

แนวทางการบริหารความเสี่ยงเชิงรุกตามกรอบ COSO ERM 2017: กลยุทธ์การควบคุมภายในเพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยีของนักบัญชี

ปนัดดา สรณะพิบูลย์^{1*}

¹สาขาวิชาการบัญชี คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏนครปฐม

*panaddas@webmail.npru.ac.th

บทคัดย่อ

บทความวิชาการนี้นำเสนอแนวทางการบริหารความเสี่ยงเชิงรุกตามกรอบ COSO ERM 2017 เพื่อเป็นกลยุทธ์สำคัญในการยกระดับการควบคุมภายในของนักบัญชี ภายใต้สถานการณ์การเปลี่ยนแปลงทางเทคโนโลยีดิจิทัลที่รวดเร็วและรุนแรง โดยเฉพาะปัญญาประดิษฐ์ การวิเคราะห์ข้อมูลขนาดใหญ่ และระบบคลาวด์ ซึ่งล้วนส่งผลกระทบต่อความเชื่อมั่นในรายงานทางการเงินและประสิทธิภาพการตรวจสอบบัญชี กรอบแนวคิด COSO ERM 2017 มุ่งเน้นถึงความสำคัญของการบูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการกำหนดกลยุทธ์และการดำเนินงานอย่างสม่ำเสมอทั้งระบบ เพื่อเปลี่ยนผ่านจากการควบคุมเชิงรับไปสู่การพยากรณ์ความเสี่ยงผ่านองค์ประกอบหลัก 5 ประการ เริ่มจากการวางรากฐานด้านวัฒนธรรมดิจิทัลและการกำหนดวัตถุประสงค์ที่สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ ตลอดจนการประยุกต์ใช้เทคโนโลยีสมัยใหม่เพื่อการรับรู้ความเสี่ยงแบบพลวัต ซึ่งช่วยให้สามารถประเมินผลกระทบและตรวจจับความผิดปกติได้ทันที

การสังเคราะห์วรรณกรรมในบทความนี้สะท้อนให้เห็นว่าปัจจัยสู่ความสำเร็จที่สำคัญประกอบด้วยความฉลาดทางวิชาชีพบัญชียุคดิจิทัล แรงสนับสนุนจากผู้บริหารระดับสูง และการสื่อสารข้อมูลที่มีคุณภาพ แนวทางเชิงรุกนี้ไม่เพียงช่วยบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์และอาชญากรรมทางเทคโนโลยี แต่ยังส่งเสริมให้นักบัญชียกระดับบทบาทสู่การเป็นหุ้นส่วนเชิงกลยุทธ์ ที่สามารถสร้างและรักษาคุณค่าขององค์กรได้อย่างยั่งยืนภายใต้สิ่งแวดล้อมทางธุรกิจที่ผันผวน

คำสำคัญ: การบริหารความเสี่ยง การควบคุมภายใน โคโซ เทคโนโลยีดิจิทัล นักบัญชี



Proactive Risk Management Guidelines Based on the COSO ERM 2017 Framework: Internal Control Strategies for Accountants in Response to Technological Transformation

Panadda Saranapiboon^{1*}

¹Department of Accounting, Faculty of Management Sciences, Nakhonpathom Rajabhat University

*panaddas@webmail.npru.ac.th

Abstract

This article academic presents a proactive risk management approach based on the COSO ERM 2017 framework, serving as a vital strategy for enhancing internal controls for accountants amidst rapid and disruptive digital transformation. Specifically, technologies such as Artificial Intelligence (AI), Big Data analytics, and Cloud computing significantly impact the reliability of financial reporting and audit efficiency. The COSO ERM 2017 framework emphasizes the integration of risk management into strategy-setting and organizational operations throughout the entire system. This facilitates a transition from reactive controls to risk forecasting through five core components, beginning with the foundation of a digital culture and the establishment of objectives aligned with risk appetite. Furthermore, the application of modern technology for dynamic risk sensing enables instantaneous impact assessment and anomaly detection.

The literature synthesis in this article reflects that key success factors include digital professional intelligence, top management support, and high-quality information communication. This proactive approach not only mitigates the impacts of cyber threats and technological crimes but also empowers accountants to elevate their roles to strategic partners, capable of sustainably creating and preserving organizational value in a volatile business environment.

Keywords: Risk Management, Internal Control, COSO, Technological, Accountants

1. บทนำ

ในยุคปัจจุบันที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทหลักในการพลิกโฉมการดำเนินงานธุรกิจอย่างรวดเร็วและรุนแรง หรือที่เรียกว่าการเปลี่ยนผ่านสู่ดิจิทัล องค์กรทุกภาคส่วนต้องเผชิญกับความท้าทายและเหตุการณ์หรือภัยคุกคามรูปแบบใหม่ที่มีความซับซ้อนภายใต้สภาวะแวดล้อมทางธุรกิจที่มีความผันผวน ส่งผลให้แบบจำลองธุรกิจแบบดั้งเดิมถูกทำลายลงอย่างรวดเร็ว [1] วิชาชีพบัญชีซึ่งทำหน้าที่เป็นกลไกหลักในการจัดทำรายงานทางการเงินและการกำกับดูแลการควบคุมภายในจึงหลีกเลี่ยงไม่ได้ที่จะต้องปรับเปลี่ยนแนวปฏิบัติงาน [2-3] การเกิดขึ้นของปัญญาประดิษฐ์ การวิเคราะห์ข้อมูลขนาดใหญ่ และระบบคลาวด์ ไม่เพียงช่วยเพิ่มประสิทธิภาพในการบันทึกรายการและการรายงานผล แต่ยังนำมาซึ่งประเด็นความเสี่ยงรูปแบบใหม่ที่ส่งผลต่อความน่าเชื่อถือของข้อมูลทางการเงินและความปลอดภัยทางไซเบอร์ของข้อมูลองค์กร [2] หากพิจารณากระบวนการควบคุมภายในและการบริหารความเสี่ยงแบบดั้งเดิม จะพบว่าส่วนใหญ่เป็นลักษณะของการตั้งรับและมุ่งเน้นการปฏิบัติตามกฎระเบียบ ซึ่งไม่เพียงพอที่จะรองรับความผันผวนของภัยคุกคามในเศรษฐกิจดิจิทัลได้อีกต่อไป [1] คณะกรรมการ COSO (Committee of Sponsoring Organizations of the Treadway Commission) จึงได้พัฒนาและปรับปรุงกรอบแนวคิดการบริหารความเสี่ยงทั่วทั้งองค์กรเป็นกรอบ COSO ERM 2017: Enterprise Risk Management-Integrating with Strategy and Performance เพื่อตอบสนองต่อการเปลี่ยนแปลงนี้ [3-4] โดยเน้นย้ำถึงความสำคัญของการบูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการกำหนดกลยุทธ์และการบริหารผลการดำเนินงาน [4-5] สำหรับนักบัญชีในประเทศไทย การทำความเข้าใจและนำกรอบแนวคิดนี้มาประยุกต์ใช้ในลักษณะเชิงรุกถือเป็นขีดความสามารถที่สำคัญที่สุดในการนำพาองค์กรผ่านพ้นวิกฤตทางเทคโนโลยี [6-7]

งานวิจัยที่ผ่านมามักแยกส่วนระหว่างกระบวนการควบคุมภายในด้านไอทีกับการบริหารความเสี่ยงระดับองค์กร ในบทความวิชาการมีวัตถุประสงค์เพื่อสังเคราะห์วรรณกรรมและข้อเสนอแนะแนวทางขับเคลื่อนเชิงนโยบายในประเทศไทยที่ครอบคลุมทุกภาคส่วน เพื่อยกระดับระบบนิเวศทางการบัญชีและบรรษัทภิบาลของประเทศให้พร้อมรับมือกับภัยคุกคามทางเทคโนโลยี รวมถึงการใช้เครื่องมือเทคโนโลยีสมัยใหม่ เพื่อเป็นแนวทางให้กับบัญชีไทยสามารถทำหน้าที่เป็นหุ้นส่วนเชิงกลยุทธ์ ที่สร้างและปกป้องคุณค่าขององค์กรได้อย่างยั่งยืน

2. การทบทวนและนำเสนอวรรณกรรม

2.1 ความหมายและความสำคัญของการบริหารความเสี่ยงและการควบคุมภายใน

การบริหารความเสี่ยงขององค์กรตามนิยามของกรอบ COSO ERM 2017 หมายถึง วัฒนธรรม ขีดความสามารถ และแนวปฏิบัติขององค์กรที่บูรณาการร่วมกับการกำหนดกลยุทธ์และการดำเนินงาน เพื่อบริหารจัดการกับความเสี่ยงในกระบวนการสร้าง รักษา และตระหนักถึงการเพิ่มคุณค่าขององค์กร [5] ขณะที่การควบคุมภายใน หมายถึง กระบวนการที่บุคลากรทุกระดับร่วมกันปฏิบัติเพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ 3 ด้าน ได้แก่ ด้านการดำเนินงานอย่างมีประสิทธิภาพ ด้านความน่าเชื่อถือของรายงานทางการเงินและรายงานที่ไม่ใช่ทางการเงิน และด้านการปฏิบัติตามกฎหมายและข้อบังคับ [8] ในบริบทของเศรษฐกิจดิจิทัล การควบคุมภายในและการบริหารความเสี่ยงเป็นกลไกสำคัญที่ช่วยลดความผิดพลาด ป้องกันการทุจริตทางเทคโนโลยี และเสริมสร้างความโปร่งใสให้แก่ผู้มีส่วนได้เสีย [9]

2.2 วิวัฒนาการของการบริหารความเสี่ยงตามกรอบ COSO ERM 2017

กรอบการบริหารความเสี่ยงขององค์กรมีการพัฒนาอย่างต่อเนื่องนับตั้งแต่ช่วงทศวรรษ 1990 โดยในปี 2004 คณะกรรมการ COSO ได้ออกกรอบแนวคิดการบริหารความเสี่ยงขององค์กรฉบับแรก (COSO ERM 2004: Integrated Framework) ที่นำเสนอแผนภาพลูกบาศก์สามมิติ (COSO Cube) ซึ่งเน้นการควบคุมภายในและการระบุความเสี่ยงตามระดับปฏิบัติการ [3] อย่างไรก็ตามเมื่อสภาพแวดล้อมทางธุรกิจมีความซับซ้อนจากเทคโนโลยีและการไหลเวียนของข้อมูลข่าวสาร เศรษฐกิจ วัฒนธรรม และเทคโนโลยีข้ามพรมแดนอย่างเสรีและรวดเร็ว COSO ได้ปรับปรุงกรอบงานครั้งสำคัญในปี 2017

ภายใต้ชื่อ COSO ERM 2017 โดยเปลี่ยนแผนภาพการนำเสนอจากลูกบาศก์เป็นเส้นริบบิ้นเกลียวคู่ (Helix Structure) สื่อถึงการผสมผสานและความผูกพันที่ขาดออกจากกันไม่ได้ระหว่างกระบวนการจัดการความเสี่ยงกับวงจรการดำเนินงานธุรกิจและการกำหนดกลยุทธ์ขององค์กรในทุกระดับ [3-4]



ภาพที่ 1 กรอบการบริหารความเสี่ยงตามแนวคิด COSO ERM 2017

ที่มา: Enterprise Risk Management—Integrating with Strategy and Performance [10]

กรอบการบริหารความเสี่ยงตามแนวคิด COSO ERM 2017 จะประกอบด้วยองค์ประกอบหลัก 5 ประการและหลักการ 20 ประการที่เชื่อมโยงและสัมพันธ์กัน [10] ซึ่งมีรายละเอียดดังนี้

องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรมองค์กร (Governance and Culture) การกำกับดูแลทำหน้าที่กำหนดทิศทางหลักขององค์กร (Sets the organization's tone) ซึ่งเป็นการเน้นย้ำถึงความสำคัญและกำหนดบทบาทหน้าที่ความรับผิดชอบในการควบคุมดูแลสำหรับการบริหารความเสี่ยงองค์กร ขณะที่วัฒนธรรมองค์กรจะเกี่ยวข้องกับคุณค่าทางจริยธรรม พฤติกรรมที่พึงประสงค์ และความเข้าใจในเรื่องความเสี่ยงภายในหน่วยงาน ประกอบด้วยหลักการที่ 1 – 5 ได้แก่ หลักการที่ 1 การกำกับดูแลความเสี่ยงของคณะกรรมการ หลักการที่ 2 การจัดตั้งโครงสร้างการดำเนินงาน หลักการที่ 3 การกำหนดวัฒนธรรมที่พึงปรารถนา หลักการที่ 4 การแสดงความมุ่งมั่นในค่านิยมหลัก และหลักการที่ 5 การดึงดูดและรักษามูลค่าที่มีความสามารถ

องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective-Setting) การบริหารความเสี่ยงองค์กร กลยุทธ์ และการกำหนดวัตถุประสงค์ จะทำงานร่วมกันในกระบวนการวางแผนเชิงกลยุทธ์ โดยมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้สอดคล้องกับกลยุทธ์ ในขณะที่วัตถุประสงค์ทางธุรกิจจะช่วยแปรกลยุทธ์ไปสู่การปฏิบัติจริง พร้อมทั้งทำหน้าที่เป็นรากฐานในการระบุ การประเมิน และการตอบสนองต่อความเสี่ยง ประกอบด้วยหลักการที่ 6 – 9 ได้แก่ หลักการที่ 6 การวิเคราะห์บริบททางธุรกิจ หลักการที่ 7 การกำหนดระดับความเสี่ยงที่ยอมรับได้ หลักการที่ 8 การประเมินกลยุทธ์ทางเลือก และหลักการที่ 9 การกำหนดวัตถุประสงค์ทางธุรกิจ

องค์ประกอบที่ 3 ผลการดำเนินงาน (Performance) ความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจจำเป็นต้องได้รับการระบุและประเมิน โดยความเสี่ยงเหล่านั้นจะถูกจัดลำดับความสำคัญตามระดับความรุนแรง ภายใต้บริบทของระดับความเสี่ยงที่ยอมรับได้ จากนั้นองค์กรจะเลือกแนวทางการตอบสนองต่อความเสี่ยง และพิจารณาภาพรวมความเสี่ยงของปริมาณความเสี่ยงทั้งหมดที่องค์กรยอมรับไว้ ซึ่งผลลัพธ์จากกระบวนการนี้จะถูกรายงานไปยังผู้มีส่วนได้เสียหลักด้านความเสี่ยง ประกอบด้วยหลักการที่ 10 – 14 ได้แก่ หลักการที่ 10 การระบุความเสี่ยง หลักการที่ 11

การประเมินความรุนแรงของความเสี่ยง หลักการที่ 12 การจัดลำดับความสำคัญของความเสี่ยง หลักการที่ 13 การกำหนดนโยบายตอบสนองต่อความเสี่ยง และหลักการที่ 14 การประเมินภาพรวมความเสี่ยง

องค์ประกอบที่ 4 การทบทวนและปรับปรุงแก้ไข (Review and Revision) โดยการทบทวนผลการดำเนินงานขององค์กร กิจกรรมจะสามารถพิจารณาได้ว่าองค์ประกอบต่าง ๆ ของการบริหารความเสี่ยงองค์กรนั้นสามารถทำหน้าที่ได้อย่างมีประสิทธิภาพเพียงใดเมื่อเวลาผ่านไป และภายใต้สภาวะที่มีการเปลี่ยนแปลงที่เป็นสาระสำคัญ ตลอดจนประเมินว่าจำเป็นต้องได้รับการปรับปรุงแก้ไขในส่วนใดบ้าง ประกอบด้วยหลักการที่ 15 – 17 ได้แก่ หลักการที่ 15 การประเมินความเปลี่ยนแปลงที่มีสาระสำคัญ หลักการที่ 16 การทบทวนความเสี่ยงและผลการปฏิบัติงาน และหลักการที่ 17 การปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่อง

องค์ประกอบที่ 5 ข้อมูล การสื่อสาร และการรายงาน (Information, Communication, and Reporting) การบริหารความเสี่ยงองค์กร จำเป็นต้องมีกระบวนการอย่างต่อเนื่องในการจัดหาและแบ่งปันข้อมูลสารสนเทศที่จำเป็น ทั้งจากแหล่งข้อมูลภายในและภายนอก ซึ่งเป็นข้อมูลที่ไหลเวียนขึ้นด้านบนลงด้านล่างและผ่านทั่วทั้งองค์กร ประกอบด้วยหลักการที่ 18 – 20 ได้แก่ หลักการที่ 18 การใช้ประโยชน์จากข้อมูลสารสนเทศและเทคโนโลยี หลักการที่ 19 การสื่อสารข้อมูลความเสี่ยงภายในองค์กร และหลักการที่ 20 การรายงานผลการบริหารความเสี่ยงและผลการดำเนินงาน

2.3 วิวัฒนาการของการควบคุมภายใน

วิวัฒนาการของการควบคุมภายในเริ่มต้นอย่างเป็นทางการเป็นรูปธรรมในปี 1992 เมื่อ COSO ตีพิมพ์กรอบการควบคุมภายในแบบบูรณาการ (Internal Control - Integrated Framework 1992) เพื่อช่วยองค์กรออกแบบและประเมินระบบการควบคุม ต่อมาในปี 2013 ได้มีการปรับปรุงอย่างเป็นทางการในกรอบ COSO 2013: Internal Control – Integrated Framework (ICIF 2013) โดยมีวัตถุประสงค์เพื่อใช้ออกแบบและประเมินความเพียงพอของระบบการควบคุมภายในให้มีประสิทธิภาพจริงในทางปฏิบัติ มีความยืดหยุ่นและรองรับสภาพแวดล้อมทางธุรกิจและเทคโนโลยีสารสนเทศที่มีความก้าวหน้ามากขึ้น โดยนำเสนอหลักการพื้นฐาน 17 ประการ ภายใต้องค์ประกอบหลัก 5 ประการ [11] ดังนี้

องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment) เป็นรากฐานสำคัญที่กำหนดทัศนคติ ค่านิยม และบรรยากาศด้านการควบคุมภายในของบุคลากรทั่วทั้งองค์กร ประกอบด้วย 5 หลักการ ได้แก่ หลักการที่ 1 องค์กรแสดงให้เห็นถึงการยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม หลักการที่ 2 คณะกรรมการแสดงออกถึงความรับผิดชอบในการกำกับดูแล และมีความเป็นอิสระจากฝ่ายบริหาร หลักการที่ 3 ฝ่ายบริหารกำหนดโครงสร้างองค์กร สายการบังคับบัญชา อำนาจหน้าที่ และความรับผิดชอบที่เหมาะสมในการบรรลุวัตถุประสงค์ หลักการที่ 4 องค์กรแสดงความมุ่งมั่นในการดึงดูด พัฒนา และรักษาบุคลากรที่มีความรู้ความสามารถ และหลักการที่ 5 องค์กรผลักดันให้บุคลากรทุกคนมีความรับผิดชอบต่อภาระหน้าที่ด้านการควบคุมภายใน

องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment) เป็นกระบวนการระบุและวิเคราะห์ความเสี่ยงที่จะส่งผลกระทบต่อวัตถุประสงค์เป้าหมายขององค์กร ประกอบด้วย 4 หลักการ ได้แก่ หลักการที่ 6 กำหนดวัตถุประสงค์และเป้าหมายไว้อย่างชัดเจนและเหมาะสม เพื่อให้สามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องได้ หลักการที่ 7 ระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์อย่างครอบคลุมทั่วทั้งองค์กร เพื่อหาแนวทางจัดการความเสี่ยงที่เหมาะสม หลักการที่ 8 พิจารณาโอกาสและประเมินความเสี่ยงในการเกิดทุจริตในรูปแบบต่าง ๆ และหลักการที่ 9 ระบุและประเมินความเปลี่ยนแปลงที่สำคัญอันอาจส่งผลกระทบต่อระบบการควบคุมภายใน

องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities) เป็นนโยบายและระเบียบปฏิบัติที่ทำให้มั่นใจว่ามาตรการตอบสนองความเสี่ยงได้รับการปฏิบัติตามเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ประกอบด้วย 3 หลักการ ได้แก่ หลักการที่ 10 ระบุและพัฒนากิจกรรมการควบคุมเพื่อลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่ยอมรับได้

หลักการที่ 11 ระบุและพัฒนากิจกรรมการควบคุมทั่วไปด้านเทคโนโลยี เพื่อสนับสนุนการบรรลุวัตถุประสงค์ และหลักการที่ 12 นำกิจกรรมการควบคุมมาปฏิบัติจริงอย่างสม่ำเสมอผ่านนโยบายที่คาดหวังและกระบวนการทำงานที่เป็นลายลักษณ์อักษร

องค์ประกอบที่ 4 สารสนเทศและการสื่อสาร (Information and Communication) เป็นกระบวนการจัดหา จัดการ และสื่อสารข้อมูลที่มีคุณภาพเพื่อให้การควบคุมภายในดำเนินไปได้ตามระบบ ประกอบด้วย 3 หลักการ ได้แก่ หลักการที่ 13 จัดทำหรือนำข้อมูลสารสนเทศที่เกี่ยวข้องและมีคุณภาพมาใช้สนับสนุนให้ระบบการควบคุมภายในบรรลุวัตถุประสงค์ หลักการที่ 14 มีการสื่อสารข้อมูลภายในองค์กร รวมถึงวัตถุประสงค์และความรับผิดชอบที่จำเป็น เพื่อให้การควบคุมภายในดำเนินไปได้อย่างมีประสิทธิภาพ และหลักการที่ 15 มีการสื่อสารกับหน่วยงานหรือผู้มีส่วนได้เสียภายนอกองค์กรในประเด็นที่อาจส่งผลกระทบต่อระบบการควบคุมภายใน

องค์ประกอบที่ 5 กิจกรรมการติดตามผล (Monitoring Activities) เป็นกระบวนการติดตาม ประเมิน และสอบทานความเพียงพอของการปฏิบัติงานตามการควบคุมภายในเมื่อเวลาผ่านไป ประกอบด้วย 2 หลักการ ได้แก่ หลักการที่ 16 ประเมินผลการควบคุมภายในทั้งในลักษณะการประเมินผลอย่างต่อเนื่องในกระบวนการทำงาน และการประเมินผลเป็นรายครั้ง และหลักการที่ 17 ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในอย่างทันเวลาต่อผู้รับผิดชอบ รวมถึงฝ่ายบริหารและคณะกรรมการ เพื่อดำเนินการปรับปรุงแก้ไขข้อผิดพลาดทันที

2.4 การวิเคราะห์ความสัมพันธ์ระหว่าง 5 องค์ประกอบและ 17 หลักการควบคุมภายในของกรอบการควบคุมภายใน COSO IC 2013 และหลักการของแนวทางการบริหารความเสี่ยงเชิงรุกตามกรอบ COSO ERM 2017: การเปลี่ยนแปลงทางเทคโนโลยีของนักบัญชี

การควบคุมภายในและการบริหารความเสี่ยงมีความสัมพันธ์แบบส่งเสริมกันอย่างใกล้ชิดและไม่สามารถแยกขาดจากกันได้ [8] ภายใต้กรอบการทำงานของ COSO ระบบการควบคุมภายในถือเป็นส่วนหนึ่งและเป็นรากฐานที่สำคัญของการบริหารความเสี่ยงองค์กร โดยกรอบควบคุมภายใน COSO IC 2013 จะมุ่งเน้นการวางรากฐานเพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่ากระบวนการทำงานมีความถูกต้อง โปร่งใส ป้องกันการทุจริต และเป็นไปตามกฎระเบียบ [12] ในขณะที่กรอบการบริหารความเสี่ยง COSO ERM 2017 จะขยายขอบเขตการทำงานขึ้นไปในระดับยุทธศาสตร์ เพื่อมุ่งเน้นการคว้าโอกาสทางธุรกิจและการสร้างมูลค่าเพิ่มผ่านการเชื่อมโยงความเสี่ยงเข้ากับการกำหนดวิสัยทัศน์ พันธกิจ และค่านิยมหลักขององค์กร [13]

การนำเทคโนโลยีเข้ามาใช้มักก่อให้เกิดความเสี่ยงรูปแบบใหม่ที่รุนแรง หากองค์กรให้ความสำคัญเฉพาะการควบคุมภายในระดับปฏิบัติการแต่ขาดมุมมองเชิงกลยุทธ์ จะนำไปสู่การทำลายมูลค่าขององค์กร ซึ่งมีสาเหตุที่สะท้อนความเป็นไปได้ที่กลยุทธ์จะไม่สอดคล้องกับพันธกิจและวิสัยทัศน์ เช่น การเร่งปรับตัวเป็นดิจิทัลด้วยการใช้ AI ประมวลผลข้อมูลโดยไม่ตรวจสอบจริยธรรมข้อมูลหรือความปลอดภัยไซเบอร์ ซึ่งอาจขัดต่อคุณค่าหลักด้านความซื่อสัตย์สุจริตขององค์กร และผลกระทบที่ตามมาจากกลยุทธ์ที่เลือกใช้ ซึ่งเทคโนโลยีแต่ละระบบย่อมมีความเสี่ยงที่แตกต่างกัน ซึ่งนักบัญชีจำเป็นต้องประเมินและตัดสินใจแลกเปลี่ยนข้อดีข้อเสียให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ เมื่อพิจารณาการทำงานประสานกันระหว่าง 5 องค์ประกอบของทั้งสองกรอบการทำงานในบทบาทของนักบัญชียุคดิจิทัล มีดังนี้



ตารางที่ 1 ความสัมพันธ์ระหว่างหลักการควบคุมภายในของกรอบการควบคุมภายใน COSO IC 2013 และหลักการของแนวทางการบริหารความเสี่ยงเชิงรุกตามกรอบ COSO ERM 2017

องค์ประกอบ COSO IC 2013	องค์ประกอบ COSO ERM 2017	แนวทางการประยุกต์ใช้แบบเชิงรุก ในการเปลี่ยนแปลงทางเทคโนโลยีของนักบัญชี
1. สภาพแวดล้อมการควบคุม (Control Environment)	1. การกำกับดูแลและวัฒนธรรมองค์กร (Governance & Culture)	ฝ่ายบริหารและคณะกรรมการต้องกำหนดนโยบายและแนวปฏิบัติที่สร้าง Digital Mindset และวัฒนธรรมตระหนักรู้ภัยไซเบอร์ นักบัญชีต้องมีบทบาทในการกำกับดูแลจริยธรรมของ AI (AI Governance) เพื่อลดข้อผิดพลาดอย่างเป็นระบบในระบบคอมพิวเตอร์หรือปัญญาประดิษฐ์ (AI) และสร้างความโปร่งใสที่ตรวจสอบได้
2. การประเมินความเสี่ยง (Risk Assessment)	2. กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy & Objective-Setting)	นักบัญชีต้องร่วมประเมินความเสี่ยงของเทคโนโลยีตั้งแต่ขั้นตอนวางแผนเชิงกลยุทธ์ เช่น การย้ายระบบบัญชีขึ้นคลาวด์ ว่าสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้หรือไม่ เพื่อป้องกันไม่ให้เกิดความล้มเหลวเชิงยุทธศาสตร์
3. กิจกรรมการควบคุม (Control Activities)	3. ผลการดำเนินงาน (Performance)	การแปรเปลี่ยนกิจกรรมการควบคุมจากระดับปฏิบัติการไปสู่การทำงานแบบอัตโนมัติ เช่น การใช้ระบบสามฝ่ายตรงกันอัตโนมัติ หรือการใช้เทคโนโลยี Blockchain ในการพิสูจน์ธุรกรรมที่สามารถตอบสนองข้อมูลที่เกิดขึ้นทันที เพื่อลดข้อผิดพลาดจากมนุษย์ และช่วยให้นักบัญชีเห็นภาพรวมความเสี่ยงสะสมขององค์กรได้ชัดเจน
4. สารสนเทศและการสื่อสาร (Information & Communication)	5. ข้อมูล การสื่อสาร และการรายงาน (Information, Communication, and Reporting)	การทำลายขอบเขตข้อมูลที่แยกส่วนกันด้วยการสร้างท่อส่งข้อมูลสารสนเทศที่ไหลเวียนขึ้น-ลงและผ่านทั่วทั้งองค์กรอย่างต่อเนื่อง นักบัญชีประยุกต์ใช้ซอฟต์แวร์ประมวลผลข้อมูลขนาดใหญ่ (Big Data) และคลาวด์ เพื่อจัดเตรียมรายงานทางการเงินและข้อมูลความเสี่ยงที่มีคุณภาพ รวดเร็ว และสามารถเข้าถึงได้ทันทีตามเวลาจริง
5. กิจกรรมการติดตามผล (Monitoring Activities)	4. การทบทวนและการปรับปรุงแก้ไข (Review & Revision)	การยกระดับจากการติดตามผลตรวจสอบเชิงรับไปสู่การตรวจสอบเชิงพยากรณ์ และการรับรู้ความเสี่ยงแบบพลวัตโดยใช้ Machine Learning หรือ AI คาดการณ์แนวโน้มความผิดปกติและตรวจจับสัญญาณเตือนภัยล่วงหน้า เพื่อปรับปรุงระบบควบคุมได้ก่อนเกิดความเสียหายจริง

2.5 กลยุทธ์การควบคุมภายในเพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยีของนักบัญชี

กลยุทธ์การควบคุมภายในสำหรับนักบัญชีในยุคดิจิทัลต้องปรับเปลี่ยนจากการควบคุมเชิงรับ (Reactive) ที่เน้นการตรวจสอบย้อนหลังไปสู่การควบคุมเชิงรุก (Proactive) ที่เน้นการพยากรณ์และป้องกันความเสี่ยงทันที โดยสามารถสรุปกลยุทธ์สำคัญได้ ดังนี้

2.5.1 การเปลี่ยนผ่านสู่ระบบการควบคุมอัตโนมัติ (Automated Controls) คือการที่นักบัญชีควรเปลี่ยนจากการควบคุมด้วยมือ (Manual) มาเป็นการฝังเงื่อนไขการควบคุมลงในซอฟต์แวร์ เพื่อลดข้อผิดพลาดจากมนุษย์และความเสี่ยงจากการทุจริต [12] องค์กรต้องเลือกและพัฒนาเป้าหมายการควบคุมด้านเทคโนโลยีเพื่อสนับสนุนความเชื่อมั่นของระบบ เช่น การใช้ระบบจับคู่เอกสารอัตโนมัติ (Automated Reconciliation) และการกำหนดสิทธิ์เข้าถึงข้อมูลตามบทบาทหน้าที่ (Role-Based Access Control) [14]

2.5.2 การบริหารความเสี่ยงเชิงรุกด้วยการวิเคราะห์ข้อมูล (Predictive Analytics) คือการนำเทคโนโลยีมาใช้เพื่อระบุความเสี่ยงในระดับพอร์ตโฟลิโอและพยากรณ์ผลกระทบต่อกลยุทธ์องค์กร เช่น การใช้ปัญญาประดิษฐ์ (AI) และ Big Data เพื่อตรวจจับสัญญาณผิดปกติในทันที (Continuous Monitoring) [10] ติดตั้งระบบแจ้งเตือน (Alert System) เมื่อมีการทำรายการที่ผิดเงื่อนไข หรือรายการที่มีแนวโน้มการทุจริตโดยวิเคราะห์จากรูปแบบข้อมูลในอดีต [13]

2.5.3 การสร้างวัฒนธรรมดิจิทัลและความปลอดภัยทางไซเบอร์ (Cyber Resilience) เนื่องจากเทคโนโลยีคลาวด์ (Cloud) และออนไลน์มีความเสี่ยงเรื่องการรั่วไหลของข้อมูล นักบัญชีจึงต้องเป็นผู้กำกับดูแลจริยธรรมข้อมูล เช่น การกำหนดนโยบายจริยธรรมปัญญาประดิษฐ์ (AI Ethics) และการบริหารจัดการแรงเสียดทานด้านความปลอดภัย (Security Friction) เพื่อให้ระบบปลอดภัยแต่ยังคงความคล่องตัว (Agility) ในการทำงาน ดังนั้นความฉลาดทางวิชาชีพบัญชีดิจิทัล (Digital Professional Intelligence) เป็นปัจจัยสำคัญต่อความสำเร็จในการควบคุมภายในยุคใหม่ [6]

2.5.4 การใช้เทคโนโลยีบล็อกเชน (Blockchain) เพื่อความโปร่งใส เป็นการนำระบบบัญชีแยกประเภทแบบกระจาย (Distributed Ledger) มาใช้เพื่อป้องกันการบิดเบือนข้อมูลหลักฐาน เช่น พัฒนาระบบบัญชีระบบสามทาง (Triple-entry Accounting) ซึ่งข้อมูลจะถูกบันทึกและสอบย้อนกันเองในเครือข่าย ทำให้ไม่สามารถแก้ไขข้อมูลย้อนหลังได้ ดังนั้น Blockchain ช่วยเพิ่มความโปร่งใสและลดความเสี่ยงในการทำทุจริตทางการเงินได้อย่างมีนัยสำคัญ [15]

2.6 งานวิจัยที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมพบว่างานวิจัยของ Laowilas [3] และ Somsak [16] ยืนยันตรงกันว่านโยบายและการสนับสนุนจากผู้บริหารระดับสูง ร่วมกับการสื่อสารข้อมูลที่มีคุณภาพและการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม เป็นปัจจัยสำคัญที่สุดที่ส่งเสริมให้การนำกรอบ COSO ERM 2017 มาใช้ปฏิบัติจริงในภาคธุรกิจประสบความสำเร็จอย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับ Kaewkham และคณะ [6] ที่ทำการศึกษาพบว่านักบัญชีที่มีความฉลาดทางวิชาชีพบัญชียุคดิจิทัลในระดับสูง จะมีทักษะและความสามารถในการวิเคราะห์ข้อมูลเพื่อควบคุมความเสี่ยงของรายงานทางการเงิน ส่งผลให้ประสิทธิภาพและความสำเร็จในงานเพิ่มขึ้นอย่างมีนัยสำคัญ นอกจากนี้ Ranglek [7] ยังได้ชี้ให้เห็นว่าระบบการประเมินความเสี่ยงทางดิจิทัลในเชิงรุกส่งผลบวกโดยตรงต่อความยั่งยืนขององค์กรท่ามกลางการแข่งขันที่รุนแรง จากการวิจัยของ Yuan [4] ได้อธิบายว่าภายหลังสถานการณ์การแพร่ระบาดของโรคโควิด-19 องค์กรต้องเปลี่ยนมุมมองต่อการบริหารความเสี่ยง จากภาระงานตรวจสอบตามรอบเวลาไปสู่การสร้างวัฒนธรรมความเสี่ยงที่ฝังตัวอยู่ในทุกกลยุทธ์และการตัดสินใจทางธุรกิจ ขณะที่ Febriani & Prasetya [17] ได้สะท้อนข้อจำกัดในทางปฏิบัติว่าองค์กรขนาดกลางมักประสบปัญหาการขาดคณะกรรมการความเสี่ยง และการไม่มีเอกสารกำหนดระดับความเสี่ยงที่ยอมรับได้ที่ชัดเจน ซึ่งสอดคล้องกับงานวิจัยของ Halar & Schwaiberger [8] ที่สรุปผลวรรณกรรมอย่างเป็นระบบว่า ระบบการควบคุมภายในที่ได้รับการปฏิรูปเข้าสู่มิติดิจิทัลอย่างสมบูรณ์ แบบจะช่วยป้องกันอุปสรรคของการทุจริตในรายงานทางการเงินได้สูงสุด [18] และปิดช่องโหว่ของการทำงานที่ล่าช้าได้อย่างเป็นรูปธรรม ผ่านการผสมผสานการทำงานของเทคโนโลยีตรวจจับอัจฉริยะร่วมกับการพยากรณ์ความเสี่ยงเชิงพยากรณ์ [19]

3. การวิเคราะห์ประเด็นตามหลักวิชาการ

จากการสังเคราะห์ข้อมูลวรรณกรรมและงานวิจัยที่เกี่ยวข้อง สามารถนำมาประเมินมิติทางวิชาการและวิเคราะห์ประเด็นสำคัญของยุทธศาสตร์การบริหารความเสี่ยงเชิงรุกของนักบัญชีไทยได้ 3 ด้านหลัก ดังนี้

3.1 การบูรณาการระดับความเสี่ยงที่ยอมรับได้เข้ากับโครงการลงทุนด้านดิจิทัล องค์กรธุรกิจในประเทศไทยจำนวนมากเริ่มทำเทคโนโลยีสารสนเทศสมัยใหม่เข้ามาปรับใช้ เช่น ระบบการวางแผนทรัพยากรองค์กรผ่านระบบคลาวด์ หรือระบบจัดการข้อมูลขนาดใหญ่ อย่างไรก็ตามความล้มเหลวมักเกิดขึ้นเนื่องจากการลงทุนเหล่านี้ขาดการบูรณาการเข้ากับระดับความเสี่ยงที่ยอมรับได้ขององค์กรตามหลักการของ COSO ERM 2017 นักบัญชีบริหารจึงต้องก้าวเข้ามามีบทบาทในการร่วมวิเคราะห์คุณค่าและโอกาสในการสูญเสียสิทธิ์หรือการสูญหายของข้อมูลบนคลาวด์ เพื่อประเมินว่าสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัทหรือไม่ และต้องเปลี่ยนบทบาทจากการเป็นผู้อนุมัติงบประมาณเป็นที่ปรึกษาเชิงยุทธศาสตร์ร่วมประเมินมูลค่าความเสี่ยง

3.2 การยกระดับสู่ระบบเตือนภัยล่วงหน้าผ่านการตรวจจับแบบแสดงผลข้อมูลทันที ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความเร็วและผลกระทบในระดับเสียวินาที เช่น ภัยคุกคามจากการโจรกรรมข้อมูลผ่านช่องโหว่ความปลอดภัยไซเบอร์ ดังนั้นระบบการควบคุมภายในและการตรวจสอบภายในแบบเดิมที่ทำเป็นรายเดือนหรือรายไตรมาสจึงไม่สามารถระงับความเสียหายได้ทันทั่วทั้งที่ นักบัญชีและผู้ตรวจสอบภายในจึงต้องประยุกต์ใช้แนวคิด Dynamic Risk Sensing และการตรวจสอบอย่างต่อเนื่อง โดยการวางตัวชี้วัดความเสี่ยงล่วงหน้าบนระบบฐานข้อมูล ซึ่งระบบจะแจ้งเตือนความผิดปกติทันทีที่เกิดรายการนอกกรอบการควบคุม ทำให้ฝ่ายบริหารสามารถรับมือและตัดสินใจได้บนข้อมูลที่ถูกต้องและปลอดภัยสูงสุด

3.3 ธรรมชาติและความรับผิดชอบของแบบจำลองอัจฉริยะ เมื่อปัญญาประดิษฐ์ (AI) เข้ามาจัดหมวดหมู่รายการทางการเงินและการพยากรณ์กระแสเงินสดโดยอัตโนมัติ สิ่งที่นักบัญชีต้องตระหนักและประเมินผ่านกรอบการกำกับดูแลและวัฒนธรรมคือความเสี่ยงด้านความผิดพลาดหรือความไม่เป็นธรรมในการตัดสินใจของระบบ และความยากในการอธิบายที่มาของการตัดสินใจของปัญญาประดิษฐ์ นักบัญชีจึงต้องร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศจัดทำนโยบายตรวจสอบแบบจำลองอัจฉริยะอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าการตัดสินใจของเทคโนโลยีมีความโปร่งใส มีจริยธรรม และยังคงความน่าเชื่อถือของรายงานทางการเงินตามมาตรฐานสากล

4. สรุปผลและแสดงทัศนะทางวิชาการ

การศึกษาในบทความวิชาการนี้สะท้อนให้เห็นว่า แนวทางการบริหารความเสี่ยงเชิงรุกตามกรอบ COSO ERM 2017 ไม่ใช่เป็นเพียงภาระหน้าที่เพิ่มเติมของฝ่ายกำกับดูแลหรือผู้ตรวจสอบภายใน แต่เป็นเครื่องมือทางกลยุทธ์ที่สำคัญที่สุดของนักบัญชีในยุคดิจิทัล การเปลี่ยนผ่านจากการควบคุมเชิงตั้งรับที่มุ่งเน้นอดีตไปสู่การบูรณาการความเสี่ยงเพื่อพยากรณ์อนาคตอย่างต่อเนื่อง คือหัวใจสำคัญที่จะช่วยให้องค์กรธุรกิจในประเทศไทยรอดพ้นจากสภาวะการหยุดชะงักทางเทคโนโลยี และรักษาความน่าเชื่อถือของข้อมูลสารสนเทศทางการเงินไว้ได้ สำหรับประเทศไทยจำเป็นต้องมีการขับเคลื่อนร่วมกันระหว่างภาครัฐ หน่วยงานกำกับดูแล สถาบันการศึกษา และภาคเอกชน เพื่อยกระดับระบบนิเวศทางการเงินและบรรษัทภิบาลของประเทศให้พร้อมรับมือกับภัยคุกคามทางเทคโนโลยี โดยมีข้อเสนอแนะแนวทางขับเคลื่อนเชิงนโยบายดังนี้

4.1 ข้อเสนอแนะเชิงนโยบายสำหรับหน่วยงานกำกับดูแลและสภาวิชาชีพบัญชี

4.1.1 การจัดทำแนวปฏิบัติสากลเฉพาะด้าน AI และ IT Governance สำหรับวิชาชีพบัญชี การออกประกาศหรือคู่มือการนำกรอบ COSO ERM 2017 มาใช้ควบคุมความเสี่ยงของเทคโนโลยีที่เกิดขึ้นใหม่เป็นการเฉพาะ เช่น ปัญญาประดิษฐ์ โดยกำหนดนโยบายความรับผิดชอบของแบบจำลองขั้นตอนการแก้ปัญหา เพื่อป้องกันความเสี่ยงด้านความลำเอียงของ AI และข้อมูลเท็จในรายงานทางการเงิน

4.1.2 การยกระดับเกณฑ์มาตรฐานการควบคุมภายในของบริษัทจดทะเบียน โดยให้ความร่วมมือกับสำนักงาน ก.ล.ต. และตลาดหลักทรัพย์แห่งประเทศไทยในการปรับปรุงแบบประเมินความเสี่ยงพหุของระบบการควบคุมภายใน ให้ปรับเปลี่ยนจากการเน้นปฏิบัติตามกฎระเบียบเชิงรับ ไปสู่การประเมินความเสี่ยงเชิงรุกและการตรวจสอบอย่างต่อเนื่อง

4.2 ข้อเสนอแนะเชิงนโยบายด้านการศึกษาและการพัฒนาทักษะบุคลากร

4.2.1 การปรับปรุงหลักสูตรการศึกษาด้านการบัญชีระดับอุดมศึกษา กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมร่วมกับสภาวิชาชีพบัญชี กำหนดมาตรฐานหลักสูตรบัญชีบัณฑิตให้เพิ่มรายวิชาบังคับด้าน “ความฉลาดทางวิชาชีพบัญชีดิจิทัล” ซึ่งประกอบด้วย การวิเคราะห์ข้อมูลความเสี่ยง การตรวจสอบเทคโนโลยีสารสนเทศ จริยธรรมการใช้ข้อมูลและ AI และวิทยาการความมั่นคงปลอดภัยไซเบอร์เบื้องต้น

4.2.2 นโยบายการพัฒนาความรู้ต่อเนื่องทางวิชาชีพ กำหนดเป็นเงื่อนไขบังคับในการเก็บชั่วโมงพัฒนาความรู้ ต่อเนื่องทางวิชาชีพ (CPD) สำหรับผู้ทำบัญชีและผู้สอบบัญชีรับอนุญาต (CPA) ให้มีสัดส่วนของหัวข้อ “การบริหารความเสี่ยงทางเทคโนโลยีและการควบคุมภายในยุคดิจิทัล” อย่างน้อย 3-6 ชั่วโมงต่อปี

4.3 ข้อเสนอแนะเชิงนโยบายสำหรับการส่งเสริมภาคธุรกิจและ SME ไทย

4.3.1 มาตรการจูงใจทางภาษีและการสนับสนุนการยกระดับสู่ “สำนักงานบัญชีดิจิทัลที่ปลอดภัย” เสนอให้ กรมสรรพากรและกระทรวงการคลัง ออกมาตรการหักลดหย่อนภาษีได้ 2 เท่า สำหรับองค์กรและสำนักงานบัญชีขนาดกลาง และขนาดย่อย (SMEs) ที่ลงทุนในระบบการควบคุมภายในอัตโนมัติ ซอฟต์แวร์ป้องกันภัยไซเบอร์ หรือซอฟต์แวร์บริหารความเสี่ยง เพื่อลดภาระต้นทุนในการปรับตัวสู่ยุคดิจิทัล

4.3.2 การสร้างระบบมาตรฐานการประเมินภัยคุกคามไซเบอร์ทางการเงินระดับชาติ พัฒนาเครื่องมือประเมิน ระดับความพร้อมและความเสี่ยงไซเบอร์ ให้สำนักงานบัญชีและภาคธุรกิจไทยใช้ประเมินตนเองล่วงหน้า เพื่อป้องกันเหตุการณ์ ข้อมูลทางการเงินรั่วไหลหรือการโจมตีโดยมัลแวร์

ดังนั้นประสิทธิภาพการปฏิบัติงานของนักบัญชีในบริบทธุรกิจยุคใหม่จะเกิดขึ้นได้อย่างมั่นคงและยั่งยืนนั้น จำเป็นต้อง ได้รับการขับเคลื่อนพร้อมกันจากทักษะความฉลาดทางวิชาชีพบัญชียุคดิจิทัล การนำกรอบการบริหารความเสี่ยงเข้าไปผสาน เป็นเนื้อเดียวกับการวางยุทธศาสตร์องค์กร และการสร้างสิ่งแวดล้อมที่ทุกฝ่ายในองค์กรตระหนักถึงความปลอดภัยทางไซเบอร์ ร่วมกัน ในอนาคตอันใกล้วิชาชีพบัญชีในประเทศไทยจะถูกท้าทายด้วยปริมาณข้อมูลสารสนเทศที่ไร้โครงสร้างและภัยไซเบอร์ที่ทวีความรุนแรงขึ้นอย่างรวดเร็ว สภาวิชาชีพบัญชีและสถาบันอุดมศึกษาจึงควรเร่งปฏิรูปหลักสูตรการศึกษาและการพัฒนา ความรู้ต่อเนื่องทางวิชาชีพ โดยบรรจุเนื้อหาด้านการวิเคราะห์ข้อมูลความเสี่ยง (Risk Data Analytics) การตรวจสอบ เทคโนโลยีสารสนเทศ (IT Audit) และจริยธรรมของปัญญาประดิษฐ์ เพื่อผลักดันให้นักบัญชีไทยยกระดับบทบาทขึ้นเป็นที่ปรึกษาเชิงกลยุทธ์ที่สามารถชี้แนะและผลักดันความสำเร็จขององค์กรในระดับสากลได้อย่างยั่งยืน

5. เอกสารอ้างอิง (References)

- [1] Vongwaree, P. (2022). Risk management guidelines for accounting firms' technological changes. *Journal of Humanities and Social Sciences*, 12(1), 45-58. (In Thai)
- [2] Prewett, K., & Terry, A. (2018). COSO's updated enterprise risk management framework: A quest for depth and clarity. *Journal of Corporate Accounting & Finance*, 29(3), 16-23.
- [3] Laowilas, R. (2021). *Factors affecting risk management based on COSO ERM 2017 for listed companies on the Market for Alternative Investment (mai)* [Unpublished master's independent study]. Thammasat University. (In Thai)
- [4] Yuan, J. (2022). Rethinking the guiding significance of COSO-ERM for enterprise risk management in the post-epidemic era. *International Journal of Social Science and Education Research*, 5(6), 60-68.



- [5] Parapuang, T. (2020). *Implementing an enterprise risk management (COSO ERM 2017): Case study Ookbee Co., Ltd.* [Unpublished master's independent study]. Thammasat University. (In Thai)
- [6] Kaewkham, J., et al. (2023). The impact of digital accounting professional intelligence on performance efficiency. *Journal of Business Administration, UTCC*. (In Thai)
- [7] Ranglek, C. (2022). Effect of proactive digital accounting support on firm sustainability of exporting business in Thailand.
- [8] Halar, P., & Schwaiberger, J. (2026). A digitally transformed system of internal control for effective financial statement fraud prevention and detection: A literature review. *Zeszyty Teoretyczne Rachunkowości*, 50(1), 33-62.
- [9] Islam, A., Papia, S. K., Akhir, A., Rahman, F., & Nashid, S. (2025). Artificial intelligence (AI)-powered predictive analytics: Driving strategic transformation in business analytics. *Journal of AI ML DL*, 1(1), 1-9.
- [10] COSO. (2017). *Enterprise Risk Management - Integrating with Strategy and Performance*.
- [11] Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control - Integrated framework*. COSO.
- [12] Tantiraviwat, T. (2022). *The influence of internal control of audited entities on the audit efficiency of auditors at the State Audit Office of the Kingdom of Thailand*. Master's thesis, Dhurakij Pundit University. (In Thai)
- [13] Chookhiatti, S., & Audsabumrungrat, J. (2020). Key points of enterprise risk management: Integrating with strategy and performance (COSO ERM (2017)). *Journal of Accounting Profession*, 16(49), 60-72. (In Thai)
- [14] Tantiraviwat, T. (2023). Relationship of internal control according to COSO ERM 2017 with audit efficiency. *Academic Journal of Dhurakij Pundit University*. (In Thai)
- [15] Singh, A., & Prabhu, S. (2023). Agile Blockchain-based Risk Management Framework. *Journal of Mechanical, Civil and Industrial Engineering*.
- [16] Somsak, H. (2022). Enterprise risk management based on COSO ERM 2017 affecting the work efficiency of accountants of accounting firms in Bangkok. *Journal of Management Innovation*, 8(3), 15-28. (In Thai)
- [17] Febriani, F., & Prasetya, M. E. (2025). Evaluation of risk management implementation using COSO ERM 2017 framework: A case study at PT XYZ. *Journal of Accounting and Business Education*, 10(2), 50-63.
- [18] Deloitte. (2024). *Applying enterprise risk management to artificial intelligence: Implementing and scaling AI with the COSO ERM framework*. Deloitte.
- [19] Ratchasethakul, K. (2021). *Enterprise risk management under conceptual framework of COSO ERM 2017: A case study of a non-life insurance company* [Unpublished master's independent study]. Thammasat University. (In Thai)