องค์ประกอบการตรวจสอบระบบสารสนเทศที่เกี่ยวข้องกับการประเมินความเสี่ยงเทคโนโลยีสารสนเทศ

INFORMATION SYSTEM AUDIT COMPONENTS RELATED TO INFORMATION TECHNOLOGY RISK ASSESSMENT

ศิริเดช คำสุพรหม*
Siridech Kumsuprom*

* คณบดี วิทยาลัยบริหารธุรกิจนวัตกรรมและการบัญชี มหาวิทยาลัยธุรกิจบัณฑิตย์
* Dean, College of Innovative Business and Accountancy, Dhurakij Pundit University
* Email: siridech.kum@dpu.ac.th

บทคัดย่อ

ปัจจุบันองค์การธุรกิจได้ปรับเปลี่ยนกระบวนการสร้างความได้เปรียบทางการแข่งขันจากเดิมโดยการประมวลผลข้อมูลและการรายงานข้อมูลผ่านสื่อสิ่งพิมพ์ มาเป็นการสร้างความได้เปรียบทางการแข่งขันสมัยใหม่โดยการผลิตเนื้อหาผ่านทางดิจิทัล ยิ่งไปกว่านั้น องค์การได้นำเทคโนโลยีสมัยใหม่ เช่น เทคโนโลยีความจริงเสมือน (Virtual Reality) มาสร้างมูลค่าให้แก่องค์การและความได้เปรียบทางการแข่งขัน และเพื่อช่วยเสริมศักยภาพการนำเสนอข้อมูลขององค์การธุรกิจ จากที่กล่าวข้างต้นอาจจะกล่าวได้ว่าข้อมูลและสารสนเทศของธุรกิจที่ถูกนำมาใช้ผ่านสังคมดิจิทัล (Digital Society) และเปิดเผยข้อมูลต่อสาธารณชน จากสถานการณ์ดังกล่าวผลกระทบเชิงลบหรือความเสี่ยงอาจจะเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ ดังนั้น องค์การควรให้ความสำคัญกับองค์ประกอบการตรวจสอบระบบสารสนเทศที่ประกอบด้วยบุคลากรด้านการตรวจสอบระบบสารสนเทศ คุณสมบัติของผู้ตรวจสอบระบบสารสนเทศภายในองค์การ และบริบทองค์การที่เกี่ยวเนื่องกับกระบวนการการประเมินความเสี่ยงผ่านผู้ตรวจสอบระบบสารสนเทศ ซึ่งองค์ประกอบเหล่านี้จะช่วยให้ประกันได้ว่าการประเมินความเสี่ยงจากผู้ตรวจสอบระบบสารสนเทศนั้นมีความถูกต้องและแม่นยำตลอดจนสามารถลดความเสี่ยงทางเทคโนโลยีได้

คำสำคัญ: บริบทองค์การ คุณลักษณะของระบบ ผู้ตรวจสอบระบบสารสนเทศ การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ

Abstract

Currently, organizations have changed competitive advantage approach from traditional, data processing and data reporting through publishing media, to modern approaches through digital media. Moreover, organizations have adopted modern technology such as virtual reality to create organization value and competitive advantage and to enhance the organizational reporting approach. It can be seen organizational data and information are disclosed through digital society, are also revealed to the public. In this circumstance, negative impact or risk could arise from using modern technology. As a result, organizations should pay more attention on the components of information system auditor (IS auditor) consisting of the IS auditor itself, characteristics of IS auditor and organizational context through IT risk assessment process done by IS auditor. This can be ensured that IT risk assessment process has not only been done by IS auditor correctly and accurately but also reducing IT risk.

Keywords: Organizational Context, System Characteristics, IS Auditor, IT Risk Assessment

บทนำ

ปัจจุบันองค์การธุรกิจปรับเปลี่ยนกระบวนการสร้างความได้เปรียบทางการแข่งขันจากเดิมที่เป็นผลิตข้อมูลและการรายงานผ่านสื่อสิ่งพิมพ์ต่างๆ มาเป็นการผลิตเนื้อหาผ่านทางดิจิทัลเพิ่มมากขึ้น ไม่ว่าจะเป็นการนำเอาเทคโนโลยีความจริงเสมือน (Virtual Reality)[1] มาสร้างความได้เปรียบทางการแข่งขัน หรือแม้แต่นำเอาเทคโนโลยีเสมือนจริง เข้ามาช่วยเพิ่มศักยภาพการนำเสนอข้อมูลขององค์การธุรกิจมากขึ้น อาจจะกล่าวได้ว่าข้อมูลและสารสนเทศของธุรกิจที่ถูกนำมาใช้ผ่านสังคมดิจิทัล (Digital Society) และเพื่อเพิ่มการเปิดเผยข้อมูลต่อสาธารณชน จากสถานการณ์ที่กล่าวมาทำให้องค์การธุรกิจพึ่งพิงหรือให้ความสำคัญกับการใช้เทคโนโลยีสารสนเทศในองค์การ ดังนั้น การพึ่งพิงเทคโนโลยีสารสนเทศดังกล่าว อาจส่งผลเชิงลบกับธุรกิจได้เช่นกัน เช่น ความเสี่ยงที่อาจจะเกิดขึ้นจากผู้ไม่ประสงค์ดี นำเอาข้อมูลขององค์การที่แพร่หลายอยู่ในหลายสื่อทางดิจิทัลขององค์การธุรกิจไปใช้ผิดวัตถุประสงค์ การกระทำการดังกล่าวอาจจะส่งผลต่อชื่อเสียงและภาพลักษณ์ขององค์การธุรกิจได้ ยิ่งไปกว่านั้นความเสี่ยงทางเทคโนโลยี ยังอาจจะรวมถึงความเสี่ยงที่เกิดขึ้นจากการเปิดเผยข้อมูลที่เป็นความลับขององค์การธุรกิจ หรือความเสี่ยงจากการขโมยข้อมูลที่สำคัญผ่านระบบเทคโนโลยีสารสนเทศ หรือแม้แต่จะเป็นความเสี่ยงทางเทคโนโลยีที่ทำให้การดำเนินธุรกิจหยุดชะงัก

เทคโนโลยีสารสนเทศในปัจจุบันช่วยอำนวยความสะดวกให้กับองค์การในการใช้ข้อมูลขนาดใหญ่ (Big Data)[2] เพื่อวิเคราะห์ข้อมูลที่เป็นประโยชน์ด้านการวางแผนและการควบคุมกระบวนการปฏิบัติงานตลอดจนกระบวนการทางธุรกิจขององค์การได้เป็นอย่างดี ขณะเดียวกันข้อมูลขนาดใหญ่ก็มีส่วนที่ทำให้ความเสี่ยงทางเทคโนโลยีเพิ่มขึ้นอีกด้วย (Ridgeway, 2018) ทั้งนี้ Ridgeway (2018) ยกตัวอย่างว่าข้อมูลขนาดใหญ่ที่เห็นผ่านรูปแบบในอินเทอร์เน็ตนั้นอาจจะไม่มีอยู่จริง ดังนั้นข้อมูลขนาดใหญ่ที่องค์การจะนำมาใช้ในการวิเคราะห์ อาจจะไม่ได้สะท้อนความเป็นจริงและอาจจะไม่ได้ช่วยแก้ไขปัญหาที่องค์การกำลังเผชิญอยู่ นอกจากนั้น ข้อมูลขนาดใหญ่ดังกล่าวอาจจะมีข้อมูลบางส่วนที่เป็นเท็จและอาจจะส่งผลก่อให้เกิดความเสี่ยงต่อชื่อเสียงและความเสียหายต่อภาพลักษณ์ขององค์การได้อีกด้วย ดังนั้น นวัตกรรมทางเทคโนโลยีที่กำลังมีบทบาทอย่างมาก ไม่ว่าจะเป็นการใช้เทคโนโลยีอัตโนมัติ หรือปัญญาประดิษฐ์ หรือแม้แต่เทคโนโลยีการเงินก็อาจจะก่อให้เกิดความเสี่ยงจากการนำเทคโนโลยีสมัยใหม่นั้นเข้ามาใช้ในองค์การ ดังนั้น บทความนี้จึงมุ่งเน้นในการศึกษาและให้ความสำคัญขององค์ประกอบการตรวจสอบระบบสารสนเทศที่เกี่ยวเนื่องกับการประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศ เพื่อช่วยให้องค์การทราบถึงองค์ประกอบของการประเมินความเสี่ยงสำหรับการตรวจสอบระบบสารสนเทศว่าองค์การควรให้ความสำคัญกับเรื่องใดเพื่อลดระดับความรุนแรงของความเสี่ยงทางเทคโนโลยีลง และป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับองค์การในอนาคต บทความนี้จะสะท้อนให้เห็นถึงแนวทางให้องค์การได้วางมาตรการและแนวทางปฏิบัติที่จะลดความเสี่ยงอันอาจจะเกิดขึ้นจากการใช้นวัตกรรมเทคโนโลยีสารสนเทศในปัจจุบัน

---

[1] Burdea and Coiffet (2003) ได้ให้คำนิยามว่า เทคโนโลยีความจริงเสมือนนั้น มีส่วนช่วยให้ผู้ที่สนใจได้รับการตอบสนองผ่านการเปลี่ยนแปลงทางจอภาพ โดยผ่านการปฏิสัมพันธ์จากการควบคุมของผู้ที่สนใจเอง ทั้งนี้การประมวลผลของภาพดังกล่าวจะทำให้เกิดการสร้างภาพจำลองเสมือนจริงที่ใกล้เคียงกับชีวิตจริงมากที่สุด ดังนั้น เทคโนโลยีความจริงเสมือนนี้จึงได้รับความนิยมในการนำมาใช้สำหรับการเสริมสร้างความได้เปรียบทางการแข่งขันขององค์การธุรกิจในปัจจุบัน

[2] Maheshwari (2017) ได้อธิบายถึงข้อมูลขนาดใหญ่ (Big Data) อยู่ 2 ระดับ คือ 1. ข้อมูลระดับพื้นฐานซึ่งเป็นการเก็บรวบรวมและการวิเคราะห์ข้อมูลทั่วไปที่เป็นประโยชน์กับองค์การซึ่งเป็นข้อมูลที่กระจายอยู่ทั่วไปในสังคมดิจิทัล และ 2. ข้อมูลระดับองค์การซึ่งเป็นการเก็บรวบรวม วิเคราะห์และจัดทำภายในองค์กรเพื่อช่วยในการตัดสินใจให้ดียิ่งขึ้น

วรรณกรรมที่เกี่ยวข้อง

การประเมินความเสี่ยงในปัจจุบันจำเป็นต้องใช้แนวทางในการปฏิบัติให้สอดคล้องกับกรอบการตรวจสอบทางเทคโนโลยีสารสนเทศ (ISACA, 2016) ซึ่งกรอบแนวคิดดังกล่าวได้รับการพัฒนาจาก (Public Company Accounting Oversight Board: PCAOB), (Institute of Internal Auditors: IIA), (American Institute of Certified Public Accountants: AICPA) และ (Information Systems Audit and Control Association: ISACA) เพื่อเป็นการประกันว่า กระบวนการของการควบคุมทางเทคโนโลยีได้ปฏิบัติอย่างรัดกุมและช่วยลดความเสี่ยงที่อาจจะเกิดขึ้นทางเทคโนโลยี ทั้งนี้ กรอบการตรวจสอบทางเทคโนโลยีประกอบด้วย 1. บริบทขององค์การที่เกี่ยวข้องกับลักษณะของธุรกิจ ลักษณะหน้าที่ความรับผิดชอบของพนักงานในองค์การ 2. ลักษณะของระบบการทำงานผ่านเทคโนโลยีขององค์การ 3. ประสบการณ์ของผู้ตรวจสอบระบบสารสนเทศ และ 4. การพัฒนาทักษะและการสร้างความเข้าใจทางการตรวจสอบเทคโนโลยีสารสนเทศผ่านการอบรมต่างๆ (ISACA, 2016; Kamil, 2013)

Hermanson and Rittenberg (2003) ได้เพิ่มเติมว่าการตรวจสอบเทคโนโลยีสารสนเทศเพื่อควบคุมความเสี่ยงที่อาจจะเกิดขึ้นนั้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศส่วนใหญ่ต้องให้ความสำคัญในด้าน 1. การป้องกันทรัพย์สินทางเทคโนโลยีสารสนเทศ 2. ระบบการประมวลผลข้อมูลของโปรแกรมสำเร็จรูปและความครบถ้วนของข้อมูล 3. ข้อมูลที่เป็นส่วนตัวและระบบความปลอดภัย ซึ่งทั้ง 3 เรื่องดังกล่าวเป็นเรื่องที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศให้ความสำคัญในการป้องกันความเสี่ยงและการควบคุมทางเทคโนโลยีสารสนเทศ สำหรับประเด็นที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศให้ความสำคัญในการตรวจสอบและการประเมินความเสี่ยงในระดับรองลงมาได้แก่ การบำรุงรักษาระบบสารสนเทศและการเปลี่ยนแปลงระบบตลอดจนระบบการประมวลผลข้อมูลที่ต่อเนื่องและแผนดำเนินงานกู้คืนระบบหรือแผนการทำงานทางเทคโนโลยีอย่างต่อเนื่อง เรื่องที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศให้ความสำคัญในการตรวจสอบน้อยที่สุด จะเกี่ยวข้องกับกระบวนการใช้ระบบงาน ระบบปฏิบัติการทางเทคโนโลยีสารสนเทศ และการพัฒนาระบบและการได้มาซึ่งระบบการทำงานทางเทคโนโลยี

ดังนั้น บทความนี้ทำการวิเคราะห์ถึงตัวแปรจากกรอบการตรวจสอบทางเทคโนโลยีสารสนเทศและแนวทางการตรวจสอบเทคโนโลยีสารสนเทศเพื่อกำหนดองค์ประกอบของการตรวจสอบระบบสารสนเทศที่เกี่ยวเนื่องกับการประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศ สำหรับช่วยให้องค์การยุคดิจิทัลในประเทศไทยสามารถนำมาใช้ในการกำหนดแนวทางปฏิบัติเกี่ยวกับการตรวจสอบระบบสารสนเทศสำหรับองค์การเพื่อจะช่วยลดความเสี่ยงที่อาจจะเกิดขึ้นกับองค์การในอนาคต

บริบทองค์การ

คุณภาพของการตรวจสอบในปัจจุบันให้ความสำคัญกับการประเมินความเสี่ยงเป็นฐาน (Risk Based Approach) ดังนั้น การควบคุมความเสี่ยงเทคโนโลยีสารสนเทศจึงจำเป็นต้องมีการกำหนดโครงสร้างของการประเมินความเสี่ยงให้สอดคล้องกับขนาดขององค์การ และจำนวนของผู้ตรวจสอบระบบสารสนเทศขององค์การ (Kamil, 2013) ยิ่งไปกว่านั้น Nuijtena, Keil, Pijla and Commandeur (2018) ได้กล่าวว่า ผู้สอบตรวจสอบระบบสารสนเทศในองค์การมีความจำเป็นอย่างยิ่งเพราะเป็นผู้ที่เข้าใจระบบสารสนเทศภายในองค์การ และมีบทบาทสำคัญในการสังเกตุความผิดปกติของกระบวนการทำงานทางเทคโนโลยีสารสนเทศ ประกอบกับเป็นผู้กำกับและติดตามความเสี่ยงที่อาจจะเกิดขึ้นทางเทคโนโลยีสารสนเทศ (Kanellou and Spathis, 2011)

นอกจากนี้ องค์การที่ประสบผลสำเร็จในการจัดการความเสี่ยงและการประเมินความเสี่ยงทางเทคโนโลยีส่วนใหญ่ให้ความสำคัญกับการกำหนดนโยบาย และระเบียบวิธีการปฏิบัติในองค์การ เนื่องจากนโยบายถือเป็นส่วนหนึ่งที่สะท้อนการสนับสนุนของผู้บริหารภายในองค์การ และยังส่งผลทำให้องค์การกำหนดแผนงานที่ชัดเจน แนวทางปฏิบัติเมื่อเกิดเหตุการณ์เชิงลบที่ส่งผลกระทบต่อองค์การ พร้อมทั้งในแผนงานดังกล่าวจะมีการระบุหน่วยงานเพื่อเป็นผู้ที่มีความรับผิดชอบโดยตรงกับเหตุการณ์หรือสถานการณ์ที่อาจจะก่อให้เกิดความเสี่ยงนั้นอีกด้วย (Filho, Hashimoto, Pedro, Souza, and De and Paulo, 2011; Shamala, Ahmad, Zolait, and Sahib, 2015)

การสนับสนุนของฝ่ายบริหารขององค์การ ถือเป็นอีกหนึ่งความสำคัญในการประเมินความเสี่ยงทางเทคโนโลยี การสนับสนุนดังกล่าวสะท้อนให้เห็นถึงทัศนคติหรือมุมมองของผู้บริหาร ที่มีต่อการเปลี่ยนแปลงทางเทคโนโลยี จากงานวิจัยของ Rhee, Ryu and Kim (2012) พบว่า พฤติกรรมของมนุษย์และการตั้งสมมติฐานกับการประเมินความเสี่ยงนั้น ถึงมุมมองในการมองโลก ไม่ว่าจะเป็นการมองโลกในแง่ดีหรือในแง่ร้าย สามารถที่จะทำให้การประเมินความเสี่ยงเกิดการคลาดเคลื่อนหรือผิดพลาดได้ ดังนั้นทัศนคติของผู้บริหารองค์การจึงมีส่วนสำคัญอย่างยิ่งที่ส่งผลกระทบโดยตรงต่อการประเมินความเสี่ยงขององค์การ และส่งผลทำให้การประเมินความเสี่ยงนั้นมีโอกาสเป็นไปได้ทั้งต่ำหรือสูงเกินไป (Fenz, Heurix, Neubauer, and Pechstein, 2014)

ปัจจัยที่สำคัญอีกประการหนึ่งของการประเมินความเสี่ยง คือการรายงานผลการประเมินความเสี่ยงตามความรับผิดชอบในแต่ละระดับของการบริหารงาน จากงานวิจัยกรณีศึกษาของสมาคมมืออาชีพด้านบัญชีเพื่อการบริหาร (Chartered Institute of Management Accountants: CIMA) โดย Palermo (2011) ได้กล่าวว่า ระบบการรายงานผลประสิทธิภาพของกระบวนการประเมินความเสี่ยง เป็นอีกหนึ่งปัจจัยที่สำคัญ เพราะระดับการรายงานของแต่ละระดับจะมีความรับผิดชอบที่แตกต่างกัน และจะส่งผลทำให้การจัดการความเสี่ยงนั้นชัดเจนมากยิ่งขึ้นในแต่ละระดับของการรายงานผลการประเมินประสิทธิภาพของการจัดการความเสี่ยง

นอกจากจากที่กล่าวมาแล้วข้างต้นเกี่ยวกับบริบทขององค์การแล้ว อีกประเด็นที่สำคัญและสามารถส่งผลกระทบต่อการประเมินความเสี่ยงทางเทคโนโลยี คือคุณลักษณะของระบบที่ใช้ในองค์การ เนื่องจากว่าถ้าองค์การใช้ระบบการทำงานที่ซับซ้อนมากๆ ก็จะส่งผลต่อการประเมินความเสี่ยงที่อาจจะขาดความน่าเชื่อถือได้ ทั้งนี้คุณลักษณะของระบบที่ใช้ในองค์การจะได้กล่าวถึงในลำดับถัดไป

คุณลักษณะของระบบ

คุณลักษณะของระบบสารสนเทศในองค์การนั้นมีความสำคัญอย่างยิ่ง เนื่องจากความซับซ้อนของกระบวนการของระบบบัญชีและระบบตรวจสอบนั้นจะวิวัฒนาการตามระบบที่นำมาใช้ในองค์การ รูปแบบของกระบวนการของระบบบัญชีจะอยู่ในรูปแบบอิเล็กทรอนิกส์เพิ่มมากขึ้น เพราะกระบวนการของระบบบัญชีในปัจจุบันไม่ว่าจะเป็นสร้างข้อมูลหรือสารสนเทศทางการบัญชี การส่งผ่านข้อมูลหรือสารสนเทศทางการบัญชี การประมวลผลข้อมูลหรือสารสนเทศทางการบัญชี การป้องกันข้อมูลหรือสารสนเทศทางการบัญชี หรือการประเมินข้อมูลหรือสารสนเทศทางการบัญชีนั้น ตลอดจนการตรวจสอบรายงานทางการเงินก็จะอยู่ในรูปแบบอิเล็กทรอนิกส์เพิ่มมากขึ้น (Kanellou and Spathis, 2011) ดังนั้น ความซับซ้อนของระบบสารสนเทศส่งผลโดยตรงต่อการประเมินความเสี่ยงของผู้ตรวจสอบระบบสารสนเทศ เพื่อก่อให้เกิดประโยชน์ในการให้ข้อมูลที่สำคัญ และป้องปรามข้อผิดพลาดที่อาจจะขึ้นต่อองค์การได้

การเปลี่ยนแปลงของระบบสารสนเทศในปัจจุบันเน้นเรื่องการทำงานผ่านระบบอิเล็กทรอนิกส์ แต่อย่างไรก็ตามการทำงานของสำนักงานบัญชีในประเทศไทยส่วนใหญ่ยังคงนำข้อมูลเข้าแบบกลุ่ม กล่าวคือสำนักงานบัญชีในประเทศไทยจะรับข้อมูลทางบัญชีและการเงินจากบริษัทผู้ว่าจ้าง เพื่อมาดำเนินการนำข้อมูลเข้าไม่ว่าจะเป็นรายการทางการรับเงิน รายการทางการจ่ายเงิน หรือรายการปรับปรุงต่างๆ ดังนั้นผู้ตรวจสอบระบบสารสนเทศยังคงต้องให้ความสำคัญเกี่ยวกับการตรวจสอบระบบสารสนเทศที่มีการนำเข้าข้อมูลแบบกลุ่มซึ่งเป็นระบบการนำข้อมูลเข้าแบบดั้งเดิม (กรมพัฒนาธุรกิจการค้า, 2558) การนำเข้าข้อมูลแบบกลุ่มดังกล่าวก็จะสะท้อนถึงการประมวลผลข้อมูลแบบกลุ่มด้วยเช่นกัน ทั้งนี้ การประมวลผลแบบกลุ่มรายการอาจจะเกิดจากการประมวลผลข้อมูลเกี่ยวข้องกับเงินเดือนซึ่งจะเกิดขึ้นตามช่วงเวลาที่กำหนด ไม่ว่าจะเป็นการเบิกจ่ายเงินเดือนทุก 15 วัน หรือทุกสิ้นเดือนของแต่ละเดือน เป็นต้น (Dickmann, and Tyson, 2005; IBM Knowledge Center, 2013)

นอกจากนี้ การประมวลผลข้อมูลในปัจจุบันปรับเปลี่ยนมาเป็นระบบออนไลน์เพิ่มมากขึ้น ทำให้การนำข้อมูลเข้าก็จะเป็นแบบออนไลน์ ควบคู่กับการประมวลผลข้อมูลก็เป็นแบบออนไลน์เช่นเดียวกัน ความแตกต่างของระบบการประมวลผลนั้นส่งผลโดยตรงต่อการควบคุมระบบสารสนเทศ เนื่องจากระบบการควบคุมดังกล่าวจะครอบคลุมถึงกระบวนการนำเข้าข้อมูล กระบวนการประมวลผลที่แตกต่างกัน ดังนั้น การปรับปรุงแฟ้มข้อมูลของแต่ละส่วนก็จะมีความแตกต่างกันและส่งผลต่อแนวทางการตรวจสอบเนื้อหาสาระที่แตกต่างกันด้วย ผู้ตรวจสอบระบบสารสนเทศจึงจำเป็นต้องวางแผนการตรวจสอบระบบสารสนเทศที่แตกต่างกัน (Allinson, 2004)

จากที่ได้กล่าวข้างต้นถึงระบบสารสนเทศที่แตกต่างกันจะส่งผลต่อการวางแผนการตรวจสอบระบบสารสนเทศที่แตกต่างกันไปด้วย ดังนั้น ความเชี่ยวชาญและประสบการณ์ของผู้ตรวจสอบระบบสารสนเทศจึงมีส่วนสำคัญที่ทำให้การวางแผนการตรวจสอบมีความถูกต้องและแม่นยำมากยิ่งขึ้น ทั้งนี้ การฝึกอบรมและประสบการณ์ของผู้ตรวจสอบระบบสารสนเทศจะกล่าวถึงในลำดับถัดไป

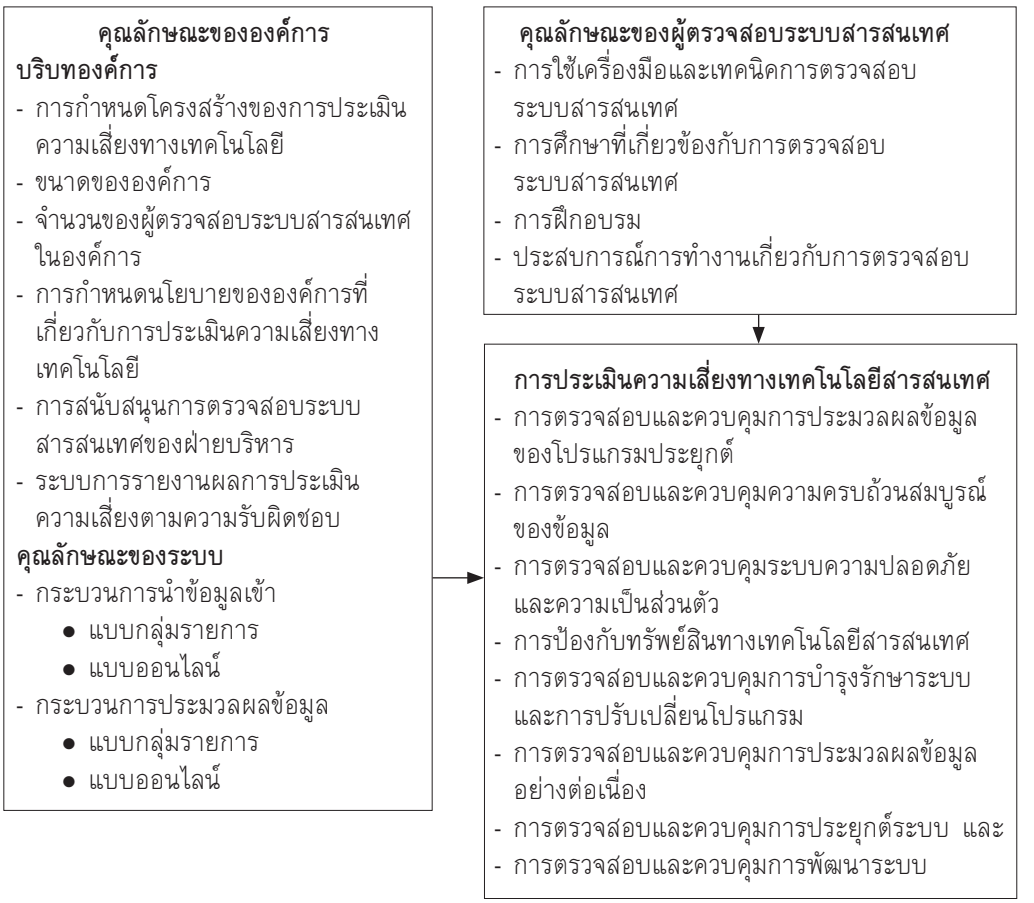
การฝึกอบรมและประสบการณ์ของผู้ตรวจสอบระบบสารสนเทศ

จากความซับซ้อนของระบบสารสนเทศภายในองค์การในปัจจุบันส่งผลทำให้ผู้ตรวจสอบระบบสารสนเทศจำเป็นต้องมีความเชี่ยวชาญ และมีประสบการณ์ไม่ว่าจะเกี่ยวข้องกับระบบสารสนเทศแต่ละประเภท ยังรวมถึงระบบการปฏิบัติการทางบัญชีและการเงิน ตลอดจนระบบการตรวจสอบระบบสารสนเทศสมัยใหม่ (Vasarhelyi and Romero, 2014) ยิ่งไปกว่านั้น Vasarhelyi and Romero (2014) และ Shaikh (2005) ได้กล่าวว่า ผู้ตรวจสอบระบบสารสนเทศจำเป็นต้องใช้เทคโนโลยีสมัยใหม่เข้ามาช่วยในการตรวจสอบรายการค้า เช่น เครื่องมือในการอ่านรายการค้าอัตโนมัติ เป็นต้น ดังนั้น การใช้เทคโนโลยีเข้ามาช่วยในการตรวจสอบจึงมีความจำเป็นที่ผู้ตรวจสอบระบบสารสนเทศต้องมีทักษะ และประสบการณ์ตรงเพื่อจะสามารถใช้เทคโนโลยีสมัยใหม่

จากงานวิจัยในอดีตของ Vasarhelyi, Lombardi and Bloch (2010) และ Vasarhelyi and Romero (2014) พบว่า ประสบการณ์ในการทำงาน การอบรมและการศึกษาของผู้ตรวจสอบระบบสารสนเทศมีความสัมพันธ์กับทักษะของการตรวจสอบเทคโนโลยีสารสนเทศ เนื่องจากผู้ตรวจสอบระบบสารสนเทศจำเป็นต้องใช้เทคโนโลยีสมัยใหม่เข้ามาช่วยให้กระบวนการตรวจสอบมีความถูกต้องและเชื่อถือได้ ดังนั้น การใช้เทคโนโลยีสมัยใหม่จึงจำเป็นต้องอาศัยผู้ตรวจสอบระบบสารสนเทศที่เข้าใจถึงระบบสารสนเทศ และความแตกต่างการรายงานผลการตรวจสอบที่มีความแตกต่างกันตามความเชี่ยวชาญ กล่าวคือผู้ตรวจสอบระบบสารสนเทศที่สำเร็จการศึกษาทางระบบสารสนเทศ หรือทางเทคโนโลยีสารสนเทศ จะรายงานผลการตรวจสอบที่แตกต่างไปจากการรายงานของผู้ตรวจสอบระบบสารสนเทศที่สำเร็จการศึกษาทางการบัญชีหรือการบริหาร เนื่องจากความเชี่ยวชาญในระบบสารสนเทศแตกต่างกันจึงส่งผลทำให้การรายงานที่เกี่ยวข้องกับระบบที่มีความซับซ้อนก็จะแตกต่างกันไปด้วย ทั้งนี้ Mahzan and Veerankutty (2011) ได้ยืนยันในทิศทางเดียวกันว่าการศึกษาของผู้ตรวจสอบระบบสารสนเทศก็มีส่วนสำคัญในการประเมินความเสี่ยงในกระบวนการของระบบสารสนเทศ ดังนั้น ผู้ตรวจสอบระบบสารสนเทศที่มีพื้นความรู้ทางการจัดการสารสนเทศ หรือแม้แต่การทำงานในหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศก็จะก่อให้เกิดประสบการณ์ที่สามารถดำเนินการตรวจสอบได้แม่นยำและถูกต้องมากยิ่งขึ้น

D'Onza, Lamboglia, and Verona (2015) อธิบายว่า ผู้ตรวจสอบระบบสารสนเทศจำเป็นต้องมีทักษะทางเทคนิคเกี่ยวกับระบบสารสนเทศและเทคโนโลยีสารสนเทศ และเข้าใจเกี่ยวกับกระบวนการในการประมวลผลทางเทคโนโลยีสารสนเทศ พร้อมทั้งมีความรู้เกี่ยวกับระบบสารสนเทศทางเทคโนโลยี เพื่อที่จะเป็นการประกันได้ว่าความเสี่ยงทางเทคโนโลยีสารสนเทศจะอยู่ในระดับที่องค์การสามารถยอมรับได้ ทั้งนี้ Shamala, et., al. (2015) กล่าวว่า การปรับปรุงกระบวนการจัดการความเสี่ยงทางเทคโนโลยีนั้น องค์การควรพัฒนาผู้ตรวจสอบระบบสารสนเทศให้มีทักษะการตรวจสอบทางเทคโนโลยีโดยผ่านการอบรมเกี่ยวกับการตรวจสอบทางเทคโนโลยีผ่านเครื่องมือทางเทคโนโลยีการตรวจสอบสมัยใหม่ ซึ่งการอบรมการพัฒนาทักษะจะดำเนินการผ่านการประชุมและการอบรมเชิงปฏิบัติการ

ยิ่งไปกว่านั้น Omoteso (2013) กล่าวเพิ่มเติมอีกว่า การตรวจสอบทางเทคโนโลยีที่มีประสิทธิภาพนั้นผู้ตรวจสอบระบบสารสนเทศจำเป็นต้องมีความเข้าใจเชิงตรรกะของกระบวนการประมวลผลสารสนเทศโดยคอมพิวเตอร์ ดังนั้น ผู้ตรวจสอบระบบสารเทศทางเทคโนโลยีจึงจำเป็นต้องมีทักษะการใช้เครื่องมือและเทคนิคทางเทคโนโลยีเพื่อพัฒนาคุณภาพการตรวจสอบสำหรับการจัดทำรายงานทางการเงินขององค์การ จากที่ได้อธิบายตัวแปรที่กล่าวมาข้างต้นจะแสดงในภาพที่ 1 ดังนี้



ภาพที่ 1 องค์ประกอบการตรวจสอบระบบสารสนเทศทางเทคโนโลยีที่เกี่ยวเนื่องกับการประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ

จากองค์ประกอบที่กล่าวมาข้างต้น องค์การควรให้ความสำคัญเพื่อช่วยเพิ่มประสิทธิภาพการตรวจสอบระบบสารสนเทศที่เกี่ยวเนื่องกับการประเมินความเสี่ยงเทคโนโลยีสารสนเทศในธุรกิจของประเทศไทย ทั้งนี้กระบวนการตรวจสอบระบบสารสนเทศจะกล่าวในลำดับถัดไป

การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ (IT Risk Assessment)

การตรวจสอบระบบสารสนเทศตามองค์ประกอบที่กล่าวข้างต้น จะส่งผลทำให้องค์กรสามารถประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ทั้งนี้ งานวิจัยของ Hermanson, Hill, and Ivancevich (2000) ได้อธิบายถึงกิจกรรมการควบคุมทางเทคโนโลยีของผู้ตรวจสอบระบบสารสนเทศที่จำเป็นต้องใช้เพื่อการประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศ ซึ่งกิจกรรมดังกล่าวจะส่งผลทำให้องค์การเชื่อมั่นได้ว่าข้อมูลหรือสารสนเทศขององค์การนั้น ได้รับการป้องกันและลดความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้เทคโนโลยีภายในองค์การ ทั้งนี้ กิจการการควบคุมความเสี่ยงดังกล่าวประกอบด้วย 1.) การตรวจสอบและควบคุมการประมวลผลข้อมูลของโปรแกรมประยุกต์ 2.) การตรวจสอบและควบคุมความครบถ้วนสมบูรณ์ของข้อมูล 3.) การตรวจสอบและควบคุมระบบความปลอดภัยและความเป็นส่วนตัว 4.) การป้องกันทรัพย์สินทางเทคโนโลยีสารสนเทศ 5.) การตรวจสอบและควบคุมการบำรุงรักษาระบบและการปรับเปลี่ยนโปรแกรม 6.) การตรวจสอบและควบคุมการประมวลผลข้อมูลอย่างต่อเนื่อง 7.) การตรวจสอบและควบคุมการประยุกต์ระบบ และ 8.) การตรวจสอบและควบคุมการพัฒนาระบบ ยิ่งไปกว่านั้น จากงานวิจัยของ Shahabuddin, Alam, and Azad, (2011) ได้อธิบายเพิ่มเติมอีกว่า กิจกรรมการควบคุมและตรวจสอบดังกล่าวจะบรรลุวัตถุประสงค์ของการตรวจสอบระบบสารสนเทศได้นั้น องค์การจำเป็นต้องมีการกำหนดเชิงนโยบายและกำหนดแนวปฏิบัติที่ชัดเจน

กิจกรรมดังกล่าวข้างต้นสอดคล้องกับเป้าหมายของการควบคุมทางเทคโนโลยีสารสนเทศ ที่ประกอบด้วย 1.) การรักษาความปลอดภัยของข้อมูลประกอบด้วยกิจกรรมการตรวจสอบและควบคุมการประมวลผลข้อมูลของโปรแกรมประยุกต์ การป้องกันทรัพย์สินทางเทคโนโลยีสารสนเทศ และการตรวจสอบและควบคุมระบบความปลอดภัยและความเป็นส่วนตัว 2.) การรักษาความครบถ้วนของข้อมูลประกอบด้วยกิจกรรมการตรวจสอบและควบคุมความครบถ้วนสมบูรณ์ของข้อมูล และ 3.) ความพร้อมของข้อมูลที่จะนำไปใช้ประโยชน์ประกอบด้วยกิจกรรมการตรวจสอบและควบคุมการบำรุงรักษาระบบและการปรับเปลี่ยนโปรแกรม การตรวจสอบและควบคุมการประมวลผลข้อมูลอย่างต่อเนื่อง การตรวจสอบและควบคุมการประยุกต์ระบบ และการตรวจสอบและควบคุมการพัฒนาระบบ (Moghaddasi, Sajjadi, and Kamkarhaghighi, 2016)

ดังนั้น การประเมินความเสี่ยงทางเทคโนโลยีสารสนเทศ จึงจำเป็นต้องได้รับการกำหนดเชิงนโยบายขององค์การเพื่อช่วยให้เกิดการดำเนินการประเมินความเสี่ยง และสอดคล้องกับกิจกรรมการควบคุมและตรวจสอบทางเทคโนโลยีสารสนเทศที่ชัดเจน

สรุป

จากการเปลี่ยนแปลงรูปแบบการดำเนินธุรกิจที่มุ่งเน้นการใช้เทคโนโลยีเข้ามาช่วยองค์การ ไม่ว่าองค์การจะนำเอาเทคโนโลยีเสมือนจริง (Virtual Reality) มาสร้างความได้เปรียบทางการแข่งขัน หรือแม้แต่นำเอาเทคโนโลยีเสมือนจริงอื่นๆ เข้ามาช่วยเพิ่มศักยภาพการนำเสนอข้อมูลขององค์การธุรกิจ ให้บรรลุวัตถุประสงค์ขององค์การและประสบผลสำเร็จในการดำเนินธุรกิจ ผู้ตรวจสอบระบบสารสนเทศจึงจำเป็นต้องคำนึงถึงองค์ประกอบของการตรวจสอบตลอดจนคุณสมบัติของผู้ตรวจสอบภายในเพื่อให้เกิดความมั่นใจได้ว่าการประเมินความเสี่ยงผ่านการตรวจสอบระบบสารสนเทศจะช่วยลดความเสี่ยงทางเทคโนโลยีที่อาจจะเกิดขึ้น ทั้งนี้ องค์การและผู้ตรวจสอบระบบสารสนเทศควรให้ความสำคัญกับการสนับสนุนการอบรมอย่างต่อเนื่องและคุณสมบัติของผู้ตรวจสอบระบบสารสนเทศเอง นอกจากนี้องค์การเองควรให้ความสำคัญกับประเภทของระบบสารสนเทศที่ประยุกต์ใช้ว่าผู้ตรวจสอบระบบสารสนเทศขององค์การมีความเชี่ยวชาญที่สามารถตรวจสอบแล้วค้นพบข้อผิดพลาด หรือข้อบ่งชี้ที่จะก่อให้เกิดความเสี่ยงทางเทคโนโลยีในอนาคตได้หรือไม่ จากองค์ประกอบต่างๆ ที่ได้กล่าวข้างต้น องค์การสามารถนำองค์ประกอบดังกล่าวใช้ในการพิจารณาเพื่อกำหนดนโยบายและแนวทางปฏิบัติการตรวจสอบระบบสารสนเทศที่เกี่ยวเนื่องกับการประเมินความเสี่ยงให้ประสบผลสำเร็จต่อไป

บรรณานุกรม

กรมพัฒนาธุรกิจการค้า. (2558). ระบบคุณภาพสำนักงานบัญชี. สืบค้นวันที่ 4 ธันวาคม 2560, จาก http://www.dbd.go.th/download/PDF_law/2.pdf

Allinson, C. (2004). The process of audit and control - a comparison of manual and electronic information systems *Policing: An International Journal of Police Strategies & Management, 27*(2), 183-205.

Burdea, C.G. and Coiffet, P. (2003). Virtual Reality Technology. (2nd edition). Hoboken, New Jersey: John Viley & Son.

D'Onza, G., Lamboglia, R., and Verona, R. (2015). Do IT audits satisfy senior manager expectations? A qualitative study based on Italian banks. *Managerial Auditing Journal, 30*(4/5), 413-434.

Maheshwari, A. (2017). *Big Data.* McGraw Hill Education.

Fenz, S., Heurix, J., Neubauer, T., and Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), 410-430.

Filho, E.L., Hashimoto, G.T., Pedro, F., Souza, J.H.P., and De and Paulo, S. (2011). The impact of corporate culture in security policies – a methodology. *The Seventh International Conference on Networking and Service* (ICNS 2011), Venice. (PP: 98-103).

Hermanson D.R, Hill, M., and Ivancevich, D.M. (2000). Information technology related activities of internal auditor, *Journal of Information Systems, 14*(1), 39-53.

Hermanson, D.R., and Rittenberg, L.E., (2003). Internal audit and organizational governance. Research Opportunities in Internal Auditing, The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

IBM Knowledge Center. (2013). *CICS Transaction Server for z/OS, Version 3.2.* Retrieved December 4, 2017, from https://www.ibm.com/support/knowledgecenter/SSGMGV_3.2.0/com.ibm. cics.ts.productoverview.doc/concepts/TransactionProcessing.html?view=embed

Information System Audit and Control Association. (ISACA). (2016). Information Systems Auditing: Tools and Techniques, Creating Audit Programs, ISACA. Retrieved December 4, 2017, from https://www.isaca.org/COBIT/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.pdf

Mahzan, N., and Veerankutty, F. (2011). IT auditing activities of public sector auditors in Malaysia. *African Journal of Business Management, 5*(5), 1551-1563.

Moghaddasi, H., Sajjadi, S., and Kamkarhaghighi, M. (2016). Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model. *The Open Medical Informatics Journal, 10,* 4-10.

Kanellou, A., and Spathis, C. (2011), Auditing in enterprise system environment: A synthesis, *Journal of Enterprise Information Management, 24*(6), 494-519.

Nuijtena, A., Keil, M., Pijla., G.V.D., and Commandeur, H. (2018). IT managers' vs. IT auditors' perceptions of risks: An actor–observer asymmetry perspective. *Information & Management, 55,* 80-93.

Omoteso, K. (2013). *Audit Effectiveness: Meeting the IT Challenge.* New York: Routledge Taylor and Francis Group.

Palermo, T. (2011). Integrating risk and performance in management reporting: Research executive summary series. *Chartered Institute of Management Accountant (CIMA), 7*(5), 1-12.

Rhee, H.S., Ryu, Y.U. and Kim, C.T. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*(2), 221-232.

Ridgeway, G. (2018). Policing in the Era of Big Data. *Annual Review of Criminology, 1,* 401-419. Retrieved December 4, 2017, from https://doi.org/10.1146/annurev-criminol062217-114209

Shahabuddin, A.M., Alam, A., and Azad, M. M. (2011). Internal Controls in Management Information System. *International Journal of Computer Information Systems, 2*(6), 58-78.

Shaikh, J.M. (2005). E-commerce impact: emerging technology – electronic auditing. *Managerial Auditing Journal, 20*(4), 408-421.

Shamala, P., Ahmad R., Zolait, A. H., and Sahib S. B. (2015). Collective information structure model for Information Security Risk Assessment (ISRA). *Journal of Systems and Information Technology, 17*(2), 193-219.

Dickmann, M., and Tyson, S. (2005). Outsourcing payroll: Beyond transaction-cost economics. Personnel Review, 34(4), 451-467.

Vasarhelyi, A. M., and Romero, S. (2014). Technology in audit engagements: A case study. *Managerial Auditing Journal, 29*(4), 350-365.

Vasarhelyi, M., Lombardi, D., and Bloch, R. (2010). The Future of Audit: A Modified Delphi Approach. SSRN Electronic Journal. 10.2139/ssrn.2488730.