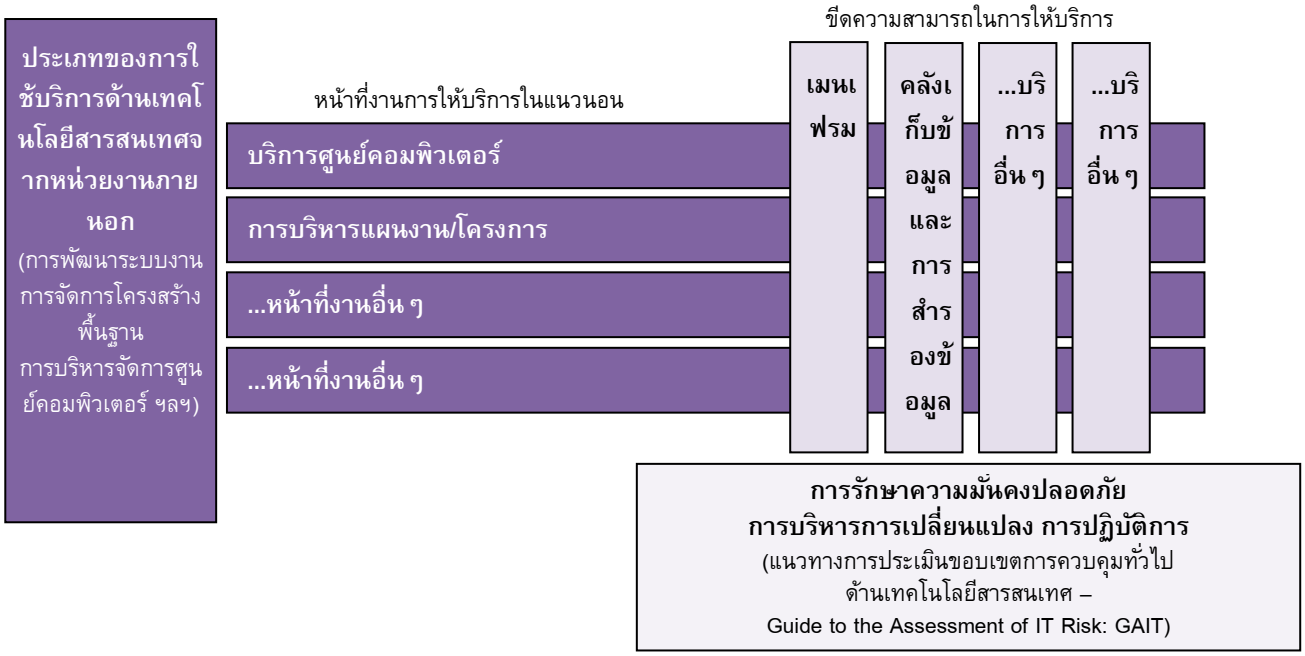
3 – การให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก: การพิจารณาความเสี่ยงและการควบคุม

สำหรับองค์กรผู้ให้บริการ

ในบทนี้จะกล่าวถึงความเสี่ยงเกี่ยวกับการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก (IT outsourcing: ITO) โดยผู้ให้บริการซึ่งให้บริการแก่องค์กรอื่นๆ ตามเงื่อนไขที่ได้ระบุไว้ในข้อตกลงกับหน่วยงานผู้ใช้งานสำหรับระดับการให้บริการ (SLA) ผู้ให้บริการควรดำเนินกิจกรรมการควบคุมด้านเทคโนโลยีสารสนเทศให้สอดรับกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อพัฒนาแนวทางการตรวจสอบที่เหมาะสม CAE ควรเริ่มต้นด้วยการทำความเข้าใจในภูมิทัศน์และสถาปัตยกรรม ITO ก่อน จากนั้น CAE ควรพิจารณาความเสี่ยงของการส่งมอบบริการและการควบคุมซึ่งได้รับการออกแบบให้ตอบสนองต่อความเสี่ยงและกำหนดวิธีการสร้างความเชื่อมั่นใน ITO ที่เหมาะสม

ความเข้าใจในภูมิทัศน์การให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

โดยปกติแล้ว บริการต่างๆ จะได้รับการจัดกลุ่มและส่งมอบตามขีดความสามารถหรือตามกลุ่มของขีดความสามารถซึ่งเรียกกันว่าหน้าที่งาน ขีดความสามารถในการให้บริการเป็นชุดความสามารถที่กำหนดไว้ ซึ่งเป็นการผสมผสานกันของทักษะ กระบวนการ เครื่องมือ เทคโนโลยีและประสบการณ์ ซึ่งจำเป็นต่อการส่งมอบโครงการและการให้บริการ เช่น การให้บริการด้านเมนเฟรม การประมวลผลด้วยเครื่องคอมพิวเตอร์ขนาดกลาง บริการคลังเก็บข้อมูลและบริการสำรองข้อมูล หน้าที่งาน เป็นกระบวนการในแนวนอน (horizontal processes) และหน้าที่งานด้านการปฏิบัติการ ซึ่งครอบคลุมขีดความสามารถในการบริการด้านต่างๆ ทำให้เกิดการบูรณาการของกระบวนการต่างๆ เครื่องมือและผลลัพธ์ ตลอดจนความสามารถในการบริการในหลายๆ เรื่อง เช่น การให้บริการศูนย์คอมพิวเตอร์ และการบริหารแผนงาน/โครงการ



จากแนวคิดพื้นฐานที่กล่าวถึงข้างต้น
จึงเป็นเรื่องสำคัญที่ต้องเข้าใจหน้าที่งานตามกรอบที่จะกล่าวต่อไป
ด้วยการเชื่อมโยงขีดความสามารถในการให้บริการกับหลักการพื้นฐานของการรักษาความมั่นคงปลอดภัย
การบริหารการเปลี่ยนแปลงและการปฏิบัติการ
ผู้ตรวจสอบภายในจะสามารถกำหนดขอบเขตของความเสี่ยงและการตรวจสอบยืนยันได้ตรงกับกระบวนการทางธุรกิจได้ดีขึ้น โดยแนวปฏิบัติทางวิชาชีพของสมาคมผู้ตรวจสอบภายใน (IIA Professional Guidance) แนวทางการประเมินการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศสำหรับธุรกิจและความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Guide to the Assessment of IT General Controls for Business and IT Risk: GAIT-R) จะกล่าวถึงแง่มุมด้านเทคโนโลยีสารสนเทศที่สำคัญซึ่งมีความจำเป็นต่อการบริหารจัดการและการลดความเสี่ยงทางธุรกิจ

ดังที่ได้กล่าวในบทที่ 2 หน้าที่งานการให้บริการในแนวนอนโดยทั่วไปจะรวมถึง:

- การพัฒนาและบริหารระบบงาน
- การบริหารโครงสร้างพื้นฐาน
- ศูนย์บริการให้ความช่วยเหลือ
- การบริการทดสอบและตรวจสอบความถูกต้องสมเหตุสมผลโดยอิสระ
- การบริหารศูนย์คอมพิวเตอร์
- การบูรณาการระบบ

- การวิจัยและพัฒนา
- การบริหารการรักษาความมั่นคงปลอดภัย
- การประมวลผลแบบกลุ่มเมฆ (เช่น บริการซอฟต์แวร์ (software-as-a-service: SaaS) บริการโครงสร้างพื้นฐานคอมพิวเตอร์ (infrastructure-as-a-service: IaaS) บริการแพลตฟอร์ม (platform-as-a-service: PaaS)

องค์กรต่างๆ
มีทางเลือกที่หลากหลายเมื่อพิจารณาถึงขีดความสามารถและหน้าที่งานในการใช้บริการจากหน่วยงานภายนอก ดังนี้:

- ผสมผสานการใช้บริการจากหน่วยงานภายนอกกับหน้าที่งานด้านเทคโนโลยีสารสนเทศภายในองค์กร (บางครั้งเรียกว่า “in-sourcing (การใช้งานภายใน)” หรือ “cosourcing (การใช้งานร่วม)”)

- เลือกใช้บริการจากหน่วยงานภายนอกเต็มรูปแบบในสมรรถนะหรือหน้าที่งานหนึ่งๆ ขณะที่ยังคงหน้าที่งานอื่นๆ ไว้ในองค์กร

- งานทั้งหมดขององค์กรใช้บริการจากผู้ให้บริการภายนอกซึ่งจะดูแลจัดการทรัพยากรด้านเทคโนโลยีที่หน้างาน (รวมทั้งเครื่องจักรอุปกรณ์ เครือข่าย และบุคลากร)

- ใช้บริการทุกงานของผู้ให้บริการภายนอกซึ่งจะ “เช่า” ฮาร์ดแวร์ ซอฟต์แวร์และการติดต่อสื่อสารให้แก่องค์กรผ่านบริการในรูปแบบของ “X-as-a-service”

โดยไม่ต้องคำนึงถึงเทคโนโลยีที่จะใช้หรือรูปแบบการใช้บริการจากหน่วยงานภายนอก หน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกควรเข้าใจขอบเขตของกระบวนการทั่วไป ความเสี่ยงหลัก การควบคุมและจุดประสงค์ของการตรวจสอบ
แนวทางการประเมินการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (GAIT)
ของสมาคมผู้ตรวจสอบภายในจะให้แนวทางที่เหมาะสมสำหรับการจัดการหน้าที่งานการให้บริการในแนวนอนตามประเภทของกระบวนการ (การรักษาความมั่นคงปลอดภัย การบริหารการเปลี่ยนแปลง และการปฏิบัติการ) เพื่อประเมินระดับความสำคัญของความเสี่ยง
และทำให้มั่นใจว่ามีการทดสอบการควบคุมหลักในแต่ละขีดความสามารถในการให้บริการต่างๆ

ขอบเขตหลักของสถาปัตยกรรมการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

ในบทนี้จะกล่าวถึงและให้ความหมายของระดับหรือขอบเขตของเทคโนโลยีสารสนเทศ ซึ่งประกอบขึ้นเป็นสถาปัตยกรรม ITO

สถาปัตยกรรมที่กล่าวนี้เป็นเรื่องทางเทคนิคและโครงสร้างการกำกับดูแลทั่วไปด้านเทคโนโลยีสารสนเทศซึ่งช่วยวางรากฐานรองรับการสร้างและการบริหารหน้าที่งานและขีดความสามารถในการให้บริการด้านเทคโนโลยีสารสนเทศ

1. **องค์กร (Organization):** องค์ประกอบสำคัญที่ช่วยให้การส่งมอบ ITO ประสบความสำเร็จคือ การจัดองค์กรและประวัติผลงานของผู้ให้บริการภายนอก
   องค์กรผู้ให้บริการควรมีการจัดโครงสร้างที่ดีที่สามารถรักษาบุคลากรที่มีความสามารถ ซึ่งมีทักษะที่เหมาะสมในบทบาทที่รับผิดชอบ
   มีการพิจารณาตัวชี้วัดความพึงพอใจของลูกค้าของผู้ให้บริการภายนอก และลูกค้ารับรู้ถึงความมีประสิทธิผลหรือไม่ มีการวิเคราะห์ความแตกต่างของทักษะ (skill-gap analysis) ครั้งสุดท้ายเมื่อไร
   คำถามเหล่านี้มีความสำคัญต่อหน่วยงานผู้ใช้งานในการประเมินว่าได้ทำสัญญากับผู้ให้บริการภายนอกที่ถูกต้องหรือไม่
   และสำคัญสำหรับผู้ให้บริการภายนอกในการวัดว่าอยู่ในสถานะที่ตอบสนองได้อย่างเต็มที่ตามความคาดหวังของลูกค้าหรือไม่

2. **ระบบปฏิบัติการ (Operating System):** คือซอฟต์แวร์ที่ปฏิบัติการอยู่บนคอมพิวเตอร์ จัดการทรัพยากรฮาร์ดแวร์คอมพิวเตอร์และให้บริการทั่วไปในการประมวลผลโปรแกรมซอฟต์แวร์ระบบงานต่างๆ
   ระบบปฏิบัติการจะทำหน้าที่เป็นตัวกลางระหว่างโปรแกรมระบบงานและฮาร์ดแวร์คอมพิวเตอร์
   นอกจากนั้น ระบบปฏิบัติการจะจัดให้มี:
   - เครื่องมือในการจัดการระบบหรือโปรแกรม ซึ่งใช้เพื่อติดตามดูแลผลการปฏิบัติการของคอมพิวเตอร์ แก้ไขจุดบกพร่อง หรือบำรุงรักษาส่วนต่างๆ ของระบบ
   - ชุดคำสั่งของโปรแกรมต่างๆ หรือหน้าที่งาน ที่โปรแกรมอาจใช้เพื่อปฏิบัติงานเฉพาะอย่าง โดยเฉพาะงานที่เกี่ยวข้องกับการเชื่อมต่อกับส่วนประกอบของระบบคอมพิวเตอร์

   บ่อยครั้งที่ระบบปฏิบัติการตกเป็นเป้าหมายของการโจมตี
   โดยเฉพาะอย่างยิ่งหากขาดการติดตั้งซอฟต์แวร์ที่ใช้แก้ไขหรือขาดการปรับปรุงให้เป็นปัจจุบันที่จำเป็น ผลลัพธ์ก็คือ เริ่มเกิดประเด็นเรื่องผลการดำเนินงานหรือสภาพพร้อมใช้งาน
   หรือระบบอาจได้รับความเสียหายจากการเข้าถึงโดยไม่ได้รับอนุญาต
   หรือการเปิดเผยข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีการกำหนดสิทธิในการเข้าถึง

3. **เครือข่าย (Network):** นอกจากอินเทอร์เน็ตและอินทราเน็ต
และความสามารถในการเชื่อมต่อเมื่อจำเป็นต้องใช้งานแล้ว
เครือข่ายต้องได้รับการปรับอย่างต่อเนื่องให้เข้ากับธุรกิจและบริการรูปแบบใหม่ที่เสนอ เช่น
การประมวลผลธุรกรรมแบบธุรกิจต่อลูกค้า (B2C) ธุรกิจต่อธุรกิจ (B2B) ธุรกิจต่อรัฐ (B2G)
การเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์ (e-learning) ศูนย์รวมการให้บริการลูกค้า (collaborative customer service) และการประชุมทางไกลแบบทันกาล (real time)
ซึ่งต้องใช้อุปกรณ์สื่อสารที่เป็นสื่อประสม มีพนักงานจำนวนมากขึ้นที่ทำงานอยู่ที่บ้าน
ทำงานระหว่างเดินทางหรือที่ทำงานเสมือนที่สามารถเชื่อมต่อได้ทันที
แรงกดดันที่จะต้องจัดให้มีการติดต่อสื่อสารที่เชื่อถือได้ ปลอดภัยและประหยัด
เป็นเรื่องที่ไม่เคยเกิดขึ้นมาก่อน และแรงกดดันนี้ก็จะเพิ่มมากขึ้นอีก ทั้งนี้ “เว็บ (the Web)”
ซึ่งอยู่นอกด่านกันบุกรุกขององค์กร
จะเกิดขึ้นในรูปแบบระบบปฏิบัติการเสมือนจริงและเป็นแพลตฟอร์มที่เป็นที่ต้องการขององค์กรมากขึ้นเรื่อยๆ

4. **ฐานข้อมูล (database):** ข้อมูลเป็นหัวใจสำคัญของธุรกิจทุกรูปแบบ “ข้อมูลเชิงปฏิบัติการ”
โดยเฉพาะอย่างยิ่งเมื่ออยู่ในรูปแบบที่แตกต่างกัน
ควรได้รับการแปลงให้อยู่ในรูปแบบที่บุคลากรจำนวนมากในองค์กรสามารถนำไปใช้ได้
ความท้าทายที่สำคัญที่สุดประการหนึ่งในการบริหารจัดการด้านเทคโนโลยีสารสนเทศคือ
การปกป้องข้อมูลที่มีความอ่อนไหว ข้อมูลลับ ข้อมูลส่วนตัว ทรัพย์สินทางปัญญา
และความลับทางการค้าซึ่งมีอยู่เป็นจำนวนมาก ไม่ให้ถูกโจมตีหรือสูญเสียไปโดยไม่เจตนา
ในทางกลยุทธ์
แนวโน้มนี้จะเพิ่มคุณค่าให้กับข้อมูลที่ไม่มีการจัดโครงสร้างและลดความสำคัญของระบบการเก็บแฟ้มข้อมูลตามลำดับขั้นแบบดั้งเดิม ซึ่งไม่ได้ออกแบบมาเพื่อใช้ในการปฏิบัติการ ณ ระดับปัจจุบัน

5. **ระบบงาน (Application):** สถาปัตยกรรมระบบงานประกอบด้วย
การบูรณาการและความสามารถในการทำงานร่วมกันของระบบงานส่วนหลัง (back-office)
ระบบงานส่วนหน้า (front-office) สำนักงานเสมือนจริง (virtual-office) คอมพิวเตอร์แบบตั้งโต๊ะ
คอมพิวเตอร์แบบพกพา เครื่อง PDA และคอมพิวเตอร์ขนาดบาง (thin-client)
ซึ่งสนับสนุนกลยุทธ์ทางธุรกิจทั้งที่ใช้อยู่ในปัจจุบันและจะใช้ในอนาคต
ระบบงานควรได้มาตรฐานเพื่อสนับสนุนกิจกรรม กระบวนการ พนักงาน ลูกค้า
ผู้ขายหรือผู้จัดหาสินค้าหรือบริการและผู้ร่วมทุน
โดยไม่ต้องคำนึงว่าระบบงานนั้นจะได้รับการติดตั้งอยู่กับที่หรือสามารถเคลื่อนย้ายได้
องค์กรขนาดใหญ่และขนาดกลางส่วนใหญ่มีระบบงานของกิจการขนาดใหญ่ เช่น
ระบบการวางแผนทรัพยากรองค์กร (Enterprise Resource planning: ERP)
และระบบบริหารงานลูกค้าสัมพันธ์ นอกจากนี้ ยังมีระบบงานที่กำหนดใช้เฉพาะกลุ่ม
และอินเทอร์เน็ตหรือระบบงานเชื่อมต่อผ่านเว็บ ซึ่งเชื่อมต่อกับลูกค้า

ผู้ขายหรือผู้จัดหาสินค้าหรือบริการและผู้ร่วมทุน
ท้ายที่สุดยังมีระบบงานที่ช่วยองค์กรจัดการระบบงานโครงสร้างพื้นฐาน
การประมวลผลและการติดต่อสื่อสาร (เช่น ระบบงานบริหารเครือข่าย และระบบต่าง ๆ)

6. **ตัวชี้วัดและการรายงาน (Metrics & Reporting):** ข้อตกลงสำหรับระดับการให้บริการ (SLA) เป็นหนึ่งในตัวชี้วัดหลักที่ใช้วัดผลการดำเนินงาน
และสามารถเป็นข้อมูลอ้างอิงแก่ผู้บริหารในการสนับสนุนการประเมินความสัมพันธ์กับลูกค้า/ผู้ขาย หรือผู้จัดหาสินค้าหรือบริการ ข้อตกลงสำหรับระดับการปฏิบัติการ (operational level agreement: OLA) จะสนับสนุน SLA และช่วยให้มีเป้าหมายเฉพาะของกระบวนการเพื่อให้บรรลุ SLA นั้น
องค์กรที่มีความสัมพันธ์ในการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ควรมีกระบวนการติดตามดูแลอย่างต่อเนื่อง
เพื่อให้มั่นใจว่าผลการดำเนินงานของผู้ให้บริการภายนอกสอดคล้องกับสัญญาการใช้บริการจากหน่วยงานภายนอก ดัชนีชี้วัดผลการดำเนินงานหลัก (KPI) และดัชนีชี้วัดความเสี่ยงหลัก (key risk indicators: KRIs)
ควรได้รับการจัดทำขึ้นเพื่อช่วยให้ลูกค้าและผู้ให้บริการภายนอกบรรลุจุดประสงค์ของธุรกิจ

7. **การบริหารแผนงาน/โครงการ (Program/Project Management):**
ในการบรรลุจุดมุ่งหมายเฉพาะที่ตั้งไว้
จะต้องดำเนินโครงการอย่างระมัดระวังตั้งแต่ต้นจนจบและมีพันธะสัญญา โดยระบุขอบเขต คุณภาพและค่าใช้จ่าย โครงการต่าง ๆ จะแตกต่างกันออกไปตามขนาดและขอบเขต
และสามารถรวมถึงการสร้างโครงสร้างพื้นฐานใหม่
การพัฒนาสินค้าใหม่และการดำเนินกระบวนการทางธุรกิจใหม่หรือการเปลี่ยนแปลงรูปแบบธุรกิจ
การประเมินโครงการดังกล่าวในขั้นตอนต่าง ๆ
จำเป็นต้องเข้าใจความเสี่ยงหลักและต้องพัฒนาชุดของเกณฑ์ประเมินหลัก

ขอบเขตความเสี่ยงหลักของการให้บริการด้านเทคโนโลยีสารสนเทศ

ในบทนี้จะให้เค้าโครงเกี่ยวกับความเสี่ยงทั่วไปของ ITO
ที่เกี่ยวข้องกับสถาปัตยกรรมการให้บริการด้านเทคโนโลยีสารสนเทศ
โดยพื้นฐานของการใช้บริการจากหน่วยงานภายนอกแล้ว เป็นที่ยอมรับว่า
แม้จะมีการถ่ายโอนความรับผิดชอบด้านการปฏิบัติงานไปยังผู้ให้บริการภายนอก
แต่หน่วยงานผู้ใช้งานยังคงมีความรับผิดชอบในการบริหารและติดตามให้มีการปฏิบัติตามนโยบาย
ขั้นตอนการปฏิบัติงานและข้อกำหนดตามระเบียบข้อบังคับ ซึ่งก็คือความเสี่ยง ITO
เพื่อบริหารความเสี่ยงนี้

หน่วยงานผู้ใช้งานควรมีแผนงานการกำกับดูแลการใช้บริการจากหน่วยงานภายนอกที่มีประสิทธิผล พร้อมด้วยกรอบการทำงานเพื่อให้ผู้บริหารระบุ วัดผล
ติดตามดูแลและควบคุมความเสี่ยงในขอบเขตของกระบวนการทำงานซึ่งสัมพันธ์กับการใช้บริการจากหน่วยงานภายนอก
ความเสี่ยงที่สัมพันธ์กับการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอกจะขึ้นอยู่กับกระบวนการที่มีการใช้บริการจากหน่วยงานภายนอก ความสัมพันธ์กับผู้ให้บริการและเทคโนโลยีที่ผู้ให้บริการใช้

ความล้มเหลวของหน่วยงานผู้ให้บริการภายนอกที่ไม่มีการควบคุม

ไม่มีการสร้างความเชื่อมั่นและการติดตามดูแลอย่างต่อเนื่องที่เหมาะสมในการให้บริการอาจส่งผลดังนี้:

- คุณภาพการให้บริการต่ำ โดยมีอัตราความล้มเหลวและข้อผิดพลาดที่ไม่อาจยอมรับได้
- การให้บริการหยุดชะงักและไม่เป็นไปตามข้อผูกพันที่มีต่อลูกค้าขององค์กร
- เกิดปัญหาเรื่องความเป็นส่วนตัว และการรักษาความลับ
- การตอบสนองล่าช้า ความพร้อมใช้งานของระบบลดลง
  มีข้อสงสัยเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลสารสนเทศ
  และมีการอะลุ้มอล่วยในเรื่องการรักษาความมั่นคงปลอดภัยและการเก็บรักษาความลับ
- เกิดปัญหาด้านเทคโนโลยีและสถาปัตยกรรมของระบบของหน่วยงานผู้ให้บริการภายนอก
  ที่เกี่ยวข้องกับความสามารถในเรื่องการปรับเปลี่ยนขนาด สมรรถนะ และผลการดำเนินงาน
- ไม่สามารถรักษามาตรฐานการควบคุมด้านการปฏิบัติงานภายในและด้านเทคโนโลยีสารสนเทศที่เหมาะสม และไม่สามารถปฏิบัติให้เป็นไปตามกฎระเบียบและข้อกำหนดของอุตสาหกรรม เช่น EU Data Protection Directive (EU DPD) US Graham-Leach-Bliley Act (GLBA) US Health Insurance Portability and Accountability act (HIPAA) International Financial Reporting Standards (IFRS) King III Report on Governance และ U.S. Sarbanes-Oxley (SOX) Act of 2002 and Payment Card Industry (PCI)
- ขีดความสามารถในการฟื้นฟูหลังเกิดเหตุภัยพิบัติและการดำเนินธุรกิจอย่างต่อเนื่องอยู่ในระดับต่ำ
- หน่วยงานผู้ใช้งานมีค่าใช้จ่ายและต้องใช้ความพยายามในการหาผู้ให้บริการภายนอกรายอื่น หรือนำกลับมาดำเนินการเอง

ความเสี่ยงของ ITO

สามารถระบุและจัดลำดับความสำคัญในมุมมองของหน่วยงานผู้ใช้งานและของผู้ให้บริการภายนอกเป็น 3 กลุ่ม คือ

- ความเสี่ยง ITO ที่เกิดร่วมกัน (ทั้งผู้ใช้บริการและผู้ให้บริการภายนอก)

- ความเสี่ยง ITO เฉพาะผู้ใช้บริการ
- ความเสี่ยง ITO เฉพาะผู้ให้บริการภายนอก

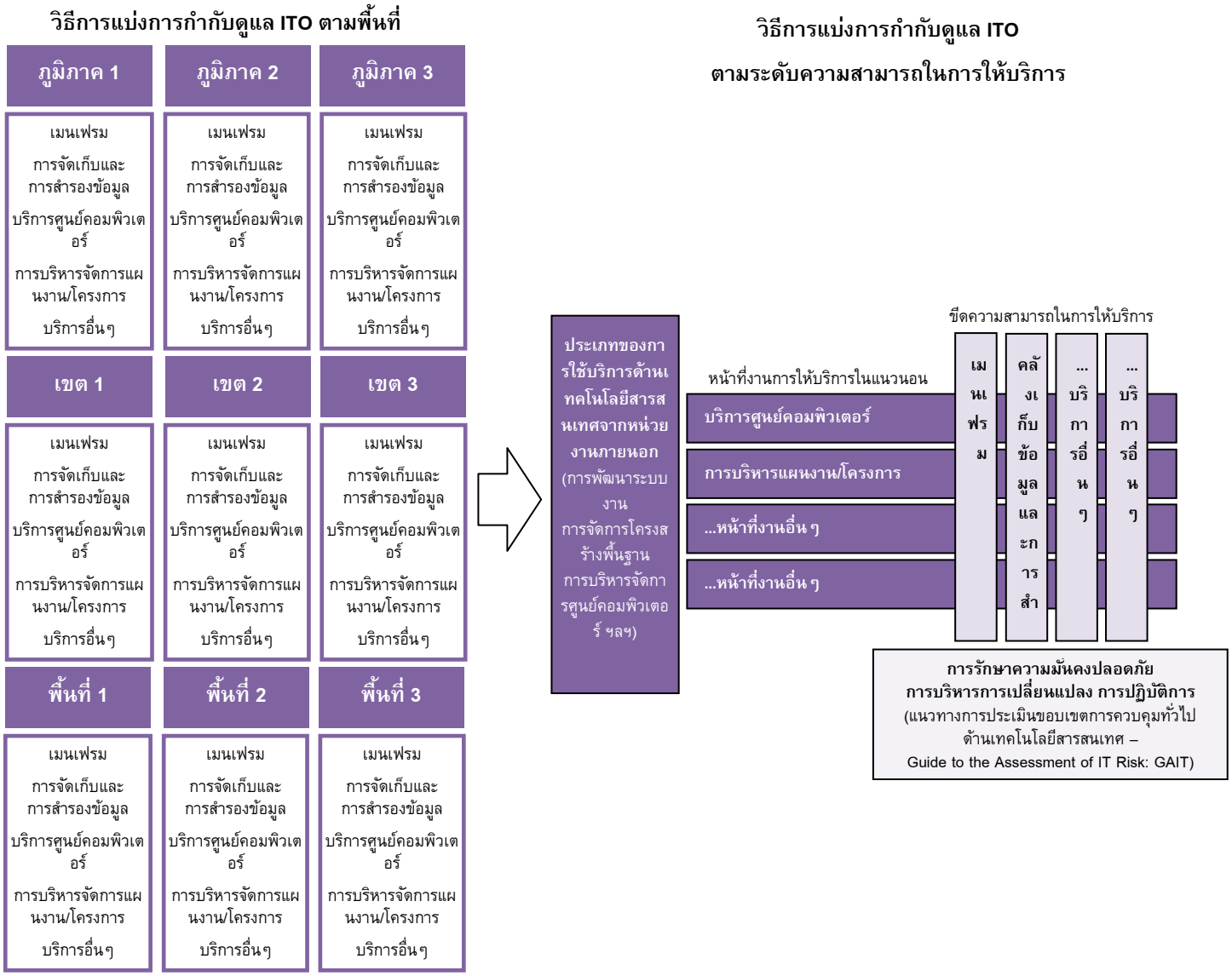
ขอบเขตของผลประโยชน์ร่วมควรได้รับการพิจารณาในลำดับต้นๆ
ในการประเมินความเสี่ยงที่พบจากการตรวจสอบ ITO

ตาราง 2: ตารางวิเคราะห์เกณฑ์ความเสี่ยงด้านไอทีโอ (ตัวอย่าง)

ประเภทความเสี่ยง	ความเสี่ยงไอทีโอ
ความเสี่ยงที่เกิดร่วมกันทั้งผู้ใช้และผู้ให้บริการ	ข้อขัดแย้งระหว่างทั้งสองฝ่ายเนื่องจากละเมิดเงื่อนไขในสัญญา
ความเสี่ยงเฉพาะผู้ใช้บริการ	ผู้ให้บริการภายนอกไม่ปฏิบัติตามสัญญา
ความเสี่ยงเฉพาะผู้ใช้บริการ	เกิดค่าใช้จ่ายนอกงบประมาณจากการใช้บริการจากหน่วยงานภายนอก
ความเสี่ยงเฉพาะผู้ใช้บริการ	สูญเสียความเป็นส่วนตัวของข้อมูล
ความเสี่ยงเฉพาะผู้ให้บริการภายนอก	มีบุคลากรไม่เพียงพอ

ความเสี่ยงในการกำกับดูแลการให้บริการ (ระเบียบวิธี รูปแบบ สัญญา)

เมื่อประเมินความเสี่ยงในสภาพแวดล้อมของการใช้บริการจากหน่วยงานภายนอก
หน่วยงานผู้ใช้งานควรพิจารณารูปแบบการกำกับดูแล ITO ที่ผู้ให้บริการใช้
ในรูปแบบการกำกับดูแลแบบเดิมซึ่งยังคงใช้อยู่นั้น
ขีดความสามารถแต่ละอย่างจะถูกจัดการแบบเบ็ดเสร็จเฉพาะตัว (silo) ซึ่งปกติจะแบ่งตามพื้นที่
โดยทีมงานที่แตกต่างกันจะใช้กระบวนการและเครื่องมือที่แตกต่างกัน ในทางกลับกัน
รูปแบบการกำกับดูแลใหม่นี้จะลดจำนวนผู้นำที่จะรับผิดชอบในแต่ละขีดความสามารถ
เป็นการบูรณาการในระดับข้ามประเทศ
เป็นแบบอัตโนมัติและผลักดันกระบวนการที่สอดคล้องกันในแต่ละขีดความสารมารถในการให้บริการ



สัญญาที่กำหนดไว้อย่างชัดเจนและมีเนื้อหาสมบูรณ์ ไม่ว่าจะอยู่ในรูปแบบใด จะช่วยให้หน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกสามารถบริหารความเสี่ยงได้

ความเสี่ยงที่ไม่เกี่ยวกับเรื่องเทคนิค

ที่มีผลต่อความสำเร็จของการใช้บริการจากหน่วยงานภายนอกจะได้รับการบริหารจัดการอย่างดีที่สุดผ่านรูปแบบการกำกับดูแลที่กำหนดไว้อย่างชัดเจนและด้วยเงื่อนไขในสัญญาที่เคร่งครัดซึ่งสนับสนุนให้เกิดความสัมพันธ์บนหลักการของการให้บริการที่เป็นเลิศ

ตาราง 3 ตัวอย่างความเสี่ยงด้านการกำกับดูแลที่มีร่วมกัน

ความเสี่ยง	คำจำกัดความและการบรรเทาความเสี่ยง
ผู้ให้บริการภายนอกไม่ปฏิบัติตามเงื่อนไขใน SLA	รวมถึงผลการดำเนินงานที่ต่ำกว่าเกณฑ์หรือบริการที่ส่งมอบที่มีคุณภาพต่ำ หน่วยงานผู้ใช้งานสามารถติดตามดูแลผลการดำเนินงานของผู้ให้บริการภายนอก รายงานผลการดำเนินงานที่ต่ำกว่าเกณฑ์ และกรณีที่จำเป็น สามารถใช้บทปรับตามที่ระบุไว้ในสัญญา นอกจากนี้ ผู้ให้บริการยังสามารถติดตามดูแล SLA และแก้ไขกระบวนการส่งมอบบริการให้เป็นไปตามข้อตกลง แม้ภายหลังกระบวนการเปลี่ยนแปลง หากการปฏิบัติตาม SLA ยังคงเป็นเรื่องยากอยู่ ผู้ให้บริการภายนอกสามารถแจ้งให้หน่วยงานผู้ใช้งานทราบ และในกรณีที่จำเป็น ก็สามารถต่อรอง SLA ใหม่ได้
ทักษะ/ระดับความรู้ของบุคลากรในโครงการของหน่วยงานผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศยังไม่เพียงพอ	บุคลากรที่มีทักษะถือเป็นปัจจัยหลักสู่ความสำเร็จของโครงการด้านเทคโนโลยีสารสนเทศ หน่วยงานผู้ใช้งานสามารถลดความเสี่ยงนี้โดยระบุคุณสมบัติที่ต้องมีในบทบาทนั้นให้ชัดเจน ส่วนผู้ให้บริการภายนอกก็สามารถลดความเสี่ยงดังกล่าวนี้ได้เช่นกันโดยรักษาความเชี่ยวชาญให้มีอย่างเพียงพอ ให้มั่นใจว่ามีการรักษาบุคลากรที่มีทักษะไว้ และรักษาบุคลากรกองกลางสำหรับลูกค้ารายสำคัญ
ช่องว่างในการติดต่อสื่อสารระหว่างหน่วยงานผู้ใช้งานและผู้ให้บริการภายนอก แนวทางการติดต่อสื่อสาร/การรายงานที่ไม่ชัดเจน	หน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกสามารถลดความเสี่ยงนี้ร่วมกัน โดยกำหนดโครงสร้างการบริหาร/แนวทางการติดต่อสื่อสารของโครงการที่จะใช้บริการจากภายนอกให้ชัดเจน และรวมแผนการติดต่อสื่อสารไว้ในแผนของโครงการ ทั้งหน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกสามารถร่วมกันกำหนดเวลาที่ต้องตอบสนองอย่างชัดเจน และท้ายที่สุด ทั้งสองฝ่ายควรทำให้เป้าหมาย กระบวนการและตารางเวลา สอดคล้องกันและสอบทานสถานะโดยเทียบกับแผนงานอย่างสม่ำเสมอ

ความเสี่ยงของการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (GAIT: การรักษาความมั่นคงปลอดภัย การบริหารการเปลี่ยนแปลง การปฏิบัติงาน)

ในการใช้ ITO
การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญในการให้บริการที่มีคุณภาพและปกป้องข้อมูลทางธุรกิจของลูกค้า แนวทาง GAIT จะให้แนวทางที่ยึดความเสี่ยงเป็นหลัก (risk-based approach) เพื่อประเมินขอบเขตการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศและเพื่อทำให้มั่นใจว่า การควบคุมหลักได้รับการทดสอบครอบคลุมโครงสร้างพื้นฐานระดับต่างๆ (เช่น ระบบงาน ฐานข้อมูล ระบบปฏิบัติการ และโครงสร้างพื้นฐานของเครือข่าย)

การรักษาความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัย เป็นรากฐานของรูปแบบ ITO
และเป็นหัวใจสำคัญในการปกป้องสินทรัพย์ของหน่วยงานผู้ใช้งาน (เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล) สัญญาควรระบุให้แน่ชัดว่า
ใช้นโยบายการรักษาความมั่นคงปลอดภัยใดและมาตรฐานใดในการกำกับดูแลการใช้ ITO กล่าวคือ จะใช้ของหน่วยงานผู้ใช้งานหรือผู้ให้บริการภายนอก และสัญญาควรบ่งชี้การเข้าถึงข้อมูล การเข้าถึงระบบงาน การเข้าถึงเครือข่าย ซอฟต์แวร์ ความเป็นส่วนตัว และแผนการดำเนินธุรกิจอย่างต่อเนื่อง นอกจากนี้ องค์กรควรเข้าใจในเรื่องต่อไปนี้:

- เทคโนโลยีด่านกันบุกรุก
- เทคโนโลยีการป้องกันไวรัส
- เทคโนโลยีที่ต้องมีใบอนุญาตให้ใช้ (Certificate authority technology)
- เทคโนโลยีไบโอเมตริก (Biometric technology) /ชีววิทยาหรือลักษณะทางกายภาพของบุคคล เช่น ลายนิ้วมือ
- การปกป้องข้อมูลมิให้สูญหาย
- ข้อกำหนดด้านกฎระเบียบ (เช่น EU DPD, HIPAA, IFRS, King III เป็นต้น)
- มาตรฐานความปลอดภัยของข้อมูลในการชำระเงินด้วยบัตรเครดิต (the Payment Card Industry Data Security Standard: PCI DSS)
- เทคโนโลยีการเข้ารหัส
- เทคโนโลยีการปฏิบัติตามกฎการรักษาความเป็นส่วนตัว
- วิธีการพิสูจน์ตัวตน
- โครงสร้างสารบบ (Directory structures)

- การบริหารจัดการช่องโหว่และภัยคุกคาม

การปกป้องข้อมูล

เป็นการยากที่จะปกป้องข้อมูลที่เป็นความลับ เป็นส่วนตัว และเป็นข้อมูลที่มีความอ่อนไหว เมื่อหน่วยงานผู้ให้บริการภายนอกได้รับข้อมูลเหล่านั้นและนำไปดำเนินการ ซึ่งอาจไม่ได้อยู่ภายใต้กฎหมายและระเบียบข้อบังคับเดียวกันกับลูกค้า ทุกแง่มุมของการใช้บริการจากหน่วยงานภายนอก การปกป้องข้อมูลสารสนเทศมักมีความสำคัญมากที่สุด โดยเฉพาะอย่างยิ่งในองค์กรภาครัฐ เช่น หน่วยงานบังคับใช้กฎหมาย และหน่วยงานด้านการป้องกัน ซึ่งการรักษาความลับเป็นสิ่งสำคัญยิ่งยวด ในธุรกิจด้านการเงินและการสาธารณสุข (healthcare) ซึ่งมักจะตกเป็นเป้าโจมตีจากผู้ไม่หวังดี

ความซับซ้อนจะเพิ่มมากขึ้นเมื่อหน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกอยู่ภายใต้กฎหมายและระเบียบข้อบังคับที่แตกต่างกัน โดยเฉพาะอย่างยิ่งเมื่อทั้งสองฝ่ายมิได้อยู่ในรัฐหรือประเทศเดียวกัน หรืออยู่ในขอบเขตอำนาจตามกฎหมายที่แตกต่างกันแม้จะอยู่ในประเทศเดียวกัน องค์กรที่อยู่ภายใต้กฎระเบียบที่เคร่งครัดควรใช้ความพยายามให้มากยิ่งขึ้น เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกของตนปฏิบัติหน้าที่ในนามขององค์กรตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

กระบวนการการรักษาความมั่นคงปลอดภัยและการปกป้องข้อมูลจะทำให้มั่นใจว่าการเข้าถึงระบบงานและข้อมูลนั้นได้รับอนุญาตอย่างถูกต้องและสินทรัพย์ได้รับการปกป้องอย่างเหมาะสม การจัดการกับความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์ที่ไม่มีอยู่จริง รายการที่ถูกตกแต่งหรือการเปิดเผยข้อมูลที่มีความอ่อนไหวโดยไม่ได้รับอนุญาต การควบคุมการรักษาความมั่นคงปลอดภัยจะเกี่ยวข้องโดยตรงกับการรับรองจากผู้บริหารว่า สินทรัพย์นั้นมีตัวตนหรือเกิดรายการนั้นๆ ขึ้นจริง

การควบคุมการเปลี่ยนแปลง

ในการใช้ ITO จะเกิดการเปลี่ยนแปลงในช่วงแรกของการถ่ายโอนและการปรับเปลี่ยนการดำเนินงานของส่วนงานที่จะใช้บริการจากภายนอก เมื่อความสัมพันธ์ในการบริการเริ่มต้นขึ้นหรือตลอดโครงการเปลี่ยนแปลงอื่นๆ ที่เกิดขึ้นตลอดอายุของสัญญา (โปรดดูหัวข้อ “การบริหารโครงการ” ซึ่งจะให้รายละเอียดเกี่ยวกับความเสี่ยงที่เกี่ยวข้อง และการควบคุมที่ได้รับการแนะนำให้รวมไว้ในการตรวจสอบ ITO)

กระบวนการการควบคุมการเปลี่ยนแปลงเป็นรากฐานเพื่อให้มั่นใจได้ถึงความถูกต้องแม่นยำของซอฟต์แวร์ระบบงาน กระบวนการคิดวิเคราะห์ในระบบงานควรจะมีการบันทึกเป็นลายลักษณ์อักษร

มีการทดสอบและกำหนดสิทธิ
เพื่อจัดการกับความเสี่ยงที่เกี่ยวกับข้อมูลสารสนเทศทางการเงินที่บันทึกไว้ไม่ถูกต้องหรือผิดช่วงเวลา
ดังนั้นการควบคุมการเปลี่ยนแปลงจึงเกี่ยวข้องโดยตรงกับการรับรองความถูกต้องจากผู้บริหารในการประเมินค่าหรือการวัดผล

การปฏิบัติการ

การบริหารการปฏิบัติการ เป็นกระบวนการในการปฏิบัติการหรือดำเนินงานระบบงาน (application) และระบบ (system) โดยปกติแล้ว
กระบวนการนี้จะรวมถึงการควบคุมเพื่อทำให้มั่นใจว่าระบบงานนั้นดำเนินงานได้ตามที่วางแผนไว้
ข้อผิดพลาดและข้อยกเว้นในการดำเนินการจะได้รับการแก้ไขในเวลาที่เหมาะสม
มีการสำรองข้อมูลระบบงานที่สำคัญหรือไฟล์ระบบไว้
และมีการรักษาความมั่นคงปลอดภัยทางกายภาพและแง่มุมอื่นๆ ของการปฏิบัติงานของศูนย์คอมพิวเตอร์

การควบคุมด้านการปฏิบัติการจะเป็นตัวควบคุมความเสี่ยงที่ระบบจะไม่พร้อมใช้งานหรือปฏิบัติการได้ไม่เต็มศักยภาพ ปัญหาในการปฏิบัติการสามารถทำให้โปรแกรมทำงานผิดขั้นตอน
ส่งผลให้เกิดสภาวะขาดสมดุล
กระบวนการปฏิบัติการทำให้มั่นใจว่าข้อมูลสารสนเทศมีความสมบูรณ์และผู้ตัดสินใจได้รับข้อมูลนั้นๆ ทันเวลา
กิจกรรมการควบคุมจะป้องกันไม่ให้เกิดการหยุดชะงักที่ไม่ได้คาดไว้หรือก่อให้เกิดข้อผิดพลาดในขณะที่กู้บริการคืน
การบริหารการปฏิบัติการเกี่ยวข้องโดยตรงกับการรับรองความถูกต้องจากผู้บริหารในความถูกต้องสมบูรณ์ (completeness) ว่าไม่มีรายการตกหล่น ซ้ำซ้อนโดยไม่ตั้งใจ หรือกระทบยอดไม่สมบูรณ์

การบริหารจัดการเหตุการณ์และปัญหา

การบริหารจัดการเหตุการณ์และปัญหาควรอธิบายควบคู่กันไป
เนื่องจากจะทำให้เกิดความชัดเจนที่สุด การบริหารจัดการเหตุการณ์จะเกี่ยวข้องกับ
“การแก้ปัญหาเฉพาะหน้า” เช่น การแก้ไขปัญหาการให้บริการหยุดชะงักหรือเหตุการณ์อื่นๆ โดยทันที
ส่วนการบริหารจัดการปัญหาจะเป็นเรื่องที่เกี่ยวกับ “การป้องกันปัญหา”
โดยระบุปัญหาและดำเนินการแก้ไขเพื่อกำจัดต้นเหตุของปัญหา (root cause)
จุดเน้นหลักของกระบวนการบริหารจัดการเหตุการณ์ควรเป็นการกู้คืนงานการให้บริการกลับมาโดยเร็วที่สุดเ

ท่าที่จะเป็นไปได้ เหตุการณ์ที่เกี่ยวข้องกับลูกค้าควรจัดอยู่ในลำดับต้นๆ
มีการประสานงานและแก้ไขปัญหาโดยผ่านศูนย์ให้บริการความช่วยเหลือ

คุณภาพข้อมูล

ข้อมูลจะมีคุณภาพก็ต่อเมื่อได้รับการเชื่อมต่อถึงกันทั้งหมดตั้งแต่จุดเริ่มต้นของห่วงโซ่การประมวลรายการ (transaction) จนจบกระบวนการ โดยมีความสมบูรณ์และน่าเชื่อถือ
ความถูกต้องและสมบูรณ์ของรายการเป็นปัจจัยที่สำคัญต่อธุรกิจ แม้ว่าหน่วยงานผู้ใช้จะเป็นเจ้าของข้อมูล ผู้ให้บริการก็ยังคงต้องรับผิดชอบในการจัดหาและจัดการสภาพแวดล้อมทางเทคโนโลยีสารสนเทศที่มีกระบวนการควบคุมต่างๆ ซึ่งอาจมีผลต่อคุณภาพของข้อมูลนั้นๆ คุณภาพของข้อมูลมีความเสี่ยง ณ แต่ละช่วงของห่วงโซ่การเชื่อมต่อตั้งแต่ต้นจนจบ ไม่ว่าจะเป็นจุดที่ข้อมูลถูกนำเข้าไปในระบบตั้งต้น ระหว่างการโอนข้อมูลจากระบบหนึ่งไปยังอีกระบบหนึ่ง หรือระหว่างกระบวนการคัดลอกข้อมูลบางส่วน แปลงและนำข้อมูลเข้าสู่อีกระบบ (ETL: extract transform and load)

การปฏิบัติการศูนย์คอมพิวเตอร์

ไม่ว่าจะเป็นการให้บริการศูนย์คอมพิวเตอร์เฉพาะงานหรือให้บริการ ITO ผ่านสภาพแวดล้อมแบบที่แบ่งตามระดับความสามารถ (leveraged environment) หรือแบบรวมศูนย์ (centralized environment)
การปฏิบัติการศูนย์คอมพิวเตอร์ก็มีแนวโน้มที่จะมีปัจจัยความเสี่ยงสืบเนื่องสูงที่สุดในการให้บริการ ITO ความเสี่ยงจะครอบคลุมถึงพอร์ตของการให้บริการศูนย์คอมพิวเตอร์และขอบเขตการปฏิบัติการที่ได้มาตรฐาน ซึ่งรวมทั้ง:

- การบริการบริหารจัดการเมนเฟรม
- การบริการสำรองและจัดเก็บข้อมูล
- การบริการให้เช่าพื้นที่เว็บไซต์ (web hosting services)
- การบริการบริหารจัดการเครื่องแม่ข่าย
- การบริการแบบกลุ่มเมฆ (cloud services)
- การบริการปรับปรุงศูนย์คอมพิวเตอร์ให้ทันสมัย
- การรักษาความมั่นคงปลอดภัยทางกายภาพ
- การควบคุมสภาพแวดล้อมสิ่งอำนวยความสะดวก (facility environmental controls)
- การติดตามดูแลให้มีการปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัย
- การบริหารสินทรัพย์

แนวทาง GAIT
จะช่วยในการระบุและประเมินความเสี่ยงสืบเนื่องด้านเทคโนโลยีสารสนเทศซึ่งควรจะได้รับการเชื่อมโยงกับความเสี่ยงทางธุรกิจ
โดยความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงชุดย่อยของความเสี่ยงทางธุรกิจ
วัตถุประสงค์ของการประมวลผลข้อมูลสารสนเทศจะเกี่ยวข้องกับกิจกรรมการควบคุมการดำเนินธุรกิจที่อ้างอิงในกรอบโครงสร้างการควบคุมภายในเชิงบูรณาการของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) โดยการทำให้กิจกรรมการควบคุมตามแนว GAIT
สอดคล้องกับจุดประสงค์ของการประมวลผลข้อมูลสารสนเทศ CAE
สามารถผลักดันให้เกิดแนวทางแบบบูรณาการที่เหมาะสมสำหรับการประเมินความเสี่ยงด้านการให้บริการด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงในการบริหารโครงการ

โครงการที่ล้มเหลวหรือมีปัญหาสามารถส่งผลกระทบต่อองค์กรอย่างมีนัยสำคัญ
ขึ้นอยู่กับความจำเป็นของโครงการนั้นที่มีต่อธุรกิจ ตัวอย่างผลกระทบที่อาจเกิดขึ้น มีดังนี้ :

- การให้บริการลูกค้าหยุดชะงัก
- สูญเสียความได้เปรียบเชิงการแข่งขัน
- เสียเบี้ยปรับเนื่องจากไม่สามารถปฏิบัติตามระเบียบข้อบังคับ
- สูญเสียรายได้
- เสียชื่อเสียง
- เกิดความล่าช้าในการเริ่มดำเนินการตามความคิดริเริ่มหรือออกสินค้าใหม่หรือกระบวนการทางกลยุทธ์ที่สำคัญ
- สูญเสียผลตอบแทนจากการลงทุน (ROI) ที่คาดการณ์ไว้
- ต้องปิดศูนย์อำนวยความสะดวก (facility) หรือเกิดความเสียหาย

ในท้ายที่สุดแล้ว ผู้บริหารเป็นผู้รับผิดชอบในการทำให้มั่นใจว่า
โครงการและผลลัพธ์ที่เป็นประโยชน์นั้นบรรลุผล
แม้ว่าผู้ให้บริการอาจต้องถูกลงโทษสำหรับความล้มเหลวที่เกิดขึ้นในโครงการ
การสอบทานความเสี่ยงที่เกี่ยวกับโครงการอาจมีส่วนช่วยให้โครงการประสบความสำเร็จ

ยิ่งโครงการได้รับการสอบทานเร็วเท่าไร ก็จะยิ่งดี การดำเนินการสอบทานในช่วงระยะแรกๆ ของโครงการจะเป็นประโยชน์มากที่สุด เพราะจะสามารถระบุประเด็นปัญหาซึ่งสามารถได้รับการแก้ไขได้โดยมีค่าใช้จ่ายน้อยกว่า เมื่อเปรียบเทียบกับประเด็นปัญหาที่พบในภายหลังหรือพบหลังจากดำเนินโครงการไปแล้ว

ประเภทของการควบคุมหลักในการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

ขอบเขตที่ครอบคลุมอย่างกว้างขวางของการให้บริการด้านเทคโนโลยีสารสนเทศนั้นมีอยู่หลากหลายและแตกต่างกันออกไปในแต่ละองค์กร ขอบเขตเหล่านี้ครอบคลุมถึงขีดความสามารถของการบริการ (เช่น สภาพแวดล้อมเครื่องแม่ข่ายขนาดกลางและอรรถประโยชน์ในการใช้คอมพิวเตอร์/การประมวลผลแบบกลุ่มเมฆ) และหน้าที่งานส่งมอบบริการ (เช่น การปฏิบัติการศูนย์คอมพิวเตอร์ การสนับสนุน ITO) การจัดระบบการควบคุมออกเป็นประเภทที่สามารถบริหารจัดการได้จะช่วยให้ผู้บริหารกำหนดวิธีการสร้างความมั่นใจและมองเห็นภาพรวมของความเสี่ยงได้อย่างสมบูรณ์

ดังที่ได้กล่าวไว้แล้ว แนวทาง GAIT ไม่ได้ระบุถึงการควบคุมหลักที่เฉพาะเจาะจง แต่จะระบุกระบวนการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Control: ITGC) และจุดประสงค์ของการควบคุมด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ซึ่งการควบคุมหลักต้องได้รับการระบุไว้และควรนำมาใช้ประโยชน์ในกระบวนการประเมินความเสี่ยง ระหว่างกระบวนการประเมินความเสี่ยง เครื่องมืออื่นๆ เช่น the Control Objectives for Information and Related Technology (COBIT) หรือ the Information Technology Infrastructure Library (ITIL) สามารถนำมาใช้เพื่อระบุแล้วจึงประเมินการควบคุมหลักด้านเทคโนโลยีสารสนเทศที่เฉพาะเจาะจง

ITIL ซึ่งพัฒนาขึ้นโดย the UK Office of Government Commerce (UK OGC) เป็นหนึ่งในกรอบโครงสร้างที่ใช้อ้างอิงที่ได้รับการยอมรับมากที่สุดสำหรับการบริหารการให้บริการด้านเทคโนโลยีสารสนเทศ โดยได้ให้ชุดของแนวปฏิบัติที่ดีที่สุดซึ่งรวบรวมจากองค์กรภาครัฐและภาคเอกชนหลายองค์กรได้ออกแบบการให้บริการโดยยึดตามกรอบโครงสร้างนี้ การตรวจสอบการให้บริการโดยอ้างอิงแนวทาง ITIL นี้สามารถให้ข้อมูลที่มีค่าแก่ผู้บริหารด้านเทคโนโลยีสารสนเทศ โดยอยู่บนพื้นฐานของมาตรฐานสากลที่ผ่านการพิจารณาอย่างรอบคอบและเป็นเหตุเป็นผลสำหรับการปรับปรุงการส่งมอบและการบริหารการให้บริการด้านเทคโนโลยีสารสนเทศ

ส่วนประกอบของการบริหารการให้บริการด้านเทคโนโลยีสารสนเทศ

การทำความเข้าใจสภาพแวดล้อมด้านสถาปัตยกรรมการปฏิบัติการที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ เป็นสิ่งจำเป็นทั้งต่อหน่วยงานผู้ใช้งานและผู้ให้บริการ

คุณภาพของบริการและความสัมพันธ์ระหว่างหน่วยงานผู้ใช้งานและผู้ให้บริการควรเป็นจุดเน้นหลักสำหรับการสอบทานทุกครั้ง

การบริหารค่าการทำงาน (configuration) และการเปลี่ยนแปลง

ภายใต้การบริหารค่าการทำงาน จะมีส่วนประกอบของโครงสร้างพื้นฐานและบริการซึ่งได้กล่าวอ้างไว้เป็นรายการค่าการทำงาน (configuration item: CI) ซึ่งจัดเก็บไว้ในฐานข้อมูลที่เรียกว่าฐานข้อมูลการบริหารจัดการค่าการทำงาน (configuration management database: CMDB) ซึ่งเป็นมากกว่าทะเบียนสินทรัพย์ กล่าวคือ มีข้อมูลสารสนเทศที่เกี่ยวข้องกับการดูแลรักษา การเคลื่อนไหวเปลี่ยนแปลง ประสบการณ์ที่เกี่ยวกับปัญหาที่พบใน CI ควบคู่กับความสัมพันธ์ระหว่าง CI และองค์ประกอบของข้อมูลสนับสนุนที่เกี่ยวข้องกัน (เช่น บุคลากรและหน่วยงาน) CMDB สามารถเป็นฐานข้อมูลทางกายภาพที่เป็นเอกเทศหรือประกอบด้วยฐานข้อมูลทางกายภาพที่หลากหลาย

CMDB ที่มีการบำรุงรักษาอย่างดีควรจะสามารถ:

- ให้ข้อมูล CI ที่ถูกต้อง (รวมถึงรายการทำงานที่ต้องพึ่งพากันและสัมพันธ์กัน) แก่กระบวนการของ ITIL และการปฏิบัติการอื่นๆ ในฐานข้อมูลระดับตรรกะที่เป็นส่วนกลาง
- รวม CI ทั้งหมดและคุณลักษณะต่างๆ ที่ต้องควบคุม
- ตรวจสอบยืนยันว่ามีข้อมูลสนับสนุน ข้อผูกพันด้านเทคโนโลยีสารสนเทศ การเงิน กฎหมาย และการรักษาความมั่นคงปลอดภัยขององค์กร
- ตรวจสอบความถูกต้องสมเหตุสมผลของข้อมูล CI ที่เก็บรักษาไว้ใน CMDB โดยเทียบกับ CI ที่ได้รับการอนุมัติแล้ว (ผ่านการบริหารการเปลี่ยนแปลง) และที่ค้นพบแล้ว (ผ่านเครื่องมือค้นหา/เครื่องมือคลังรายการ) โดยการพิสูจน์ความถูกต้อง การปฏิบัติตามระเบียบข้อบังคับและการตรวจสอบ

การบริหารการเปลี่ยนแปลงเป็นแนวปฏิบัติเพื่อให้มั่นใจว่า การเปลี่ยนแปลง CI ทุกครั้งจะดำเนินการตามที่วางแผนไว้และได้รับการอนุมัติ ซึ่งรวมทั้งการทำให้มั่นใจว่าการเปลี่ยนแปลงแต่ละครั้งมีเหตุผลทางธุรกิจหรือทางเทคโนโลยีสนับสนุน มีการระบุ CI และบริการด้านเทคโนโลยีสารสนเทศที่เฉพาะเจาะจงซึ่งได้รับผลกระทบจากการเปลี่ยนแปลง ได้รับการอนุมัติที่เหมาะสมสำหรับการเปลี่ยนแปลงจากผู้เชี่ยวชาญด้านธุรกิจและด้านเทคนิคที่เหมาะสม มีการวางแผนการเปลี่ยนแปลง มีการทดสอบการเปลี่ยนแปลง และมีแผนการนำกลับคืนสู่สภาพเดิมถ้าการเปลี่ยนแปลงส่งผลให้ CI ไม่อยู่ในสถานะตามที่คาดไว้ การเปลี่ยนแปลงคือ การเปลี่ยนแปลงแก้ไขใดๆ

ก็ตามต่อสภาพแวดล้อมทางการบริหารด้านเทคโนโลยีสารสนเทศ ซึ่งรวมทั้ง การเพิ่ม การลบ หรือการทดแทนองค์ประกอบใดๆ ของ CI หรือบริการในสภาพแวดล้อมนั้นๆ

การบริหารขีดความสามารถและความต่อเนื่องในการให้บริการ

ขณะที่ธุรกิจเติบโต ความต้องการในระบบเทคโนโลยีสารสนเทศก็เพิ่มขึ้น และขีดความสามารถของเครือข่าย คลังเก็บข้อมูล การประมวลผล และการสนับสนุน ควรจะเติบโตไปพร้อมกันกับความต้องการที่เพิ่มขึ้น การตรวจสอบ ITO ควรตรวจสอบความถูกต้องสมเหตุสมผลว่า มีกระบวนการที่ทำให้มั่นใจว่า มีการติดตามดูแลขีดความสามารถและวางแผนสำหรับขีดความสามารถในอนาคตไว้เป็นอย่างดีเป็นการล่วงหน้า โดยได้รับความร่วมมือจากฝ่ายธุรกิจ และแผนที่กล่าวนี้ได้รับการสอบทานเป็นระยะ การบริหารจัดการขีดความสามารถที่ดีจะทำให้มั่นใจว่าคุณภาพของการให้บริการเป็นไปอย่างต่อเนื่องตลอดเวลา

การบริหารความต่อเนื่องจะทำให้มั่นใจว่าการดำเนินงานทางธุรกิจที่สำคัญสามารถดำเนินต่อไปได้ในกรณีที่การให้บริการหยุดชะงักหรือเกิดภัยพิบัติ รายละเอียดของแผนความต่อเนื่องจะได้รับการบันทึกเป็นลายลักษณ์อักษรไว้ในแผนการดำเนินธุรกิจต่อเนื่องและแผนฟื้นฟูหลังเกิดเหตุภัยพิบัติ และควรมั่นใจว่าขอบเขตของแผนการดำเนินธุรกิจต่อเนื่องระบุถึงวัตถุประสงค์และระยะเวลาของการฟื้นฟูที่ชัดเจนและเป็นไปได้ โดยแผนที่กล่าวได้รับการออกแบบและพัฒนาเพื่อสนับสนุนการฟื้นฟูหน้าที่งานทางธุรกิจที่สำคัญ และได้รับการสอบทาน ปรับปรุงให้เป็นปัจจุบัน และฝึกซ้อมแผนอย่างสม่ำเสมอ

การบริหารข้อตกลงสำหรับระดับการให้บริการ

SLA เป็นแกนหลักของสัญญาการให้บริการและควรวัดผลได้อย่างชัดเจน ตัวเลขสถิติทั้งหมดที่สัมพันธ์กับ SLA ควรได้รับการจัดทำขึ้นจากระบบและมีการป้องกันการแก้ไข การตรวจสอบ ITO ควรตรวจสอบยืนยันว่าผู้บริหารในระดับที่เหมาะสมได้รับรายงาน SLA และมีการสอบทานที่เป็นประโยชน์ การบริหารจัดการ SLA ยังรวมถึงการจัดทำเอกสาร การดำเนินการ การติดตามดูแลและการบริหารคำร้องทุกข์ คำชมเชย และข้อคิดเห็นจากลูกค้า

นอกจากนี้ แนวปฏิบัติต่อไปนี้ควรได้รับการประเมินในการตรวจสอบ ITO โดยเป้าหมายของระดับการให้บริการทั้งหมดควรจะ:

- ชัดเจนและไม่คลุมเครือ

- ได้รับการยอมรับและอนุมัติโดยลูกค้าและผู้ให้บริการ
- วัดผลได้

เป้าหมายทั้งหมดใน OLA หรือ สัญญาที่ตกลงไว้กับผู้ให้บริการภายนอก (underpinning contract: UC) ควรสอดคล้องกับ SLA

การบริหารจัดการเหตุการณ์และปัญหา

กระบวนการบริหารจัดการเหตุการณ์ควรบันทึกผลกระทบของทุกเหตุการณ์ในรูปของตัวเลขอย่างชัดเจน รวมทั้งจำนวนผู้ใช้งานที่ได้รับผลกระทบ ชั่วโมงทำงานที่สูญเสียไป ระดับความซับซ้อน ผลกระทบต่อรายได้ของธุรกิจ และผลกระทบต่อการปฏิบัติตามระเบียบข้อบังคับ
การตรวจสอบควรต้องครอบคลุมรายงานเหตุการณ์ทั้งหมดและตรวจสอบว่าเหตุการณ์ดังกล่าวได้รับการแก้ไขอย่างน่าพอใจหรือไม่
มีการวิเคราะห์ต้นเหตุของปัญหาและมีการเตรียมการป้องกันเพื่อหลีกเลี่ยงไม่ให้เกิดปัญหาซ้ำอีก

ปัจจัยสำคัญสู่ความสำเร็จของกระบวนการบริหารเหตุการณ์คือ:

- ข้อมูลการบริหารเหตุการณ์แบบรวมศูนย์
- การเข้าถึงสารสนเทศ CMDB
- ตัวชี้วัดผลการปฏิบัติงาน
- ความเป็นเจ้าของที่ชัดเจนในแต่ละเหตุการณ์
- การบริหารการมอบหมายให้ผู้รับผิดชอบกรณีที่เกิดเหตุการณ์ขึ้น
- การจัดหมวดหมู่ของเหตุการณ์ให้เป็นมาตรฐาน
- การเข้าถึง SLA

กระบวนการบริหารปัญหาควรมีขั้นตอนดังต่อไปนี้:

- การระบุปัญหาและจัดประเภทของปัญหา
- การตรวจสอบหาความจริงและค้นหาสาเหตุของปัญหา
- การประเมินข้อผิดพลาด
- การยุติปัญหา/ข้อผิดพลาด
- การสื่อสาร สถานะ/การปรับปรุงให้เป็นปัจจุบัน

การบริหารแผนงาน/โครงการ

การสอบทานโครงการในฐานะเป็นส่วนหนึ่งของการตรวจสอบ ITO ควรมุ่งเน้นไปที่ขอบเขตหลัก 5 ประการ (ดู GTAG 12: Auditing IT Projects) คือ:

- การสอดคล้องกันของเทคโนโลยีสารสนเทศกับธุรกิจ
- การบริหารโครงการ
- ความพร้อมของผลลัพธ์ด้านเทคโนโลยีสารสนเทศ
- การบริหารการเปลี่ยนแปลง
- การใช้งานเมื่อเริ่มโครงการแล้ว

การสอบทานโครงการควรจัดให้มีการควบคุมปัจจัยสู่ความสำเร็จต่อไปนี้

1. **การมีส่วนร่วมของผู้ใช้งาน –**
   ผู้ใช้งานด้านธุรกิจและด้านเทคโนโลยีสารสนเทศมีส่วนร่วมในกระบวนการตัดสินใจและการรวบรวมสารสนเทศ
2. **การสนับสนุนจากผู้บริหาร –**
   ผู้บริหารหลักช่วยให้เกิดการสอดคล้องกันกับกลยุทธ์ทางธุรกิจและการเงินรวมถึงให้การสนับสนุนในการแก้ไขข้อขัดแย้ง
3. **วัตถุประสงค์ทางธุรกิจที่ชัดเจน –** ผู้มีส่วนได้เสียเข้าใจคุณค่าหลัก (core value) ของโครงการและเห็นถึงการสอดคล้องกันกับกลยุทธ์ทางธุรกิจ
4. **การปรับให้เหมาะสมและกระชับ –**
   การพัฒนาด้วยการทำซ้ำและกระบวนการหาค่าที่เหมาะสมที่สุดเพื่อหลีกเลี่ยงคุณสมบัติที่ไม่จำเป็นและเชื่อมั่นว่าได้รวมคุณสมบัติที่สำคัญไว้
5. **ผู้เชี่ยวชาญด้านการบริหารโครงการ –**
   การใช้ผู้จัดการโครงการที่มีความเข้าใจในทักษะพื้นฐานและเข้าใจการปฏิบัติงาน เช่น Project management Professional ที่ต้องได้รับการรับรองจาก Project Management Institute
6. **การบริหารทางการเงิน –** ความสามารถในการบริหารทรัพยากรด้านการเงิน การประเมินความเสี่ยง และการแสดงให้เห็นถึงคุณค่าของโครงการ
7. **บุคลากรที่มีทักษะ –** การจัดหา การบริหาร และการควบคุมบุคลากรของโครงการที่มีทักษะเพื่อให้งานก้าวหน้าต่อไปได้ เมื่อต้องเผชิญกับปัญหาการลาออกและอุปสรรคอื่นๆ ด้านบุคลากร

8. **ระเบียบวิธีที่เป็นทางการ –**
   ชุดของเทคนิคเชิงกระบวนการที่กำหนดไว้ล่วงหน้าซึ่งจะช่วยสร้างแผนการทำงานว่าเหตุการณ์อะไรควรเกิดขึ้นอย่างไรและเมื่อไรตามลำดับก่อนหลัง
9. **เครื่องมือและโครงสร้างพื้นฐาน –**
   การสร้างและการบริหารโครงสร้างพื้นฐานของโครงการด้วยเครื่องมือที่ช่วยให้สามารถบริหารงานบุคลากร ข้อกำหนด การเปลี่ยนแปลง ความเสี่ยง ผู้ขายและผู้ให้บริการ และการบริหารเชิงคุณภาพ

ตาราง 4 การพิจารณาการควบคุมโครงการในแต่ละขั้นตอน (ตัวอย่าง)

ขั้นตอนโครงการ	การพิจารณาการควบคุม
การออกแบบและพัฒนา	▪ เหตุผลทางธุรกิจที่ชัดเจนและมั่นคง ▪ การประเมินค่าใช้จ่ายและประโยชน์ตามที่เป็นจริงและครอบคลุมได้ครบถ้วน ▪ การมีส่วนร่วมของผู้มีส่วนได้เสียหลักทั้งหมดตั้งแต่ขั้นตอนเริ่มต้น. ▪ การพิจารณาอย่างถี่ถ้วนในการควบคุมด้านการรักษาความมั่นคงปลอดภัยและด้านความถูกต้องครบถ้วน
การบริหารโครงการ	▪ การเป็นผู้นำเชิงรุกและการรายงานแบบทันกาล ▪ การมีส่วนร่วมของผู้มีส่วนได้เสียหลักทั้งหมด ▪ การระบุปัญหาและรายงานต่อผู้บริหารระดับสูง ▪ ตารางการทำงานตามที่เป็นได้จริงและเป้าหมายที่ชัดเจน ▪ การทดสอบที่เข้มงวดและทดลองนำร่องก่อนใช้งานจริง
การนำไปใช้	▪ การบริหารการเปลี่ยนแปลงและการฝึกอบรม ▪ การติดตามประโยชน์อย่างสม่ำเสมอและเชื่อถือได้ ▪ การประเมินความพึงพอใจของลูกค้าอย่างต่อเนื่อง

วิธีการสร้างความเชื่อมั่นในการส่งมอบบริการ ITO

ในบทนี้จะให้โครงร่างคร่าว ๆ เกี่ยวกับวิธีการต่าง ๆ ที่ผู้บริหารควรใช้เพื่อให้เกิดความเชื่อมั่นในเรื่องความเสี่ยงที่เกี่ยวข้องสัมพันธ์กับ ITO การบริหารความเสี่ยง ITO ควรจะทำโดยผู้ให้บริการและหน่วยงานผู้ใช้งาน

และจะประสบความสำเร็จมากยิ่งขึ้นถ้าทั้งสองฝ่ายมีความสัมพันธ์ที่แน่นแฟ้น
ผู้ให้บริการจะเสียเปรียบเชิงการแข่งขันอย่างชัดเจน
ถ้าไม่เห็นคุณค่าของความจำเป็นของการได้รับและการให้ความเชื่อมั่นผ่านการตรวจสอบและติดตามดูแล
เมื่อเปรียบเทียบกับผู้ให้บริการที่เข้าใจความจำเป็นของลูกค้าในเรื่องการสร้างความเชื่อมั่น

บทบาทของผู้ตรวจสอบภายในต่อการให้บริการ

องค์กรอาจจะไม่สามารถบรรลุวัตถุประสงค์ถ้าปราศจากกลไกการให้บริการที่มีประสิทธิผล
ผู้ตรวจสอบภายในเป็นผู้มีความเข้าใจอย่างลึกซึ้งเป็นพิเศษและอยู่ในตำแหน่งที่เหมาะสมที่จะประเมินนโยบาย ขั้นตอนการทำงานและการปฏิบัติการต่างๆ
เพื่อติดตามผลสำเร็จของวัตถุประสงค์ขององค์กรและเพื่อระบุ
รวมทั้งบริหารความเสี่ยงต่อวัตถุประสงค์เหล่านั้น

ผู้ตรวจสอบภายในอาจจะ:

- ให้ความเชื่อมั่นโดยสอบทานระบบการบริหารเพื่อระบุและจัดการความเสี่ยงที่มีต่อการให้บริการอย่างมีประสิทธิผล
- ให้ความเชื่อมั่นโดยดำเนินการสอบทานการบริหารการให้บริการให้ครอบคลุมและครบถ้วนอยู่เสมอ
- ให้ความเชื่อมั่นโดยการสอบทานระบบการรายงานผลการปฏิบัติงานและระบบต่างๆ ที่ใช้ในการติดตามและบริหารให้บรรลุเป้าหมายต่างๆ
- ได้รับความเชื่อมั่นโดยอ้างอิงผู้ให้ความเชื่อมั่นรายอื่นๆ
- สวมบทบาทเป็นที่ปรึกษาเชิงรุกมากขึ้นในทุกแง่มุมตลอดกระบวนการให้บริการ ตัวอย่างเช่น การมีส่วนร่วมตั้งแต่เริ่มต้นออกแบบระบบเพื่อให้มั่นใจว่ามีการระบุความจำเป็นของหน่วยงานผู้ใช้งาน หรือโดยติดตามการดำเนินการของผู้บริหาร

การตรวจสอบ ITO

กระบวนการใช้บริการจากหน่วยงานภายนอกอาจเปิดโอกาสให้ลูกค้าและผู้ให้บริการภายนอกต้องเผชิญกับความเสี่ยงต่างๆ ที่จะเกิดขึ้นตามมา
ซึ่งสามารถส่งผลกระทบอย่างร้ายแรงต่อกิจกรรมของลูกค้าและผู้ให้บริการ
การบริหารความเสี่ยงเหล่านี้โดยการปรับปรุงคุณภาพและประสิทธิภาพของการควบคุมภายในทำให้การตรวจสอบ ITO กลายเป็นองค์ประกอบที่จำเป็นสำหรับทุกองค์กรที่มีส่วนร่วมในกระบวนการนี้
ในระดับองค์กรแล้ว การตรวจสอบ ITO ไม่เพียงแต่จะได้รับการรวมไว้ในกระบวนการตรวจสอบภายใน

แต่สามารถรวมไว้ในกระบวนการตรวจสอบภายนอกด้วยก็ได้ นอกจากนั้น การตรวจสอบ ITO ยังสามารถขยายจากหน่วยงานผู้ใช้บริการไปยังผู้ให้บริการผ่านความร่วมมือระหว่างกัน โดยแนวทางการตรวจสอบอื่นๆ เช่น การทดสอบติดตามดูรายการตั้งแต่ต้นจนจบ (walkthrough) และการติดตามดูแลอย่างต่อเนื่องสามารถทำให้ความร่วมมือระหว่างผู้ให้บริการและลูกค้าดียิ่งขึ้นและยังช่วยกระดับความเชื่อมั่นที่ได้รับจากการตรวจสอบด้วย

ISAE 3402[4]/SSAE 16[5]

ISAE 3402
เป็นมาตรฐานที่ได้รับการยอมรับอย่างกว้างขวางและบ่งชี้ว่าผู้ให้บริการได้ให้สำนักงานบัญชีและสำนักงานสอบบัญชีที่เป็นอิสระตรวจสอบวัตถุประสงค์และกิจกรรมการควบคุมของตน
รายงานของบุคคลที่สามต่อการควบคุมภายในขององค์กรที่ให้บริการจะอธิบายกระบวนการควบคุมการบริการต่างๆ ของผู้ให้บริการภายนอก
รายงานดังกล่าวนี้ให้ข้อมูลแก่ผู้ใช้งานเพื่อประเมินและจัดการกับความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการจากภายนอก ถ้าผู้ให้บริการผ่านการสอบทานด้วย ISAE 3402
จะได้รับความน่าเชื่อถือมากยิ่งขึ้นซึ่งจำเป็นต่อการปฏิบัติตามระเบียบข้อบังคับและการบัญชีของลูกค้า
การตรวจสอบผู้ให้บริการเป็นสิ่งจำเป็นสำหรับหน่วยงานผู้ใช้งานที่จะสามารถตรวจสอบยืนยันว่า
มีกระบวนการตรวจสอบและการควบคุมที่เหมาะสม เพื่อบริหารธุรกิจให้เป็นไปตามกฎหมาย Sarbanes-Oxley มาตรา 404(b)

มาตรฐานต่าง ๆ

มาตรฐานระหว่างประเทศ: ในเดือนธันวาคม พ.ศ. 2552 IAASB[6] ได้ยอมรับ ISAE 3402 มาใช้เป็นกระบวนการ “ให้ความเชื่อมั่น”
เพื่อประเมินการปฏิบัติตามระเบียบข้อบังคับเกี่ยวกับการควบคุมด้านเทคโนโลยีสารสนเทศและด้านกระบวนการขององค์กรผู้ให้บริการ การให้ความเชื่อมั่น (attestation)
เกี่ยวข้องกับการตรวจสอบเพื่อให้ข้อสรุปของผู้สอบบัญชีต่อสาระสำคัญมากกว่ารูปแบบการนำเสนอรายงานทางการเงินอย่างตรงไปตรงมา การให้ความเชื่อมั่นดังกล่าวจะมีความเข้มงวดน้อยกว่าการตรวจสอบ
อย่างไรก็ตาม รายงานของผู้ตรวจสอบการให้บริการก็อาจยังคงต้องมีอยู่ เมื่อลูกค้าขององค์กรร้องขอ

4 ISAE 3402: International Standard on Assurance Engagement 3402
5 SSAE 16: Statements on Standards for Attestations Engagement 16
6 IAASB: the International Auditing and Assurane Standard Board

มาตรฐานของสหรัฐอเมริกา: ในเดือนเมษายน พ.ศ. 2553 คณะกรรมการมาตรฐานการสอบบัญชี (Auditing Standards Board: ASB) ของ AICPA[7] ได้ออก SSAE 16
ซึ่งเป็นรายงานให้ความเชื่อมั่นเช่นเดียวกับ ISAE 3402

รายงานการควบคุมองค์กรผู้ให้บริการ (Service Organization Control Reports: SOC Reports) ของ AICPA: ในการปฏิบัติตาม SSAE 16 สถาบัน AICPA
ได้ยอมรับรายงานการควบคุมองค์กรผู้ให้บริการจำนวน 3 ฉบับ
เพื่อขยายขอบเขตของประเด็นที่ผู้สอบบัญชีจะตรวจสอบในฐานะผู้ให้บริการตรวจสอบ (service auditor)
การดำเนินการดังกล่าวจะช่วยให้องค์กรได้รับความไว้วางใจในกระบวนการให้บริการมากยิ่งขึ้น ภายใต้ SOC การให้บริการตรวจสอบแบ่งออกเป็น 3 ประเภท
ซึ่งได้รับการออกแบบเพื่อให้ผู้ให้บริการสามารถตอบสนองต่อความต้องการเฉพาะอย่างและปรับจุดเน้น (refocus) เกี่ยวกับความเสี่ยงเฉพาะ (niche risk):

- รายงาน SOC1 –
  รายงานเกี่ยวกับการควบคุมขององค์กรผู้ให้บริการซึ่งเกี่ยวเนื่องกับการควบคุมภายในของหน่วยงานผู้ใช้ต่อการรายงานทางการเงิน
- รายงาน SOC2 –
  รายงานการควบคุมขององค์กรผู้ให้บริการซึ่งเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัย สภาพพร้อมใช้งาน ความถูกต้องครบถ้วนของการประมวลผล
  การรักษาความลับหรือความเป็นส่วนตัว
- รายงาน SOC3 – รายงานเกี่ยวกับกระบวนการให้บริการที่เชื่อถือได้ขององค์กรผู้ให้บริการ

ความน่าเชื่อถือของผู้สอบบัญชีในการตรวจสอบภายใน

หน้าที่งาน: มาตรฐานการให้ความเชื่อมั่นฉบับใหม่
จะช่วยให้ผู้สอบบัญชีไม่เพียงแต่เชื่อถือคำอธิบายของผู้บริหารเกี่ยวกับกระบวนการควบคุมต่างๆ แต่ยังรวมถึงผู้ตรวจสอบภายในของผู้ให้บริการด้วย

ปัญหาเกี่ยวกับความน่าเชื่อถือที่มากเกินไป

ในอดีต มาตรฐาน SAS 70 Type II
มักถูกนำมาใช้เป็นมาตรฐานที่ใช้ปฏิบัติจริงกับบริษัทที่มีหลักทรัพย์ซื้อขายในตลาดหลักทรัพย์

7 AICPA: American Institute of Certified Public Accountants

เพื่อให้เป็นไปตามกฎหมาย Sarbanes-Oxley มาตรา 404(b)
ตามข้อกำหนดว่าด้วยการเปิดเผยข้อมูลเกี่ยวกับ “การตรวจสอบและควบคุม”
ซึ่งรวมถึงสัญญาการใช้บริการจากหน่วยงานภายนอก อย่างไรก็ตาม รายงาน “การให้ความเชื่อมั่น”
ฉบับใหม่นี้ จะตัดข้อมูลของผู้ใช้งานออก
เพราะผู้สอบบัญชีจะไม่ได้ใช้ดุลยพินิจมากเท่ากับการดำเนินงานภายใต้ SAS 70 Type II โดยสรุป
หน่วยงานผู้ใช้งานจะใช้ดุลยพินิจของตนในการพิจารณายอมรับรายงานการให้ความเชื่อมั่นและอาจขอรายงานดังกล่าวเป็นกรณีพิเศษในส่วนที่เกี่ยวกับวัตถุประสงค์การควบคุมที่หน่วยงานผู้ใช้งานระบุไว้
หน่วยงานผู้ใช้จึงต้องพึ่งพาผู้ให้บริการมากขึ้นเพื่อวิเคราะห์ความเสี่ยง
และผู้ใช้งานจำเป็นต้องตรวจสอบข้อบกพร่องจากการวิเคราะห์ดังกล่าว

ภายใต้มาตรฐานการให้ความเชื่อมั่นฉบับใหม่
เป็นความรับผิดชอบของผู้ให้บริการที่จะระบุความเสี่ยงที่เผชิญอยู่และวางแผนว่าจะติดตามดูแลและบรรเทาความเสี่ยงเหล่านั้นอย่างไร เพื่อให้มั่นใจว่าจะบรรลุวัตถุประสงค์ของการควบคุมที่กำหนดไว้

การติดตามดูแล KRI

การติดตามดูแลความเสี่ยงที่เกิดขึ้นใหม่และตอบสนองโดยทันทีเป็นการเตรียมการล่วงหน้า KRI เป็นตัวชี้วัดหนึ่งที่ใช้ในการจัดการว่ากิจกรรมหนึ่งๆ มีความเสี่ยงอย่างไร ในขณะที่ KPI
จะวัดว่าสิ่งที่ได้ดำเนินการไปนั้นดีมากน้อยเพียงใด KRI
จะเป็นตัวชี้วัดความเป็นไปได้ที่จะเกิดผลกระทบเชิงลบในอนาคต
โดยเป็นเสมือนสัญญาณเตือนล่วงหน้าที่บ่งชี้ถึงการเปลี่ยนแปลงของความเสี่ยงขององค์กร ดังนั้น KRI
จึงเป็นองค์ประกอบพื้นฐานหนึ่งของกรอบโครงสร้างความเสี่ยงและการควบคุมที่สมบูรณ์และแนวปฏิบัติด้านการจัดการความเสี่ยงที่ดี ตัวชี้วัดเหล่านั้นแสดงให้เห็นว่าองค์กรได้รับผลกระทบ
หรือมีความเป็นไปได้สูงที่จะได้รับผลกระทบจากความเสี่ยงที่เกินกว่าที่องค์กรจะรับได้ นั่นคือ
ควรยอมรับเฉพาะความเสี่ยงที่ระบุว่ายอมรับได้ก่อนที่จะดำเนินการ การติดตามดูแล KRI
จะเป็นประโยชน์ในการช่วยให้ธุรกิจลดความสูญเสียลงและปิดช่องว่างโดยดำเนินการเชิงรุกกับสถานการณ์ความเสี่ยงก่อนที่เหตุการณ์จะเกิดขึ้นจริง หน่วยงานผู้ใช้งานและผู้ให้บริการภายนอกควรพัฒนาและปรับใช้ KRI ให้เป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยง

การดำเนินการประเมินและติดตามดูแลตัวชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องจะทำให้เกิดความเชื่อมั่นและที่สำคัญกว่านั้นคือ
สามารถหยิบยกปัญหาขึ้นมาพิจารณาได้อย่างทันเวลาเพื่อให้ผู้บริหารดำเนินการและป้องกันความเสี่ยง

ภาคผนวก A

แผนการตรวจสอบวงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

แผนการตรวจสอบต่อไปนี้เป็นแนวทางพื้นฐานสำหรับการประเมินความเสี่ยงและกระบวนการของหน่วยงานผู้ใช้งานเมื่อตัดสินใจใช้บริการจากหน่วยงานภายนอก
การมีส่วนร่วมของผู้ตรวจสอบภายในในวงจรการใช้บริการจากหน่วยงานภายนอกอาจแตกต่างกันออกไปอย่างมีนัยสำคัญขึ้นอยู่กับหน้าที่งานการให้ความเชื่อมั่นอื่นๆ หรือการมีส่วนร่วมของผู้เชี่ยวชาญภายนอก ประสบการณ์ของผู้บริหารเกี่ยวกับกฎเกณฑ์ของโครงการและการใช้บริการจากหน่วยงานภายนอก หรือเวลาที่ให้เพื่อให้มีการตรวจสอบด้วย แผนการตรวจสอบนี้ให้ตัวอย่างการมีส่วนร่วมใน 2 กรณี คือ การสอบทานเต็มขอบเขตในทุกขั้นตอน หรือในกรณีของงานที่มีคุณค่าสูง (high-value areas) ซึ่งการตรวจสอบอาจมุ่งเน้นการปฏิบัติงานให้เสร็จภายในเวลาที่ได้รับอย่างจำกัด หรือความเห็นที่เป็นอิสระที่อาจทำให้ผู้บริหารคลายกังวลลง
มีปัจจัยหลายประการที่สามารถดำเนินการให้สำเร็จลุล่วงโดยขึ้นอยู่กับการพิจารณาถึงความคาดหวังและความเสี่ยงที่องค์กรยอมรับได้หรือช่วงความเบี่ยงเบนของความเสี่ยงที่องค์กรยอมรับได้ของผู้มีส่วนได้เสียในการตรวจสอบ

วงจรการใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก
ขั้นตอนการตรวจสอบ
เขตงาน
ด สูญเสียสินทรัพย์ ผลตอบแทนจากการลงทุน (ROI) ลดลง
สนุนมีความน่าเชื่อถือและสมบูรณ์ (ตามความจำเป็น) หรือไม่
ะโยชน์และความเสี่ยงหรือไม่
ไม่
งธุรกิจที่น่าเชื่อถือหรือไม่
สินทรัพย์และผลตอบแทนจากการลงทุน (ROI) หรือเสียภาพลักษณ์ขององค์กรเพราะคุณภาพบริการอาจลดลง มีโอกาสเกิดผลกระทบเชิงลบต่อการปฏิบัติตามกฎระเบียบ
เชื่อถือหรือไม่และพิจารณาความเสี่ยงเชิงธุรกิจและความเสี่ยงในการนำไปใช้ทั้งหมด
ประโยชน์ที่จะได้ในรายละเอียดรวมอยู่ในความเสี่ยงของการปฏิบัติการและผลกระทบจากความล้มเหลวหรือไม่
น์ของค่าใช้จ่าย/ประโยชน์ที่จะได้หรือไม่
างโปร่งใสและน่าเชื่อถือหรือไม่
สัมพันธ์กันหรือไม่?
นกระบวนการหรือไม่
าหรือไม่
บนพื้นฐานของสัญญาที่นำไปสู่ความสำเร็จ
การปกป้องจากช่องว่างของความจำเป็นในการส่งมอบงานที่มีคุณภาพ อยู่ในสภาพพร้อมใช้งาน และมีความถูกต้องครบถ้วน/การรักษาความลับ สูญเสียสินทรัพย์ ยอาจเกิดผลกระทบต่อความจำเป็นในการปฏิบัติตามกฎหมายด้านการกำกับดูแล
ซื้อจัดจ้างที่เหมาะสมหรือไม่
องทำเพื่อสร้างความมั่นใจด้านการควบคุม (เช่น ความจำเป็นในการให้ความเชื่อมั่นสำหรับ SAS 70 หรือ SSAE # 16 ใหม่ หรือISAE 3402) ญาอย่างมีประสิทธิผลและรวมอยู่ในข้อตกลงสุดท้ายหรือไม่
สือชี้ชวนให้ประกวดราคา.
รองรับความจำเป็นในการปฏิบัติงาน
ของโครงการ

ล และการเงิน ได้เข้ามามีส่วนร่วมตามความจำเป็นหรือไม่
กอบแผนการสิ้นสุดสัญญา
ผลที่เกิดจากการดำเนินงานของผู้บริหารด้านการปฏิบัติการและทีมงานของโครงการ ประเมินความเพียงพอและความสมบูรณ์
เศษในเรื่องความเพียงพอของมาตรฐานการควบคุมซึ่งดำเนินการโดยผู้ให้บริการและบุคลากรด้านการปฏิบัติตามระเบียบข้อบังคับ
เป็นไปตามแผนเพื่อเริ่มปฏิบัติการใหม่
OI) เนื่องจากแผนงานไม่มีประสิทธิภาพและไม่มีการบริหารความเสี่ยง กล่าวคือ การบริการหยุดชะงักและส่งผลกระทบต่อลูกค้า คุณภาพการปฏิบัติการต่ำกว่าที่ตั้งเป้าไว้
อบเข้าร่วมประชุมการกำกับดูแลเพื่อช่วยให้มั่นใจว่าโครงการเป็นไปตามข้อปฏิบัติที่เป็นมาตรฐาน
ื่อประเมินการสอบทานของฝ่ายบริหารต่อการปฏิบัติการของผู้ให้บริการและวิธีการที่จะทำให้เกิดความเชื่อมั่นในความสามารถของผู้ให้บริการและประวัติการให้บริการที่มี
มาะสม
อไม่ รวมทั้งมีการบรรเทาความเสี่ยงและแจ้งต่อผู้มีส่วนได้เสียอย่างเหมาะสม
บัติการที่มีการใช้บริการจากหน่วยงานภายนอก
มเสียหายต่อลูกค้าและการสูญเสียสินทรัพย์และผลตอบแทนจากการลงทุน (ROI) กระบวนการไม่เสถียรและไม่ได้ให้ประโยชน์สูงสุดตามที่วางแผนไว้
ิตามข้อกำหนดในสัญญาจะได้รับการประเมินและสอบทานเป็นประจำโดยผู้บริหารอย่างไร
น ๆ (KPIs)
อสารและใช้ประโยชน์ในการปรับปรุงการปฏิบัติการ/สัญญา ทั้งในปัจจุบันและในอนาคตอย่างไร
ามสัมพันธ์กับหน่วยงานที่ให้บริการภายนอกมีการพัฒนาและปรับปรุงขึ้นหรือไม่
ในผลตอบแทนจากการลงทุน (ROI) และคุณภาพการปฏิบัติการในอนาคต ไม่สามารถหาทางเลือกที่ดีกว่าหรือมีค่าใช้จ่ายเพิ่มขึ้นที่ไม่สมเหตุสมผล
ออะไรเพื่อให้มั่นใจถึงการต่อรองใหม่ในอนาคตที่จะได้ประโยชน์สูงสุด
ปรียบเทียบใหม่และการศึกษาภาวะตลาดใหม่
าจากผลการดำเนินงาน
กรรมและผลการดำเนินงานจริงเพื่อให้มั่นใจว่าผู้เชี่ยวชาญและเจ้าของกระบวนการผลักดันให้เกิดการปรับปรุงก่อนการต่อรองใหม่จะเกิดขึ้น
น่วยงานภายนอกสามารถกลับสู่สภาพเดิมและได้รับการพิจารณาในเหตุผลทางธุรกิจ/กลยุทธ์ ถ้าจำเป็นต้องกลับไปใช้บริการแบบเดิม
รือโอกาสที่ดีกว่า ขาดอำนาจต่อรองในอนาคต สูญเสียสินทรัพย์และการบริการหยุดชะงักถ้านำกลับมาดำเนินการเองหรือทำสัญญากับผู้ให้บริการรายอื่น
ภายนอกล้มเหลว

ผล
เหลว เรื่องดังกล่าวได้รับการพิจารณาในเหตุผลทางธุรกิจและความจำเป็นในผลตอบแทนจากการลงทุน (ROI) หรือไม่
ธิผลเพื่อลดช่องโหว่ใดๆ ที่อาจเกิดขึ้นหรือไม่?
าร รวมทั้งได้มีการกำหนดไว้ล่วงหน้าหรือไม่
ามจำเป็นที่ต้องนำกลับมาดำเนินการเอง รวมทั้งข้อกังวลในเชิงเศรษฐกิจมหภาค การเมือง และสภาพภูมิศาสตร์หรือไม่
นธุรกิจต่อเนื่อง (BCP) หรือไม่ และความพยายามในการดำเนินธุรกิจต่อเนื่องยังใช้งานได้อย่างต่อเนื่องหรือไม่
พันธ์ทางธุรกิจอย่างไร

ภาคผนวก B

แผนการตรวจสอบการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

แผนการตรวจสอบต่อไปนี้เป็นแนวทางขั้นพื้นฐานสำหรับประเมินองค์กรผู้ให้บริการ บริการเฉพาะที่จัดให้หรือที่ใช้ควรได้รับการกำหนดไว้และควรเพิ่มเติมการควบคุมที่จำเป็นไว้ในแผนการตรวจสอบ

แนวทางนี้ได้รับการออกแบบมาเพื่อรับมือกับความเสี่ยงในขอบเขตที่เกี่ยวกับการตรวจสอบแบบเต็มขอบเขต (full scope audit) หรือการทดสอบติดตามดูรายการตั้งแต่ต้นจนจบเกี่ยวกับการควบคุมที่ออกแบบไว้ (control design walkthrough)

การตรวจสอบแบบเต็มขอบเขตมีจุดมุ่งหมายเพื่อให้ความเชื่อมั่นในประสิทธิผลของการปฏิบัติการในกิจกรรมควบคุมต่างๆ

ส่วนการทดสอบติดตามดูรายการตั้งแต่ต้นจนจบมีวัตถุประสงค์เพื่อให้ผลการประเมินแก่ผู้บริหารเกี่ยวกับการออกแบบกิจกรรมควบคุมต่างๆ

ขั้นตอนการทดสอบติดตามดูรายการตั้งแต่ต้นจนจบจะได้รับการจัดลำดับตามความจำเป็นในกรณีที่มีข้อจำกัดด้านทรัพยากร งบประมาณหรือเวลา

แผนการตรวจสอบการให้บริการด้านเทคโนโลยีสารสนเทศจา	
ขั้นตอนการตรวจสอบ	**การตร**
การกำกับดูแล	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าความสัมพันธ์ (สัญญา) ระหว่างลูกค้าและผู้ให้บริการภายนอกมีการกำกับดูแลและควบคุมดูแลที่เพียงพอหรือไม่	
ความเสี่ยง: ความสัมพันธ์ระหว่างลูกค้าและผู้ให้บริการลดลง	
● สัญญาควรระบุการแบ่งความรับผิดชอบ และควรระบุว่าดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยและมาตรฐานใด รวมทั้งระบุวัตถุประสงค์ที่ชัดเจนของระดับการให้บริการ	
● ระดับทักษะของบุคลากรควรเพียงพอกับบริการที่ให้	
● การสื่อสารระหว่างผู้ให้บริการภายนอกและผู้ใช้บริการเป็นระเบียบแบบแผนและเพียงพอที่จะสนับสนุนความสัมพันธ์ของสัญญา	
การรักษาความมั่นคงปลอดภัย	
วัตถุประสงค์การตรวจสอบ: ประเมินสภาวะความมั่นคงปลอดภัยในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศแต่ละขั้น	
ความเสี่ยง: อาจมีการเข้าถึงระบบลูกค้าโดยไม่ได้รับอนุญาต หรือข้อมูลอาจสูญหาย รั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต	
● มีนโยบายและขั้นตอนการรักษาความมั่นคงปลอดภัยและมีการปฏิบัติตาม	
● มีการระบุและปกป้องข้อมูลที่มีความอ่อนไหว	
● มีการควบคุมการเข้าถึงในทุกระดับ (ได้แก่ การจัดทำเป็นเอกสาร การให้อำนาจ การสอบทานและการถอดถอน)	
● มีการกำหนดและการปฏิบัติตามข้อกำหนดด้านระเบียบข้อบังคับหรือด้านกฎหมาย	
● มีการติดตั้งซอฟต์แวร์ที่ใช้แก้ไขในระบบ	
● มีกระบวนการติดตามดูแลการรักษาความมั่นคงปลอดภัยเชิงรุก	
คุณภาพข้อมูล	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่ามีการควบคุมเพียงพอเพื่อให้มั่นใจในคุณภาพของข้อมูลหรือไม่	
ความเสี่ยง: ข้อมูลไม่ครบถ้วน ไม่ถูกต้อง หรือไม่ทันเวลา	
● ในการเชื่อมต่อ ควรมีการควบคุมความถูกต้องครบถ้วนของข้อมูล เช่น ขั้นตอนวิธีการแบบแฮช (hash algorithms) การนับจำนวนรายการ (record counts)	
● งานการประมวลผลข้อมูลได้รับการติดตามดูแลว่าสำเร็จหรือล้มเหลวและมีกระบวนการจัดการแก้ไขความล้มเหลวนั้น	
● การส่งผ่านข้อมูลข้ามระบบเครือข่ายที่เชื่อถือได้ (trusted boundaries) ควรได้รับการปกป้องอย่างเหมาะสม (เช่น การเข้ารหัส)	
การบริหารจัดการค่าการทำงาน	
วัตถุประสงค์การตรวจสอบ: ประเมินการมีอยู่จริง ความครบถ้วน และความถูกต้องของฐานข้อมูลค่าการทำงาน	
ความเสี่ยง: ฐานข้อมูลไม่สนับสนุนกระบวนการด้านการปฏิบัติการ	
● ให้ข้อมูล CI ที่ถูกต้องแม่นยำ (รวมทั้งการพึ่งพาและความสัมพันธ์) แก่ ITIL และกระบวนการปฏิบัติการอื่นๆ ในฐานข้อมูลระดับตรรกะที่เป็นส่วนกลาง	

● อธิบาย CI ทั้งหมดและคุณลักษณะต่างๆ ที่ต้องควบคุม	
● ตรวจสอบยืนยันว่ามีข้อมูลสนับสนุน ข้อผูกพันด้านเทคโนโลยีสารสนเทศ การเงิน กฎหมาย และการรักษาความมั่นคงปลอดภัยขององค์กร	
● ตรวจสอบความถูกต้องสมเหตุสมผลของข้อมูล CI ที่เก็บรักษาไว้ใน CMDB โดยเทียบกับสถานะที่ได้รับการอนุมัติแล้ว (ผ่านการบริหารการเปลี่ยนแปลง) และที่ค้นพบแล้ว (ผ่านเครื่องมือค้นหา/เครื่องมือคลังรายการ) โดยการพิสูจน์ความถูกต้อง การปฏิบัติตามระเบียบข้อบังคับและการตรวจสอบ	
การบริหารการเปลี่ยนแปลง	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าการเปลี่ยนแปลงได้ดำเนินการตามแผนที่วางไว้และได้รับการอนุมัติ	
ความเสี่ยง: การเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่อยู่ในแผนอาจส่งผลให้เกิดปัญหาต่อการปฏิบัติงานของระบบและฟังก์ชั่นการทำงานต่างๆ	
● มีการทดสอบเพื่อสอบทานการทำงานของการเปลี่ยนแปลงก่อนที่จะนำไปใช้ในสภาพแวดล้อมจริง	
○ การเปลี่ยนแปลงได้รับการอนุมัติและจัดทำเป็นเอกสารก่อนการนำไปดำเนินการในสภาพแวดล้อมจริง	
○ มีการแบ่งแยกหน้าที่อย่างเหมาะสมเพื่อป้องกันการแก้ไขโปรแกรมในสภาพแวดล้อมจริงโดยไม่ได้รับอนุญาต	
● คลังโปรแกรม – ทั้งคลังระบบงานและเค้าร่างฐานข้อมูล (ตามความเหมาะสม) ได้รับการสอบทานเพื่อให้มั่นใจว่าการเปลี่ยนแปลงมีความเหมาะสม	
การบริหารขีดความสามารถ	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่ามีการติดตามดูแลและบริหารขีดความสามารถของระบบให้ทันกับความต้องการของธุรกิจ	
ความเสี่ยง: ขีดความสามารถของระบบไม่สอดคล้องกับความต้องการของธุรกิจ	
● มีกระบวนการที่ทำให้มั่นใจว่ามีการติดตามดูแลขีดความสามารถและการวางแผนขีดความสามารถในอนาคต	
● มีการวางแผนโดยธุรกิจมีส่วนร่วม ซึ่งเป็นการดำเนินการล่วงหน้าก่อนที่จะเกิดความต้องการจริง	
● มีการสอบทานการวางแผนขีดความสามารถอย่างสม่ำเสมอ	
● มีการติดตามดูแลขีดความสามารถ ดูแลและสอบทานผลลัพธ์เพื่อดูแนวโน้ม	
ความต่อเนื่องในการให้บริการ	
วัตถุประสงค์การตรวจสอบ: ประเมินว่าองค์กรมีแผนการดำเนินธุรกิจอย่างต่อเนื่องและแผนการฟื้นฟูระบบหลังเกิดภัยพิบัติที่มีประสิทธิผลหรือไม่	
ความเสี่ยง: การปฏิบัติการทางธุรกิจที่มีความสำคัญไม่สามารถดำเนินได้อย่างต่อเนื่องหลังจากเกิดภัยพิบัติหรือธุรกิจหยุดชะงัก	
● แผนการดำเนินธุรกิจอย่างต่อเนื่องได้รับการจัดทำเป็นเอกสาร	
● แผนการฟื้นฟูหลังเกิดภัยพิบัติได้รับการจัดทำเป็นเอกสาร	
● แผนต่างๆ ได้รับการสอบทานและอนุมัติ และมีการสอบทานอย่างสม่ำเสมอ	
● แผนต่างๆ ได้รับการทดสอบ/ฝึกซ้อมเป็นประจำ (อย่างน้อยปีละครั้ง)	
● แผนต่างๆ มีวัตถุประสงค์และระยะเวลาของการฟื้นฟูที่เป็นไปได้	
● แผนต่างๆ ได้รับการพัฒนาเพื่อสนับสนุนหน้าที่งานทางธุรกิจที่มีความสำคัญ	
การบริหารข้อตกลงสำหรับระดับการให้บริการ (SLA)	

วัตถุประสงค์การตรวจสอบ: ประเมินว่าสัญญาครอบคลุมถึง SLA และองค์กรได้ติดตามดูแลและรายงานเกณฑ์วัดของ SLA	
ความเสี่ยง: เกิดผลกระทบเชิงลบต่อความพึงพอใจของลูกค้า มีการประเมินถึงบทปรับ ไม่ต่อสัญญาหรืออาจจะยกเลิกสัญญา	
● เป้าหมายทั้งหมดของระดับการให้บริการชัดเจนและไม่คลุมเครือ	
● เป้าหมายทั้งหมดของระดับการให้บริการเป็นที่ตกลงและได้รับการอนุมัติโดยหน่วยงานผู้ใช้งานและผู้ให้บริการภายนอก	
● เป้าหมายทั้งหมดของระดับการให้บริการวัดผลได้	
● เป้าหมายทั้งหมดในข้อตกลงสำหรับระดับการปฏิบัติการและสัญญาที่ตกลงไว้กับผู้ให้บริการภายนอก สอดคล้องกับ SLA	
● เกณฑ์วัดต่างๆ ได้รับการจัดทำขึ้นจากระบบและมีการป้องกันการแก้ไข	
● มีการนำเสนอ SLA ต่อผู้บริหาร (และลูกค้า) เพื่อสอบทาน	
● มีกระบวนการจัดการกับคำร้องทุกข์จากลูกค้า	
การบริหารจัดการเหตุการณ์	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าองค์กรมีกระบวนการในการดำเนินการกับเหตุการณ์ต่างๆ	
ความเสี่ยง: ธุรกิจหยุดชะงักและมีปัญหาผลการดำเนินงาน	
● มีกระบวนการและเครื่องมือเพื่อดำเนินการกับปัญหา	
● ข้อมูลในการบริหารจัดการเหตุการณ์เป็นแบบรวมศูนย์และเข้าถึงได้	
● บุคลากรในการบริหารจัดการเหตุการณ์สามารถเข้าถึงข้อมูลสารสนเทศใน CMDB	
● เหตุการณ์ต่างๆ จะถูกจัดการด้วยตัวชี้วัดผลการดำเนินงานที่ชัดเจนคือ เวลาที่เหตุการณ์อยู่ในความรับผิดชอบ (time to own: TTO) และเวลาที่ใช้แก้ไข (time to fix: TTF)	
● เกณฑ์วัดได้รับการสอบทานโดยผู้บริหารและดำเนินการแก้ไขตามจำเป็น	
● บุคลากรในการบริหารเหตุการณ์ได้รับการฝึกอบรม	
● เหตุการณ์จะถูกจัดกลุ่มและลำดับความสำคัญในแนวทางที่สนับสนุนธุรกิจ	
การบริหารจัดการปัญหา	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าองค์กรมีกระบวนการในการจัดการปัญหา	
ความเสี่ยง: ต้นเหตุของปัญหาไม่ได้รับการระบุ และเหตุการณ์ต่างๆ ยังคงทำให้ธุรกิจหยุดชะงัก	
● ปัญหาต่างๆ ได้รับการระบุและแบ่งระดับ	
● ปัญหาต่างๆ ได้รับการตรวจสอบและวิเคราะห์หาสาเหตุ โดยมีการบันทึกต้นเหตุของปัญหา	
● ปัญหาต่างๆ ได้รับการแก้ไข และมีการสื่อสารถึงสถานะ/การปรับให้เป็นปัจจุบันให้ผู้บริหารรับทราบ	
การปฏิบัติการศูนย์คอมพิวเตอร์	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าศูนย์คอมพิวเตอร์ที่มีผลกระทบต่อการให้บริการมีโครงสร้างพื้นฐานเหมาะสมที่จะป้องกันระบบใช้งานไม่ได้หรือการบริการหยุดชะงัก (โดยปกติแล้ว ควรเป็น Tier III ตามที่กำหนดโดย Uptime Institute)	
ความเสี่ยง: ผู้ให้บริการไม่สามารถจัดหาและดูแลรักษาการส่งมอบบริการ	
● มีการรักษาความมั่นคงปลอดภัยทางกายภาพและในเชิงตรรกะ และได้รับการบริหารจัดการอย่างเหมาะสม	

• มีการติดตามดูแลระดับอุณหภูมิและความชื้น	
• มีการติดตั้งระบบไฟฟ้า/UPS (universal power supply) และสายดิน เพื่อป้องกันการล้มเหลวเฉพาะจุด ไฟดับหรือการบริการหยุดชะงัก	
• มีการติดตั้งเครื่องดักจับควันไฟและมาตรการป้องกันไฟไหม้ รวมทั้งมีการทดสอบเป็นระยะๆ	
การบริหารโปรแกรม/โครงการ	
วัตถุประสงค์การตรวจสอบ: พิจารณาว่าองค์กรใช้ระเบียบวิธีที่เป็นมาตรฐานในการบริหารโครงการหรือไม่	
ความเสี่ยง: โครงการไม่บรรลุวัตถุประสงค์ของธุรกิจ โครงการเกินกำหนดในตารางเวลาและงบประมาณ	
การออกแบบและพัฒนา – พิจารณาว่ามีการบรรลุตามเกณฑ์ต่อไปนี้ :	
• มีเหตุผลทางธุรกิจที่ชัดเจนและมั่นคงสำหรับโครงการ	
• มีการประเมินต้นทุนและประโยชน์ตามที่เป็นจริงและมีเนื้อหาครอบคลุม	
• ผู้มีส่วนได้เสียหลักทุกคนมีส่วนร่วมในขั้นตอนแต่เนิ่นๆ	
• มีการพิจารณาอย่างละเอียดรอบคอบถึงเรื่องการควบคุมการรักษาความมั่นคงปลอดภัยและความถูกต้องครบถ้วน	
การบริหารโครงการ – พิจารณาว่ามี:	
• การเป็นผู้นำเชิงรุกและการรายงานแบบทันกาล	
• การมีส่วนร่วมของผู้มีส่วนได้เสียหลักทุกคน	
• การระบุปัญหาและรายงานต่อผู้เกี่ยวข้องในระดับสูงต่อไป	
• มีตารางการทำงานตามที่เป็นได้จริงและมีเป้าหมายที่ชัดเจน	
• การทดสอบที่เข้มงวดและมีการนำร่องก่อนใช้งานจริง	
การนำไปใช้งาน – พิจารณาว่ามี:	
• การบริหารการเปลี่ยนแปลงและการฝึกอบรม	
• การติดตามผลประโยชน์เป็นประจำและเชื่อถือได้	
• การประเมินความพึงพอใจของลูกค้าอย่างต่อเนื่อง	