GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

เทคโนโลยีสารสนเทศ ความเสี่ยงและวิธีการควบคุม

ฉบับที่ 2

The Institute of Internal Auditors

แนวทางการตรวจสอบเทคโนโลยีระดับโลก

(Global Technology Audit Guide (GTAG®) 1)

เทคโนโลยีสารสนเทศ
ความเสี่ยงและวิธีการควบคุม

ฉบับที่ 2

มีนาคม 2555

บทสรุปสำหรับผู้บริหาร

GTAG ฉบับนี้จะช่วยให้หัวหน้าหน่วยงานตรวจสอบภายใน (Chief Audit Executive - CAE) และผู้ตรวจสอบภายในก้าวทันต่อการเปลี่ยนแปลงและความซับซ้อนของโลก IT โดยการจัดทำเป็นแนวทางที่เป็นลายลักษณ์อักษรให้กับผู้บริหารสายธุรกิจ (ซึ่งไม่ใช่ผู้บริหารด้าน IT) นำไปใช้งานได้ ผู้บริหารและคณะกรรมการต่างมีความคาดหวังว่าหน่วยงานตรวจสอบภายในจะให้ความเชื่อมั่นในความเสี่ยงที่สำคัญทั้งหมด ซึ่งรวมถึงความเสี่ยงที่เกิดขึ้นจากการนำ IT มาใช้งานหรือมาช่วยในงาน GTAG ที่ออกมาเป็นชุดจะช่วยให้ CAE และผู้ตรวจสอบภายในมีความรู้เพิ่มขึ้นเกี่ยวกับความเสี่ยง การควบคุม และประเด็นด้านการกำกับดูแลเทคโนโลยีโดยรอบเทคโนโลยีต่างๆ เป้าหมายของ GTAG ฉบับนี้คือต้องการช่วยให้ผู้ตรวจสอบภายในเกิดความสะดวกใจมากขึ้นเกี่ยวกับวิธีการควบคุมทั่วไปด้าน IT เพื่อที่พวกเขาจะได้สามารถพูดคุยกับคณะกรรมการ และสามารถแลกเปลี่ยนความคิดเห็นเกี่ยวกับความเสี่ยงและการควบคุมกับหัวหน้าหน่วยงานสารสนเทศ (CIO) และผู้บริหารด้าน IT GTAG ฉบับนี้ได้อธิบายถึงวิธีการที่ผู้ที่มีหน้าที่ในการกำกับดูแล ผู้บริหารระดับสูง ผู้เชี่ยวชาญด้าน IT และผู้ตรวจสอบภายในระบุประเด็นความเสี่ยงและวิธีการควบคุมที่สำคัญที่เกี่ยวข้องกับ IT ได้ รวมทั้งได้นำเสนอกรอบแนวทางที่เกี่ยวข้องสำหรับการประเมินความเสี่ยงและวิธีการควบคุมด้าน IT

ยิ่งกว่านั้นยังเป็นการปูพื้นฐานสำหรับ GTAG ฉบับอื่นๆ ที่ครอบคลุมรายละเอียดที่มากขึ้นสำหรับหัวข้อ IT ที่เฉพาะเจาะจงมากขึ้น และบทบาทและภาระหน้าที่ในทางธุรกิจที่เกี่ยวข้อง

แนวทางฉบับนี้เป็นฉบับที่สองในชุดแนวทางชุดแรกของ GTAG กล่าวคือ GTAG 1: วิธีการควบคุมเทคโนโลยีสารสนเทศ - ซึ่งถูกตีพิมพ์ในเดือนมีนาคม 2548 เป้าหมายคือ เพื่อแสดงให้เห็นภาพรวมของหัวข้อเรื่องความเสี่ยงและวิธีการควบคุมที่เกี่ยวข้องกับ IT

1. บทนำ

จุดประสงค์ของ GTAG ฉบับนี้ ก็คือ เพื่ออธิบายเรื่องความเสี่ยงและวิธีการควบคุมด้าน IT ในรูปแบบที่ช่วยให้ CAE และผู้ตรวจสอบภายในเข้าใจและสื่อสารถึงความจำเป็นที่ต้องมีวิธีการควบคุมด้าน IT ที่แข็งแกร่ง โดยได้จัดรูปแบบในลักษณะที่จะช่วยนำพาผู้อ่านสามารถอ่านทำความเข้าใจในกรอบสำหรับการประเมินวิธีการควบคุมด้าน IT ได้ตั้งแต่ต้นจนจบ และช่วยให้ผู้อ่านให้ความสนใจหัวข้อเฉพาะตามที่ตนต้องการได้ GTAG ฉบับนี้ได้ให้ภาพรวมขององค์ประกอบสำคัญในการประเมินการควบคุมด้าน IT โดยเน้นถึงบทบาทและหน้าที่ของผู้ที่มีส่วนสำคัญภายในองค์กรที่จะสามารถขับเคลื่อนการกำกับดูแลทรัพยากร IT ผู้อ่านบางคนอาจคุ้นเคยกับบางแง่มุมใน GTAG ฉบับนี้ แต่บางส่วนก็จะให้มุมมองใหม่ๆ ว่าจะมีแนวทางจัดการความเสี่ยงและวิธีการควบคุมด้าน IT อย่างไร เป้าหมายหนึ่งของ GTAG ฉบับนี้และฉบับอื่นๆ ในชุดนี้คือองค์ประกอบในการประเมินการควบคุมด้าน IT สามารถใช้เพื่อให้ความรู้แก่ผู้อื่นได้ว่า ความเสี่ยงและวิธีการควบคุมด้าน IT คืออะไร และเหตุใดผู้บริหารและตรวจสอบภายในจึงควรมั่นใจได้ว่า มีการให้ความสนใจในเรื่องความเสี่ยงด้าน IT และวิธีการควบคุมขั้นพื้นฐานอย่างเหมาะสม เพื่อที่จะส่งเสริมและคงไว้ซึ่งสภาพแวดล้อมการควบคุมด้าน IT ที่มีประสิทธิผลได้

แม้ว่าเทคโนโลยีจะสร้างโอกาสในการเจริญเติบโตและการพัฒนา แต่ในอีกมุมนั้น ก็มาพร้อมกับภัยคุกคาม เช่น การเปลี่ยนแปลงที่เกิดขึ้นอย่างรวดเร็ว (Disruptive) การหลอกลวง การโจรกรรม และการทุจริต เป็นต้น มีผลงานวิจัยที่ได้แสดงให้เห็นว่า ผู้โจมตีจากภายนอกนั้นเป็นภัยต่อองค์กร แต่บุคคลภายในที่มองว่าเชื่อถือได้ (Trusted insider) กลับเป็นภัยคุกคามที่ยิ่งใหญ่กว่ามาก ยังโชคดีที่เทคโนโลยีสามารถจัดให้มีการปกป้ององค์กรจากภัยคุกคามได้ ดังเช่นที่แนวปฏิบัติฉบับนี้จะแสดงให้เห็นต่อไป ผู้บริหารควรรู้จักที่จะถามคำถามที่ถูกต้อง และคำตอบหมายถึงอะไร ตัวอย่างเช่น:

- เหตุใดเราจำเป็นต้องทำความเข้าใจกับความเสี่ยงและวิธีการควบคุมด้าน IT?
  2 เรื่อง คือ ความเชื่อมั่นและความเชื่อถือได้ ผู้บริหารมีบทบาทสำคัญในการทำให้มั่นใจได้ว่าข้อมูลความน่าเชื่อถือ ส่วนการให้ความเชื่อมั่นในเบื้องต้นมาจากการพึ่งพาซึ่งกันและกันของวิธีการควบคุมต่างๆ ในทางด้านธุรกิจ รวมทั้งจากหลักฐานที่แสดงว่ามีวิธีการควบคุมอยู่อย่างเพียงพอและทำงานอย่างต่อเนื่อง ฝ่ายบริหารต้องชั่งน้ำหนักระหว่างหลักฐานที่ได้มาจากวิธีการควบคุมและหลักฐานที่ได้มาจากการตรวจสอบ และสรุปผลว่ามันสามารถให้ความมั่นใจได้อย่างสมเหตุสมผล
- อะไรบ้างที่เราควรปกป้อง? ความไว้วางใจ (Trust) ควรได้รับการปกป้อง เพราะเป็นสิ่งที่ทำให้มั่นใจในธุรกิจและประสิทธิภาพ วิธีการควบคุมก่อให้เกิดพื้นฐานสำหรับความไว้วางใจ แม้ว่าจะเป็นสิ่งที่มักจะมองไม่เห็น เทคโนโลยีก่อให้เกิดพื้นฐานสำหรับวิธีการควบคุมทางธุรกิจเป็น

ส่วนใหญ่หรือแทบทั้งหมด ความเชื่อถือได้ของข้อมูลและกระบวนการทางการเงิน (ซึ่งปัจจุบันเป็นข้อกำหนดที่หลีกเลี่ยงไม่ได้ในหลายๆ องค์กร) ทั้งหลายทั้งปวงเป็นเรื่องของความไว้วางใจ

- วิธีการควบคุมทาง IT ได้ถูกนำไปใช้ที่ไหนบ้าง? ในทุกที่ โดย IT หมายรวมถึงองค์ประกอบของเทคโนโลยี กระบวนการ บุคลากร องค์กร และสถาปัตยกรรมด้าน IT รวมทั้งข้อมูลด้วย วิธีการควบคุมด้าน IT หลายๆ วิธี โดยลักษณะแล้วเป็นเรื่องทางด้านเทคนิค และ IT ก็ให้เครื่องมือสำหรับวิธีการควบคุมทางธุรกิจหลายๆ วิธี
- เป็นหน้าที่ของใคร? ทุกคน อย่างไรก็ตาม ผู้บริหารต้องกำหนดบุคคลหรือหน่วยงานที่เป็นเจ้าของและมีหน้าที่ในการควบคุมและเผยแพร่ให้ชัดเจน มิฉะนั้น จะไม่มีใครรับผิดชอบและผลลัพธ์ที่ตามมาอาจจะถึงขั้นรุนแรงได้
- ควรประเมินความเสี่ยงและวิธีการควบคุมด้าน IT เมื่อใด? ควรทำเสมอๆ เนื่องจาก IT มีสภาพแวดล้อมที่เปลี่ยนแปลงไปอย่างรวดเร็ว ส่งผลให้เกิดการเปลี่ยนแปลงในกระบวนการและการเปลี่ยนแปลงในทางองค์กร ความเสี่ยงใหม่ๆ เกิดขึ้นอย่างรวดเร็ว วิธีการควบคุมจะต้องแสดงหลักฐานของความมีประสิทธิผลได้อย่างต่อเนื่อง และหลักฐานเหล่านั้นจะต้องได้รับการประเมินผลอย่างสม่ำเสมอ
- ต้องควบคุมแค่ไหนจึงจะเพียงพอ? ฝ่ายบริหารจะต้องตัดสินใจเลือกวิธีการควบคุมที่เหมาะสมบนพื้นฐานของระดับความเสี่ยงและช่วงเบี่ยงเบนของความเสี่ยงที่ยอมรับได้และกฎระเบียบข้อบังคับที่เกี่ยวข้อง วิธีการควบคุมไม่ใช่วัตถุประสงค์ แต่วิธีการควบคุมมีอยู่เพื่อช่วยให้บรรลุวัตถุประสงค์ในทางธุรกิจได้ วิธีการควบคุมนั้นเป็นต้นทุนในการทำธุรกิจและอาจมีราคาแพง แต่ก็ยังไม่แพงเท่ามูลค่าความเสียหายของผลกระทบที่อาจเกิดขึ้นได้หากมีวิธีการควบคุมที่ไม่เพียงพอ

วิธีการควบคุมด้าน IT เป็นสิ่งจำเป็นต่อการปกป้องทรัพย์สิน ลูกค้า คู่ค้า และข้อมูลที่เป็นความลับ แสดงให้เห็นถึงความปลอดภัยมีประสิทธิภาพและพฤติกรรมเชิงจริยธรรม และรักษาไว้ซึ่งภาพลักษณ์ชื่อเสียงและความไว้วางใจ ในตลาดโลกและสภาพข้อบังคับทางกฎหมายในปัจจุบันที่สิ่งเหล่านี้อาจเกิดความสูญเสียได้ง่าย CAE สามารถใช้แนวปฏิบัติฉบับนี้เพื่อเป็นพื้นฐานในการประเมินกรอบการควบคุมด้าน IT ขององค์กรและวิธีปฏิบัติของตรวจสอบภายในในเรื่องความเสี่ยงและวิธีการควบคุมด้าน IT การปฏิบัติตามกฎระเบียบ และการให้ความเชื่อมั่น นอกจากนี้ ยังสามารถใช้เพื่อเผชิญกับความท้าทายจากการเปลี่ยนแปลงที่เกิดขึ้นตลอดเวลา ความซับซ้อนที่กำลังเพิ่มขึ้นเรื่อยๆ การพัฒนาไปอย่างรวดเร็วของภัยคุกคามและความจำเป็นในการปรับปรุงประสิทธิภาพ

ไม่มีวิธีการควบคุมด้าน IT ใดที่แยกไปอยู่ต่างหาก ทุกวิธีเหล่านั้นอยู่ในรูปแบบที่ต้องพึ่งพาซึ่งกันและกันอย่างต่อเนื่องและบูรณาการเพื่อสร้างเกราะป้องกัน แต่ก็อาจถูกทำลายได้หากมีจุดใดจุดหนึ่งของการเชื่อมโยงเกิดอ่อนแอขึ้น วิธีการควบคุมด้าน IT ขึ้นอยู่กับข้อผิดพลาดและการฝ่าฝืนกฎเกณฑ์ของผู้บริหาร ซึ่งอาจเป็นได้ตั้งแต่วิธีง่ายๆ ไปจนถึงเรื่องทางเทคนิคขั้นสูง และมีอยู่ในสภาพแวดล้อมที่มีการเปลี่ยนแปลงตลอดเวลา วิธีการควบคุมด้าน IT ประกอบด้วยองค์ประกอบที่สำคัญ 2 องค์ประกอบ: กล่าวคือ วิธีการควบคุมทางธุรกิจที่เป็นแบบอัตโนมัติ (ซึ่งเป็นการควบคุมเพื่อสนับสนุนการบริหารจัดการและการกำกับดูแลธุรกิจ) และการควบคุมสภาพแวดล้อมด้าน IT และการปฏิบัติงาน (ซึ่งสนับสนุนระบบงานต่างๆ และโครงสร้างพื้นฐานทางด้าน IT) CAE จำเป็นต้องคำนึงและประเมินองค์ประกอบทั้งสอง โดย CAE อาจมองว่าวิธีการควบคุมทางธุรกิจโดยอัตโนมัตินั้น คือวิธีการควบคุมที่ต้องอาศัยทักษะในการตรวจสอบทั้งด้านธุรกิจร่วมกันกับด้าน IT มาใช้ในงานตรวจสอบแบบบูรณาการ (integrated audit) CAE อาจต้องการแยกวิธีการควบคุมทั่วไปทางด้าน IT หรือ General Computer Controls (GCCs) โดยตั้งอยู่บนพื้นฐานของทักษะทางด้านเทคนิคและความสามารถอื่นๆ ที่จำเป็นในการประเมินระบบงานต่างๆ โครงสร้างพื้นฐานและการปฏิบัติงานต่างๆ ที่ใช้เทคนิคมากกว่า ตัวอย่างเช่น โปรแกรมการวางแผนทรัพยากรทางธุรกิจขององค์กร (Enterprise Resource Planning -ERP) ซึ่งต้องใช้ความรู้ทางด้านเทคนิคในการทำความเข้าใจและประเมินวิธีการควบคุมบนโครงสร้างฐานข้อมูลของ ERP การเข้าถึงระบบของผู้ใช้งาน (user access) การกำหนดค่าติดตั้งของระบบ (system configuration) และรายงานทางการเงิน CAE จะพบว่าในการประเมินโครงสร้างพื้นฐาน IT เช่น เครือข่าย เราเตอร์ (อุปกรณ์เชื่อมต่อเครือข่าย) ไฟร์วอลล์ (ระบบรักษาความปลอดภัยของเครือข่าย) เครือข่ายไร้สาย และอุปกรณ์เคลื่อนที่แบบไร้สาย ต้องอาศัยผู้มีทักษะเฉพาะและมีประสบการณ์ในการตรวจสอบ บทบาทผู้ตรวจสอบภายในเกี่ยวกับวิธีการควบคุมด้าน IT จะเริ่มต้นด้วยการมีความเข้าใจในหลักการแนวคิดเป็นอย่างดี ไปจนถึงจุดสุดท้ายด้วยการเสนอผลจากการประเมินความเสี่ยงและการควบคุม การตรวจสอบภายในจะต้องมีปฏิสัมพันธ์อย่างมีนัยสำคัญกับบุคลากรในตำแหน่งที่มีหน้าที่ในการควบคุม และจำเป็นต้องมีการเรียนรู้อย่างต่อเนื่อง และทำการประเมินซ้ำเมื่อมีเทคโนโลยีใหม่ๆ เกิดขึ้น รวมทั้งเมื่อโอกาส การนำมาใช้งาน การพึ่งพาอาศัย กลยุทธ์ ความเสี่ยง ความต้องการ (requirements) มีการเปลี่ยนแปลง

วิธีการควบคุมด้าน IT จะช่วยให้เกิดความมั่นใจในความน่าเชื่อถือของข้อมูลและการให้บริการสารสนเทศ วิธีการควบคุมด้าน IT จะช่วยบรรเทาความเสี่ยงที่มีมาพร้อมกับการใช้เทคโนโลยีขององค์กร วิธีการควบคุมมีได้ตั้งแต่จากการมีนโยบายขององค์กรไปจนถึงการนำไปใช้ปฏิบัติงานจริงภายใต้วิธีใช้งานที่กำหนดไว้ หรือเริ่มจากการป้องกันการเข้าถึงทางกายภาพไปจนถึงความสามารถในการติดตามร่องรอยการกระทำและรายการธุรกรรมไปถึงบุคคลผู้รับผิดชอบได้ และเริ่มจากรายการแก้ไขอัตโนมัติไปจนถึงการวิเคราะห์ความสมเหตุสมผลสำหรับข้อมูลที่มีขนาดใหญ่

ต่อไปนี้เป็นตัวอย่างของแนวคิดเรื่องการควบคุมหลัก (Key control):

- วิธีการควบคุมด้าน IT ที่มีอยู่ในระบบของการควบคุมภายในจะก่อให้เกิดความเชื่อมั่น โดยความเชื่อมั่นนี้ ควรมีอย่างต่อเนื่องและให้ร่องรอยของหลักฐานที่เชื่อถือได้
- การให้ความเชื่อมั่นของผู้ตรวจสอบภายใน คือการประเมินอย่างเป็นอิสระ และเที่ยงธรรม ว่าวิธีการควบคุมที่เกี่ยวข้องกับ IT ได้ดำเนินไปตามที่ตั้งใจไว้ ความเชื่อมั่นนี้ตั้งอยู่บนพื้นฐานของความเข้าใจ การตรวจสอบ และประเมินวิธีการควบคุมที่สำคัญที่ใช้จัดการความเสี่ยงที่เกี่ยวข้อง และดำเนินการทดสอบอย่างเพียงพอเพื่อให้มั่นใจว่าวิธีการควบคุมเหล่านั้นได้รับการออกแบบมาอย่างเหมาะสม และยังทำงานได้อย่างมีประสิทธิผลและอย่างต่อเนื่อง

มีกรอบอยู่หลากหลายสำหรับการจัดประเภทวิธีการควบคุมด้าน IT และวัตถุประสงค์ของวิธีการควบคุม แนวปฏิบัติฉบับนี้ใคร่แนะนำให้แต่ละองค์กรพิจารณานำองค์ประกอบที่สามารถนำไปใช้งานได้จริง ของกรอบที่มีอยู่ในปัจจุบัน เพื่อจัดประเภทและประเมินความเสี่ยงและวิธีการควบคุมด้าน IT

2. ความรู้เบื้องต้นเกี่ยวกับพื้นฐานของความเสี่ยงและวิธีการควบคุมทางธุรกิจที่เกี่ยวข้องกับ IT

2.1 แนวคิดหลัก

องค์กรหลายๆ องค์กร ยังคงใช้ประโยชน์จากศักยภาพของเทคโนโลยีซึ่งมีการเปลี่ยนแปลงตลอดเวลาอย่างต่อเนื่อง เพื่อพัฒนาสินค้าและบริการในลักษณะที่นำมาซึ่งความท้าทายต่อวิชาชีพการตรวจสอบภายใน มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (มาตรฐาน) ของ IIA ได้ตั้งข้อสังเกตไว้โดยเฉพาะว่า ผู้ตรวจสอบภายในจะต้องประเมินและสรุปผลความเสี่ยงและวิธีการควบคุมสำหรับระบบสารสนเทศที่ใช้ภายในองค์กร IIA ได้ให้มุมมองเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยงและวิธีการควบคุมที่เกี่ยวกับ IT โดยผ่าน GTAG ในอีกหลายๆ ฉบับ ดังนี้ GTAG 4: การบริหารการตรวจสอบด้าน IT (Management of IT Auditing) ซึ่งได้อธิบายความเสี่ยงด้าน IT และการส่งผลต่อความเสี่ยงด้าน IT ทั้งหมด (IT risk universe) GTAG 11: การพัฒนาแผนการตรวจสอบด้าน IT (Developing the IT Audit Plan) ซึ่งจะช่วยให้ผู้ตรวจสอบภายในประเมินสภาพแวดล้อมทางธุรกิจที่มีการนำเทคโนโลยีไปใช้งานและแง่มุมที่เป็นไปได้ของการตรวจสอบ IT ทั้งหมด (IT audit universe) GTAG 8: การตรวจสอบวิธีการควบคุมระบบงาน (Auditing Application Controls) ครอบคลุมเฉพาะแง่มุมของการตรวจสอบวิธีการควบคุมในระบบงานและแนวทางที่ผู้ตรวจสอบภายในสามารถนำมาปรับใช้เมื่อทำการประเมินวิธีการควบคุม

คำว่าคณะกรรมการ (Board) ที่ใช้ใน GTAG ฉบับนี้ มีความหมายตามที่ได้กำหนดไว้ในภาคอภิธานศัพท์ของมาตรฐาน: “คณะกรรมการคือคณะบุคคลที่ทำหน้าที่ในการกำกับดูแลองค์กร เช่น คณะกรรมการองค์กร คณะกรรมการกำกับดูแล หัวหน้าหน่วยงานหรือองค์คณะที่ทำหน้าที่ร่างกฎหมาย คณะกรรมการนโยบาย หรือทรัสตีขององค์กรที่ไม่แสวงหาผลกำไร หรือองค์คณะอื่นๆ ที่ได้รับแต่งตั้ง รวมถึงคณะกรรมการตรวจสอบที่หัวหน้าหน่วยงานตรวจสอบภายในต้องรายงานตามหน้าที่ต่อ”

เนื่องจาก GTAG ฉบับนี้จะสำรวจให้ลึกลงไป ในการประเมินความเสี่ยงและวิธีการควบคุมด้าน IT ที่มีอยู่ที่จะใช้จัดการกับความเสี่ยงเหล่านั้น จะต้องมีมาพร้อมกับสภาพแวดล้อมของกระบวนการทางธุรกิจที่ได้กำหนดไว้แล้ว และวัตถุประสงค์บางประการขององค์กรที่จำเป็นต้องบรรลุให้ได้ตามที่ผู้บริหารระดับสูงและคณะกรรมการได้ให้แนวทางไว้ ความเสี่ยงด้าน IT เป็นเพียงส่วนหนึ่งในภาพรวมของการเชื่อมต่อที่ซับซ้อนระหว่างบุคลากร กระบวนการโครงสร้างพื้นฐาน และสภาพแวดล้อมความเสี่ยงขององค์กรที่มีอยู่และควรได้รับการจัดการในคราวเดียวกันทั้งหมดโดยองค์กร

ผู้ตรวจสอบภายในจำเป็นต้องเข้าใจในวิธีการควบคุมต่างๆ ที่มีอยู่มากมายเพื่อใช้บรรเทาความเสี่ยงด้าน IT วิธีการควบคุมอาจจะถูกนึกถึงในลักษณะที่มีอยู่ในลำดับชั้นหนึ่งๆ ที่ต้องพึ่งพาการเชื่อมต่อของวิธีการ

ควบคุมต่างๆ ในทางการปฏิบัติงานอย่างมีประสิทธิผล รวมทั้งการตระหนักว่า ความล้มเหลวของชุดวิธีการควบคุมชุดหนึ่งจะสามารถนำไปสู่การพึ่งพาและการตรวจสอบที่จำเป็นในกลุ่มวิธีการควบคุมอื่นที่มากขึ้นได้ ในเอกสารฉบับนี้ จะกล่าวถึงวิธีการควบคุมในรูปของคำต่างๆ เป็นต้นว่า การกำกับดูแล การบริหาร สิ่งที่เกี่ยวข้องทางเทคนิค และระบบงาน/แอพพลิเคชัน ขึ้นอยู่กับว่าผู้ใดในองค์กรจะเป็นคนนำวิธีการควบคุมเหล่านั้นไปใช้ปฏิบัติและดูแลวิธีการควบคุมเหล่านั้น

อีกมุมมองหนึ่งของวิธีการควบคุมทางด้าน IT คือ มองในแง่ของวิธีการควบคุมทั่วไป และวิธีการควบคุมระบบงาน/แอพพลิเคชัน วิธีการควบคุมทั่วไปโดยธรรมชาติแล้วมักจะกระจายอยู่ไปทั่วและมักจะได้รับการพูดถึงในหลายๆ งานตรวจสอบ ตัวอย่างได้แก่ การปฏิบัติงานด้าน IT การพัฒนาและบำรุงรักษาระบบงาน การบริหารจัดการผู้ใช้งาน การบริหารการเปลี่ยนแปลง และการสำรองและกู้ข้อมูล เป็นต้น วิธีการควบคุมระบบงานจะก่อให้เกิดประเภทของวิธีการควบคุมอีกกลุ่มหนึ่ง ซึ่งรวมถึงวิธีการควบคุมที่มีอยู่ในระบบงานที่เกี่ยวกับ การนำเข้า (Input) การประมวลผล (Processing) และสิ่งที่ได้จากการประมวลผล (output)

GTAG ฉบับนี้จะสำรวจการใช้วิธีการควบคุมต่างๆ ในการบริหารและกำกับดูแลโครงสร้างพื้นฐาน กระบวนการ และบุคลากรที่สนับสนุนธุรกิจโดยผ่านทางเทคโนโลยี การกำกับดูแลทาง IT ภายในองค์กรยังคงต้องมีวัฒนาการอย่างต่อเนื่อง เนื่องมาจากการใช้ IT ที่มีอย่างไม่หยุดหย่อน เทคโนโลยี รวมทั้งการดูแลโดยฝ่ายบริหารและคณะกรรมการที่เพิ่มมากขึ้น

2.2 การกำกับดูแลด้าน IT

เมื่อกล่าวถึงหัวข้อวิธีการควบคุมด้าน IT สิ่งสำคัญที่ต้องคำนึงถึงคือ การกำกับดูแลด้าน IT ซึ่งจะให้กรอบเพื่อที่จะมั่นใจได้ว่า IT จะสามารถสนับสนุนความต้องการทางธุรกิจโดยรวมขององค์กรได้ สิ่งที่สำคัญสำหรับผู้บริหารงานด้าน IT คือ ต้องมีความเข้าใจอย่างแท้จริงในกระบวนการทางธุรกิจขององค์กรซึ่งถูกนำมาใช้เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายตามที่ผู้บริหารระดับสูงและคณะกรรมการได้กำหนดไว้ การกำกับดูแลด้าน IT ไม่ใช่เพียงประกอบด้วยวิธีการควบคุมที่จำเป็นเพื่อจัดการกับความเสี่ยงที่ได้ระบุไว้แล้วเท่านั้น แต่ยังเป็นโครงสร้างที่บูรณาการวิธีปฏิบัติด้าน IT และบุคลากรเข้าด้วยกันซึ่งจะต้องสอดคล้องกันเป็นอย่างมากกับ (และช่วยให้บรรลุ) กลยุทธ์และเป้าหมายโดยรวมขององค์กร

CAE จำเป็นต้องมีความสามารถที่จะประเมินโครงสร้างการกำกับดูแลด้าน IT และความสามารถของโครงสร้างนี้ในการส่งมอบผลงานให้แก่องค์กรรวมทั้งปรับปรุงประสิทธิภาพของกิจกรรมด้าน IT ได้ มีงานวิจัยที่ได้ชี้ให้เห็นว่า การกำกับดูแลด้าน IT ที่ดีนั้น จะนำไปสู่ผลการดำเนินงานทางธุรกิจที่ดีขึ้น รวมทั้งการนำ IT มาใช้ในทางธุรกิจเพื่อบรรลุวัตถุประสงค์เชิงกลยุทธ์ ก็จะมีความสอดคล้องกันมากขึ้น

การกำกับดูแลด้าน IT ประกอบไปด้วย ความเป็นผู้นำ โครงสร้างองค์กร และกระบวนการ ซึ่งจะทำให้มั่นใจได้ว่า IT จะดำรงอยู่และสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรได้

ตามข้อกำหนดของ IIA ในมาตรฐาน 2110.A2 ที่ระบุว่า หน่วยงานตรวจสอบภายในต้องประเมินว่าการกำกับดูแลด้าน IT ขององค์กรนั้น สนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่ ดังนั้น CAE จึงจำเป็นที่ต้องมีการเตรียมตัวเพื่อประเมินด้านที่สำคัญของงานที่ใช้ IT ทั้งหมด

การประยุกต์ใช้หลักการกำกับดูแลด้าน IT ที่เหมาะสมนั้น จะสามารถมีอิทธิพลและส่งผลต่อทั้งองค์กรและวิธีที่ IT มีปฏิสัมพันธ์กับธุรกิจได้

- **การระบุและการบริหารความเสี่ยงด้าน IT และ การสร้างความพร้อมของการปฏิบัติงานด้าน IT ที่ได้รับการปรับปรุงมาแล้ว**: กล่าวคือ การกำกับดูแลด้าน IT จะช่วยให้มั่นใจได้ว่า มีการเชื่อมโยงกันอย่างใกล้ชิดกับหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงซึ่งรวมถึงการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM) การกำกับดูแลด้าน IT จำเป็นต้องเป็นส่วนที่บูรณาการเข้าไปในการบริหารความเสี่ยงของบริษัทโดยรวม เพื่อที่จะได้มีการผนวกเทคนิคที่เหมาะสมเข้าไปในกิจกรรมด้าน IT ทั่วทั้งองค์กร ซึ่งรวมถึงการสื่อสารถึงสถานะความเสี่ยงไปยังผู้มีส่วนได้ส่วนเสียที่สำคัญด้วย CAE ควรสอบทานกิจกรรมการบริหารความเสี่ยงที่องค์กรนำมาใช้ในองค์กรทั้งหมด และตรวจสอบให้มั่นใจว่า มีการเชื่อมโยงระหว่างการบริหารความเสี่ยงด้าน IT กับกิจกรรมความเสี่ยงของบริษัท และมีการดูแลใส่ใจในข้อมูลในรายการความเสี่ยงด้าน IT (IT Risk Profile) แล้วอย่างเหมาะสม

- **การเสริมสร้างความสัมพันธ์ระหว่างธุรกิจและ IT**: การกำกับดูแลด้าน IT ก่อให้เกิดกลไกอย่างหนึ่งในการเชื่อมโยงการใช้ IT กับกลยุทธ์และเป้าหมายโดยรวมขององค์กร ความสัมพันธ์ระหว่างธุรกิจและ IT จะทำให้มั่นใจได้ว่า มีการใช้ทรัพยากร IT ไปทำสิ่งที่ถูกต้องในเวลาที่เหมาะสม การสื่อสารระหว่าง IT และธุรกิจควรเป็นไปอย่างสะดวกราบรื่นและให้ข้อมูล ให้ความเข้าใจอย่างลึกซึ้งว่า IT กำลังส่งมอบอะไรให้ รวมทั้งสถานะของการดำเนินการเหล่านั้น CAE ควรตรวจสอบถึงความสอดคล้องและมั่นใจได้ว่า มีกระบวนการบริหารระบบงาน โครงการ และทรัพยากร (IT Portfolio Management) ที่รัดกุม ซึ่งจะเอื้อให้หน่วยงานธุรกิจและสายงาน IT ร่วมมือกันในการจัดลำดับความสำคัญของทรัพยากร โครงการใหม่ๆ และการตัดสินใจในการลงทุนทั้งหมด

- **ความชัดเจนในความสามารถของฝ่ายบริหารของ IT ให้บรรลุตามวัตถุประสงค์**: หน่วยงาน IT จะต้องกำหนดกลยุทธ์ของตนเพื่อสนับสนุนธุรกิจ ซึ่งส่วนหนึ่งก็คือ ทำให้มั่นใจได้ว่าการดำเนินงานด้าน IT ในแต่ละวันนั้นมีประสิทธิภาพและไม่มีความเสื่อมเสีย มีการกำหนดตัวชี้วัดและ

เป้าหมายที่ไม่เพียงแต่จะช่วยให้ IT สามารถปฏิบัติงานบนพื้นฐานของกลยุทธ์เท่านั้น แต่ยังเป็นแนวทางให้แก่กิจกรรมที่บุคลากรจะใช้ในการปรับปรุงความสมบูรณ์ (maturity) ของวิธีปฏิบัติด้าน IT ด้วย ผลลัพธ์ที่ได้จะช่วยให้หน่วยงาน IT สามารถดำเนินการตามกลยุทธ์ให้บรรลุวัตถุประสงค์ของตนตามที่กำหนดไว้และได้รับความเห็นชอบจากผู้นำขององค์กรแล้ว CAE ควรประเมินว่าการเชื่อมโยงระหว่างตัวชี้วัดและวัตถุประสงค์ด้าน IT นั้นสอดคล้องกับเป้าหมายขององค์กร และใช้เป็นตัวชี้วัดความคืบหน้าของความคิดริเริ่มใหม่ๆ ที่ได้รับการอนุมัติ นอกจากนี้ CAE ยังสามารถช่วยพิสูจน์ได้ว่าเกณฑ์นั้นสามารถใช้วัดผลได้อย่างมีประสิทธิผลและแสดงให้เห็นมุมมองที่สมจริงของการปฏิบัติงาน IT และการกำกับดูแลด้าน IT ที่อยู่บนพื้นฐานของยุทธวิธีและกลยุทธ์

- **การบริหารความเสี่ยงและการระบุโอกาสในการปรับปรุงอย่างต่อเนื่องสำหรับผลลัพธ์ทางธุรกิจและทางด้าน IT**: การบริหารความเสี่ยงเป็นองค์ประกอบสำคัญต่อโครงสร้างการกำกับดูแลด้าน IT ที่มีประสิทธิผลภายในองค์กรหนึ่งๆ การระบุและการจัดการความเสี่ยงด้าน IT จะช่วยส่งเสริมให้หน่วยงาน IT ดำเนินงานด้าน IT ได้อย่างมีประสิทธิผลมากยิ่งขึ้น ในขณะเดียวกันก็ระบุโอกาสในการปรับปรุงวิธีปฏิบัติด้าน IT ให้ดีขึ้นได้ไปพร้อมๆ กัน ควรมีการกำหนดตัวผู้เป็นเจ้าของความเสี่ยงด้าน IT ผู้ซึ่งจะสื่อสารสถานะของการบริหารความเสี่ยงตามกระบวนวิธีที่กำหนดให้แก่ผู้บริหารในทุกระดับได้รับทราบ CAE มีบทบาทสำคัญในการตรวจพิสูจน์ความสม่ำเสมอของความเสี่ยงด้าน IT ทั้งหมด และจะใช้ข้อมูลนี้เพื่อช่วยในการกำหนดประเด็นของงานตรวจสอบภายในทั้งหมด (internal audit universe) เพื่อการประเมินความเสี่ยงและการจัดทำแผนการตรวจสอบได้อย่างเป็นอิสระ แนวทางความเสี่ยงสำหรับผู้ปฏิบัติงานด้าน IT (The Risk IT Practitioner Guide) ที่พัฒนาโดยสถาบัน ITGI (IT Governance Institute) และ ISACA ได้ให้กรอบในการระบุและประเมินความเสี่ยงด้าน IT พร้อมๆ กับแสดงการเชื่อมโยงโดยตรงไปยัง Control Objectives for Information and Related Technology (COBIT)

- **การกำกับดูแลด้าน IT ช่วยปรับปรุงความสามารถในการปรับตัวของ IT ต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจและทางด้าน IT**: การกำกับดูแลด้าน IT จะก่อให้เกิดรากฐานสำหรับ IT ในการจัดการภาระหน้าที่ของ IT ได้ดีขึ้น และสนับสนุนธุรกิจโดยผ่านกระบวนการ รวมทั้งบทบาทและภาระหน้าที่ของบุคลากรด้าน IT ตามที่ได้กำหนดไว้ เมื่อมีการกำหนดอย่างเป็นทางการแล้ว IT ก็จะสามารถระบุความผิดปกติที่อาจเกิดขึ้นในแต่ละวันและมองเห็นแนวโน้มได้ดีขึ้น ซึ่งจะนำไปสู่การระบุสาเหตุที่แท้จริงของสถานการณ์และประเด็นปัญหา นอกจากนี้ IT ยังจะมีความสามารถในการปรับตัวให้ยืดหยุ่นมากขึ้นเพื่อรองรับคำขอเฉพาะกิจเป็นครั้งคราวหรือสมรรถนะในทางธุรกิจที่สูงขึ้น CAE ในทุกวันนี้ ต้องสามารถประเมินแหล่งกำเนิด

ของข้อมูลได้ (เช่น ข้อมูลจาก Help desk และบัตรจัดการปัญหา) เพื่อประเมินว่า IT ได้ดำเนินการกับประเด็นปัญหาที่ไม่เคยพบมาก่อนอย่างไร นอกจากนี้ CAE ยังสามารถสอบทานกระบวนการจัดการ portfolio ด้าน IT (IT portfolio management processes) เพื่อทำความเข้าใจว่า มีการจัดลำดับความสำคัญของความต้องการต่างๆ อย่างไร และมีความยืดหยุ่นในการจัดลำดับความสำคัญใหม่ให้เป็นไปตามลำดับความสำคัญที่เปลี่ยนไปขององค์กรหรือไม่

ในขณะที่หน่วยงานตรวจสอบภายในทำการประเมินโครงสร้างการกำกับดูแลและวิธีปฏิบัติด้าน IT ขององค์กร องค์ประกอบที่สำคัญหลายอย่างซึ่งนำไปสู่การกำกับดูแลด้าน IT ที่มีประสิทธิผลจะถูกนำมาประเมิน ได้แก่:

- **ภาวะผู้นำ** (Leadership): ประเมินความสัมพันธ์ระหว่างวัตถุประสงค์ด้าน IT และความต้องการในปัจจุบัน/ในเชิงกลยุทธ์ขององค์กร ประเมินการมีส่วนร่วมของผู้นำของหน่วยงาน IT ในการพัฒนาและดำเนินการตามเป้าหมายเชิงกลยุทธ์ขององค์กรอย่างต่อเนื่อง สอบทานว่ามีการมอบหมายบทบาทและภาระหน้าที่ภายในหน่วยงานด้าน IT อย่างไร รวมทั้งสอบทานว่าบุคลากรได้ปฏิบัติตามที่ได้กำหนดไว้หรือไม่ นอกจากนี้ ให้สอบทานบทบาทของผู้บริหารระดับสูงและคณะกรรมการในการช่วยสร้างและคงไว้ซึ่งระบบการกำกับดูแลด้าน IT ที่แข็งแกร่ง
- **โครงสร้างองค์กร**: สอบทานว่าและบุคลากรด้านธุรกิจและด้าน IT มีการโต้ตอบและสื่อสารความต้องการในปัจจุบันและอนาคตโดยผ่านโครงสร้างองค์กรที่มีอยู่กันอย่างไร รวมถึงบทบาทที่จำเป็นและสายการรายงานที่มีอยู่ในอันที่จะช่วยให้ IT สามารถสนับสนุนความต้องการของธุรกิจได้อย่างเพียงพอ ในขณะเดียวกัน ก็เปิดโอกาสให้หน่วยงานธุรกิจได้ระบุความต้องการของตนโดยผ่านกระบวนการประเมินและการจัดลำดับความสำคัญที่เป็นทางการ
- **กระบวนการด้าน IT**: ประเมินกิจกรรมและวิธีการควบคุมในกระบวนการด้าน IT ที่ใช้อยู่ในการบริหารจัดการความต้องการของธุรกิจไป ในขณะเดียวกันก็ให้ความเชื่อมั่นในกระบวนการทางธุรกิจและระบบงานที่รองรับอยู่ หน่วยงาน IT ใช้กระบวนการต่างๆ เพื่อสนับสนุนสภาพแวดล้อมด้าน IT และช่วยให้บริการตามความคาดหวังได้อย่างสม่ำเสมอ ประเมินและตัดสินว่า จะวัดว่า IT ช่วยให้องค์กรบรรลุเป้าหมายได้อย่างไร
- **การบริหารความเสี่ยง**: สอบทานกระบวนการต่างๆ ของหน่วยงาน IT ในการระบุ ประเมิน และเฝ้าติดตาม/บรรเทาความเสี่ยงที่มีอยู่ภายในสภาพแวดล้อมด้าน IT นอกจากนี้ ต้องตัดสินถึงความรับผิดชอบที่บุคลากรมีอยู่ภายในกระบวนการบริหารความเสี่ยง และความคาดหวังเหล่านี้จะบรรลุผลได้ดีเพียงใด ทำความเข้าใจว่ามีเหตุการณ์อะไรที่เกิดขึ้นและส่งผลกระทบต่อหน่วยงานด้าน IT เพื่อที่จะตัดสินว่ามีวิธีปฏิบัติในการบริหารความเสี่ยงที่เหมาะสมอยู่แล้วหรือไม่ และตัดสิน

ว่าข้อมูลทางสถิติที่เกี่ยวกับความเสี่ยง (เช่น ความถี่ของความเสี่ยง ผลกระทบ เทคนิคในการลดความเสี่ยง) ได้มีการบันทึกเป็นเอกสารไว้อย่างเหมาะสม และปรับปรุงให้เป็นปัจจุบันภายหลังจากเกิดเหตุการณ์ขึ้น

- **กิจกรรมการควบคุม**: ประเมินกิจกรรมการควบคุมด้าน IT ที่สำคัญซึ่งได้กำหนดไว้เพื่อบริหารงานด้าน IT ของตนและเพื่อสนับสนุนองค์กรโดยรวม ตรวจสอบภายในควรต้องสอบทานความเป็นเจ้าของ การจัดทำเอกสาร และการประเมินตนเอง นอกจากนี้ ชุดของวิธีการควบคุมที่กำหนดไว้ควรแข็งแกร่งพอที่จะจัดการกับความเสี่ยงที่ได้ระบุไว้ได้

3. ผู้มีส่วนได้เสียภายในองค์กรและภาระหน้าที่ด้าน IT

องค์กรแต่ละแห่งต้องทำความเข้าใจและบริหารสภาพแวดล้อมด้าน IT ของตนเอง ยิ่งไปกว่านั้น องค์กรจะต้องเข้าใจและตระหนักถึงความพึ่งพา IT ของกระบวนการทางธุรกิจ รวมทั้ง ความจำเป็นที่ต้องปฏิบัติให้สอดคล้องตามกฎหมายและระเบียบข้อบังคับต่างๆ

องค์กรอาจใช้โอกาสทางธุรกิจหรือสูญเสียโอกาส ก็เป็นผลมาจากความสำเร็จหรือความล้มเหลวในการบริหารจัดการและการนำ IT ไปใช้งาน การกำกับดูแลด้าน IT ที่มีประสิทธิผลจะเพิ่มโอกาสที่ IT จะช่วยให้ธุรกิจสามารถบรรลุเป้าหมาย และเพิ่มโอกาสที่ทรัพยากรจะได้รับการบริหารจัดการอย่างระมัดระวังรอบคอบ

ตาราง[1]ต่อไปนี้แสดงถึงหน้าที่ในการกำกับดูแลที่เกี่ยวข้องกับคณะกรรมการ ฝ่ายบริหาร ผู้บริหารระดับสูง และผู้ตรวจสอบภายใน จากมุมมองของการกำกับดูแลด้าน IT

บทบาท	ภาระหน้าที่
คณะกรรมการ	**คณะกรรมการควรจะ:** • ทำความเข้าใจคุณค่าในเชิงกลยุทธ์ของหน้าที่งานด้าน IT • รับทราบถึงบทบาทและผลกระทบของ IT ที่มีต่อองค์กร • กำหนดทิศทางในเชิงกลยุทธ์และผลลัพธ์ที่คาดหวัง • พิจารณาวิธีการที่ผู้บริหารมอบหมายภาระหน้าที่ • ดูแลวิธีการแปลงสภาพ (transformation) ที่เกิดขึ้น • ทำความเข้าใจในข้อจำกัดในการดำเนินงานของผู้บริหาร • ดูแลความสอดคล้องเป็นไปในทิศทางเดียวกันกับองค์กร • ควบคุมสั่งการให้ผู้บริหารส่งมอบคุณค่าที่วัดได้ผ่านทาง IT • ดูแลความเสี่ยงขององค์กรโดยรวม • สนับสนุนให้มีการเรียนรู้ การเติบโตก้าวหน้า และการบริหารทรัพยากร • ดูแลวิธีการวัดผลการดำเนินงาน • เป็นผู้ได้รับความเชื่อมั่น

[1] *ตารางนี้แสดงถึงบางส่วนที่ได้มาจากบทบรรยายสรุป (ตีพิมพ์ครั้งที่ 2) เรื่อง การกำกับดูแลด้านไอทีจากการประชุมคณะกรรมการของสถาบันไอทีภิบาล (ITGI) นำมาใช้โดยได้รับอนุญาตจาก ITGI และ ISACA แล้ว สงวนลิขสิทธิ์*

บทบาท	ภาระหน้าที่
ผู้บริหารระดับสูง	**ผู้บริหารระดับสูงควรจะ:** ● รับทราบถึงบทบาทและผลกระทบของ IT ที่มีต่อกิจการ ● ไล่เรียงกลยุทธ์ นโยบาย และเป้าหมายลงไปในแต่ละระดับของกิจการ และจัดทิศทางด้าน IT ให้เป็นไปในแนวทางเดียวกันกับเป้าหมายของกิจการ ● ตัดสินถึงความสามารถและเงินลงทุนที่ต้องการ ● มอบหมายความรับผิดชอบ ● ค้ำจุนการปฏิบัติงานในปัจจุบัน ● กำหนดโครงสร้างองค์กรและทรัพยากรที่จำเป็น ● กำหนดความรับผิดชอบที่ชัดเจนในกระบวนการบริหารความเสี่ยงและการควบคุมที่เกี่ยวกับ IT ● วัดผลการดำเนินงาน ● มุ่งเน้นไปที่สมรรถนะหลักของธุรกิจที่ IT จะต้องสนับสนุน ● มุ่งเน้นไปที่กระบวนการ IT ที่สำคัญที่ช่วยเพิ่มคุณค่าให้กับธุรกิจ ● สร้างองค์กรที่ยืดหยุ่นและปรับตัวได้ง่าย โดยนำข้อมูลและองค์ความรู้มาใช้ให้เกิดประโยชน์ ● เสริมสร้างการส่งมอบคุณค่าให้เข้มแข็งมากขึ้น ● พัฒนากลยุทธ์เพื่อให้ต้นทุนด้าน IT เป็นไปอย่างคุ้มค่าเหมาะสม ● มีกลยุทธ์การจัดจ้างหน่วยงานภายนอกที่ชัดเจน
บริหารระดับอาวุโส	**ผู้บริหารระดับอาวุโสควรจะ:** ● บริหารธุรกิจและความคาดหวังของผู้บริหารระดับสูงที่เกี่ยวข้องด้าน IT ● ผลักดันให้เกิดการพัฒนาแผนกลยุทธ์ด้าน IT และนำไปลงมือปฏิบัติ ● เชื่อมโยงงบประมาณด้าน IT ให้สอดคล้องกับวัตถุประสงค์และเป้าหมาย ● ให้ความเชื่อมั่นว่าคุณค่าที่ส่งมอบนั้น เป็นไปตามกำหนดเวลาและอยู่ในงบประมาณ ● นำมาตรฐาน นโยบายและกรอบการควบคุมด้าน IT มาปรับใช้ ● แจ้งและให้ความรู้แก่ผู้บริหารระดับสูงในประเด็นด้าน IT ● พยายามหาหนทางเพิ่มคุณค่างาน IT ● ให้ความเชื่อมั่นว่าโครงการที่เกี่ยวกับ IT มีการบริหารจัดการที่ดี ● จัดทำโครงสร้างพื้นฐาน IT ที่เอื้อให้เกิดสิ่งที่มีต้นทุนที่คุ้มค่า และแบ่งปันข้อมูลในระบบที่ช่วยสนับสนุนการตัดสินใจทางธุรกิจ (Business Intelligence-BI) ● ให้ความเชื่อมั่นเกี่ยวกับ ความพร้อมของทรัพยากรทาง IT ทักษะและโครงสร้างพื้นฐาน ในการบรรลุวัตถุประสงค์และสร้างคุณค่าแก่องค์กร

บทบาท	ภาระหน้าที่
	• ประเมินความเสี่ยง บรรเทาความเสี่ยงอย่างมีประสิทธิภาพ และให้ผู้มีส่วนได้เสียรับทราบความเสี่ยงได้อย่างโปร่งใส • ให้ความเชื่อมั่นว่า ได้มีการกำหนดผู้มีบทบาทสำคัญในการจัดการความเสี่ยงด้าน IT และมีกำลังคนเพื่อบทบาทนั้นๆ อย่างเหมาะสม • ให้ความเชื่อมั่นในการบริหารงานประจำวัน (day-to-day) และการสอบทานกระบวนการและวิธีการควบคุมด้าน IT • มีมาตรการวัดผลการดำเนินงานที่แสดงให้เห็นได้ว่าเชื่อมโยงตรงไปยังกลยุทธ์ • มุ่งเน้นไปที่สมรรถนะหลักด้าน IT
หน่วยงานตรวจสอบภายใน	**หน่วยงานตรวจสอบภายในควรจะ:** • ให้ความเชื่อมั่นว่า มีความเชี่ยวชาญในการตรวจสอบงานด้าน IT ระดับพื้นฐานของหน่วยงานที่เพียงพอ • รวมการประเมินงานด้าน IT เข้าไปในกระบวนการวางแผน • ประเมินว่าการกำกับดูแลด้าน IT ขององค์กรสนับสนุนและสอดคล้องกับกลยุทธ์และวัตถุประสงค์หรือไม่ • ระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร • ประเมินวิธีการควบคุมที่ตอบสนองต่อความเสี่ยงที่มีอยู่ในระบบสารสนเทศขององค์กร • ให้ความเชื่อมั่นว่าหน่วยงานตรวจสอบภายในมีผู้เชี่ยวชาญด้าน IT ที่สามารถปฏิบัติงานตรวจสอบให้สำเร็จได้ • พิจารณานำเทคนิคการตรวจสอบที่อาศัยเทคโนโลยีมาใช้ในงานตรวจสอบตามสมควร

นอกเหนือจากผู้มีส่วนได้เสียภายในองค์กรแล้ว สิ่งสำคัญคือต้องคำนึงถึงบุคคลภายนอกที่เกี่ยวข้องด้วย เป็นต้นว่า ผู้สอบบัญชี หน่วยงานภาครัฐ ความคาดหวังของสาธารณชน และองค์กรระหว่างประเทศเพื่อกำหนดมาตรฐานสากล

4. การวิเคราะห์ความเสี่ยง

วิธีการควบคุมด้าน IT ได้ถูกคัดเลือกและนำไปใช้ปฏิบัติโดยอิงความเสี่ยงที่วิธีการควบคุมเหล่านั้นได้รับการออกแบบมาเพื่อจัดการกับความเสี่ยงเหล่านั้น เมื่อความเสี่ยงได้รับการระบุแล้ว ก็จะมีการกำหนดมาตรการตอบสนองต่อความเสี่ยงที่เหมาะสม ซึ่งมาตรการเหล่านั้นเป็นไปได้ตั้งแต่ไม่ดำเนินการอย่างใดเลย ไปจนถึงยอมรับความเสี่ยงว่าเป็นต้นทุนของการดำเนินธุรกิจ และไปจนถึงการประยุกต์ใช้วิธีการควบคุมเฉพาะอย่างในวงกว้าง ในส่วนนี้จะอธิบายถึงแนวคิดที่ว่าเมื่อไหร่ที่ควรจะประยุกต์ใช้วิธีการควบคุมด้าน IT

มันจะเป็นงานที่ค่อนข้างตรงไปตรงมาในการสร้างบัญชีรายการวิธีการควบคุมด้าน IT ซึ่งได้รับการแนะนำให้ต้องนำไปใช้ปฏิบัติภายในแต่ละองค์กร อย่างไรก็ตาม วิธีการควบคุมแต่ละวิธีต่างก็มีค่าใช้จ่ายเฉพาะที่อาจจะไม่สมเหตุสมผลในแง่ของความคุ้มค่าของต้นทุนเมื่อพิจารณาถึงประเภทขององค์กรและภาคอุตสาหกรรม นอกจากนี้ ยังไม่มีรายการวิธีการควบคุมใดที่สามารถนำไปใช้ได้กับองค์กรทุกประเภท แม้ว่าจะมีคำแนะนำที่ดีมากมายในการเลือกวิธีการควบคุมที่เหมาะสม แต่ก็ยังต้องใช้การตัดสินใจที่รัดกุม วิธีการควบคุมจะต้องเหมาะสมกับระดับความเสี่ยงที่องค์กรจะเผชิญ ซึ่ง CAE ควรที่จะสามารถแนะนำคณะกรรมการตรวจสอบถึงกรอบการควบคุมภายในที่น่าเชื่อถือและให้ความเชื่อมั่นในระดับที่เหมาะสมกับระดับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) ในเรื่องนี้ Committee of Sponsoring Organizations of the Treadway Commission (COSO)[2] ได้กำหนดคำนิยามของความเสี่ยงที่ยอมรับได้ (risk appetite) ไว้ดังนี้:

"...ระดับของความเสี่ยงอย่างกว้างๆ ซึ่งบริษัทหรือองค์กรใดๆ เต็มใจที่จะยอมรับได้ในการมุ่งสู่เป้าหมายขององค์กร ฝ่ายบริหารจะคำนึงถึงระดับความเสี่ยงที่ยอมรับได้ขององค์กรเป็นอันดับแรกในการประเมินทางเลือกเชิงกลยุทธ์ต่างๆ จากนั้น จึงจะคำนึงถึงระดับความเสี่ยงที่ยอมรับได้ในการกำหนดวัตถุประสงค์ให้สอดคล้องกับกลยุทธ์ที่เลือกมา และคำนึงถึงระดับความเสี่ยงที่ยอมรับได้ในการพัฒนากลไกในการจัดการความเสี่ยงที่เกี่ยวข้องทั้งหลาย"

[2] The Committee of Sponsoring Organizations of the Treadway Commission คือ "คณะกรรมาธิการที่จัดตั้งขึ้นเพื่อดำเนินการเกี่ยวกับการทุจริตรายงานทางการเงิน" รายละเอียดดูได้ที่ www.coso.org

นอกจากระดับความเสี่ยงที่ยอมรับได้แล้ว CAE ควรคำนึงถึงค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ (risk tolerance) ซึ่ง COSO ได้ให้คำนิยามของค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ ไว้ดังนี้

"...ค่าเบี่ยงเบนไปจากระดับที่ยอมรับได้ซึ่งสัมพันธ์กับการบรรลุวัตถุประสงค์ขององค์กร ในการกำหนดค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้นั้น ฝ่ายบริหารจะคำนึงถึงความสำคัญที่เกี่ยวข้องกันกับวัตถุประสงค์ขององค์กรที่เกี่ยวข้อง และทำให้ค่าเบี่ยงเบนฯ สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้"

ดังนั้น CAE ควรพิจารณาว่า:

- สภาพแวดล้อมด้าน IT ขององค์กรนั้นสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) ขององค์กรหรือไม่
- กรอบการควบคุมภายในเพียงพอที่จะทำให้มั่นใจได้ว่าผลการดำเนินงานขององค์กรยังคงอยู่ในช่วงของค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ (Risk tolerance) หรือไม่

4.1 ข้อควรคำนึงเกี่ยวกับความเสี่ยงในการตัดสินถึงความเพียงพอของวิธีการควบคุมด้าน IT

การบริหารความเสี่ยงสามารถนำไปประยุกต์ใช้ได้กับกิจกรรมทั้งหมดในองค์กร (ไม่ใช่แค่กับการใช้ IT) เราไม่สามารถแยกพิจารณาด้าน IT ออกไปต่างหาก แต่จะต้องพิจารณาว่า IT เป็นส่วนสำคัญที่ผนวกเข้าไปในกระบวนการทางธุรกิจทั้งหมดในองค์กร การเลือกวิธีการควบคุมด้าน IT ไม่ได้เป็นเรื่องของการดำเนินการนำเอาวิธีการควบคุมตามที่ได้แนะนำกันไว้ว่าเป็นวิธีปฏิบัติที่เป็นเลิศ (Best practices) มาใช้แค่นั้น แต่วิธีการควบคุมจะต้องเพิ่มคุณค่าให้กับองค์กรโดยการลดความเสี่ยงอย่างมีประสิทธิภาพและช่วยเพิ่มประสิทธิผลได้ เมื่อพิจารณาถึงความเพียงพอของวิธีการควบคุมด้าน IT ที่มีอยู่ในกรอบการควบคุมภายในขององค์กร CAE ควรคำนึงถึงกระบวนการที่กำหนดโดยฝ่ายบริหารเพื่อตัดสินถึง:

- การใช้ประโยชน์ คุณค่า และความสำคัญของข้อมูล
- ระดับความเสี่ยงที่ยอมรับได้และค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ขององค์กร ในแต่ละหน้าที่งานและกระบวนการทางธุรกิจ
- ความเสี่ยงด้าน IT ที่องค์กรเผชิญ และคุณภาพของบริการที่ให้แก่ผู้ใช้งาน
- ความซับซ้อนของโครงสร้างพื้นฐานด้าน IT
- วิธีการควบคุมด้าน IT ที่เหมาะสม และประโยชน์ที่วิธีการควบคุมเหล่านั้นมีให้

ความถี่ของการวิเคราะห์ความเสี่ยงเป็นสิ่งสำคัญและจะได้รับอิทธิพลเป็นอย่างมากจากการเปลี่ยนแปลงทั้งภายในและภายนอกที่เกิดขึ้น การเปลี่ยนแปลงทางเทคโนโลยีที่เป็นไปอย่างรวดเร็วจะส่งผลกระทบแต่ละองค์กรแตกต่างกัน บางองค์กรจะต้องตอบสนองต่อความเสี่ยงที่มีมาพร้อมกับการเปลี่ยนแปลงเทคโนโลยีที่เป็นไปอย่างรวดเร็ว ในขณะที่องค์กรอื่นๆ อาจตัดสินใจที่จะตอบสนองอย่างค่อยเป็นค่อยไป

4.1.1 สภาพแวดล้อมด้าน IT

การวิเคราะห์และประเมินความเสี่ยงที่เกี่ยวข้องกับ IT เป็นเรื่องซับซ้อน โครงสร้างพื้นฐานด้าน IT นั้นประกอบไปด้วย ฮาร์ดแวร์ ซอฟต์แวร์ การติดต่อสื่อสาร ระบบงาน โปรโตคอล (ซึ่งก็คือ กฎเกณฑ์) และข้อมูล รวมถึงการนำมาใช้งานในหลายๆ พื้นที่ทางกายภาพ ไม่ว่าจะอยู่ภายใต้โครงสร้างองค์กรเดียวกันหรือระหว่างองค์กรกับสิ่งแวดล้อมภายนอก โครงสร้างพื้นฐานหมายรวมถึง บุคลากรที่มีปฏิสัมพันธ์กับองค์ประกอบทางกายภาพและทางตรรกะของระบบต่างๆ

ประเด็นอื่นๆ ที่ต้องพิจารณารวมถึง ความเสี่ยงที่เกี่ยวข้องกับโครงการและผู้ให้บริการ ตัวอย่างเช่น ความเสี่ยงของโครงการได้แก่ ความไม่เพียงพอของงบประมาณ ทรัพยากร การบริหารงานโครงการ และความซำนาญทางเทคนิค สำหรับความเสี่ยงของผู้ให้บริการซึ่งเป็นบุคคลที่สามและความเสี่ยงของคู่ค้า ผู้ตรวจสอบงานด้าน IT ควรวิเคราะห์ประเด็นปัญหาต่างๆ เช่น ความมั่นคงของกิจการ ความเข้มแข็งทางการเงิน การสอบทานวิธีการควบคุมด้าน IT และสิทธิในการเข้าตรวจสอบ เป็นต้น

การจัดทำรายการองค์ประกอบของโครงสร้างพื้นฐานด้าน IT จะเผยให้เห็นข้อมูลพื้นฐานเกี่ยวกับช่องโหว่ของสภาพแวดล้อมด้าน IT ได้ ตัวอย่างเช่น ระบบงานทางธุรกิจและเครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ตจะเสี่ยงต่อภัยคุกคามที่ไม่ได้มีอยู่ในระบบและเครือข่ายตนเอง เนื่องจากการเชื่อมต่ออินเทอร์เน็ตเป็นองค์ประกอบสำคัญของระบบงานธุรกิจและเครือข่ายเป็นส่วนใหญ่ องค์กรต้องแน่ใจได้ว่าระบบและสถาปัตยกรรมโครงสร้างเครือข่ายนั้นมีวิธีการควบคุมพื้นฐานที่ทำให้มั่นใจในความปลอดภัยขั้นพื้นฐานได้

รายการองค์ประกอบด้าน IT ขององค์กร อันประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ระบบเครือข่ายและข้อมูลที่สมบูรณ์ จะก่อให้เกิดพื้นฐานที่จำเป็นต่อการประเมินช่องโหว่ภายในโครงสร้างพื้นฐานด้าน IT ส่วนแผนผังสถาปัตยกรรมโครงสร้างระบบนั้นจะช่วยให้ทราบถึงการนำเอาองค์ประกอบต่างๆ ไปใช้งานและมีการเชื่อมต่อกับองค์ประกอบอื่นๆ ที่อยู่ทั้งภายในและภายนอกองค์กรอย่างไร สำหรับผู้เชี่ยวชาญด้านความปลอดภัยของสารสนเทศนั้น รายการและสถาปัตยกรรมขององค์ประกอบโครงสร้างพื้นฐานด้าน IT จะรวมถึงการใส่วิธีการควบคุมความปลอดภัยและเทคโนโลยีที่สามารถเผยให้เห็นถึงช่องโหว่สำคัญได้ โชคไม่ดีที่ข้อมูลเกี่ยวกับระบบหรือเครือข่ายก็สามารถเผยช่องโหว่ให้แก่ผู้ที่จ้องจะโจมตีได้ด้วย ดังนั้น การเข้าถึงข้อมูลดังกล่าวจะต้องถูกจำกัดให้เฉพาะกับผู้ที่จำเป็นต้องใช้งานเท่านั้น การตั้งค่าระบบและกำหนด

สภาพแวดล้อมเครือข่ายอย่างเหมาะสมจะช่วยลดจำนวนของข้อมูลที่ผู้ที่จ้องจะโจมตีจะดูได้ และสภาพแวดล้อมที่ปลอดภัยจะเป็นเป้าหมายที่น่าดึงดูดน้อยลงสำหรับผู้ที่จ้องจะโจมตี

4.1.2 ความเสี่ยงด้าน IT ที่องค์กรเผชิญอยู่

CAE จะหารือประเด็นความเสี่ยงด้าน IT กับหัวหน้าหน่วยงานสารสนเทศ (CIO) และเจ้าของกระบวนการ (Process owner) เพื่อประเมินว่า ผู้เกี่ยวข้องทุกคนมีความตระหนักและความเข้าใจที่เหมาะสมหรือไม่เกี่ยวกับความเสี่ยงด้านเทคนิคที่องค์กรเผชิญอยู่โดยผ่านการใช้งาน IT ไป รวมทั้งบทบาทของตนในการนำเอาวิธีการควบคุมไปปฏิบัติและคงไว้ซึ่งวิธีการควบคุมที่มีประสิทธิผล

4.1.3 ระดับความเสี่ยงที่ยอมรับได้และค่าเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้

ด้วยความรู้ที่มีเกี่ยวกับความเสี่ยงด้าน IT ผู้ตรวจสอบต้องสามารถสอบยันประสิทธิผลของวิธีการควบคุมด้าน IT ที่มีอยู่ว่า สามารถตอบสนองต่อระดับความเสี่ยงเกี่ยวกับด้าน IT และค่าเบี่ยงเบนที่ยอมรับได้ซึ่งองค์กรได้กำหนดไว้แล้ว การประเมินของผู้ตรวจสอบจะเกี่ยวข้องกับการหารือกับผู้บริหาร - หรืออาจหารือกับคณะกรรมการก็ได้ ระดับรายละเอียดของการหารือเหล่านี้สามารถกำหนดได้จากข้อมูล/ความเห็นที่ได้จาก CIO หัวหน้าหน่วยงานความมั่นคงปลอดภัยด้านสารสนเทศ (Chief Information Security Officer - CISO) และเจ้าของกระบวนการ (Process owners)

องค์กรที่ใช้กระบวนการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management - ERM) จะต้องรวมเอาความเสี่ยงด้าน IT เข้าเป็นส่วนหนึ่งของกระบวนการนี้ ERM ได้แก่วิธีการและกระบวนการในการบริหารจัดการความเสี่ยง และเพิ่มโอกาสในการบรรลุวัตถุประสงค์ขององค์กร โดยทั่วไปแล้ว จะเริ่มต้นด้วยการระบุเหตุการณ์บางอย่าง หรือสถานการณ์ที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กร (เช่น ความเสี่ยงจากการละเมิดข้อมูล หรือข้อมูลรั่วไหล) โดยทำการประเมินทั้งโอกาสเกิดและระดับความรุนแรงของผลกระทบ (เช่น ความเสี่ยงตามธรรมชาติจากข้อมูลรั่วไหลมีโอกาสเกิดในระดับสูง และผลกระทบก็อยู่ในระดับสูงด้วย) การกำหนดมาตรการตอบสนองต่อความเสี่ยง (เช่น การกำหนดนโยบายใหม่ขึ้นมาเพื่อปกป้องความปลอดภัยของข้อมูลขององค์กร) และเฝ้าติดตามความคืบหน้าในการดำเนินการตามมาตรการที่กำหนดขึ้น (เช่น นำกิจกรรมด้าน IT ที่เป็นมาตรการรักษาความปลอดภัยวิธีใหม่มาใช้เพื่อหลีกเลี่ยงการละเมิดข้อมูล) ด้วยการระบุและจัดการกับความเสี่ยงและโอกาสในเชิงรุกนี้ องค์กรจะเพิ่มความสามารถในการปกป้องและสร้างคุณค่าให้กับผู้มีส่วนได้เสียได้ การใช้แนวทางนี้ ERM จะช่วยให้CAE เข้าใจได้ถึงความเสี่ยงที่สำคัญขององค์กรทั้งหมด และใช้มุมมองนี้เพื่อกำหนดลำดับความสำคัญของงานตรวจสอบ กำหนดกิจกรรมในงานตรวจสอบแต่ละงาน และกำหนดระดับความเสี่ยงและค่าเบี่ยงเบนที่ยอมรับได้[3]

[3] จากเอกสารเรื่อง COSO, Strengthening Enterprise Risk Management for Strategic Advantage 4 พฤศจิกายน 2552

4.1.4 ทำการวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยงควรดำเนินการโดยมีหน่วยงานหรือแผนกต่างๆ ภายในองค์กรเข้ามามีส่วนร่วม ซึ่งรวมถึงหัวหน้าหน่วยงานด้านความเสี่ยง (Chief Risk Officer - CRO) CAE หน่วยงานด้าน IT และตัวแทนจากหน่วยธุรกิจ

คำถามพื้นฐานที่เกี่ยวข้องกับกระบวนการประเมินความเสี่ยง ได้แก่:

- สินทรัพย์ด้าน IT (ซึ่งรวมถึงสินทรัพย์ที่มีตัวตนจับต้องได้และไม่มีตัวตนเช่น ข้อมูลหรือชื่อเสียง) ใดบ้างที่มีความเสี่ยง? และคุณค่าของ การรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของสินทรัพย์เหล่านั้นคืออะไร?
- อะไรที่เกิดขึ้นแล้วจะส่งผลกระทบในทางร้ายให้แก่คุณค่าของข้อมูลได้ (เหตุการณ์ภัยคุกคาม)? นัยแห่งคำถามนี้ก็คือ เรื่องของการวิเคราะห์ช่องโหว่ (Vulnerability) และจับคู่ช่องโหว่กับภัยคุกคาม (Threat) ที่อาจส่งผลผลกระทบต่อสินทรัพย์ด้านข้อมูลได้
- หากมีภัยคุกคามกรณีหนึ่งเกิดขึ้น ผลกระทบจะร้ายแรงเพียงใด?
- คาดว่าเหตุการณ์ความเสี่ยงจะเกิดขึ้นบ่อยเพียงใด (ความถี่ของการเกิดขึ้น)?
- คำตอบของคำถามสี่ข้อแรก มีความแน่นอนเพียงใด (การวิเคราะห์ความไม่แน่นอน)?
- สามารถทำอะไรได้บ้างเพื่อลดความเสี่ยง?
- ต้นทุน จะเป็นเท่าใด?
- จะคุ้มค่าหรือไม่?

การกำหนดคุณค่าของข้อมูลที่ประมวลผลและจัดเก็บไว้นั้นไม่ใช่เรื่องง่าย เนื่องจากคุณค่านั้นจะประกอบอยู่ในลักษณะที่มีหลากหลายมิติ CAE จะพบว่า การทำงานร่วมกับ CRO นั้นจะเป็นประโยชน์ในการประสานงานและจัดให้ความเสี่ยงที่เกี่ยวข้องกับ IT เป็นไปในแนวทางเดียวกัน โดย CAE และ CRO อาจต้องการแบ่งปันข้อมูลระหว่างกันเกี่ยวกับวิธีการจัดลำดับความเสี่ยงที่สำคัญ ความครอบคลุมของความเสี่ยง หรือการจัดสรรทรัพยากรที่เหมาะสม ทั้งนี้ ขึ้นอยู่กับขนาดและความเสี่ยงขององค์กร

4.2 กลยุทธ์การบรรเทาความเสี่ยง

เมื่อความเสี่ยงได้รับการระบุและวิเคราะห์แล้ว ไม่จำเป็นที่จะต้องนำเอาวิธีการควบคุมมาใช้เพื่อจัดการกับความเสี่ยงในทุกครั้งเสมอไป ความเสี่ยงบางอย่างอาจมีผลกระทบเพียงเล็กน้อยหากเกิดขึ้นจริง หรือแทบจะไม่มีโอกาสเกิดขึ้นได้เลย และอาจไม่คุ้มค่าหากจะนำเอากระบวนการควบคุมที่มีต้นทุนสูงมาใช้จัดการ

โดยทั่วไปแล้ว วิธีการจัดการความเสี่ยงมีอยู่หลายวิธี

- **ยอมรับความเสี่ยง** (Accept the risk) หนึ่งในหน้าที่หลักของงานทางการบริหารก็คือ การจัดการกับความเสี่ยง ความเสี่ยงบางตัวอาจเล็กน้อยเนื่องจากผลกระทบและโอกาสเกิดนั้นต่ำ ในกรณีนี้ อาจยอมรับความเสี่ยงได้อย่างมีสติ ขณะที่ต้นทุนในการดำเนินธุรกิจนั้นยังมีความเหมาะสม พร้อมๆ กับการสอบทานความเสี่ยงเป็นระยะๆ เพื่อให้มั่นใจได้ว่าผลกระทบจะยังคงอยู่ในระดับต่ำ

- **กำจัดความเสี่ยง** (Eliminate the risk) เป็นไปได้ที่ความเสี่ยงจะเกี่ยวเนื่องมากับการใช้เทคโนโลยีบางอย่าง ผู้จัดหา (supplier) หรือผู้ขาย (vendor) บางราย ความเสี่ยงสามารถถูกกำจัดได้ด้วยการนำเทคโนโลยีที่มีความสามารถมากขึ้นมาแทนที่ และโดยเพิ่มจำนวนผู้จัดหาและผู้ขายที่มีความสามารถให้มากรายขึ้น

- **หาผู้ร่วมรับความเสี่ยง** (Share the risk) แนวทางการบรรเทาความเสี่ยงสามารถแบ่งปันความเสี่ยงกับคู่ค้าและผู้จัดหาได้ ตัวอย่างที่ดีคือ การจัดจ้างหน่วยงานภายนอกเพื่อบริหารจัดการโครงสร้างพื้นฐาน ในกรณีเช่นนี้ ผู้จัดหาจะลดความเสี่ยงที่เกี่ยวกับการจัดการโครงสร้างพื้นฐานด้าน IT ให้กับองค์กรได้ เนื่องจากมีความสามารถในการดำเนินการที่สูงกว่าและสามารถเข้าถึงพนักงานที่มีความชำนาญทักษะสูงกว่าองค์กรที่ว่าจ้างได้ นอกจากนี้ความเสี่ยงยังอาจบรรเทาลงได้โดยการโอนความเสี่ยงไปยังบริษัทประกันภัย

- **ควบคุม/บรรเทาความเสี่ยง** (Control/Mitigate the risk) แทนที่จะใช้ (หรือใช้ร่วมกับ) ตัวเลือกอื่นๆ วิธีการควบคุมอาจได้รับการออกแบบและนำไปใช้เพื่อป้องกันความเสี่ยงที่จะเกิดขึ้นเองตามธรรมชาติ ไปจนถึงเพื่อลดโอกาสที่จะเกิดความเสี่ยงขึ้น หรือเพื่อลดผลกระทบที่ตามมาได้

5. การประเมินด้าน IT - ภาพรวม

วิธีการควบคุมด้าน IT จะถูกนำมาใช้ก็ต่อเมื่อการควบคุมหรือการบรรเทาความเสี่ยงเป็นทางเลือกที่ดีที่สุด ถึงแม้ว่าวิธีการควบคุมด้าน IT ถูกนำไปใช้โดยคำนึงถึงความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสมแล้ว แต่ก็ยังมีชุดของวิธีการควบคุมพื้นฐานที่ควรนำมาใช้เพื่อก่อให้เกิดการควบคุมด้าน IT ในระดับพื้นฐาน

วิธีการควบคุมด้าน IT ควรเป็นส่วนหนึ่งของกระบวนการด้าน IT หลักๆ ซึ่งเกี่ยวกับ การวางแผน การจัดองค์กร การจัดซื้อจัดหา การเปลี่ยนแปลง การส่งมอบบริการด้าน IT รวมทั้งความสนับสนุนจาก IT และการเฝ้าติดตามโดย IT โดยทั่วไปแล้ว วิธีการควบคุมด้าน IT หลายๆ วิธี ซึ่งรองรับกระบวนการทาง IT ที่หลากหลายเหล่านี้ มักจะเป็นวิธีการควบคุมโครงสร้างพื้นฐานด้าน IT ที่ครอบคลุมเรื่องต่างๆ เช่น วิธีการควบคุมเครือข่าย การควบคุมฐานข้อมูล การควบคุมระบบปฏิบัติการ และการควบคุมอุปกรณ์ฮาร์ดแวร์ เป็นต้น วิธีการควบคุมด้าน IT ที่ครอบคลุมระบบงานต่างๆ และในหลายๆ กรณีก็ครอบคลุมกิจกรรมทางธุรกิจที่สำคัญ ได้แก่ วิธีการควบคุมการแก้ไขข้อมูลนำเข้า วิธีการควบคุมความสมบูรณ์ของการประมวลผล หรือวิธีการควบคุมการกระทบยอด และวิธีการควบคุมโดยการรายงานความผิดปกติ CAE ควรได้รับข้อมูลในภาพรวมของวิธีการควบคุมที่สำคัญและกระบวนการทางธุรกิจกระบวนการใดที่มีวิธีการควบคุมเหล่านั้นรองรับ โดยถือเป็นขั้นตอนแรกในการทำความเข้าใจความเสี่ยงและวิธีการควบคุมด้าน IT คำอธิบายกระบวนการและผังโครงสร้างองค์กรเป็นเครื่องมืออย่างหนึ่งที่สามารถใช้เพื่อให้มองเห็นภาพรวมได้ นอกจากนี้ CAE ควรทำความเข้าใจกับความริเริ่มหรือโครงการใหม่ๆ ของ IT ที่สำคัญ เพื่อให้เข้าใจได้ว่าโครงสร้างพื้นฐานด้าน IT และระบบงานอาจจะมีการเปลี่ยนแปลงไปได้อย่างไรบ้างในระหว่างช่วงระยะเวลาของโครงการ ข้อมูลนี้จะช่วยให้ CAE สามารถทำการประเมินความเสี่ยงตั้งแต่เริ่มต้นซึ่งจะช่วยให้ทำการวิเคราะห์เชิงลึกมากขึ้นได้ต่อไป

คำถามบางข้อที่สามารถนำมาใช้ได้ในการประเมินสภาพแวดล้อมการควบคุม และการเลือกชุดวิธีการควบคุมที่เหมาะสม

- มีนโยบายด้าน IT ซึ่งรวมถึงวิธีการควบคุมด้าน IT อยู่หรือไม่?
- ภาระหน้าที่ในการปฏิบัติงานและการควบคุมด้าน IT ต่างๆ ได้มีการกำหนด มอบหมายและยอมรับแล้วหรือไม่?
- วิธีการควบคุมนั้นได้ถูกออกแบบมาอย่างมีประสิทธิผลหรือไม่?
- วิธีการควบคุมนั้นทำงานได้อย่างมีประสิทธิผลหรือไม่?
- วิธีการควบคุมนั้นบรรลุผลตามที่ต้องการหรือไม่?
- การผสมกันระหว่างวิธีการควบคุมแบบป้องกัน (Prevention) แบบตรวจพบ (Detective) และแบบแก้ไข (Corrective) มีประสิทธิผลหรือไม่?

- วิธีการควบคุมต่างๆ ได้ก่อให้เกิดหลักฐานที่แสดงถึงกรณีที่เกินค่าตัวแปรการควบคุม (control parameters) หรือเมื่อวิธีการควบคุมเหล่านั้นล้มเหลวหรือไม่? มีวิธีการแจ้งเตือนฝ่ายบริหารเมื่อการควบคุมล้มเหลวอย่างไรและ ขั้นตอนในการดำเนินต่อควรเป็นอย่างไร?
- มีการจัดเก็บหลักฐานไว้หรือไม่? (เช่น โดยผ่านทางร่องรอยหลักฐานเพื่อการตรวจสอบ)
- มีการจัดเก็บอุปกรณ์และเครื่องมือในโครงสร้างพื้นฐานด้าน IT ไว้อย่างปลอดภัยปลอดภัย ทั้งทางกายภาพ (physical) และเชิงตรรกะ (logical) หรือไม่?
- มีการใช้กลไกการควบคุมการเข้าถึงและการยืนยันตัวตนในการเข้าถึงระบบงานหรือไม่?
- มีวิธีการควบคุมเพื่อปกป้องสภาพแวดล้อมการทำงานและปกป้องข้อมูลจากไวรัสและโปรแกรมที่ประสงค์ร้ายอื่นๆ หรือไม่?
- มีการใช้วิธีการควบคุมที่เกี่ยวกับไฟร์วอลล์ (Firewall) หรือไม่?
- มีนโยบายเกี่ยวกับไฟร์วอลล์ (Firewall) หรือไม่?
- มีการประเมินช่องโหว่ (Vulnerability assessment) ทั้งภายนอกและภายใน และมีการระบุความเสี่ยงและได้รับการแก้ไขอย่างเหมาะสมหรือไม่?
- มีการบริหารจัดการความเปลี่ยนแปลงและการกำหนดค่าตั้งต้นระบบ (Configuration) รวมทั้งกระบวนการประกันคุณภาพหรือไม่?
- มีกระบวนการของการเฝ้าติดตามประเมินผลและกระบวนการวัดผลการให้บริการอย่างเป็นระบบหรือไม่?
- ได้มีการคำนึงถึงความเสี่ยงของการใช้บริการจากภายนอกหรือไม่? (สำหรับรายละเอียดเกี่ยวกับเรื่องนี้ โปรดดู *GTAG 7: การจัดจ้างหน่วยงานด้าน IT จากภายนอก*)

ในอุตสาหกรรมบัตรชำระเงิน (Payment card) ได้กำหนดให้มีมาตรฐานที่เกี่ยวกับความปลอดภัยของข้อมูลมาตรฐานหนึ่งซึ่งใช้กันอย่างแพร่หลายและกว้างขวาง เรียกว่า มาตรฐานความปลอดภัยของข้อมูลในอุตสาหกรรมบัตรชำระเงิน (PCI Data Security Standards - PCI DSS): ซึ่งเริ่มใช้ในปีพ.ศ.2549 โดยสภามาตรฐานความปลอดภัยของข้อมูลในอุตสาหกรรมบัตรชำระเงิน (PCI Security Standards Council) ซึ่งเป็นหน่วยงานที่เป็นที่เปิดกว้างระดับโลก มีหน้าที่ในการพัฒนา การบริหารจัดการ การให้ความรู้ และการสร้างความตระหนักรู้ถึงมาตรฐานความปลอดภัย PCI ต่างๆ ได้แก่ PCI DSS มาตรฐานความปลอดภัยข้อมูลบนแอพพลิเคชันการชำระเงิน (PA-DSS) และข้อกำหนดด้านความปลอดภัยของธุรกรรม PIN (PTS)

CAE สามารถใช้มาตรฐาน PCI DSS ในระดับสูงเพื่อตัดสินว่า มีกิจกรรมความปลอดภัยประเภทใดบ้างที่ควรจะนำมาพิจารณาสำหรับองค์กรหรือไม่ (ขอให้ดูภาพรวมมาตรฐานความปลอดภัยข้อมูล PCI ในระดับสูงที่จะตามมาต่อไป)

บทนำและภาพรวมของมาตรฐานความปลอดภัยข้อมูล PCI

มาตรฐานความปลอดภัยของข้อมูล (DSS) ในอุตสาหกรรมบัตรชำระเงิน (PCI) นั้นได้รับการพัฒนาขึ้นเพื่อส่งเสริมและปรับปรุงความปลอดภัยในข้อมูลผู้ถือบัตรและอำนวยความสะดวกเพื่อให้เกิดการยอมรับเอามาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูลที่สอดคล้องกันทั่วโลก PCI DSS ได้ระบุข้อกำหนดทางเทคนิคและการปฏิบัติงานขั้นพื้นฐานที่ออกแบบมาเพื่อปกป้องข้อมูลของผู้ถือบัตร มาตรฐาน PCI DSS ใช้ได้กับทุกองค์กรที่เกี่ยวข้องในการประมวลผลบัตรชำระเงิน ซึ่งได้แก่ ร้านค้า (merchant) ผู้ประมวลผลรายการ (Processor) ผู้ซื้อ (Acquirer) ผู้ออกบัตร (Issuer) และผู้ให้บริการ (Service provider) รวมไปถึงหน่วยงานอื่นๆ ทั้งหมดที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล หรือส่งข้อมูลผู้ถือบัตร มาตรฐาน PCI DSS ประกอบด้วยข้อกำหนดขั้นต่ำสำหรับการปกป้องข้อมูลผู้ถือบัตร และอาจเสริมด้วยวิธีการควบคุมและวิธีปฏิบัติเพิ่มเติมต่างๆ เพื่อลดความเสี่ยง ตารางด้านล่างนี้เป็นภาพรวมระดับสูงของข้อกำหนด PCI DSS จำนวน 12 ข้อ

มาตรฐานความปลอดภัยของข้อมูลระดับสูงของ PCI (PCI Data Security Standard) ภาพรวมระดับสูง	
การสร้างและดำรงไว้ซึ่งเครือข่าย (network) ที่ปลอดภัย	1. ติดตั้งและบำรุงรักษาการกำหนดค่าไฟร์วอลล์เพื่อปกป้องข้อมูลผู้ถือบัตร 2. อย่าใช้รหัสผ่านระบบและพารามิเตอร์ความปลอดภัยอื่นๆ ที่กำหนดมาจากผู้จำหน่าย
ปกป้องข้อมูลของผู้ถือบัตร	3. ปกป้องข้อมูลผู้ถือบัตรที่ได้เก็บไว้ 4. เข้ารหัสข้อมูลผู้ถือบัตรที่ส่งผ่านข้อมูลทางเครือข่ายที่เปิดสาธารณะ
ดูแลรักษาโปรแกรมในการบริหารจัดการช่องโหว่	5. ใช้และปรับปรุงซอฟต์แวร์หรือโปรแกรมป้องกันไวรัสเป็นประจำ 6. พัฒนาและดูแลรักษาระบบและแอพพลิเคชันที่ปลอดภัย
ใช้มาตรการการควบคุมการเข้าถึงที่เข้มข้น	7. จำกัดการเข้าถึงข้อมูลผู้ถือบัตรตามหลักการความจำเป็นต้องรู้ของธุรกิจ 8. กำหนด ID เฉพาะให้กับแต่ละบุคคลที่มีสิทธิเข้าถึงคอมพิวเตอร์ 9. จำกัดการเข้าถึงทางกายภาพ = ข้อมูลผู้ถือบัตร
เฝ้าระวังและทดสอบเครือข่ายเป็นประจำ	10. ตามรอยและเฝ้าติดตาม ทุกๆ การเข้าถึงทรัพยากรเครือข่ายและข้อมูลผู้ถือบัตร 11. ทดสอบระบบและกระบวนการรักษาความปลอดภัยเป็นประจำ
คงไว้ซึ่งนโยบายความปลอดภัยของสารสนเทศ	12. คงไว้ซึ่งนโยบายที่เน้นความปลอดภัยของข้อมูลสำหรับบุคลากรทุกคน

4

[4] PCI DSS Requirements and Security Assessment Procedures, V2.0, ลิขสิทธิ์ปี 2553 ของสภามาตรฐานความปลอดภัยของข้อมูลในอุตสาหกรรมบัตรชำระเงิน (PCI Security Standards Council LLC)

การประเมินการควบคุมด้าน IT เป็นกระบวนการที่ต่อเนื่อง วิธีการทางธุรกิจมักจะมีการเปลี่ยนแปลงอยู่ตลอดเวลาเนื่องจากเทคโนโลยีที่มีวิวัฒนาการมาอย่างต่อเนื่อง และภัยคุกคามก็เกิดขึ้นได้เมื่อมีการค้นพบช่องโหว่ใหม่ๆ วิธีการตรวจสอบจะดีขึ้นเมื่อผู้ตรวจสอบภายในยอมรับในแนวทางที่ถือว่า ประเด็นการควบคุมด้าน IT ใดซึ่งสนับสนุนวัตถุประสงค์ทางธุรกิจย่อมมีความสำคัญมาเป็นลำดับแรกเสมอ ฝ่ายบริหารจะกำหนดตัวชี้วัดและการรายงานเกี่ยวกับการควบคุมด้าน IT และผู้ตรวจสอบจะยืนยันถึงความถูกต้องและให้ความคิดเห็นต่อคุณค่าที่ได้รับ ผู้ตรวจสอบภายในควรประสานกับฝ่ายบริหารในทุกระดับเพื่อความเห็นพ้องร่วมกันในเรื่องความถูกต้องและประสิทธิผลของตัวชี้วัด และความเชื่อมั่นที่มีต่อการรายงาน

กระบวนการตรวจสอบภายในมีการกำหนดรูปแบบอย่างเป็นทางการในการระบุถึงวิธีการควบคุมด้าน IT ที่อยู่ภายใต้ระบบการควบคุมภายในทั้งหมด รูปที่ 1 – โครงสร้างของการตรวจสอบด้าน IT แบ่งการประเมินออกเป็นชุดขั้นตอนที่เป็นเหตุเป็นผลกัน ดังนี้

รูปที่ 1 – โครงสร้างของการตรวจสอบด้าน IT

การประเมินวิธีการควบคุมด้าน IT	ทำความเข้าใจวิธีการควบคุมด้าน IT	การกำกับดูแล – การบริหารจัดการ - สิ่งที่เกี่ยวกับทางเทคนิค
		โปรแกรมใช้งานทั่วไป
		การป้องกัน การตรวจพบ การแก้ไข
		ข้อมูลสารสนเทศ - ความปลอดภัย
	ความสำคัญของวิธีการควบคุมด้าน IT	ความน่าเชื่อถือ – ประสิทธิผล
		ข้อได้เปรียบทางการแข่งขัน
		ข้อบังคับและข้อกำหนดตามกฎหมาย
	บทบาทและหน้าที่	การกำกับดูแล
		การบริหารจัดการ
		การตรวจสอบ
	การอิงความเสี่ยง	การวิเคราะห์ความเสี่ยง
		การจัดการความเสี่ยง
		การควบคุมขั้นพื้นฐาน
	การเฝ้าระวังและเทคนิคต่าง ๆ	กรอบการควบคุม
		ความถี่
	การประเมิน	ระเบียบวิธีการ
		การติดต่อกับคณะกรรมการตรวจสอบ

บทบาทของผู้ตรวจสอบภายในในการควบคุมด้าน IT นั้นจะเริ่มต้นด้วยการทำความเข้าใจในแนวคิดเป็นอย่างดี และไปจนถึงการให้ผลลัพธ์ของการประเมินความเสี่ยงและการควบคุม CAE ควรดูแลให้มีการเรียนรู้อย่างต่อเนื่อง และทำการประเมินซ้ำเมื่อมีเทคโนโลยีใหม่ๆ เกิดขึ้น รวมทั้งเมื่อมีการเปลี่ยนแปลงเกี่ยวกับ ความพึงพาใน IT กลยุทธ์ ความเสี่ยง และข้อกำหนดต่างๆ

6. การทำความเข้าใจในความสำคัญของวิธีการควบคุมด้าน IT

แม้ว่า GTAG ฉบับนี้จะเกี่ยวข้องกับความเสี่ยงและการควบคุมด้าน IT โดยเฉพาะ แต่สภาพแวดล้อมการควบคุมภายใน IT (เช่น ทัศนคติที่สื่อมาจากหัวหน้าหน่วยงานสารสนเทศ (CIO) บรรยากาศทางจริยธรรม ปรัชญาการบริหารจัดการ และรูปแบบการดำเนินงาน) ล้วนมีความสำคัญยิ่งและควรได้รับการประเมิน ควรศึกษารายละเอียดในแนวปฏิบัติ (Practice Guide) ของสมาคมผู้ตรวจสอบภายใน (IIA) เรื่อง “การตรวจสอบสภาพแวดล้อมการควบคุม” ในการพิจารณาถึงสภาพแวดล้อมการควบคุมภายในด้าน IT

COSO ได้ให้คำจัดความของการควบคุมภายใน ไว้ว่า: “หมายถึง กระบวนการที่เป็นผลมาจากการออกแบบโดยคณะกรรมการ ผู้บริหาร และบุคลากรอื่นๆ ขององค์กร เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่า องค์กรจะสามารถบรรลุวัตถุประสงค์ดังต่อไปนี้ได้:

- ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน
- ความเชื่อถือได้ของรายงานทางการเงิน
- การปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ ที่ใช้บังคับองค์กรนั้นๆ”

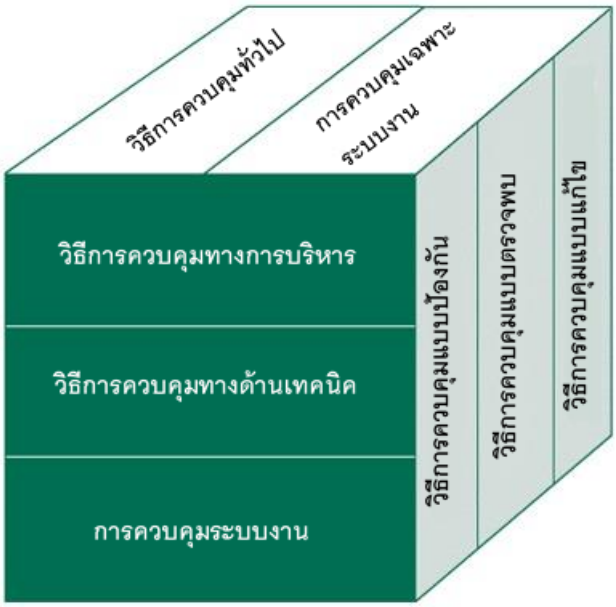
วิธีการควบคุมด้าน IT จะถูกห้อมล้อมไปด้วยกระบวนการเหล่านั้นซึ่งให้ความเชื่อมั่นในเรื่องข้อมูลและการให้บริการข้อมูล และช่วยควบคุมหรือบรรเทาความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีขององค์กร วิธีการควบคุมเหล่านี้เริ่มจากนโยบายขององค์กรที่เป็นลายลักษณ์อักษรไปจนถึงการปฏิบัติตามคู่มือที่กำหนดไว้ จากการป้องกันการเข้าถึงข้อมูล ทางกายภาพไปจนถึงความสามารถในการติดตามการกระทำและรายการธุรกรรมของบุคคลที่มีหน้าที่ในแต่ละรายการ และจากการแก้ไขโดยอัตโนมัติไปจนถึงการวิเคราะห์ความสมเหตุสมผลสำหรับข้อมูลขนาดใหญ่

CAE ไม่จำเป็นต้องรู้ทุกอย่างเกี่ยวกับวิธีการควบคุมด้าน IT รวมถึงความซับซ้อนทางเทคนิคทั้งหมด วิธีการควบคุมโดยส่วนใหญ่เหล่านี้เป็นเรื่องของผู้เชี่ยวชาญที่สามารถจัดการความเสี่ยงเฉพาะด้านที่เกี่ยวข้องกับแต่ละองค์ประกอบของระบบและโครงสร้างพื้นฐานของระบบเครือข่าย

6.1 วิธีการควบคุมทั่วไปด้าน IT และวิธีการควบคุมเฉพาะระบบงาน

วิธีการควบคุมอาจจัดแบ่งเป็นประเภทเพื่อช่วยให้เข้าใจถึงวัตถุประสงค์ของวิธีการเหล่านั้น และจุดที่เหมาะสมกับระบบโดยรวมของการควบคุมภายใน (ดูรูปที่ 2 - การจัดประเภทของการควบคุมบางอย่าง) โดยการทำความเข้าใจการจำแนกประเภทเหล่านี้ นักวิเคราะห์การควบคุมและผู้ตรวจสอบจะสามารถกำหนดตำแหน่งของตนที่อยู่ในกรอบการควบคุมได้ดีขึ้น และตอบคำถามสำคัญๆ ได้ดีขึ้น เช่น: วิธีการควบคุมแบบตรวจพบเพียงพอที่จะระบุข้อผิดพลาดที่สามารถหลุดรอดผ่านวิธีการควบคุมแบบป้องกันมาได้หรือไม่? วิธีการควบคุมแบบแก้ไขสามารถแก้ไขข้อผิดพลาดเมื่อตรวจพบได้ในทันทีหรือไม่? การจำแนก

ประเภทของการควบคุมด้าน IT โดยทั่วไปจะแบ่งเป็นวิธีการควบคุมทั่วไป (General Controls) และวิธีการควบคุมระบบงาน (Application Controls) สำหรับคำนิยามเพิ่มเติมเกี่ยวกับวิธีการควบคุมที่เกี่ยวข้องกับ IT โปรดดูที่ GTAG 8 เรื่อง การตรวจสอบวิธีการควบคุมระบบงาน (Auditing Application Controls)



รูปที่ 2 : การจัดประเภทของการควบคุมบางอย่าง

6.1.1 วิธีการควบคุมทั่วไปด้าน IT

วิธีการควบคุมทั่วไปจะถูกนำมาใช้ในทุกองค์ประกอบของระบบ ในทุกกระบวนการ และข้อมูลสำหรับองค์กรหรือสภาพแวดล้อมของระบบใดระบบหนึ่ง วิธีการควบคุมทั่วไปได้แก่ การกำกับดูแลด้าน IT การบริหารความเสี่ยง การบริหารทรัพยากร การดำเนินงานด้าน IT การพัฒนาและบำรุงรักษาระบบงาน การจัดการผู้ใช้ระบบ ความปลอดภัยเชิงตรรกะ ความปลอดภัยทางกายภาพ การจัดการการเปลี่ยนแปลง การสำรองข้อมูลและกู้คืน และความต่อเนื่องของธุรกิจ วิธีการควบคุมทั่วไปบางอย่างจะเกี่ยวข้องกับกระบวนการทางธุรกิจ (เช่น การแบ่งแยกหน้าที่ หรือการจัดการกำกับดูแล) ในขณะที่การควบคุมอื่นๆ เป็นเรื่องทางเทคนิคมากๆ (เช่น วิธีการควบคุมซอฟต์แวร์ระบบและวิธีการควบคุมซอฟต์แวร์เครือข่าย) และเกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญ วิธีการควบคุมทั่วไปจะต้องได้รับการตรวจสอบจากผู้ตรวจสอบภายในเนื่องจากวิธีการเหล่านั้นจะก่อให้เกิดพื้นฐานของสภาพแวดล้อมการควบคุมด้าน IT หากการควบคุมทั่วไปอ่อนแอและไม่น่าเชื่อถือ (เช่น การควบคุมการเปลี่ยนแปลงและการเข้าถึง) และไม่สามารถเชื่อมั่นได้ ผู้ตรวจสอบอาจจำเป็นต้องเปลี่ยนวิธีการทดสอบสำหรับบริเวณที่ได้รับผลกระทบ

6.1.2 การควบคุมเฉพาะระบบงาน

วิธีการควบคุมเฉพาะระบบงาน[5] เกี่ยวข้องกับขอบเขตของกระบวนการทางธุรกิจแต่ละกระบวนการ หรือระบบงานแต่ละระบบ และรวมถึง วิธีการควบคุมที่อยู่ภายในระบบงานที่เกี่ยวกับ การนำเข้าข้อมูลสู่ระบบ การประมวลผลข้อมูล การนำเสนอผลลัพธ์จากระบบ วิธีการควบคุมระบบงานยังหมายรวมไปถึง การแก้ไขข้อมูล (data edits) การแบ่งแยกหน้าที่งานของหน่วยงานทางธุรกิจ (เช่น การเริ่มทำรายการ กับการอนุมัติรายการ) การเปรียบเทียบยอดรวมจากการประมวลผล การบันทึกทะเบียนรายการในระบบ และการรายงานข้อผิดพลาด

หน้าที่ของวิธีการควบคุมวิธีหนึ่งจะมีความเกี่ยวข้องอย่างยิ่งกับการประเมินการออกแบบและประสิทธิผลของวิธีการควบคุมนั้น วิธีการควบคุมโดยปกติแล้วจะแบ่งออกเป็น แบบป้องกัน แบบตรวจพบ และแบบแก้ไข วิธีการควบคุมแบบป้องกัน (Preventive controls) นั้นจะป้องกันความผิดพลาด การละเว้นหรือการละเมิดความปลอดภัยไม่ให้เกิดขึ้น ตัวอย่างเช่น การแก้ไขการป้อนข้อมูลแบบง่ายๆ ที่ป้องกันไม่ให้ป้อนข้อมูลที่เป็นตัวอักษรในฟิลด์ที่เป็นตัวเลข วิธีการควบคุมการเข้าถึงที่ปกป้องข้อมูลสำคัญหรือทรัพยากรระบบจากผู้ไม่ได้รับอนุญาต และวิธีการควบคุมทางเทคนิคที่ซับซ้อนและมีการเปลี่ยนแปลงได้เสมอ เช่น โปรแกรมป้องกันไวรัส การติดตั้งไฟร์วอลล์ และระบบป้องกันการบุกรุก (IPS-intrusion prevention systems) เป็นต้น

วิธีการควบคุมแบบตรวจพบ (Detective controls) จะตรวจหาข้อผิดพลาดหรือเหตุการณ์ที่เล็ดรอดผ่านการควบคุมแบบป้องกันมาได้ ตัวอย่างเช่น วิธีการควบคุมแบบตรวจพบอาจระบุหมายเลขบัญชีของบัญชีที่ไม่ใช้งานหรือบัญชีที่ถูกตั้งค่าสถานะให้เฝ้าติดตามเพื่อนำมาตรวจสอบกิจกรรมที่น่าสงสัย การควบคุมแบบตรวจพบยังรวมถึงการติดตามและวิเคราะห์เพื่อเปิดเผยกิจกรรมหรือเหตุการณ์ที่เกินกว่าวงเงินที่ได้รับอนุมัติ หรือขัดต่อรูปแบบของข้อมูลซึ่งเป็นที่รับทราบซึ่งอาจบ่งบอกถึงการทำรายการที่ไม่เหมาะสมได้ สำหรับการส่งผ่านข้อมูลที่ละเอียดอ่อนผ่านทางการสื่อสารอิเล็กทรอนิกส์นั้น การควบคุมแบบตรวจพบจะสามารถระบุได้ว่า ข้อความที่ส่งนั้นมีการดัดแปลง หรือ ไม่สามารถระบุตัวตนผู้ส่งได้

วิธีการควบคุมแบบแก้ไข (Corrective controls) จะทำการแก้ไขข้อผิดพลาด การละเลย หรือเหตุการณ์ผิดปกติทันทีที่ตรวจพบ วิธีการควบคุมแบบแก้ไขจะมีอยู่หลากหลาย มีตั้งแต่การแก้ไขข้อผิดพลาดในการป้อนข้อมูลอย่างง่ายๆ ไปจนถึงการระบุและลบผู้ใช้งานหรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตออกจากระบบหรือเครือข่าย ไปจนถึงการกู้คืนระบบจากอุบัติการณ์ การหยุดชะงัก หรือเกิดภัยพิบัติ

---

[5] สภามาตรฐานความปลอดภัยของข้อมูลในอุตสาหกรรมบัตรชำระเงิน (PCI Security Standards Council), ข้อกำหนดมาตรฐานความปลอดภัยของข้อมูลสำหรับอุตสาหกรรมชำระเงินด้วยบัตรและวิธีการประเมินความปลอดภัย (Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures) รุ่นที่ 2.0., ตุลาคม 2553

โดยทั่วไปแล้ว การควบคุมจะมีประสิทธิภาพมากที่สุดคือ ต้องป้องกันข้อผิดพลาดไม่ให้เกิดขึ้น หรือตรวจพบโดยเร็วที่สุดเพื่อให้การแก้ไขง่ายขึ้น

การจำแนกประเภทการควบคุมอื่นๆ ที่หลากหลายดังที่อธิบายไว้ในเอกสารฉบับนี้อาจมีประโยชน์ในการประเมินประสิทธิผลของวิธีการควบคุมเหล่านั้น ตัวอย่างเช่น วิธีการควบคุมแบบอัตโนมัติ (Automated controls) มีแนวโน้มที่จะมีความน่าเชื่อถือมากกว่าวิธีการควบคุมที่ทำด้วยมือ (Manual controls) และวิธีการควบคุมโดยไม่ต้องอาศัยการตัดสินใจ (nondiscretionary) มีแนวโน้มที่จะถูกนำมาใช้อย่างต่อเนื่องมากกว่าวิธีการควบคุมโดยอาศัยการตัดสินใจ (discretionary) การจำแนกประเภทวิธีการควบคุมอื่นๆ เช่น ภาคบังคับ (Mandatory) ภาคสมัครใจ (Voluntary) แบบเสริม (Complementary) แบบทดแทน (Compensating) แบบทำซ้ำ (Redundant) แบบต่อเนื่อง (Continuous) แบบตามความต้องการ (on-demand) และแบบอิงเหตุการณ์ (event-driven)

6.2 การกำกับดูแลด้าน IT การบริหาร และวิธีการควบคุมทางเทคนิค

อีกรูปแบบหนึ่งของการจำแนกประเภทวิธีการควบคุมก็คือ การจำแนกตามกลุ่มที่มีหน้าที่ทำให้แน่ใจว่า ได้มีการนำวิธีการควบคุมนั้นไปปรับใช้งานและดูแลรักษาอย่างเหมาะสม สำหรับวัตถุประสงค์ในการประเมินบทบาทและหน้าที่นั้น คู่มือนี้ในเบื้องต้นได้จัดหมวดหมู่ของวิธีการควบคุมด้าน IT ออกเป็น การกำกับดูแล การบริหาร การควบคุมด้านเทคนิค และการควบคุมเฉพาะระบบงาน

สองระดับแรก (การกำกับดูแลและการบริหาร) ประยุกต์ใช้ได้มากที่สุดกับเนื้อหาของแนวปฏิบัติฉบับนี้ อย่างไรก็ตาม อาจจะเป็นประโยชน์ในการทำความเข้าใจถึงวิธีการควบคุมพิเศษในระดับสูงขึ้น โดยเฉพาะที่ได้ถูกกำหนดไว้ภายในโครงสร้างพื้นฐานด้าน IT ทางด้านเทคนิคและระบบงาน วิธีการควบคุมทางด้านเทคนิคและวิธีการควบคุมเฉพาะระบบงานคือหัวข้อของ GTAG 8 เรื่อง การตรวจสอบวิธีการควบคุมระบบงาน (Auditing Application Controls)

6.2.1 วิธีการควบคุมด้วยการกำกับดูแลด้าน IT

ภาระหน้าที่หลักสำหรับการดูแลการควบคุมภายในจะตกอยู่กับคณะกรรมการในบทบาทของผู้ที่ต้องรักษาไว้ซึ่งกรอบของการกำกับดูแล การควบคุมทาง IT ณ ที่ระดับการกำกับดูแล จะเกี่ยวข้องกับการดูแลการบริหารข้อมูลอย่างมีประสิทธิผล หลักการต่างๆ และกระบวนการ รวมทั้งให้ความเชื่อมั่นได้ว่ามีอยู่จริงและมีการนำไปปฏิบัติอย่างถูกต้อง วิธีการควบคุมเหล่านี้เชื่อมโยงกับแนวคิดในเรื่องการกำกับดูแล ซึ่งถูกขับเคลื่อนโดยเป้าหมายและกลยุทธ์ขององค์กร และโดยข้อกำหนดจากหน่วยงานภายนอก เช่น หน่วยงานทางการที่มีหน้าที่กำกับดูแลต่างๆ

6.2.2 วิธีการควบคุมทางการบริหาร

ภาระหน้าที่ของผู้บริหารต่อการควบคุมภายในโดยทั่วไปนั้น มักเกี่ยวข้องเข้าไปถึงในทุกพื้นที่ขององค์กร โดยจะให้ความสนใจเป็นพิเศษกับสินทรัพย์ที่สำคัญ ข้อมูลที่ละเอียดอ่อน และหน้าที่งานด้านปฏิบัติการ ผู้บริหารจะต้องทำให้แน่ใจได้ว่า วิธีการควบคุมด้าน IT ที่จำเป็นต่อการบรรลุวัตถุประสงค์ที่กำหนดไว้ขององค์กรนั้นได้มีการนำมาปรับใช้ และทำให้แน่ใจถึงการประมวลผลที่เชื่อถือได้และดำเนินการอย่างต่อเนื่อง วิธีการควบคุมเหล่านี้จะถูกนำไปใช้โดยเป็นผลมาจากการกระทำโดยเจตนาฝ่ายบริหารในการที่จะตอบสนองต่อความเสี่ยงที่มีต่อองค์กร กระบวนการ และสินทรัพย์ต่างๆ

6.2.3 วิธีการควบคุมทางด้านเทคนิค

วิธีการควบคุมทางเทคนิคมักจะเป็นแกนสำคัญที่ช่วยค้ำจุนกรอบการควบคุมทางการบริหาร ดังนั้น หากการควบคุมทางเทคนิคอ่อนแอ ก็จะส่งผลกระทบต่อกรอบการควบคุมทั้งหมด ตัวอย่างเช่น ด้วยการป้องกันการเข้าถึงและการบุกรุกที่ไม่ได้รับอนุญาต วิธีการควบคุมทางเทคนิคจะให้พื้นฐานของความเชื่อมั่นในความถูกต้องของข้อมูล (ซึ่งรวมถึงหลักฐานการเปลี่ยนแปลงทั้งหมดและสิ่งที่รับรองความถูกต้องของการเปลี่ยนแปลงเหล่านั้น) วิธีการควบคุมเหล่านี้มีรูปแบบเฉพาะกับเทคโนโลยีที่ใช้ภายในโครงสร้างพื้นฐานด้าน IT ขององค์กร ตัวอย่างของวิธีการควบคุมทางเทคนิค เช่น การควบคุมระบบปฏิบัติการ (OS) การควบคุมฐานข้อมูล การเข้ารหัสและการบันทึกประวัติรายการ (logging)

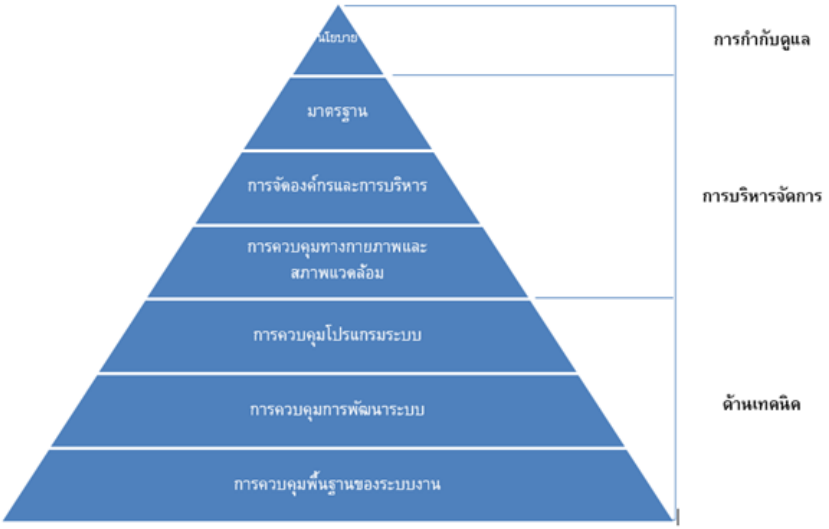
6.2.4 การควบคุมระบบงาน

ตามที่ได้จัดให้มีไว้แล้ว วิธีการควบคุมระบบงานจะเกี่ยวข้องกับขอบเขตของแต่ละกระบวนการทางธุรกิจหรือแต่ละระบบงาน วิธีการควบคุมแล้วอาจเป็นสิ่งที่โดยลักษณะแล้วเป็นด้านเทคนิค แต่ก็อาจไม่ใช่ด้านเทคนิคก็ได้ โดยขึ้นอยู่กับประเด็นของการควบคุม วิธีการควบคุมเหล่านี้ได้แก่ วิธีการควบคุมการนำข้อมูลเข้าสู่ระบบ วิธีการควบคุมการประมวลผล และการผลลัพธ์จากการประมวลผล ในส่วนที่ 6.3.7 ของเอกสารฉบับนี้จะอธิบายการควบคุมเฉพาะระบบงานในเชิงลึกมากขึ้น

6.3 วิธีการควบคุมด้าน IT - สิ่งที่คาดหวัง

วิธีการควบคุมแต่ละวิธีภายในองค์กรสามารถจำแนกได้ภายในลำดับชั้นของวิธีการควบคุมด้าน IT กล่าวคือ เริ่มต้นจากคำแถลงนโยบายในภาพรวมระดับสูงที่กำหนดโดยฝ่ายบริหารและอนุมัติรับรองโดยคณะกรรมการ ไล่ลงไปจนถึงกลไกของการควบคุมเฉพาะอย่างที่ผนวกเข้าไปในระบบงาน

รูปที่ 3 – ลำดับชั้นของวิธีการควบคุมด้าน IT แสดงให้เห็นถึงวิธีการ "จากบนลงล่าง" ที่เป็นเหตุเป็นผลกันทั้งในการพิจารณาวิธีการควบคุมที่จะนำมาใช้งาน และในการกำหนดบริเวณที่ต้องมุ่งเน้นทรัพยากรการตรวจสอบภายในในระหว่างการสอบทานสภาพแวดล้อมการทำงานด้าน IT ทั้งหมด องค์ประกอบที่แตกต่างกันของลำดับชั้นไม่ได้แยกจากกันโดยเด็ดขาด โดยจะเชื่อมต่อซึ่งกันและกัน และมักจะทับซ้อนและผสมผสานเข้าด้วยกัน การควบคุมแต่ละประเภทภายในลำดับชั้น ได้อธิบายไว้ด้านล่าง



รูปที่ 3 – ลำดับชั้นของวิธีการควบคุมด้าน IT

6.3.1 นโยบาย

ทุกองค์กรต้องกำหนดเป้าหมายและวัตถุประสงค์โดยผ่านแผนกลยุทธ์และนโยบาย หากไม่มีการแถลงถึงนโยบายและมาตรฐานที่ชัดเจนในการกำหนดทิศทาง องค์กรอาจสับสนและดำเนินงานอย่างไม่มีประสิทธิผล

เนื่องจากเทคโนโลยีมีความสำคัญต่อทุกองค์กร ควรมีการสร้างนโยบายที่ชัดเจนเกี่ยวกับ IT ในทุกแง่มุม ซึ่งได้รับอนุมัติจากฝ่ายบริหารและรับรองโดยคณะกรรมการ และสื่อสารไปยังพนักงาน นโยบายอาจมีความแตกต่างกันขึ้นอยู่กับขนาดขององค์กรและขอบเขตของการนำ IT ไปปรับใช้ สำหรับองค์กรขนาดเล็กนโยบายฉบับเดียวอาจเพียงพอ – โดยที่ต้องมีเนื้อหาครอบคลุมส่วนที่เกี่ยวข้องทั้งหมด แต่องค์กรขนาดใหญ่มักจะต้องการนโยบายที่ละเอียดมากกว่าและเฉพาะเจาะจงมากขึ้น

ตัวอย่าง นโยบายด้าน IT ที่อาจจะรวมสิ่งต่างๆ ดังต่อไปนี้ เช่น:

- นโยบายทั่วไปที่กำหนดระดับของความปลอดภัยและความเป็นส่วนตัวครอบคลุมทั่วทั้งองค์กร นโยบายนี้ควรสอดคล้องกับกฎหมายในประเทศและกฎหมายระหว่างประเทศที่เกี่ยวข้อง และควรระบุระดับของการควบคุมและความปลอดภัยที่จำเป็น ซึ่งโดยปกติจะขึ้นอยู่กับระดับความละเอียดอ่อน (sensitivity) ของระบบและข้อมูลที่ถูกประมวลผล
- ข้อความเกี่ยวกับการจัดประเภทข้อมูลและสิทธิการเข้าถึงข้อมูลในแต่ละระดับ ในนโยบายควรกำหนดข้อจำกัดในการใช้ข้อมูลเหล่านี้โดยบุคคลผู้ที่ได้รับอนุมัติสิทธิในการเข้าถึง
- คำนิยามของแนวคิดเกี่ยวกับการเป็นเจ้าของข้อมูลและเจ้าของระบบ รวมทั้งอำนาจที่จำเป็นในการสร้าง แก้ไขหรือลบข้อมูล ซึ่งควรเป็นนโยบายทั่วไปที่ใช้กำหนดขอบเขตที่ผู้ใช้งานสามารถสร้างระบบงานหรือแอพพลิเคชันของตนเองได้

- นโยบายด้านบุคคลากร ซึ่งระบุและบังคับใช้เงื่อนไขสำหรับพนักงานในบริเวณที่มีความอ่อนไหว (sensitive areas) โดยรวมถึงการตรวจสอบข้อมูลภูมิหลังของพนักงานที่เข้าใหม่ก่อนรับเข้าทำงานในองค์กร และกำหนดให้พนักงานต้องลงนามในข้อตกลงเพื่อยอมรับภาระหน้าที่ของตนที่มีต่อระดับของการควบคุม การรักษาความปลอดภัย และการรักษาความลับที่องค์กรต้องการ นโยบายนี้มักจะให้รายละเอียดที่เกี่ยวข้องกับกระบวนการทางวินัยด้วย
- คำนิยามข้อกำหนดของแผนต่อเนื่องทางธุรกิจในภาพรวม นโยบายเหล่านี้ควรให้ความมั่นใจได้ว่าทุกๆ ด้านของธุรกิจจะได้รับการพิจารณาเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด หรือเมื่อมีภัยพิบัติเกิดขึ้น

6.3.2 มาตรฐาน

องค์กรควรมีพิมพ์เขียว (blue print) ด้าน IT ที่สนับสนุนกลยุทธ์โดยรวม และกำหนดลักษณะทั่วๆ ไปของนโยบายและมาตรฐานด้าน IT ที่จะตามมา[6]

มาตรฐานจะกำหนดวิธีการทำงานเพื่อที่จะบรรลุวัตถุประสงค์ขององค์กร การยอมรับและบังคับใช้มาตรฐานจะช่วยส่งเสริมให้เกิดประสิทธิภาพ และสร้างความมั่นใจในความสม่ำเสมอภายในสภาพแวดล้อมการทำงานด้าน IT (IT operating environment)

องค์กรขนาดใหญ่อาจมีทรัพยากรมากมายเพียงพอที่จะสร้างมาตรฐานเป็นของตนเอง แต่ในองค์กรขนาดเล็กอาจไม่มีทรัพยากรที่เพียงพอ มีแหล่งข้อมูลมากมายเกี่ยวกับมาตรฐานและวิธีปฏิบัติที่เป็นเลิศ (best practice) ตัวอย่างเช่น สิ่งที่ผู้บริหาร IT ควรพิจารณา มีดังนี้:

- **กระบวนการพัฒนาระบบ**: เมื่อองค์กรพัฒนาระบบงานขึ้นใช้เอง มาตรฐานจะถูกนำมาปรับใช้กับกระบวนการในการออกแบบ การพัฒนาโปรแกรม การทดสอบระบบ การติดตั้งใช้งานระบบ และการบำรุงรักษาระบบและโปรแกรม หากองค์กรว่าจ้างผู้ให้บริการภายนอกให้พัฒนาระบบหรือจัดซื้อระบบจากผู้ขายมาใช้งาน CAE ควรตรวจสอบให้แน่ใจว่ามีข้อตกลงสัญญากำหนดให้ผู้ให้บริการนั้นใช้มาตรฐานที่สอดคล้องกับมาตรฐานขององค์กร หรือเป็นที่ยอมรับขององค์กร
- **การกำหนดค่าซอฟต์แวร์ระบบ**: เนื่องจากซอฟต์แวร์ระบบมีองค์ประกอบการควบคุมขนาดใหญ่ภายในสภาพแวดล้อมด้าน IT มาตรฐานที่เกี่ยวข้องกับการกำหนดค่าระบบให้มีความปลอดภัยจึงเริ่มได้รับการยอมรับอย่างกว้างขวางจากองค์กรและผู้ให้บริการด้านเทคโนโลยีชั้นนำ วิธีที่ผลิตภัณฑ์ต่างๆ (เช่น ระบบปฏิบัติการซอฟต์แวร์ระบบเครือข่าย และระบบจัดการฐานข้อมูล) จะถูกตั้งค่าระบบนั้น จะสามารถช่วยเพิ่มความปลอดภัยหรือจะสร้างจุดอ่อนที่จะบุกรุกก็ได้

[6] *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน* ของสมาคมผู้ตรวจสอบภายในได้ยืนยันว่า หน่วยงานตรวจสอบภายในจะต้องตรวจสอบกลยุทธ์ด้าน IT มาตรฐานของ IIA ที่ 2110.A2 ระบุว่า "หน่วยงานตรวจสอบภายในต้องประเมินว่าการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่"

- **การควบคุมระบบงาน**: ระบบงานทั้งหมดที่สนับสนุนกิจกรรมทางธุรกิจนั้นจำเป็นต้องได้รับการควบคุม มาตรฐานจึงเป็นสิ่งจำเป็นสำหรับระบบงานทั้งหมดที่องค์กรพัฒนาขึ้นเองหรือที่จัดซื้อมาใช้งาน และมาตรฐานควรกำหนดประเภทของวิธีการควบคุมต่างๆ ที่จะต้องมีในกิจกรรมทางธุรกิจทั้งหมด รวมทั้งวิธีการควบคุมเฉพาะที่ควรใช้กับกระบวนการและข้อมูลที่มีความละเอียดอ่อน
- **โครงสร้างของข้อมูล**: การมีคำนิยามของข้อมูลที่สอดคล้องกันในทุกระบบงานอย่างเต็มรูปแบบจะช่วยให้มั่นใจได้ว่า ระบบที่ต่างกันจะสามารถเข้าถึงข้อมูลร่วมกันได้อย่างราบรื่น และมีวิธีการควบคุมความปลอดภัยสำหรับข้อมูลส่วนตัวและข้อมูลที่มีความละเอียดอ่อนอื่นๆ
- **การจัดทำเอกสาร**: ในมาตรฐานควรระบุการจัดทำเอกสารขั้นต่ำที่จำเป็นสำหรับระบบงาน ในแต่ละระบบหรือในการติดตั้งใช้งานด้าน IT ตลอดถึงข้อกำหนดสำหรับทุกประเภทของระบบงาน กระบวนการ และศูนย์ประมวลผลข้อมูล ที่แตกต่างกัน

เช่นเดียวกับเรื่องนโยบาย มาตรฐานที่กำหนดขึ้นควรได้รับการอนุมัติจากผู้บริหารและทำให้ทุกคนสามารถนำไปใช้ปฏิบัติได้

6.3.3 จัดโครงสร้างองค์กรและการบริหารจัดการ

การจัดโครงสร้างองค์กรและการบริหารมีบทบาทสำคัญในระบบการควบคุมด้าน IT ทั้งหมด รวมไปถึงทุกด้านของการดำเนินงานขององค์กร โครงสร้างองค์กรที่เหมาะสมช่วยให้สามารถกำหนดสายการรายงานและภาระหน้าที่รวมทั้งกำหนดระบบการควบคุมที่มีประสิทธิผลที่จะถูกนำไปปฏิบัติได้ โดยทั่วไปแล้ววิธีการควบคุมที่สำคัญมักจะรวมถึง การแบ่งแยกหน้าที่งานที่ไม่ควรอยู่ด้วยกัน วิธีการควบคุมทางด้านการเงิน และการบริหารจัดการความเปลี่ยนแปลง

6.3.3.1 การแบ่งแยกหน้าที่

การแบ่งแยกหน้าที่เป็นองค์ประกอบสำคัญของวิธีการควบคุมหลายๆ อย่าง โครงสร้างขององค์กรไม่ควรอนุญาตให้การทำหน้าที่ในทุกๆ ด้านของการประมวลผลข้อมูลตกอยู่ในมือของบุคคลเพียงคนเดียว หน้าที่งานของการเริ่มจัดทำรายการ การอนุมัติ การป้อนข้อมูล การประมวลผล และการเช็คสอบข้อมูลควรจะต้องแยกออกจากกัน เพื่อให้มั่นใจได้ว่าไม่มีบุคคลใดเพียงคนเดียวที่สามารถสร้างข้อผิดพลาด ข้อยกเว้นหรือรายการผิดปกติอื่นๆ แล้วอนุมัติรายการและ/หรือปกปิดหลักฐานได้ วิธีการควบคุมโดยการแบ่งแยกหน้าที่งานสำหรับระบบงาน/แอพพลิเคชันนั้น สามารถทำได้โดยการให้สิทธิการเข้าถึงระบบที่สอดคล้องกับข้อกำหนดของหน้าที่งาน (Job requirement) ในหน้าที่งานการประมวลผลและการเข้าถึงข้อมูล

การแบ่งแยกหน้าที่แบบดั้งเดิมในสภาพแวดล้อม IT นั้น จะมีการแบ่งแยกระหว่างการพัฒนาระบบ (system development) และการปฏิบัติงานด้าน IT (IT operation) ซึ่งการปฏิบัติงานด้าน IT ควรมีหน้าที่ในการดูแลให้ระบบในสภาพแวดล้อมที่ใช้งานจริง (production systems) ดำเนินไปได้ (ยกเว้นการ

ปรับปรุงระบบเมื่อมีการเปลี่ยนแปลงโปรแกรม) และไม่ควรมีหน้าที่ในกระบวนการพัฒนาระบบ วิธีการควบคุมนี้รวมถึงข้อจำกัดที่ป้องกันไม่ให้ผู้ดูแลระบบ (operator) เข้าถึง หรือแก้ไข โปรแกรมใช้งาน (production program) ระบบ หรือข้อมูลได้ ในขณะเดียวกัน บุคลากรผู้พัฒนาระบบไม่ควรจะต้องมีการติดต่อกับระบบที่ใช้งานจริง (production) ด้วยการมอบหมายหน้าที่เฉพาะเช่นนี้ในระหว่างการติดตั้งระบบและเมื่อมีการเปลี่ยนแปลงด้านอื่นๆ หลักการแบ่งแยกหน้าที่ก็จะสามารถบังคับใช้ได้ ในองค์กรขนาดใหญ่มีอยู่หลายๆ หน้าที่งานที่ควรได้รับการพิจารณา เพื่อให้มั่นใจได้ว่ามีการแบ่งแยกหน้าที่งานที่เหมาะสม

6.3.3.2 วิธีการควบคุมทางด้านการเงิน

เนื่องจากองค์กรต่างๆ ต้องใช้เงินลงทุนอย่างมากมายในด้าน IT จึงมีความจำเป็นที่จะต้องมีวิธีการควบคุมงบประมาณและวิธีการควบคุมในทางการเงินอื่นๆ เพื่อให้แน่ใจได้ว่า เทคโนโลยีที่ลงทุนไปนั้นจะให้ผลตอบแทนกลับมาจากการลงทุนหรือช่วยให้ลดค่าใช้จ่ายได้ตามที่คาดการณ์ไว้ ดังนั้น ควรกำหนดกระบวนการทางการบริหารไว้ เพื่อรวบรวม วิเคราะห์ และรายงานประเด็นเหล่านี้ แต่น่าเสียดายที่การพัฒนาด้าน IT ใหม่ๆ มักประสบกับค่าใช้จ่ายที่สูงเกินความจำเป็น และล้มเหลวในการประหยัดค่าใช้จ่ายหรือรายได้ตามที่คาดไว้ ซึ่งเป็นผลมาจากการประมาณการผิดพลาดหรือการวางแผนที่ไม่ดีพอ

6.3.3.3 การบริหารการเปลี่ยนแปลง

กระบวนการบริหารการเปลี่ยนแปลง[7] ช่วยให้มั่นใจได้ว่า การเปลี่ยนแปลงใน สภาพแวดล้อม IT ซอฟต์แวร์ระบบ ระบบงาน (application systems) และข้อมูลนั้น จะถูกนำไปใช้ในลักษณะที่มีการบังคับใช้การแบ่งแยกหน้าที่ที่เหมาะสม ทำให้มั่นใจได้ว่า การเปลี่ยนแปลงนั้นใช้การได้และนำไปใช้ปฏิบัติได้ตามที่ต้องการ รวมทั้งป้องกันการแสวงหาโอกาสจากการเปลี่ยนแปลงเพื่อการทำทุจริต หากไม่มีการบริหารการเปลี่ยนแปลงแล้ว ความพร้อมใช้งานและการให้บริการของระบบอาจได้รับผลกระทบอย่างรุนแรงได้

6.3.4 การควบคุมทางกายภาพและสภาพแวดล้อม

อุปกรณ์ด้าน IT เป็นสิ่งที่แสดงให้ถึงเงินลงทุนที่สำคัญสำหรับในหลายๆ องค์กรซึ่งจะต้องได้รับการปกป้องจากความเสียหายหรือการสูญเสียโดยอุบัติเหตุหรือโดยเจตนา วิธีการควบคุมทางกายภาพและสภาพแวดล้อม (ซึ่งแต่เดิมได้ถูกพัฒนาขึ้นสำหรับศูนย์คอมพิวเตอร์ขนาดใหญ่ที่เป็นที่ตั้งของเครื่องคอมพิวเตอร์ประมวลผลที่มีสมรรถนะสูง (mainframe)) ปัจจุบันมีความสำคัญเท่าเทียมกันกับคอมพิวเตอร์ในระบบไคลเอนต์ - เซิร์ฟเวอร์ และระบบงานบนเว็บ แม้ว่าอุปกรณ์ที่ใช้กันทั่วไปในทุกวันนี้จะได้รับการออกแบบมาเพื่อความสะดวกในการใช้งานในสภาพแวดล้อมที่เป็นสำนักงานทั่วไป แต่คุณค่าที่มีต่อธุรกิจและต้นทุนรวมทั้งความอ่อนไหวของระบบงานที่ใช้ในกระบวนการทางธุรกิจนั้นก็มีนัยสำคัญ

[7] ดู GTAG 2 ของ IIA เรื่อง *วิธีการควบคุมการบริหารการเปลี่ยนแปลงและการปิดช่องโหว่: สิ่งสำคัญต่อความสำเร็จขององค์กร (Change and Patch Management Controls: Critical for Organizational Success)*

อุปกรณ์ทั้งหมดจะต้องได้รับการปกป้อง ซึ่งรวมถึงเครื่องแม่ข่าย (Server) และเครื่องคอมพิวเตอร์ตั้งโต๊ะ (Workstation) ที่อนุญาตให้พนักงานใช้เพื่อเข้าถึงระบบงาน วิธีการควบคุมทางกายภาพและสภาพแวดล้อมโดยทั่วไป มักจะได้แก่ :

- ตั้งเครื่องแม่ข่ายไว้ในห้องที่ปิดกุญแจ ซึ่งจำกัดการเข้าถึง โดยให้เข้าได้เฉพาะคนที่ได้รับอนุญาต
- จำกัดการเข้าถึงเครื่องแม่ข่ายให้เข้าได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
- จัดหาอุปกรณ์ตรวจจับและระงับเหตุไฟไหม้
- จัดเก็บอุปกรณ์ ระบบงานและข้อมูลที่มีความอ่อนไหว ไว้ให้ห่างจากสภาพแวดล้อมที่เสี่ยงอันตราย เช่น ที่ๆ อยู่ในระดับต่ำซึ่งเสี่ยงต่อน้ำท่วม เส้นทางบินหรือ สถานที่จัดเก็บของเหลวที่ติดไฟได้

ในการพิจารณาถึงความปลอดภัยทางกายภาพและสภาพแวดล้อมนั้น ควรคำนึงถึงการวางแผนฉุกเฉิน[8] ด้วย องค์กรจะทำอย่างไรเมื่อเกิดไฟไหม้หรือน้ำท่วม หรือเมื่อมีภัยคุกคามอื่นใดแสดงตัวขึ้น? องค์กรจะดำเนินงานต่อไปได้อย่างไร? การวางแผนประเภทนี้มีมากไปกว่าแค่การจัดเตรียมไฟฟ้าสำรองสำหรับการประมวลผลไว้ให้พร้อมใช้งานและการสำรองข้อมูลของระบบงานที่ใช้เป็นประจำเท่านั้น โดยต้องคำนึงถึงด้านโลจิสติกส์ และการประสานงานที่จำเป็นสำหรับกิจกรรมทางธุรกิจรอบด้าน สุดท้ายแล้วประวัติศาสตร์ได้แสดงให้เห็นมาบ่อยๆ ว่า แผนต่อเนื่องทางธุรกิจซึ่งไม่เคยได้รับการทดสอบในสถานการณ์จำลองเสมือนจริงจนสำเร็จนั้น เป็นแผนที่เชื่อถือไม่ได้

6.3.5 วิธีการควบคุมซอฟต์แวร์ระบบ

ผลิตภัณฑ์ซอฟต์แวร์ระบบ (systems software) จะช่วยให้อุปกรณ์ IT สามารถใช้งานได้โดยผ่านทางระบบงานและผู้ใช้งาน ผลิตภัณฑ์เหล่านี้ได้แก่ ระบบปฏิบัติการ (เช่น Windows และ UNIXเป็นต้น) ซอฟต์แวร์เครือข่าย และไฟร์วอลล์ (Firewall) ผลิตภัณฑ์ป้องกันไวรัส และระบบจัดการฐานข้อมูล (DBMS) (เช่น Oracle และ DB2 เป็นต้น)

ผู้เชี่ยวชาญด้านการตรวจสอบ IT ควรประเมินวิธีการควบคุมในส่วนนี้ องค์กรขนาดเล็กไม่น่าจะมีทรัพยากรในการจ้างผู้เชี่ยวชาญดังกล่าวและควรพิจารณาการใช้ทรัพยากรจากภายนอก ไม่ว่าผู้ตรวจสอบภายในด้าน IT จะเป็นพนักงานขององค์กรเอง หรือเป็นผู้ให้บริการจากภายนอกที่องค์กรจ้างมาก็ตาม พวกเขาต้องมีชุดความรู้ที่เฉพาะเจาะจง ความรู้ส่วนใหญ่สามารถมาได้จากประสบการณ์ แต่ก็ต้องมีการปรับปรุงเพิ่มเติมความรู้ดังกล่าวต้องอย่างต่อเนื่องเพื่อให้ทันต่อสถานการณ์ปัจจุบันและมีประโยชน์ต่อองค์กร

[8] ดู GTAG 10 ของ IIA เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

ซอฟต์แวร์ระบบอาจจะมีความซับซ้อนสูงมาก และสามารถนำไปปรับใช้กับองค์ประกอบและอุปกรณ์ภายในสภาพแวดล้อมของระบบและเครือข่าย การกำหนดค่าซอฟต์แวร์ต้องกำหนดให้รองรับความต้องการเฉพาะทางที่สูงมาก และโดยปกติแล้ว จะต้องใช้ความเชี่ยวชาญระดับสูงในการดูแลค่าความปลอดภัย เทคนิคในการตั้งค่าระบบจะสามารถควบคุมการเข้าถึงโดยผ่านทางระบบงาน (logical access) ถึงแม้ว่าบางระบบงานจะมีวิธีการควบคุมการเข้าถึงโดยระบบงานเหล่านั้นเองและอาจเปิดโอกาสให้ผู้ใช้ที่ไม่ได้รับอนุญาตทำการเจาะเข้าระบบได้ เทคนิคการตั้งค่าระบบยังให้วิถีทางที่จะบังคับใช้วิธีการแยกหน้าที่ สร้างร่องรอยเฉพาะสำหรับการตรวจสอบ (audit trails) และใช้วิธีการควบคุมความสมบูรณ์ถูกต้องของข้อมูล (data integrity control) โดยผ่านรายการควบคุมการเข้าถึง (access control list) การกลั่นกรองข้อมูล (filter) และบันทึกกิจกรรม (activity log)

วิธีการควบคุมทางเทคนิคที่สำคัญบางวิธีที่คาดว่าควรจะมีอยู่ในสภาพแวดล้อม IT ที่มีการจัดการที่ดี ได้แก่:

- สิทธิการเข้าถึงได้รับการจัดสรรและควบคุมตามนโยบายขององค์กรที่ได้ระบุไว้
- มีการบังคับใช้วิธีการควบคุมโดยการแบ่งแยกหน้าที่ผ่านซอฟต์แวร์ระบบและวิธีการควบคุมอื่นๆ ที่ใช้ในการกำหนดค่า
- มีการประเมินการบุกรุกและช่องโหว่[9] มีวิธีการป้องกัน และการตรวจหาการบุกรุก และมีการเฝ้าระวังอย่างต่อเนื่อง
- มีการทดสอบการบุกรุกอยู่เป็นประจำ
- มีบริการการเข้ารหัส ในที่ซึ่งมี requirement กำหนดไว้ว่าต้องเป็นความลับ
- มีกระบวนการบริหารการเปลี่ยนแปลง (รวมถึงการจัดการซ่อมแซมช่องโหว่ของโปรแกรม -- Patch) เพื่อให้แน่ใจว่ามีกระบวนการควบคุมอย่างรัดกุมทุกครั้งที่มีการเปลี่ยนแปลงและการซ่อมแซมเกิดขึ้นกับซอฟต์แวร์ระบบ องค์ประกอบของเครือข่ายและข้อมูล[10]

6.3.6 วิธีการควบคุมการพัฒนาและการจัดหาระบบ

องค์กรหลายแห่งไม่ค่อยใช้กระบวนวิธี (methodology) เดียวสำหรับการได้มาหรือการพัฒนาระบบทั้งหมด แต่จะเลือกกระบวนวิธีให้เหมาะสมกับสถานการณ์เฉพาะ ผู้ตรวจสอบด้าน IT ควรประเมินว่าองค์กรมีวิธีการควบคุมในการพัฒนาหรือจัดหาระบบงานหรือไม่? และวิธีการควบคุมนั้นได้ก่อให้เกิดวิธีการควบคุมที่มีประสิทธิผลหลายๆ วิธีซึ่งควบคุมระบบงานและข้อมูลที่ระบบทำการประมวลผลหรือไม่? โดยการตรวจสอบวิธีการต่างๆ ในการพัฒนาระบบงานอย่างละเอียด ผู้ตรวจสอบภายในจะเชื่อมั่นได้ว่าการควบคุม

[9] ดู GTAG 6 เรื่อง การบริหารและการตรวจสอบช่องโหว่ (Managing and Auditing IT Vulnerabilities)

[10] ดู GTAG 2 เรื่อง วิธีการควบคุมการบริหารการเปลี่ยนแปลงและการซ่อมแซมช่องโหว่ (Change and Patch Management Controls: Critical for Organizational Success)

ภายในระบบงานนั้นเพียงพอ ประเด็นการควบคุมขั้นพื้นฐานบางอย่างควรได้รับการดำเนินการในการพัฒนาและการจัดหาระบบงานทั้งหมด ตัวอย่างเช่น:

- ควรบันทึกความต้องการของผู้ใช้งาน (User requirements) ไว้เป็นเอกสาร และควรมีการวัดผลความสำเร็จด้วย
- การออกแบบระบบควรเป็นไปตามกระบวนการที่เป็นทางการ เพื่อให้แน่ใจว่าความต้องการของผู้ใช้และวิธีการควบคุมได้รับการออกแบบให้มีอยู่ในระบบ
- การพัฒนาระบบควรดำเนินการในลักษณะที่มีโครงสร้างเพื่อให้มั่นใจว่า ความต้องการผู้ใช้งานและฟีเจอร์ (features) ต่างๆ ที่ได้ออกแบบและอนุมัติไว้แล้วนั้น ได้ถูกรวมอยู่ในระบบงานที่สำเร็จแล้ว
- การทดสอบระบบควรให้ความมั่นใจได้ว่า องค์ประกอบของระบบแต่ละส่วน สามารถทำงานได้ตามต้องการ การเชื่อมต่อ (interface) ระหว่างระบบงานดำเนินการได้ตามที่คาดไว้ และเจ้าของระบบให้การยืนยันว่ามีฟังก์ชั่นต่างๆ ในการใช้งานตามที่ตั้งใจไว้แล้ว
- กระบวนการบำรุงรักษาระบบงาน ควรให้ความมั่นใจได้ว่า การเปลี่ยนแปลงภายในระบบงานได้ดำเนินการตามรูปแบบการควบคุมที่กำหนดไว้อย่างสม่ำเสมอ และมีกระบวนการตรวจพิสูจน์ (Validation process) อย่างมีโครงสร้าง เพื่อที่จะเชื่อมั่นได้ในการบริหารการเปลี่ยนแปลงนั้น

ในกรณีที่การพัฒนาระบบเป็นการว่าจ้างผู้ให้บริการจากภายนอกให้ทำการพัฒนาระบบ ในสัญญาว่าจ้างควรกำหนดให้มีวิธีการควบคุมในลักษณะเดียวกัน เทคนิคและวิธีการควบคุมการบริหารโครงการควรเป็นส่วนหนึ่งในกระบวนการพัฒนาระบบ (ไม่ว่าจะเป็นการพัฒนาขึ้นใช้เองภายในองค์กรหรือว่าจ้างให้ผู้ให้บริการจากภายนอกพัฒนา) ฝ่ายบริหารควรได้รับทราบว่า โครงการจะเสร็จตามเวลาและภายในงบประมาณและทรัพยากรถูกใช้อย่างมีประสิทธิภาพหรือไม่? กระบวนการรายงานควรให้ความเชื่อมั่นได้ว่า ฝ่ายบริหารเข้าใจถึงสถานะปัจจุบันของโครงการพัฒนาระบบ และจะไม่มีความประหลาดใจใดๆ เกิดขึ้นเมื่อมีการส่งมอบระบบงาน[11] ในการประเมินโครงการพัฒนาหรือจัดหาระบบงาน สามารถดูรายละเอียดได้จาก GTAG 12 เรื่อง การตรวจสอบโครงการด้าน (IT Auditing IT Projects)

6.3.7 การควบคุมเฉพาะระบบงาน (Application Controls)[12]

วัตถุประสงค์ของการควบคุมเฉพาะระบบงาน (application systems) คือเพื่อให้มั่นใจว่า:

- ข้อมูลที่นำเข้าระบบงานทั้งหมด แม่นยำ สมบูรณ์ ได้รับอนุมัติ และถูกต้อง
- ข้อมูลทั้งหมดได้รับการประมวลผลตามที่ตั้งใจไว้

[11] ดู GTAG 14 ของ IIA เรื่อง *การตรวจสอบแอพพลิเคชันที่ผู้ใช้พัฒนาขึ้น (Auditing User-developed Applications)*

[12] ดู GTAG 8 ของ IIA เรื่อง *การตรวจสอบวิธีการควบคุมระบบงาน (Auditing Application Controls)*

- ข้อมูลที่จัดเก็บไว้ทั้งหมดมีความถูกต้องและครบถ้วน
- ผลลัพธ์ที่ได้จากระบบงาน (output) ทั้งหมด ถูกต้องและครบถ้วน
- มีการบันทึกรายการ (Record) ไว้เพื่อสามารถตามรอยกระบวนการของข้อมูลได้ ตั้งแต่การนำเข้าสู่ระบบไปจนถึงการจัดเก็บข้อมูล และไปจนกระทั่งได้รับผลลัพธ์ในขั้นสุดท้าย

การสอบทานวิธีการควบคุมระบบงานเฉพาะนั้น เดิมเป็นหน้าที่ของผู้ตรวจสอบด้าน IT ที่ต้องมีความเชี่ยวชาญเฉพาะทาง อย่างไรก็ตาม เนื่องจากวิธีการควบคุมระบบงานเฉพาะได้เข้าไปเป็นส่วนหนึ่งในวิธีการควบคุมทางธุรกิจในปัจจุบันในสัดส่วนที่สูงมาก ดังนั้น จึงเป็นประเด็นสำคัญที่ผู้ตรวจสอบภายในทุกคนควรคำนึงถึงให้มากด้วย

วิธีการควบคุมทั่วไป (generic controls) หลายประเภทที่ควรมีอยู่ในระบบงานไม่ว่าจะเป็นระบบใด

- **วิธีการควบคุมการนำเข้าข้อมูล** (Input controls): วิธีการควบคุมประเภทนี้ส่วนใหญ่ใช้เพื่อตรวจสอบความสมบูรณ์ถูกต้องของข้อมูลที่บันทึกลงในระบบงานที่รองรับกระบวนการทางธุรกิจ ไม่ว่าจะเป็นการบันทึกข้อมูลจากพนักงานโดยตรง หรือจากคู่ค้าธุรกิจในระยะไกล (Remote) หรือผ่านทางระบบงานที่เปิดใช้งานบนเว็บ การนำเข้าข้อมูลจะถูกเช็คสอบเพื่อให้มั่นใจว่าข้อมูลที่นำเข้ายังคงอยู่ภายในค่าพารามิเตอร์ตามที่กำหนดไว้
- **วิธีการควบคุมการประมวลผล** (Processing controls): วิธีการควบคุมประเภทนี้มีวิธีการในรูปแบบอัตโนมัติเพื่อให้มั่นใจว่า มีการประมวลผลที่เสร็จสมบูรณ์ ถูกต้องและได้รับอนุมัติ
- **วิธีการควบคุมการผลลัพธ์** (Output controls): วิธีการควบคุมประเภทนี้จะเกี่ยวกับสิ่งที่ได้กระทำกับข้อมูล โดยควรมีการเปรียบเทียบผลลัพธ์ที่ได้กับผลลัพธ์ที่คาดหวังและเช็คสอบผลลัพธ์กับข้อมูลที่นำเข้าด้วย
- **วิธีการควบคุมความถูกต้องสมบูรณ์** (Integrity controls): วิธีการควบคุมเหล่านี้สามารถเฝ้าติดตามข้อมูลที่อยู่ในกระบวนการและ/หรือที่ถูกจัดเก็บไว้ เพื่อให้แน่ใจว่าข้อมูลยังคงมีความคงเส้นคงวาและถูกต้อง
- **ร่องรอยทางการบริหาร** (Management trail): วิธีการควบคุมประวัติรายการประมวลผล (ซึ่งมักเรียกว่า ร่องรอยสำหรับการตรวจสอบ -- audit trail) จะช่วยให้ฝ่ายบริหารสามารถติดตามรายการจากแหล่งกำเนิดข้อมูล (source) ไปจนถึงผลลัพธ์ขั้นสุดท้าย และเพื่อติดตามย้อนกลับโดยเริ่มจากผลลัพธ์เพื่อระบุรายการและเหตุการณ์ตามที่ได้มีบันทึกไว้ ควรมีวิธีการควบคุมเหล่านี้ให้เพียงพอที่จะเฝ้าติดตามตรวจสอบประสิทธิผลของวิธีการควบคุมทั้งหมด และระบุจุดที่เกิดข้อผิดพลาดได้ใกล้เคียงกับแหล่งที่เกิดข้อผิดพลาดเหล่านั้นให้ได้มากที่สุด

6.4 การรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยของข้อมูล[13] เป็นส่วนที่สำคัญส่วนหนึ่งของวิธีการควบคุมด้าน IT การรักษาความ

[13] ดู GTAG 15 ของ IIA เรื่อง *การกำกับดูแลความปลอดภัยของสารสนเทศ (Information Security Governance)*

ปลอดภัยของข้อมูลนำไปปรับใช้ได้กับทั้งโครงสร้างพื้นฐานและข้อมูล และถือเป็นรากฐานสำหรับความน่าเชื่อถือของวิธีการควบคุมทาง IT วิธีอื่นๆ เป็นส่วนใหญ่ แต่จะมีข้อยกเว้นก็คือ วิธีการควบคุมที่เกี่ยวข้องกับด้านการเงินของ IT (เช่น การวัดผลตอบแทนจากการลงทุน และวิธีการควบคุมงบประมาณ) และวิธีการควบคุมการบริหารโครงการบางประเภท องค์ประกอบซึ่งเป็นที่ยอมรับโดยทั่วไปของการรักษาความปลอดภัยของข้อมูล ได้แก่:

- **การรักษาความลับ** (Confidentiality): ข้อมูลที่เป็นความลับจะเปิดเผยได้ก็ต่อเมื่อมีความเหมาะสมเท่านั้น และข้อมูลจะต้องได้รับการป้องกันไม่ให้มีการเปิดเผยหรือมีการดักจับข้อมูลโดยไม่ได้รับอนุญาต การรักษาความลับรวมถึงข้อพิจารณาในเรื่องข้อมูลส่วนบุคคลด้วย
- **ความสมบูรณ์ครบถ้วน** (Integrity): ความสมบูรณ์ครบถ้วนของข้อมูลหมายถึง สภาวะของข้อมูลที่ยังคงสภาพที่ถูกต้องและสมบูรณ์อยู่ ซึ่งรวมถึง ความน่าเชื่อถือของการประมวลผลและการรายงานทางการเงิน
- **ความพร้อมใช้งาน** (Availability): ข้อมูลสารสนเทศจะต้องพร้อมใช้งานสำหรับธุรกิจ ลูกค้าและคู่ค้าพันธมิตร ไม่ว่าจะเป็นเมื่อใด ที่ไหน และในลักษณะที่ต้องการ ความพร้อมใช้งานได้แก่ ความสามารถในการกู้คืนสถานการณ์ที่เกิดความสูญเสีย การหยุดชะงัก หรือกรณีที่ข้อมูลและบริการด้าน IT เกิดความเสียหาย รวมทั้งจากภัยพิบัติที่สำคัญซึ่งเกิดขึ้น ณ สถานที่จัดเก็บข้อมูล

6.5 กรอบการควบคุมด้าน IT

เป็นเวลานานกว่า 50 ปีมาแล้วที่องค์กรต่างๆ ได้นำ IT มาใช้งาน วิธีการควบคุมไม่ได้เป็นเงื่อนไขตั้งต้นที่ใช้ได้เสมอไปกับอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่เกิดขึ้นใหม่ การพัฒนาและการนำวิธีการควบคุมมาปรับใช้ค่อนข้างล้าหลังไม่ทันต่อการรับรู้ถึงความเสี่ยงใหม่ๆ ที่เกิดขึ้นในระบบต่างๆ และภัยคุกคามที่บุกรุกผ่านทางช่องโหว่ดังกล่าวด้วย ยิ่งไปกว่านั้น วิธีการควบคุมด้าน IT ไม่ได้ถูกกำหนดไว้ในมาตรฐานซึ่งเป็นที่ยอมรับในระดับสากลที่สามารถนำไปปรับใช้กับระบบได้ทั้งหมดหรือกับองค์กรซึ่งใช้งานระบบเหล่านั้น

กรอบการควบคุมก็คือ วิธีที่มีโครงสร้างชัดเจนในการจัดประเภท และการระบุวิธีการควบคุมเพื่อทำให้สภาพแวดล้อมด้าน IT มีความมั่นคงปลอดภัยอย่างเพียงพอ กรอบฯ เป็นได้ทั้งแบบทางการหรือไม่เป็นทางการ แนวทางที่เป็นทางการจะสามารถตอบสนองต่อข้อกำหนดทางกฎหมายหรือข้อบังคับที่ใช้บังคับองค์กรต่างๆ ได้อย่างทันท่วงที กระบวนการในการเลือกหรือสร้างกรอบการควบคุมนั้น ควรมีทุกฝ่ายเข้ามาเกี่ยวข้อง ซึ่งรวมถึงเจ้าของกระบวนการทางธุรกิจ และฝ่ายที่รับผิดชอบในการนำวิธีการควบคุมไปลงมือปฏิบัติ กรอบการควบคุมควรถูกนำไปปรับใช้และมีการใช้งานจริงในทุกส่วนงานทั่วทั้งองค์กร

7. ความสามารถและทักษะที่จำเป็นในงานตรวจสอบด้าน IT

ตามที่ IPPF ได้กำหนดไว้ ผู้ตรวจสอบภายในได้รับการคาดหวังว่า จะปฏิบัติตามและเชิดชูหลักการสี่ประการ อันได้แก่ ความมีคุณธรรม ความเที่ยงธรรม การรักษาความลับ และความสามารถ สำหรับหลักการในเรื่องความสามารถ (Competency) นั้นได้กำหนดให้ผู้ตรวจสอบภายในให้บริการได้เฉพาะงานที่พวกเขามีความรู้ ทักษะ และประสบการณ์ที่จำเป็นต่องานนั้นๆ เท่านั้น นอกจากนี้ ในมาตรฐานคุณสมบัติ มาตรฐานที่ 1210: เรื่อง ความเชี่ยวชาญ ระบุไว้ว่า “ผู้ตรวจสอบภายในต้องมีความรู้ ทักษะ และความสามารถอื่นๆ ที่จำเป็นต่อการปฏิบัติหน้าที่ที่ได้รับมอบหมาย หน่วยงานตรวจสอบภายในโดยรวมแล้วต้องมีหรือได้รับ ความรู้ ทักษะ และความสามารถ อื่นๆ ที่จำเป็นต้องนำมาใช้ในการปฏิบัติงานตามหน้าที่ของหน่วยงานนั้น”

CAE ต้องได้รับคำแนะนำและความช่วยเหลือที่ดีพอ หากผู้ตรวจสอบภายในขาดความรู้ ทักษะ และความสามารถอื่นที่จำเป็นในการปฏิบัติงานตรวจสอบไม่ว่าจะเป็นบางส่วนหรือทั้งหมดของงาน ทาง IIA ได้จัดทำกรอบความสามารถแบบบูรณาการ (Integrated Competency Framework) เพื่อช่วยระบุความสามารถที่จำเป็นต้องมีในหน่วยงานตรวจสอบภายใน แนวทางนี้ได้เชื่อมโยงความเสี่ยงทางธุรกิจซึ่งได้ระบุมาแล้วกับกระบวนการด้าน IT ที่เกี่ยวข้อง ดังนั้น CAE ควรทราบว่าต้องใช้ทักษะและความสามารถด้าน IT ประเภทใดและระดับใดในการตรวจสอบประสิทธิผลของวิธีการควบคุมที่ใช้ควบคุมความเสี่ยงทางธุรกิจที่ได้ระบุมาแล้ว ตารางต่อไปนี้ แสดงบางตัวอย่างในการทำแผนที่ความเสี่ยงทางธุรกิจเทียบกับวิธีการควบคุมด้าน IT ที่จำเป็นรวมทั้งทักษะ/ความสามารถที่จำเป็นในการปฏิบัติงานตรวจสอบ

ความเสี่ยงทางธุรกิจ	วิธีการควบคุมด้าน IT	ทักษะและความสามารถด้าน IT
การจัดการความปลอดภัยของสารสนเทศ	วิธีการควบคุมความปลอดภัยทางตรรกะที่ดีพอ	การบริหารความปลอดภัย ได้แก่ วิธีการควบคุมการเข้าถึงระบบบนเครือข่าย ระบบปฏิบัติการ ฐานข้อมูล และระดับระบบงาน/แอพพลิเคชัน
การหยุดชะงักทางธุรกิจที่สำคัญ	เชื่อมั่นได้ในความพร้อมใช้งาน (Availability) ของระบบงานที่รองรับกระบวนการทางธุรกิจ (business applications) ที่สำคัญ	การวางแผนต่อเนื่องทางธุรกิจและแผนฉุกเฉินการกู้คืนเมื่อเกิดเหตุภัยพิบัติสำหรับอุปกรณ์ด้าน IT (รวมถึงโครงสร้างพื้นฐานของเครือข่าย ระบบปฏิบัติการ ฐานข้อมูลและระบบงาน/แอพพลิเคชัน)
รายงานทางการเงินและรายงานทางการบริหารไม่ถูกต้องและไม่สมบูรณ์	ทำให้การรักษาความลับและความพร้อมใช้งานข้อมูลมีความปลอดภัย	วิธีการควบคุมระบบงานเฉพาะ วิธีการควบคุมการเปลี่ยนแปลงแก้ไข และวิธีการควบคุมวงจรชีวิตการพัฒนาระบบ (SDLC)

หากในหน่วยงานตรวจสอบภายใน ไม่มีบุคลากรใดที่มีทักษะและความสามารถด้าน IT ที่จำเป็นแล้ว CAE อาจต้องหาผู้ให้บริการภายนอกเพื่อมาช่วยสนับสนุนหรือมาเสริมกำลังให้พนักงานภายในหน่วยงาน เช่น การจัดจ้างหน่วยงานภายนอกมาทำงานตรวจสอบ (Out-sourcing) หรือการจัดจ้างหน่วยงานภายนอกมาร่วมตรวจสอบกับผู้ตรวจสอบภายใน (Co-sourcing)[14]

[14] ดู คำแนะนำวิธีปฏิบัติ (Practice Advisory) ของ IIA ที่ 1210.A1-1: เรื่อง การใช้บริการจากภายนอกเพื่อสนับสนุนหรือเสริมกำลังหน่วยงานตรวจสอบภายใน (Obtaining External Service Providers to Support or Complement the Internal Audit Activity)

8. การใช้กรอบการควบคุม

แต่ละองค์กรควรพิจารณากรอบการควบคุมต่างๆ ที่มีอยู่เพื่อตัดสินว่า กรอบใดหรือส่วนใดของกรอบที่ใกล้เคียงกับความต้องการมากที่สุด ทุกคนในองค์กรที่มีภาระหน้าที่โดยตรงต่อวิธีการควบคุมเหล่านั้นควรมีส่วนเกี่ยวข้องกับกระบวนการในการเลือกหรือสร้างกรอบการควบคุม หน่วยงานตรวจสอบภายในจะประเมินความเพียงพอของกรอบงานและใช้กรอบเป็นบริบทในการวางแผนและการปฏิบัติงานตรวจสอบภายใน

CAE จำเป็นต้องมีความรู้โดยรวมเกี่ยวกับประเด็นความเสี่ยงด้าน IT เพื่อประเมินประสิทธิผลและความเหมาะสมของวิธีการควบคุมด้าน IT CAE จะวางแผนการตรวจสอบและจัดสรรทรัพยากรโดยอาศัยประเด็นความเสี่ยงด้าน IT ที่ควรให้ความสนใจโดยดูระดับความเสี่ยงตามธรรมชาติ (inherent risks) การวิเคราะห์และประเมินความเสี่ยงไม่สามารถมองว่าเป็นกระบวนการที่ทำแค่เพียงครั้งเดียวโดยเฉพาะอย่างยิ่งเมื่อประยุกต์ใช้กับทางด้าน IT เทคโนโลยีที่เปลี่ยนแปลงอยู่ตลอดเวลาและรวดเร็วย่อมมาพร้อมกับความเสี่ยงและภัยคุกคาม การจัดหมวดหมู่วิธีการควบคุมด้าน IT ตามตำแหน่งในทางองค์กร วัตถุประสงค์และการทำหน้าที่ภายในขององค์กรนั้น จะมีประโยชน์ในการประเมินคุณค่าและความเพียงพอซึ่งรวมทั้งความเพียงพอของระบบควบคุมภายในด้วย ความรู้เกี่ยวกับวิธีการควบคุมด้าน IT ที่มีอยู่มากมายหลากหลาย แรงผลักดันให้เกิดวิธีการควบคุม และบทบาทและภาระหน้าที่ในองค์กร จะช่วยในการวิเคราะห์และประเมินความเสี่ยงให้ครอบคลุมในภาพรวมได้ ในการประเมินประสิทธิผลของวิธีการควบคุมนั้น จะมีประโยชน์หากจะทำความเข้าใจว่า วิธีการควบคุมเหล่านั้นเป็นสิ่งที่ต้องทำ (Mandatory) หรือเลือกทำได้ตามความสมัครใจ (voluntary) ต้องใช้การตัดสินใจ (discretionary) หรือไม่ต้องใช้การตัดสินใจ (nondiscretionary) ทำด้วยมือ (Manual) หรือทำโดยอัตโนมัติ (automated) หรือเป็นการควบคุมขั้นต้น (primary) หรือรองลงมา (secondary) และขึ้นอยู่กับการฝ่าฝืนกฎของผู้บริหาร (Management override) หรือไม่

ท้ายที่สุด การประเมินวิธีการควบคุมด้าน IT จะเกี่ยวข้องกับการเลือกวิธีการควบคุมที่สำคัญเพื่อนำมาทำการทดสอบ ประเมินผลการทดสอบ และการตัดสินว่าหลักฐานได้บ่งชี้ว่ามีจุดอ่อนในวิธีการควบคุมที่สำคัญนั้นหรือไม่ รายการตรวจสอบ (checklist) ที่มีอยู่ในภาคผนวกจะสามารถช่วยให้เชื่อมั่นได้ว่า ได้มีการพิจารณาประเด็นต่างๆ ที่เกี่ยวข้องแล้วในขณะที่ทำการวางแผนและกำกับการประเมินวิธีการควบคุมด้าน IT โดยตรวจสอบภายใน ปัจจุบันมีกรอบและแนวทางมากมายที่จะสามารถช่วย CAE หรือผู้บริหารอื่นในการกำหนดความต้องการ (requirement) ที่เกี่ยวกับการควบคุมด้าน IT ได้ อย่างไรก็ตาม องค์กรควรจะสำรวจกรอบการควบคุมต่างๆ ให้มากพอเพื่อตัดสินใจว่า กรอบฯใดจะเหมาะสมกับความต้องการและวัฒนธรรมขององค์กรของตนมากที่สุด

8.1 เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (Computer Aided Audit Techniques - CAATs) และการใช้วิธีการวิเคราะห์ข้อมูล

CAE ควรพิจารณาการใช้เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วยมาใช้งาน (โดยเฉพาะอย่างยิ่งเครื่องมือวิเคราะห์ข้อมูล -- data analysis tools) เพื่อให้ได้มุมมองเกี่ยวกับความเสี่ยงด้าน IT ใกล้เคียงกับเวลาที่เกิดขึ้นจริงมากขึ้น และเพื่อระบุความผิดปกติที่อาจเกิดขึ้นได้ ในสภาพแวดล้อมที่องค์กรและหน่วยงานตรวจสอบภายในจำเป็นต้องทำงานให้มากขึ้นโดยใช้ทรัพยากรให้น้อยลง การวิเคราะห์ข้อมูลจะเปิดโอกาสให้ CAE ใช้ประโยชน์จากข้อมูลที่มีอยู่ทั่วทั้งองค์กรและระบุบริเวณที่มีความสำคัญซึ่งต้องมุ่งเน้นในการประเมินความเสี่ยงหรือในกิจกรรมการตรวจสอบ การวิเคราะห์ข้อมูลยังสามารถช่วยให้แนวทางแก่ CAE ในการประเมินประสิทธิผลในการทำงานของวิธีการควบคุมภายในได้อย่างสม่ำเสมอ และสอบทานตัวชี้วัดของความเสี่ยงที่เกิดขึ้นใหม่ได้ เครื่องมือวิเคราะห์ข้อมูลที่มีอยู่จะช่วยเพิ่มฟังก์ชันการทำงานในการตรวจสอบข้อมูลและประมวลผลข้อมูลจำนวนมากได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม มีความท้าทายที่สำคัญหลายอย่าง ได้แก่ CAE จำเป็นต้องแสวงหาทักษะทางเทคนิค การเข้าถึงเครื่องมือวิเคราะห์ข้อมูล การใช้ประโยชน์จากเครื่องมือในการรายงาน/การดึงข้อมูล การเข้าถึงแหล่งข้อมูล และสร้างกลยุทธ์ที่มุ่งเน้นความเสี่ยงที่สูงที่สุดขององค์กร

การตรวจสอบอย่างต่อเนื่องนั้นมีความคล้ายคลึงกับการเฝ้าติดตามอย่างต่อเนื่อง เนื่องจากข้อมูลจะถูกวิเคราะห์หรือประเมินตลอดเวลาโดยผู้ตรวจสอบภายใน การเฝ้าติดตามอย่างต่อเนื่องเป็นภาระหน้าที่ของผู้บริหาร ตรวจสอบภายในอาจต้องทดสอบ สอบทาน หรือใช้ประโยชน์จากการเฝ้าติดตามอย่างต่อเนื่องของผู้บริหาร สำหรับข้อมูลเพิ่มเติมสามารถดูได้ที่ GTAG 3 เรื่อง *การตรวจสอบอย่างต่อเนื่อง: นัยของการให้ความเชื่อมั่น การเฝ้าติดตามประเมินผล และการประเมินความเสี่ยง (Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment)*

8.2 การใช้การประเมินความเสี่ยงโดยอัตโนมัติ

CAE อาจพบว่า ในการสร้างความน่าเชื่อถือให้กับการประเมินความเสี่ยงนั้น ต้องมีการให้คะแนนที่เป็นตัวเลขหรือการประเมินความเสี่ยงโดยละเอียด มีเครื่องมือบางประเภทที่สามารถนำมาใช้เพื่อทำให้กระบวนการวิเคราะห์ความเสี่ยงเป็นไปโดยอัตโนมัติ เครื่องมือเหล่านี้จะทำการให้คะแนนความเสี่ยง อธิบายระดับความรุนแรงของผลกระทบ และจัดลำดับโอกาสเกิด ท่ามกลางปัจจัยอื่นๆ การประเมินความเสี่ยงโดยอัตโนมัติจะช่วยให้สามารถเปรียบเทียบและจัดลำดับความเสี่ยงได้ การเก็บรวบรวมปัจจัยความเสี่ยงตามธรรมชาติ (Inherent risk) และความเสี่ยงที่คงเหลืออยู่ (Residual risk) จะช่วยให้ CAE สามารถให้ข้อมูลสรุป อันได้แก่ แผนที่ความเสี่ยง (Heat map) หรือรายการข้อมูลความเสี่ยง (Risk profile) ที่ตรง

กับข้อมูลความเสี่ยงขององค์กร การทำให้การบริหารหน่วยงานตรวจสอบภายในเป็นไปโดยอัตโนมัติเป็นเรื่องสำคัญที่หน่วยงานตรวจสอบภายในสามารถสร้างขึ้นเองได้ และประเด็นหนึ่งที่มีโอกาสเป็นไปได้คือทำให้กระบวนการประเมินความเสี่ยงเป็นไปโดยอัตโนมัติ (เช่น การใช้เครื่องมือการลงคะแนนเพื่อให้ฝ่ายบริหารบันทึกการให้ค่าคะแนนความเสี่ยง)

การตรวจสอบมีส่วนสนับสนุนต่อการควบคุมด้าน IT อย่างไร

ในช่วงสองสามทศวรรษที่ผ่านมา เป็นช่วงเวลาที่มีภาพสะท้อนให้เห็นว่า ฝ่ายบริหารและผู้ตรวจสอบเห็นพ้องต้องกันว่าผู้ตรวจสอบสามารถเพิ่มคุณค่าให้กับองค์กรได้ จากการใช้ความเชี่ยวชาญด้านการควบคุมเพื่อพัฒนากระบวนการที่จะให้ความมั่นใจว่า วิธีการควบคุมที่เหมาะสมได้ถูกติดตั้งเข้าไปในระบบใหม่แล้ว ซึ่งจะดีกว่าไปเพิ่มวิธีการควบคุมเข้าไปหลังจากที่ได้ตรวจพบข้อบกพร่อง กิจกรรมเหล่านี้เกิดขึ้นพร้อมๆ กับการพัฒนาการควบคุมและการประเมินความเสี่ยงด้วยตนเอง ซึ่งเป็นกระแสหลักในโลกการตรวจสอบ การให้คำปรึกษาโดยหน่วยงานตรวจสอบ และการตรวจสอบโดยอาศัยพื้นฐานความเสี่ยงกลายเป็นสิ่งที่แพร่หลายไปทั่ว ในปี 2533 และในปีถัดๆ มา ก็เริ่มมีการให้ความสำคัญกับการจัดการด้านความปลอดภัยของข้อมูลมากขึ้นเนื่องจากมีการโจมตีทางไซเบอร์เพิ่มขึ้นทั้งในจำนวนและความรุนแรง เหตุการณ์เหล่านี้ได้ช่วยกำหนดบทบาทสำคัญให้กับผู้ตรวจสอบด้าน IT รวมถึง การตระหนักรู้ของโลกธุรกิจ ถึงความสำคัญของการจัดการความปลอดภัยของข้อมูลอย่างมีประสิทธิผล

8.3 การรายงานการควบคุมด้าน IT

CAE จำเป็นต้องสื่อสารกับผู้มีส่วนได้ส่วนเสียหลักขององค์กร (เช่น คณะกรรมการตรวจสอบผู้บริหารระดับสูงหน่วยงานกำกับดูแลผู้สอบบัญชีภายนอกหรือ CIO) เกี่ยวกับผลของการปฏิบัติงานการให้ความเชื่อมั่น CAE สามารถใช้รูปแบบรายงานที่มีอยู่มากมาย และแนวทางต่างๆ ก็มีได้ตั้งแต่การปรับปรุงข้อมูลให้ทันสมัย ไปจนถึงการวัดผลเชิงดุลยภาพ (Balance scorecard) หรือไปจนถึงการนำเสนอข้อมูลให้กับผู้บริหารแบบส่วนตัว

แนวทางหนึ่งคือ เริ่มต้นด้วยนำเสนอข้อมูลที่เป็นปัจจุบัน (Update) อย่างง่ายๆ เกี่ยวกับการประเมินเริ่มแรก CAE ควรกำหนดระดับความเสี่ยงตามธรรมชาติที่มีอยู่ในกระบวนการ IT ที่สำคัญ ตัวอย่างเช่น CAE สามารถกำหนดระดับความเสี่ยงตามธรรมชาติและสอบทานร่วมกับ CIO หรือผู้มีส่วนได้เสียด้าน IT ที่สำคัญ ในส่วนที่เกี่ยวกับกระบวนการพัฒนาระบบ (SDLC) การปฏิบัติงาน (IT operation) การวางแผนต่อเนื่องทางธุรกิจ (BCP) เครือข่าย (Network) การรักษาความปลอดภัยของข้อมูลสารสนเทศ (Information security) และการบริหารการเปลี่ยนแปลง (Change management) บ่อยครั้งที่ความเสี่ยงตามธรรมชาตินั้นขึ้นอยู่กับกลยุทธ์และโครงสร้างหน่วยงานด้าน IT หน่วยงานด้าน IT ในบางองค์กรอาจใช้

วิธีการจัดจ้างผู้ให้บริการภายนอกองค์กร หรือดำเนินการในรูปแบบที่มีการควบคุมจากส่วนกลาง หรือแบบกระจายศูนย์ ในการนำเสนอรายงานข้อมูลปัจจุบันอาจรายงานถึง สิ่งที่ตรวจพบ หรือประเด็นที่สำคัญ ความคืบหน้าในการดำเนินการตามข้อเสนอแนะจากการตรวจสอบอาจเป็นส่วนหนึ่งในการรายงานข้อมูลด้าน IT ที่เป็นปัจจุบันด้วย

อีกวิธีหนึ่งคือ การรายงานในรูปแบบการวัดผลเชิงดุลยภาพ (Balance Scorecard) สิ่งนี้อาจสอดคล้องกับการรายงานเกี่ยวกับกลยุทธ์หรือการดำเนินงานของ CIO ซึ่งใช้วิธีการวัดผลเชิงดุลยภาพในงานด้าน IT ทางสถาบัน Balanced Scorecard ได้จัดให้มีแม่แบบรายงาน (Template) ในรูปแบบหนึ่งที่สามารถดูกิจกรรมด้าน IT จากมุมมอง 4 ด้าน ได้แก่ ด้านการเงิน (Financial) ด้านกระบวนการทางธุรกิจภายในองค์กร (Internal business process) ด้านการเรียนรู้และการเติบโต (Learning and growing) และด้านลูกค้า(Customer) เมื่อ CAE มีการรายงานเกี่ยวกับ IT โดยเป็นส่วนหนึ่งของรายงานการตรวจสอบตามปกติต่อคณะกรรมการ คณะกรรมการตรวจสอบ หรือผู้บริหารนั้น ในรายงานโดยทั่วๆ ไปมักจะบรรจุประเด็นปัญหาที่เกี่ยวข้องกับเหตุการณ์ละเมิดความปลอดภัยของข้อมูล ข้อยกเว้นที่เกิดในกระบวนการจัดการการเปลี่ยนแปลง (change management exceptions) สถานะของการพัฒนาโครงการ รายงานปัญหาในการปฏิบัติงาน การใช้จ่ายเงินลงทุน หรือตัวชี้วัดอื่นๆ ที่วัดความเสี่ยงและการควบคุมด้าน IT ที่สำคัญ แนวทางดังกล่าวควรเป็นแนวทางที่ครอบคลุมและบูรณาการความเสี่ยงและวิธีการควบคุมทั้งหมด (มุมมองจากทางธุรกิจไปจนถึง IT) ให้อยู่ในเพียงรูปแบบเดียว

บางครั้ง CAE อาจจำเป็นต้องรายงานต่อผู้บริหารเป็นการส่วนตัว การรายงานแบบนี้โดยทั่วไปจะต้องครอบคลุมประเด็นที่มีนัยสำคัญ ตัวอย่างเช่น ประเด็นที่ทีมตรวจสอบภายในไม่สามารถเข้าถึงข้อมูลที่ร้องขอได้หลังจากได้พยายามหลายครั้ง บุคลากรหลักด้าน IT ไม่ยอมเปิดเผยข้อมูลที่ครบถ้วนหรือทั้งหมดให้ทราบ หรือผู้บริหารด้าน IT ให้ผู้ตรวจสอบภายในออกจากการประชุมของคณะกรรมการอำนวยการหลัก (key steering committee) กล่าวคือคือ ไม่มีที่นั่งในการประชุม ปัญหาที่ท้าทายอีกประการหนึ่งสำหรับการรายงานแบบส่วนตัวอาจจะเป็นเรื่องการขาดการสนับสนุนจาก CIO ซึ่ง “ทัศนคติหรือท่าทีของผู้บริหาร (Tone at the Top)” ที่สื่อออกมานี้อาจทำให้เกิดวัฒนธรรมองค์กรที่ไม่ถูกต้อง และเป็นการปิดกั้นการดำเนินการเพื่อแก้ไขความเสี่ยงหรือปล่อยให้วิธีการควบคุมด้าน IT ที่สำคัญไม่ได้รับการเฝ้าระวัง

9. บทสรุป

การประเมินความเสี่ยงและวิธีการควบคุมด้าน IT แสดงให้ (สำหรับ CAE ใหม่และที่มีประสบการณ์) เห็นได้ว่าเป็นขั้นตอนหนึ่งในขั้นตอนแรกๆ ในการทำความเข้าใจเกี่ยวกับสภาพแวดล้อมด้าน IT และความสำคัญของ IT ต่อการบริหารความเสี่ยงในทางธุรกิจ การอ่านและนำ GTAG ฉบับนี้ไปปรับใช้จะช่วยเป็นแนวทางให้กับ CAE และผู้ตรวจสอบภายในอื่นได้เข้าใจถึงความเสี่ยงด้าน IT และการควบคุมที่นำมาใช้ CAE จะสามารถให้แนวทางเกี่ยวกับความเสี่ยงด้าน IT และการควบคุมได้ในระหว่างการประชุมหารือร่วมกับผู้มีส่วนได้ส่วนเสียที่สำคัญขององค์กร

ขั้นตอนต่อไปคือ การประเมินและทำความเข้าใจในการกำกับดูแลด้าน IT จะช่วยให้ CAE สามารถระบุได้ว่าใครเป็นผู้รับผิดชอบอะไรในด้าน IT บ้าง และวิธีการที่ผู้นำด้าน IT ร่วมกับผู้นำในทางธุรกิจนำกลยุทธ์ด้าน IT ไปปฏิบัติเป็นอย่างไร ในบริบทนี้ CAE ควรระลึกไว้เสมอว่า มาตรฐานของ IIA ที่ 2110.A2 เรียกร้องให้มี “การประเมินการกำกับดูแลด้าน IT” ในส่วนที่ 3 (หัวข้อ ผู้มีส่วนได้เสียภายในและภาระหน้าที่ด้าน IT) ของแนวปฏิบัติฉบับนี้มีบทสรุปที่เป็นประโยชน์เกี่ยวกับบทบาทและภาระหน้าที่ที่สำคัญ

เมื่อ CAE ประเมินการกำกับดูแลด้าน IT แล้ว การวิเคราะห์ความเสี่ยงด้าน IT คือขั้นตอนต่อไปที่ต้องเกิดขึ้นในกระบวนการ น่าเสียดายที่ยังไม่มีรายการตรวจสอบ (Checklist) ที่เป็นสากลเพื่อใช้ในการวิเคราะห์ความเสี่ยงด้าน IT แต่ละองค์กร (ซึ่งขับเคลื่อนโดยข้อกำหนดเกี่ยวกับลักษณะและขนาดของธุรกิจ) จะดำเนินงานภายใต้โครงสร้างพื้นฐานด้านเทคโนโลยี ระบบงาน/แอพพลิเคชัน การเชื่อมต่อผ่านระบบงาน (Interface) ที่แตกต่างกัน และใช้นโยบายเพื่อให้บรรลุกลยุทธ์ด้าน IT ที่แตกต่าง CAE ควรทำการวิเคราะห์ความเสี่ยงโดยใช้กระบวนวิธีที่มีโครงสร้างชัดเจน ตัวอย่างเช่น ตามที่ระบุไว้ในมาตรฐานการบริหารความเสี่ยงของ ISO (ISO 31000) และใช้ประโยชน์จากความรู้จากผู้นำหลักด้าน IT (เช่น CIO และผู้บริหารอื่นๆ) ในบริบทของความเสี่ยงโดยรวมขององค์กร การพัฒนาความสัมพันธ์ที่สร้างความสามัคคีและความไว้วางใจจะช่วยให้เกิดความโปร่งใสในการวิเคราะห์ความเสี่ยงตามธรรมชาติและความเสี่ยงที่คงเหลืออยู่

มีต้นแบบ (model) และแนวทาง มากมายในการวิเคราะห์ความเสี่ยงด้าน IT และ CAE ควรเลือกต้นแบบที่เหมาะสมกับองค์กรของตน รายละเอียดเกี่ยวกับบทบาทและหน้าที่งานด้าน IT ที่สำคัญหลายอย่างจะมีอยู่ในส่วนที่ 6 (หัวข้อ การทำความเข้าใจในความสำคัญของวิธีการควบคุมด้าน IT) ของเอกสารฉบับนี้ CAE ให้คะแนนความเสี่ยงด้าน IT และกำหนดสิ่งที่จะต้องรวมอยู่ในแผนการตรวจสอบโดยรวม

CAE ต้องระบุและประเมินทักษะทางเทคนิคและความสามารถที่จำเป็นที่ต้องใช้ตามแผนตรวจสอบโดยรวม CAE อาจพิจารณากระบวนวิธีที่มีใน GAIT ของ IIA ในการใช้แนวทางจากบนลงล่าง (Top-down) โดยอิงตามพื้นฐานความเสี่ยง อย่างไรก็ตาม ความเชี่ยวชาญเฉพาะบางอย่าง อาจไม่คุ้มค่าที่

จะต้องจัดจ้างบุคลากรให้เป็นพนักงานประจำเสมอไป CAE สามารถเลือกใช้วิธีการพัฒนาบุคลากรภายในให้มีทักษะทางเทคนิคเฉพาะ ว่าจ้างเฉพาะทักษะที่จำเป็น หรือจัดจ้างผู้ให้บริการจากภายนอกแทน ส่วนการร่วมทำงานกับผู้ให้บริการภายนอกองค์กร (Co-sourcing) จะช่วยเพิ่มโอกาสให้กับองค์กรทุกขนาดในการใช้ผู้เชี่ยวชาญจากภายนอกและได้รับทราบมุมมองเกี่ยวกับแนวโน้มด้าน IT รวมทั้งผลกระทบจากความเสี่ยงที่เป็นปัจจุบัน

การประเมินความเสี่ยงและวิธีการควบคุมด้าน IT นั้น ต้องมีการวางแผนอย่างรอบคอบและเป็นขั้นเป็นตอน CAE ควรวางแผนโดยกำหนดเวลาและทรัพยากรที่มีทักษะที่เพียงพอเหมาะสม เพื่อปฏิบัติงานอย่างมืออาชีพและสร้างกระบวนการที่ยั่งยืนสำหรับการวิเคราะห์ที่เป็นไปอย่างต่อเนื่อง

10. ผู้เขียนและผู้สอบทาน

ผู้เขียน:

Steve Mar, CFSA, CISA

Rune Johannessen, CIA, CCSA, CISA

Stephen Coates, CIA, CGAP, CISA

KarineWegrzynowicz, CIA

Thomas Andreesen, CISA, CRISC

ผู้สอบทาน:

Steve Hunt, CIA

Steve Jameson, CIA, CCSA, CFSA, CRMA

ผู้สนับสนุนข้อมูลอื่น ๆ:

Dragon Tai, CIA, CCSA

11. ภาคผนวก: รายการตรวจสอบกรอบการควบคุมด้าน IT

CAE สามารถใช้รายการตรวจสอบ (Checklist) นี้เพื่อตรวจสอบกรอบการควบคุมด้าน IT อย่างละเอียด เพื่อที่จะมั่นใจได้ว่าองค์กรได้กำหนดองค์ประกอบของการควบคุมไว้ครบถ้วนทั้งหมดแล้ว รายการตรวจสอบนี้ยังช่วยให้ CAE เข้าใจถึงประเด็นต่างๆ และวางแผนการตรวจสอบภายในให้ครอบคลุมในทุกพื้นที่ที่ต้องมีการควบคุม

การดำเนินการ	คำถาม
1. ระบุสภาพแวดล้อมการควบคุมด้าน IT ขององค์กร ซึ่งรวมถึง ก. คุณค่า/ค่านิยมองค์กร (Values) ข. ปรัชญาองค์กร (Philosophy) ค. สไตล์การบริหารจัดการ (Management style) ง. ความตระหนักด้าน IT (Awareness) จ. การจัดองค์กร (Organization) ฉ. นโยบาย (Policies) ช. มาตรฐาน (Standards)	■ มีนโยบายและมาตรฐานขององค์กรที่อธิบายถึงความจำเป็นที่ต้องมีวิธีการควบคุมด้าน IT อยู่หรือไม่?
2. ระบุกฎหมายและระเบียบที่เกี่ยวข้องที่มีผลกระทบต่อการควบคุมด้าน IT เช่น: ก. การกำกับดูแลกิจการ (Governance) ข. การรายงาน (Reporting) ค. การปกป้องข้อมูล (Data protection) ง. การปฏิบัติตามข้อกำหนดกฎหมาย (Compliance)	■ มีกฎหมายอะไรบ้างที่ส่งผลต่อความจำเป็นที่ต้องมีวิธีการควบคุมด้าน IT? ■ ผู้บริหารได้ดำเนินการตามขั้นตอนเพื่อให้แน่ใจในการปฏิบัติตามกฎหมาย ข้อบังคับเหล่านี้?
3. ระบุบทบาทและภาระหน้าที่สำหรับการควบคุมทาง IT ที่เกี่ยวข้องกับ: **ก. คณะกรรมการ** 1) คณะกรรมการตรวจสอบ (Audit Committee) 2) คณะกรรมการความเสี่ยง (Risk Committee) 3) คณะกรรมการกำกับดูแล (Governance committee) 4) คณะกรรมการด้านการเงิน (Finance Committee) **ข. ฝ่ายบริหาร** 1) ผู้บริหารสูงสุด(CEO) 2) CFO และ Controller 3) CIO 4) หัวหน้าเจ้าหน้าที่รักษาความปลอดภัย (CSO) 5) CISO 6) CRO **ค. ผู้ตรวจสอบ** ก. ผู้ตรวจสอบภายใน ข. ผู้ตรวจสอบบัญชี	■ มีการจัดสรรภาระหน้าที่ที่เกี่ยวข้องกับวิธีการควบคุมด้าน IT ทั้งหมด ไปให้แต่ละบุคคลหรือไม่ ■ การจัดสรรภาระหน้าที่เข้ากันได้กับความจำเป็นที่ต้องปรับใช้วิธีการแบ่งแยกหน้าที่งานหรือไม่ ■ มีการจัดทำเอกสารภาระหน้าที่ด้าน ITหรือไม่? ■ มีการสื่อสารถึงภาระหน้าที่ในการควบคุมด้าน IT ให้ทั้งองค์กรได้รับทราบหรือไม่? ■ พนักงานแต่ละคนเข้าใจในภาระหน้าที่ของตนอย่างชัดเจนเกี่ยวกับวิธีการควบคุมด้าน IT หรือไม่? ■ มีหลักฐานอะไรบ้างที่ระบุให้เห็นการปฏิบัติหน้าที่ของแต่ละบุคคล? ■ ตรวจสอบภายในได้จัดจ้างผู้เชี่ยวชาญด้านตรวจสอบ IT มาเพื่อระบุถึงประเด็นปัญหาเกี่ยวกับการควบคุมด้าน IT หรือไม่?

การดำเนินการ	คำถาม
4. ระบุกระบวนการประเมินความเสี่ยง ซึ่งในกระบวนการมีการระบุถึงสิ่งเหล่านี้หรือไม่ ก. ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) ข. ช่วงเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ (Risk tolerance) ค. การวิเคราะห์ความเสี่ยง (Risk analysis) ง. การจับคู่ความเสี่ยงกับวิธีการควบคุมด้าน IT (Matching risks to IT controls)	■ มีการกำหนดระดับความเสี่ยงที่ยอมรับได้และช่วงเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ขององค์กรอย่างไร? ■ ระดับความเสี่ยงที่ยอมรับได้และช่วงเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้ขององค์กรได้รับการอนุมัติโดยระดับคณะกรรมการหรือไม่? ■ ทุกคนที่มีหน้าที่ในการควบคุมด้าน IT มีความเข้าใจอย่างชัดเจนในระดับความเสี่ยงที่ยอมรับได้และช่วงเบี่ยงเบนไปจากระดับความเสี่ยงที่ยอมรับได้หรือไม่? ■ องค์กรใช้กระบวนการวิเคราะห์ความเสี่ยงที่เป็นทางการหรือไม่? ■ ทุกคนที่มีหน้าที่ในการควบคุมทาง IT เข้าใจในกระบวนการหรือไม่? ■ เป็นกระบวนการที่นำไปปฏิบัติใช้อย่างสม่ำเสมอทั่วทั้งองค์กรหรือไม่?
5. ระบุกระบวนการเฝ้าติดตามประเมินผลทั้งหมด ซึ่งรวมถึง: ก. การกำกับดูแล (Regulatory) ข. งานปกติภายในองค์กร (Normal In-house) ค. นอกเหนือจากการตรวจสอบภายใน (Other than internal auditing)	■ มีกระบวนการอะไรบ้างในการเฝ้าติดตามการปฏิบัติตามกฎหมายที่เกี่ยวข้องทั้งหมด รวมทั้งนโยบายและมาตรฐานปฏิบัติงานภายในองค์กรด้วย ■ ฝ่ายบริหารมีกระบวนการเฝ้าติดตามประเมินผลที่นอกเหนือจากการตรวจสอบภายในหรือไม่?
6. ระบุข้อมูลสารสนเทศและกลไกการสื่อสารเช่น: ก. ข้อมูลเกี่ยวกับการควบคุม (Control information) ข. การควบคุมที่ล้มเหลว (Control failures)	■ มีตัวชี้วัดอะไรบ้างที่เสนอต่อคณะกรรมการองค์กร คณะอนุกรรมการ และฝ่ายบริหาร ที่เกี่ยวกับความปลอดภัยด้าน IT? ■ มีรายงานเพิ่มเติมอะไรบ้างที่จัดทำให้แก่คณะกรรมการและผู้บริหารเป็นประจำ? ■ ผู้บริหารได้รับรายงานอยู่เสมอๆ เมื่อการควบคุมทาง IT เกิดความล้มเหลวขึ้น หรือไม่ ■ คณะกรรมการและคณะอนุกรรมการ ได้รับรายงานในทำนองเดียวกันเมื่อการควบคุมด้าน ITเกิดความล้มเหลว หรือไม่?

เกี่ยวกับ IPPF

กรอบโครงสร้างการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) เป็นกรอบโครงสร้างแนวคิดที่จัดโครงสร้างของแนวทางต่างๆ ที่ได้รับการอนุมัติให้ประกาศใช้ จัดทำโดยสมาคมผู้ตรวจสอบภายใน แนวทาง IPPF ประกอบด้วย:

แนวทางภาคบังคับ

การปฏิบัติตามหลักการต่างๆ ที่กำหนดไว้ในแนวทางภาคบังคับเป็นสิ่งที่ต้องทำ และจำเป็นสำหรับการปฏิบัติงานวิชาชีพของการตรวจสอบภายใน แนวทางภาคบังคับได้รับการพัฒนาตามกระบวนการตรวจทานอย่างรอบคอบ (Due diligence process) ตามที่ได้กำหนดไว้ ซึ่งรวมถึงช่วงเวลาของการเปิดเผยต่อสาธารณชนเพื่อเปิดรับข้อมูลความคิดเห็นจากผู้มีส่วนได้เสีย องค์ประกอบในภาคบังคับของ IPPF มีอยู่ 3 องค์ประกอบ กล่าวคือ นิยามของการตรวจสอบภายใน, ประมวลจรรยาบรรณ และ *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (มาตรฐาน)*

องค์ประกอบ	**คำนิยาม**
นิยาม	นิยามของการตรวจสอบภายใน ระบุถึงวัตถุประสงค์ขั้นพื้นฐาน ลักษณะและขอบเขตของการตรวจสอบภายใน
ประมวลจรรยาบรรณ	ประมวลจรรยาบรรณระบุถึงหลักการและความคาดหวังซึ่งกำกับความประพฤติของบุคคลและองค์กรที่ปฏิบัติงานตรวจสอบภายใน ประมวลจรรยาบรรณได้อธิบายถึงข้อกำหนดขั้นต่ำสำหรับความประพฤติที่คาดหวังแทนที่จะระบุกิจกรรมเฉพาะอย่าง
มาตรฐานวิชาชีพสากล	*มาตรฐาน* มุ่งเน้นที่หลักการและให้กรอบสำหรับการปฏิบัติงานและการส่งเสริมการตรวจสอบภายใน *มาตรฐาน*เป็นข้อกำหนดภาคบังคับ ซึ่งประกอบด้วย: • คำแถลงถึงข้อกำหนดขั้นพื้นฐานสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน และสำหรับการประเมินประสิทธิผลของการปฏิบัติงาน ซึ่งมีการนำไปปรับใช้กันทั่วโลก ทั้งในระดับองค์กรและระดับบุคคล • บทตีความที่อธิบายคำศัพท์เฉพาะและแนวคิดต่างๆ ที่มีอยู่ในคำแถลงให้ชัดเจนขึ้น จำเป็นต้องพิจารณาทั้งคำแถลงในมาตรฐานและบทตีความเพื่อให้เกิดความเข้าใจและนำ*มาตรฐาน*ไปปรับใช้อย่างถูกต้อง *มาตรฐาน*ได้ใช้คำบางคำซึ่งได้มีการให้ความหมายไว้โดยเฉพาะอยู่ในภาคอภิธานศัพท์แล้ว

แนวทางที่แนะนำอย่างยิ่งให้นำไปใช้

แนวทางที่แนะนำอย่างยิ่งให้นำไปใช้นี้ ได้รับการรับรองจาก IIA โดยผ่านกระบวนการอนุมัติอย่างเป็นทางการ ซึ่งได้อธิบายถึงวิธีปฏิบัติสำหรับการนำเอา นิยามการตรวจสอบภายในของ IIA ประมวลจรรยาบรรณ และมาตรฐานวิชาชีพฯ ไปปรับใช้ได้อย่างมีประสิทธิผล องค์ประกอบ 3 ประการของแนวทางที่แนะนำให้นำไปใช้ของ IPPF ได้แก่ เอกสารแสดงจุดยืน (Position Papers) คำแนะนำวิธีปฏิบัติ (Practice Advisory) และแนวปฏิบัติ (Practice Guides)

องค์ประกอบ	**คำนิยาม**
เอกสารแสดงจุดยืน (Position Papers)	เอกสารแสดงความคิดเห็นเป็นเอกสารที่จะช่วยให้ผู้ที่มีความสนใจในงานตรวจสอบภายใน (ไม่ใช่แค่เฉพาะผู้ที่มีอาชีพตรวจสอบภายใน) ได้ทำความเข้าใจถึงนัยสำคัญของประเด็นการกำกับดูแล ความเสี่ยง หรือการควบคุม รวมถึงความเกี่ยวข้องที่สิ่งเหล่านั้นมีต่อบทบาทและภาระหน้าที่ของการตรวจสอบภายใน
คำแนะนำวิธีปฏิบัติ (Practice Advisory)	คำแนะนำวิธีปฏิบัติ จะช่วยผู้ตรวจสอบภายในในการนำเอา นิยามของการตรวจสอบภายใน ประมวลจรรยาบรรณ และมาตรฐาน ไปประยุกต์ใช้ได้ รวมทั้งช่วยส่งเสริมและเผยแพร่วิธีปฏิบัติที่ดีได้ ซึ่งคำแนะนำเหล่านี้จะอธิบายถึง แนวทาง กระบวนวิธี และสิ่งที่ควรคำนึงในการปฏิบัติงานตรวจสอบภายใน แต่ไม่ใช่กระบวนการหรือวิธีการปฏิบัติงานโดยละเอียด คำแนะนำฯ ได้รวมถึงวิธีปฏิบัติที่เกี่ยวข้องกับ: ระหว่างประเทศ ในประเทศ หรือประเด็นเฉพาะบางอุตสาหกรรม; เฉพาะบางประเภทของงานตรวจสอบ; และประเด็นทางกฎหมายหรือข้อบังคับต่างๆ
แนวปฏิบัติ (Practice Guides)	แนวปฏิบัติ ได้ให้แนวทางในการปฏิบัติงานตรวจสอบภายในโดยละเอียด ซึ่งประกอบด้วย กระบวนการและวิธีปฏิบัติงานโดยละเอียด เป็นต้นว่า เครื่องมือและเทคนิค โปรแกรม และแนวทางปฏิบัติทีละขั้นตอน รวมไปถึงตัวอย่างของสิ่งที่ส่งมอบ (deliverables)

GTAG ฉบับนี้เป็นแนวปฏิบัติภายใต้ IPPF

สำหรับเอกสารแนวทางอื่นๆ ที่ได้รับอนุมัติแล้ว สามารถเยี่ยมชมได้ที่ www.theiia.org/guidance-standards

GTAG®

เกี่ยวกับสมาคม

ก่อตั้งขึ้นในปีพ.ศ. 2484 สมาคมผู้ตรวจสอบภายใน (IIA) เป็นสมาคมทางด้านวิ ชาชีพตรวจสอบภายในระดับสากล สำนักงานใหญ่ของสมาคมตั้งอยู่ที่ Altamonte Springs มลรัฐฟลอริดา สหรัฐอเมริกา IIA เป็นกระบอกเสียงให้แก่ผู้ปฏิบัติวิชาชีพตรวจสอบภายในทั่วโลก เป็นหน่วยงานที่ได้รับการยอมรับว่าเป็นผู้นำในการเป็นผู้ให้การสนับสนุน และผู้ให้ความรู้หลักเกี่ยวกับวิชาชีพตรวจสอบภายใน

เกี่ยวกับแนวปฏิบัติ (Practice Guides)

แนวปฏิบัติให้แนวทางสำหรับการดำเนินกิจกรรมตรวจสอบภายในโดยละเอียด ซึ่งรวมถึงรายละเอียดของกระบวนการและวิธีการต่างๆ เช่น เครื่องมือและเทคนิค โปรแกรม และขั้นตอนทีละขั้น รวมถึงตัวอย่างผลงานที่ส่งมอบ แนวปฏิบัติเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) และเป็นส่วนหนึ่งของที่แนะนำเป็นอย่างยิ่ง การปฏิบัติตามแนวปฏิบัตินี้จึงไม่มีการบังคับ แต่ก็แนะนำเป็นอย่างยิ่งให้ใช้ แนวปฏิบัติได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวทางการตรวจสอบเทคโนโลยีระดับโลก (Global Technologies Audit Guide หรือ GTAG) เป็นแนวปฏิบัติ (Practice Guide) ประเภทหนึ่ง ซึ่งเขียนขึ้นโดยใช้ภาษาทางธุรกิจที่ตรงไปตรงมา เพื่อกล่าวถึงประเด็นปัญหาต่างๆ เกี่ยวกับการบริหารจัดการ การควบคุม หรือความมั่นคงปลอดภัย ในทางเทคโนโลยีสารสนเทศในเวลาที่เหมาะสม

สำหรับเอกสารแนะนำแนวทางอื่นๆ ที่จัดทำและรับรองโดยสมาคมผู้ตรวจสอบภายใน ท่านสามารถเยี่ยมชมเว็บไซต์ของเราได้ที่ www.globaliia.org/standards-guidance

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

The Institute of Internal Auditors

www.globaliia.org