บทความวิจัย

การนำองค์กรในด้านการรักษาความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงของธนาคารไทย

จักรกฤษ ไวโสภา* และ บวร ปภัสราทร
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 08 9997 7013 อีเมล: jakkrit.vi@mail.kmutt.ac.th DOI: 10.14416/j.kmutnb.2024.07.012
รับเมื่อ 27 ตุลาคม 2565 แก้ไขเมื่อ 10 มกราคม 2566 ตอบรับเมื่อ 7 กุมภาพันธ์ 2566 เผยแพร่ออนไลน์ 31 กรกฎาคม 2567

บทคัดย่อ

ภัยคุกคามทางไซเบอร์ถือเป็นความเสี่ยงและส่งผลกระทบต่อการดำเนินธุรกิจของธนาคาร การรักษาความมั่นคงทางไซเบอร์จึงเป็นสิ่งสำคัญต่อธุรกิจของธนาคาร โดยที่ประสิทธิผลของการรักษาความมั่นคงไซเบอร์ขึ้นอยู่กับบทบาทในการนำองค์กรของผู้บริหารระดับสูงของธนาคารตลอดจนมีมาตรฐานและกฎระเบียบที่เกี่ยวข้องอยู่หลายประการ อย่างไรก็ตามยังไม่มีแนวทางและวิธีการปฏิบัติในการนำองค์กรอย่างมีประสิทธิผลที่กำหนดไว้ในมาตรฐานและกฎระเบียบเหล่านั้น งานวิจัยนี้จึงเสนอแนวทางในการนำองค์กร และวิธีการในการรักษาความมั่นคงทางไซเบอร์อย่างมีประสิทธิผล สำหรับผู้บริหารระดับสูงของธนาคาร โดยแนวทางในการนำองค์กรอย่างมีประสิทธิผลดำเนินการตาม Baldrige Cybersecurity Excellence Builder ส่วนวิธีการปฏิบัติตามแนวทางที่เสนอนั้นเรียบเรียงขึ้นจาก แนวทางการรักษาความมั่นคงทางไซเบอร์ของ NIST แนวทางการกำกับดูแลเทคโนโลยีสารสนเทศ COBIT5 มาตรฐานด้านความมั่นคงทางไซเบอร์ที่เกี่ยวข้อง 4 มาตรฐาน ได้แก่ ISO/IEC 27001:2013 CIS Control 7.1 ISA 62443-2-1-2009 และ NIST.SP.800-53 Revision 4 มาตรฐานระบบบริหารงานคุณภาพ ISO 9001:2015 และระเบียบปฏิบัติของธนาคารแห่งประเทศไทยตลอดจนกฎหมายที่เกี่ยวข้อง วิธีปฏิบัติตามแนวทางการนำองค์กรที่เรียบเรียงขึ้นจึงสอดคล้องกับมาตรฐานความมั่นคงทางไซเบอร์ ครอบคลุมแนวทางการนำองค์กรของผู้บริหารระดับสูงในเรื่อง การกำหนดภารกิจ วิสัยทัศน์ และค่านิยมที่เกี่ยวกับรักษาความมั่นคงทางไซเบอร์ที่ส่งผลครอบคลุมไปถึงผู้มีส่วนได้ส่วนเสียทั้งหมด การปฏิบัติตนให้แสดงถึงความมุ่งมั่นในการรักษาความมั่นคงทางด้านไซเบอร์อย่างจริงจัง การแสดงให้เห็นความมุ่งมั่นต่อการปฏิบัติตามกฎหมายและจริยธรรมความมั่นคงทางไซเบอร์อย่างเข้มงวด การสื่อสารและการสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสีย การสร้างสภาพแวดล้อมเพื่อให้การดำเนินงานบรรลุผลตามนโยบายด้านความมั่นคงทางไซเบอร์ และการมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์ หากผู้บริหารระดับสูงของธนาคารปฏิบัติตามแนวทางและวิธีการที่นำเสนอนอกจากจะมั่นใจได้ว่าการจัดการการรักษาความมั่นคงทางไซเบอร์มีคุณภาพและเป็นไปตามมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงทางไซเบอร์ที่ยอมรับกันทั่วไปแล้วยังช่วยให้มั่นใจได้ว่ามีการปฏิบัติตามระเบียบและกฎหมายที่เกี่ยวข้องอย่างครบถ้วน ส่งผลให้การรักษาความมั่นคงทางไซเบอร์เป็นไปอย่างมีประสิทธิผล

คำสำคัญ: ธนาคาร ความมั่นคงทางไซเบอร์ การนำองค์กร

การอ้างอิงบทความ: จักรกฤษ ไวโสภา และ บวร ปภัสราทร, "การนำองค์กรในด้านการรักษาความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงของธนาคารไทย," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 34, ฉบับที่ 4, หน้า 1–13, เลขที่บทความ 244-186483, ต.ค.–ธ.ค. 2567.

วารสารวิชาการพระจอมเกล้าพระนครเหนือ ปีที่ 34 ฉบับที่ 4 ต.ค.–ธ.ค. 2567
The Journal of KMUTNB., Vol. 34, No. 4, Oct.–Dec. 2024

Research Article

Cybersecurity Leadership for Senior Executives of Thai Banking Firms

Jakkrit Visopa* and Borworn Papasratorn
School of Information Technology, King Mongkut's University of Technology Thonburi, Bangkok, Thailand

* Corresponding Author, Tel. 08 9997 7013, E–mail: jakkrit.vi@mail.kmutt.ac.th
DOI: 10.14416/j.kmutnb.2024.07.012
Received 27 October 2022; Revised 10 January 2023; Accepted 7 February 2023; Published online: 31 July 2024

Abstract

Cyber threat is one of the most important risks for banking firms. Leadership is one of the critical success factors for having effective cybersecurity. Baldrige Cybersecurity Excellence Builder framework identifies what leaders should do to ensure the effectiveness of cybersecurity in organization; however, the framework does not provide detail on approaches for the identified activities. This paper proposes approaches for bank executives to lead cybersecurity in Thai banking firms. The proposed leadership approaches were based on the leadership category from the Baldrige Cybersecurity Excellence Builder. The approaches for each item in the leadership category were synthesized from 2 popular cybersecurity frameworks, 4 cybersecurity standards, and 1 quality management system standard. The approaches were also complied with Bank of Thailand regulation and associated laws. The cybersecurity frameworks in this research included NIST Cybersecurity Framework and COBIT5. The cybersecurity standards being studied in this research are ISO/IEC 27001:2013, CIS Control 7.1, ISA 62443-2-1-2009 and NIST.SP.800-53 Revision 4. The proposed approaches also followed the quality management standard, ISO 9001:2015. The proposed leading approaches covered all leading items for leading effective cybersecurity, including mission-vision-value setting for cybersecurity, demonstration of cybersecurity commitment, commitment to legal and ethical behavior, communication and engagement with stakeholders, creation of environment for cybersecurity policies implementation, and focused on cybersecurity action to achieve the cybersecurity objectives. Following the proposed leadership approaches will not only ensure effectiveness of cybersecurity in banking operation, but also reduce risks and impacts on business loss from both internal and external cyber threats.

Keywords: Banking Firm, Cybersecurity, Leadership

Please cite this article as: J. Visopa and B. Papasratorn, "Cybersecurity leadership for senior executives of Thai banking firms," *The Journal of KMUTNB*, vol. 34, no. 4, pp. 1–13, ID. 244-186483, Oct.–Dec. 2024 (in Thai).

1. บทนำ

ปัจจุบันมีการสูญเสียจากการโจมตีทางไซเบอร์ที่มีมูลค่ามากกว่า 100 ล้านเหรียญดอลลาร์สหรัฐของธนาคารประเทศสมาชิกในระหว่าง ค.ศ. 2013–2018 [1] และรายงานมูลค่าความสูญเสียจากความเสี่ยงทางไซเบอร์ (Cyber Value at Risk) ซึ่งเป็นส่วนหนึ่งของความเสี่ยงด้านการปฏิบัติการของธนาคาร ได้บันทึกสถิติข้อมูลมูลค่าความสูญเสียจากการปฏิบัติงานของธนาคาร ระหว่าง ค.ศ. 2002–2017 จาก 74 ธนาคารขนาดใหญ่ในอเมริกาเหนือ ลาตินอเมริกา เอเชียแปซิฟิก ยุโรป และแอฟริกา พบว่า มีความสูญเสียจากเหตุการณ์ทางไซเบอร์ 0.25–0.65% หรือประมาณ 2.45–6.46 พันล้านยูโร ของมูลค่าความสูญเสียด้านการปฏิบัติการของธนาคารทั้งหมด นอกจากนี้ในรายงานยังระบุเพิ่มเติมว่า มีความเป็นไปได้ที่การสูญเสียจากเหตุการณ์ด้านไซเบอร์สามารถเพิ่มสูงขึ้นถึง 1 ใน 3 ของมูลค่าความสูญเสียจากการปฏิบัติการของธนาคารทั้งหมด [2] ในขณะที่รายงานการโจมตีทางไซเบอร์ในประเทศไทย ค.ศ. 2017–2018 พบว่ากลุ่มบริการที่ตกเป็นเป้าหมายสูงสุด ในลำดับที่ 1 และ 3 เป็นกลุ่มบริการทางการเงิน [3]

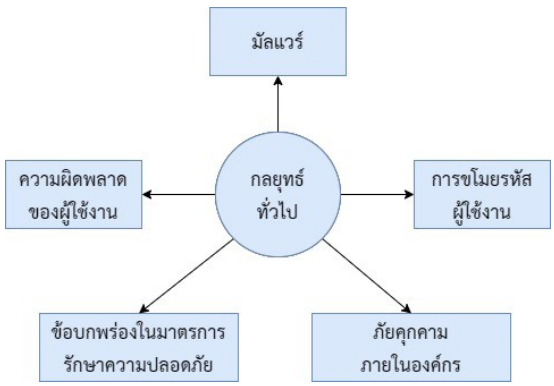
ประสิทธิผลของการรักษาความมั่นคงทางไซเบอร์ขึ้นอยู่กับการนำองค์กรของผู้นำ ซึ่งการนำองค์กรส่งผลต่อการรักษาความมั่นคงทางไซเบอร์ [4] ดังนั้นในงานวิจัยนี้จึงได้ศึกษา Baldrige Excellence Framework ซึ่งประสบความสำเร็จเป็นอย่างดีในการสร้างความเป็นเลิศในการดำเนินงาน ให้กับองค์กรที่นำไปปฏิบัติ [5] และร่วมกับ Baldrige Cybersecurity Excellence Builder ที่นำเสนอหัวข้อคำถามสำคัญ ในการการนำองค์กรด้านการรักษาความมั่นคงทางไซเบอร์ [6] เพื่อสังเคราะห์ขึ้นเป็นแนวทางการปฏิบัติในการนำองค์กรในด้านการรักษาความมั่นคงทางไซเบอร์ โดยวิธีการปฏิบัติตามแนวทางที่เสนอสังเคราะห์ขึ้นมาจาก NIST Cybersecurity Framework [7] มาตรฐานการรักษาความมั่นคงทางไซเบอร์ 4 มาตรฐาน ได้แก่ ISO/IEC 27001:2013 [8] CIS Control 7.1 [9] ISA 62443-2-1-2009 [10] และ NIST. SP.800-53 Revision 4 [11] มาตรฐานบริหารงานคุณภาพ ISO 9001:2015 [12] และกรอบการกำกับดูแลเทคโนโลยีสารสนเทศ COBIT5 [13] โดยคำนึงถึงความสอดคล้องกับระเบียบปฏิบัติและกฎหมายที่เกี่ยวข้อง ได้แก่ กรอบการประเมินความพร้อมด้าน Cyber Resilience ของธนาคารแห่งประเทศไทย (ธปท.) [14] พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 [15] และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 [16]

โดยมีวัตถุประสงค์เพื่อให้ได้แนวทางการนำองค์กรธนาคารในเรื่องการรักษาความมั่นคงทางไซเบอร์ ที่มีวิธีการปฏิบัติที่เป็นไปตามมาตรฐานการรักษาความมั่นคงทางไซเบอร์ มาตรฐานบริหารงานคุณภาพ กรอบการกำกับดูแลเทคโนโลยีสารสนเทศ โดยต้องสอดคล้องกับระเบียบปฏิบัติและกฎหมายไทยพร้อมกันด้วย

2. วัสดุ อุปกรณ์และวิธีการวิจัย

2.1 ภัยคุกคามทางไซเบอร์และความสูญเสียที่เกิดขึ้นกับธนาคาร

การโจมตีทางไซเบอร์ ก่อให้เกิดความเสียหายที่สำคัญต่อระบบชำระเงินระหว่างประเทศ (SWIFT) ตั้งแต่ ค.ศ. 2013–2018 มีมูลค่าความสูญเสียรวมมากกว่า 100 ล้านเหรียญดอลลาร์สหรัฐโดยมีกลยุทธการโจมตีที่ถูกรวมรวมไว้ 5 รูปแบบ ได้แก่ การใช้มัลแวร์ การขโมยรหัสผู้ใช้งาน ภัยคุกคามภายในองค์กร ข้อบกพร่องในมาตรการรักษาความปลอดภัย และความผิดพลาดของผู้ใช้งาน ตามรูปที่ 1 [1]



รูปที่ 1 การโจมตีทางไซเบอร์ที่พบในระบบ SWIFT

ความสูญเสียของธนาคารและสถาบันการเงินขนาดใหญ่ทั่วโลกตั้งแต่ปี 2002–2017 จากการดำเนินงานของธนาคารมีมูลค่ามหาศาล โดยจำแนกต้นเหตุความเสียหายดังแสดงใน ตามตารางที่ 1

ตารางที่ 1 มูลค่าความสูญเสียจากการดำเนินงานธนาคารแต่ละประเภท

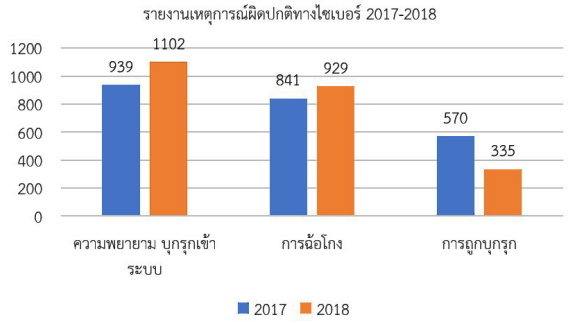
ประเภทภัยคุกคาม	มูลค่าความสูญเสีย
การฉ้อโกงจากภายในองค์กร	4,596 ล้านยูโร
การฉ้อโกงจากภายนอกองค์กร	2,612 ล้านยูโร
ความสูญเสียที่เกี่ยวกับบุคคลากร	1,070 ล้านยูโร
ความประมาทเลินเล่อ	67,263 ล้านยูโร
ภัยพิบัติ	260 ล้านยูโร
เทคโนโลยีและโครงสร้างพื้นฐาน	3,277 ล้านยูโร
กระบวนการบริหารจัดการ	7,221 ล้านยูโร

จากมูลค่าความสูญเสียจากการดำเนินงานธนาคารทั้งหมดสามารถแยกเป็นความสูญเสียที่เกิดจากภัยคุกคามทางไซเบอร์คิดเป็นมูลค่า 2.45–6.46 พันล้านยูโร อย่างไรก็ตามมูลค่าการสูญเสียที่เกี่ยวข้องกับไซเบอร์อาจสูงถึง 1 ใน 3 ของมูลค่าความสูญเสียจากการดำเนินงานของธนาคารทั้งหมด ซึ่งมาจากการคุกคามทางไซเบอร์ประเภทต่าง ๆ ดังแสดงในตารางที่ 2 [2]

รายงานการโจมตีทางไซเบอร์ในประเทศไทยระหว่าง ค.ศ. 2017–2018 พบการโจมตีสูงสุด 3 ลำดับแรก ได้แก่ การพยายามบุกรุกเข้าระบบ การฉ้อโกง และการถูกบุกรุกตามรูปที่ 2 โดยมีกลุ่มบริการที่ตกเป็นเป้าหมาย 3 ลำดับแรก ได้แก่ บริการทางการเงินต่างประเทศ บริการทางเทคโนโลยีและบริการทางการเงินในประเทศ [3]

ตารางที่ 2 ประเภทภัยคุกคามทางไซเบอร์ที่ก่อให้เกิดความสูญเสียต่อการดำเนินงานธนาคาร

ประเภทภัยคุกคาม	คำอธิบาย
การฉ้อโกงจากภายในองค์กร	กิจกรรมที่ไม่ได้รับอนุญาต: เช่น การซื้อขายหุ้นโดยไม่ได้รับอนุญาต การไม่รายงานการทำธุรกรรม เป็นต้น
	การโจรกรรมจากภายในองค์กร: การสร้างความเสียหายต่อระบบโดยเจตนาจากเจ้าหน้าที่ภายในองค์กร
	ความปลอดภัยของระบบภายในองค์กร: ความเสียหายที่เกิดขึ้นโดยเจตนาจากเจ้าหน้าที่ภายในองค์กร
การฉ้อโกงจากภายนอกองค์กร	การโจรกรรมและการฉ้อโกงภายนอกองค์กร: เช่น การปล้น การปลอมแปลง การโอนเช็คลอย
	ความปลอดภัยของระบบภายนอกองค์กร: ความเสียหายที่เกิดขึ้นโดยเจตนาเช่น ฮาร์ดแวร์/ซอฟแวร์ ได้รับความเสียหายจาก การเจาะระบบ การโจรกรรมข้อมูล
การหยุดชะงักของธุรกิจและความล้มเหลวของระบบ	เทคโนโลยีและโครงสร้างพื้นฐาน: ความสูญเสียที่เกิดจากการหยุดชะงักของธุรกิจหรือความล้มเหลวของโครงสร้างพื้นฐานสารสนเทศ



รูปที่ 2 รายงานการโจมตีทางไซเบอร์ในประเทศไทย

2.2 เกณฑ์บัลดริจ (Baldrige Excellence Framework)

เป็นกรอบการดำเนินงานที่ช่วยให้องค์กรบรรลุเป้าหมาย ปรับปรุงผลลัพธ์ และเพิ่มขีดความสามารถในการแข่งขันมากยิ่งขึ้นประกอบด้วย 4 ส่วน ได้แก่ ส่วนที่ 1 การตอบคำถามโครงสร้างองค์กร ส่วนที่ 2 การตอบคำถามในหมวด 1–7 ได้แก่ 1) การนำองค์กร 2) กลยุทธ์ 3) ลูกค้า 4) การวัด การวิเคราะห์ และการจัดการ 5) บุคลากร 6) การปฏิบัติการ และ 7) การติดตามผลลัพธ์ที่สำคัญ มีหลายองค์กรนำกรอบการดำเนินการนี้ไปปฏิบัติและสร้างความเป็นเลศให้เกิดขึ้น [17]

2.3 สร้างความเป็นเลิศด้านความมั่นคงทางไซเบอร์ของบัลดริจ (Baldrige Cybersecurity Excellence Builder)

เป็นเครื่องมือประเมินที่ผสมผสานระหว่าง NIST Cybersecurity Framework และ Baldrige Excellence Framework ที่ช่วยให้องค์กรเข้าใจถึงประสิทธิผลของการจัดการความเสี่ยงด้านความมั่นคงทางไซเบอร์ โดยงานวิจัยนี้มุ่งเน้นไปที่ส่วนที่ 2 หมวดที่ 1 ด้านการนำองค์กร ซึ่งแบ่งเป็นคำถามในการประเมิน เป็นสองส่วนหลักคือ คำถามการประเมินสำหรับการนำองค์กรด้านความมั่นคงทางไซเบอร์และกำกับดูแลและความรับผิดชอบต่อสังคม โดยมีการอ้างอิงไปยัง NIST Cybersecurity Framework ตามตารางที่ 3

ตารางที่ 3 บทบาทหน้าที่ของการนำองค์กรของ Baldrige Cybersecurity Excellence Builder

1. การนำองค์กร	**กรอบการดำเนินงานด้านความมั่นคงทางไซเบอร์ NIST**
1.1 การนำองค์กรเพื่อความมั่นคงทางไซเบอร์	ID-BE, RC-CO
1.2 การกำกับดูแลองค์กรและความรับผิดชอบต่อสังคม	ID-GV, RS-CO

Baldrige Cybersecurity Excellence Builder ประกอบด้วยคำถามสำหรับการประเมินการนำองค์กรดังนี้

1.1 การนำองค์กรเพื่อความมั่นคงทางไซเบอร์: ผู้นำระดับสูงด้านความมั่งคงทางไซเบอร์ นำองค์กรด้านนโยบายและการดำเนินงานด้านความมั่งคงทางไซเบอร์อย่างไร

1.1.1 ผู้นำจะนำภารกิจวิสัยทัศน์และค่านิยมขององค์กรไปใช้กับพนักงานซัพพลายเออร์และคู่ค้าหลักและลูกค้าสำคัญและผู้มีส่วนได้เสียอื่น ๆ ตามความเหมาะสมอย่างไร

1.1.2 การกระทำของผู้นำแสดงให้เห็นถึงความมุ่งมั่นในการรักษาความมั่นคงทางไซเบอร์อย่างไร

1.1.3 การกระทำของผู้นำแสดงให้เห็นถึงความมุ่งมั่นต่อพฤติกรรมทางกฎหมายและจริยธรรมอย่างไร

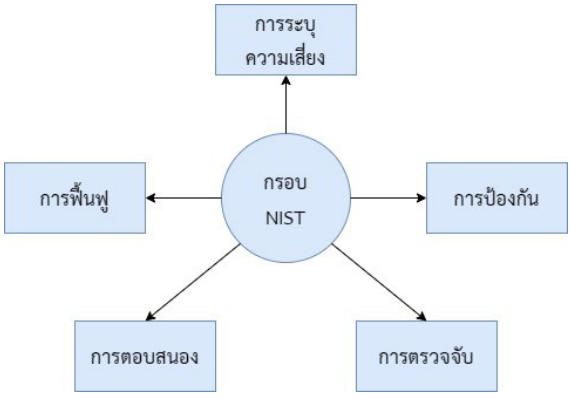
1.1.4 การสื่อสารและมีส่วนร่วมของผู้นำกับผู้นำองค์กรอื่น ๆ บุคลากร พันธมิตรที่สำคัญ ลูกค้าหลัก และผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงทางไซเบอร์อย่างไร

1.1.5 ผู้นำสามารถสร้างสภาพแวดล้อมสำหรับนโยบายและการดำเนินงานด้านความมั่นคงทางไซเบอร์ที่ประสบความสำเร็จในปัจจุบันและในอนาคตได้อย่างไร

1.1.6 ผู้นำมุ่งเน้นในการดำเนินการเพื่อบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์ขององค์กรให้สอดคล้องกับภารกิจได้อย่างไร [6]

2.4 มาตรฐานการรักษาความมั่นคงทางไซเบอร์

2.4.1 กรอบการรักษาความมั่นคงทางไซเบอร์ NIST ประกอบด้วย 5 ฟังก์ชันสำคัญได้แก่ 1) กรอบการระบุความเสี่ยงของสภาพแวดล้อมในองค์กร (Identify) 2) กรอบการป้องกันระบบขององค์กร (Protect) 3) กระบวนการและการกำหนดขั้นตอนเพื่อตรวจจับสิ่งผิดปกติ (Detect) 4) การตอบสนองเมื่อเกิดสถานการณ์ผิดปกติ (Respond) และ 5) การฟื้นฟูหลังเกิดเหตุการณ์เพื่อให้สถานการณ์กลับมาสู่ปกติ (Recovery) ตามรูปที่ 3 [7]



รูปที่ 3 กรอบการรักษาความมั่นคงทางไซเบอร์ NIST

2.4.2 มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 เป็นมาตรฐานที่ให้ความสำคัญในการบริหารจัดการด้านความมั่นคงปลอดภัย 3 ส่วน ได้แก่ 1) การปกป้องระบบสารสนเทศให้เข้าถึงได้เฉพาะผู้มีสิทธิ์ 2) การป้องกันความถูกต้องของสารสนเทศไม่ให้ถูกเปลี่ยนแปลงแก้ไขให้ผิดไปจากความจริง และ 3) การปกป้อง

ความพร้อมใช้งานของระบบสารสนเทศไม่ให้เกิดการหยุดชะงักซึ่งส่งผลกระทบต่อธุรกิจ [8]

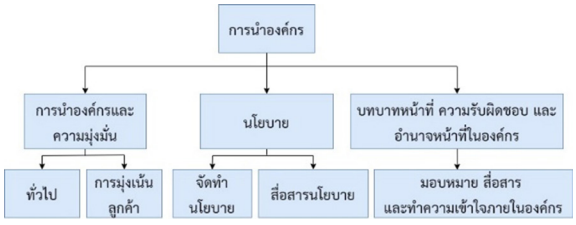
2.4.3 CIS Control 7.1 เป็นแนวทางปฏิบัติที่ดีที่ช่วยลดการโจมตีระบบและเครือข่าย ประกอบด้วย 20 วิธีการในการควบคุมความมั่นคงปลอดภัย [9]

2.4.4 มาตรฐานความมั่นคงปลอดภัยสำหรับอุสาหกรรมอัตโนมัติและการควบคุมระบบ ANSI/ISA-62443-2-1-2009 มี 3 องค์ประกอบหลัก ได้แก่ 1) การวิเคราะห์ความเสี่ยง 2) การจัดการความเสี่ยงด้วย CSMS และ 3) การตรวจติดตามและปรับปรุง CSMS [10]

2.4.5 NIST Special Publication 800-53 Revision 4 เป็นรายการควบคุมความปลอดภัยและความเป็นส่วนตัวในระบบข้อมูลของรัฐบาลกลางสหรัฐฯ ประกอบด้วยควบคุมความปลอดภัย 18 ด้าน [11]

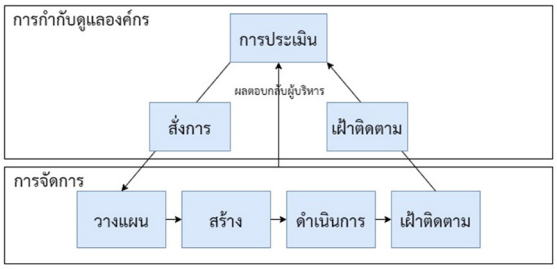
2.5 กรอบการนำองค์กรและกำกับดูแลสำหรับผู้นำ

2.5.1 ระบบบริหารงานคุณภาพ ISO 9001:2015 เป็นมาตรฐานระบบการจัดการคุณภาพประกอบด้วย 8 หลักการ โดยมีการนำองค์กร (Leadership) อยู่ในหลักการที่ 5 ของมาตรฐานระบบการจัดการคุณภาพ โดยผู้นำมีบทบาทหลัก ได้แก่ การนำองค์กร การกำหนดนโยบาย และการกำหนดบทบาทหน้าที่ความรับผิดชอบภายในองค์กรตามรูปที่ 4 [12]



รูปที่ 4 บทบาทการนำองค์กรของผู้นำ ISO 9001:2015

2.5.2 กรอบการดำเนินธุรกิจในการกำกับดูแล IT ในองค์กร COBIT5 เป็นกรอบการดำเนินงานในการกำกับดูแล IT ระดับองค์กร โดยการกำกับดูแลนั้นมี 3 ส่วนได้แก่ การสั่งการ การติดตาม และการประเมิน ตามรูปที่ 5 [13]



รูปที่ 5 การกำกับดูแลและจัดการองค์กร COBIT5

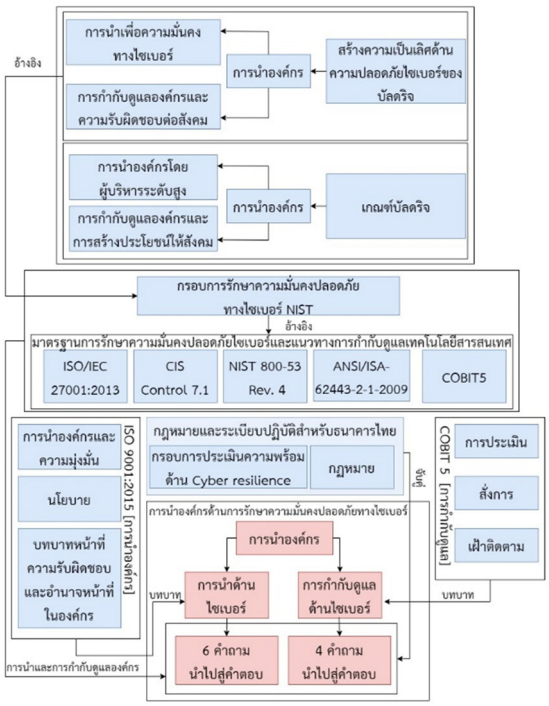
2.6 วิธีการดำเนินงานวิจัย

งานวิจัยนี้ใช้ระเบียบวิธีการวิจัยแบบ Systematic Literature Review ที่เสนอโดย Snyder 2019 [18] ประกอบด้วย 3 ส่วน ได้แก่

2.6.1 การออกแบบ

กำหนดประเภทบทความวิจัย มาตรฐานด้านการรักษาความมั่นคงทางไซเบอร์ บทบาทการนำองค์กรและการกำกับดูแลของผู้บริหารระดับสูง กฎระเบียบของธนาคารและกฎหมาย ที่สมควรทบทวนโดยคำนึงถึงประโยชน์ที่ได้รับจากการทบทวน และความสอดคล้องกับวัตถุประสงค์งานวิจัย โดยเริ่มจาก Baldrige Cybersecurity Excellence Builder ซึ่งเป็นฐานของงานวิจัย ที่ชี้ให้เห็นส่วนประกอบของการนำองค์กรและการกำกับดูแลด้านความมั่นคงทางไซเบอร์ แนวทางการรักษาความมั่นคงทางไซเบอร์ของ NIST แนวทางการกำกับดูแลเทคโนโลยีสารสนเทศ COBIT5 และมาตรฐานด้านความมั่นคงทางไซเบอร์ 4 มาตรฐาน เป็นวิธีการในการนำองค์กรด้านการรักษาความมั่นคงทางไซเบอร์ ที่งานวิจัยนี้นำมาสังเคราะห์และคัดเลือกมาเป็น วิธีการปฏิบัติ มาตรฐานระบบบริหารงานคุณภาพ ISO 9001:2015 ใช้ในการกำหนดบทบาทหน้าที่ในการนำองค์กร และใช้แนวทางการกำกับดูแลเทคโนโลยีสารสนเทศ COBIT5 ใช้สำหรับกำหนดบทบาทหน้าที่ในการกำกับดูแลของผู้นำองค์กร นอกจากนี้ยังใช้ระเบียบปฏิบัติของธนาคารแห่งประเทศไทย (Cyber Resilience) และกฎหมายที่เกี่ยวข้องด้านการรักษาความมั่นคงทางไซเบอร์ ระบุลงในวิธีการปฏิบัติ เพื่อให้มั่นใจได้ว่าวิธีการที่คัดเลือกมาจากมาตรฐานการรักษาความมั่นคงทาง

ไซเบอร์สอดคล้องกับระเบียบและกฎหมายของธนาคารในประเทศไทยโดยมีรายละเอียดการออกแบบดังแสดงในรูปที่ 6



รูปที่ 6 การสังเคราะห์แนวทางในการนำองค์กรด้านการรักษาความมั่นคงทางไซเบอร์ที่ครอบคลุมมาตรฐาน แนวทางปฏิบัติ ระเบียบ และกฎหมายที่เกี่ยวข้อง

2.6.2 ดำเนินการทบทวนและคัดเลือก

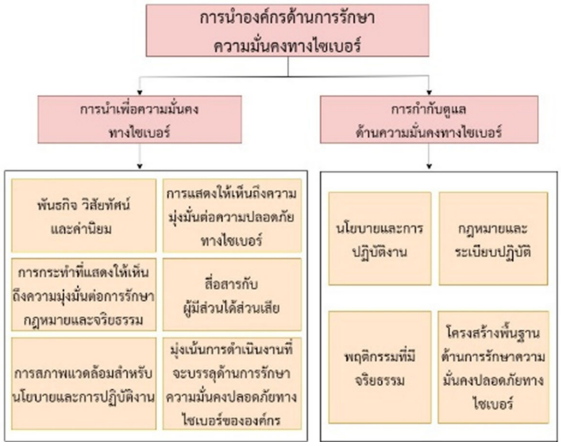
ทบทวนความเหมาะสมและความน่าเชื่อถือ โดยทบทวนจาก การเป็นมาตรฐานความมั่นคงทางไซเบอร์ ที่เป็นมาตรฐานสากล บทบาทการนำองค์กรและการกำกับดูแลที่มีการใช้งานอย่างแพร่หลาย ระเบียบปฏิบัติของธนาคารที่มีออกโดยธนาคารแห่งประเทศไทย และกฎหมายที่ประกาศโดยรัฐบาล และคัดเลือกเพื่อใช้ในการวิเคราะห์ต่อไป

2.6.3 การวิเคราะห์

จากข้อมูลที่ได้รับเลือกถูกนำมาวิเคราะห์ให้ได้วิธีการปฏิบัติด้านความมั่นทางไซเบอร์ตามแนวทางของแนวทางของ Baldrige Cybersecurity Excellence Builder โดยสังเคราะห์วิธีการปฏิบัติจากมาตรฐานต่าง ๆ ที่เลือกไว้ โดยวิธีการปฏิบัตินั้นต้องเหมาะสมและมีประสิทธิผลสำหรับบทบาทหน้าที่ในการนำองค์กรและกำกับดูแลของผู้บริหารระดับสูงของธนาคาร รวมทั้งสอดคล้องกับระเบียบปฏิบัติของธนาคารแห่งประเทศไทย และกฎหมาย ที่เกี่ยวข้องกับธนาคาร

3. ผลการทดลอง

การนำองค์กรในด้านการรักษาความมั่นคงทางไซเบอร์ในธนาคาร ประกอบด้วยแนวทางสำคัญ สองประการ ได้แก่ การนำองค์กร (Leading) และ การกำกับดูแล (Governance) โดยการนำองค์กรประกอบด้วย 6 เรื่อง ได้แก่ การกำหนดภารกิจ วิสัยทัศน์ และค่านิยมองค์กร การปฏิบัติตนเพื่อแสดงถึงความมุ่งมั่นด้านการรักษาความมั่นคงทางไซเบอร์ การปฏิบัติตนเพื่อแสดงถึงความมุ่งมั่นด้านกฎหมายและจริยธรรม การสื่อสารกับผู้มีส่วนได้ส่วนเสีย การสร้างสภาพแวดล้อมเพื่อบรรลุผลต่อนโยบายด้านความมั่นคงทางไซเบอร์ และการมุ่งเน้นเพื่อบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์ และการกำกับดูแล ประกอบด้วย 4 เรื่อง ได้แก่ การกำกับดูแลด้านนโยบายและการดำเนินการ การกำกับดูแลด้านกฎหมายและระเบียบปฏิบัติ การกำกับดูแลด้านพฤติกรรมที่มีจริยธรรม และการกำกับดูแลด้านโครงสร้างพื้นฐานการรักษาความมั่นคงทางไซเบอร์ ดังแสดงในรูปที่ 7



รูปที่ 7 วิธีการปฏิบัติตามแนวทางในการนำองค์กรด้านความมั่นคงทางไซเบอร์ที่สังเคราะห์ขึ้นตามรูปที่ 6

วิธีปฏิบัติการนำองค์กรด้านความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงสำหรับธนาคารไทยมีสัญลักษณ์และความหมายประกอบดังแสดงในตารางที่ 4

ตารางที่ 4 สัญลักษณ์และความหมายประกอบ

สัญลักษณ์	ตัวอย่าง	ความหมาย/คำนิยาม
R	R[2.1]	กรอบการประเมินความพร้อมด้าน Cyber resilience ข้อที่ 2.1
§	[§76]	ใช้ระบุมาตรากฎหมาย มาตรา 76
L1	L1[§52]	พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 มาตรา 52
L2	L2[§72]	พ.ร.บ.คุมครองข้อมูลส่วนบุคคล 2562 มาตรา 72

การนำองค์กรของผู้บริหารระดับสูงของธนาคารมี 6 เรื่อง แต่ละเรื่องมีวิธีปฏิบัติในการนำองค์กรด้านความมั่นคงทางไซเบอร์ดังต่อไปนี้

3.1 วิธีปฏิบัติเพื่อกำหนดภารกิจ วิสัยทัศน์ และค่านิยม

วิธีปฏิบัติเพื่อกำหนดภารกิจ วิสัยทัศน์และค่านิยมธนาคารที่เกี่ยวกับรักษาความมั่นคงทางไซเบอร์ที่ส่งผลครอบคลุมไปถึงผู้มีส่วนได้ส่วนเสียทั้งหมดมีวิธีปฏิบัติดังแสดงในตารางที่ 5

ตารางที่ 5 วิธีปฏิบัติการกำหนด ภารกิจ วิสัยทัศน์ และค่านิยม

R[1.2.1] กำหนดให้มีกลยุทธ์ด้านการรักษาความมั่นคงทางไซเบอร์สอดคล้องกับกลยุทธ์ธุรกิจของธนาคาร ID.BE-1: COBIT5 APO08.01, ID.BE-3: COBIT5 APO02.01	L1[§44], R[1.2.2, 6.1-6.3] กำหนดนโยบายการรักษาความมั่นคงทางไซเบอร์สำหรับห่วงโซ่อุปทานของธนาคาร ID.BE-1: NIST SP 800-53r4 SA-12, ISO/IEC 27001:2013 A.15.1, ID.BE-4: COBIT5 APO10.01
L1[§44(1)], R[2.1-2.2] ชี้นำให้มีการระบุความเสี่ยงด้านความมั่นคงทางไซเบอร์ของธุรกิจและห่วงโซ่อุปทานของธนาคาร ID.BE-1: APO08.04, APO10.04, ID.BE-3: INST SP 800-53r4 PM-11	L1[§44(1)], R[2.1-2.2] ชี้นำให้มีการจัดลำดับความสำคัญของระบบเพื่อระบุความเสี่ยงด้านความมั่นคงทางไซเบอร์ของธนาคาร ID.BE-3: ISA 62443-2-1:2009 4.2.3.6
R[6.1-6.3] ชี้นำให้มีการระบุข้อตกลงการให้บริการในการรักษาความมั่นคงทางไซเบอร์กับผู้ให้บริการของธนาคาร ID.BE-1: COBIT 5 APO10.03, ISO/IEC 27001:2013 A.15.1.3	

3.2 วิธีปฏิบัติตนเพื่อแสดงให้เห็นถึงความมุ่งมั่นในการรักษาความมั่นคงทางไซเบอร์

วิธีปฏิบัติตนเพื่อแสดงถึงความมุ่งมั่นในการรักษาความมั่นคงทางไซเบอร์อย่างจริงจังสำหรับผู้บริหารระดับสูงของธนาคารมีวิธีปฏิบัติดังแสดงในตารางที่ 6

ตารางที่ 6 วิธีปฏิบัติตนเพื่อแสดงให้เห็นถึงความมุ่งมั่นในการรักษาความมั่นคงทางไซเบอร์

มีบทบาทในการนำเพื่อกำหนดสถาปัตยกรรมองค์กรในรักษาความมั่นคงทางไซเบอร์ให้เป็นไปในแนวทางเดียวกับกลยุทธ์ทางธุรกิจของธนาคาร ID.BE-2: COBIT5 APO03.01	R[4.3.2.10, 5.1.1.5] ชี้นำให้เห็นปัจจัยภายในและภายนอกธนาคารที่มีผลกระทบต่อความมั่นคงทางไซเบอร์ ID.BE-2: ISO/IEC 27001:2013 Clause 4.1
แสดงความโปร่งใสในการจัดการกลยุทธ์ด้านการรักษาความมั่นคงทางไซเบอร์ของธนาคาร ID.BE-2: COBIT5 APO02.06	

3.3 วิธีปฏิบัติเพื่อแสดงให้เห็นถึงความมุ่งมั่นต่อพฤติกรรมทางกฎหมายและจริยธรรม

วิธีปฏิบัติเพื่อแสดงให้เห็นความมุ่งมั่นต่อการปฏิบัติตามกฎหมายและจริยธรรมความมั่นคงทางไซเบอร์อย่างเข้มงวดสำหรับผู้บริหารระดับสูงของธนาคารมีวิธีปฏิบัติดังแสดงในตารางที่ 7 และตารางที่ 8

ตารางที่ 7 วิธีปฏิบัติเพื่อแสดงให้เห็นถึงความมุ่งมั่นต่อพฤติกรรมทางกฎหมายและจริยธรรม

R[6.1.1.6] สั่งการและเฝ้าติดตามให้มีนโยบายความพร้อมใช้งานและขีดความสามารถด้านความมั่นคงทางไซเบอร์ให้เป็นไปตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมาย ID.BE-4: COBIT5 BAI04.02	R[2.1] สั่งการและเฝ้าติดตามให้มีนโยบายบริหารจัดการความเสี่ยงของทรัพย์สินสารสนเทศให้เป็นไปตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมาย ID.BE-4: COBIT5 BAI09.02
L1[§45, 56], R[5.1.1-5.1.2] สั่งการและเฝ้าติดตามให้มีการจัดการความต่อเนื่องที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ให้เป็นไปตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมาย ID.BE-4: COBIT5 DSS04.02	L1[§45, 54], R[5.2] สั่งการและเฝ้าติดตามให้มีการบริหารจัดการกระบวนการแก้ปัญหาด้านความมั่นคงทางไซเบอร์ให้เป็นไปตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมาย ID.BE-4: COBIT5 BAI03.02

ตารางที่ 8 วิธีปฏิบัติเพื่อแสดงให้เห็นถึงความมุ่งมั่นต่อพฤติกรรมทางกฎหมายและจริยธรรม (ต่อ)

L1[§54], R[1.3]	L1[§45, 54, 56], R[1.3.1.2]
สั่งการให้มีการบริหารจัดการความเสี่ยงจากเหตุการณ์ผิดปกติด้านความมั่นคงทางไซเบอร์ตามระเบียบปฏิบัติของหน่วยงานกำกับดูแลธนาคารและกฎหมาย	สั่งการให้มีการ ติดตาม วัดผลประเมินการปฏิบัติตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมายในรักษาความมั่นคงทางไซเบอร์
RC.CO-1: COBIT 5 EDM03.02	RC.CO-2: COBIT 5 MEA03.02

3.4 วิธีปฏิบัติในการสื่อสารและสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสีย

วิธีปฏิบัติในการสื่อสารและการสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสียสำหรับผู้บริหารระดับสูงของธนาคารมีวิธีปฏิบัติดังแสดงในตารางที่ 9

ตารางที่ 9 วิธีปฏิบัติในการสื่อสารและสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสีย

L1[§52, 54, 57, 58, 73], L2[§76], R[1.2.2.4, 4.4.4]	R[1.2.2.4, 4.4.4]
กำหนดให้มีหลักเกณฑ์การสื่อสารระหว่างผู้นำระดับสูงกับทีมงานขององค์กร และผู้มีส่วนได้ส่วนเสียภายนอกองค์กรเมื่อเกิดเหตุการณ์ผิดปกติด้านความมั่นคงทางไซเบอร์	กำหนดให้มีการติดต่อสื่อสารกับกลุ่มเฉพาะด้านการรักษาความมั่นคงทางไซเบอร์ เพื่อแลกเปลี่ยนข้อมูลและความรู้เมื่อเกิดเหตุการณ์ผิดปกติ
RC.CO-1 - RC.CO-3: ISO/IEC 27001:2013 Clause 7.4	RC.CO-1: ISO/IEC 27001:2013 A.6.1.4
R[5.3]	L1[§42(2), 44(2), 45], R[5.1.3.3]
สั่งการให้มีการสื่อสารแผนฉุกเฉินไปยังผู้มีส่วนได้ส่วนเสียของธนาคารเมื่อเกิดเหตุการณ์ผิดปกติด้านความมั่นคงทางไซเบอร์	สั่งการให้มีการประสานงานเพื่อรับมือเหตุการณ์ด้านความมั่นคงทางไซเบอร์ไปยังผู้มีส่วนเกี่ยวข้องเมื่อเกิดเหตุผิดปกติ
RC.CO-3: NIST SP 800-53r4 CP-2	RC.CO-3: NIST SP 800-53r4 IR-4

3.5 วิธีปฏิบัติในการสร้างสภาพแวดล้อมด้านความมั่นคงทางไซเบอร์

วิธีปฏิบัติในการสร้างสภาพแวดล้อมเพื่อให้การดำเนินงานบรรลุผลตามนโยบายด้านความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงของธนาคารมีวิธีปฏิบัติดังแสดงในตารางที่ 10

ตารางที่ 10 วิธีปฏิบัติในการสร้างสภาพแวดล้อมด้านความมั่นคงทางไซเบอร์

L1[§42(3), 44], R[1.1.2.1, 3.1]	L1[§45], R[1.2.2.4, 1.2.2.6, 1.4.1.6, 4.4]
กำหนดให้มีแผนการรักษาความมั่นคงทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญของธนาคาร	กำหนดให้มีมาตรการป้องกันภัยคุกคามด้านความมั่นคงทางไซเบอร์จากภายนอกธนาคาร
ID.BE-2: NIST SP 800-53r4 PM-8	ID.BE-5: ISO/IEC 27001:2013 A.11.1.4
R[2.2.1.1, 2.2.1.4, 3.1.1.12, 3.2.4.2, 3.2.5.1, 3.2.6.2, 4.3.1.5, 6.1.1.2]	กำหนดให้มีการติดตาม ปรับปรุงและประมาณการสมรรถนะของทรัพยากรด้านความมั่นคงทางไซเบอร์ของธนาคารเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ
กำหนดให้มีมาตรการการวิเคราะห์ภาวะวิกฤตด้านความมั่นคงทางไซเบอร์เพื่อจัดการความเสี่ยงในห่วงโซ่อุปทานของธนาคาร	ID.BE-4: ISO/IEC 27001:2013 A.11.2.2
ID.BE-4: INST SP 800-53r4 SA-14	
กำหนดให้มีมาตรการป้องกันไฟฟ้า สายไฟและสายสื่อสารเพื่อป้องกันการสกัดกั้น การรบกวน และการสร้างความเสียหายแก่การให้บริการ และข้อมูลสารสนเทศของธนาคาร	กำหนดให้มีทางเลือกสำรองด้านโทรคมนาคม และแหล่งจ่ายไฟฉุกเฉินสำหรับโครงสร้างพื้นฐานสำคัญของธนาคาร
ID.BE-4: ISO/IEC 27001:2013 A.11.2.3, NIST SP 800-53r4 PE-9	ID.BE-4: NIST SP 800-53r4 CP-8, CP-11, PE-11
กำหนดให้มีมาตรการป้องกันอุปกรณ์ IT ที่มีความสำคัญต่อธุรกิจจากความล้มเหลวในการจ่ายพลังงานไฟฟ้าและสาเหตุภัยคุกคามทางไซเบอร์อื่น ๆ ที่ส่งผลต่อการหยุดให้บริการของธนาคาร	
ID.BE-4: ISO/IEC 27001:2013 A.11.2.2	

3.6 วิธีปฏิบัติเพื่อมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์

วิธีปฏิบัติเพื่อมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงของธนาคารมีวิธีปฏิบัติดังแสดงในตารางที่ 11

ตารางที่ 11 วิธีปฏิบัติเพื่อมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์

R[6.3] กำหนดให้มีการติดตามและทบทวนการให้บริการของผู้ให้บริการด้านการรักษาความมั่นคงทางไซเบอร์ ID.BE-1: ISO/IEC 27001:2013 A.15.2.1	R[5.1.2.4-5.1.2.6, 5.1.2.8, 6.3.17] กำหนดให้ติดตามและประเมินความพร้อมใช้งานของการประมวลผลข้อมูลสารสนเทศ ID.BE-5: ISO/IEC 27001:2013 A.17.1.2, A.17.2.1
L1[§42(2), 44(2), 45], R[5.1.1] กำหนดให้มีแผนฉุกเฉินสำหรับระบบสารสนเทศ เพื่อฟื้นฟูระบบในสถานการณ์ไม่พึงประสงค์ ID.BE-1, ID.BE-5: NIST SP 800-53r4 CP-2	L1[§42(2), 44(2), 45], R[5.1.1] กำหนดให้มีแผนความต่อเนื่องในการบริหารจัดการ การรักษาความมั่นคงสารสนเทศในสถานการณ์ไม่พึงประสงค์ ID.BE-5: ISO/IEC 27001:2013 A.17.1.1

4. อภิปรายผลและสรุป

4.1 อภิปรายผล

บทบาทของผู้บริหารระดับสูงของธนาคารมีสองส่วน ได้แก่ การนำองค์กรและกำกับดูแลด้านความมั่นคงทางไซเบอร์ ในงานวิจัยนี้มุ่งเน้นเฉพาะด้านการนำองค์กร เนื่องจากส่วนของการกำกับดูแลด้านความมั่นคงทางไซเบอร์นั้นปรากฏเป็นรูปธรรมในหลากหลายรูปแบบและเป็นที่รู้จักกันอย่างแพร่หลายในกลุ่มผู้บริหารระดับสูงของธนาคาร เช่น คู่มือปฏิบัติของธนาคาร ดังนั้นงานวิจัยนี้จึงเสนอวิธีปฏิบัติในการนำองค์กรในการรักษาความมั่นคงทางไซเบอร์สำหรับผู้บริหารระดับสูงของธนาคารโดยใช้แนวทางของ Baldrige Cybersecurity Excellence Builder เป็นฐานสำหรับวิธีปฏิบัติ โดยเลือกแนวทางดำเนินการและมาตรฐานสากลในการรักษาความมั่นคงทางไซเบอร์ ได้แก่ NIST Cybersecurity Framework ISO/IEC 27001:2013 CIS Control 7.1 ANSI/ISA-62443-2-1 2009 NIST 800-53 Revision 4 COBIT 5 และ ISO 9001:2015 เป็นวิธีปฏิบัติในการนำองค์กรตามแนวทางของ Baldrige ที่สอดคล้องกับระเบียบปฏิบัติและกฎหมายไทย โดยกรอบการนำองค์กรในการรักษาความมั่นคงทางไซเบอร์ประกอบด้วย 6 แนวทาง การนำองค์กรสำคัญได้แก่ การกำหนดภารกิจ วิสัยทัศน์ และค่านิยมที่เกี่ยวกับรักษาความมั่นคงทางไซเบอร์ที่ส่งผลครอบคลุมไปถึงผู้มีส่วนได้ส่วนเสียทั้งหมด การปฏิบัติตนให้แสดงถึงความมุ่งมั่นในการรักษาความมั่นคงทางด้านไซเบอร์อย่างจริงจัง การแสดงให้เห็นความมุ่งมั่นต่อการปฏิบัติตามกฎหมายและจริยธรรมความมั่นคงทางไซเบอร์อย่างเข้มงวด การสื่อสารและการสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสีย การสร้างสภาพแวดล้อมเพื่อให้การดำเนินงานบรรลุผลตามนโยบายด้านความมั่นคงทางไซเบอร์ และการมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์

Baldrige Cybersecurity Excellence Builder ให้แนวทางเพื่อประเมินประสิทธิผลของผู้นำในการรักษาความมั่นคงทางไซเบอร์แต่ไม่ระบุวิธีการปฏิบัติ ในขณะที่มาตรฐานการรักษาความมั่นคงทางไซเบอร์ต่าง ๆ นั้น คือ กรอบในการกำหนดวิธีการปฏิบัติแต่ไม่ระบุถึงแนวทางการนำองค์กรที่เป็นบทบาทของผู้นำ ดังนั้นในงานวิจัยนี้จึงเป็นการบูรณาการระหว่างแนวทางในการนำองค์กรที่เป็นบทบาทของผู้นำเข้ากับวิธีการปฏิบัติโดยใช้แนวทางการนำองค์กรจาก Baldrige Cybersecurity Excellence Builder และ ใช้วิธีปฏิบัติจากมาตรฐานการรักษาความมั่นคงทางไซเบอร์สากล ในงานวิจัยนี้ได้มีการเลือกวิธีปฏิบัติจากมาตรฐานการรักษาความมั่นคงทางไซเบอร์ที่เกี่ยวข้องและสอดคล้องกับการนำองค์กรตามแนวทางของ Baldrige รวมทั้งพิจารณาความสอดคล้องกับระเบียบปฏิบัติของธนาคารแห่งประเทศไทย ในส่วนของกรอบการประเมินความพร้อมด้าน Cyber Resilience และกฎหมายการรักษาความมั่นคงทางไซเบอร์ที่เกี่ยวข้องกับกิจการธนาคาร ได้แก่ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาเป็นวิธีปฏิบัติในการนำองค์กรด้านการรักษาความมั่นคงทางไซเบอร์ของผู้บริหารระดับสูง

ผู้บริหารระดับสูง (Executive Level) ของธนาคารสามารถใช้วิธีปฏิบัติในการนำองค์กรเพื่อรักษาความมั่นคงทางไซเบอร์เป็นแนวทางปฏิบัติได้ดังต่อไปนี้

1) ผู้บริหารระดับสูงของธนาคารกำหนดภารกิจ วิสัยทัศน์ และค่านิยมที่เกี่ยวกับรักษาความมั่นคงทางไซเบอร์ที่ส่งผลครอบคลุมไปถึงผู้มีส่วนได้ส่วนเสียทั้งหมด โดย กำหนดนโยบายการรักษาความมั่นคงทางไซเบอร์สำหรับห่วงโซ่อุปทานของธนาคาร เพื่อลดความสูญเสียจากการทุจริตของพนักงานที่ถือว่าเป็นส่วนหนึ่งของภัยคุกคามทางไซเบอร์ประเภท การทุจริตภายในองค์กร (Internal fraud) [2] หรือเป็นภัยคุคามภายใน (Insider threat) [1]

2) ผู้บริหารระดับสูงของธนาคารแสดงถึงความมุ่งมั่นในการรักษาความมั่นคงทางด้านไซเบอร์อย่างจริงจัง โดยชี้นำให้เห็นปัจจัยภายในและภายนอกธนาคารที่มีผลกระทบต่อความมั่นคงทางไซเบอร์ เช่น ชี้นำให้เห็นถึงความสำคัญของการเก็บรักษาข้อมูลส่วนตัวเพื่อป้องกันภัยคุกคามจากการถูกขโมยข้อมูลส่วนตัว (User Credential Compromise) ที่สามารถเชื่อมโยงในการเข้าถึงระบบสำคัญและสร้างความสูญเสียต่อธนาคาร [1]

3) ผู้บริหารระดับสูงของธนาคารสามารถแสดงให้เห็นความมุ่งมั่นต่อการปฏิบัติตามกฎหมายและจริยธรรมความมั่นคงทางไซเบอร์อย่างเข้มงวด โดยสั่งการและเฝ้าติดตามให้มีการจัดการความต่อเนื่องที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ให้เป็นไปตามระเบียบของหน่วยงานกำกับดูแลธนาคารและกฎหมาย เพื่อลดความสูญเสียจากการหยุดให้บริการจากเทคโนโลยีและโครงสร้างพื้นฐาน (Technology & Infrastructure) ซึ่งถือเป็นภัยคุกคามทางไซเบอร์ [2] รวมทั้งเป็นการปฏิบัติตามระเบียบและกฎหมายของธนาคารไทย [14] และ [15]

4) ผู้บริหารระดับสูงของธนาคารสื่อสารและการสร้างความผูกพันกับผู้มีส่วนได้ส่วนเสีย โดยกำหนดให้มีการติดต่อสื่อสารกับกลุ่มเฉพาะด้านการรักษาความมั่นคงทางไซเบอร์เพื่อแลกเปลี่ยนข้อมูล และความรู้เมื่อเกิดเหตุการณ์ผิดปกติเพื่อถอดบทเรียนในการเฝ้าระวังป้องกัน รวมทั้งลดความสูญเสียจากเหตุการณ์ โดยเฉพาะเหตุการณ์ทางไซเบอร์ที่เกิดจากการบุกรุก (Intrusions) เข้าสู่ระบบของธนาคาร [3] จากกลุ่ม Hacker ภายนอก (External Fraud) [2] การได้มาซึ่งข้อมูลของกลุ่ม Hacker สามารถช่วยในการเฝ้าระวังและป้องกันได้อย่างมีประสิทธิภาพ

5) ผู้บริหารระดับสูงของธนาคารสร้างสภาพแวดล้อมเพื่อให้การดำเนินงานบรรลุผลตามนโยบายด้านความมั่นคงทางไซเบอร์ โดยกำหนดให้มีมาตรการป้องกันภัยคุกคามด้านความมั่นคงทางไซเบอร์จากภายนอกธนาคาร เพื่อลดความสูญเสียจากภัยคุกคามทางไซเบอร์ ที่ใช้ข้อบกพร่องในมาตรการรักษาความปลอดภัย (Flaws in Security Measures) [1] ในการบุกรุกระบบสำคัญของธนาคาร [3]

6) ผู้บริหารระดับสูงของธนาคารมุ่งเน้นให้การดำเนินการของธนาคารบรรลุวัตถุประสงค์ด้านความมั่นคงทางไซเบอร์ โดยกำหนดให้มีแผนความต่อเนื่องในการบริหารจัดการ การรักษาความมั่นคงปลอดภัยสารสนเทศในสถานการณ์ไม่พึงประสงค์ของธนาคาร เพื่อเฝ้าระวังและติดตามภัยคุกคามทางไซเบอร์ที่พร้อมจะโจมตีและสร้างความเสียหายให้กับธนาคารได้ตลอดเวลาเช่น ภัยคุกคามจากมัลแวร์ [1] และการบุกรุก [3] จากภัยคุกคามภายนอก [2] งานวิจัยนี้มีความคล้ายกับ Toward Cybersecurity Leadership Framework [19] ที่ นำเสนอลักษณะของผู้นำที่เหมาะสมในการนำองค์กรเพื่อรักษาความมั่นคงทางไซเบอร์ใน 5 ฟังก์ชันของ NIST Cybersecurity Framework เช่น ผู้นำที่มีลักษณะผู้รับใช้ (Servant Leadership) เหมาะสมในการนำองค์กรในฟังก์ชัน Identify (การระบุ) และ Recover (การฟื้นฟู) ส่วนผู้นำที่มีความยืดหยุ่น (Resilient Leader) เหมาะสมในการนำองค์กรในฟังก์ชัน Respond (การตอบสนอง) แต่ไม่มีวิธีปฏิบัติสำหรับผู้นำ งานวิจัยนี้จึงนำเสนอวิธีการการนำองค์กรด้านความมั่นคงทางไซเบอร์ของผู้บริหารระดับสูงที่ผู้บริหารระดับสูงสำหรับธนาคารนำไปปฏิบัติได้ รวมทั้งระบุชัดเจนว่าวิธีการปฏิบัตินั้นสอดคล้องกับกฎหมายและระเบียบปฏิบัติในเรื่องใดบ้าง

งานวิจัยนี้เป็นงานวิจัยเชิงไม่ประจักษ์ (Nonempirical Research) ซึ่งเป็นการวิจัยที่หาความจริงจากข้อมูลเอกสารที่มีความแตกต่างจากงานวิจัยเชิงประจักษ์ (Empirical Research) ที่ใช้การเก็บข้อมูลปฐมภูมิในการวิเคราะห์เช่น การเก็บข้อมูลจากการสัมภาษณ์ผู้เชี่ยวชาญ ดังนั้นงานวิจัยนี้เป็นการสังเคราะห์วิธีการปฏิบัติของผู้บริหารระดับสูง โดยไม่ใช้

ความคิดเห็นจากผู้เชี่ยวชาญ แต่สังเคราะห์ขึ้นจากข้อมูลที่ได้มีการทบทวนก่อนการตีพิมพ์ (Peer Review) โดยมุ่งหมายให้เป็นการลดทอนความลำเอียงจากความคิดเห็นในแต่ละปัจเจกบุคคล

นอกเหนือจากประเด็นการนำองค์กรของผู้บริหารระดับสูงแล้วงานวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงทางไซเบอร์ในกิจการธนาคาร ควรมีการศึกษาปัจจัยอื่นที่เกี่ยวของกับการรักษาความมั่นคงทางไซเบอร์เพิ่มเติม อาทิ บริบทองค์กร บริบทลูกค้า และการวัดประสิทธิผลในการรักษาความมั่นคงทางไซเบอร์ ซึ่งอาจใช้แนวทางของ Baldrige Cybersecurity Excellence Builder เป็นกรอบในการวิจัยเพื่อให้เกิดประสิทธิผลเพิ่มมากขึ้นในการรักษาความมั่นคงทางไซเบอร์สำหรับกิจการธนาคาร

4.2 สรุป

การนำองค์กรด้านความมั่นคงทางไซเบอร์ของผู้บริหารระดับสูงสำหรับธนาคารไทยใช้แนวทางของ Baldrige Cybersecurity Excellence Builder เป็นพื้นฐาน และเลือกใช้วิธีปฏิบัติจากมาตรฐานการรักษาความมั่นคงทางไซเบอร์สากล โดยสอดคล้องกับระเบียบปฏิบัติของธนาคาร และกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงทางไซเบอร์ที่ได้จากงานวิจัยนี้ ผู้บริหารระดับสูง (Executive Level) ของธนาคารสามารถใช้ปฏิบัติในการนำองค์กรด้านความมั่นคงทางไซเบอร์ เพื่อลดความสูญเสียจากเหตุการณ์ภัยคุกคามทางไซเบอร์ของธนาคาร รวมทั้งยังทำให้การดำเนินงานของธนาคารสอดคล้องกับระเบียบปฏิบัติของ ธนาคารแห่งประเทศไทย และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งอาจส่งผลให้ประสบความสำเร็จในการรักษาความมั่นคงทางไซเบอร์ในการดำเนินงานของธนาคารทั้งในปัจจุบันและอนาคต

เอกสารอ้างอิง

[1] X. M. Liu, "A risk-based approach to cybersecurity: A case study of financial messaging networks data breaches," *The Coastal Business Journal*, vol. 18, no. 1, pp. 21–38, 2021.

[2] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach. (2020, Feb.). *BIS Working Papers No 840: Operational and cyber risks in the financial sector* [Online]. Available: https://www.bis.org/publ/work840.pdf

[3] ETDA. (2019). 2017–2018 ThaiCERT Annual Report. (2nd ed.). Electronic Transactions Development Agency. Bangkok, Thailand. [Online](in Thai). Available: https://www.etda.or.th/th/Useful-Resource/documents-for-download/ThaiCERT-Annual-Report-2017-2018-Thai-Version.aspx

[4] H. Melissa "Leadership and responsibility for cybersecurity,"*Georgetown Journal of International Affairs*, Special Issue on International Engagement on Cyber 2012: Establishing Norms and Improving Security, pp. 71–80, 2012.

[5] *2019–2020 Baldrige Excellence Framework: Proven Leadership and Management Practices for High Performance*, National Institute of Standards and Technology, 2019.

[6] NIST. (2019). Baldrige Cybersecurity Excellence Builder: Key questions for improving your organization's cybersecurity performance Version 1.1. [Online]. Available: https://www.nist.gov/document/baldrige-cybersecurity-excellence-builder-v11pdf

[7] NIST. (2018, April 16). Framework for improving critical infrastructure cybersecurity Version 1.1 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[8] International Organization for Standardization

ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements, 2013.

[9] *Critical Security Controls V7.1*, 2019.

[10] *Security for industrial automation and control systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program*, ANSI/ISA-62443-2-1 (99.02.01), 2009.

[11] *NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations*, 2013.

[12] *International Organization for Standardization ISO 9001 Quality management system – Requirements*, 2015.

[13] *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT (ISACA)*, 2012.

[14] Bank of Thailand. (2021, December 30). *Cyber Resilience Assessment Framework*. [Online]. (in Thai). Available: https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%20resilience%20framework%202019.pdf

[15] Thailand government, "Cybersecurity Act, B.E. 2562," 2019 (in Thai).

[16] Thailand government, "Personal Data Protection Act, B.E. 2562," 2019 (in Thai).

[17] NIST. (2022, March). *Three Organizations Win 2021 Baldrige Awards for Performance Excellence*. [Online]. Available: https://www.nist.gov/news-events/news/2022/03/three-organizations-win-2021-baldrige-awards-performance-excellence

[18] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333–339, 2019.

[19] S. Cleveland and M. Cleveland, "Toward cybersecurity leadership framework," in *MWAIS 2018 Proceedings*, Saint Louis, Missouri, 2018, pp. 1–5.