บทที่ 4
ผลการวิจัย

การศึกษาและวิจัยในครั้งนี้เป็นการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม โดยการศึกษาผู้วิจัยได้กำหนดให้มีวัตถุประสงค์หลัก 6 ข้อ ดังต่อไปนี้

1. เพื่อศึกษาถึงอิทธิพลของปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และอิทธิพลของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
2. เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
3. เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
4. เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
5. เพื่อทำการพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

โดยในบทนี้ ผู้วิจัยจะได้นำเสนอผลการวิจัยตามลำดับของวัตถุประสงค์หลักทั้ง 5 ข้อ ที่ได้ดำเนินการศึกษาและวิจัย ซึ่งจะได้แสดงเป็นลำดับดังต่อไปนี้

4.1 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1

ผลการศึกษาและวิจัย เพื่อทำให้สามารถตอบวัตถุประสงค์ข้อที่ 1 ผู้วิจัยได้ทำการศึกษาโดยใช้เครื่องมือคือ แบบสอบถามเพื่อเก็บรวมรวมข้อมูลสำรวจความคิดเห็นในประเด็นของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ทั้งนี้เพื่อให้การศึกษามีความครอบคลุมมากที่สุด ผู้วิจัยจึงได้ออกแบบเครื่องมือเป็นแบบสอบถามซึ่งมีทั้งหมด 7 ส่วน ได้แก่ ส่วนที่ 1 ข้อมูล

ทั่วไปขององค์กรของผู้ตอบแบบสอบถาม ส่วนที่ 2 ข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทของผู้ตอบแบบสอบถาม ส่วนที่ 3 ความคิดเห็นเกี่ยวกับความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ส่วนที่ 4 ความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัล ส่วนที่ 5 ความคิดเห็นเกี่ยวกับปัญหาภัยคุกคามทางไซเบอร์ ส่วนที่ 6 ความคิดเห็นเกี่ยวกับการจัดการเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และส่วนที่ 7 ข้อมูลสภาพการดำเนินงานที่เกี่ยวข้องกับการจัดการความต่อเนื่องทางธุรกิจ รายละเอียดของแบบสอบถามผู้วิจัยได้นำไปบรรจุในภาคผนวกของรายงานวิจัยฉบับนี้ ผู้วิจัยได้นำเสนอผลการศึกษาดังต่อไปนี้

ตอนที่ 1 ผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลทั่วไปขององค์กร

ตอนที่ 2 ผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

ตอนที่ 3 ผลการวิเคราะห์ระดับความคิดเห็นของความร่วมมือกัน การจัดการภัยคุกคามทางไซเบอร์ การจัดการเสี่ยงทางไซเบอร์ ความสามารถการคืนสภาพได้ และการดำเนินงานการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยใช้สถิติเชิงพรรณนา

ตอนที่ 4 ผลการวิเคราะห์การตรวจสอบข้อมูลก่อนการวิเคราะห์โมเดลสมการโครงสร้าง

ตอนที่ 5 ผลการวิเคราะห์ข้อมูลเพื่อตอบวัตถุประสงค์ของการศึกษา

ตอนที่ 6 ผลการวิเคราะห์เส้นทาง

ตอนที่ 7 ผลการวิเคราะห์เพื่อตอบสมมติฐานการวิจัย

สำหรับการนำเสนอผลการวิเคราะห์ข้อมูล ผู้วิจัยได้กำหนดสัญลักษณ์ที่ใช้แทนตัวแปรและค่าสถิติ รวมถึงกำหนดความหมายของสัญลักษณ์ที่ใช้แทนตัวแปรและค่าสถิติ เพื่อให้การนำเสนอผลการวิเคราะห์ข้อมูลมีความเข้าใจตรงกันเกี่ยวกับสัญลักษณ์ต่าง ๆ ที่ใช้ในการวิจัยครั้งนี้ ซึ่งสามารถแสดงได้ดังตารางที่ 4.1 ดังนี้

ตารางที่ 4.1 แสดงสัญลักษณ์และความหมายของสัญลักษณ์ที่ใช้แทนตัวแปรและค่าสถิติ

สัญลักษณ์	ความหมาย
$\bar{X}$	ค่าเฉลี่ยเลขคณิต (Arithmetic Mean)
S.D.	ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)
MIN	คะแนนต่ำสุด (Minimum)
MAX	คะแนนสูงสุด (Maximum)

ตารางที่ 4.1 (ต่อ)

สัญลักษณ์	ความหมาย
T-Value	ค่าสถิติทดสอบซึ่งมีการแจกแจงแบบ t
p-Value	ค่าสัดส่วนของความผิดพลาดที่เกิดขึ้นจากการปฏิเสธสมมติฐานและเป็นค่าที่คำนวณได้จากข้อมูลเชิงประจักษ์ (Observed Significant Level)
δ	ความคลาดเคลื่อนของการวัดตัวแปรที่สังเกตได้ภายนอก
E	ความคลาดเคลื่อนของการวัดตัวแปรที่สังเกตได้ภายใน
SE	ความคลาดเคลื่อนมาตรฐาน
b	ค่าน้ำหนักองค์ประกอบ
B	ค่าน้ำหนักองค์ประกอบมาตรฐานเป็นรายองค์ประกอบ (Standardized Solution)
λ	น้ำหนักองค์ประกอบมาตรฐาน
SK	ค่าความเบ้ (Skewness)
KU	ค่าความโด่ง (Kurtosis)
r	ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน (Pearson Product Moment Correlation Coefficient)
CV	สัมประสิทธิ์การกระจาย (Coefficient of Variation)
ρ_c	ความเที่ยงของตัวแปรแฝง (Construct Reliability)
ρ_v	ค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Average Variance Extracted)
TE	ขนาดอิทธิพลรวม (Total Effects)
IE	ขนาดอิทธิพลทางอ้อม (Indirect Effects)
DE	ขนาดอิทธิพลทางตรง (Direct Effects)
χ^2	ดัชนีตรวจสอบความกลมกลืนประเภทค่าสถิติไค-แสควร์ (Chi-square)
df	ค่าองศาความเป็นอิสระ (Degree of Freedoms)
R^2	ค่าสัมประสิทธิ์การพยากรณ์ (Coefficient of Determination)
P	ระดับนัยสำคัญทางสถิติ
N	จำนวนกลุ่มตัวอย่าง
CFI	ดัชนีวัดความสอดคล้องกลมกลืนเชิงสัมพัทธ์ (Comparative Fit Index)
GFI	ดัชนีวัดระดับความกลมกลืน (Goodness of Fit Index)

ตารางที่ 4.1 (ต่อ)

สัญลักษณ์	ความหมาย
AGFI	ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (Adjusted Goodness of Fit Index)
RMSEA	ดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (Root Mean Square Error of Approximation)
SCC	ความร่วมมือกันของโซ่อุปทานดิจิทัล (Digital Supply Chain Collaboration)
X1	การแบ่งปันข้อมูลร่วมกัน (Information Sharing)
X2	การไว้ใจ (Trust)
X3	ความร่วมมือกันในการสื่อสาร (Collaborative Communication)
X4	การสร้างความรู้ร่วมกัน (Knowledge Sharing)
CBT	ภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Threats)
X5	แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (External Motivation of Cyber Attacks)
X6	ช่องโหว่ของดำเนินงานภายใน (Internal Organizational Vulnerabilities)
X7	การรับมือต่อภัยคุกคามไซเบอร์ (Threats Coping)
CBR	การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Supply Chain Risk Management)
X8	ด้านบุคลากร (People)
X9	ด้านกระบวนการ (Process)
X10	ด้านเทคโนโลยี (Technology)
CRS	การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber-Resilient Supply Chain)
Y1	ความคล่องตัว (Agility)
Y2	ความทนทาน (Robust)
BCM	การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Business Continuity Management)
Y3	แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)
Y4	แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan)
Y5	การจัดการวิกฤต (Crisis Management)
Y6	การจัดการเหตุฉุกเฉิน (Emergency Management)

ตอนที่ 1 ผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลทั่วไปขององค์กร

ผู้วิจัยนำเสนอผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลทั่วไปขององค์กร จากผู้ตอบแบบสอบถาม ซึ่งสามารถแสดงได้ดังตารางที่ 4.2

จากผลการวิเคราะห์ในตารางที่ 4.2 ผู้ตอบแบบสอบถามมีจำนวนทั้งหมด 1,864 คน โดยผู้ตอบแบบสอบถามส่วนใหญ่มาจากองค์กรที่มีประเภทธุรกิจในภาคการค้า มีจำนวน 757 คน คิดเป็นร้อยละ 40.61 รองลงมา อยู่ในภาคบริการ มีจำนวน 682 คน คิดเป็นร้อยละ 36.59 อยู่ในภาคการผลิต มีจำนวน 359 คน คิดเป็นร้อยละ 19.26 และอยู่ในภาคการเกษตร มีจำนวน 66 คน คิดเป็นร้อยละ 3.54

ผู้ตอบแบบสอบถามส่วนใหญ่ มาจากองค์กรที่มีระยะเวลาในการดำเนินกิจการ 10 ปี ขึ้นไป จำนวน 750 คน คิดเป็นร้อยละ 40.23 รองลงมาคือ มีระยะเวลาในการดำเนินกิจการ 4-9 ปี จำนวน 616 คน คิดเป็น ร้อยละ 33.05 มีระยะเวลาในการดำเนินกิจการ 1-3 ปี จำนวน 400 คน คิดเป็นร้อยละ 21.46 และมีระยะเวลาในการดำเนินกิจการน้อยกว่า 1 ปี จำนวน 98 คน คิดเป็นร้อยละ 5.26

ตารางที่ 4.2 แสดงจำนวนและร้อยละข้อมูลทั่วไปขององค์กร

ข้อมูลทั่วไป	รายละเอียด	จำนวน	ร้อยละ
ประเภทธุรกิจ	ภาคการค้า	757	40.61
	ภาคบริการ	682	36.59
	ภาคการผลิต	359	19.26
	ภาคการเกษตร	66	3.54
	รวม	**1,864**	**100.00**
ระยะเวลาที่ดำเนินกิจการ	น้อยกว่า 1 ปี	98	5.26
	1 - 3 ปี	400	21.46
	4 - 9 ปี	616	33.05
	10 ปี ขึ้นไป	750	40.23
	รวม	**1,864**	**100.00**
จำนวนพนักงาน	1 - 5 คน	112	6.01
	6 - 10 คน	128	6.87
	11 - 50 คน	369	19.80

ตารางที่ 4.2 (ต่อ)

ข้อมูลทั่วไป	รายละเอียด	จำนวน	ร้อยละ
	51 - 100 คน	425	22.80
	101 - 199 คน	181	9.71
	200 คนขึ้นไป	649	34.81
	รวม	**1,864**	**100.00**
ขอบเขตระดับตลาด	ระดับภูมิภาค	481	25.80
	ระดับประเทศ	1083	58.10
	ระดับนานาชาติ	297	15.93
	อื่น ๆ	3	0.17
	รวม	**1,864**	**100.00**
ตำแหน่งที่รับผิดชอบ	กรรมการผู้จัดการ/รองกรรมการผู้จัดการ	85	4.56
	ผู้อำนวยการฝ่าย/รองผู้อำนวยการฝ่าย	77	4.13
	ผู้จัดการแผนก/รองผู้จัดการแผนก	210	11.27
	หัวหน้าแผนก/รองหัวหน้าแผนก	433	23.23
	พนักงาน/เจ้าหน้าที่ปฏิบัติการ	763	40.93
	พนักงาน/เจ้าหน้าที่สนับสนุนปฏิบัติการ	248	13.30
	อื่น ๆ	48	2.58
	รวม	**1,864**	**100.00**
สัดส่วนพนักงานที่รู้ IT	น้อยกว่า 50%	281	15.08
	51 - 60%	301	16.15
	61 - 70%	535	28.70
	71 - 80%	467	25.05
	มากกว่า 80%	274	14.70
	ไม่มีพนักงานที่มีความรู้ทางด้านไอทีเลย	6	0.32
	รวม	**1,864**	**100.00**

ผู้ตอบแบบสอบถามส่วนใหญ่มาจากองค์กรที่มีจำนวนพนักงาน 200 คนขึ้นไป จำนวน 649 คน คิดเป็นร้อยละ 34.81 รองลงมาคือ มีจำนวนพนักงาน 51-100 คน จำนวน 425 คน คิดเป็นร้อยละ 22.80 มีจำนวนพนักงาน 11-50 คน จำนวน 369 คน คิดเป็นร้อยละ 19.80 มีจำนวนพนักงาน 101-199 คน จำนวน 181 คน คิดเป็นร้อยละ 9.71 มีจำนวนพนักงาน 6-10 คน จำนวน 128 คน คิดเป็นร้อยละ 6.87 และมีจำนวนพนักงาน 1-5 คน จำนวน 112 คน คิดเป็น 6.01

ผู้ตอบแบบสอบถามส่วนใหญ่มาจากองค์กรที่มีขอบเขตระดับตลาดที่อยู่ในระดับประเทศจำนวน 1,083 คน คิดเป็นร้อยละ 58.1 รองลงมา อยู่ในระดับภูมิภาค จำนวน 481 คน คิดเป็นร้อยละ 25.80 อยู่ในระดับนานาชาติ จำนวน 297 คน คิดเป็นร้อยละ 15.93 และอื่น ๆ จำนวน 3 คน คิดเป็นร้อยละ 0.17

ผู้ตอบแบบสอบถามส่วนใหญ่มีตำแหน่งที่รับผิดชอบในตำแหน่งพนักงาน/เจ้าหน้าที่ปฏิบัติการ จำนวน 763 คน คิดเป็นร้อยละ 40.93 รองลงมาคือ ตำแหน่งหัวหน้าแผนก/รองหัวหน้าแผนก จำนวน 433 คิดเป็นร้อยละ 23.23 ตำแหน่งพนักงาน/เจ้าหน้าที่สนับสนุนปฏิบัติการ จำนวน 248 คน คิดเป็นร้อยละ 13.30 ตำแหน่งผู้จัดการแผนก/รองผู้จัดการแผนก 210 คน คิดเป็นร้อยละ 11.27 ตำแหน่งกรรมการผู้จัดการ/รองกรรมการผู้จัดการ 85 คน คิดเป็นร้อยละ 4.56 ตำแหน่งผู้อำนวยการฝ่าย/รองผู้อำนวยการฝ่าย 77 คน คิดเป็นร้อยละ 4.13 และตำแหน่งอื่น ๆ จำนวน 48 คน คิดเป็นร้อยละ 2.58

ผู้ตอบแบบสอบถามส่วนใหญ่มาจากองค์กรที่มีสัดส่วนพนักงานที่รู้ IT 61-70% จำนวน 535 คิดเป็นร้อยละ 28.70 รองลงมา มีสัดส่วนพนักงานที่รู้ IT 71-80% จำนวน 467 คน คิดเป็นร้อยละ 25.05 มีสัดส่วนพนักงานที่รู้ IT 51-60% จำนวน 301 คน คิดเป็นร้อยละ 16.15 มีสัดส่วนพนักงานที่รู้ IT น้อยกว่า 50% จำนวน 281 คน คิดเป็นร้อยละ 15.08 มีสัดส่วนพนักงานที่รู้ IT มากกว่า 80% จำนวน 274 คน คิดเป็นร้อยละ 14.70 และไม่มีพนักงานที่มีความรู้ทางด้านไอทีเลย จำนวน 6 คน คิดเป็นร้อยละ 0.32

ตอนที่ 2 ผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

ผู้วิจัยนำเสนอผลการวิเคราะห์ค่าสถิติพื้นฐานข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยการวิจัยเชิงพรรณนาจำแนกตาม รายงานหรือแจ้งเตือนพนักงานว่าได้ตกเป็นเหยื่อจากการโจมตีทางไซเบอร์ แผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์ การใช้งานอย่างเข้มงวดเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้าน

สารสนเทศ การทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งสามารถแสดงได้ดังตารางที่ 4.3

ตารางที่ 4.3 แสดงจำนวนและร้อยละข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

ข้อมูลทั่วไป	**รายละเอียด**	**จำนวน**	**ร้อยละ**
รายงานจากพนักงานเมื่อโดนโจมตี	ใช่ ได้รายงานทุกครั้งที่พบ	536	28.76
	ใช่ แต่น้อยมาก	671	36.01
	ได้แจ้งเป็นบางครั้ง	443	23.76
	ไม่เคยได้แจ้งเลย	211	11.31
	อื่น ๆ	3	0.16
	รวม	**1,864**	**100.00**
แผนฉุกเฉินในการรับมือต่อการโจมตี	มี	880	47.21
	ไม่มี	826	44.31
	กำลังดำเนินการ	140	7.51
	อื่น ๆ	18	0.97
	รวม	**1,864**	**100.00**
การใช้งานอย่างเข้มงวดเกี่ยวกับ	มี	709	38.04
นโยบายรักษาความปลอดภัยไซเบอร์	มีเป็นบางครั้ง	750	40.24
	ไม่มี	234	12.55
	ไม่ทราบ	171	9.17
	รวม	**1,864**	**100.00**
มีการทบทวนนโยบายในการรักษา	มี	688	36.91
ความปลอดภัยไซเบอร์	มีเป็นบางครั้ง	752	40.34
	ไม่มี	233	12.50
	ไม่ทราบ	188	10.09
	อื่น ๆ	3	.16
	รวม	**1,864**	**100.00**

จากผลการวิเคราะห์ในตารางที่ 4.3 ผู้ตอบแบบสอบถามมีจำนวนทั้งหมด 1,864 คน โดยการสอบถามในประเด็นขององค์กรของผู้ตอบแบบสอบถามว่า ได้รับรับรายงานหรือแจ้งเตือนพนักงานว่าได้ตกเป็นเหยื่อจากการโจมตีทางไซเบอร์แล้วหรือไม่ ผู้ตอบแบบสอบถามแสดงความคิดเห็นสำหรับคำตอบว่า ใช่แต่น้อยมาก มีจำนวน 671 คน คิดเป็นร้อยละ 36.01 รองลงมาผู้ตอบแบบสอบแสดงความคิดเห็นสำหรับคำตอบว่า ใช่ ได้รับรายงานทุกครั้งที่พบ มีจำนวน 536 คน คิดเป็นร้อยละ 28.76 ผู้ตอบแบบสอบถามแสดงความคิดเห็นสำหรับคำตอบว่า ได้แจ้งเป็นบางครั้ง มีจำนวน 443 คน คิดเป็นร้อยละ 23.76 ผู้ตอบแบบสอบถามแสดง ความคิดเห็นสำหรับคำตอบว่า ไม่เคยได้รับแจ้งเลย มีจำนวน 211 คน คิดเป็นร้อยละ 11.31 และผู้ตอบแบบสอบถามแสดงความคิดเห็นสำหรับคำตอบ อื่น ๆ มีจำนวน 3 คน คิดเป็นร้อยละ 0.17

สำหรับประเด็น บริษัทของท่านมีแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์หรือไม่ ผู้ตอบแบบสอบถามส่วนใหญ่ แสดงความคิดเห็นว่าบริษัทของผู้ตอบแบบสอบถามมีแผนฉุกเฉินในการรับมือต่อสถานการณ์การโจมตีทางไซเบอร์ จำนวน 880 คน คิดเป็นร้อยละ 47.21 รองลงมาคือ ไม่มีแผนฉุกเฉินในการรับมือต่อสถานการณ์การโจมตีทางไซเบอร์ จำนวน 826 คน คิดเป็น ร้อยละ 44.31 กำลังดำเนินการภายใต้แผนฉุกเฉินในการรับมือต่อสถานการณ์การโจมตีทางไซเบอร์ จำนวน 140 คน คิดเป็นร้อยละ 7.51 และอื่น ๆ จำนวน 18 คน คิดเป็นร้อยละ 0.97

สำหรับประเด็น บริษัทของท่านมีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอยู่แล้วหรือไม่ ผู้ตอบแบบสอบถามส่วนใหญ่แสดงความคิดเห็นว่า บริษัทของผู้ตอบแบบสอบถาม มีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นบางครั้ง จำนวน 750 คน คิดเป็นร้อยละ 40.24 รองลงมา มีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอยู่แล้ว จำนวน 709 คน คิดเป็นร้อยละ 38.04 ไม่มีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน 234 คน คิดเป็นร้อยละ 12.55 และไม่ทราบว่ามีการใช้งานอย่างเข้มงวด เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จำนวน 171 คน คิดเป็นร้อยละ 9.17

สำหรับประเด็น บริษัทของท่านมีการทบทวน เกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่แล้วหรือไม่ ผู้ตอบแบบสอบถามส่วนใหญ่แสดงความคิดเห็นว่า บริษัทของผู้ตอบแบบสอบถาม มีการทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นบางครั้ง จำนวน 752 คน คิดเป็นร้อยละ 40.34 รองลงมาคือ มีการทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่แล้ว จำนวน 688 คน คิดเป็นร้อยละ 36.91

ไม่มีการทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 233 คน คิดเป็นร้อยละ 12.50 ไม่ทราบว่ามีมีการทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน 188 คน คิดเป็นร้อยละ 10.09 และอื่น ๆ จำนวน 3 คน คิดเป็นร้อยละ 0.16

นอกจากนั้นผู้วิจัยต้องการทราบความคิดเห็นของผู้ตอบแบบสอบถาม ในประเด็นของการให้ความสำคัญในเรื่องต่าง ๆ โดยมีการใช้การวิจัยเชิงพรรณนาต่อประเด็นดังกล่าว อีกทั้งผู้วิจัยต้องการจัดลำดับความสำคัญในเรื่องที่สอบถามไป ประเด็นที่สอบถามไปได้แก่ ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศที่องค์กรใช้อยู่ในปัจจุบัน รูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ รวมไปถึงนโยบายความมั่นคงปลอดภัยไซเบอร์ที่บริษัทได้ดำเนินการอยู่ในขณะนี้ ซึ่งได้มีการนำเสนออยู่ในตารางที่ 4.4 – 4.6 ตามลำดับดังนี้

ตารางที่ 4.4 ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่องค์กรใช้อยู่ในปัจจุบัน

	ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ	จำนวนนับได้	อันดับความคิดเห็น
1	โปรแกรมป้องกันไวรัส (Anti-virus Software)	1,489	1
2	ไฟร์วอลล์ (Firewall)	773	2
3	Application-level Firewall	115	12
4	ระบบเครือข่ายเสมือน (VPN : Virtual Private Network)	244	9
5	โปรแกรมป้องกันสปายแวร์ (Anti-spyware Software)	333	8
6	ระบบตรวจจับการบุกรุก (Instruction Detection Systems)	413	5
7	ระบบป้องกันการบุกรุก (Instruction Prevention Systems)	356	7
8	การเข้ารหัสข้อมูลที่สื่อสารระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์เน็ตเวิร์ค (Encryption for Data Transit)	386	6
9	การเข้ารหัสข้อมูลที่ถูกเก็บในอุปกรณ์เก็บข้อมูล (Encryption for Data in Storage)	479	4
10	โปรแกรมการจัดการลงบันทึกเข้าออก (Log Management Software)	582	3
11	เครื่องมือสืบสวนด้านนิติวิทยาศาสตร์สำหรับระบบคอมพิวเตอร์ (Forensics Tools)	104	13

ตารางที่ 4.4 (ต่อ)

	ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ	จำนวนนับได้	อันดับความคิดเห็น
12	ระบบรักษาความมั่นคงปลอดภัยเครือข่ายไร้สาย (Specialized Wireless Security System)	183	10
13	ระบบรักษาความมั่นคงปลอดภัยเครื่องลูกข่าย/ระบบควบคุมการเข้าใช้เครือข่าย (Endpoint Security Client Software/NAC)	126	11
14	ระบบยืนยันตัวผู้ใช้ด้วยชีวมิติ (Biometrics)	45	14
15	อื่น ๆ	28	15

จากผลการวิเคราะห์ในตารางที่ 4.4 ผู้ตอบแบบสอบถามมีจำนวนทั้งหมด 1,864 คน ในแบบสอบถามให้ผู้ตอบแบบสอบถามสามารถเลือกตอบได้มากกว่า 1 ข้อ เป็นการสอบถามความคิดเห็นในประเด็นของ การที่มีระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่องค์กรของผู้ตอบแบบสอบถามใช้อยู่ในปัจจุบัน จากผลการสำรวจพบว่า ระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่องค์กรใช้อยู่ในปัจจุบัน แสดงให้เห็นว่าบริษัทส่วนใหญ่โปรแกรมป้องกันไวรัส (Anti-virus Software) ใช้ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยมีความคิดเห็นมากที่สุด รองลงมาจะใช้ไฟร์วอลล์ (Firewall) โปรแกรมการจัดการลงบันทึกเข้าออก (Log Management Software) การเข้ารหัสข้อมูลที่ถูกเก็บในอุปกรณ์เก็บข้อมูล (Encryption for Data in Storage) ระบบตรวจจับการบุกรุก (Instruction Detection Systems) การเข้ารหัสข้อมูลที่สื่อสารระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์เน็ตเวิร์ค (Encryption for Data Transit) ระบบป้องกันการบุกรุก (Instruction Prevention Systems) โปรแกรมป้องกันสปายแวร์ (Anti-spyware Software) ระบบเครือข่ายเสมือน (VPN : Virtual Private Network) ระบบรักษาความมั่นคงปลอดภัยเครือข่ายไร้สาย (Specialized Wireless Security System) ระบบรักษาความมั่นคงปลอดภัยเครื่องลูกข่าย/ระบบควบคุมการเข้าใช้เครือข่าย (Endpoint Security Client Software/NAC) Application-level Firewall เครื่องมือสืบสวนด้านนิติวิทยาศาสตร์สำหรับระบบคอมพิวเตอร์ (Forensics Tools) ระบบยืนยันตัวผู้ใช้ด้วยชีวมิติ (Biometrics) และอื่น ๆ ตามลำดับ

ตารางที่ 4.5 รูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ

	รูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ	จำนวนนับได้	อันดับความคิดเห็น
1	ตรวจสอบความมั่นคงปลอดภัยโดยบุคลากรภายในองค์กร (Security Audits by Internal Staff)	1,386	1
2	ทดสอบหาความบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยบุคลากรภายในองค์กร (Penetration Testing by Internal Staff)	492	2
3	ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยองค์กรภายนอก (Security Audits by External Organization)	383	3
4	ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยเครื่องมืออัตโนมัติ (Automated Tools)	376	4
5	ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยโปรแกรมเฝ้าติดตามผ่านเว็บไซต์ (Web Activity Monitoring Software)	202	5
6	อื่น ๆ	44	6

จากผลการวิเคราะห์ในตารางที่ 4.5 ผู้ตอบแบบสอบถามมีจำนวนทั้งหมด 1,864 คน ในแบบสอบถามให้ผู้ตอบแบบสอบถามสามารถเลือกตอบได้มากกว่า 1 ข้อ เป็นการสอบถามความคิดเห็นในประเด็นของ รูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ จากผลการสำรวจพบว่า ผู้ตอบแบบสอบถามมีความคิดเห็นว่า การตรวจสอบความมั่นคงปลอดภัยโดยบุคลากรภายในองค์กร (Security Audits by Internal Staff) เป็นรูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ มากที่สุด รองลงมา คือ การทดสอบหาความบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยบุคลากรภายในองค์กร (Penetration Testing by Internal Staff) ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยองค์กรภายนอก (Security Audits by External Organization) ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยเครื่องมืออัตโนมัติ (Automated Tools) ตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยโปรแกรมเฝ้าติดตามผ่านเว็บไซต์ (Web Activity Monitoring Software) และอื่น ๆ ตามลำดับ

ตารางที่ 4.6 นโยบายความมั่นคงปลอดภัยไซเบอร์อะไรบ้างที่บริษัทของท่านได้ดำเนินการอยู่ในขณะนี้

	นโยบายความมั่นคงปลอดภัยไซเบอร์ที่บริษัทดำเนินการอยู่ในในขณะนี้	จำนวนนับได้	อันดับความคิดเห็น
1	มีแผนพัฒนาความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ	987	1
2	มีการจ้างบริษัทจากภายนอกในการจัดการเรื่องความมั่นคงปลอดภัยทางคอมพิวเตอร์	378	7
3	มีแผนการประเมินความเสี่ยง/ช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ	154	8
4	มีการเช่าศูนย์ที่ให้บริการในการตรวจสอบคอมพิวเตอร์/เครือข่าย	102	12
5	มีเอกสารมาตรฐานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์อย่างเป็นทางการ	145	9
6	มีการฝึกอบรมบุคลากรให้รับรู้ถึงกระบวนการการรักษาความมั่นคงปลอดภัย	394	6
7	มีการเก็บรักษาสื่อ อุปกรณ์ในการสำรองข้อมูล	808	3
8	มีการควบคุมเกี่ยวกับซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์	884	2
9	มีการจัดการสื่อทางคอมพิวเตอร์ที่สามารถถอดได้ (ตัวอย่างเช่น USB)	794	4
10	มีมาตรการในการรักษาความมั่นคงปลอดภัยสำหรับการนำเอาอุปกรณ์ส่วนตัวมาใช้	464	5
11	มีมาตรฐานความมั่นคงปลอดภัยสำหรับการใช้งานการประมวลผลแบบคลาวด์	109	11
12	ไม่ทราบว่ามีหรือไม่	133	10
13	ไม่มีตามหัวข้อข้างบน	10	14
14	อื่น ๆ	25	13

จากผลการวิเคราะห์ในตารางที่ 4.6 ผู้ตอบแบบสอบถามมีจำนวนทั้งหมด 1,864 คน ในแบบสอบถามให้ผู้ตอบแบบสอบถามสามารถเลือกตอบได้มากกว่า 1 ข้อ เป็นการสอบถามความ

คิดเห็นในประเด็นเรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์อะไรบ้างที่บริษัทของท่านได้ดำเนินการอยู่ในขณะนี้ จากผลการสำรวจพบว่า บริษัทของผู้ตอบแบบสอบถามมีแผนพัฒนาความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศเป็นรูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ มากที่สุด รองลงมา คือ มีการควบคุมเกี่ยวกับซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์ มีการเก็บรักษาสื่อ อุปกรณ์ในการสำรองข้อมูล มีการจัดการสื่อทางคอมพิวเตอร์ที่สามารถถอดได้ (ตัวอย่างเช่น USB) มีมาตรการในการรักษาความมั่นคงปลอดภัยสำหรับการนำเอาอุปกรณ์ส่วนตัวมาใช้ มีการฝึกอบรมบุคลากรให้รับรู้ถึงกระบวนการการรักษาความมั่นคงปลอดภัย มีการจ้างบริษัทจากภายนอกในการจัดการเรื่องความมั่นคงปลอดภัยทางคอมพิวเตอร์ มีแผนการประเมินความเสี่ยง/ช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ มีเอกสารมาตรฐานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์อย่างเป็นทางการ ไม่ทราบว่ามีหรือไม่ มีมาตรฐานความมั่นคงปลอดภัยสำหรับการใช้งานการประมวลผลแบบคลาวด์ มีการเช่าศูนย์ที่ให้บริการในการตรวจสอบคอมพิวเตอร์/เครือข่าย อื่นๆ และ ไม่มีหัวข้อตามด้านบน ตามลำดับ

ตอนที่ 3 ผลการวิเคราะห์ระดับความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัล การจัดการภัยคุกคามทางไซเบอร์ร์ของโซ่อุปทานดิจิทัล การจัดการเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล และสภาพการดำเนินงานที่เกี่ยวข้องกับการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยใช้สถิติเชิงพรรณนา

3.1 ความร่วมมือกันของโซ่อุปทานดิจิทัล

ความร่วมมือกันของโซ่อุปทานดิจิทัล (Digital Supply Chain Collaboration) ที่ศึกษามีจำนวน 4 ด้าน ได้แก่ การแบ่งปันข้อมูลร่วมกัน (Information Sharing) ความไว้ใจ (Trust) ความร่วมมือกันในการสื่อสาร (Collaborative Communication) และการสร้างความรู้ร่วมกัน (Knowledge Sharing) ในการศึกษาเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัล ตามความคิดเห็นของผู้ตอบแบบสอบถาม เกณฑ์ที่ใช้ในการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล มี 5 ระดับ โดยกำหนดเกณฑ์ดังต่อไปนี้ (5) หมายถึงตรงกับความเป็นจริงมากที่สุด (4) หมายถึงตรงกับความเป็นจริงมาก (3) หมายถึงตรงกับความเป็นจริงปานกลาง (2) หมายถึงตรงกับความเป็นจริงน้อย และ (1) หมายถึงตรงกับความเป็นจริงน้อยที่สุด ผลการวิเคราะห์ข้อมูลความร่วมมือกันของโซ่อุปทานดิจิทัล สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.7 ดังนี้

ตารางที่ 4.7 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัล

ความร่วมมือกันของโซ่อุปทานดิจิทัล (Digital Supply Chain Collaboration)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
การแบ่งปันข้อมูลร่วมกัน	**3.69**	**0.91**	**มาก**
1. บริษัทมีกระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่นๆ ในโซ่อุปทานดิจิทัล	3.76	0.83	มาก
2. กระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่นๆ ในโซ่อุปทานดิจิทัลที่มีอยู่นั้น เป็นกระบวนการที่มีประสิทธิภาพ	3.67	0.88	มาก
3. บริษัทได้มีการแบ่งปันข้อมูลด้านกลยุทธ์ให้กับทั้งลูกค้าและผู้จำหน่าย	3.63	0.94	มาก
4. การดำเนินการในเรื่องของการแบ่งปันข้อมูลที่ผ่านมาทำให้เกิดประโยชน์ต่อบริษัทเป็นอย่างมาก	3.66	0.94	มาก
5. การแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัลเป็นผลทำให้เกิดความร่วมมือกันในโซ่อุปทานดิจิทัล	3.71	0.94	มาก
ความไว้ใจ	**3.73**	**0.85**	**มาก**
1. คู่ค้าที่มีอยู่ในโซ่อุปทานดิจิทัลที่มีอยู่มีความซื่อสัตย์ในการติดต่อเพื่อทำธุรกิจกับบริษัทของท่าน	3.82	0.78	มาก
2. คู่ค้าที่อยู่ในโซ่อุปทานดิจิทัล มีการป้องกันความลับของลูกค้าที่ได้รับจากบริษัทของท่าน	3.73	0.82	มาก
3. คู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลได้ให้ข้อมูลที่ถูกต้องกับบริษัทของท่านเสมอ	3.66	0.88	มาก
4. คู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลของท่าน เต็มใจที่จะให้ความช่วยเหลือและสนับสนุนกับบริษัทของท่านโดยไม่มีข้อยกเว้น	3.73	0.85	มาก
5. เมื่อบริษัทของท่านประสบต่อปัญหาใด ๆและแจ้งไปยังคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลคู่ค้าเหล่านั้นจะปฏิบัติต่อบริษัทของท่านด้วยความเข้าใจ	3.68	0.88	มาก

ตารางที่ 4.7 (ต่อ)

ความร่วมมือกันของโซ่อุปทานดิจิทัล (Digital Supply Chain Collaboration)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
ความร่วมมือกันในการสื่อสาร	**3.70**	**0.89**	**มาก**
1. บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการจัดการประชุมร่วมกันอย่างสม่ำเสมอ	3.55	0.97	มาก
2. บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการสื่อสารกันแบบเปิดและแบบสองทางอยู่แล้ว	3.69	0.84	มาก
3. บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการสื่อสารทั้งที่เป็นทางการและไม่เป็นทางการ	3.74	0.86	มาก
4. บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีช่องทางในการสื่อสารกันอยู่หลายช่องทาง	3.81	0.90	มาก
5. บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการประสานงานระหว่างกัน โดยส่วนใหญ่จะใช้การสื่อสารทาง ด้านข้อความระหว่างกัน	3.72	0.87	มาก
การสร้างความรู้ร่วมกัน	**3.68**	**0.86**	**มาก**
1. บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าใน โซ่อุปทานดิจิทัลที่เกี่ยวกับกลยุทธ์ในการดำเนินการร่วมกันเพื่อความสำเร็จที่จะเกิดขึ้นในระยะยาว	3.63	0.91	มาก
2. บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าใน โซ่อุปทานดิจิทัลในการแลกเปลี่ยนแนวความคิดใหม่ ๆ เพื่อความสัมพันธ์ที่ดีต่อกันในระยะยาว	3.74	0.78	มาก
3. บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าใน โซ่อุปทานดิจิทัล เกี่ยวกับการพัฒนาโอกาสทางด้านนวัตกรรม โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการจัดการความเสี่ยงและความไม่แน่นอนทางด้านธุรกิจที่จะเกิดขึ้น	3.68	0.87	มาก
เฉลี่ยรวม	**3.70**	**0.87**	**มาก**

จากตารางที่ 4.7 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านการแบ่งปันข้อมูลร่วมกันอยู่ในระดับมาก ($\bar{X}$ = 3.69, S.D. = 0.91) โดยสามารถเรียงลำดับความคิดเห็นด้านการแบ่งปันข้อมูลร่วมกัน จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ บริษัทมีกระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัล ($\bar{X}$ = 3.76, S.D. = 0.83) รองลงมาคือ การแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัลเป็นผลทำให้เกิดความร่วมมือกันในโซ่อุปทานดิจิทัล ($\bar{X}$ = 3.71, S.D. = 0.94) กระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัลที่มีอยู่นั้น เป็นกระบวนการที่มีประสิทธิภาพ ($\bar{X}$ = 3.67, S.D. = 0.88) การดำเนินการในเรื่องของการแบ่งปันข้อมูลที่ผ่านมาทำให้เกิดประโยชน์ต่อบริษัทเป็นอย่างมาก ($\bar{X}$ = 3.66, S.D. = 0.94) และบริษัทได้มีการแบ่งปันข้อมูลด้านกลยุทธ์ให้กับทั้งลูกค้าและผู้จำหน่าย ($\bar{X}$ = 3.63, S.D. = 0.94) ตามลำดับ

ส่วนด้านความไว้ใจพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านความไว้ใจอยู่ในระดับมาก ($\bar{X}$ = 3.73, S.D. = 0.85) โดยสามารถเรียงลำดับความคิดเห็นด้านความไว้ใจจากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ คู่ค้าที่มีอยู่ในโซ่อุปทานดิจิทัลที่มีอยู่มีความซื่อสัตย์ในการติดต่อเพื่อทำธุรกิจกับบริษัทของท่าน ($\bar{X}$ = 3.82, S.D. = 0.78) รองลงมาคือคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัล มีการป้องกันความลับของลูกค้าที่ได้รับจากบริษัทของท่าน ($\bar{X}$ = 3.73, S.D. = 0.82) คู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลของท่านเต็มใจที่จะให้ความช่วยเหลือและสนับสนุนกับบริษัทของท่านโดยไม่มีข้อยกเว้น ($\bar{X}$ = 3.73, S.D. = 0.85) เมื่อบริษัทของท่านประสบต่อปัญหาใด ๆ และแจ้งไปยังคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลคู่ค้าเหล่านั้นจะปฏิบัติต่อบริษัทของท่านด้วยความเข้าใจ ($\bar{X}$ = 3.68, S.D. = 0.88) คู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลได้ให้ข้อมูลที่ถูกต้องกับบริษัทของท่านเสมอ ($\bar{X}$ = 3.66, S.D. = 0.88) ตามลำดับ

ส่วนด้านความร่วมมือกันในการสื่อสารพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านความร่วมมือกันในการสื่อสารอยู่ในระดับมาก ($\bar{X}$ = 3.70, S.D. = 0.89) โดยสามารถเรียงลำดับความคิดเห็นด้านความร่วมมือกันในการสื่อสาร จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุด ไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุดดังนี้ บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัลมีช่องทางในการสื่อสารกันอยู่หลายช่องทาง ($\bar{X}$ = 3.81, S.D. = 0.90) รองลงมาคือ บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการสื่อสารทั้งที่เป็นทางการและไม่เป็นทางการ ($\bar{X}$ = 3.74, S.D. = 0.86) บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัล มีการประสานงานระหว่างกัน โดยส่วนใหญ่จะใช้การสื่อสารทางด้านข้อความระหว่างกัน ($\bar{X}$ = 3.72, S.D. = 0.87) บริษัทของท่านและคู่ค้า

ในโซ่อุปทานดิจิทัล มีการสื่อสารกันแบบเปิดและแบบสองทางอยู่แล้ว ($\bar{X}$ = 3.69, S.D. = 0.84) บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัลมีการจัดการประชุมร่วมกันอย่างสม่ำเสมอ ($\bar{X}$ = 3.55, S.D. = 0.97) ตามลำดับ

ส่วนด้านการสร้างความรู้ร่วมกันพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านการสร้างความรู้ร่วมกันอยู่ในระดับมาก ($\bar{X}$ = 3.68, S.D. = 0.86) โดยสามารถเรียงลำดับความคิดเห็นด้านการสร้างความรู้ร่วมกันจากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุดดังนี้ บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานดิจิทัล ในการแลกเปลี่ยนแนวความคิดใหม่ ๆ เพื่อความสัมพันธ์ที่ดีต่อกันในระยะยาว ($\bar{X}$ = 3.74, S.D. = 0.78) รองลงมาคือ บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานดิจิทัลเกี่ยวกับการพัฒนาโอกาสทางด้านนวัตกรรม โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการจัดการความเสี่ยงและความไม่แน่นอนทางด้านธุรกิจที่จะเกิดขึ้น ($\bar{X}$ = 3.68, S.D. = 0.87) และบริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานดิจิทัลที่เกี่ยวกับกลยุทธ์ในการดำเนินการร่วมกันเพื่อความสำเร็จที่จะเกิดขึ้นในระยะยาว ($\bar{X}$ = 3.63, S.D. = 0.91) ตามลำดับ

เมื่อพิจารณาในภาพรวมพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมอยู่ในระดับมาก ($\bar{X}$ = 3.70, S.D. = 0.87)

3.2 การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

ปัญหาภัยคุกคามไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Threat of Digital Supply Chain) ที่ศึกษามีจำนวน 3 ด้าน ได้แก่ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (External Motivation of Cyber Attacks) ช่องโหว่ของดำเนินงานภายใน (Internal Organizational Vulnerabilities) การรับมือต่อภัยคุกคามไซเบอร์ (Threats Coping) ในการศึกษาเกี่ยวกับปัญหาภัยคุกคามทางไซเบอร์ ตามความคิดเห็นของผู้ตอบแบบสอบถาม เกณฑ์ที่ใช้ในการวัดปัญหาภัยคุกคามไซเบอร์ มี 5 ระดับ โดยกำหนดเกณฑ์ดังต่อไปนี้ (5) หมายถึง ตรงกับความเป็นจริงมากที่สุด (4) หมายถึง ตรงกับความเป็นจริงมาก (3) หมายถึง ตรงกับความเป็นจริงปานกลาง (2) หมายถึง ตรงกับความเป็นจริงน้อย (1) หมายถึง ตรงกับความเป็นจริงน้อยที่สุด ผลการวิเคราะห์ข้อมูลปัญหาภัยคุกคามทางไซเบอร์ สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.8 ดังนี้

ตารางที่ 4.8 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Threat Supply Chain	**ระดับความคิดเห็น**		
	$\bar{X}$	**S.D.**	**แปลผล**
แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก	**3.50**	**0.98**	**ปานกลาง**
1. ผู้บุกรุกเข้าสู่เครือข่ายมีวัตถุประสงค์ในการทดสอบขีดความสามารถของตนเอง หรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จ	3.34	1.03	ปานกลาง
2. ความรุนแรงขององค์กรอาชญากรรมที่มุ่งกระทำต่อธุรกรรมทางการเงินและทรัพย์สินทางปัญญาของวิสาหกิจ	3.60	0.95	มาก
3. การโจมตีทางไซเบอร์ที่เกิดขึ้นกับวิสาหกิจมักจะมีสาเหตุมาจากการความแตกต่างทางด้านอุดมการณ์และการเมือง	3.55	0.94	มาก
4. นโยบายทางภาครัฐส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มีต่อบริษัทท่าน	3.49	0.99	ปานกลาง
ช่องโหว่ของการดำเนินงานภายใน	**3.54**	**0.93**	**มาก**
1. การดำเนินการและยึดมั่นในกลยุทธ์และมาตรฐานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่านจะส่งผลให้เกิดการโจมตีทางไซเบอร์นั้นลดลง	3.52	0.94	มาก
2. การอบรมพนักงานรวมไปถึงการทำให้พนักงานได้ตระหนักถึงภัยคุกคามทางไซเบอร์จะทำให้การโจมตีทางไซเบอร์นั้นลดลงได้	3.53	0.95	มาก
3. ความสามารถในการพัฒนาทักษะความสามารถบุคลากรในบริษัทของท่านจะส่งต่อการจัดการความปลอดภัยในโลกไซเบอร์ให้มีประสิทธิภาพมากขึ้น	3.57	0.89	มาก
การรับมือต่อภัยคุกคามไซเบอร์	**3.50**	**0.93**	**ปานกลาง**
1. บริษัทของท่านมีการกำหนดนโยบาย (Policy) ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไว้อย่างชัดเจนในการเพื่อใช้ในการรับมือต่อภัยคุกคามไซเบอร์	3.33	0.94	ปานกลาง

ตารางที่ 4.8 (ต่อ)

การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Threat Supply Chain)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
2. บริษัทของท่านมีการกำหนดกรอบการดำเนินงาน (Frame work) อย่างเป็นระบบแบบแผนที่ชัดเจนและสามารถปฏิบัติได้ในการรับมือกับภัยคุกคามด้านไซเบอร์ขององค์กร	3.67	0.89	มาก
3. บริษัทของท่านมีการประเมินผลการปฏิบัติขององค์กรทั้งการประเมินภายในด้วยตนเอง และการประเมินจากภายนอก เพื่อติดตามความก้าวหน้า ปัญหาข้อขัดข้อง ข้อจำกัดอุปสรรคต่างๆ เพื่อหาทางแก้ไขปัญหาและอุปสรรคแต่เนิ่นๆ สำหรับการรับมือกับภัยคุกคามด้านไซเบอร์	3.62	0.90	มาก
เฉลี่ยรวม	**3.52**	**0.92**	**มาก**

การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล จากตารางที่ 4.8 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับปัญหา ภัยคุกคามไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอกอยู่ในระดับปานกลาง ($\bar{X}$ = 3.50, S.D. = 0.98) โดยสามารถเรียงลำดับความคิดเห็นด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ ความรุนแรงขององค์กรอาชญากรรมที่มุ่งกระทำต่อธุรกรรมทางการเงินและทรัพย์สินทางปัญญาของวิสาหกิจ ($\bar{X}$ = 3.60, S.D. = 0.95) รองลงมาคือ การโจมตีทางไซเบอร์ที่เกิดขึ้นกับวิสาหกิจมักจะมีสาเหตุมาจากการความแตกต่างทางด้านอุดมการณ์และการเมือง ($\bar{X}$ = 3.55, S.D. = 0.94) นโยบายทางภาครัฐส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มีต่อบริษัทท่าน ($\bar{X}$ = 3.49, S.D. = 0.99) และ ผู้บุกรุกเข้าสู่เครือข่ายมีวัตถุประสงค์ในการทดสอบขีดความสามารถของตนเอง หรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จ ($\bar{X}$ = 3.34, S.D. = 1.03) ตามลำดับ

ส่วนด้านช่องโหว่ของการดำเนินงานภายใน พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านช่องโหว่ของการดำเนินงานภายในอยู่ในระดับมาก ($\bar{X}$ = 3.54, S.D. = 0.93)

โดยสามารถเรียงลำดับความคิดเห็นด้านช่องโหว่จากการดำเนินงานภายใน จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ ความสามารถในการพัฒนาทักษะความสามารถบุคลากรในบริษัทของท่านจะส่งต่อการจัดการความปลอดภัยในโลกไซเบอร์ให้มีประสิทธิภาพมากขึ้น ($\bar{X}$ = 3.57, S.D. = 0.89) รองลงมาคือ การอบรมพนักงานรวมไปถึงการทำให้พนักงานได้ตระหนักถึงภัยคุกคามทางไซเบอร์จะทำให้การโจมตีทางไซเบอร์นั้นลดลงได้ ($\bar{X}$ = 3.53, S.D. = 0.95) และการดำเนินการและยึดมั่นในกลยุทธ์และมาตรฐานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่านจะส่งผลให้เกิดการโจมตีทางไซเบอร์นั้นลดลง ($\bar{X}$ = 3.52, S.D. = 0.94) ตามลำดับ

ส่วนด้านการรับมือต่อภัยคุกคามไซเบอร์พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านการรับมือต่อภัยคุกคามไซเบอร์อยู่ในระดับปานกลาง ($\bar{X}$ = 3.50, S.D. = 0.93) โดยสามารถเรียงลำดับความคิดเห็นด้านการรับมือต่อภัยคุกคามไซเบอร์ จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ บริษัทของท่านมีการกำหนดกรอบการดำเนินงาน (Frame work) อย่างเป็นระบบแบบแผนที่ชัดเจนและสามารถปฏิบัติได้ในการรับมือกับภัยคุกคามด้านไซเบอร์ขององค์กร ($\bar{X}$ = 3.67, S.D. = 0.89) รองลงมาคือ บริษัทของท่านมีการประเมินผลการปฏิบัติขององค์กรทั้งการประเมินภายในด้วยตนเอง และการประเมินจากภายนอกเพื่อติดตามความก้าวหน้า ปัญหาข้อขัดข้อง ข้อจำกัดอุปสรรคต่าง ๆ เพื่อหาทางแก้ไขปัญหาและอุปสรรคแต่เนิ่นๆ สำหรับการรับมือกับภัยคุกคามด้านไซเบอร์ ($\bar{X}$ = 3.62, S.D. = 0.90) และ บริษัทของท่านมีการกำหนดนโยบาย (Policy) ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไว้อย่างชัดเจนในการเพื่อใช้ในการรับมือต่อภัยคุกคามไซเบอร์ ($\bar{X}$ = 3.33, S.D. = 0.94) ตามลำดับ

เมื่อพิจารณาในภาพรวมพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นเกี่ยวกับปัญหาภัยคุกคามไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมอยู่ในระดับมาก ($\bar{X}$ = 3.52, S.D. = 0.92)

3.3 การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Supply Chain Cyber Risk Management) ที่ศึกษามีจำนวน 3 ด้าน ได้แก่ ด้านบุคลากร (People) ด้านกระบวนการ (Process) และด้านเทคโนโลยี (Technology) ในการศึกษาเกี่ยวกับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ตามความคิดเห็นของผู้ตอบแบบสอบถาม เกณฑ์ที่ใช้ในการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มี 5 ระดับ โดยกำหนดเกณฑ์ดังต่อไปนี้ (5) หมายถึง ตรงกับความเป็นจริงมากที่สุด (4) หมายถึง ตรงกับความเป็นจริงมาก (3) หมายถึง ตรงกับความเป็น

จริงปานกลาง (2) หมายถึง ตรงกับความเป็นจริงน้อย (1) หมายถึง ตรงกับความเป็นจริงน้อยที่สุด ผลการวิเคราะห์ข้อมูลปัญหาภัยคุกคามไซเบอร์ สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.9 ดังนี้

ตารางที่ 4.9 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Supply Chain Cyber Risk Management)	**ระดับความคิดเห็น**		
	$\bar{X}$	**S.D.**	**แปลผล**
ด้านบุคลากร	**3.71**	**0.88**	**มาก**
1. บุคลากรของบริษัทท่านมีความสามารถและความชำนาญและความเชี่ยวชาญต่อการจัดการความเสี่ยงอยู่ในระดับสูง	3.69	0.82	มาก
2. บุคลากรของบริษัทของท่านมีความตระหนักถึงการจัดการความเสี่ยงเป็นอย่างดี	3.69	0.89	มาก
3. บริษัทของท่านมีการจัดการความเสี่ยงด้วยการสนับสนุนให้พนักงานทำงานร่วมกันเป็นทีม	3.76	0.93	มาก
4. บริษัทของท่านมีนโยบายให้พนักงานสร้างความสัมพันธ์ที่ดีไม่ว่าจะเป็นทั้งลูกค้า ผู้จำหน่าย รวมไปถึงคู่ค้าต่าง ๆ	3.70	0.88	มาก
ด้านกระบวนการ	**3.75**	**0.86**	**มาก**
1. บริษัทของท่านได้มีการดำเนินการในเรื่องของการติดตั้งโปรแกรมป้องกันไวรัสไว้แล้ว	3.79	0.85	มาก
2. บริษัทของท่านมีระบบรักษาความปลอดภัยของข้อมูลในการที่จะรักษาข้อมูลต่าง ๆ ที่สำคัญของบริษัทของท่าน	3.76	0.83	มาก
3. บริษัทของท่านมีการจัดการในเรื่องของระบบเครือข่ายในการป้องการการเข้ามาโจมตีจากผู้ไม่หวังดี	3.75	0.87	มาก
4. บริษัทของท่านมีระบบในการจัดการบัญชีรายชื่อผู้เข้าใช้งานในระบบต่าง ๆ โดยการสร้างกฎเกณฑ์ในการตั้งค่าไว้อย่างมีประสิทธิภาพ	3.76	0.87	มาก

ตารางที่ 4.9 (ต่อ)

การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Supply Chain Cyber Risk Management)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
5. ภัยคุกคามทางไซเบอร์ในปัจจุบันนี้ ทำให้เกิดผลเสียต่อระบบเครือข่ายคอมพิวเตอร์ของท่านอย่างมาก	3.66	0.90	มาก
ด้านเทคโนโลยี	**3.65**	**0.86**	**มาก**
1. โครงสร้างพื้นฐานอันประกอบไปด้วย สถาปัตยกรรมของระบบ ผู้ใช้งานระบบ รวมไปถึงผู้ให้บริการจากภายนอก ได้รับการจัดการเพื่อรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ	3.65	0.82	มาก
2. ท่านมีความเชื่อมั่นต่อเทคโนโลยีในการรักษาความปลอดภัย เมื่อบริษัทของท่านได้ประสบกับปัญหาภัยคุกคามทางไซเบอร์ นั่นหมายความว่าปัญหาภัยคุกคามดังกล่าวจะไม่ส่งผลกระทบต่องานของท่าน	3.65	0.90	มาก
เฉลี่ยรวม	**3.72**	**0.87**	**มาก**

จากตารางที่ 4.9 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านบุคลากร อยู่ในระดับมาก ($\bar{X}$ = 3.71, S.D. = 0.88) โดยสามารถเรียงลำดับความคิดเห็นด้านบุคลากร จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ บริษัทของท่านมีการจัดการความเสี่ยงด้วยการสนับสนุนให้พนักงานทำงานร่วมกันเป็นทีม ($\bar{X}$ = 3.76, S.D. = 0.93) รองลงมาคือ บริษัทของท่านมีนโยบายให้พนักงานสร้างความสัมพันธ์ที่ดีไม่ว่าจะเป็นทั้งลูกค้า ผู้จำหน่าย รวมไปถึงคู่ค้าต่าง ๆ ($\bar{X}$ = 3.70, S.D. = 0.88) บุคลากรของบริษัทท่านมีความสามารถและความชำนาญและความเชี่ยวชาญต่อการจัดการความเสี่ยงอยู่ในระดับสูง ($\bar{X}$ = 3.69, S.D. = 0.82) และ บุคลากรของบริษัทของท่านมีความตระหนักถึงการจัดการความเสี่ยงเป็นอย่างดี ($\bar{X}$ = 3.69, S.D. = 0.89) ตามลำดับ

ส่วนด้านกระบวนการพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านกระบวนการ อยู่ในระดับมาก ($\bar{X}$ = 3.75, S.D. = 0.86) โดยสามารถเรียงลำดับความคิดเห็นด้านกระบวนการ จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด

ดังนี้ บริษัทของท่านได้มีการดำเนินการในเรื่องของการติดตั้งโปรแกรมป้องกันไวรัสไว้แล้ว ($\bar{X}$ = 3.79, S.D. = 0.85) รองลงมาคือ บริษัทของท่านมีระบบรักษาความปลอดภัยของข้อมูลในการที่จะรักษาข้อมูลต่าง ๆ ที่สำคัญของบริษัทของท่าน ($\bar{X}$ = 3.76, S.D. = 0.83) บริษัทของท่านมีระบบในการจัดการบัญชีรายชื่อผู้เข้าใช้งานในระบบต่าง ๆ โดยการสร้างกฎเกณฑ์ในการตั้งค่าไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.76, S.D. = 0.87) บริษัทของท่านมีการจัดการในเรื่องของระบบเครือข่ายในการป้องการการเข้ามาโจมตีจากผู้ไม่หวังดี ($\bar{X}$ = 3.75, S.D. = 0.87) และ ภัยคุกคามทางไซเบอร์ในปัจจุบันนี้ ทำให้เกิดผลเสียต่อระบบเครือข่ายคอมพิวเตอร์ของท่านอย่างมาก ($\bar{X}$ = 3.66, S.D. = 0.90) ตามลำดับ

ส่วนด้านเทคโนโลยีพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านเทคโนโลยีอยู่ในระดับมาก ($\bar{X}$ = 3.65, S.D. = 0.86) โดยสามารถเรียงลำดับความคิดเห็นด้านเทคโนโลยี จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ โครงสร้างพื้นฐานอันประกอบไปด้วย สถาปัตยกรรมของระบบ ผู้ใช้งานระบบ รวมไปถึงผู้ให้บริการจากภายนอก ได้รับการจัดการเพื่อรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.65, S.D. = 0.82) รองลงมาคือ ท่านมีความเชื่อมั่นต่อเทคโนโลยีในการรักษาความปลอดภัย เมื่อบริษัทของท่านได้ประสบกับปัญหาภัยคุกคามทางไซเบอร์ นั่นหมายความว่าปัญหาภัยคุกคามดังกล่าวจะไม่ส่งผลกระทบต่องานของท่าน ($\bar{X}$ = 3.65, S.D. = 0.90)

เมื่อพิจารณาในภาพรวมพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นเกี่ยวกับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมอยู่ในระดับมาก ($\bar{X}$ = 3.72, S.D. = 0.87)

3.4 การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber-Resilient Supply Chain) ที่ศึกษามีจำนวน 2 ด้าน ได้แก่ ความคล่องตัว (Agility) และความทนทาน (Robust) ในการศึกษาเกี่ยวกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลตามความคิดเห็นของผู้ตอบแบบสอบถาม เกณฑ์ที่ใช้ในการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล มี 5 ระดับ โดยกำหนดเกณฑ์ดังต่อไปนี้ (5) หมายถึง ตรงกับความเป็นจริงมากที่สุด (4) หมายถึง ตรงกับความเป็นจริงมาก (3) หมายถึง ตรงกับความเป็นจริงปานกลาง (2) หมายถึง ตรงกับความเป็นจริงน้อย (1) หมายถึง ตรงกับความเป็นจริงน้อยที่สุด ผลการวิเคราะห์ข้อมูลปัญหาภัยคุกคามไซเบอร์ สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.10 ดังนี้

ตารางที่ 4.10 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber-Resilient Supply Chain)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
ความคล่องตัว	**3.70**	**0.87**	**มาก**
1. บริษัทของท่านสามารถที่จะทำการตรวจจับถึงภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว	3.68	0.84	มาก
2. บริษัทของท่านสามารถที่จะทำการตัดสินใจกระทำการใดๆ เมื่อพบกับภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว	3.73	0.85	มาก
3. บริษัทของท่านสามารถที่ตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว	3.73	0.88	มาก
4. บริษัทของท่านสามารถที่ปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่างๆ ภายในบริษัทได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัทของท่าน	3.65	0.92	มาก
ความทนทาน	**3.66**	**0.85**	**มาก**
1. บริษัทของท่าน สามารถที่จะกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก	3.63	0.83	มาก
2. บริษัทของท่าน สามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ๆ หลังจากการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก	3.65	0.83	มาก
3. บริษัทของท่านได้เตรียมความพร้อมเกี่ยวกับการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก	3.65	0.87	มาก

ตารางที่ 4.10 (ต่อ)

การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber-Resilient Supply Chain)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
4. บริษัทของท่าน สามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานดิจิทัลต่อไปได้ แม้จะถูกโจมตีจากภัยคุกคามที่ทำให้การดำเนินงานเกิดการชะงัก	3.66	0.88	มาก
5. บริษัทของท่าน สามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่อุปทานดิจิทัล หลังจากที่ถูกโจมตีจากภัยคุกคาม ที่ทำให้การดำเนินงานเกิดการชะงัก	3.67	0.83	มาก
6. บริษัทของท่าน สามารถที่จะดึงเอาความรู้ ความหมายต่างๆ ที่เป็นประโยชน์อันเกิดจากการถูกโจมตีจากภัยคุกคาม เพื่อนำมาเป็นข้อมูลในการแก้ปัญหาอาจถูกโจมตีในครั้งต่อไป	3.67	0.86	มาก
เฉลี่ยรวม	**3.67**	**0.86**	**มาก**

ตารางที่ 4.10 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม พบว่าผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านความคล่องตัว อยู่ในระดับมาก ($\bar{X}$ = 3.70, S.D. = 0.87) โดยสามารถเรียงลำดับความคิดเห็นด้านความคล่องตัว จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุดดังนี้ บริษัทของท่านสามารถที่จะทำการตัดสินใจกระทำการใดๆ เมื่อพบกับภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว ($\bar{X}$ = 3.73, S.D. = 0.85) รองลงมาคือ บริษัทของท่านสามารถที่ตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว ($\bar{X}$ = 3.73, S.D. = 0.88) บริษัทของท่านสามารถที่จะทำการตรวจจับถึงภัยคุกคามที่เข้ามาโจมตี การดำเนินธุรกรรมต่าง ๆ ภายในบริษัทของท่านด้วยความรวดเร็ว ($\bar{X}$ = 3.68, S.D. = 0.84) และ บริษัทของท่านสามารถที่ปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่างๆ ภายในบริษัทได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัทของท่าน ($\bar{X}$ = 3.65, S.D. = 0.92) ตามลำดับ

ส่วนด้านความทนทานพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านความทนทาน อยู่ในระดับมาก ($\bar{X}$ = 3.66, S.D. = 0.85) โดยสามารถเรียงลำดับความคิดเห็นด้านความทนทาน จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ บริษัทของท่าน สามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่อุปทานดิจิทัล หลังจากที่ถูกโจมตีจากภัยคุกคาม ที่ทำให้การดำเนินงานเกิดการชะงัก ($\bar{X}$ = 3.67, S.D. = 0.83) รองลงมาคือ บริษัทของท่าน สามารถที่จะดึงเอาความรู้ ความหมายต่าง ๆ ที่เป็นประโยชน์อันเกิดจากการถูกโจมตีจากภัยคุกคาม เพื่อนำมาเป็นข้อมูลในการแก้ปัญหาอาจถูกโจมตีในครั้งต่อไป ($\bar{X}$ = 3.67, S.D. = 0.86) บริษัทของท่าน สามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานดิจิทัลต่อไปได้ แม้จะถูกโจมตีจากภัยคุกคามที่ทำให้การดำเนินงานเกิดการชะงัก ($\bar{X}$ = 3.66, S.D. = 0.88) บริษัทของท่านสามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ ๆ หลังจากการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก ($\bar{X}$ = 3.65, S.D. = 0.83) บริษัทของท่านได้เตรียมความพร้อมเกี่ยวกับการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก ($\bar{X}$ = 3.65, S.D. = 0.87) และบริษัทของท่าน สามารถที่จะกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก ($\bar{X}$ = 3.63, S.D. = 0.83) ตามลำดับ

เมื่อพิจารณาในภาพรวมพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นเกี่ยวกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมอยู่ในระดับมาก ($\bar{X}$ = 3.67, S.D. = 0.86)

3.5 การจัดการความต่อเนื่องทางธุรกิจดิจิทัล

การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Digital Business Continuity Management) ที่ศึกษามีจำนวน 4 ด้าน ได้แก่ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan) การจัดการวิกฤต (Crisis Management) การจัดการเหตุฉุกเฉิน (Emergency Management) ในการศึกษาเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจ ตามความคิดเห็นของผู้ตอบแบบสอบถาม เกณฑ์ที่ใช้ในการวัดการจัดการความต่อเนื่องทางธุรกิจมี 5 ระดับ โดยกำหนดเกณฑ์ดังต่อไปนี้ (5) หมายถึง ตรงกับความเป็นจริงมากที่สุด (4) หมายถึง ตรงกับความเป็นจริงมาก (3) หมายถึง ตรงกับความเป็นจริงปานกลาง (2) หมายถึง ตรงกับความเป็นจริงน้อย (1) หมายถึง ตรงกับความเป็นจริงน้อยที่สุด ผลการวิเคราะห์ข้อมูลปัญหาภัยคุกคามไซเบอร์ สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.11 ดังนี้

ตารางที่ 4.11 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Digital Business Continuity Management)	ระดับความคิดเห็น		
	$\bar{X}$	S.D.	แปลผล
แผนความต่อเนื่องทางธุรกิจ	**3.70**	**0.86**	**มาก**
1. แผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยที่สามารถทำให้กิจการดำเนินต่อไปได้	3.68	0.81	มาก
2. แผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ	3.74	0.82	มาก
3. แผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้	3.68	0.87	มาก
4. แผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจ และจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัท พร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม	3.66	0.90	มาก
5. แผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้	3.74	0.88	มาก
แผนกู้คืนภัยพิบัติ	**3.73**	**0.86**	**มาก**
1. แผนกู้คืนภัยพิบัติ ได้เข้ามาจัดการเกี่ยวกับเครื่องมืออุปกรณ์ ที่จะนำมาใช้แก้ปัญหาเมื่อเกิดภัยพิบัติได้อย่างมีประสิทธิภาพ	3.70	0.83	มาก
2. แผนกู้คืนภัยพิบัติ ทำให้มีการจัดการเกี่ยวกับระบบการจัดการเครือข่ายในบริษัทได้อย่างมีประสิทธิภาพ	3.74	0.79	มาก
3. แผนกู้คืนภัยพิบัติ ทำให้สามารถประหยัดค่าใช้จ่ายในการกู้คืนระบบ เนื่องจากมีการทำแผนการปฏิบัติรองรับไว้แล้ว	3.77	0.84	มาก
4. การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยในการรักษาชื่อเสียงของบริษัทของท่านกับลูกค้าและคู่ค้าได้	3.74	0.91	มาก

ตารางที่ 4.11 (ต่อ)

การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Digital Business Continuity Management)	ระดับความคิดเห็น		
	$\bar{x}$	S.D.	แปลผล
5. การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยให้มั่นใจได้ว่า บริษัทของท่านจะปฏิบัติตามกฎระเบียบของอุตสาหกรรมได้	3.71	0.89	มาก
การจัดการวิกฤต	**3.65**	**0.82**	**มาก**
1. การจัดการวิกฤตทำให้เกิดความเชื่อมั่นในสายตาของคู่ค้าในโซ่อุปทานดิจิทัลต่อปัญหาทางด้านความเสี่ยงที่บริษัทของท่านกำลังประสบอยู่	3.64	0.81	มาก
2. การจัดการวิกฤต ยิ่งดำเนินการได้เร็วมากแค่ไหน ยิ่งมีผลต่อชื่อเสียงของบริษัทมากขึ้นเท่านั้น	3.66	0.81	มาก
3. การจัดการวิกฤต ทำให้คู่ค้าในโซ่อุปทานดิจิทัลเห็นได้ว่าบริษัทของท่านมีความเป็นมืออาชีพในการบริหาร	3.66	0.83	มาก
การจัดการเหตุฉุกเฉิน	**3.63**	**0.89**	**มาก**
1. บริษัทของท่านมีการเตรียมการสำหรับการป้องกัน (Prevent) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ	3.65	0.85	มาก
2. บริษัทของท่านมีการเตรียมพร้อมรับมือ (Preparedness) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ	3.63	0.92	มาก
3. บริษัทของท่านมีแผนในการตอบสนอง (Response) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ	3.65	0.91	มาก
4. บริษัทของท่านมีแผนสำหรับการฟื้นฟูแก้ไข (Recovery) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ	3.60	0.90	มาก
เฉลี่ยรวม	**3.68**	**0.86**	**มาก**

จากตารางที่ 4.11 แสดงการวิเคราะห์ข้อมูลระดับความคิดเห็นเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านแผนการจัดการความต่อเนื่องทางธุรกิจ อยู่ในระดับมาก

($\bar{X}$ = 3.70, S.D. = 0.86) โดยสามารถเรียงลำดับความคิดเห็นด้านแผนการจัดการความต่อเนื่องทางธุรกิจ จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ แผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.74, S.D. = 0.82) รองลงมาคือ แผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้ ($\bar{X}$ = 3.74, S.D. = 0.88) แผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยงที่สามารถทำให้กิจการดำเนินต่อไปได้ ($\bar{X}$ = 3.68, S.D. = 0.81) แผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้ ($\bar{X}$ = 3.68, S.D. = 0.87) และแผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจ และจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัท พร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม ($\bar{X}$ = 3.66, S.D. = 0.90) ตามลำดับ

ส่วนด้านแผนกู้คืนภัยพิบัติ พบว่าผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านแผนกู้คืนภัยพิบัติ อยู่ในระดับมาก ($\bar{X}$ = 3.73, S.D. = 0.86) โดยสามารถเรียงลำดับความคิดเห็นด้านแผนกู้คืนภัยพิบัติ จากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ แผนกู้คืนภัยพิบัติทำให้สามารถประหยัดค่าใช้จ่ายในการกู้คืนระบบ เนื่องจากมีการทำแผนการปฏิบัติรองรับไว้แล้ว ($\bar{X}$ = 3.77, S.D. = 0.84) รองลงมาคือ แผนกู้คืนภัยพิบัติทำให้มีการจัดการเกี่ยวกับระบบการจัดการเครือข่ายในบริษัทได้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.74, S.D. = 0.79) การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยในการรักษาชื่อเสียงของบริษัทของท่านกับลูกค้าและคู่ค้าได้ ($\bar{X}$ = 3.74, S.D. = 0.91) การมีโซลูชั่นในการกู้คืนระบบสามารถช่วยให้มั่นใจได้ว่า บริษัทของท่านจะปฏิบัติตามกฎระเบียบของอุตสาหกรรมได้ ($\bar{X}$ = 3.71, S.D. = 0.89) และแผนกู้คืนภัยพิบัติได้เข้ามาจัดการเกี่ยวกับเครื่องมืออุปกรณ์ ที่จะนำมาใช้แก้ปัญหาเมื่อเกิดภัยพิบัติได้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.70, S.D. = 0.83) ตามลำดับ

ส่วนด้านการจัดการวิกฤต พบว่าผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านการจัดการวิกฤต อยู่ในระดับมาก ($\bar{X}$ = 3.65, S.D. = 0.82) โดยสามารถเรียงลำดับความคิดเห็นด้านการจัดการวิกฤต จากรายการข้อคำถาม ที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ การจัดการวิกฤตยิ่งดำเนินการได้เร็วมากแค่ไหน ยิ่งมีผลต่อชื่อเสียงของบริษัทมากขึ้นเท่านั้น ($\bar{X}$ = 3.66, S.D. = 0.81) รองลงมาคือการจัดการวิกฤต ทำให้คู่ค้าในโซ่อุปทานดิจิทัลเห็นได้ว่าบริษัทของท่านมีความเป็นมืออาชีพในการบริหาร ($\bar{X}$ = 3.66, S.D. = 0.83) และ การจัดการวิกฤตทำให้เกิดความเชื่อมั่นในสายตาของคู่ค้าในโซ่อุปทานดิจิทัล ต่อปัญหาทางด้านความเสี่ยงที่บริษัทของท่านกำลังประสบอยู่ ($\bar{X}$ = 3.64, S.D. = 0.81) ตามลำดับ

ส่วนด้านการจัดการเหตุฉุกเฉิน พบว่าผู้ตอบแบบสอบถามมีระดับความคิดเห็นด้านการจัดการเหตุฉุกเฉิน อยู่ในระดับมาก ($\bar{X}$ = 3.63, S.D. = 0.89) โดยสามารถเรียงลำดับความคิดเห็นด้านการจัดการเหตุฉุกเฉินจากรายการข้อคำถามที่มีค่าเฉลี่ยมากที่สุดไปหารายการข้อคำถามที่มีค่าเฉลี่ยต่ำสุด ดังนี้ บริษัทของท่านมีการเตรียมการสำหรับการป้องกัน (Prevent) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.65, S.D. = 0.85) รองลงมาคือ บริษัทของท่านมีแผนในการตอบสนอง (Response) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.65, S.D. = 0.91) บริษัทของท่านมีการเตรียมพร้อมรับมือ (Preparedness) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.63, S.D. = 0.92) และบริษัทของท่านมีแผนสำหรับการฟื้นฟูแก้ไข (Recovery) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ ($\bar{X}$ = 3.60, S.D. = 0.90) ตามลำดับ

เมื่อพิจารณาในภาพรวมพบว่า ผู้ตอบแบบสอบถามมีระดับความคิดเห็นเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจของโซ่อุปทานดิจิทัลของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมอยู่ในระดับมาก ($\bar{X}$ = 3.68, S.D. = 0.86)

ตอนที่ 4 ผลการวิเคราะห์การตรวจสอบข้อมูลก่อนการวิเคราะห์โมเดลสมการโครงสร้าง

4.1 ผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่สังเกตได้

การวิเคราะห์ข้อมูลในส่วนนี้ จะเป็นการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่สังเกตได้ เพื่อที่จะทำการตรวจสอบการแจกแจงปกติของตัวแปรเดียว ซึ่งเป็นข้อตกลงเบื้องต้นของการตรวจสอบข้อมูลก่อนวิเคราะห์ข้อมูลก่อนการวิเคราะห์โมเดลสมการโครงสร้าง โดยในงานวิจัยนี้ได้ใช้โปรแกรม AMOS มาทำการวิเคราะห์ เนื่องจากการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรจะทำให้นักวิจัยทราบว่าลักษณะการแจกแจงของตัวแปรเป็นแบบใด โดยผู้วิจัยได้ทำการวิเคราะห์ด้วยสถิติเชิงพรรณนา ที่ประกอบด้วย ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard deviation) ค่าความเบ้ (Skewness) ความโด่ง (Kurtosis) เพื่อทำให้สามารถสรุปได้ว่า ตัวแปรในการวิจัยแต่ละตัวมีการแจกแจงแบบปกติหรือไม่อย่างไร โดยการตรวจสอบการแจกแจงปกติของตัวแปรเดียวนิยมตรวจสอบโดยพิจารณาค่าความเบ้ (Skewness) ความโด่ง (Kurtosis) (ธานี จิตร์รัว และคณะ, 2559) ซึ่งประกอบด้วย ค่าสถิติพื้นฐานของตัวแปรที่สังเกตได้ ซึ่งเป็นตัวแปรบ่งชี้ของตัวแปรแฝง (Latent Variable) จำนวน 5 องค์ประกอบ คือ (1) ความร่วมมือกันของโซ่อุปทานดิจิทัล (Digital Supply Chain Collaboration) โดยมีตัวแปรที่สังเกตได้ที่ศึกษาจำนวน 4 ด้าน ได้แก่ การแบ่งปันข้อมูลร่วมกัน (Information Sharing) ความไว้ใจ (Trust) ความร่วมมือกันในการสื่อสาร (Collaborative Communication) และ การสร้างความรู้ร่วมกัน (Knowledge Sharing) (2) ปัญหาภัยคุกคามไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Threat Problem) โดยมีตัวแปรที่สังเกตได้ที่ศึกษา

จำนวน 3 ด้าน ได้แก่ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (External Motivation of Cyber Attacks) ช่องโหว่ของดำเนินงานภายใน (Internal Organizational Vulnerabilities) การรับมือต่อภัยคุกคามไซเบอร์ (Threats Coping) (3) การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Supply Chain Cyber Risk Management) โดยมีตัวแปรที่สังเกตได้ที่ศึกษาจำนวน 3 ด้าน ได้แก่ ด้านบุคลากร (People) ด้านกระบวนการ (Process) และด้านเทคโนโลยี (Technology) (4) การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber-Resilient Supply Chain) โดยมีตัวแปรที่สังเกตได้ที่ศึกษาจำนวน 2 ด้าน ได้แก่ ความคล่องตัว (Agility) และความทนทาน (Robust) และ (5) การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Digital Business Continuity Management) โดยมีตัวแปรที่สังเกตได้ที่ศึกษาจำนวน 4 ด้าน ได้แก่ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan) การจัดการวิกฤต (Crisis Management) การจัดการเหตุฉุกเฉิน (Emergency Management)

ตารางที่ 4.12 แสดงค่าสถิติพรรณนาลักษณะของตัวแปร (N = 1,864)

ตัวแปร	$\bar{X}$	S.D.	MIN	MAX	แปลผล	Skewness	Kurtosis
X1	3.69	0.768	1.000	5.000	มาก	-0.902	1.376
X2	3.73	0.704	1.000	5.000	มาก	-0.809	1.302
X3	3.70	0.720	1.000	5.000	มาก	-0.798	1.244
X4	3.68	0.770	1.000	5.000	มาก	-0.675	0.692
X5	3.56	0.825	1.000	5.000	มาก	-0.553	0.112
X6	3.60	0.753	1.000	5.000	มาก	-0.726	1.016
X7	3.66	0.798	1.000	5.000	มาก	-0.806	1.026
X8	3.72	0.729	1.000	5.000	มาก	-0.809	0.975
X9	3.73	0.699	1.000	5.000	มาก	-0.905	1.262
X10	3.62	0.755	1.000	5.000	มาก	-0.470	0.229
Y1	3.70	0.757	1.000	5.000	มาก	-0.687	0.629
Y2	3.66	0.729	1.000	5.000	มาก	-0.707	0.807
Y3	3.70	0.722	1.000	5.000	มาก	-0.687	0.933
Y4	3.73	0.743	1.000	5.000	มาก	-0.929	1.212
Y5	3.65	0.732	1.000	5.000	มาก	-0.666	0.952
Y6	3.63	0.801	1.000	5.000	มาก	-0.676	0.467

จากตารางที่ 4.12 แสดงการวิเคราะห์ค่าสถิติพรรณนาลักษณะของตัวแปรที่สังเกตได้ พบว่า ตัวแปรที่สังเกตได้ส่วนใหญ่มีค่าเฉลี่ยอยู่ในระดับมาก ($\overline{X}$ = 3.56 - 3.73) ซึ่งค่าเฉลี่ยดังกล่าวแสดงให้เห็นว่าผู้ตอบแบบสอบถามมีความเห็นว่าธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมมีความร่วมมือกันของโซ่อุปทานดิจิทัลในด้านการแบ่งปันข้อมูลร่วมกัน ความไว้ใจ ความร่วมมือกันในการสื่อสาร และการสร้างความรู้ร่วมกันอยู่ในระดับมาก มีปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลในด้าน แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก ช่องโหว่ของดำเนินงานภายใน และการรับมือต่อภัยคุกคามไซเบอร์อยู่ในระดับมาก มีการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลในด้านบุคลากร กระบวนการ และเทคโนโลยีอยู่ในระดับมาก ในประเด็นของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้ตอบแบบสอบถามมีความเห็นว่า ธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมมีความสามารถการการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ในด้านความคล่องตัวและความทนทานอยู่ในระดับมาก ส่วนการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ผู้ตอบแบบสอบถามมีความเห็นว่า ธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม มีการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในด้าน แผนความต่อเนื่องทางธุรกิจ แผนกู้คืนภัยพิบัติ การจัดการวิกฤต และการจัดการเหตุฉุกเฉิน อยู่ในระดับมาก และมีค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) อยู่ระหว่าง 0.69 - 0.82 แสดงให้เห็นว่าข้อมูลมีการกระจายอยู่ใกล้กับค่าเฉลี่ย เนื่องจากค่าส่วนเบี่ยงเบนมาตรฐานดังกล่าวมีค่าไม่เกิน 1

เมื่อพิจารณาค่าความเบ้ (Skewness) หรือความไม่สมมาตรของการแจกแจงในภาพรวม พบว่า ตัวแปรที่มีอยู่ในแบบจำลองทั้งหมดมีการแจกแจงในลักษณะเบ้ซ้าย (ค่าความเบ้เป็นลบ) แสดงว่าข้อมูลของตัวแปรทั้งหมดมีค่าคะแนนสูงกว่าค่าเฉลี่ย โดยมีค่าความเบ้อยู่ระหว่าง -0.553 ถึง -0.902 เมื่อพิจารณาค่าความโด่ง (Kurtosis) หรือความสูงของการแจกแจง พบว่า ตัวแปรที่มีอยู่ในแบบจำลองทั้งหมดมีค่าความโด่งต่ำกว่าปกติ (Platykurtic) โดยค่าความโด่งที่คำนวณได้จะมากกว่าศูนย์หรือมีค่าเป็นบวก แสดงว่าข้อมูลของตัวแปรที่สังเกตได้ดังกล่าวมีการกระจายข้อมูลในลักษณะโค้งแบนกว่าปกติ ข้อมูลมีการกระจายมากกว่าการแจกแจงปกติ ซึ่งหมายความว่าข้อมูลของตัวแปรที่สังเกตได้มีการกระจายมาก โดยมีค่าความโด่งอยู่ระหว่าง 0.112 ถึง 1.376 แต่อย่างไรก็ตาม เมื่อพิจารณาค่าความเบ้และความโด่ง พบว่า ค่าความเบ้และความความโด่งมีความแตกต่างจากศูนย์เพียงเล็กน้อย แต่จัดว่าใกล้ศูนย์ จึงถือว่าตัวแปรที่สังเกตได้มีการแจกแจงเป็นโค้งปกติ มีความเหมาะสมที่จะนำไปวิเคราะห์โมเดลสมการเชิงโครงสร้างต่อไป

4.2 ผลการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้

ผู้วิจัยทำการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้โดยพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson's Product Moment Correlation) ทำให้ได้เมทริกซ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ เพื่อตรวจสอบข้อตกลงเบื้องต้นของการวิเคราะห์โมเดลสมการเชิงโครงสร้าง เนื่องจากข้อตกลงเบื้องต้นที่สำคัญของการวิเคราะห์องค์ประกอบ คือ ตัวแปรต้องมีความสัมพันธ์กัน เพื่อวัตถุประสงค์หลักของการวิเคราะห์องค์ประกอบในการรวมกลุ่มของ ตัวแปรที่สัมพันธ์กัน ซึ่งการตรวจสอบว่าตัวแปรมีความสัมพันธ์กันมากหรือไม่ ผู้วิจัยใช้ค่าสถิติทดสอบ 2 ค่า คือ Kaiser-Mayer-Olkin Measure of Sampling Adequacy (KMO) และสถิติ Bartlett's test of sphericity เพื่อทดสอบว่าตัวแปรที่สังเกตได้ทั้งหมดเป็นเมทริกซ์เอกลักษณ์ (Identity Matrix) หรือไม่ (สุภมาส อังศุโชติ และคณะ, 2554) ผลการวิเคราะห์สามารถนำเสนอได้ดังตารางที่ 4.13 ดังต่อไปนี้

ตารางที่ 4.13 แสดงค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรที่สังเกตได้

	X1	**X2**	**X3**	**X4**	**X5**	**X6**	**X7**	**X8**	**X9**	**X10**	**Y1**	**Y2**	**Y3**	**Y4**	**Y5**	**Y6**
X1	1.000															
X2	.797**	1.000														
X3	.804**	.826**	1.000													
X4	.771**	.794**	.785**	1.000												
X5	.688**	.659**	.655**	.690**	1.000											
X6	.715**	.702**	.696**	.720**	.803**	1.000										
X7	.745**	.719**	.728**	.705**	.694**	.764**	1.000									
X8	.709**	.697**	.719**	.685**	.619**	.679**	.743**	1.000								
X9	.729**	.715**	.753**	.686**	.609**	.715**	.787**	.784**	1.000							
X10	.708**	.714**	.724**	.750**	.702**	.731**	.748**	.712**	.748**	1.000						
Y1	.738**	.741**	.736**	.754**	.679**	.708**	.756**	.743**	.782**	.812**	1.000					
Y2	.702**	.734**	.720**	.748**	.666**	.699**	.727**	.712**	.738**	.827**	.855**	1.000				
Y3	.705**	.715**	.729**	.722**	.629**	.686**	.733**	.735**	.799**	.775**	.823**	.829**	1.000			
Y4	.688**	.675**	.713**	.621**	.566**	.644**	.742**	.738**	.825**	.682**	.756**	.714**	.803**	1.000		
Y5	.669**	.673**	.673**	.660**	.602**	.663**	.702**	.684**	.755**	.704**	.750**	.767**	.776**	.770**	1.000	
Y6	.680**	.690**	.688**	.724**	.635**	.650**	.703**	.683**	.719**	.763**	.795**	.808**	.787**	.722**	.769**	1.000

Bartlett's test of sphericity = 35325.806, df = 120, p = 0.000, KMO = 0.974

หมายเหตุ **p < 0.01

จากตารางที่ 4.13 ผลการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรที่สังเกตได้ จำนวน 16 ตัวแปร พบว่า ความสัมพันธ์ระหว่างตัวแปรทั้งหมด 120 คู่ ซึ่งเป็นตัวแปรที่สังเกตได้ทั้งหมดมีความสัมพันธ์กันและความสัมพันธ์ของตัวแปรทุกคู่มีทิศทางเดียวกัน โดยมีค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรเป็นความสัมพันธ์ทางบวก มีขนาดของความสัมพันธ์หรือค่าสัมประสิทธิ์สหสัมพันธ์อยู่ระหว่าง 0.566 - 0.855 อย่างมีนัยสำคัญทางสถิติที่ระดับ .01

เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ที่ใช้วัดตัวแฝงเดียวกัน พบว่า ตัวแปรที่สังเกตได้ทุกคู่มีความสัมพันธ์ในทิศทางเดียวกัน (ทางบวก) อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 โดยตัวแปรที่สังเกตได้ที่มีระดับความสัมพันธ์กันสูงมาก ($r > 0.8$) จำนวน 5 คู่ และตัวแปรที่สังเกตได้ที่มีความสัมพันธ์กันในระดับสูง ($0.6 < r < 0.8$) จำนวน 14 คู่ ตัวแปรที่สังเกตได้คู่ที่มีความสัมพันธ์กันสูงมากที่สุด คือ ความคล่องตัว (Y1) กับ ความทนทาน (Y2) ($r = 0.855$) ส่วนตัวแปรคู่ที่มีความสัมพันธ์กันต่ำที่สุด คือ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) กับ การรับมือต่อภัยคุกคามไซเบอร์ (X7) ($r = 0.694$)

เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ที่ใช้วัดตัวแฝงต่างกัน พบว่า ตัวแปรที่สังเกตได้ทุกคู่มีความสัมพันธ์ในทิศทางเดียวกัน (ทางบวก) อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 โดยตัวแปรที่สังเกตได้ที่มีระดับความสัมพันธ์กันสูงมาก ($r > 0.8$) จำนวน 6 คู่ ตัวแปรที่สังเกตได้ที่มีความสัมพันธ์กันในระดับสูง ($0.6 < r < 0.8$) จานวน 94 คู่ และตัวแปรที่สังเกตได้ที่มีความสัมพันธ์กันในระดับปานกลาง ($0.4 < r < 0.6$) จำนวน 1 คู่ ตัวแปรที่สังเกตได้คู่ที่มีความสัมพันธ์กันสูงมากที่สุด คือ ความทนทาน (Y2) กับ แผนความต่อเนื่องทางธุรกิจ (Y3) ($r = 0.829$) ส่วนตัวแปรคู่ที่มีความสัมพันธ์กันต่ำที่สุด คือ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) กับ แผนกู้คืนภัยพิบัติ (Y4) ($r = 0.566$) แต่อย่างไรก็ตาม เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ทุกคู่ ในภาพรวม พบว่า ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ทุกคู่ส่วนใหญ่มีค่าไม่เกิน 0.80 ความสัมพันธ์ดังกล่าวแสดงให้เห็นว่าตัวแปรที่สังเกตได้มีระดับความสัมพันธ์ไม่สูงมากนัก ไม่เกิดปัญหาภาวะเส้นตรงร่วมเชิงพหุ (Multicollineartiry) และตัวแปรที่สังเกตได้ทั้งหมดอยู่บนองค์ประกอบร่วมกัน ดังนั้นมีความเหมาะสมที่จะนำไปวิเคราะห์โมเดลสมการเชิงโครงสร้าง

เมื่อพิจารณาค่าสถิติ Bartlett's test of sphericity พบว่า มีค่าเท่ากับ 35325.806, $df = 120$, $p = 0.000$ แสดงว่า เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ไม่เป็นเมทริกซ์เอกลักษณ์ (Indentity matrix) อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 ตัวแปรมีความสัมพันธ์กันอย่างเพียงพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ สอดคล้องกับผลการวิเคราะห์ Kaiser-Mayer-Olkin (KMO)

ซึ่งมีค่าใกล้ 1 (0.974) แสดงให้เห็นว่าตัวแปรที่สังเกตได้มีความสัมพันธ์กันมาก เหมาะสมในการนำไปใช้ในการตรวจสอบความสอดคล้องกลมกลืนกับโมเดลการวิจัยกับข้อมูลเชิงประจักษ์ต่อไป เนื่องจาก ค่าดัชนีมีค่า 0.80 ขึ้นไป แสดงว่า ข้อมูลเหมาะสมที่จะทำการวิเคราะห์องค์ประกอบ (Factor Analysis) ดีมาก (สุภมาส อังศุโชติ และคณะ, 2554 อ้างอิงจาก Hair et al., 2006)

ตอนที่ 5 ผลการวิเคราะห์ข้อมูลเพื่อตอบวัตถุประสงค์ของการศึกษา

5.1 ผลการวิเคราะห์ความตรงเชิงโครงสร้างของโมเดลการวัด (Construct Validity)

ผู้วิจัยได้ทำการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA) เพื่อการตรวจสอบความเหมาะสมและถูกต้องของโมเดลสมการเชิงโครงสร้างด้วยการพิจารณาค่าน้ำหนักองค์ประกอบ และค่า R^2 เพื่อตรวจสอบความผันแปรร่วมของตัวบ่งชี้ ซึ่งสามารถนำเสนอผลการวิเคราะห์แบ่งออกเป็น 5 ส่วน ได้แก่ (1) ความร่วมมือกันของโซ่อุปทานดิจิทัล (2) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (3) การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (4) ความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และ (5) การจัดการความต่อเนื่องทางธุรกิจดิจิทัล ดังนี้

1. ความร่วมมือกันของโซ่อุปทานดิจิทัล

ตัวแปรองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ประกอบด้วย 4 องค์ประกอบ ได้แก่ การแบ่งปันข้อมูลร่วมกัน (Information Sharing: X1) ความไว้ใจ (Trust: X2) ความร่วมมือกันในการสื่อสาร (Collaborative Communication: X3) และ การสร้างความรู้ร่วมกัน (Knowledge Sharing: X4)

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบทั้ง 4 องค์ประกอบของความร่วมมือกันของโซ่อุปทานดิจิทัล จำนวน 6 คู่ พบว่าค่าสหสัมพันธ์ของตัวแปรที่สังเกตได้แตกต่าง จากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 มีค่าความสัมพันธ์กันในระดับสูงระหว่าง 0.771-0.826 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.14

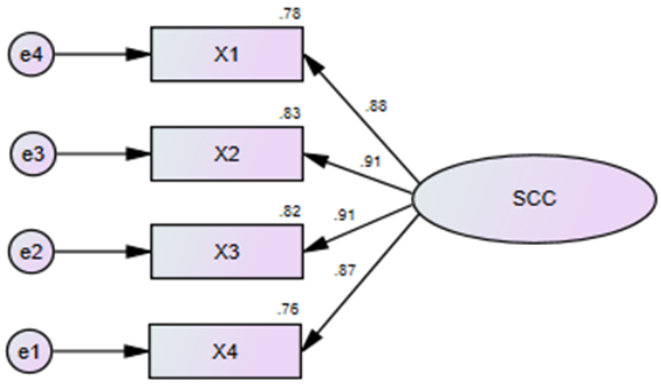
ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบเพื่อวิเคราะห์เมทริกซ์สหสัมพันธ์ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 6651.774 องศาอิสระ (*df*) เท่ากับ 6 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 แสดงว่า เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.869 แสดงว่า ตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้

ตารางที่ 4.14 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC)

	X1	X2	X3	X4
X1	1.000			
X2	.797**	1.000		
X3	.804**	.826**	1.000	
X4	.771**	.794**	.785**	1.000
MEAN	3.69	3.73	3.70	3.68
S.D.	0.769	0.704	0.720	0.770
Bartlett's test of sphericity Chi Square = 6651.774, df = 6, p = 0.000, KMO = 0.869				

หมายเหตุ **p < 0.01

สำหรับโมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล และผลการตรวจสอบความตรงของโมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล แสดงได้ดังภาพประกอบที่ 4.1 และตารางที่ 4.15 ตามลำดับ



ภาพประกอบที่ 4.1 แสดงโมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล

ตารางที่ 4.15 แสดงผลการตรวจสอบความตรงของโมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
X1	0.882	-	-	0.205	0.778
X2	0.909	0.016	57.529	0.294	0.826
X3	0.908	0.017	57.701	0.285	0.824
X4	0.871	0.019	52.845	0.186	0.758
Chi-Square = 3.382, *df* = 2, *p*-value = 0.184, RMSEA = 0.019, GFI = 0.999, AGFI = 0.996					

ผลการวิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 3.382 องศาอิสระ (*df)* เท่ากับ 2 *p*-value เท่ากับ 0.184 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.019 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.999 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.996 แสดงให้เห็นว่า โมเดลการวัดความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของความร่วมมือกันของโซ่อุปทานดิจิทัล พบว่า ตัวแปรมีน้ำหนักความสำคัญในการบ่งชี้ความเป็น ความร่วมมือกันของโซ่อุปทานดิจิทัล ทั้งหมด 4 ตัวแปร ซึ่งเรียงลำดับความสำคัญจากมากไปน้อย คือ ความไว้ใจ (X2) ความร่วมมือกันในการสื่อสาร (X3) การแบ่งปันข้อมูลร่วมกัน (X1) และการสร้างความรู้ร่วมกัน (X4) ตามลำดับ โดยมีค่าน้ำหนักองค์ประกอบเท่ากับ 0.909, 0.908, 0.882 และ 0.871 ตามลำดับ และมีความผันแปรร่วมของตัวบ่งชี้ความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 83, 82, 78 และ 76 ตามลำดับ ดังนั้นตัวแปรที่สังเกตได้ของตัวแปรแฝงด้านความร่วมมือกันของโซ่อุปทานดิจิทัลจึงสามารถใช้วัดความวมมือกันของโซ่อุปทานดิจิทัลได้จริง

2. ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตัวแปรองค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ประกอบด้วย 3 องค์ประกอบ ได้แก่ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (External Motivation of Cyber Attacks: X5) ช่องโหว่ของดำเนินงานภายใน (Internal Organizational Vulnerabilities: X6) และการรับมือต่อภัยคุกคามไซเบอร์ (Threats Coping: X7)

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบทั้ง 3 องค์ประกอบของปัญหาภัยคุกคามไซเบอร์ จำนวน 3 คู่ พบว่าค่าสหสัมพันธ์ของตัวแปรที่สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 มีค่าความสัมพันธ์กันในระดับสูงระหว่าง 0.357-0.661 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.16

ตารางที่ 4.16 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT)

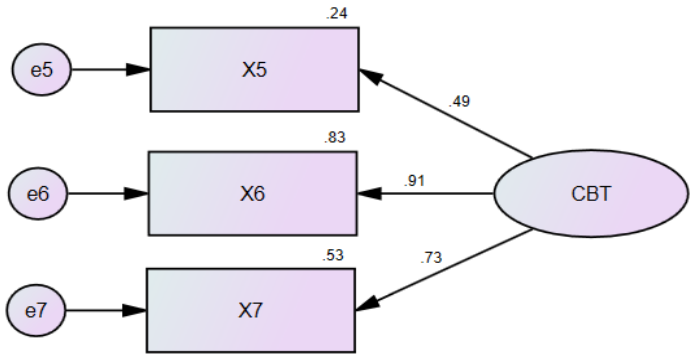
	X5	**X6**	**X7**
X5	1.000		
X6	.448**	1.000	
X7	.357**	.661**	1.000
MEAN	3.56	3.60	3.66
S.D.	0.825	0.753	0.798
Bartlett's test of sphericity Chi Square = 1495.720, df = 3, p = 0.000, KMO = 0.629			

หมายเหตุ **p < 0.01

ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 1495.720 องศาอิสระ (*df*) เท่ากับ 3 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 แสดงว่าเมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.629 แสดงว่า ตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้สำหรับโมเดลการวัดปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยผลการตรวจสอบความตรง ของโมเดลการวัดปัญหาภัยคุกคามไซเบอร์ แสดงได้ดังภาพประกอบที่ 4.2 และตารางที่ 4.17 ตามลำดับ

ผลการ วิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 0.419 องศาอิสระ (*df)* เท่ากับ 1 *p*-value เท่ากับ 0.517 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.000 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 1.000 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.999 แสดงให้เห็นว่าโมเดลการวัดปัญหา

ภัยคุกคามไซเบอร์ (CBT) มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล พบว่า ตัวแปรมีน้ำหนักความสำคัญในการบ่งชี้ความเป็น ปัญหาภัยคุกคามไซเบอร์ทั้งหมด 3 ตัวแปร ซึ่งเรียงลำดับความสำคัญจากมากไปน้อย คือ ช่องโหว่ของดำเนินงานภายใน (X6) การรับมือต่อภัยคุกคามไซเบอร์ (X7) และแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก(X5) ตามลำดับ โดยมีค่าน้ำหนักองค์ประกอบเท่ากับ 0.911, 0.726 และ 0.492 ตามลำดับ และมีความผันแปรร่วมของตัวบ่งชี้ปัญหาภัยคุกคามไซเบอร์ ร้อยละ 83, 53 และ 24 ตามลำดับ ดังนั้นตัวแปรที่สังเกตได้ของตัวแปรแฝงด้านปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล จึงสามารถใช้วัดปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลได้จริง



ภาพประกอบที่ 4.2 แสดงโมเดลการวัดปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทาน

ตารางที่ 4.17 แสดงผลการตรวจสอบความตรงของโมเดลการวัดปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบของปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
X5	0.492	-	-	0.044	0.242
X6	0.911	0.081	21.780	0.378	0.829
X7	0.726	0.069	19.718	0.112	0.526
Chi-Square = 0.419, *df* = 1, *p*-value = 0.517, RMSEA = 0.000, GFI = 1.000, AGFI = 0.999					

3. การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตัวแปรองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ประกอบด้วย 3 องค์ประกอบ ได้แก่ บุคลากร (People: X8) ด้านกระบวนการ (Process: X9) และด้านเทคโนโลยี (Technology: X10)

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบทั้ง 3 องค์ประกอบของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล จำนวน 3 คู่ พบว่าค่าสหสัมพันธ์ของตัวแปร ที่สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 มีค่าความสัมพันธ์กันในระดับสูงระหว่าง 0.712-0.784 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.18

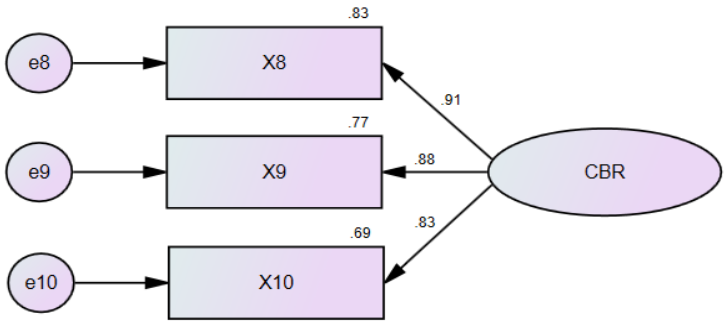
ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 3485.395 องศาอิสระ (*df*) เท่ากับ 3 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 แสดงว่า เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.746 แสดงว่า ตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้

ตารางที่ 4.18 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR)

	X8	**X9**	**X10**
X8	1.000		
X9	0.802**	1.000	
X10	0.760**	0.733**	1.000
MEAN	3.73	3.73	3.62
S.D.	0.783	0.699	0.755
Bartlett's test of sphericity Chi Square = 3746.789, df = 3, p = 0.000, KMO = 0.748			

หมายเหตุ **p < 0.01

สำหรับโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการตรวจสอบ ความตรงของโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล แสดงได้ดังภาพประกอบที่ 4.3 และตารางที่ 4.19 ตามลำดับ



ภาพประกอบที่ 4.3 แสดงโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตารางที่ 4.19 แสดงผลการตรวจสอบความตรงของโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
X8	0.912	-	-	0.425	0.832
X9	0.880	0.017	56.644	0.310	0.774
X10	0.833	0.019	50.446	0.201	0.694
Chi-Square = 1.078, *df* = 1, *p*-value = 0.299, RMSEA = 0.006, GFI = 1.000, AGFI = 0.998					

ผลการวิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 1.078 องศาอิสระ (*df*) เท่ากับ 0 *p*-value เท่ากับ 0.299 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.006 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 1.000 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.998 แสดงให้เห็นว่าโมเดลการวัดการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน

ดิจิทัล พบว่า ตัวแปรมีน้ำหนักความสำคัญในการบ่งชี้ในเรื่องการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลทั้งหมด 3 ตัวแปร ซึ่งเรียงลำดับความสำคัญจากมากไปน้อย คือ ความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลด้านบุคลากร (People: X8) ด้านกระบวนการ (Process : X9) และด้านเทคโนโลยี (Technology : X10) ตามลำดับ โดยมีค่าน้ำหนักองค์ประกอบเท่ากับ 0.912, 0.880 และ 0.833 ตามลำดับ และมีความผันแปรร่วมของตัวบ่งชี้ความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 83, 77 และ 69 ตามลำดับ ดังนั้นตัวแปรที่สังเกตได้ของตัวแปรแฝงด้านความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลจึงสามารถใช้วัดความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลได้จริง

4. การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตัวแปรองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ประกอบด้วย 2 องค์ประกอบ ได้แก่ ความคล่องตัว (Agility: Y1) และความคงทน (Robustness: Y2)

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบทั้ง 2 องค์ประกอบของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล จำนวน 1 คู่ พบว่าค่าสหสัมพันธ์ของตัวแปรที่สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 มีค่าความสัมพันธ์กันในระดับสูง ซึ่งมีค่าเท่ากับ 0.855 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.20

ตารางที่ 4.20 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS)

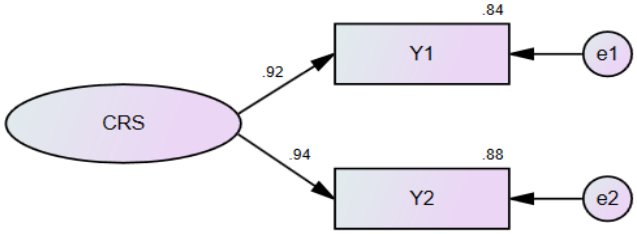
	Y1	**Y2**
Y1	1.000	
Y2	0.860**	1.000
MEAN	3.70	3.66
S.D.	0.757	0.729
Bartlett's test of sphericity Chi Square = 2438.970, df = 1, p = 0.000, KMO = 0.500		

หมายเหตุ **p < 0.01

ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 2438.970 องศาอิสระ (*df*) เท่ากับ 1 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 แสดงว่า

เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.500 แสดงว่า ตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้

สำหรับโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการตรวจสอบความตรงของโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล แสดงได้ ดังภาพประกอบที่ 4.4 และตารางที่ 4.21 ตามลำดับ



ภาพประกอบที่ 4.4 แสดงโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตารางที่ 4.21 แสดงผลการตรวจสอบความตรงของโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
Y1	0.918			0.395	0.842
Y2	0.937	0.014	72.636	0.539	0.877
Chi-Square = 1.421, *df* = 1, *p*-value = 0.233, RMSEA = 0.015, GFI = 0.999, AGFI = 0.998					

ผลการวิเคราะห์โมเดลการวัด พบว่าค่า ไคสแควร์ (Chi-Square) เท่ากับ 1.421 องศาอิสระ (*df*) เท่ากับ 1 *p*-value เท่ากับ 0.233 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.015 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.999 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.998 แสดงให้เห็นว่าโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล พบว่า ตัวแปร

มีน้ำหนักความสำคัญในการบ่งชี้ในเรื่องการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ทั้งหมด 2 ตัวแปร ซึ่งเรียงลำดับความสำคัญจากมากไปน้อย คือ การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลความคงทน (Robustness: Y2) และด้านความคล่องตัว (Agility: Y1) ตามลำดับ โดยมีค่าน้ำหนักองค์ประกอบเท่ากับ 0.937 และ 0.818 ตามลำดับ และมีความผันแปรร่วมของตัวบ่งชี้ความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 88 และ 84 ตามลำดับ ดังนั้นตัวแปรที่สังเกตได้ของตัวแปรแฝงด้านการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลจึงสามารถใช้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลได้จริง

5. การจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ตัวแปรองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ประกอบด้วย 4 องค์ประกอบ ได้แก่ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: Y3) แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan: Y4) การจัดการวิกฤต (Crisis Management: Y5) และการจัดการเหตุฉุกเฉิน (Emergency Management: Y6)

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบทั้ง 4 องค์ประกอบ ของการจัดการความความต่อเนื่องทางธุรกิจดิจิทัล จำนวน 6 คู่ พบว่าค่าสหสัมพันธ์ของตัวแปรที่ สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 มีค่าความสัมพันธ์กันในระดับสูงระหว่าง 0.722-0.803 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.22

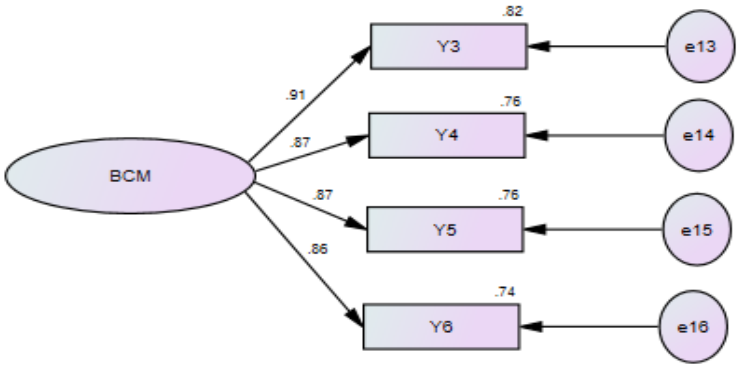
ตารางที่ 4.22 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM)

	Y3	**Y4**	**Y5**	**Y6**
Y3	1.000			
Y4	.803**	1.000		
Y5	.776**	.770**	1.000	
Y6	.787**	.722**	.769**	1.000
MEAN	3.70	3.73	3.65	3.63
S.D.	0.722	0.743	0.732	0.801
Bartlett's test of sphericity Chi Square = 6100.823, df =6, p = 0.000, KMO = 0.852				

หมายเหตุ **p < 0.01

ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 6100.823 องศาอิสระ (*df*) เท่ากับ 6 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 แสดงว่า เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.852 แสดงว่า ตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้

สำหรับโมเดลการวัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และผลการตรวจสอบความตรงของโมเดลการจัดการความต่อเนื่องทางธุรกิจดิจิทัล แสดงได้ดังภาพประกอบที่ 4.5 และตารางที่ 4.23 ตามลำดับ



ภาพประกอบที่ 4.5 แสดงโมเดลการวัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ตารางที่ 4.23 แสดงผลการตรวจสอบความตรงของโมเดลการวัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจดิจิทัล)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
Y3	0.908			0.181	0.739
Y4	0.872	0.018	54.985	0.221	0.763
Y5	0.874	0.018	55.245	0.215	0.760
Y6	0.860	0.020	53.397	0.314	0.824
Chi-Square = 60.190, *df* = 2, *p*-value = 0.000, RMSEA = 0.125, GFI = 0.985, AGFI = 0.926					

ผลการวิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 60.190 องศาอิสระ (*df)* เท่ากับ 2 *p*-value เท่ากับ 0.000 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.125 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.985 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.926 แสดงให้เห็นว่าโมเดลการวัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (CBM) มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของการจัดการความต่อเนื่องทางธุรกิจ พบว่า ตัวแปรมีน้ำหนักความสำคัญในการบ่งชี้ในเรื่องการจัดการความต่อเนื่องทางธุรกิจดิจิทัลทั้งหมด 4 ตัวแปร ซึ่งเรียงลำดับความสำคัญจากมากไปน้อย คือ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: Y3) การจัดการวิกฤต (Crisis Management: Y5) แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan: Y4) และการจัดการเหตุฉุกเฉิน (Emergency Management: Y6) ตามลำดับ โดยมีค่าน้ำหนักองค์ประกอบเท่ากับ 0.908, 0.874, 0.872 และ 0.860 ตามลำดับ และมีความผันแปรร่วมของตัวบ่งชี้การจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 74, 76, 76 และ 82 ตามลำดับ ดังนั้นตัวแปรที่สังเกตได้ของตัวแปรแฝงด้านการจัดการความต่อเนื่องทางธุรกิจจึงสามารถใช้วัดการจัดการความต่อเนื่องทางธุรกิจได้จริง

5.2 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันของตัวแปรแฝงภายนอก

ผู้วิจัยได้ทำการวิเคราะห์องค์ประกอบเชิงยืนยันสำหรับตัวแปรทั้ง 3 องค์ประกอบ คือ ความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อพิจารณาน้ำหนักองค์ประกอบของรายการคำถาม รวมถึงเพื่อเป็น การตรวจสอบและยืนยันว่าตัวบ่งชี้หรือตัวแปรที่สังเกตได้ โดยจะได้นำไปใช้วัดเฉพาะตัวแปรแฝงตามที่กำหนดเท่านั้น

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบย่อยทั้ง 10 องค์ประกอบขององค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล รวมทั้งหมด 45 คู่ พบว่า ค่าสหสัมพันธ์ของ ตัวแปรที่สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 ทั้ง 45 คู่ มีความสัมพันธ์กันในระดับสูงและสูงมากระหว่าง 0.609 - 0.826 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.24

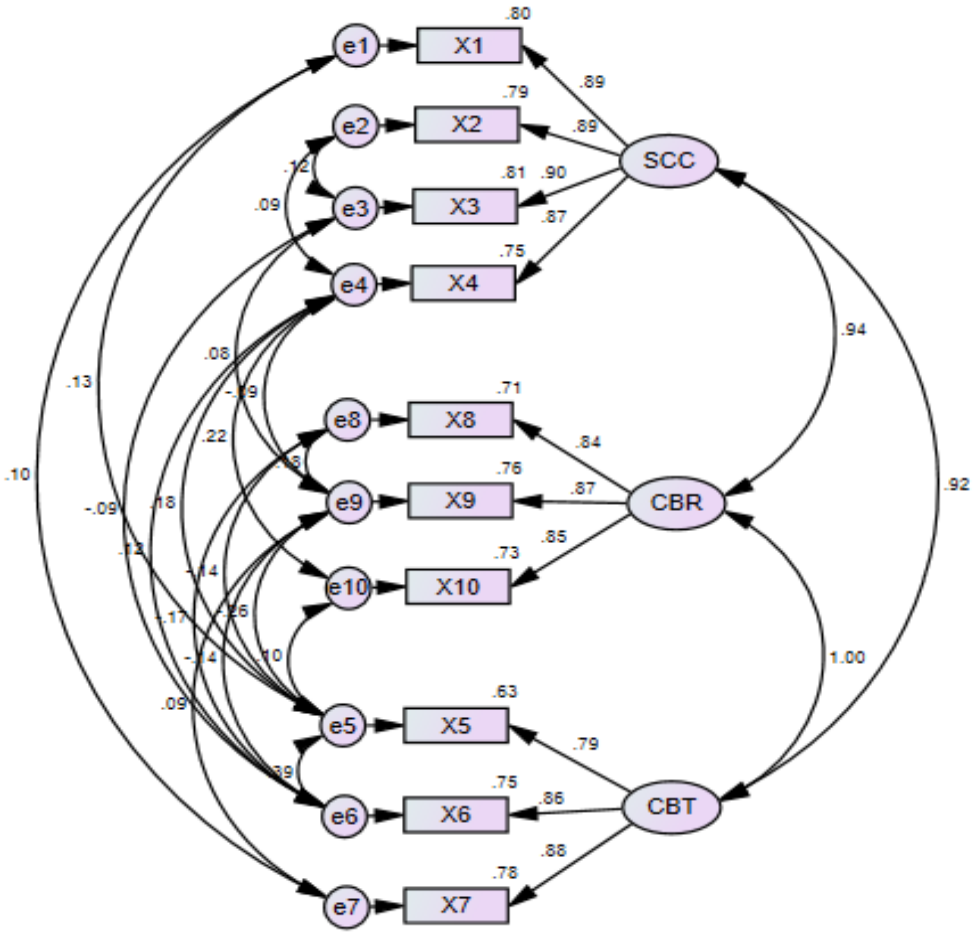
ตารางที่ 4.24 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดความร่วมมือกันของโซ่ปุทาน (SCC) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR)

	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10
X1	1.000									
X2	.797**	1.000								
X3	.804**	.826**	1.000							
X4	.771**	.794**	.785**	1.000						
X5	.688**	.659**	.655**	.690**	1.000					
X6	.715**	.702**	.696**	.720**	.803**	1.000				
X7	.745**	.719**	.728**	.705**	.694**	.764**	1.000			
X8	.709**	.697**	.719**	.685**	.619**	.679**	.743**	1.000		
X9	.729**	.715**	.753**	.686**	.609**	.715**	.787**	.784**	1.000	
X10	.708**	.714**	.724**	.750**	.702**	.731**	.748**	.712**	.748**	1.000
MEAN	3.69	3.73	3.70	3.68	3.56	3.60	3.66	3.73	3.73	3.62
S.D.	0.769	0.704	0.720	0.770	0.825	0.753	0.798	0.783	0.699	0.755
Bartlett's test of sphericity Chi Square = 19352.424, df =45, p = 0.000, KMO = 0.956										

หมายเหตุ **p < 0.01

ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 19352.424 องศาอิสระ (*df*) เท่ากับ 45 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 แสดงว่า เมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.956 แสดงว่าตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้ดีมาก

สำหรับการวิเคราะห์องค์ประกอบเชิงยืนยันโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลแสดงได้ตามภาพประกอบที่ 4.6 และตารางที่ 4.25 แสดงผลการตรวจสอบความตรงของโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล



ภาพประกอบที่ 4.6 แสดงผลการวิเคราะห์องค์ประกอบเชิงยืนยันโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการวิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 16.824 องศาอิสระ (*df)* เท่ากับ 14 *p*-value เท่ากับ 0.265 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.010 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.998 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.993 แสดงให้เห็นว่าโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งเป็นตัวแปรที่สังเกตได้ทั้งหมด 10 ตัวแปร มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของทุกองค์ประกอบมีค่าแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยมีค่าตั้งแต่ 0.791 - 0.903 ค่าสัมประสิทธิ์ความเที่ยงของตัวแปรที่สังเกตได้ทุกตัวซึ่งวัดได้จากค่า R^2 มีค่าตั้งแต่ 0.625 - 0.815 ซึ่งสามารถอธิบายได้ดังนี้

ตารางที่ 4.25 แสดงผลการตรวจสอบความตรงของโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบ)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
X1	0.893				0.797
X2	0.888	0.016	55.337		0.789
X3	0.903	0.016	57.955		0.815
X4	0.868	0.018	53.453		0.753
X5	0.791				0.625
X6	0.864	0.019	52.107		0.746
X7	0.882	0.026	42.274		0.778
X8	0.843				0.711
X9	0.873	0.018	52.501		0.762
X10	0.852	0.021	46.183		0.725
Chi-Square = 16.824, *df* = 14, *p*-value = 0.265, RMSEA = 0.010, GFI = 0.998, AGFI = 0.993					

(1) องค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ ความร่วมมือกันในการสื่อสาร (X3) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.903 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 81.5 รองลงมาคือ การแบ่งปันข้อมูลร่วมกัน (X1) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.893 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 79.7 ความไว้ใจ (X2) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.888 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 78.9 และ การสร้างความรู้ร่วมกัน (X4) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.868 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 75.3

(2) องค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ การรับมือต่อภัยคุกคามไซเบอร์ (X7) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.882 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 77.8 รองลงมาคือ ช่องโหว่ของดำเนินงานภายใน (X6) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.864 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 74.6 และแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.791 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 62.5

(3) องค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทานดิจิทัล (CBR) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ ด้านกระบวนการ (X9) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.873 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทานดิจิทัล ร้อยละ 76.2 รองลงมาคือ ด้านเทคโนโลยี (X10) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.852 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทานดิจทัล ร้อยละ 72.5 และด้านบุคลากร (X8) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.843 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทานดิจิทัล ร้อยละ 71.1

สำหรับการปรับโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลแสดงได้ ตามตารางที่ 4.26

ตารางที่ 4.26 แสดงการปรับโมเดลการวัดองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

ค่าดัชนี	เกณฑ์	ก่อนปรับ		หลังปรับ	
		ค่าสถิติ	ผลการพิจารณา	ค่าสถิติ	ผลการพิจารณา
CMIN	< 2.00	20.607	ไม่ผ่านเกณฑ์	1.203	ผ่านเกณฑ์
RMSEA	< 0.05	0.103	ไม่ผ่านเกณฑ์	0.010	ผ่านเกณฑ์
GFI	≥ 0.95	0.925	ไม่ผ่านเกณฑ์	0.998	ผ่านเกณฑ์
AGFI	≥ 0.95	0.871	ไม่ผ่านเกณฑ์	0.993	ผ่านเกณฑ์

ผลการวิเคราะห์ตัวแปรองค์ประกอบเชิงยืนยันสำหรับ ตัวแปรความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล พบว่า โมเดลการวัดตัวแปรแฝงทั้ง 3 โมเดล มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์โดยมีค่าดัชนีความกลมกลืนทั้ง 4 ดัชนีที่ผ่านเกณฑ์การยอมรับ คือ ค่าดัชนีไค-สแควร์สัมพัทธ์ (CMIN) เท่ากับ 1.203 ค่าดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.998 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.993 และ ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.010 ดังนั้น จึงสรุปได้ว่าโมเดลแบบจำลองสมการเชิงโครงสร้างมีความเหมาะสม กลมกลืนกับข้อมูลเชิงประจักษ์

5.3 ผลการวิเคราะห์องค์ประกอบเชิงยืนยันของตัวแปรแฝงภายใน

ผู้วิจัยได้ทำการวิเคราะห์องค์ประกอบเชิงยืนยันสำหรับตัวแปรทั้ง 2 องค์ประกอบ ได้แก่ องค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล เพื่อพิจารณาน้ำหนักองค์ประกอบของรายการคำถาม รวมถึงเพื่อเป็นการตรวจสอบและยืนยันว่าตัวบ่งชี้หรือตัวแปรที่สังเกตได้ใช้วัดเฉพาะตัวแปรแฝงตามที่กำหนดเท่านั้น

ผู้วิจัยทำการตรวจสอบค่าสหสัมพันธ์ระหว่างองค์ประกอบย่อยทั้ง 6 องค์ประกอบขององค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล รวมทั้งหมด 15 คู่ พบว่า ค่าสหสัมพันธ์ของตัวแปรที่สังเกตได้แตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ทั้ง 15 คู่ มีความสัมพันธ์กันในระดับสูงและสูงมากระหว่าง 0.714 - 0.855 ผลการวิเคราะห์เมทริกซ์สหสัมพันธ์แสดงได้ดังตารางที่ 4.27

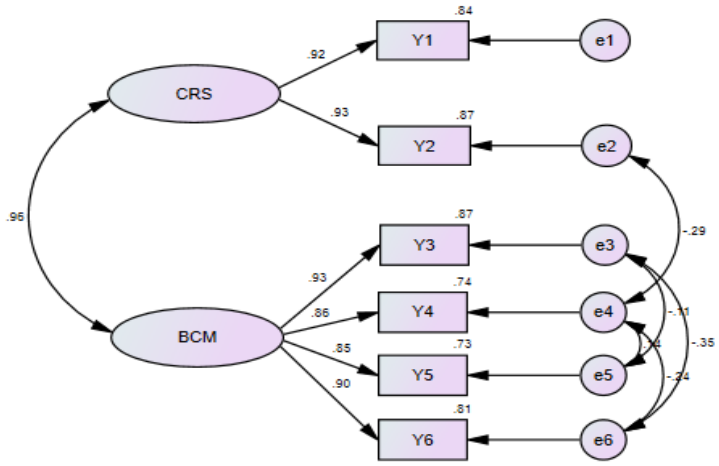
ผู้วิจัยได้ใช้สถิติ Bartlett's test of sphericity ในการทดสอบ จากผลการวิเคราะห์ได้ค่า Bartlett's test of Sphericity Chi-Square เท่ากับ 11707.468 องศาอิสระ (*df*) เท่ากับ 15 *p*-value เท่ากับ 0.000 ซึ่งแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 แสดงว่าเมทริกซ์สัมประสิทธิ์สหสัมพันธ์ของตัวแปรที่สังเกตได้ไม่ใช่เมทริกซ์เอกลักษณ์ (Identity Matrix) และตัวแปรมีความสัมพันธ์กันมากพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ และค่าดัชนี Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.921 แสดงว่าตัวแปรมีความเหมาะสมที่จะวิเคราะห์องค์ประกอบได้ดีมาก

ตารางที่ 4.27 แสดงเมทริกซ์สหสัมพันธ์ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานของตัวแปรที่สังเกตได้ของโมเดลการวัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM)

	Y1	Y2	Y3	Y4	Y5	Y6
Y1	1.000					
Y2	.855**	1.000				
Y3	.823**	.829**	1.000			
Y4	.756**	.714**	.803**	1.000		
Y5	.750**	.767**	.776**	.770**	1.000	
Y6	.795**	.808**	.787**	.722**	.769**	1.000
Bartlett's test of sphericity Chi Square = 11707.468, df =15, p = 0.000, KMO = 0.921						

หมายเหตุ **p < 0.01

สำหรับการวิเคราะห์องค์ประกอบเชิงยืนยันโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล แสดงได้ตามภาพประกอบที่ 4.7 และตารางที่ 4.28 ที่ได้แสดงผลการตรวจสอบความตรงของโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล



ภาพประกอบที่ 4.7 แสดงผลการวิเคราะห์องค์ประกอบเชิงยืนยันโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ตารางที่ 4.28 แสดงผลการตรวจสอบความตรงของโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจ (ค่าน้ำหนักองค์ประกอบ ความตรงของตัวแปรที่สังเกตได้ และสัมประสิทธิ์คะแนนองค์ประกอบ)

ตัวแปร	น้ำหนักองค์ประกอบ				
	สัมประสิทธิ์	SE	t	คะแนนองค์ประกอบ	R^2
Y1	0.918				0.843
Y2	0.930	0.014	69.360		0.866
Y3	0.932				0.868
Y4	0.860	0.017	54.388		0.739
Y5	0.854	0.017	53.590		0.729
Y6	0.902	0.019	57.275		0.814
Chi-Square = 2.269, *df* = 3, *p*-value = 0.518, RMSEA = 0.000, GFI = 1.000, AGFI = 0.997					

ผลการวิเคราะห์โมเดลการวัด พบว่าค่าไค-สแควร์ (Chi-Square) เท่ากับ 2.269 องศาอิสระ (*df*) เท่ากับ 3 *p*-value เท่ากับ 0.518 ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.000 ดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 1.000 ดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.997 แสดงให้เห็นว่าโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจ ซึ่งเป็นตัวแปรที่สังเกตได้ทั้งหมด 6 ตัวแปร มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เมื่อพิจารณาองค์ประกอบย่อยของทุกองค์ประกอบมีค่าแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยมีค่าตั้งแต่ 0.854 - 0.932 ค่าสัมประสิทธิ์ความเที่ยงของตัวแปรที่สังเกตได้ทุกตัว ซึ่งวัดได้จากค่า R^2 มีค่าตั้งแต่ 0.729 - 0.868 ซึ่งสามารถอธิบายได้ดังนี้

(1) องค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ ความคงทน (Y2) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.930 และมีความแปรผันร่วมกันกับองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 86.6 และความคล่องตัว (Y1) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.918 และมีความแปรผันร่วมกันกับองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 84.3

(2) องค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ (BCM) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ แผนความต่อเนื่องทางธุรกิจ (Y3) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.932 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 86.8 รองลงมาคือ การจัดการเหตุฉุกเฉิน (Y6) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.902 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 81.4 แผนกู้คืนภัยพิบัติ (Y4) น้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.860 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 73.9 และการจัดการวิกฤต (Y5) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.854 และมีความแปรผันร่วมกันกับองค์ประกอบองค์การสีเขียว ร้อยละ 72.9

สำหรับการปรับโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจ แสดงได้ตามตารางที่ 4.29 ผลการวิเคราะห์ตัวแปรองค์ประกอบเชิงยืนยันสำหรับ ตัวแปรความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล พบว่า โมเดลการวัดตัวแปรแฝงทั้ง 3 โมเดล มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์โดยมีค่าดัชนีความกลมกลืนทั้ง 4 ดัชนีที่ผ่านเกณฑ์การยอมรับ คือค่าดัชนีไค-สแควร์สัมพัทธ์(CMIN) เท่ากับ 1.203 ค่าดัชนีวัดระดับความกลมกลืน (GFI) เท่ากับ 0.998 ค่าดัชนีวัดระดับความกลมกลืนที่ปรับแก้แล้ว (AGFI) เท่ากับ 0.993 และ ค่าดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนโดยประมาณ (RMSEA) เท่ากับ 0.010 ดังนั้น จึงสรุปได้ว่าโมเดลแบบจำลองสมการเชิงโครงสร้างมีความเหมาะสม กลมกลืนกับข้อมูลเชิงประจักษ์

ตารางที่ 4.29 แสดงการปรับโมเดลการวัดองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน และการจัดการความต่อเนื่องทางธุรกิจ

ค่าดัชนี	เกณฑ์	ก่อนปรับ		หลังปรับ	
		ค่าสถิติ	ผลการพิจารณา	ค่าสถิติ	ผลการพิจารณา
CMIN	< 2.00	29.373	ไม่ผ่านเกณฑ์	0.756	ผ่านเกณฑ์
RMSEA	< 0.05	0.123	ไม่ผ่านเกณฑ์	0.000	ผ่านเกณฑ์
GFI	$\geq$ 0.95	0.962	ผ่านเกณฑ์	1.000	ผ่านเกณฑ์
AGFI	$\geq$ 0.95	0.899	ไม่ผ่านเกณฑ์	0.997	ผ่านเกณฑ์

5.4 ผลการวิเคราะห์ความเที่ยงของตัวแปรแฝง (Construct Reliability: ρ_c) และค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Average Variance Extracted: ρ_v)

ผู้วิจัยทำการตรวจสอบความเที่ยงของตัวแปรแฝง (Construct Reliability : ρ_c) และค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Average Variance Extracted : ρ_v) โดยค่าความเที่ยงของตัวแปรแฝง (Construct Reliability : ρ_c) ควรมีค่ามากกว่า 0.60 และค่าเฉลี่ยของการผันแปรที่ถูกสกัดได้ (Average Variance Extracted : ρ_v) ซึ่งเป็นค่าเฉลี่ยความแปรปรวนของตัวแปรแฝงที่อธิบายได้ด้วยตัวแปรที่สังเกตได้ ซึ่งมีค่าเทียบเท่ากับค่าไอเกน (Eigen values) ในการวิเคราะห์องค์ประกอบเชิงสำรวจ ควรมีค่ามากกว่า 0.50 (สุภมาส อังศุโชติ และคณะ, 2554 อ้างอิงจาก Diamantopoulos & Siguaw, 2000)

จึงสรุปว่า การผันแปรในตัวชี้วัดส่วนใหญ่เกิดขึ้นจากตัวแปรสร้างมากกว่าเป็นข้อผิดพลาดของมาตรวัด ซึ่งแสดงว่าตัวแปรแฝงมีความเที่ยง ซึ่งสามารถแสดงผลการวิเคราะห์ได้ดังตารางที่ 4.30 ความเที่ยงของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Construct Reliability : ρ_c & Average Variance Extracted : ρ_v)

ตารางที่ 4.30 แสดงความเที่ยงของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Construct Reliability : ρ_c & Average Variance Extracted : ρ_v)

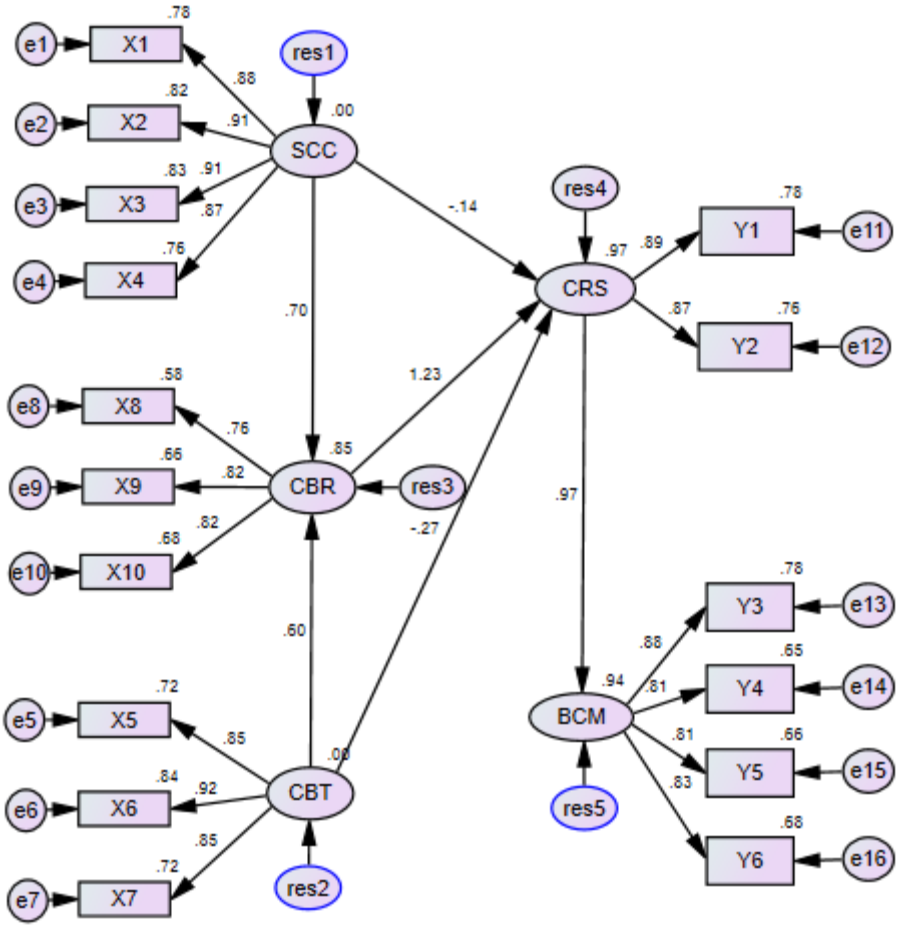
ตัวแปรแฝง	ความเที่ยงตัวแปรแฝง (ρ_c)	ความแปรปรวนเฉลี่ยที่สกัดได้ด้วยองค์ประกอบ (ρ_v)
SCC	0.964	0.789
CBT	0.923	0.717
CBR	0.936	0.733
CRS	0.955	0.854
BCM	0.964	0.788

จากตารางที่ 4.30 แสดงให้เห็นว่าความเที่ยงของตัวแปรแฝงทุกตัวมีค่าสูง โดยมีค่า ρ_c อยู่ระหว่าง 0.923 - 0.964 ซึ่งมากกว่า 0.60 และค่าเฉลี่ยความแปรปรวนที่สกัดได้ด้วยองค์ประกอบมีค่า ρ_v อยู่ระหว่าง 0.717 - 0.854 ซึ่งมากกว่า 0.50 แสดงว่า จากการประเมินโมเดลมาตรวัดได้หลักฐานที่ชัดเจนว่า การนิยามปฏิบัติการตัวแปรแฝงทั้งหมดถูกต้องและเชื่อถือได้

5.5 ผลการวิเคราะห์โมเดลสมการโครงสร้างตามสมมติฐาน

ผู้วิจัยได้ทำการวิเคราะห์โมเดลความสัมพันธ์ระหว่างความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ด้วยวิธีการ Maximum Liklihood ด้วยโปรแกรมสำเร็จรูป AMOS 21.0.0 เพื่อทำการเปรียบเทียบถึงความกลมกลืนระหว่างโมเดลที่พัฒนาขึ้นกับข้อมูลเชิงประจักษ์ โดยเกณฑ์ในการตรวจสอบความสอดคล้องกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ ผู้วิจัยพิจารณาจากค่าสถิติ ที่ประกอบด้วย ดัชนีค่า Chi-Square, CMIN, CFI, GFI, AGFI, RMSEA และ SRMR ซึ่งผลการวิเคราะห์โมเดล ครั้งแรก พบว่า ค่าดัชนีความกลมกลืนยังไม่สอดคล้องกับข้อมูลเชิงประจักษ์ หรือยังไม่เป็นไปตามเกณฑ์ที่กำหนดไว้ โดยพิจารณาจากค่า χ^2 เท่ากับ 3907.534 *df* เท่ากับ 98 *p*-value เท่ากับ 0.000 CFI เท่ากับ 0.892 GFI เท่ากับ 0.815 AGFI เท่ากับ 0.743 RMSEA เท่ากับ 0.144 และ SRMR เท่ากับ 0.276 ซึ่งผู้วิจัยได้นำเสนอโมเดลความสัมพันธ์ระหว่างความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจ ดังภาพประกอบที่ 4.8 ที่แสดงการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวม และตารางที่ 4.31 ที่แสดงการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวม

จากตารางที่ x31 แสดงให้เห็นว่าโมเดลความสัมพันธ์ระหว่างความร่วมมือกันของโซ่อุปทานดิจิทัล ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ที่ผู้วิจัยได้พัฒนาขึ้นมาจากแนวคิดและทฤษฎีที่เกี่ยวข้องยังไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยพิจารณาจากค่าสถิติที่คำนวณได้ คือ ค่า χ^2 เท่ากับ 3907.534 *df* เท่ากับ 98 *p*-value เท่ากับ 0.000 CFI เท่ากับ 0.892 GFI เท่ากับ 0.815 AGFI เท่ากับ 0.743 RMSEA เท่ากับ 0.144 และ SRMR เท่ากับ 0.276 ซึ่งค่าสถิติที่สำคัญบางตัวยังไม่ผ่านเกณฑ์ตามที่กำหนดไว้ (Joreskog & Sorbom, 1996)



ภาพประกอบที่ 4.8 แสดงการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวม

ตารางที่ 4.31 แสดงการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวม

ดัชนีความกลมกลืน	เกณฑ์	ค่าดัชนีที่วัดได้	ผลการพิจารณา
CMIN	< 2.00	39.873	ไม่ผ่านเกณฑ์
CFI	≥ 0.95	0.892	ไม่ผ่านเกณฑ์
GFI	≥ 0.95	0.815	ไม่ผ่านเกณฑ์
AGFI	≥ 0.95	0.743	ไม่ผ่านเกณฑ์
RMSEA	< 0.05	0.144	ไม่ผ่านเกณฑ์
SRMR	< 0.05	0.276	ไม่ผ่านเกณฑ์

ผู้วิจัยจึงได้ดำเนินการปรับโมเดล (Model Modification) โดยพิจารณาจากคำแนะนำในการปรับพารามิเตอร์ในโมเดลด้วยค่าดัชนีปรับโมเดล (Model Modification Indices: MI) จากนั้นปรับพารามิเตอร์โดยยินยอมให้ผ่อนคลายข้อตกลงเบื้องต้นให้ค่าความคลาดเคลื่อนสัมพันธ์กันได้ จนกระทั่งค่าดัชนีความกลมกลืนมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยรายละเอียดของ การปรับแก้โมเดลเพื่อให้มีความสอดคล้องกลมกลืน (Model fit) กับข้อมูลเชิงประจักษ์ ผู้วิจัยนำเสนอผลได้ดังตารางที่ 4.32 แสดงรายละเอียดการปรับโมเดลให้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

ตารางที่ 4.32 แสดงรายละเอียดการปรับโมเดลให้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

ครั้งที่	คู่ความสัมพันธ์ของค่าความคลาดเคลื่อนที่ทำการปรับ	χ^2	*df*	*p*-value	RMSEA
1	SCC กับ CBT	1724.566	97	0.0000	0.095
2	X9 กับ Y4	1424.670	96	0.000	0.086
3	X5 กับ X6	1197.796	95	0.000	0.079
4	X10 กับ Y2	1100.245	94	0.000	0.076
5	X4 กับ Y4	1015.229	93	0.000	0.073
6	X5 กับ X9	939.533	92	0.000	0.070
7	X4 กับ X9	876.409	91	0.000	0.068
8	X7 กับ Y4	830.260	90	0.000	0.066
9	Y2 กับ Y4	781.175	89	0.000	0.065
10	X9 กับ Y2	713.186	88	0.000	0.062
11	X10 กับ Y4	672.814	87	0.000	0.060
12	X8 กับ X9	633.643	86	0.000	0.058
13	X8 กับ Y4	601.370	85	0.000	0.057
14	X8 กับ Y2	570.044	84	0.000	0.056
15	X4 กับ X7	546.457	83	0.000	0.055
16	X4 กับ CBT	508.974	82	0.000	0.053
17	X1 กับ CBT	480.38	81	0.000	0.051
18	X5 กับ Y4	456.32	80	0.000	0.050

ตารางที่ 4.32 (ต่อ)

ครั้งที่	คู่ความสัมพันธ์ของค่าความคลาดเคลื่อนที่ทำการปรับ	χ^2	*df*	*p*-value	RMSEA
19	Y1 กับ Y5	437.655	79	0.000	0.049
20	X10 กับ Y5	419.103	78	0.000	0.048
21	X4 กับ Y6	403.047	77	0.000	0.048
22	Y5 กับ Y6	383.853	76	0.000	0.047
23	X1 กับ Y2	369.144	75	0.000	0.046
24	Y4 กับ Y5	353.090	74	0.000	0.045
25	Y5 กับ CBT	338.072	73	0.000	0.044
26	Y3 กับ Y4	320.671	72	0.000	0.043
27	X9 กับ Y3	300.416	71	0.000	0.042
28	X5 กับ Y3	287.567	70	0.000	0.041
29	X1 กับ X10	275.395	69	0.000	0.040
30	X9 กับ Y5	260.56	68	0.000	0.039
31	X5 กับ Y5	249.876	67	0.000	0.038
32	X5 กับ X8	236.116	66	0.000	0.037
33	X5 กับ X7	218.355	65	0.000	0.036
34	X7 กับ X9	202.96	64	0.000	0.034
35	X4 กับ X8	191.926	63	0.000	0.033
36	X3 กับ Y4	182.912	62	0.000	0.032
37	X3 กับ X9	166.817	61	0.000	0.031
38	X1 กับ Y3	156.397	60	0.000	0.029
39	X3 กับ X8	144.478	59	0.000	0.028
40	X3 กับ Y2	133.284	58	0.000	0.026
41	X7 กับ X10	120.99	57	0.000	0.025
42	X7 กับ Y2	105.991	56	0.000	0.022
43	X1 กับ Y4	99.39	55	0.000	0.021

ตารางที่ 4.32 (ต่อ)

ครั้งที่	คู่ความสัมพันธ์ของค่าความคลาดเคลื่อนที่ทำการปรับ	χ^2	*df*	*p*-value	RMSEA
44	X2 กับ X6	93.74	54	0.001	0.020
45	Y2 กับ Y6	87.537	53	0.002	0.019
46	X10 กับ Y6	41.740	30	0.075	0.014

จากตารางที่ 4.32 พบว่าในการปรับแก้โมเดลครั้งที่ 1 ระหว่าง SCC และ CBT ที่มีความสัมพันธ์กัน พบว่า มีการเปลี่ยนแปลงไปในทิศทางที่ดีขึ้น คือ χ^2 ลดลงจาก 3907.534 เป็น 1724.566 และค่า RMSEA ก็ลดลงเช่นเดียวกันจาก 0.144 เป็น 0.095 แสดงให้เห็นว่าการปรับแก้โมเดลเพื่อให้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ด้วยวิธีการดังกล่าวได้ผลค่อนข้างดี และไม่เป็นการแก้ไขแนวคิดและทฤษฎีที่ใช้ในการวิจัยด้วย เพราะเป็นการปรับที่ความคลาดเคลื่อนมาตรฐานของตัวแปรเชิงประจักษ์โดยไม่ได้เปลี่ยนทิศทางความสัมพันธ์ระหว่างตัวแปรในแบบจำลอง จากการปรับแก้โมเดลดังกล่าว โดยการวิเคราะห์ค่าดัชนีความกลมกลืนของโมเดลโดยรวม ซึ่งผลที่ได้จากการวิเคราะห์ที่ผู้วิจัยได้ดำเนินการปรับโมเดลทำให้สามารถนำเสนอผลการวิเคราะห์ได้ดังตารางที่ 4.33 ซึ่งเป็นการแสดงผลของการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวมหลังจากการปรับแก้โมเดล เพื่อให้มีความสอดคล้องกลมกลืน (Model Fit) กับข้อมูลเชิงประจักษ์

ตารางที่ 4.33 แสดงการวิเคราะห์ค่าดัชนีความสอดคล้องกลมกลืนของโมเดลโดยรวมหลังจากการปรับแก้โมเดล

ดัชนีความกลมกลืน	**เกณฑ์**	**ค่าดัชนีที่วัดได้**	**ผลการพิจารณา**
CMIN	< 2.00	1.391	ผ่านเกณฑ์
CFI	$\geq$ 0.95	1.000	ผ่านเกณฑ์
GFI	$\geq$ 0.95	0.997	ผ่านเกณฑ์
AGFI	$\geq$ 0.95	0.987	ผ่านเกณฑ์
RMSEA	< 0.05	0.014	ผ่านเกณฑ์
SRMR	< 0.05	0.003	ผ่านเกณฑ์

จากตารางที่ 4.33 เมื่อพิจารณาค่าดัชนีความกลมกลืนของโมเดล พบว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์โดยมีค่าดัชนีความกลมกลืนทั้ง 6 ดัชนีที่ผ่านเกณฑ์การยอมรับ ได้แก่ค่าดัชนี CMIN เท่ากับ 1.391 CFI เท่ากับ 1.000 GFI เท่ากับ 0.997 AGFI เท่ากับ 0.987 RMSEA เท่ากับ 0.014 และ SRMR = 0.003 จากผลการวิเคราะห์ค่าดัชนีความสอดคล้องความกลมกลืนของโมเดลโดยรวมหลังจากการปรับแก้โมเดล จึงสรุปได้ว่าโมเดลแบบจำลองสมการเชิงโครงสร้างมีความเหมาะสม กลมกลืนกับข้อมูลเชิงประจักษ์ซึ่งสามารถอธิบายได้ ดังนี้

1. ค่าไค-สแควร์สัมพัทธ์ (CMIN) มีค่าเท่ากับ 1.391 แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เนื่องจากค่าไค-สแควร์สัมพัทธ์มีค่าน้อยกว่า 2.00

2. ดัชนีวัดความสอดคล้องกลมกลืนเชิงสัมพัทธ์ (Comparative Fit Index : CFI) มีค่าเท่ากับ 1.000 แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เนื่องจากค่า CFI มีค่า 0.90 ขึ้นไป

3. ดัชนีวัดความสอดคล้องกลมกลืนเชิงสัมบูรณ์ (Absolute Fit Index) ซึ่งผู้วิจัยพิจารณาค่า 2 ดัชนี คือ ดัชนีวัดความกลมกลืน (Goodness of Fit Index : GFI) มีค่าเท่ากับ 0.997 และดัชนีวัดความกลมกลืนที่ปรับแก้ไขแล้ว (Adjusted Goodness of Fit Index : AGFI) มีค่าเท่ากับ 0.987 แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เนื่องจากค่า GFI และค่า AGFI มีค่าระหว่าง 0 ถึง 1 และค่า GFI และค่า AGFI ที่ยอมรับได้มีค่ามากกว่า 0.95

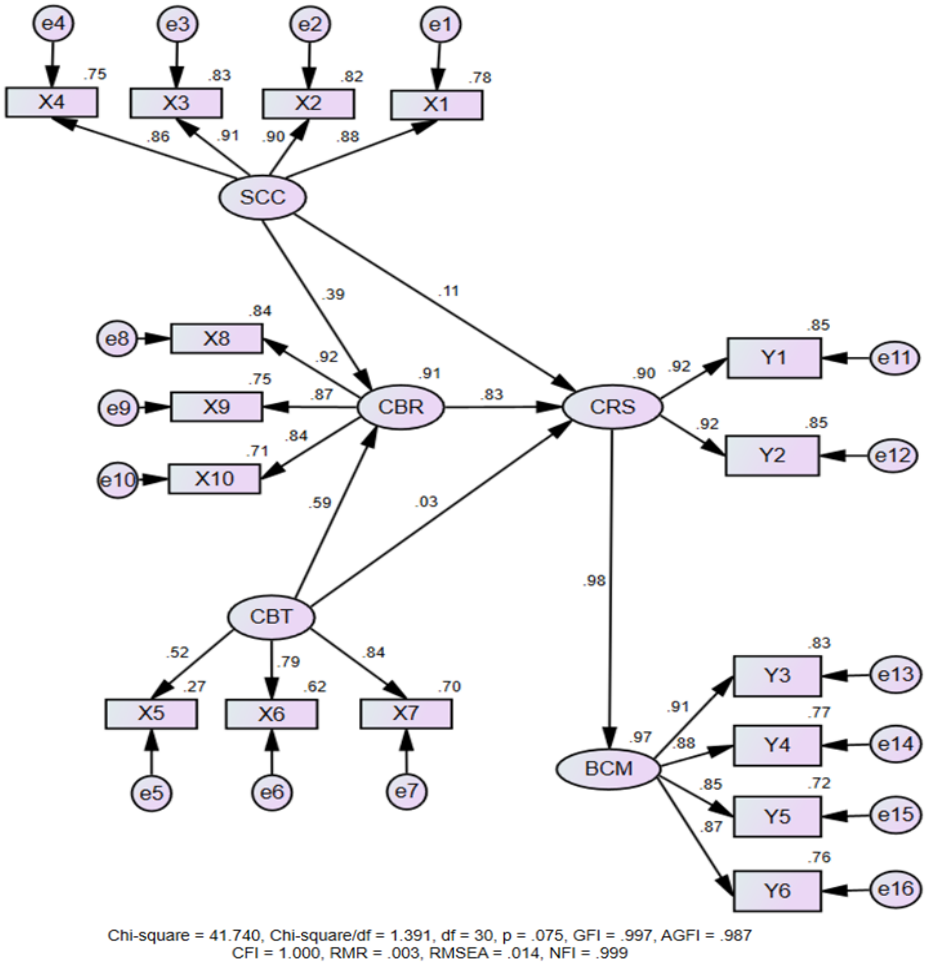
4. ดัชนีรากที่สองของค่าเฉลี่ยความคลาดเคลื่อนกำลังสองของการประมาณค่า (Root Mean Square Error of Approximation : RMSEA) มีค่าเท่ากับ 0.014 หมายถึง โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เนื่องจากค่า RMSEA มีค่าน้อยกว่า 0.05 หรือมีค่าระหว่าง 0.05 ถึง 0.08

5. ดัชนีวัดความสอดคล้องกลมกลืนในรูปความคลาดเคลื่อน โดยดัชนีที่ผู้วิจัยนำมาใช้ในการพิจารณา คือ รากที่สองของค่าเฉลี่ยกำลังสองของส่วนเหลือมาตรฐาน (Standardized Root Mean Square Residual : SRMR) มีค่าเท่ากับ 0.003 แสดงว่า โมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ เนื่องจากมีค่าน้อยกว่า 0.05

ตอนที่ 6 ผลการวิเคราะห์เส้นทาง

6.1 ผลการวิเคราะห์อิทธิพลเชิงสาเหตุของความสามารถสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลและการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ผู้วิจัยทำการวิเคราะห์อิทธิพลเชิงสาเหตุของความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการการจัดการความต่อเนื่องทางธุรกิจดิจิทัล เพื่อทำการตอบคำถาม การวิจัยและสมมติฐานการวิจัย โดยผู้วิจัยนำได้เสนอผลของอิทธิพลทางตรง (Direct Effects : DE) อิทธิพลทางอ้อม (Indirect Effects : IE) และอิทธิพลรวม (Total Effects : TE) ตามสมมติฐานกับข้อมูลเชิงประจักษ์ พบว่า โมเดลดังกล่าว มีความสอดคล้องกับข้อมูลเชิงประจักษ์ ดังภาพประกอบที่ 4.9



ภาพประกอบที่ 4.9 แสดงผลการวิเคราะห์อิทธิพลของตัวแปรในโมเดลเชิงสาเหตุของปัจจัยที่ส่งผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

และตารางที่ 4.34 แสดงการวิเคราะห์อิทธิพลของตัวแปรในโมเดลเชิงสาเหตุของปัจจัยที่ส่งผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (อิทธิพลทางตรง อิทธิพลทางอ้อม และอิทธิพลรวม)

ตารางที่ 4.34 แสดงการวิเคราะห์อิทธิพลของตัวแปรในโมเดลเชิงสาเหตุของปัจจัยที่ส่งผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ปัจจัยเหตุ	**SCC**			**CBT**			**CBR**			**CRS**		
ปัจจัยผล	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**
CBR	0.394	0.394	-	0.590	0.590	-	-	-	-	-	-	-
CRS	0.431	0.106	0.325	0.515	0.027	0.488	0.827	0.827	-			
BCM	0.424	-	0.424	0.506	-	0.506	0.813	-	0.813	0.983	0.983	-

ค่าสถิติ

ไคว์-สแควร์ = 41.740, *df* = 30, *p*-value = 0.075, GFI = 0.997, AGFI = 0.987, RMR = 0.003, RMSEA = 0.014

ตัวแปร	**X1**	**X2**	**X3**	**X4**	**X5**	**X6**	**X7**	**X8**	**X9**	**X10**
ความเที่ยง	0.782	0.815	0.831	0.748	0.272	0.616	0.704	0.838	0.749	0.709
ตัวแปร	**Y1**	**Y2**	**Y3**	**Y4**	**Y5**	**Y6**				
ความเที่ยง	0.855	0.852	0.831	0.769	0.723	0.758				

สมการโครงสร้างของตัวแปร	**CBR**	**CRS**	**BCM**
R-Square	0.913	0.902	0.967

เมทริกซ์สหสัมพันธ์ระหว่างตัวแปรแฝง

ตัวแปรแฝง	**SCC**	**CBT**	**CBR**	**CRS**	**BCM**
SCC	1.000				
CBT	0.882	1.000			
CBR	0.914	0.937	1.000		
CRS	0.885	0.895	0.948	1.000	
BCM	0.870	0.880	0.933	0.983	1.000

หมายเหตุ $p < 0.01$

จากตารางที่ 4.34 แสดงผลการทดสอบความสอดคล้องของโมเดลเชิงสาเหตุของปัจจัยที่ส่งผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลของการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ตามสมมติฐานกับข้อมูลเชิงประจักษ์ พบว่า โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยพิจารณาจากค่าสถิติที่ใช้ตรวจสอบความสอดคล้องระหว่างโมเดลกับข้อมูลเชิงประจักษ์ ได้แก่ ค่าไคว์-สแควร์ มีค่าเท่ากับ 41.740 องศาอิสระเท่ากับ 30 ค่าความน่าจะเป็น (p) เท่ากับ 0.075 นั่นคือ ค่าไคว์-สแควร์ แตกต่างจากศูนย์อย่างไม่มีนัยสำคัญ แสดงว่ายอมรับสมมติฐานหลักที่ว่า โมเดลเชิงสาเหตุของปัจจัยที่ส่งผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการจัดการความต่อเนื่องทางธุรกิจดิจิทัลที่พัฒนาขึ้นสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งสอดคล้องกับผลการวิเคราะห์ค่าดัชนีวัดความกลมกลืน (GFI) มีค่าเท่ากับ 0.997 ค่าดัชนีวัดความกลมกลืนที่ปรับแก้แล้ว (AGFI) มีค่าเท่ากับ 0.987 ซึ่งมีค่าเข้าใกล้ 1 และค่าดัชนีรากกำลังสองเฉลี่ยของส่วนที่เหลือ (RMR) มีค่าเท่ากับ 0.003 ซึ่งเข้าใกล้ศูนย์ โดยรายละเอียดดังกล่าวผู้วิจัยได้กล่าวไว้แล้วอย่างละเอียดในส่วนของผลการวิเคราะห์ค่าดัชนีความกลมกลืนของโมเดลปัจจัยเหตุที่มีผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และผลการการจัดการความต่อเนื่องทางธุรกิจดิจิทัลข้างต้น

เมื่อพิจารณาค่าความเที่ยงของตัวแปรที่สังเกตได้ พบว่า ตัวแปรที่สังเกตได้มีค่าความเที่ยงอยู่ระหว่าง 0.272 - 0.855 โดยตัวแปรที่มีความเที่ยงสูงสุด คือ ความคล่องตัว (Y1) มีค่าความเที่ยงเท่ากับ 0.855 รองลงมาคือ ความคงทน (Y2) มีค่าความเที่ยงเท่ากับ 0.852 และการจัดการความเสี่ยงทางไซเบอร์ด้านบุคลากร (X8) มีค่าความเที่ยงเท่ากับ 0.838 ส่วนตัวแปรที่มีความเที่ยงต่ำสุด คือ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) มีค่าความเที่ยงเท่ากับ 0.272

สำหรับค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของสมการโครงสร้างตัวแปรแฝงภายใน พบว่า ค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทาน (CBR) มีค่าเท่ากับ 0.913 หรือตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทาน (CBR) ได้ร้อยละ 91.3 ค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) มีค่าเท่ากับ 0.902 หรือตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้ร้อยละ 90.2 และค่าสัมประสิทธิ์การพยากรณ์ (R^2) ของผลการการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) มีค่าเท่ากับ 0.967 หรือตัวแปรในโมเดลสามารถอธิบายความแปรปรวนของผลการการจัดการความต่อเนื่องทางธุรกิจ (BCM) ได้ร้อยละ 96.7

เมทริกซ์สหสัมพันธ์ระหว่างตัวแปรแฝง พบว่า ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรแฝงมีค่าอยู่ระหว่าง 0.870 - 0.983 โดยตัวแปรทุกคู่ มีความสัมพันธ์แบบทิศทางเดียวกัน คือ มีค่าความสัมพันธ์เป็นบวก และตัวแปรแฝงทุกคู่ที่มีความสัมพันธ์กันสูงมาก (r > 0.8) ซึ่งมีจำนวนทั้งหมด 10 คู่ ตัวแปรแฝงที่มีค่าสัมประสิทธิ์สหสัมพันธ์มากที่สุดซึ่งมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.981 (r = 0.983) คือ การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) กับความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) รองลงมาคือความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) กับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.948 (r = 0.948) การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) กับปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.937 (r = 0.937) การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) กับการจัดการความเสี่ยงทางไซเบอร์ของ โซ่อุปทานดิจิทัล (CBR) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.933 (r = 0.933) การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) กับความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.914 (r = 0.914) ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) กับ ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.895 (r = 0.895) ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) กับความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.885 (r = 0.885) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) กับความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.882 (r = 0.882) การจัดการความต่อเนื่องทางธุรกิจ (BCM) กับปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.880 (r = 0.880) และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) กับความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.870 (r = 0.870)

เมื่อพิจารณาอิทธิพลทางตรงและทางอ้อมที่ส่งผลต่อตัวแปรการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) พบว่า ตัวแปรดังกล่าวได้รับอิทธิพลทางตรงจากความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) โดยมีขนาดอิทธิพลทางตรงเท่ากับ 0.983 ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ .01 นอกจากนี้ การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) ได้รับอิทธิพลทางอ้อมจากการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) และความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) โดยมีขนาดอิทธิพลเท่ากับ 0.813, 0.506, และ 0.424 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ .01

นอกจากอิทธิพลทางตรงและทางอ้อมที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) ยังมีตัวแปรอื่น ๆ ที่ได้รับอิทธิพลทางตรงและทางอ้อม ได้แก่ ตัวแปรความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลทางตรงจากการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) และปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) โดยมีขนาดของอิทธิพลเท่ากับ 0.827, 0.027, 0.106 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01 นอกจากนี้ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลทางอ้อมจากปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) และความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) โดยมีขนาดของอิทธิพลเท่ากับ 0.488 และ 0.325 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01 และตัวแปรการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ที่ได้รับอิทธิพลทางตรงจากปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) และความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) โดยมีขนาดของอิทธิพลเท่ากับ 0.590 และ 0.394 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

จากการพิจารณาถึงอิทธิพลทางตรงและทางอ้อมที่ส่งผลต่อตัวแปรการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) และการจัดการความต่อเนื่องทางธุรกิจ (BCM) สามารถสรุปถึงอิทธิพลทางตรงและทางอ้อมของตัวแปรต่างๆ เหล่านี้ได้ดังต่อไปนี้

1) ความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) และความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) โดยมีขนาดอิทธิพลทางตรงเท่ากับ 0.394, 0.106 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

2) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) และความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) โดยมีขนาดอิทธิพลทางตรงเท่ากับ 0.590, 0.027 ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

3) การจัดความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีอิทธิพลทางตรงเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) โดยมีขนาดอิทธิพลทางตรงเท่ากับ 0.827 ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

4) ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลดิจิทัล (BCM) โดยมีขนาดอิทธิพลทางตรงเท่ากับ 0.983 ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

5) ความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) และ ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีอิทธิพลทางอ้อมเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ผ่านการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) โดยมีขนาดอิทธิพลทางอ้อมเท่ากับ 0.325 และ 0.488 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

6) ความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) ผ่านความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) โดยมีขนาดอิทธิพลทางอ้อมเท่ากับ 0.424, 0.506 และ 0.813 ตามลำดับ ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01

6.2 ผลการวิเคราะห์ค่าน้ำหนักองค์ประกอบของตัวแปรที่สังเกตได้

ผู้วิจัยทำการวิเคราะห์ค่าน้ำหนักองค์ประกอบของตัวแปรที่สังเกตได้ เพื่อพิจารณาถึงองค์ประกอบร่วมที่สามารถอธิบายถึงความสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ ซึ่งผลการวิเคราะห์สามารถแสดงได้ดังตารางที่ 4.35 แสดงค่าน้ำหนักองค์ประกอบของตัวแปรที่สังเกตได้

ตารางที่ 4.35 แสดงค่าน้ำหนักองค์ประกอบของตัวแปรที่สังเกตได้

องค์ประกอบ/ตัวแปร	น้ำหนักองค์ประกอบ				สัมประสิทธิ์คะแนนองค์ประกอบ
	b_{sc}	SE	t	R^2	
SCC					
X1	0.884	-	-	0.782	0.173
X2	0.903	0.016	56.898	0.815	0.231
X3	0.912	0.017	58.083	0.831	0.256
X4	0.865	0.019	52.118	0.748	0.128

ตารางที่ 4.35 (ต่อ)

องค์ประกอบ/ตัวแปร	น้ำหนักองค์ประกอบ				สัมประสิทธิ์คะแนนองค์ประกอบ
	b_{sc}	SE	t	R^2	
CBT					
X5	0.521	-	-	0.272	0.056
X6	0.785	0.066	20.714	0.616	0.096
X7	0.839	0.072	42.772	0.704	0.158
CBR					
X8	0.915	-	-	0.838	0.224
X9	0.886	0.016	57.748	0.749	0.179
X10	0.842	0.019	50.610	0.709	0.057
CRS					
Y1	0.925	-	-	0.855	0.227
Y2	0.923	0.014	69.880	0.852	0.312
BCM					
Y3	0.912	-	-	0.831	0.160
Y4	0.877	0.018	55.413	0.769	0.217
Y5	0.850	0.018	53.834	0.723	0.071
Y6	0.871	0.019	56.909	0.758	0.105

หมายเหตุ $p < 0.01$

จากตารางที่ 4.35 ผลการวิเคราะห์ค่าน้ำหนักองค์ประกอบของตัวแปรที่สังเกตได้ พบว่า มีค่าเป็นบวกทั้งหมด มีขนาดตั้งแต่ 0.521 ถึง 0.925 และแตกต่างจากศูนย์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ทุกตัว โดยตัวแปรที่สังเกตได้ที่มีค่าน้ำหนักองค์ประกอบมากที่สุดคือ องค์ประกอบความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้แก่ ความคล่องตัว (Y1) มีน้ำหนักองค์ประกอบเท่ากับ 0.925 ส่วนตัวแปรที่สังเกตได้ที่มีน้ำหนักองค์ประกอบน้อยที่สุด คือ องค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ได้แก่ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) มีน้ำหนักองค์ประกอบเท่ากับ 0.521 ค่าสัมประสิทธิ์ความเที่ยงของตัวแปรที่สังเกตได้ทุกค่า (R^2) ซึ่งบอกค่าความแปรปรวนร่วมของตัว

แปรที่สังเกตได้ภายนอก (X1 ถึง X10) มีค่าตั้งแต่ 0.272 - 0.838 และตัวแปรที่สังเกตได้ภายใน (Y1 ถึง Y6) มีค่าตั้งแต่ 0.723 - 0.855 เมื่อพิจารณาค่าน้ำหนักองค์ประกอบมาตรฐาน (B) เป็นรายองค์ประกอบ พบว่า

1. องค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ ความร่วมมือกันในการสื่อสาร (X3) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.912 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 83.1 รองลงมาคือ ความไว้ใจ (X2) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.903 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 81.5 การแบ่งปันข้อมูลร่วมกัน (X1) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.884 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 78.2 และการสร้างความรู้ร่วมกัน (X4) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.865 และมีความแปรผันร่วมกันกับองค์ประกอบความร่วมมือกันของโซ่อุปทานดิจิทัล ร้อยละ 74.8

2. องค์ประกอบปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ การรับมือต่อภัยคุกคามไซเบอร์ (X7) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.839 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามไซเบอร์ ร้อยละ 70.4 รองลงมาคือ ช่องโหว่ของดำเนินงานภายใน (X6) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.785 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามไซเบอร์ ร้อยละ 70.4 และแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.521 และมีความแปรผันร่วมกันกับองค์ประกอบปัญหาภัยคุกคามไซเบอร์ ร้อยละ 27.2

3. องค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทานดิจิทัล (CBR) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ ด้านบุคลากร (X8) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.915 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทาน ร้อยละ 83.8 รองลงมาคือ ด้านกระบวนการ (X9) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.866 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทาน ร้อยละ 74.9 และด้านเทคโนโลยี (X10) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.842 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุทาน ร้อยละ 70.9

4. องค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือความคล่องตัว (Y1) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.925 และมีความแปรผันร่วมกันกับองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่

อุปทานดิจิทัล ร้อยละ 85.5 และความคงทน (Y2) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.923 และมีความแปรผันร่วมกันกับองค์ประกอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ร้อยละ 85.2

5. องค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ (BCM) ตัวแปรที่มีน้ำหนักความสำคัญมากที่สุด คือ แผนความต่อเนื่องทางธุรกิจ (Y3) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.912 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 83.1 รองลงมาคือ แผนกู้คืนภัยพิบัติ (Y4) น้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.877 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 76.9 การจัดการเหตุฉุกเฉิน (Y6) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.871 และมีความแปรผันร่วมกันกับองค์ประกอบการจัดการความต่อเนื่องทางธุรกิจ ร้อยละ 75.8 และการจัดการวิกฤต (Y5) มีน้ำหนักองค์ประกอบมาตรฐานเท่ากับ 0.850 และมีความแปรผันร่วมกันกับองค์ประกอบองค์การสีเขียว ร้อยละ 72.3

ตอนที่ 7 ผลการวิเคราะห์เพื่อตอบสมมติฐานการวิจัย (ข้อที่ 1-6)

ผลการวิเคราะห์ดังกล่าวข้างต้น ผู้วิจัยสามารถนำเสนอผลการวิจัยเพื่อตอบคำถามการวิจัยและสมมติฐานการวิจัย โดยมีรายละเอียดดังนี้

จากคำถามการวิจัย “ปัจจัยอะไรบ้างที่ส่งผลต่อความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ในการจัดการความต่อเนื่องของธุรกิจดิจิทัล” ผู้วิจัยได้ทำการกำหนดสมมติฐานเพื่อตอบคาถามการวิจัยดังกล่าวข้างต้น ดังนี้

สมมติฐานข้อที่ 1: ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการทดสอบสมมติฐาน พบว่า ความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีอิทธิพลทางตรงเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลรวมจากความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) เท่ากับ 0.431 โดยเป็นอิทธิพลทางตรงเท่ากับ 0.106 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัล ที่มุ่งเน้นความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ในด้านการแบ่งปันข้อมูลร่วมกัน (X1) ได้แก่ การที่บริษัทมีกระบวนการในแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัล โดยที่กระบวนการในการแบ่งปันข้อมูลระหว่างบริษัทอื่น ๆ ในโซ่อุปทานดิจิทัลที่มีอยู่นั้นเป็นกระบวนการที่มีประสิทธิภาพ อีกทั้งบริษัทยังได้มีการแบ่งปันข้อมูลด้านกลยุทธ์ให้กับทั้งลูกค้าและผู้จำหน่าย ซึ่งการดำเนินการในเรื่องการของการแบ่งปันข้อมูลที่ผ่านมานั้น

ทำให้เกิดประโยชน์ต่อบริษัทเป็นอย่างมาก และการแบ่งปันข้อมูลระหว่างบริษัทอื่นๆ ในโซ่อุปทานดิจิทัลเป็นทำให้เกิดความร่วมมือกันในโซ่อุปทานดิจิทัล และด้านความไว้ใจ (X2) ได้แก่ บริษัทคู่ค้าที่มีอยู่ในโซ่อุปทานดิจิทัลที่มีอยู่นั้นมีความซื่อสัตย์ในการติดต่อในการที่จะทำธุรกิจกับบริษัทของท่าน โดยที่บริษัทคู่ค้าเหล่านั้นที่อยู่ในโซ่อุปทานดิจิทัลมีการป้องกันความลับของลูกค้าที่ได้รับจากบริษัทของท่าน อีกทั้งบริษัทคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลได้ให้ข้อมูลที่ถูกต้องกับบริษัทของท่านอยู่เสมอ รวมไปถึงการที่บริษัทคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัลของท่านเต็มใจที่จะให้ความช่วยเหลือและสนับสนุนกับบริษัทของท่านโดยไม่มีข้อยกเว้น และเมื่อบริษัทของท่านประสบต่อปัญหาใดๆ และได้มีการแจ้งไปยังคู่ค้าที่อยู่ในโซ่อุปทานดิจิทัล บริษัทคู่ค้าเหล่านั้นจะปฏิบัติต่อบริษัทของท่านด้วยความเข้าใจ และในด้านความร่วมมือกันในการสื่อสาร (X3) ได้แก่ บริษัทของท่านและคู่ค้าในโซ่อุปทานดิจิทัลได้จัดให้มีการประชุมร่วมกันอย่างสม่ำเสมอ มีการสื่อสารกันแบบเปิดและแบบสองทางอยู่เป็นประจำ มีการสื่อสารทั้งที่เป็นทางการและไม่เป็นทางการ มีช่องทางในการสื่อสารกันอยู่หลายช่องทาง อีกทั้งยังมีการประสานงานระหว่างกันโดยส่วนใหญ่จะใช้การสื่อสารทางด้านข้อความระหว่างกัน รวมถึงมีความร่วมมือกันในด้านการสร้างความรู้ร่วมกัน (X4) ได้แก่ บริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุปทานดิจิทัลที่จะเกี่ยวกับกลยุทธ์ในการดำเนินการร่วมกันเพื่อความสำเร็จที่จะเกิดขึ้นในระยะยาว บริษัทของท่านมีการสร้างความรู้ร่วมกันกันกับคู่ค้าในโซ่อุปทานดิจิทัลในการแลกเปลี่ยนแนวความคิดใหม่ๆ เพื่อความสัมพันธ์ที่ดีต่อกันในระยะยาว รวมไปถึงบริษัทของท่านมีการสร้างความรู้ร่วมกันกับคู่ค้าในโซ่อุทานเกี่ยวกับการพัฒนาโอกาสทางด้านนวัตกรรมโดยเฉพาะในเรื่องที่เกี่ยวข้องกับการจัดการความเสี่ยงและความไม่แน่นอนทางด้านธุรกิจที่จะเกิดขึ้นได้มีระดับที่สูงขึ้น จะทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ในด้านที่เกี่ยวกับความคล่องตัว (Y1) ได้แก่บริษัทของท่านสามารถที่จะทำการตรวจจับถึงภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว บริษัทของท่านสามารถที่จะทำการตัดสินใจกระทำการใดๆ เมื่อพบภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว บริษัทของท่านสามารถตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่างๆ ภายในบริษัทของท่านด้วยความรวดเร็ว และบริษัทของท่านสามารถที่ปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่างๆ ภายในบริษัทได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัทของท่าน และความคงทน (Y2) ได้แก่ บริษัทของท่านสามารถที่จะกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก บริษัทของท่านสามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ๆ หลังจากการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก บริษัทของท่านได้

เตรียมความพร้อมเกี่ยวกับการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามที่ทำการดำเนินงานเกิดการหยุดชะงัก บริษัทของท่าน สามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานดิจิทัลต่อไปได้ แม้จะถูกโจมตีจากภัยคุกคามที่ทำให้การดำเนินงานเกิดการชะงัก บริษัทของท่าน สามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่อุปทานดิจิทัล หลังจากที่ถูกโจมตีจากภัยคุกคาม ที่ทำให้การดำเนินงานเกิดการชะงัก และ บริษัทของท่าน สามารถที่จะดึงเอาความรู้ความหมายต่างๆ ที่เป็นประโยชน์อันเกิดจากการถูกโจมตีจากภัยคุกคาม เพื่อนำมาเป็นข้อมูลในการแก้ปัญหาอาจถูกโจมตีในครั้งต่อไป มีระดับที่ลดลง

นอกจากนี้ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลทางอ้อมจากความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) เท่ากับ 0.325 แสดงให้เห็นว่า เมื่อวิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ด้านการแบ่งปันข้อมูลร่วมกัน (X1) ด้านความไว้ใจ (X2) ด้านความร่วมมือกันในการสื่อสาร (X3) ด้านการสร้างความรู้ร่วมกัน (X4) ในระดับสูงขึ้น จะทำให้การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลด้านบุคลากร (X8) ด้านกระบวน (X9) และด้านเทคโนโลยี (X10) มีระดับที่สูงขึ้น ซึ่งส่งผลทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ด้านความคล่องตัว (Y1) และด้านความคงทน (Y2) มีระดับที่สูงขึ้นด้วยเช่นเดียวกัน

สมมติฐานข้อที่ 2 : การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการทดสอบสมมติฐาน พบว่า การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีอิทธิพลทางตรงเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลรวมจากการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) เท่ากับ 0.515 โดยเป็นอิทธิพลทางตรงเท่ากับ 0.027 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัล ที่มุ่งเน้นการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ในด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) ได้แก่ ผู้บุกรุกเข้าสู่เครือข่ายมีวัตถุประสงค์ในการทดสอบขีดความสามารถของตนเองหรือต้องการท้าทายโดยการเจาะระบบให้สำเร็จ โดยที่ความรุนแรงขององค์กรอาชญากรรมที่มุ่งกระทำต่อธุรกรรมทางการเงินและทรัพย์สินทางปัญญาของวิสาหกิจ และการโจมตีทางไซเบอร์ที่เกิดขึ้นกับวิสาหกิจมักจะมีสาเหตุมาจากความแตกต่างทางด้านอุดมการณ์และการเมือง รวมทั้งนโยบายทางภาครัฐส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มีต่อบริษัท และด้านช่องโหว่ของการดำเนินงานภายใน

(X6) ได้แก่ กลยุทธ์ นโยบายและมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันของบริษัทที่ทำงานเป็นผลทำให้เกิดการโจมตีทางไซเบอร์ การดำเนินการและยึดมั่นในกลยุทธ์และมาตรฐานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทท่านจะส่งผลให้เกิดการโจมตีทางไซเบอร์นั้นลดลง โดยที่การอบรมพนักงานรวมไปถึงการทำให้พนักงานได้ตระหนักถึงภัยคุกคามไซเบอร์จะทำให้การโจมตีทางไซเบอร์นั้นลดลงได้ และจากการที่มีโครงสร้างพื้นฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อ่อนแอในบริษัทนั้นจะส่งผลให้เกิดการโจมตีทางไซเบอร์ที่มากขึ้น อีกทั้งความสามารถในการพัฒนาทักษะความสามารถของบุคลากรในบริษัทนั้นจะส่งผลต่อการจัดการความปลอดภัยในโลกไซเบอร์ให้มีประสิทธิภาพมากขึ้น รวมไปถึงด้านการรับมือต่อภัยคุกคามไซเบอร์ (X7) ได้แก่ การที่บริษัทมีการกำหนดนโยบาย (Policy) ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไว้อย่างชัดเจนในการเพื่อใช้ในการรับมือต่อภัยคุกคามไซเบอร์ และมีความชัดเจนในการบูรณาการในการกำหนดโครงสร้าง (Organization) การจัดหน่วยและการบรรจุบุคคลที่มีคุณลักษณะพิเศษและมีความเชี่ยวชาญเฉพาะด้าน มีมาตรฐานการปฏิบัติงาน และเป็นแบบอย่างที่ดีในด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โดยที่มีการกำหนดกรอบการดำเนินงาน (Frame work) อย่างเป็นระบบแบบแผนที่ชัดเจนและสามารถปฏิบัติได้ในการรับมือกับภัยคุกคามด้าน ไซเบอร์ขององค์กร รวมไปถึงการที่มีการประเมินผลการปฏิบัติขององค์กรทั้งการประเมินภายในด้วยตนเอง และการประเมินจากภายนอก เพื่อติดตามความก้าวหน้า ปัญหาข้อขัดข้อง ข้อจำกัดอุปสรรคต่างๆ เพื่อหาทางแก้ไขปัญหาและอุปสรรคแต่เนิ่นๆ สำหรับการรับมือกับภัยคุกคามด้านไซเบอร์ ในระดับที่สูงขึ้น จะทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ในด้านที่เกี่ยวกับความคล่องตัว (Y1) และด้านความคงทน (Y2) มีระดับที่ลดลง

นอกจากนี้ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลทางอ้อมจากการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) เท่ากับ 0.488 แสดงให้เห็นว่า เมื่อวิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีการจัดการภัยคุกคามไซเบอร์ ด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) ด้านช่องโหว่ของการดำเนินงานภายใน (X6) และด้านการรับมือต่อภัยคุกคามไซเบอร์ (X7) ในระดับที่สูงขึ้น จะทำให้การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลด้านบุคลากร (X8) ด้านกระบวน (X9) และด้านเทคโนโลยี (X10) มีระดับที่สูงขึ้น ซึ่งส่งผลทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ด้านความคล่องตัว (Y1) และด้านความคงทน (Y2) มีระดับที่สูงขึ้นด้วยเช่นเดียวกัน

สมมติฐานข้อที่ 3 : การจัดการความเสี่ยงของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการทดสอบสมมติฐาน พบว่าการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) มีอิทธิพลทางตรงเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ได้รับอิทธิพลรวมจากการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล เท่ากับ 0.827 ซึ่งทั้งหมดเป็นอิทธิพลทางตรงเท่ากับ 0.827 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลที่มุ่งเน้นในเรื่องการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ด้านบุคลากร (X8) ได้แก่ บุคลากรของบริษัทท่านมีความสามารถและความชำนาญและความเชี่ยวชาญต่อการจัดการความเสี่ยงอยู่ในระดับสูง และบุคลากรของบริษัทของท่านมีความตระหนักถึงการจัดการความเสี่ยงเป็นอย่างดี โดยที่ บุคลากรในตำแหน่งผู้จัดการของบริษัทท่านมีความรู้ความชำนาญต่อการจัดการความเสี่ยงเป็นอย่างดี และบริษัทของท่านมีการจัดการความเสี่ยงด้วยการสนับสนุนให้พนักงานทำงานร่วมกันเป็นทีม รวมทั้งบริษัทของท่านมีนโยบายให้พนักงานสร้างความสัมพันธ์ที่ดีไม่ว่าจะเป็นทั้งลูกค้า ผู้จำหน่าย รวมไปถึงคู่ค้าต่าง ๆ และด้านกระบวนการ (X9) ได้แก่บริษัทของท่านได้มีการดำเนินการในเรื่องของการติดตั้งโปรแกรมป้องกันไวรัสไว้แล้ว และบริษัทของท่านมีระบบรักษาความปลอดภัยของข้อมูลในการที่จะรักษาข้อมูลต่าง ๆ ที่สำคัญของบริษัทของท่าน โดยที่บริษัทของท่านมีการจัดการในเรื่องของระบบเครือข่ายในการป้องการการเข้ามาโจมตีจากผู้ไม่หวังดีและบริษัทของท่านมีระบบในการจัดการบัญชีรายชื่อผู้เข้าใช้งานในระบบต่าง ๆ โดยการสร้างกฎเกณฑ์ในการตั้งค่าไว้อย่างมีประสิทธิภาพ อีกทั้งภัยคุกคามทางไซเบอร์ในปัจจุบันนี้ ทำให้เกิดผลเสียต่อระบบเครือข่ายคอมพิวเตอร์ของท่านอย่างมาก และภัยคุกคามทางไซเบอร์ในปัจจุบันนี้ ทำให้เกิดผลเสียต่อระบบเครือข่ายคอมพิวเตอร์ของท่านอย่างมาก นอกจากนี้บริษัทของท่านมีทรัพยากร และความสามารถในการรักษาความปลอดภัย ที่จะรับมือต่อการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ และข้อมูลที่สำคัญของบริษัทท่านได้รับการจัดการต่อการรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ ปัจจุบันบริษัทของท่านได้รับผลประโยชน์จากการดำเนินการในด้านการจัดการความเสี่ยงที่มาจากการโจมตีทางไซเบอร์ รวมถึงด้านเทคโนโลยี (X10) ได้แก่ โครงสร้างพื้นฐานอันประกอบไปด้วย สถาปัตยกรรมของระบบ ผู้ใช้งานระบบ รวมไปถึงผู้ให้บริการจากภายนอก ได้รับการจัดการเพื่อรับมือจากการโจมตีที่เกิดจากภัยคุกคามทางไซเบอร์ไว้อย่างมีประสิทธิภาพ และท่านไม่สามารถเข้าถึงเครื่องมือทางด้านเทคโนโลยีที่สามารถสนับสนุนการทำงานของท่านได้ เมื่อท่านประสบกับการจัดการภัยคุกคามทางไซเบอร์ โดยที่ท่านมี

ความเชื่อมั่นต่อเทคโนโลยีในการรักษาความปลอดภัย เมื่อบริษัทของท่านได้ประสบกับการจัดการภัยคุกคามทางไซเบอร์ นั่นหมายความว่า การจัดการภัยคุกคามดังกล่าวจะไม่ส่งผลกระทบต่องานของท่าน และบริษัทของท่านมักจะหาวิธีการใหม่ๆ ในการรักษาความปลอดภัยจากการโจมตีทางไซเบอร์มาใช้เองโดยไม่ได้ทำการปรึกษาจากที่ปรึกษาจากภายนอกเลย ในระดับที่สูงขึ้นแล้ว จะทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ด้านความคล่องตัว (Y1) และด้านความคงทน (Y2) มีระดับที่สูงขึ้นด้วยเช่นเดียวกัน

สมมติฐานข้อที่ 4 : ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

ผลการทดสอบสมมติฐาน พบว่าความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ได้รับอิทธิพลรวมจากความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) เท่ากับ 0.394 ซึ่งทั้งหมดเป็นอิทธิพลทางตรงเท่ากับ 0.394 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลที่มุ่งเน้นในเรื่องความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ในด้านการแบ่งปันข้อมูลร่วมกัน (X1) ด้านความไว้ใจ (X2) ด้านความร่วมมือกันในการสื่อสาร (X3) และด้านการสร้างความรู้ร่วมกัน (X4) ในระดับที่สูงขึ้นแล้ว จะทำให้การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ในด้านบุคลากร (X8) ด้านกระบวนการ (X9) และด้านเทคโนโลยี (X10) อยู่ในระดับที่สูงขึ้นด้วยเช่นกัน

สมมติฐานข้อที่ 5 : การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

ผลการทดสอบสมมติฐาน พบว่าการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ได้รับอิทธิพลรวมจากการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) เท่ากับ 0.590 ซึ่งทั้งหมดเป็นอิทธิพลทางตรงเท่ากับ 0.590 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลที่มุ่งเน้นในเรื่องการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ในด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) ด้านช่องโหว่ของการดำเนินงานภายใน (X6) และด้านการรับมือต่อภัยคุกคามไซเบอร์ (X7) ในระดับที่สูงขึ้น

แล้ว จะทำให้การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ในด้านบุคลากร (X8) ด้านกระบวนการ (X9) และด้านเทคโนโลยี (X10) อยู่ในระดับที่สูงขึ้นด้วยเช่นกัน

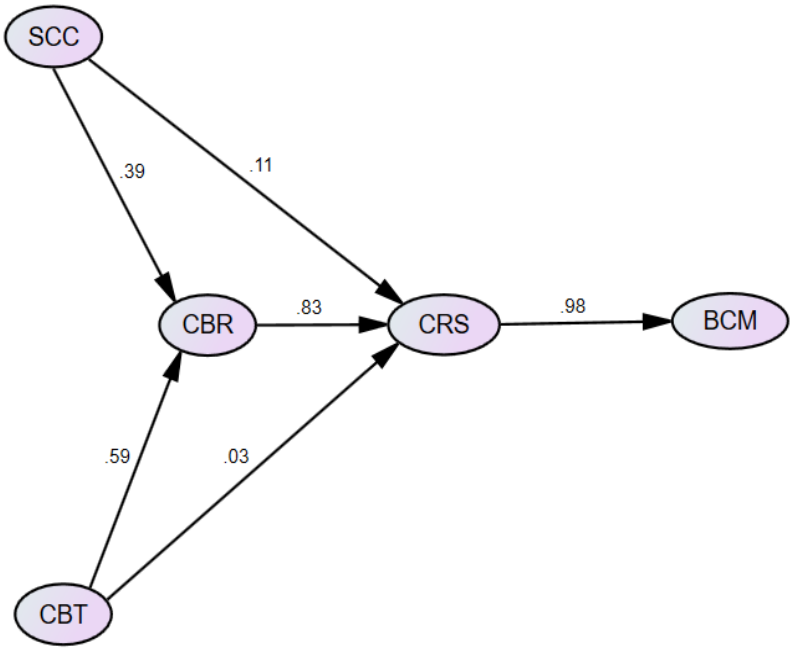
สมมติฐานข้อที่ 6 : ความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ผลการทดสอบสมมติฐาน พบว่าความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจ (BCM) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 โดยที่การจัดการความต่อเนื่องทางธุรกิจ (BCM) ได้รับอิทธิพลรวมจากความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) เท่ากับ 0.983 โดยเป็นอิทธิพลทางตรงเท่ากับ 0.983 สามารถอธิบายได้ว่าการที่วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ด้านความคล่องตัว (Y1) และด้านความคงทน (Y2) ในระดับที่สูงขึ้นแล้ว จะทำให้วิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีการจัดการความต่อเนื่องทางธุรกิจ (BCM) ด้านแผนความต่อเนื่องทางธุรกิจ (Y3) ได้แก่ แผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยงที่สามารถทำให้กิจการดำเนินต่อไปได้ และแผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ โดยที่แผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้ และแผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจและจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัท พร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม รวมทั้งแผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้ มีการจัดการความต่อเนื่องทางธุรกิจด้านแผนกู้คืนภัยพิบัติ (Y4) ได้แก่ แผนกู้คืนภัยพิบัติได้เข้ามาจัดการเกี่ยวกับเครื่องมืออุปกรณ์ ที่จะนำมาใช้แก้ปัญหาเมื่อเกิดภัยพิบัติได้อย่างมีประสิทธิภาพ และแผนกู้คืนภัยพิบัติทำให้มีการจัดการเกี่ยวกับระบบการจัดการเครือข่ายในบริษัทได้อย่างมีประสิทธิภาพ โดยที่แผนกู้คืนภัยพิบัติทำให้สามารถประหยัดค่าใช้จ่ายในการกู้คืนระบบ เนื่องจากมีการทำแผนการปฏิบัติรองรับไว้แล้วและการมีโซลูชั่นในการกู้คืนระบบสามารถช่วยในการรักษาชื่อเสียงของบริษัทของท่านกับลูกค้าและคู่ค้าได้ รวมทั้งการมีโซลูชั่นในการกู้คืนระบบสามารถช่วยให้มั่นใจได้ว่า บริษัทของท่านจะปฏิบัติตามกฎระเบียบของอุตสาหกรรมได้ มีแผนการจัดการความต่อเนื่องทางธุรกิจด้านการจัดการวิกฤต (Y5) ได้แก่ การจัดการวิกฤตทำให้เกิดความเชื่อมั่นในสายตาของคู่ค้าในโซ่อุปทานดิจิทัล ต่อปัญหาทางด้านความเสี่ยงที่บริษัทของท่านกำลังประสบอยู่ การจัดการวิกฤต ยิ่งดำเนินการได้เร็วมากแค่ไหน ยิ่งมีผลต่อชื่อเสียงของบริษัทมากขึ้นเท่านั้น และ การจัดการวิกฤต ทำ

ให้คู่ค้าในโซ่อุปทานดิจิทัลเห็นได้ว่า บริษัทของท่านมีความเป็นมืออาชีพในการบริหาร มีการจัดการความต่อเนื่องทางธุรกิจด้านการจัดการเหตุฉุกเฉิน (Y6) ได้แก่ บริษัทของท่านมีการเตรียมการสำหรับการป้องกัน (Prevent) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ บริษัทของท่านมีการเตรียมพร้อมรับมือ (Preparedness) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ บริษัทของท่านมีแผนในการตอบสนอง (Response) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ และบริษัทของท่านมีแผนสำหรับการฟื้นฟูแก้ไข (Recovery) ต่อเหตุฉุกเฉินที่จะเกิดขึ้นไว้อย่างมีประสิทธิภาพ เพิ่มขึ้นในระดับสูงเช่นเดียวกัน

นอกจากนี้การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) ได้รับอิทธิพลทางอ้อมจากความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) เท่ากับ 0.424 จากการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) เท่ากับ 0.506 และจากการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) เท่ากับ 0.827 ซึ่งเป็นค่าอิทธิพลที่มีนัยสำคัญทางสถิติที่ระดับ 0.01 แสดงว่าเมื่อวิสาหกิจขนาดกลางและขนาดย่อมในธุรกิจดิจิทัลมีความร่วมมือกันของโซ่อุปทานดิจิทัล (SCC) ด้านการแบ่งปันข้อมูลร่วมกัน (X1) ด้านความไว้ใจ (X2) ด้านความร่วมมือกันในการสื่อสาร (X3) และด้านการสร้างความรู้ร่วมกัน (X4) มีการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBT) ด้านแรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก (X5) ด้านช่องโหว่ของการดำเนินงานภายใน (X6) และด้านการรับมือต่อภัยคุกคามไซเบอร์ (X7) มีการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (CBR) ด้านบุคลากร (X8) ด้านกระบวนการ (X9) และด้านเทคโนโลยี (X10) ในระดับที่สูง จะทำให้ความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (CRS) ด้านความคล่องตัว (Y1) และด้านความคงทน (Y2) ในระดับที่สูงขึ้น ซึ่งส่งผลทำให้การจัดการความต่อเนื่องทางธุรกิจดิจิทัล (BCM) ด้านแผนความต่อเนื่องทางธุรกิจ (Y3) ด้านแผนกู้คืนภัยพิบัติ (Y4) ด้านด้านการจัดการวิกฤต (Y5) และด้านการจัดการเหตุฉุกเฉิน (Y6) ในระดับสูงขึ้นเช่นเดียวกัน

ผลการทดสอบสมมติฐานการวิจัยเกี่ยวกับปัจจัยที่ส่งผลต่อความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ในการจัดการความต่อเนื่องของธุรกิจดิจิทัล สามารถสรุปได้ดังภาพประกอบที่ 4.10 แสดงปัจจัยที่ส่งผลต่อความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ในการจัดการความต่อเนื่องของธุรกิจดิจิทัล สำหรับวิสาหกิจขนาดกลางและขนาดย่อม และตารางที่ 4.36 แสดงผลการทดสอบสมมติฐานการวิจัย



ภาพประกอบที่ 4.10 แสดงปัจจัยที่ส่งผลต่อความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ในการจัดการความต่อเนื่องของธุรกิจดิจิทัล สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

ตารางที่ 4.36 แสดงผลการทดสอบสมมติฐานการวิจัย ข้อที่ 1-6

ข้อที่	สมมติฐาน	ผลการทดสอบ
1	ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	ยอมรับสมมติฐาน
2	การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	ยอมรับสมมติฐาน
3	การจัดการความเสี่ยงของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	ยอมรับสมมติฐาน

ตารางที่ 4.36 (ต่อ)

ข้อที่	สมมติฐาน	ผลการทดสอบ
4	ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล	ยอมรับสมมติฐาน
5	การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล	ยอมรับสมมติฐาน
6	ความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ยอมรับสมมติฐาน

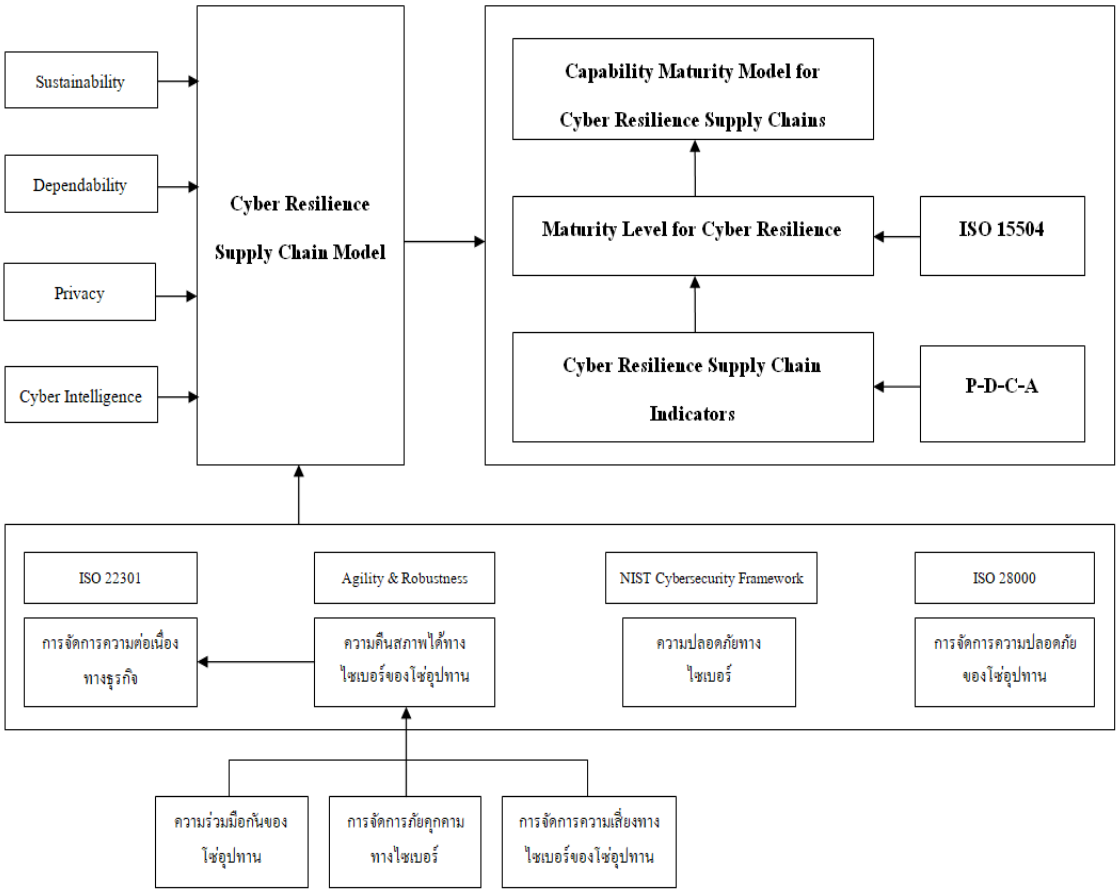
4.2 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2

การศึกษาเพื่อตอบวัตถุประสงค์ในข้อที่ 2 เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ผลการพัฒนาตัวแบบวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีการดำเนินการในขั้นตอน ต่าง ๆ 2 ขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 พัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

แนวทางในการพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ผู้วิจัยสามารถสรุปแนวคิดไว้ดังภาพประกอบที่ 4.11

จากภาพประกอบที่ 4.11 การพัฒนา **ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล** ที่ผู้วิจัยนำเสนอนั้น ได้ทำการศึกษาโดยอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (NIST) ที่ประกอบด้วย 5 งานหลัก (Function) 23 กลุ่มงาน (Category) (NIST, 2018) ที่ได้พัฒนาขึ้นมาโดยมีการอ้างอิงจากมาตรฐาน CIS CSC, COBIT 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013 และ NIST SP 800-53 Rev.4 นอกจากนี้ผู้วิจัยได้ทำการศึกษามาตรฐานเพิ่มเติมเพื่อทำให้สามารถพัฒนากรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล โดยมาตรฐานเหล่านั้น ประกอบด้วย



ภาพประกอบที่ 4.11 แนวทางการพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ISO/IEC 27001:2013 มาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

1. ISO/IEC 27002:2013 ข้อปฏิบัติสำหรับสนับสนุน ISO 27001 ซึ่งระบุแนวทางปฏิบัติที่ดีที่สุด (Best Practice) สำหรับการเริ่มต้น การพัฒนา และการบำรุงรักษา ISMS

2. ISO/IEC 27005:2018 มาตรฐานด้านการบริหารจัดการความเสี่ยงด้านไซเบอร์ที่ประกอบด้วยเทคโนโลยีสารสนเทศ (Info rmationtechnology) , เทคนิคความมั่นคงปลอดภัย (Security techniques), การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management systems)

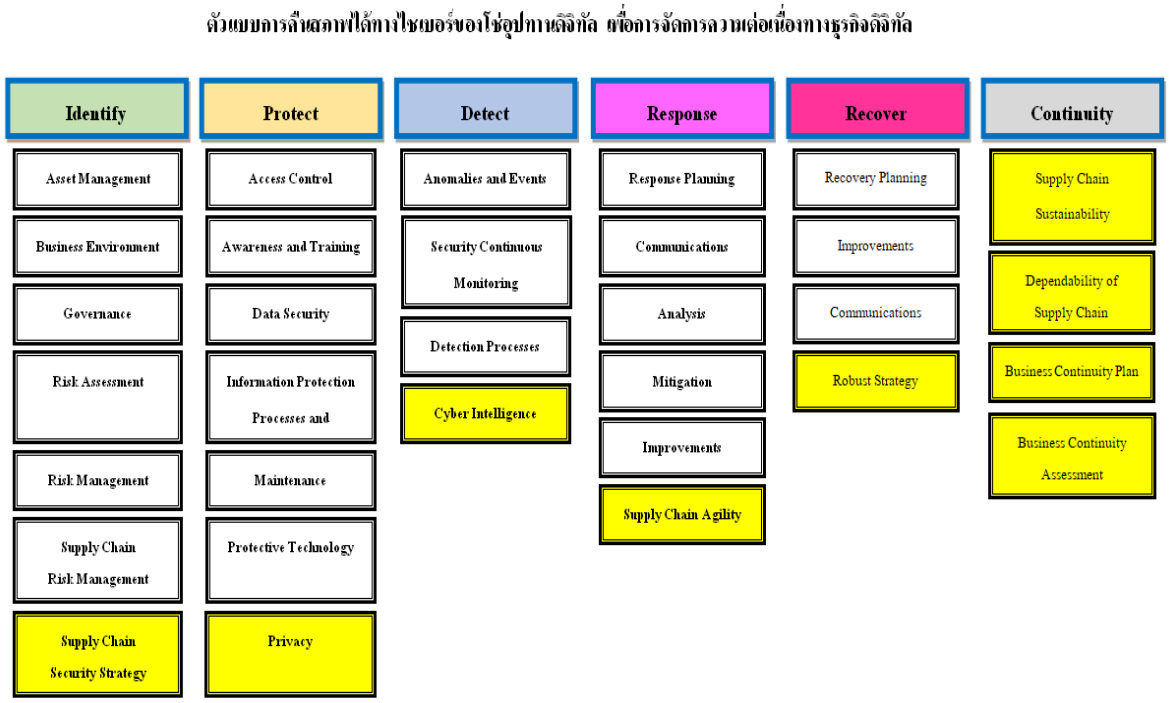
3. ISO 22301:2012 มาตรฐานด้านการบริหารจัดการความต่อเนื่องทางธุรกิจ)Business Continuity Management Systems) เป็นมาตรฐานที่ช่วยให้แต่ละองค์กรสามารถวางแผนรับมือกับภัยพิบัติรูปแบบต่าง ๆ ได้อย่างเป็นระบบ โดยเฉพาะอย่างยิ่ง การโจมตีไซเบอร์

4. ISO/IEC 27032:2012 ส่วนขยายของ ISO 27001 ซึ่งเกี่ยวข้องในเรื่อง Confidentiality, Integrity และ Availability กับความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บริการ รวมไปถึงสิ่งที่จับต้องไม่ได้)Virtual Assets) เช่น ชื่อเสียง เป็นต้น

5. IS/IEC 28000 เป็นมาตรฐานที่กำหนดข้อกำหนดของระบบการจัดการความปลอดภัยของซัพพลายเชนและจัดเตรียมรูปแบบการจัดการให้กับองค์กรที่ต้องการนำระบบนี้ไปใช้ มีจุดมุ่งหมายในการจัดการความเสี่ยงอย่างมีประสิทธิภาพโดยจัดกิจกรรมขององค์กรด้านความปลอดภัยของโซ่อุปทานดิจิทัลภายใต้ระบบเดียวกับระบบการจัดการอื่น ๆ

6. ISO 31000:2009 มาตรฐานด้านการบริหารจัดการความเสี่ยงระดับองค์กร

มาตรฐานต่าง ๆ ที่ใช้ ในการศึกษานี้ คือ เป็นมาตรฐานสากลที่ใช้สำหรับระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลทำให้กระบวนการทำงานขององค์กรภายใต้โซ่อุปทานดิจิทัล สามารถที่จะทำงานได้อย่างมีความปลอดภัยจากสภาพแวดล้อมทางดิจทัลที่เป็นอยู่ในปัจจุบัน ด้วยการทำงานที่มีขั้นตอนชัดเจน และมีความพร้อมในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ สร้างความเชื่อถือคู่ค้าที่อยู่ภายใต้โซ่อุปทานดิจิทัล จากการศึกษาข้อมูลดังกล่าวข้างต้นทำให้ผู้วิจัยสามารถนำเสนอกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model ที่ได้พัฒนาขึ้น โดยแสดงไว้ในภาพประกอบที่ 4.12



ภาพประกอบที่ 4.12 ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

รายละเอียดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล สามารถแบ่งออกได้เป็น 6 หมวด 32 มิติการดำเนินการ โดยสามารถอธิบายได้ดังต่อไปนี้

หมวดที่ 1 การระบุ (Identify) เป็นการระบุ แลเข้าใจถึงบริบทต่าง ๆ ของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลมีรายละเอียดมิติในการดำเนินการจะประกอบด้วย

มิติที่ 1 การจัดการทรัพยากรขององค์กร (Asset Management) ข้อมูล บุคลากร อุปกรณ์ ระบบและสิ่งอำนวยความสะดวกที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจได้รับการระบุและจัดการให้สอดคล้องกับความสำคัญเชิงสัมพันธ์กับ วัตถุประสงค์ทางธุรกิจและกลยุทธ์ความเสี่ยงขององค์กร

มิติที่ 2 สภาวะแวดล้อมทางธุรกิจ (Business Environment) สร้างความเข้าใจในภารกิจขององค์กร วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสียและกิจกรรมขององค์กร และจัดลำดับความสำคัญ ข้อมูลเหล่านี้ เพื่อกำหนดบทบาทความรับผิดชอบและการตัดสินใจในการจัดการความเสี่ยงทางไซเบอร์

มิติที่ 3 การกำกับดูแล (Governance) นโยบายขั้นตอนและกระบวนการในการจัดการและตรวจสอบความต้องการด้านกฎระเบียบ กฎหมาย ความเสี่ยง สิ่งแวดล้อมและการดำเนินงานขององค์กรและแจ้งให้ทราบถึงการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

มิติที่ 4 การประเมินความเสี่ยง (Risk Assessment) การทำความเข้าใจขององค์กรต่อความเสี่ยงในโลกไซเบอร์ที่มีผลต่อการดำเนินงานขององค์กร รวมถึงภารกิจหน้าที่ทรัพย์สินขององค์กร บุคลากร และภาพลักษณ์หรือชื่อเสียง

มิติที่ 5 กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy) มีการกำหนดลำดับความสำคัญขององค์กร ข้อจำกัด การยอมรับความเสี่ยงและข้อสมมติฐาน ที่ต้องได้รับการจัดทำขึ้นมา และใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงในการดำเนินงาน

มิติที่ 6 การจัดการความเสี่ยงของโซ่อุปทานดิจิทัล (Supply Chain Risk Management) ลำดับความสำคัญขององค์กร ข้อจำกัด การยอมรับความเสี่ยงและข้อสมมติฐานถูกกำหนดขึ้นและใช้เพื่อสนับสนุนการตัดสินใจความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในโซ่อุปทานดิจิทัล องค์กรได้กำหนดและดำเนินการตามกระบวนการเพื่อระบุประเมินและจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

มิติที่ 7 กลยุทธ์การจัดการความปลอดภัยของโซ่อุปทานดิจิทัล (Supply Chain Security Strategy) เพื่อเป็นการกำหนดกลยุทธ์ที่ใช้ในการจัดการความปลอดภัยของโซ่อุปทานดิจิทัล เพื่อสร้างความเชื่อมั่นให้กับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียต่อโซ่อุปทานดิจิทัล

หมวดที่ 2 การป้องกัน (Protect) เป็นการวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กรต่อความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีรายละเอียดของกลุ่มงานในหมวดนี้คือ

มิติที่ 1 การควบคุมการเข้าถึง (Access Control) การจำกัดการเข้าถึงสินทรัพย์และสิ่งอำนวยความสะดวกที่เกี่ยวข้อง เฉพาะผู้ใช้งาน กระบวนการและอุปกรณ์ที่ได้รับอนุญาต และมีการจัดการที่สอดคล้องกับความเสี่ยงที่ประเมินจากการเข้าถึงกิจกรรมและธุรกรรมที่ไม่ได้รับอนุญาต

มิติที่ 2 การตระหนักและการฝึกอบรม (Awareness and Training) ต้องมีการให้ศึกษาเรื่องความปลอดภัยในโลกไซเบอร์ต่อบุคลากร รวมถึงการต้องฝึกอบรมอย่างเพียงพอในการปฏิบัติหน้าที่และความรับผิดชอบด้านความปลอดภัยของข้อมูลที่สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

มิติที่ 3 ความปลอดภัยของข้อมูล (Data Security) ข้อมูลและบันทึกได้รับการจัดการสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับความ (ข้อมูล) ซื่อสัตย์และความพร้อมของข้อมูล

มิติที่ 4 ขั้นตอนและกระบวนการการป้องกันข้อมูล (Information Protection Processes and Procedures) นโยบายความปลอดภัย วัตถุประสงค์ ขอบเขต บทบาท กระบวนการ ความรับผิดชอบ ข้อผูกพันการจัดการและการประสานงานระหว่างหน่วยงานขององค์กร ระบบข้อมูลและขั้นตอน การบำรุงรักษา และใช้ในการป้องกันทรัพย์สิน

มิติที่ 5 การบำรุงรักษา (Maintenance) การบำรุงรักษาและซ่อมแซมการควบคุมระบบงานที่เกี่ยวข้อง และส่วนประกอบของระบบสารสนเทศนั้นดำเนินการสอดคล้องกับนโยบายและขั้นตอน

มิติที่ 6 เทคโนโลยีการป้องกัน (Protective Technology) โซลูชันด้านความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อรับรองความปลอดภัยและการคืนสภาพได้ของระบบและสินทรัพย์ให้สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

มิติที่ 7 ความเป็นส่วนบุคคล (Privacy) เพื่อช่วยให้องค์กรกำหนดมาตรการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้องกับข้อมูลที่ระบุตัวตนของลูกค้า, คู่ค้า ได้ภายในสภาพแวดล้อมทางดิจิทัล และบทบาทหน้าที่ในการประมวลผลข้อมูลบุคคลตามหลักการจัดการข้อมูลบุคคล

หมวดที่ 3 การตรวจจับ (Detect) เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ มีรายละเอียดของกลุ่มงานในหมวดนี้ดังนี้

มิติที่ 1 สถานการณ์และเหตุการณ์ที่มีความผิดปกติ (Anomalies and Events) การตรวจหากิจกรรมที่ผิดปกติในเวลาที่เหมาะสมและเข้าใจถึงผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ดังกล่าว

มิติที่ 2 การตรวจสอบความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring) ระบบข้อมูลและสินทรัพย์จะถูกตรวจสอบเป็นระยะ ๆ เพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์และตรวจสอบประสิทธิภาพของมาตรการป้องกัน

มิติที่ 3 กระบวนการการตรวจสอบ (Detection Processes) กระบวนการและขั้นตอนการตรวจจับนั้นต้องได้รับการบำรุงรักษาและทดสอบเพื่อให้แน่ใจว่ามีการรับรู้เหตุการณ์ที่ผิดปกติอย่างทันเวลาและเพียงพอ

มิติที่ 4 ข่าวกรองทางไซเบอร์ (Cyber Intelligence) กระบวนการในการสืบค้น ตรวจสอบ วิเคราะห์ และพิสูจน์ว่า ข่าวที่ได้รับทางไซเบอร์นั้นมีความน่าเชื่อถือ และทำการจัดทำรายงานส่งต่อให้กับผู้ที่เกี่ยวข้อง

หมวดที่ 4 การรับมือ (Respond) เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น รายละเอียดของกลุ่มงานในหมวดนี้มีดังนี้

มิติที่ 1 การวางแผนการรับมือ (ResponsePlanning) กระบวนการและขั้นตอนการรับมือ ต้องได้รับการดำเนินการ และบำรุงรักษาอยู่อย่างตลอด เพื่อให้มั่นใจว่ามีการตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบทันเวลา

มิติที่ 2 การสื่อสารเกี่ยวกับการรับมือ (Communications) กิจกรรมการตอบสนองมีการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกตามความเหมาะสมเพื่อรวมการสนับสนุนจากหน่วยงานบังคับใช้กฎหมาย

มิติที่ 3 การวิเคราะห์เพื่อการรับมือ (Analysis) มีการวิเคราะห์เพื่อให้มั่นใจว่ามีการตอบสนองที่เพียงพอและสนับสนุนกิจกรรมการกู้คืน

มิติที่ 4 การบรรเทาสถานการณ์ (Mitigation) มีการดำเนินกิจกรรมเพื่อการป้องกัน รวมถึงกิจกรรมการบรรเทาสถานการณ์ ผลกระทบและกำจัดเหตุการณ์

มิติที่ 5 การพัฒนาแนวทางการรับมือ (Improvements) กิจกรรมการรับมือเพื่อตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ต้องมีการปรับปรุงโดยการรวมบทเรียนที่ได้เรียนรู้จากกิจกรรมการตรวจจับ ตอบสนองในปัจจุบันและก่อนหน้า

มิติที่ 6 ความคล่องตัวของโซ่อุปทานดิจิทัล (Supply Chain Agility) ความสามารถของโซ่อุปทานดิจิทัลที่ให้ความสนใจต่อการปรับตัวของระบบอย่างรวดเร็วในสถานการณ์ที่ต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่สามารถคาดเดาได้ ด้วยการแสดงปฏิกิริยาตอบโต้ (React) การตอบสนอง (Respond) การปรับตัว (Adapt) รวมไปถึงการกำหนด ค่าใหม่ (Re-Configure)

หมวดที่ 5 การฟื้นฟู (Recover) เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ ฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม รายละเอียดของกลุ่มงานในหมวดนี้มีดังนี้

มิติที่ 1 การวางแผนการฟื้นฟูระบบ (Recovery Planning) กระบวนการและขั้นตอนการกู้คืนจะถูกดำเนินการและบำรุงรักษาเพื่อให้แน่ใจว่าระบบหรือทรัพย์สินจะได้รับผลกระทบจากเหตุการณ์ความปลอดภัยทางไซเบอร์ในเวลาที่เหมาะสม

มิติที่ 2 การพัฒนาแนวทางการฟื้นฟูระบบ (Improvements) การวางแผนและกระบวนการกู้คืนจะได้รับการปรับปรุงโดยผสมผสานบทเรียนที่เรียนรู้เข้ากับกิจกรรมในอนาคต

มิติที่ 3 การสื่อสารเกี่ยวกับการฟื้นฟูระบบ (Communications) กิจกรรมการฟื้นฟูจะได้รับการประสานงานกับฝ่ายภายในและภายนอก เช่นศูนย์ประสานงานผู้ให้บริการอินเทอร์เน็ตเจ้าของระบบที่ถูกโจมตี ผู้ที่ตกเป็นเหยื่อ และผู้ขาย

มิติที่ 4 กลยุทธ์ความคงทน (Robust Strategy) เป็นความสามารถของโซ่อุปทานดิจิทัลที่จะดำเนินงานตามหน้าที่ต่อไปแม่ว่าจะมีความเสียหายบางอย่างเกิดขึ้นต่อโซ่อุปทานดิจิทัล โดยยังจะต้องสามารถรักษาสถานะของโซ่อุปทานดิจิทัลให้มีความเสถียรได้เหมือนกับก่อนที่มีการเปลี่ยนแปลง และจะต้องสามารถทนทานได้มากกว่าการตอบสนอง

หมวดที่ 6 ความต่อเนื่อง (Continuity) เป็นการดำเนินการตามขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง

มิติที่ 1 ความยั่งยืนของโซ่อุปทานดิจิทัล (Supply Chain Sustainability) การจัดการต่อผลกระทบด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม รวมถึงการส่งเสริมการกำกับดูแลกิจการที่ดี ตลอดวัฏจักรชีวิตของสินค้าและบริการ

มิติที่ 2 ความเชื่อได้ของโซ่อุปทานดิจิทัล (Dependability of Supply Chain) ความสามารถในการให้บริการที่เชื่อถือได้อย่างสมเหตุสมผล ที่สามารถส่งมอบโดยระบบซึ่งเป็นพฤติกรรมที่สามารถรับรู้ได้โดยผู้ใช้งาน โดยความเชื่อถือได้ของโซ่อุปทานดิจิทัลจะมีคุณลักษณะ (attributes) ที่ประกอบด้วย ความพร้อมใช้งาน (availability), ความน่าเชื่อถือ (reliability), ความปลอดภัย (safety), การรักษาความลับ (confidentiality), ความสมบูรณ์)integrity), ความสามารถในการบำรุงรักษา (maintainability) และความมั่นคงปลอดภัย (security)

มิติที่ 3 แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) การวางแผนการต่อการจัดการธุรกิจเพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องเหตุการณ์ที่ไม่คาดคิดที่อาจเกิดขึ้นได้ โดยมีบทบาทที่สำคัญนอกเหนือไปจากที่จะช่วยป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นได้ต่อทรัพย์สิน ข้อมูลขององค์กร โอกาสในการสร้างรายได้ รวมไปถึงการเสริมสร้างภาพลักษณ์ขององค์กรในด้านการจัดการที่ดีเพื่อสร้างความมั่นใจต่อผู้ลงทุนและลูกค้า โดยต้องสามารถดำเนินการได้อย่างต่อเนื่องพร้อมทั้งสามารถบ่งบอกถึงสาเหตุของผลกระทบและความเสียหายทำให้สามารถแก้ไขปัญหาได้อย่างถูกต้องและรวดเร็ว และเหมาะสมกับสถานการณ์ได้

มิติที่ 4 การประเมินความต่อเนื่องทางธุรกิจ (Business Continuity Assessment) ศึกษาผลกระทบจากสถานการณ์ภายในและภายนอกที่จะส่งผลกระทบต่อการดำเนินธุรกิจเพื่อใช้ในการจัดความสำคัญของแต่ละกิจกรรมในธุรกิจว่าได้รับผลกระทบอย่างไรจากแต่ละเหตุการณ์ ทั้งในด้านสินค้าและบริการ พร้อมทั้งสามารถที่จะระบุได้ถึงความเร่งด่วนในแต่ละขั้นตอนเพื่อใช้ในการออกแบบแผนการป้องกันต่อไป

ขั้นตอนที่ 2 พัฒนาตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)

หลักในการกำหนดตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ในการกำหนดตัวชี้วัดเพื่อใช้เป็นแนวทางในการบรรลุถึงระดับความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ใช้หลักการทำงานของวงล้อเดมิ่ง)The Deming Cycle) หรือ วัฏจักรวางแผนปฏิบัติ-ตรวจสอบ-ทำ- (Plan-Do-Check-Act Cycle) อ้างใน ณัฏพันธ์ เขจรนันท์ (2549) ซึ่งวงล้อเดมิ่ง จะช่วยให้ การทำงานสามารถพัฒนาคุณภาพของงานอย่างต่อเนื่อง โดยพิจารณาลดหรือกำจัดกิจกรรมที่ไม่ก่อให้เกิดประโยชน์ออกจากการปฏิบัติงาน โดยแยกงานที่ไม่ก่อให้เกิดคุณค่า (No Value) ออกจากงานที่สร้างคุณค่าให้แก่ผลิตภัณฑ์หรือบริการ ซึ่งจะช่วยให้กระบวนการปฏิบัติงานมีความกระชับและพัฒนาขึ้นอย่างต่อเนื่อง โดยแนวทางสำหรับการทำงานของวงจรเดมิ่งประกอบด้วย

1. การวางแผน (Plan) เป็นการกำหนดแผนงานที่สามารถประเมินความก้าวหน้าของงานได้อย่างเป็นรูปธรรม

2. การทำ (Do) เป็นการดำเนินการตามแผนติดตาม และตรวจสอบความก้าวหน้าของกระบวนการ โดยเก็บรวบรวมข้อมูลตามระยะเวลาที่กำหนดเพื่อเป็นหลักฐานในการวิเคราะห์

3. การตรวจสอบ (Check) เป็นการตรวจสอบข้อมูลการดำเนินงานว่าจะสามารถบรรลุตามแผนที่กำหนดไว้หรือไม่ เพื่อพิจารณาปรับแผนหรือหยุดโครงการถ้าเกิดความไม่สอดคล้องระหว่างความเป็นจริงกับความต้องการ

4. การปฏิบัติ (Act) เป็นการตรวจสอบกระบวนการและจัดทำเอกสารเพื่อนำแผนงานทีที่พัฒนาจนประสบความสำเร็จ ไปเป็นแนวทางและมาตรฐานในการปฏิบัติงานต่อไป ทำให้มีการพัฒนาคุณภาพของงานอย่างต่อเนื่อง

ดังนั้นผู้วิจัยได้ทำการกำหนดตัวชี้วัดความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยได้พิจารณาจากการนำเอากลุ่มงาน (Category) ของแต่ละหน้าที่งาน (Function) ไปทำการทบทวนวรรณกรรม เพื่อดำเนินการในการจัดทำตัวชี้วัดในแต่ละกลุ่มงาน จากผลของการดำเนินการดังกล่าวทำให้ผู้วิจัยสามารถกำหนดตัวชี้วัด ได้ตามกลุ่มงานแต่ละตัว สามารถสรุปได้ตารางที่ 4.37 และ ตารางที่ 4.38 ตามลำดับ

ตารางที่ 4.37 จำนวนตัวชี้วัดของแต่ละกลุ่มงานในแต่ละหน้าที่งาน

Function	**Category**	**จำนวนตัวชี้วัด**	
IDENTIFY	Asset Management	5	33
	Business Environment	3	
	Governance	5	
	Risk Assessment	7	
	Risk Management Strategy	3	
	Supply Chain Risk Management	6	
	Supply Chain Security Strategy	4	
PROTECT	Identity Management, Authentication and Access Control	10	45
	Awareness and Training	4	
	Data Security	3	
	Information Protection Processes and Procedures	11	
	Maintenance	3	
	Protective Technology	8	
	Privacy	6	
DETECT	Anomalies and Events	5	16
	Security Continuous Monitoring	4	
	Detection Processes	5	
	Cyber Intelligence	2	
RESPOND	Response Planning	2	20
	Communications	4	
	Analysis	5	
	Mitigation	4	
	Improvements	1	
	Supply Chain Agility	4	

ตารางที่ 4.37 (ต่อ)

Function	Category	จำนวนตัวชี้วัด	
RECOVER	Recovery Planning	2	11
	Improvements	1	
	Communications	3	
	Robust Strategy	5	
CONTINUITY	Supply Chain Sustainability	3	17
	Dependability of Supply Chain	6	
	Business Continuity Plan	5	
	Business Continuity Assessment	3	

ตารางที่ 4.38 ตัวชี้วัดการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

Category	ตัวชี้วัด	
IDENTIFY		
Asset Management	1	มีการจัดทำทะเบียนรายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศที่ประกอบด้วย อุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน และข้อมูล โดยยังไม่ได้พิจารณาถึงระดับของความสำคัญใด ๆ เป็นเพียงจัดให้มีฐานข้อมูลของสินทรัพย์ที่มีอยู่ในบริษัท เพื่อให้ทราบจำนวนที่มีอยู่
	2	ดำเนินการจัดทำระบบทะเบียนรายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ โดยจัดระดับความสำคัญของทรัพย์สิน ที่พิจารณาจากชั้นความลับของข้อมูล หรือ ผลกระทบที่มีต่อมูลค่าทางธุรกิจ อีกทั้งยังมีกระบวนการในการปรับปรุงรายการทรัพย์สินให้ทันสมัยและเป็นปัจจุบันอย่างต่อเนื่อง เพื่อให้ทราบว่ามีสินทรัพย์ใดที่เพิ่มขึ้นใหม่ ถูกโยกย้าย ถูกเปลี่ยนแปลง หรือกำลังจะหมดอายุการใช้งาน หรือสิ้นสุดการให้บริการ

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	3	มีเครื่องมือและกระบวนการที่สามารถใช้ติดตาม ปรับปรุง และจัดลำดับความสำคัญ ของทะเบียนทรัพย์สิน โดยจัดทำเป็นรูปแบบของรายงานได้ตามความต้องการ อีกทั้งยังสามารถที่ใช้ในการตรวจจับเพื่อป้องกันการเปลี่ยนแปลงแก้ไขอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงานและข้อมูลโดยไม่ได้รับอนุญาตได้อย่างทันท่วงที
	4	มีการกำหนดถึงการเปลี่ยนแปลง แก้ไข การตั้งค่าของระบบ อุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน และเครื่องมือด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษร และต้องประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยอย่างเพียงพอก่อนการดำเนินการ รวมทั้งต้องมีเครื่องที่ใช้ในการตรวจจับ และระงับการเปลี่ยนแปลงใดๆ ที่ไม่ได้รับอนุญาต
	5	มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ของผู้ที่เกี่ยวข้อง ครอบคลุมผู้ผลิต ผู้ให้บริการ ผู้สนับสนุนการให้บริการ และการบำรุงรักษาอย่างเพียงพอ และมีการประเมินความเสี่ยงจากกระบวนการในการพิจารณาและอนุมัติการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศในทุกๆ ขั้นตอน
Business Environment	6	มีการวางระบบการทำงานรวมไปถึงบทบาทหน้าที่ความรับผิดชอบทั้งในองค์กร ภาคธุรกิจ ตลอดจนเครือข่ายในโซ่อุปทานดิจิทัลภายใต้โครงสร้างพื้นฐานที่สำคัญร่วมกันอย่างมีประสิทธิภาพและเหมาะสมกับงาน
	7	มีการสื่อสารในประเด็นของภารกิจ วัตถุประสงค์ และกิจกรรมขององค์กรให้กับเครือข่ายในโซ่อุปทานดิจิทัลภายใต้โครงสร้างพื้นฐานที่สำคัญให้รับทราบ และสามารถทำงานร่วมกันได้
	8	มีการกำหนดฟังก์ชั่นการพึ่งพาและฟังก์ชั่นที่สำคัญ (Dependencies and critical functions) เพื่อการคืนสภาพได้เพื่อรองรับการส่งมอบบริการที่สำคัญในทุก ๆ สถานะการทำงานทั้งหมดไม่ว่าจะอยู่ภายใต้การโจมตี ระหว่างการกู้คืน หรือในสภาวะปกติ

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Governance	9	มีการกำหนดแนวทางในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยจัดทำเป็นเพียงประกาศเพื่อให้บุคลากรภายใน รวมไปถึงผู้ที่เกี่ยวข้องภายนอกรับทราบถึงแนวการปฏิบัติ แต่ยังไม่ได้มีกระบวนการ หน่วยงานที่รับผิดชอบโดยตรง
	10	มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามไซเบอร์ และการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อจัดการความเสี่ยงทั้งภายในและภายนอกบริษัท
	11	มีการกำหนดนโยบายรักษาความมั่นปลอดภัยไซเบอร์ โดยมีการคำนึงถึงผลการวิเคราะห์หรือข้อมูลที่ได้มาจากองค์ความรู้ด้านภัยคุกคามไซเบอร์ รวมถึงกระบวนการในการเชื่อมโยง ปรับปรุง และทบทวนนโยบายต้องเกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ทั้งหมดของบริษัท
	12	มีการจัดการเกี่ยวกับข้อกฎหมายและข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วยความเป็นส่วนตัวและหน้าที่การเป็นพลเมือง ให้ได้รับความเข้าใจมากยิ่งขึ้น
	13	มีกระบวนการกำกับดูแลและการจัดการความเสี่ยงแก้ไขปัญหาความเสี่ยงทางไซเบอร์
Risk Assessment	14	มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นกรณี ๆ ไป โดยส่วนมากจะกระทำเมื่อมีได้ประสบกับเหตุการณ์ที่เข้ามาโจมตีต่อการดำเนินงานในองค์กร ซึ่งสามารถแก้ไขได้โดยบุคลากรภายใน แต่ถ้าแก้ไขไม่ได้ก็จะทำการว่าจ้างให้ผู้ให้บริการภายนอกเข้ามาดำเนินการ
	15	มีกระบวนการในการประเมินความเสี่ยงทางไซเบอร์ที่สามารถระบุระบบงานด้าน IT ที่สำคัญ (Critical System) หรือธุรกรรมที่มีความเสี่ยงสูง (High-risk Transaction) ที่จำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านไซเบอร์อย่างใกล้ชิด และมีแนวทางในการลดและควบคุมความเสี่ยง

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	16	มีการกำหนดให้มีการประเมินความเสี่ยงทางไซเบอร์ ด้านที่อาจส่งผลกระทบต่อข้อมูลลูกค้าอย่างสม่ำเสมอ โดยให้มีครอบคลุมถึงความเสี่ยงที่เกิดขึ้นจากการติดตั้งและการนำเทคโนโลยีใหม่มาใช้ การออกผลิตภัณฑ์และบริการใหม่ รวมถึงการเชื่อมต่อใหม่
	17	มีการกำหนดให้มีการประเมินความเสี่ยงทางไซเบอร์ ที่อาจเกิดจากการที่ Software หรือ Hardware ที่หมดอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการให้บริการ (End-of-Support) แล้ว
	18	มีกระบวนการประเมินความเสี่ยงทางไซเบอร์ ที่สามารถแสดงถึงความเสี่ยงจากการจัดหาผลิตภัณฑ์ใหม่ รวมถึงพันธมิตร (Relationships) รายใหม่ ๆ ที่เกิดขึ้น
	19	มีการปรับปรุงขอบเขตการประเมินความเสี่ยงทางไซเบอร์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับความเสี่ยงหรือวิธีการบริหารจัดการความเสี่ยงรูปแบบใหม่ ๆ ที่อาจเกิดขึ้นในอนาคต
	20	มีการกำหนดให้มีการประเมินความเสี่ยงทางไซเบอร์ ด้านความปลอดภัยในข้อมูลของบริษัทที่สำคัญ ข้อมูลลูกค้า รวมไปถึงข้อมูลของพันธมิตร เพื่อให้สามารถระบุภัยคุกคามทางไซเบอร์ที่มีโอกาสสร้างความเสียหายที่อาจเกิดขึ้นตลอดจนความเพียงพอของนโยบาย ขั้นตอนการปฏิบัติ และระบบการจัดเก็บข้อมูลที่สำคัญ ๆ ของบริษัท
Risk Management Strategy	21	มีการกำหนดกลยุทธ์และนโยบายในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยผู้บริหารได้จัดทำเป็นประกาศเพื่อให้บุคลากรรับทราบ แต่ยังไม่ได้มีกระบวนการ ขั้นตอน กิจกรรม และหน่วยงานหรือบุคคลที่รับผิดชอบอย่างชัดเจน
	22	มีการกำหนดกลยุทธ์ในการรักษาความปลอดภัยไซเบอร์ รวมทั้งจัดให้มีการทบทวนกลยุทธ์ ที่ครอบคลุมถึงเทคโนโลยี นโยบาย และระเบียบวิธีปฏิบัติ ที่อยู่ภายใต้กลยุทธ์การจัดการความเสี่ยงขององค์กร
	23	มีการกำหนดกระบวนการการจัดการความเสี่ยง การกำหนดความทนทานต่อความเสี่ยง ให้สอดคล้องกับทิศทางของเทคโนโลยี ภายใต้โครงสร้างพื้นฐานที่สำคัญ ขององค์กรไว้อย่างชัดเจน

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Supply Chain Risk Management	24	มีการวางแผนในการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล ที่ได้จัดทำไว้เป็นระเบียบวิธีการในการปฏิบัติ แต่ยังไม่ได้มีการวางแผนในขั้นตอนของการดำเนินการ
	25	มีการร่วมมือกันในการกำหนด จัดตั้ง ประเมิน จัดการ และตกลงร่วมกันต่อกระบวนการในการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล จากผู้ที่มีส่วนได้ส่วนเสียขององค์กร
	26	มีการกำหนด และจัดลำดับความสำคัญในระบบสารสนเทศ องค์ประกอบและบริการของซัพพลายเออร์และคู่ค้าที่เป็นบุคคลที่สาม และมีการประเมินโดยใช้กระบวนการในการประเมินความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล
	27	มีการออกแบบสัญญากับซัพพลายเออร์และคู่ค้าที่เป็นบุคคลที่สาม ด้วยการวัดผลที่เหมาะสม เพื่อให้บรรลุต่อวัตถุประสงค์ต่อการรักษาความปลอดภัยทางไซเบอร์และแผนในการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล
	28	มีการประเมินซัพพลายเออร์และคู่ค้าบุคคลที่สามอยู่เป็นประจำ โดยใช้การตรวจสอบ หรือการประเมินรูปแบบอื่น ๆ รวมถึงผลการทดสอบ เพื่อยืนยันว่าถึงการปฏิบัติตามภาระผูกพันตามสัญญา
	29	มีการวางแผนและทดสอบต่อการตอบสนองและการกู้คืน ที่นำไปใช้กับซัพพลายเออร์และผู้ให้บริการบุคคลที่สาม
Supply Chain Security Strategy	30	บริษัทได้มีการกำหนดให้มีกลยุทธ์ในการรักษาความปลอดภัยไซเบอร์ของโซ่อุปทานดิจิทัล รวมทั้งจัดให้มีการทบทวนกลยุทธ์ ที่ครอบคลุมถึงเทคโนโลยี นโยบาย และระเบียบวิธีปฏิบัติ ที่อยู่ภายใต้กลยุทธ์การจัดการความเสี่ยงขององค์กร
	31	บริษัทมีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ที่ครอบคลุมในเรื่องของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล การบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามไซเบอร์ และการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ที่

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
		สอดคล้องกับมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับกันทั่วไป
	32	บริษัทมีการกำหนดโครงการที่สนับสนุนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโซ่อุปทานดิจิทัล ที่สอดคล้องกับทิศทางของเทคโนโลยี หรือมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับโดยทั่วไป
	33	การกำหนดนโยบายรักษาความมั่นปลอดภัยทางด้านเทคโนโลยีของบริษัท มีการคำนึงถึงผลการวิเคราะห์หรือข้อมูลที่ได้มาจากองค์ความรู้ด้านภัยคุกคามไซเบอร์ของโซ่อุปทานดิจิทัล รวมถึงกระบวนการในการเชื่อมโยง ปรับปรุง และทบทวนนโยบายต้องเกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ทั้งหมดของบริษัท
PROTECT		
Identity Management, Authentication and Access Control	34	บริษัทมีการกำหนดวิธีการเข้าถึงข้อมูลของพนักงานไว้ โดยแยกตามระดับหน้าที่ความรับผิดชอบของพนักงานแต่ละคน ซึ่งจะยังไม่ได้พิจารณาว่าลำดับความสำคัญของข้อมูลเหมาะสมกับพนักงานในระดับใดมากนัก
	35	บริษัทมีการใช้วิธีการในการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากลในการพิสูจน์ตัวตนและการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สายและมีการเปลี่ยน Encryption Key สำหรับการเข้ารหัสอย่างสม่ำเสมอ และมีการออกแบบ และแบ่งระบบเครือข่ายภายในไว้เป็นโซนต่างๆ รวมถึงการวางมาตรการป้องกันตามระดับของความเสี่ยงจากการถูกโจมตีทางไซเบอร์
	36	บริษัทมีกระบวนการควบคุมและติดตามการเปลี่ยนแปลงการตั้งค่าอุปกรณ์คอมพิวเตอร์ รวมถึงการมีมาตรการในการควบคุม เพื่อป้องกันไม่ให้มีการติดตั้งโปรแกรมจากผู้ใช้งานที่ไม่ได้รับอนุญาต
	37	บริษัทมีการกำหนดสิทธิ์การเข้าถึงระบบงานและข้อมูลสลับให้พนักงานโดยเป็นไปตามหลักการการแบ่งแยกหน้าที่ที่ดี โดยกำหนดขอบเขตหน้าที่ความรับผิดชอบตามความจำเป็น โดยมอบหมายให้ผู้มีอำนาจทำการอนุมัติ

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
		การเปลี่ยนแปลง การยกเลิก และการสอบทานสิทธิ์ ซึ่งต้องสอดคล้องกับระดับความเสี่ยงที่บริษัทได้กำหนดไว้
	38	บริษัทมีการแยกบัญชีผู้ใช้งานของผู้ดูแลระบบ เป็น 2 บัญชีผู้ใช้งาน คือ สำหรับการใช้งานทั่วไป และสำหรับการบริหารจัดการระบบที่จำเป็นต้องใช้สิทธิสูง หรือมีการอนุญาตให้ใช้งานสิทธิสูงตามความจำเป็น
	39	บริษัท มีการกำหนดมาตรการควบคุมในการพิสูจน์ตัวตนลูกค้าผู้ใช้งานผลิตภัณฑ์และบริการทางการเงินผ่านระบบ Internet ที่สอดคล้องตามระดับความเสี่ยง
	40	บริษัทมีมาตรการควบคุมการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันการเข้าถึงอุปกรณ์เทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารของบริษัท โดยไม่ได้รับอนุญาต รวมทั้งมาตรการการบริหารจัดการการเข้าถึงทางกายภาพของระบบงาน IT ที่สำคัญ
	41	บริษัทกำหนดให้มีการเข้ารหัสช่องทางการเชื่อมต่อและใช้วิธีการพิสูจน์ตัวตนแบบ Multifactor ในการอนุญาตให้พนักงานหรือบุคคลภายนอกที่ได้รับอนุญาต เข้าใช้ระบบงาน IT ที่สำคัญ (Critical System) ของบริษัท จากระยะไกลผ่านเครือข่ายภายนอก
	42	บริษัทมีมาตรการการควบคุมเพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงการจัดเก็บกุญแจเข้ารหัส (Cryptographic Keys) ที่เกี่ยวข้องกับบริษัท อีกทั้งมีมาตรการรักษาความปลอดภัยของกุญแจเข้ารหัสที่ใช้สำหรับระบบงาน IT ที่สำคัญ (Critical System) ทั้งด้าน Physical และ Logical โดยใช้อุปกรณ์รักษาความปลอดภัย
	43	บริษัทใช้วิธีการพิสูจน์ตัวตนอย่างเข้มงวด (Strong Authentication) ด้วยวิธีการตามมาตรฐานสากลที่ยอมรับได้ เพื่ออนุญาตให้บุคคลภายนอกเข้าใช้ระบบงานและระบบเครือข่ายของบริษัท
Awareness and Training	44	มีการจัดการฝึกอบรมด้านการรักษาความปลอดภัยทางไซเบอร์ให้กับบุคลากร แต่ยังไม่มีแบบแผน ใด ๆ โดยส่วนมากจะเป็นการอบรมเพื่อให้บุคลากรตระหนักถึงความสำคัญ รู้จัก และสามารถแก้ไขสถานการณ์ได้ใน

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
		เบื้องต้น เมื่อต้องประสบกับเหตุการณ์การโจมตี หรือเมื่ออุปกรณ์ที่ใช้งานเกิดอาการผิดปกติจากภัยคุกคามทางไซเบอร์ เช่น โดนไวรัส
	45	บริษัทมีการจัดการอบรมและพัฒนาทักษะ ความรู้ ความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับบุคลากรที่รับผิดชอบอย่างเพียงพอและต่อเนื่อง โดยเนื้อหาต้องครอบคลุมถึงภัยคุกคามทางไซเบอร์ในปัจจุบันและในอนาคตที่จะเกิดขึ้น และจัดให้มีการวัดผลภายหลังการจัดการอบรม เพื่อเสริมสร้างความรู้และความตระหนักในเรื่องภัยคุกคามทางไซเบอร์ที่บริษัทต้องเผชิญ
	46	บริษัทจัดให้มีการสร้างความตระหนักและความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยการนำเอาสิ่งที่ได้เรียนรู้ (Lesson Learned) จากการทดสอบไปสร้างความตระหนักให้เกิดกับบุคลากรของบริษัท
	47	ผู้บริหารของบริษัท มีความเข้าใจ ความรับผิดชอบดูแลให้การอบรม และพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับให้ตระหนักถึงหน้าที่และความรับผิดชอบของตน เพื่อให้เกิดผลในทางปฏิบัติ
Data Security	48	บริษัทมีการกำหนดระดับของความลับของข้อมูล ตามสิทธิของพนักงานแต่ละคนที่จะสามารถเข้าถึงได้ การนำเอาข้อมูลไปเก็บหรือนำออกมาใช้ไม่ได้มีกระบวนการหรือเครื่องมือที่ใช้ในการป้องกันถึงความปลอดภัยทั้งสิ้น
	49	บริษัทกำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูลสารสนเทศ โดยมีการเข้ารหัสข้อมูลลับทุกครั้ง ในขณะรับส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่มีความน่าเชื่อถือ รวมทั้งยังมีเครื่องมือที่ใช้ในการป้องกันการเข้าถึงหรือนำข้อมูลลับออกจากบริษัท
	50	บริษัทมีการปกปิดหรือลบข้อมูลในส่วนสำคัญของลูกค้าก่อนนำไปใช้งานเพื่อให้เป็นไปตามกฎหมาย หลักเกณฑ์ของทางการ และนโยบายของบริษัทที่ได้กำหนดไว้

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Information Protection Processes and Procedures	51	บริษัทมีการกำหนดกระบวนการ ขั้นตอนการทำงานให้กับพนักงานและบุคลากรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แต่ยังเป็นเพียงกระบวนการและขั้นตอนเบื้องต้นเท่านั้น ยังไม่มีการดำเนินการใดๆ ที่เป็นระบบและแบบแผน
	52	บริษัทมีการจัดทำ Baseline Standards ด้านเทคโนโลยีสารสนเทศ โดยอิงมาตรฐานสากล และตั้งค่าอุปกรณ์คอมพิวเตอร์ รวมทั้งสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อให้เป็นไปตาม Security Baseline Standards ที่กำหนด
	53	บริษัทกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (Secure Coding) และสอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติให้สอดคล้องกับวงจรการพัฒนาระบบ (Development Life Cycle)
	54	บริษัทมีการกำหนดกระบวนการในการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ป้องกันเครือข่าย โดยการตรวจสอบความถูกต้องในการตั้งค่าอย่างสม่ำเสมอ มีการติดตั้งระบบในการตรวจจับและปิดกั้นการโจมตีหรือบุกรุกโดยไม่ได้รับอนุญาต รวมถึงมาตรการเชิงเทคนิคหรือเครื่องมือที่ใช้ในการป้องกันการเชื่อมต่อการเข้าถึงเครือข่ายภายในบริษัทจากพนักงานภายในหรือบุคคลภายนอกที่ไม่ได้รับอนุญาต
	55	บริษัทมีแผนการดำเนินงานด้านการสำรองข้อมูล ที่ได้รับการดูแลและทดสอบอยู่อย่างสม่ำเสมอ
	56	บริษัทได้มาตรการให้มีการปฏิบัติตามนโยบายและข้อบังคับเกี่ยวกับสภาพแวดล้อมการทำงานจริงสำหรับสินทรัพย์ขององค์กร
	57	บริษัทกำหนดระเบียบวิธีปฏิบัติการทำลายข้อมูลสารสนเทศ (Information Disposal) ครอบคลุม ขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลให้สอดคล้องกับระดับความสำคัญของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การควบคุมการทำลายในลักษณะ Dual Control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดให้มี

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
		การจัดทำทะเบียนการทำลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล Serial Number และวิธีการที่ใช้ทำลายข้อมูล
	58	บริษัทมีมาตรการในการป้องกันข้อมูลโดยได้มีการพัฒนากระบวนการอย่างต่อเนื่องพร้อมกับได้มีการถ่ายทอดเทคโนโลยีในการป้องกันให้กับผู้ที่เกี่ยวข้องได้อย่างมีประสิทธิผล
	59	บริษัทมีแผนการตอบสนอง (การตอบสนองเหตุการณ์และความต่อเนื่องทางธุรกิจ) และแผนการกู้คืน (การกู้คืนเหตุการณ์และการกู้คืนความเสียหาย) ที่สามารถจัดการได้ พร้อมกับการทดสอบอยู่อย่างสม่ำเสมอ
	60	บริษัทได้ทำการบรรจุงานด้านการรักษาความปลอดภัยทางไซเบอร์เข้าไปรวมอยู่ในการปฏิบัติงานด้านทรัพยากรมนุษย์ บุคลากรซึ่งรวมถึงพนักงานและผู้บริหารที่รับผิดชอบงานด้านการรักษาความมั่นคงไซเบอร์ต้องมีคุณสมบัติ ความรู้และความเชี่ยวชาญเป็นไปตามที่บริษัทกำหนด และสามารถปฏิบัติงานได้ตามหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย
	61	บริษัทมีการจัดทำแผนการประเมินช่องโหว่ (Vulnerabilities Assessment) เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริงและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
Maintenance	62	บริษัทมีการวางแผนการบำรุงรักษาและซ่อมแซมสินทรัพย์ของบริษัท แต่จะเป็นการดำเนินการเป็นกรณี ๆ ไปที่พบว่าสินทรัพย์ดังกล่าวมีการสูญเสียหรือหมดอายุการใช้งาน
	63	บริษัทมีมาตรการในการการบำรุงรักษาและซ่อมแซมสินทรัพย์ขององค์กรโดยจะต้องถูกดำเนินการและบันทึกด้วยเครื่องมือที่ได้รับการอนุมัติและควบคุม
	64	บริษัทมีมาตรการสำหรับการบำรุงรักษาสินทรัพย์องค์กรโดยระยะไกล โดยจะต้องได้รับการอนุมัติ บันทึกและดำเนินการในลักษณะที่ต้องสามารถป้องกันต่อการเข้าถึงที่ไม่ได้รับอนุญาต

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Protective Technology	65	บริษัทมีการป้องกันภัยคุกคามทางไซเบอร์ โดยในเบื้องต้นได้ใช้โปรแกรม Anti-Virus ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ในบริษัท แต่ยังไม่ได้มีการจัดการไปถึงอุปกรณ์ที่พนักงานนำมาใช้งานเอง รวมไปถึงเครือข่ายต่างๆ ที่ยังไม่สามารถดำเนินการป้องกันได้อย่างทั่วถึง
	66	บริษัทมีขอบเขตการตรวจสอบการประเมินความมั่นคงปลอดภัย การจัดเก็บและรับส่งข้อมูลที่มีความสำคัญของบริษัท ความเพียงพอของระบบการบริหารจัดการและควบคุมความเสี่ยงทางไซเบอร์ การแลกเปลี่ยนข้อมูล รวมไปถึงความสามารถในการรับมือต่อเหตุการณ์ผิดปกติทางไซเบอร์ว่ามีความสอดคล้องกับระดับความเสี่ยงทางไซเบอร์ที่กำหนดไว้ในระดับบริษัท
	67	บริษัทมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลแบบพกพา ให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น รวมทั้งมีมาตรการควบคุมเพื่อป้องกันการถ่ายโอนข้อมูลที่เป็นความลับ การรั่วไหลของข้อมูลจากอุปกรณ์ที่สูญหายหรือถูกโจรกรรม และยังมีกระบวนการในการทำลายข้อมูลจากอุปกรณ์ที่ไม่ได้ใช้งานแล้ว
	68	บริษัทมีมาตรการเชิงเทคนิคหรือเครื่องมือเพื่อใช้ป้องกันการเชื่อมต่อ หรือการเข้าถึงระบบเครือข่ายภายในของบริษัท โดยอุปกรณ์ที่ไม่ได้รับอนุญาต
	69	บริษัทแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกออกจากระบบเครือข่ายภายในบริษัท ออกจากกันอย่างชัดเจน
	70	บริษัทมีอุปกรณ์ป้องกันเครือข่ายติดตั้งไว้ในระบบเครือข่ายไร้สายเพื่อป้องกันการเข้าถึงเครือข่ายภายใน และจำกัดการติดต่อสื่อสารที่ไม่ได้รับอนุญาต (Unauthorized Traffic)
	71	บริษัทใช้วิธีการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากลในการพิสูจน์ตัวตนและการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สาย
	72	บริษัทแบ่งระบบเครือข่ายภายในเป็นโซนต่างๆ (Network Segmentation) และวางมาตรการการป้องกันตามระดับความเสี่ยงจากการถูกโจมตีทางไซเบอร์

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Privacy	73	บริษัทมีการวางแผนในเรื่องการใช้งานระบบ สำหรับพนักงานและบุคลากร โดยจัดตามลำดับความสำคัญของการดำเนินงาน และความจำเป็นที่ต้องใช้งาน โดยมีสิทธิในการใช้งานที่แตกต่างกันออกไป
	74	บริษัทมีมาตรการการควบคุมการเข้าถึง OS, Application, และอุปกรณ์คอมพิวเตอร์ ด้วยการพิสูจน์ตัวตน การกำหนดความซับซ้อนของรหัสผ่าน จำนวนครั้งสูงสุดของการใส่รหัสผ่านผิด และเงื่อนไขในการตั้งรหัสผ่านซ้ำกับรหัสเดิม การเปลี่ยนค่า Default password จากการเข้าใช้งานครั้งแรก โดยมีการเข้ารหัสของ password ที่ปลอดภัยทั้งในการจัดเก็บ และระหว่างการรับส่ง
	75	บริษัมีการแยกบัญชีผู้ใช้งานของระบบที่ไม่ได้ใช้งานจริง ออกจากบัญชีผู้ใช้งานของระบบที่ใช้งานจริงอย่างชัดเจน
	76	บริษัทมีระบบการแจ้งเตือนเมื่อระบบมีการเปลี่ยนแปลงสิทธิในการเข้าถึงของผู้ใช้งาน ให้ผู้ที่เกี่ยวข้องทราบโดยอัตโนมัติตามระดับความเสี่ยง เช่น Email หรือ SMS
	77	บริษัทมีมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานสิทธิสูงอย่างเข้มงวด รวมถึงมาตรการควบคุมผู้ดูแลระบบฐานข้อมูลในการเข้าถึงระบบฐานข้อมูล (Database System) เพื่อป้องกันการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต
	78	บริษัทมีมาตรการควคุมการป้องกัน Malware และ Man-in-the-Middle ในขั้นตอนการพิสูจน์ตัวตนของลูกค้าในการทำธุรกรรมที่มีความเสี่ยงสูงตามที่บริษัทกำหนดว่าเป็นธุรกรรมที่มีความเสี่ยงสูงผ่านเครือข่าย Internet
DETECT		
Anomalies and Events	79	บริษัทมีการดำเนินการต่อเหตุการณ์ผิดปกติที่เกิดขึ้น แบบแก้ไขสถานการณ์เป็นกรณี ๆ ไป และยังไม่มีการวางแผนไว้อย่างเป็นระบบ และยังไม่มีบุคลากรที่คอยเฝ้าระวังหรือตรวจสอบความผิดปกติจากภัยคุกคามทางไซเบอร์

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	80	บริษัทมีกระบวนการหรือระบบที่สามารถเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบที่น่าสงสัย หรือเข้าข่ายเป็นการทุจริตในขั้นตอนการพิสูจน์ตัวตนพนักงาน และบุคคลภายนอก และแจ้งเตือนผู้ที่รับมอบอำนาจอัตโนมัติเพื่อดำเนินการแก้ไขอย่างทันท่วงที
	81	บริษัทจัดให้มีการเก็บบันทึกเหตุการณ์อย่างมั่นคงปลอดภัยถึงการบันทึกการเข้าถึง (Access Log) การบันทึกการดำเนินงาน (Activity Log) ที่สำคัญ บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log) และบันทึกด้านการรักษาความปลอดภัย (Security Event Log) โดยสามารถดูย้อนหลังได้ด้วยวิธีการที่ปลอดภัย
	82	บริษัทมีการสอบทาน Access Log และ Activity Log ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย
	83	บริษัทมีมาตรการและกระบวนการในการตรวจจับการเข้าถึงระบบงานที่สำคัญ (Critical System) เพื่อตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตหรือมีการพยายามเข้าถึงอย่างผิดปกติ พร้อมกับมีการประเมินและกำหนดความเหมาะสมของการตั้งค่าเกณฑ์ความผิดปกติ (Thresholds) สำหรับข้อมูลการบันทึกเหตุการณ์ (Log) อย่างสม่ำเสมอ เพื่อติดตามและรายงานพฤติกรรมที่ผิดปกติ
Security Continuous Monitoring	84	บริษัทมีการโปรแกรม Anti-Virus ในการเฝ้าระวังต่อภัยคุกคามทางไซเบอร์ที่อาจจะเข้ามาในระบบเครือข่ายของบริษัท ทั้งอาจจะตั้งใจและไม่ตั้งใจของพนักงานที่ทำงานอยู่ภายในองค์กร
	85	บริษัทมีระบบการติดตามและวิเคราะห์เพื่อใช้แจ้งเตือนพฤติกรรมที่ผิดปกติของผู้ใช้งานตามระดับความเสี่ยง เช่น การใช้งานระบบเครือข่าย การทำงานนอกเวลาทำการ หรือการใช้อุปกรณ์ที่ไม่ได้รับอนุญาต มีเครื่องมือสำหรับตรวจจับเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบและแจ้งเตือนไปยังผู้ที่รับผิดชอบโดยอัตโนมัติ เมื่อถึง Thresholds ที่กำหนดไว้ เพื่อดำเนินการแก้ไขอย่างทันท่วงที

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	86	บริษัทมีกระบวนการเฝ้าระวังการเข้าใช้งานโดยผู้ใช้งานที่ไม่ได้รับอนุญาต การเชื่อมต่อกับระบบของบริษัท ด้วยอุปกรณ์ที่ไม่ได้รับอนุญาต และการติดตั้ง Software ที่ไม่ได้รับอนุญาต
	87	บริษัทมีกระบวนการเฝ้าระวังเหตุการณ์ต่างๆ โดยเชื่อมโยงข้อมูลจากหลายแหล่ง เช่น ระบบเครือข่าย ระบบงาน และ Firewall
Detection Processes	88	บริษัทมีการใช้โปรแกรม Anti-Virus ในการตรวจหา ติดตามต่อภัยคุกคามทางไซเบอร์ที่อาจจะเข้ามาในระบบเครือข่ายของบริษัท ทั้งอาจจะตั้งใจและไม่ตั้งใจของพนักงานที่ทำงานอยู่ภายในองค์กร
	89	บริษัทมีกระบวนการหรือมาตรการแจ้งเตือนเมื่อพบเหตุการณ์ที่มีโอกาสเป็นการโจมตีทางไซเบอร์ เพื่อให้หน่วยงาน ผู้รับผิดชอบในการเฝ้าระวัง การรักษาความมั่นคงปลอดภัยทราบอย่างทันการณ์
	90	บริษัทมีเครื่องมือและกระบวนการในการตรวจจับและแจ้งเตือน เมื่อตรวจพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ เพื่อรายงานให้หน่วยงานหรือผู้ที่มีหน้าที่รับผิดชอบในการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ทราบและดำเนินการแก้ไข
	91	บริษัทมีเครื่องมือหรือกระบวนการในการตรวจจับการพยายามบุกรุกเครือข่าย มีเครื่องมือตรวจจับเหตุการณ์ผิดปกติ (Incident) มีเครื่องมือที่สามารถตรวจจับเมื่อมีการเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ และมีเครื่องมือตรวจจับและแจ้งเตือนเหตุการณ์ตามคามเสี่ยงของทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยสามารถแจ้งเตือนไปยังหน่วยงานหรือผู้รับผิดชอบที่เกี่ยวข้องทันที ให้สามารถดำเนินการรับมือได้อย่างรวดเร็ว (Proactive)
	92	บริษัทมีเครื่องมือเพื่อวิเคราะห์เชื่อมโยงข้อมูลเหตุการณ์ผิดปกติจากแหล่งต่างๆ ของบริษัท แบบ Real Time จากอุปกรณ์เครือข่าย หรืออุปกรณ์รักษาความปลอดภัยเครือข่ายของระบบที่สำคัญ และ มีเครื่องมือที่สามารถตรวจจับภัยคุกคามจากภายในและภายนอกที่เชื่อมโยงในระดับองค์กร รวมถึงแจ้งเตือนหน่วยงานที่รับผิดชอบ และหน่วยงานที่เกี่ยวข้อง

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Cyber Intelligence	93	บริษัทมีการมอบหมายให้มี ผู้ทำหน้าที่บริหารจัดการเหตุการณ์ผิดปกติเมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์ของโซ่อุปทานดิจิทัลเกิดขึ้น และผู้ทำหน้าที่ติดตามและวิเคราะห์ Cyber Threat Intelligence ต้องมีการทำงานอย่างใกล้ชิดและมีบูรณาการ
	94	บริษัทมีการเชื่อมโยงและวิเคราะห์ Threat Intelligence ข้อมูลการบริหารจัดการระบบเครือข่ายและข้อมูลการรับมือเหตุการณ์ผิดปกติ เพื่อเตรียมรับมือภัยคุกคามและตอสนองในเชิงรุกต่อเหตุการณ์ผิดปกติที่อาจเกิดขึ้น
RESPOND		
Response Planning	95	บริษัทแผนการรับมือของบริษัทต่อภัยคุกคามทางไซเบอร์ยัง โดยเป็นการแก้ปัญหาเมื่อเกิดปัญหาภัยคุกคามทางไซเบอร์ ที่พนักงานของบริษัทจะเป็นผู้ที่คอยแก้ปัญหา โดยอาจจะขอความช่วยเหลือจากบริษัทที่ให้บริการจากภายนอก
	96	บริษัทมีแผนฉุกเฉินที่รองรับการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยการจัดทำต้องครอบคลุมกระบวนการดังนี้ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) การประเมินความเสี่ยง (Risk Analysis) การวางกลยุทธ์สำหรับแผนฉุกเฉิน การจัดทำแผนฉุกเฉิน การสื่อสารและฝึกอบรมให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก การทดสอบปรับปรุงและสอบทานแผนฉุกเฉิน โดยการจัดการแผนฉุกเฉินดังกล่าว ต้องสามารถดำเนินการได้ทั้งในระหว่างและหลังจากที่ถูกโจมตี
Communications	97	บริษัทมีการประกาศแจ้งให้ทราบเพื่อเป็นการสื่อสารให้เข้าใจถึงระเบียบวิธีปฏิบัติเมื่อต้องตกอยู่ภายใต้เหตุการณ์ทางไซเบอร์ที่เกิดเหตุการณ์ผิดปกติขึ้น
	98	บริษัทมีการกำหนดช่องทางในการสื่อสารและการส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้องเพื่อให้พนักงานสามารถรายงานข้อมูลเหตุการณ์ทางไซเบอร์ได้อย่างทันการณ์

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	99	บริษัทมีการกำหนดเงื่อนไขในการรายงานเหตุการณ์ผิดปกติทางไซเบอร์หรือช่วงโหว่ของระบบที่ตรวจพบเสนอผู้บริหารระดับสูงตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
	100	บริษัทมีแผนการสื่อสารในการแจ้งองค์กรหรือหน่วยงานภายนอกที่เกี่ยวข้องถึงเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้นซึ่งอาจจะกระทบต่อองค์กร หรือลูกค้าขององค์กร รวมถึงลูกค้าให้ได้รับทราบตามความจำเป็นและเหมาะสม
Analysis	101	บริษัทมีขั้นตอนในการวิเคราะห์ผลกระทบ เพียงแต่ได้รับข้อมูลภัยคุกคามที่ได้มาเพื่อนำมาใช้แก้ปัญหาต่อสถานการณ์ที่เกิดเหตุการณ์ผิดปกติทางไซเบอร์ได้ในระดับหนึ่ง
	102	บริษัทมีการตรวจสอบ วิเคราะห์สาเหตุ และประเมินผลกระทบ เพื่อจัดทำแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) ตามลำดับความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันการณ์
	103	บริษัทมีแผนการรับมือภัยคุกคามและตอบบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) สอดคล้องกับแผนฉุกเฉินที่รองรับการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนบริหารจัดการภาวะวิกฤต
	104	บริษัทมีมาตรฐานและระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital (Digital Forensics) ไว้อย่างชัดเจน
	105	บริษัทมีการจัดประเภทของเหตุการณ์ บันทึก และติดตามเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น และมีกระบวนการติดต่อผู้รับผิดชอบในการวิเคราะห์ รับมือภัยคุกคาม และตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
Mitigation	106	บริษัทยังมีมาตรการที่ใช้ในการบรรเทาต่อภัยคุกคามทางไซเบอร์ที่ยังมีความไม่ชัดเจน ส่วนใหญ่จะเป็นการดำเนินการเมื่อเกิดเหตุการณ์ผิดปกติขึ้น
	107	บริษัทจัดให้มีกระบวนการการจำกัดการเข้าถึง ยกเลิกการใช้งาน ทำลาย หรือทดแทนทรัพย์สินด้านเทคโนโลยีสารสนเทศ ที่มีผลกระทบจากเหตุการณ์ผิดปกติทางไซเบอร์ รวมถึงการวิเคราะห์เหตุการณ์ผิดปกติทางด้านความมั่นคงปลอดภัยตั้งแต่ช่วงแรกเมื่อตรวจพบเหตุการณ์บุกรุกเพื่อตอบสนองและลดผลกระทบต่อเหตุการณ์ดังกล่าวที่อาจเกิดขึ้น
	108	บริษัทมีกระบวนการที่ทำให้มั่นใจว่าทรัพย์สินทางด้านเทคโนโลยีสารสนเทศที่ได้รับผลกระทบจากเหตุการณ์ผิดปกติทางไซเบอร์ มีการตั้งค่าใหม่อย่างเหมาะสม และทดสอบความพร้อมก่อนนำไปใช้งานจริง เพื่อลดความเสี่ยงจากการนำทรัพย์สินดังกล่าวกลับมาใช้งานอีกครั้ง
	109	บริษัทจัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ กรณีที่บริษัทได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ทั้งในระดับหน่วยงานและบริษัท รวมถึงการเชื่อมต่อกับหน่วยงานภายนอกที่เกี่ยวข้อง รวมถึงจัดให้มีการทดสอบระบบงานสำคัญที่ติดตั้งที่หน่วยงานภายนอกอย่างสม่ำเสมอ โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อบริษัททั้งระบบ นอกจากนี้ยังมีการทดสอบต่อระบบสำรองเพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง
Improvements	110	บริษัทได้มีการนำสิ่งที่ได้เรียนรู้ (Lessons Learned) จากการถูกโจมตีหรือเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น ทั้งภายในและภายนอกบริษัท มาปรับปรุงแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์
Supply Chain Agility	111	บริษัทมีกระบวนการในการตรวจจับภัยคุกคามทางไซเบอร์ที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ที่จะสามารถเกิดขึ้นได้ในโซ่อุปทานดิจิทัลด้วยความรวดเร็ว

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	112	บริษัทมีขั้นตอนในการตัดสินใจที่จะกระทำการใด ๆ เมื่อพบกับภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานดิจิทัลด้วยความรวดเร็ว
	113	บริษัทมีความสามารถในการตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานดิจิทัลด้วยความรวดเร็ว
	114	บริษัทมีกระบวนการที่สามารถจะปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานดิจิทัลได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัท
RECOVER		
Recovery Planning	115	มีแผนการกู้คืนต่อเหตุการณ์ผิดปกติที่ดำเนินการอยู่ยังสามารถจัดการต่อภัยคุกคามทางไซเบอร์ได้อยู่ในระดับหนึ่ง
	116	บริษัทมีแผนการกู้คืนต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยการจัดทำต้องครอบคลุมกระบวนการดังนี้ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) การประเมินความเสี่ยง (Risk Analysis) การวางกลยุทธ์สำหรับแผนฉุกเฉิน การจัดทำแผนฉุกเฉิน การสื่อสารและฝึกอบรมให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก การทดสอบปรับปรุงและสอบทานแผนฉุกเฉิน โดยการจัดการแผนฉุกเฉินดังกล่าวต้องสามารถดำเนินการได้ทั้งในระหว่างและหลังจากที่ถูกโจมตี
Improvements	117	บริษัทได้มีการนำสิ่งที่ได้เรียนรู้ (Lessons Learned) จากการถูกโจมตีหรือเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น ทั้งภายในและภายนอกบริษัท มาปรับปรุงแผนการกู้คืนต่อเหตุการณ์ผิดปกติทางไซเบอร์
Communications	118	บริษัทจัดให้มีการสื่อสารเรื่องความปลอดภัยเพื่อสร้างความมั่นใจต่อการดำเนินงานให้แก่บุคลากรภายในรับทราบ
	119	บริษัทจัดให้มีการประชาสัมพันธ์ในมาตรการ และกิจกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้แก่หน่วยงานภายในและภายนอกบริษัท ลูกค้า ซัพพลายเออร์ และผู้มีส่วนได้เสียเพื่อสร้างความเชื่อมั่น และน่าเชื่อถือ

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	120	บริษัทมีกระบวนการในการเรียกชื่อเสียงของบริษัทกลับคืนมาหลังจากที่ได้รับผลจากเหตุการณ์ผิดปกติทางไซเบอร์ไว้อย่างชัดเจน
Robust Strategy	121	บริษัทมีกระบวนการในการกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานในโซ่อุปทานดิจิทัลเกิดการหยุดชะงัก
	122	บริษัทมีความสามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ ๆ หลังจากการถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานเกิดการหยุดชะงัก
	123	บริษัทมีมาตรการเกี่ยวกับการเตรียมความพร้อมด้านการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานเกิดการหยุดชะงัก
	124	บริษัทสามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานดิจิทัลต่อไปได้แม้จะถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำให้การดำเนินงานเกิดการชะงัก
	125	บริษัทสามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่อุปทานดิจิทัลหลังจากที่ถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำให้การดำเนินงานเกิดการชะงัก
CONTINUITY		
Supply Chain Sustainability	126	บริษัทได้มีการตั้งคณะกรรมการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดยมีบทบาทหน้าที่ในการกำหนดกลยุทธ์ นโยบาย และแผนงานเทคโนโลยีสารสนเทศ ให้ครอบคลุมความมั่นคงปลอดภัยไซเบอร์และสอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ตลอดทั้งโซ่อุปทานดิจิทัล รวมทั้งดูแลติดตามการดำเนินงาน ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	127	บริษัทมีผู้บริหารที่เห็นความสำคัญและจำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยได้เข้ามามีบทบาทและหน้าที่ความรับผิดชอบในการกำหนดและอนุมัติกลยุทธ์ นโยบาย รวมทั้งกำกับดูแล และติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้สอดคล้องกับการดำเนินธุรกรรมในโซ่อุปทานดิจิทัล
	128	บริษัทมีการจัดสรรงบประมาณที่เพียงพอ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ครอบคลุม ถึงระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐาน (Infratructure) รวมทั้งบุคลากร เครื่องมือและบริการที่เกี่ยวข้อง
Dependability of Supply Chain	129	บริษัทมีการกำหนดถึงความพร้อมต่อกระบวนการการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยระบบจะต้องสามารถเปิดใช้งานได้ทันทีเมื่อมีการร้องขอจากผู้ใช้งาน
	130	บริษัทมีการกำหนดความน่าเชื่อถือต่อการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยระบบจะต้องสามารถจัดการได้ตามความคาดหวังหรือความต้องการของผู้ใช้งาน
	131	บริษัทมีการกำหนดถึงความปลอดภัยต่อการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยระบบจะต้องสามารถแสดงให้เห็นได้ถึงความเสี่ยหายที่อาจจะเกิดขึ้น
	132	บริษัทมีการกำหนดถึงความสามารถในการป้องกันตัวเองจากการโจมตีที่จะส่งผลถึงความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล จากผู้บุกรุกที่เจตนาจะเข้ามาโจมตีหรือโดยไม่ได้ตั้งใจ
	133	บริษัทมีการกำหนดถึงความสามารถในการต่อต้าน และกู้คืนจากเหตุการณ์ที่เกิดจากการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้หน่วยงานเสียหาย ต่อโซ่อุปทานดิจิทัล โดยเมื่อถูกโจมตีแล้วระบบจะยังต้องสามารถดำเนินการต่อไปได้

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	134	บริษัทมีการกำหนดถึงความสามารถการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่จะต้องแสดงให้เห็นถึงขอบเขตที่ระบบสามารถปรับให้เข้ากับความต้องการใหม่
Business Continuity Plan	135	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยงที่สามารถทำให้กิจการดำเนินต่อไปได้
	136	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ
	137	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้
	138	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจ และจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัทพร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม
	139	บริษัทมีแผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้
Business Continuity Assessment	140	บริษัทได้ดำเนินการจัดให้มีการประเมินความต่อเนื่องทางธุรกิจ โดยทำการตรวจสอบด้านการรักษาความมั่นคงความปลอดภัยไซเบอร์ โดยดำเนินการติดตามอย่างสม่ำเสมอเพื่อป้องกันและรับมือต่อภัยคุกคามไซเบอร์ได้อย่างทันท่วงที
	141	บริษัทได้จัดให้มีหน่วยงานที่มีหน้าที่และความรับผิดชอบในการประเมินความต่อเนื่องทางธุรกิจ และจัดการความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องกับการปฏิบัติงานประจำ และงานที่ได้รับมอบหมาย รวมทั้งติดตาม จัดทำรายงาน เฝ้าระวังภัยคุกคาม และศึกษาแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการจัดการความต่อเนื่องทางธุรกิจ โดยนำเสนอรายงานต่อคณะกรรมการที่ไดรับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง

ตารางที่ 4.38 (ต่อ)

Category	ตัวชี้วัด	
	142	บริษัทมีขอบเขตการตรวจสอบกระบวนการการจัดทำการประเมินความต่อเนื่องทางธุรกิจที่บริษัทยอมรับได้ โดยมีความเหมาะสมกับขนาดและความซับซ้อนของการดำเนินธุรกิจ รวมไปถึงการสอบทานระดับความของต่อเนื่องทางธุรกิจกับผลที่ได้ควบคู่กับประเมินความพร้อมด้าน Cyber Resilience

4.3 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3

การศึกษาเพื่อตอบวัตถุประสงค์ในข้อที่ 3 เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ผลการพัฒนาตัวแบบวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีการดำเนินการในขั้นตอนต่าง ๆ 2 ขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 พัฒนาระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains)

การกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ทำการนิยามระดับของวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ไว้โดยทำการนิยามไว้ดังตารางที่ 4.39

ตารางที่ 4.39 นิยามของระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

Level	Description	Characteristics
1	**ระดับเริ่มต้น (Initial Level)** เป็นระดับที่บริษัทต่าง ๆ ต้องจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยอาศัยความสามารถของบุคลากรเพียงอย่างเดียว ซึ่งมีลักษณะของการทำงาน ที่ยังไม่เป็นทางการ	1. มีหลักฐานเอกสารที่บ่งบอกว่าองค์กรหรือบริษัทมีการกล่าวถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล และความต้องการที่จะมีอยู่ แต่ยังไม่มีการนำเอามาตรฐานใด ๆ มาใช้ในกระบวนการ 2. ไม่มีกฎเกณฑ์และการสื่อสารภายในบริษัทในด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
	มากนักยังไม่มีการควบคุมที่ ไม่มีการวางแผนงานที่เป็นระบบจึงทำให้ไม่สามารถประเมินคุณภาพในการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่เกิดขึ้นว่าจะมีคุณภาพดีหรือไม่	ที่เป็นกระบวนการที่เป็นมาตรฐาน 3. เมื่อเกิดปัญหาก็จะดำเนินการแก้ปัญหาเฉพาะกรณี ๆ ไป จะเป็นการประชุมกันภายในองค์กรเพื่อดำเนินการจัดการ 4. มีกระบวนการที่จัดการต่อความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลที่ไม่สามารถคาดเดาได้ (unpredictable process) 5. ไม่มีการกำหนดขั้นตอนในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลในองค์กร 6. ยังไม่มีระบบสารสนเทศที่ใช้ในการจัดการที่ดีในองค์กร 7. การอบรมพนักงานยังไม่มีประสิทธิภาพ หรือบางทีก็ยังไม่มีการอบรมใด ๆ เลย
2	**ระดับจัดการเบื้องต้น (Repeatable Level)** ในระดับนี้มีแนวทางในการจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลเบื้องต้น มีการวางแผน การทำงานอย่างเป็นระบบ มีการจัดทำเอกสาร สามารถตรวจสอบ และนำไปปฏิบัติได้ บริษัทต่าง ๆ สามารถเข้าสู่ระดับนี้ได้ จะสามารถจัดการต่อปัญหาภัยคุกคามทางไซเบอร์ที่มีลักษณะแบบเดียวกันให้ประสบผลสำเร็จได้ เช่นเดียวกับภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลที่สามารถจัดการได้สำเร็จไปแล้ว	1. เริ่มมีการทำความเข้าใจในบริบทขององค์กร และมีความตระหนัก ต่อความสำคัญในการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 2. มีการกำหนดความจำเป็นและความคาดหวังขององค์กรต่อการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 3. มีการนำเอาระบบสารสนเทศ การพยากรณ์ และตัวชี้วัดเบื้องต้นมาใช้สำหรับการจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 4. เริ่มต้นการพัฒนาในการกำหนดมาตรฐาน กิจกรรมและตัวชี้วัดด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล 5. มีการดำเนินการในด้านการวางแผน การส่งมอบ การตรวจสอบรวมไปถึงการจัดทำเอกสารที่เกี่ยวกับกระบวนการ นโยบาย และขั้นตอนในการดำเนินงานในด้านการจัดการต่อปัญหาภัยคุกคาม

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
		ทางไซเบอร์ของโซ่อุปทานดิจิทัล 6. มีการนำเอานโยบาย แผนการไปใช้ปฏิบัติ เพื่อให้บรรลุผลของการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 7. มีการตรวจสอบ และกำกับดูแล แนวทางในการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 8. มีการให้ความสำคัญต่อปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์ ได้มีการกำหนดขึ้นอย่างเป็นทางการซึ่งอาจจะต้องมีการเปลี่ยนแปลงกระบวนการในการดำเนินงานขององค์กร ที่ดำเนินการโดยฝ่ายผู้บริหารขององค์กร 9. การเลือกกระบวนการด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ถูกกำหนดเพื่อปรับปรุง และควบคุมกระบวนการหลักขององค์กร และจะมีการวางแผนการตรวจสอบการลงทุนอย่างมีประสิทธิภาพ โดยจะทำการดำเนินการในบริบทตามกรอบแนวคิดโครงสร้างพื้นฐานทางด้านไอทีขององค์กรหรือบริษัทนั้น ๆ 10. มีการกำหนดขั้นพื้นฐานเกณฑ์ในการวัดความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลรวมถึงเทคนิควิธีสำหรับการประเมิน แต่อย่างไรก็ตามวิธีการดังกล่าวก็ยังไม่ได้ถูกปรับใช้ทั่วทั้งองค์กรหรือบริษัท 11. องค์กรยังไม่มีการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลอย่างเป็นรูปแบบ รวมถึงไม่มีการสื่อสารเกี่ยวกับการกำกับดูแลและแบ่งความรับผิดชอบให้แต่ละบุคคล

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
		12. เครื่องมือที่จะนำมาใช้สำหรับการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล จะยังมีข้อจำกัดในการถูกเลือกและนำไปใช้ เนื่องจากยังขาดผู้เชี่ยวชาญ โดยจะสามารถทำได้เพียงการนำมาใช้วัดในเรื่องความปลอดภัยได้เท่านั้น แต่อาจจะยังไม่ได้ถูกนำมาใช้แบบสมบูรณ์
3	**ระดับที่มีการกำหนดกระบวนการขึ้นอย่างชัดเจน (Defined Level)** ในระดับนี้เป็นการพัฒนาเพิ่มขึ้นจาก Repeatable Level การเข้าสู่ระดับบริษัทต่าง ๆ จะต้องมีการกำหนดแนวทางในการปฏิบัติงานด้านการจัดทำเอกสาร และกำหนดมาตรฐานในการปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลได้อย่างเหมาะสม โดยมาตรฐานดังกล่าว ต้องมีแนวปฏิบัติแบบเดียวกันทั้งองค์กร นั้นคือ องค์กรเริ่มมีระเบียบวิธีการปฏิบัติงานที่เป็นมาตรฐานของตนเอง	1. มีการยอมรับในความสำคัญของการป้องกันภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีการกำหนดค่าพื้นฐานของตัวชี้วัด มีการเชื่อมโยงผลลัพธ์กับสิ่งที่มีอยู่ โดยได้ทำการกำหนดไว้ให้เป็นเอกสารที่ชัดเจนมากขึ้น 2. มีการบูรณาการในนโยบายกระบวนการ ระบบสารสนเทศ หน่วยงาน รวมไปถึงกิจกรรมที่เป็นแนวทางในการปฏิบัติให้มีรูปแบบ หรือมีมาตรฐานมากขึ้น โดยกำหนดเป็นกลยุทธ์ การวางแผนการดำเนินงาน รวมไปถึงกระบวนการตรวจสอบ ขั้นตอนของกระบวนการให้มีความเป็นมาตรฐานมากขึ้น มีการสื่อสารที่เป็นขั้นตอนและการอบรมที่มีแบบแผน 3. มีการพัฒนาระบบงานในการรักษาความมั่นคงปลอดภัยให้มีมาตรฐานในการปฏิบัติงาน โดยอาจจะมีการนำหลักการที่เป็นมาตรฐาน เช่น ISO ต่าง ๆ เข้ามาใช้ในการปฏิบัติการ 4. มีการกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลและแผนการในการบรรลุวัตถุประสงค์นั้น 5. มีการกำหนดถึงบทบาทหน้าที่ความรับผิดชอบของหน่วยงานและตัวบุคคล 6. ตัวชี้วัดของกิจกรรมทั้งหมดจะถูกบันทึก และ

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
		ติดตาม ซึ่งจะนำไปสู่การปรับปรุงต่อไป การวัดต่างๆ มีแบบแผนมีมาตรฐาน แต่การนำปฏิบัตินั้นยังไม่มีความชำนาญนัก บุคคลจะได้รับการฝึกอบรมเพื่อเรียนรู้การใช้เครื่องมือในการวัดตามมาตรฐาน จะยังไม่มีการวิเคราะห์รากฐานของปัญหา โดยจะทำเป็นครั้งคราวเท่านั้น
4	**ระดับมีการจัดการ (Managed Level)** เป็นการพัฒนาเพิ่มขึ้นจาก Defined Level ลักษณะการปฏิบัติในระดับนี้ผู้จัดทำต้องมีการรวบรวมข้อมูล รายละเอียดการปฏิบัติงานต่างๆ ที่เกิดขึ้นไว้ในรูปของสถิติ (Statistical Process Control) เพื่อนำข้อมูลนั้นมาใช้ในการศึกษาวิเคราะห์ผลการทำงาน สามารถวัดผลและควบคุมกระบวนการในการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล	1. มีการมีความเข้าใจเรื่องของความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยเกิดจากการอบรมอย่างมีแบบแผน ทำให้มีความเข้าใจที่ชัดเจน มีการกำหนดความรับผิดชอบและการตรวจสอบที่มีมาตรฐาน 2. กระบวนการทางด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล มีความสอดคล้องกับกลยุทธ์ขององค์กร การปรับปรุงกระบวนการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลเป็นไปตามหลักความเข้าใจในเชิงปริมาณ มีการนำหลักการทางสถิติมาใช้ในการวิเคราะห์ผลการทำงาน โดยสามารถประเมิน วัดผลและควบคุมกระบวนการในการดำเนินงาน และมีความเป็นไปได้ที่จะตรวจสอบหรือวัดผลการปฏิบัติงาน 3. ผู้มีส่วนได้ส่วนเสียในทุก ๆ กระบวนการจะมีความตระหนักในความเสี่ยงรวมถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ในเชิงคุณค่าที่จะได้รับการจัดการ รวมทั้งมีการกำหนดเกณฑ์ความคลาดเคลื่อนของกระบวนการที่ต้องดำเนินการ 4. มีกระบวนการมากมายที่ต้องทำแต่ไม่ใช่ว่าทุกกระบวนการจะเป็นการทำงานที่ประสิทธิภาพเสมอ

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
		ไป บางครั้งกระบวนการอาจจะต้องปรับปรุงมีการวิเคราะห์รากของปัญหาเป็นไปตามมาตรฐาน 5. เริ่มเห็นความสำคัญของกระบวนการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) และมีการปฏิบัติในประเด็นนี้ผู้เชี่ยวชาญภายในองค์กรมีส่วนร่วมเพื่อแลกเปลี่ยนเรียนรู้ถึงความต้องการต่างๆ
5	**ระดับปรับปรุงให้เหมาะสมที่สุด (Optimizing Level)** เป็นระดับที่ได้นำเอาหลักการจัดการคุณภาพ (Continuous Process Improvement) มาใช้ เพื่อป้องกันไม่ให้เกิดข้อบกพร่องในการปฏิบัติงาน และนำไปสู่ การพัฒนาอย่างต่อเนื่อง รวมถึงเพื่อให้บริษัทต่าง ๆ สามารถปรับเปลี่ยนตัวเองให้สอดคล้องกับการเปลี่ยนแปลงทางด้านเทคโนโลยีได้	1. มีการนำเอาหลักการของการจัดการคุณภาพมาใช้ในการกระบวนการด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ในองค์กร โดยพัฒนาให้อยู่ในระดับที่เป็นการปฏิบัติที่ดีที่สุด ด้วยพื้นฐานที่มาจากการปรับปรุงอย่างต่อเนื่องและเป็นตัวแบบให้กับองค์กรอื่น 2. การฝึกอบรมและการสื่อสารได้รับการสนับสนุนจากผู้บริหารมากขึ้น 3. นโยบายต่าง ๆ ที่นำไปใช้ในองค์กรมีการปรับใช้ได้อย่างรวดเร็วและสนับสนุนต่อความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล อย่างเต็มที่ 4. ปัญหาและความเบี่ยงเบนที่เกิดขึ้นถูกวิเคราะห์จากรากของปัญหาทั้งหมด โดยการปฏิบัติที่มีประสิทธิภาพ ในระดับนี้จะได้มีการนำเอาเทคโนโลยี สารสนเทศมาใช้เพื่อขยาย บูรณาการ และปรับให้เป็นการทำงานที่เป็นอัตโนมัติ รวมถึงมีเครื่องมือหลายๆ เครื่องมือเพื่อปรับปรุงคุณภาพและประสิทธิภาพ 5. มีการกำหนดความเสี่ยง และผลลัพธ์ที่เกิดขึ้นว่ามีอะไรบ้าง รวมถึงความสมดุลของการสื่อสารระหว่างองค์กร 6. มีการกำหนดผู้เชี่ยวชาญจากภายนอกเพื่อใช้ในการตรวจสอบ การประเมินตนเองและมีการสื่อสาร

ตารางที่ 4.39 (ต่อ)

Level	Description	Characteristics
		เกี่ยวกับความคาดหวังด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลถูกขยายภายในองค์กร 7. มีเทคโนโลยีที่เหมาะสมเพื่อที่จะสนับสนุนการวัด การวิเคราะห์ การติดต่อสื่อสารและการอบรมในด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลขององค์กรและมีการเชื่อมโยงอย่างมีกลยุทธ์

เมื่อได้ทำการวิเคราะห์และสังเคราะห์ “ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Cyber-Resilient Supply Chain Model)” ตามในภาพประกอบที่4.12 เพื่อพัฒนาให้เป็น “ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Capability Maturity Model for Cyber-Resilient Supply Chain)” ตามในภาพประกอบที่ 4.13

Level 1 Initial การทำงานที่ยังไม่เป็นทางการ ยังไม่มีการควบคุม ไม่มีการวางแผนงานที่เป็นระบบ	**Level 2** Repeatable มีการวางแผนการทำงานอย่างเป็นระบบ สามารถตรวจสอบ และนำไปปฏิบัติได้	**Level 3** Defined มีการกำหนดแนวทางและมาตรฐานในการปฏิบัติงาน	**Level 4** Managed วิเคราะห์ผลการทำงาน สามารถวัดผล และควบคุมกระบวนการ	**Level 5** Optimizing มีการจัดการคุณภาพในการปฏิบัติงานและการพัฒนาอย่างต่อเนื่อง
				10 มีการจัดทำเอกสารที่ใช้ในการประเมินและตรวจสอบผลการดำเนินงาน
				9 มีการประเมินผล พัฒนาและปรับปรุงอย่างต่อเนื่อง
			8 มีการวิเคราะห์ผล โดยใช้สถิติ เพื่อประเมินวัดผล และควบคุมการดำเนินงาน	8 มีการวิเคราะห์ผล โดยใช้สถิติ เพื่อประเมินวัดผล และควบคุมการดำเนินงาน
		7 มีการจัดทำเอกสารการตรวจสอบกำกับดูแลการดำเนินการ	7 มีการจัดทำเอกสารการตรวจสอบกำกับดูแลการดำเนินการ	7 มีการจัดทำเอกสารการตรวจสอบกำกับดูแลการดำเนินการ
		6 มีการกำหนดบทบาทหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลต่างๆ	6 มีการกำหนดบทบาทหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลต่างๆ	6 มีการกำหนดบทบาทหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลต่างๆ
	5 มีการตรวจสอบ และกำกับดูแลต่อแนวทางในการปฏิบัติ	5 มีการตรวจสอบ และกำกับดูแลต่อแนวทางในการปฏิบัติ	5 มีการตรวจสอบ และกำกับดูแลต่อแนวทางในการปฏิบัติ	5 มีการตรวจสอบ และกำกับดูแลต่อแนวทางในการปฏิบัติ
	4 มีการนำเอานโยบาย/แผนที่ได้วางไว้ไปสู่การปฏิบัติ	4 มีการนำเอานโยบาย/แผนที่ได้วางไว้ไปสู่การปฏิบัติ	4 มีการนำเอานโยบาย/แผนที่ได้วางไว้ไปสู่การปฏิบัติ	4 มีการนำเอานโยบาย/แผนที่ได้วางไว้ไปสู่การปฏิบัติ
3 มีการประกาศ/สื่อสาร/อบรมทั้งภายในและภายนอกองค์กร	3 มีการประกาศ/สื่อสาร/อบรมทั้งภายในและภายนอกองค์กร	3 มีการประกาศ/สื่อสาร/อบรมทั้งภายในและภายนอกองค์กร	3 มีการประกาศ/สื่อสาร/อบรมทั้งภายในและภายนอกองค์กร	3 มีการประกาศ/สื่อสาร/อบรมทั้งภายในและภายนอกองค์กร
2 มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น	2 มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น	2 มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น	2 มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น	2 มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น
1 มีการกำหนดนโยบาย / จัดทำแผนวัตถุประสงค์และแผนการดำเนินงาน	1 มีการกำหนดนโยบาย / จัดทำแผนวัตถุประสงค์และแผนการดำเนินงาน	1 มีการกำหนดนโยบาย / จัดทำแผนวัตถุประสงค์และแผนการดำเนินงาน	1 มีการกำหนดนโยบาย / จัดทำแผนวัตถุประสงค์และแผนการดำเนินงาน	1 มีการกำหนดนโยบาย / จัดทำแผนวัตถุประสงค์และแผนการดำเนินงาน

ภาพประกอบที่ 4.13 ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ในการจัดการความต่อเนื่องทางธุรกิจดิจิทัลของโซ่อุปทานดิจิทัลนั้น จะมีองค์ประกอบและตัวชี้วัดภายในที่แสดงถึงระดับความสามารถของวิสาหกิจขนาดกลางและขนาดย่อม ในการตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีและความสามารถในการคืนสภาพได้ด้านไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งคะแนนที่ได้รับจากการประเมินผลของบุคลากรของวิสาหกิจขนาดกลางและขนาดย่อมในฐานะตัวแทนองค์กร ที่ผ่านทั้ง 32 มิติการดำเนินงาน ทำให้สามารถแสดงถึงระดับวุฒิภาวะความสามารถสำหรับการคืนสภาพได้ด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลได้ดังตารางที่ 4.40 นี้

ตารางที่ 4.40 ระดับวุฒิภาวะความสามารถการสร้างคืนสภาพได้ด้านไซเบอร์ของโซ่อุปทานดิจิทัล

ระดับวุฒิภาวะความสามารถ (Capability Maturity Level)	**ตัวชี้วัดระดับวุฒิภาวะความสามารถ (Maturity Indicator Level)**	
Level 1 : Initial	MIL1	มีการกำหนดนโยบาย จัดทำแผน /วัตถุประสงค์และแผนการดำเนินงาน
	MIL2 MIL3	มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น มีการประกาศอบรม ทั้งภายในและภายนอกองค์กร/สื่อสาร/
Level 2 : Repeatable	MIL4	มีการนำเอานโยบายแผนที่ได้วางไว้ไปสู่การปฏิบัติ/
	MIL5:	มีการตรวจสอบ และกำกับดูแล ต่อแนวทางในการปฏิบัติ
Level 3 : Defined	MIL6	มีการกำหนดบทบาทหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลต่าง ๆ
	MIL7	มีการจัดทำเอกสารการตรวจสอบ กำกับดูแลการดำเนินการ
Level 4 : Managed	MIL8	มีการวิเคราะห์ผล โดยใช้สถิติ เพื่อประเมิน วัดผล และควบคุมการดำเนินงาน
Level 5 : Optimizing	MIL9	มีการประเมินผล พัฒนาและปรับปรุงอย่างต่อเนื่อง
	MIL10	มีการจัดทำเอกสารที่ใช้ในการประเมิน และตรวจสอบผลการดำเนินงาน

สามารถสรุป Level ต่าง ๆ ของตัวชี้วัดระดับวุฒิภาวะความสามารถได้ดังต่อไปนี้

ตัวชี้วัดระดับวุฒิภาวะความสามารถ ที่ 1 – 3 จัดอยู่ใน Level 1 Initial

ตัวชี้วัดระดับวุฒิภาวะความสามารถ ที่ 1 – 5 จัดอยู่ใน Level 2 Repeatable

ตัวชี้วัดระดับวุฒิภาวะความสามารถ ที่ 1 – 7 จัดอยู่ใน Level 3 Defined

ตัวชี้วัดระดับวุฒิภาวะความสามารถ ที่ 1 – 8 จัดอยู่ใน Level 4 Managed

ตัวชี้วัดระดับวุฒิภาวะความสามารถ ที่ 1 – 10 จัดอยู่ใน Level 5 Optimizing

ขั้นตอนที่ 2 พัฒนาแนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทาง ไซเบอร์ของโซ่อุปทานดิจิทัล

เกณฑ์การประเมินตัวชี้วัด ผู้วิจัยได้มีเกณฑ์ในการกำหนดการตอบดังต่อไปนี้

1. Answer การประเมินตามตัวชี้วัดในแต่ละมิติ โดยแต่ละตัวชี้วัดจะให้ผู้ประเมินพิจารณาคะแนน 5 ระดับ โดยแต่ละระดับจะใช้เกณฑ์การให้คะแนนระดับการปฏิบัติ ตามตัวชี้วัดตามมาตรฐาน ISO/IEC 15504 โดยมีรายละเอียดระดับความสำเร็จ ในการปฏิบัติตามตัวชี้วัดดังต่อไปนี้

ระดับ 5 หมายถึง มีความสำเร็จในการปฏิบัติ ตามตัวชี้วัดมากที่สุด (Fully achieved)

ระดับ 4 หมายถึง มีความสำเร็จในการปฏิบัติ ตามตัวชี้วัดมาก (Mostly achieved)

ระดับ 3 หมายถึง มีความสำเร็จในการปฏิบัติ ตามตัวชี้วัดปากลาง (Averaged achieved)

ระดับ 2 หมายถึง มีความสำเร็จในการปฏิบัติ ตามตัวชี้วัดน้อย (Partially achieved)

ระดับ 1 หมายถึง ไม่มีความสำเร็จในการปฏิบัติ ตามตัวชี้วัด (Not achieved)

2. Importance เป็นค่าน้ำหนักในการประเมินตัวชี้วัดแต่ละตัว โดยผู้วิจัยมองว่าในการกำหนดระดับความสำเร็จของตัวชี้วัดแต่ละตัวในข้อที่ 1(Answer) นั้น ยังควรจะต้องมีการกำหนดระดับความสำคัญของระดับคะแนนที่ระบุลงไปด้วย ค่าน้ำหนักจะมีค่าดังต่อไปนี้

- Importance “None” factor = 0 (not included in scoring)
- Importance “Low” factor = 0. 5 (score divided by 2)
- Importance “Normal” factor = 1 (score not affected)
- Importance “High” factor = 2 (score doubled)
- Importance “Critical” factor = 4 (score quadrupled)

4.4 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 4

การศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 4 เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการสร้างคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล จากผลการศึกษาตามวัตถุประสงค์ในข้อที่ 3 เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ซึ่งผู้วิจัยได้ทำการพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model), ตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของ โซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators), ระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains) และแนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทาง ไซเบอร์ของโซ่อุปทานดิจิทัลไปแล้วนั้น

ในขั้นนี้ผู้วิจัยจะได้นำผลที่ได้จากการศึกษาไปตรวจสอบความเหมาะสมและความสอดคล้อง โดยจะได้ใช้ระเบียบวิธีดำเนินงานวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยวิธีการสัมภาษณ์เชิงลึก (In-depth Interview) พร้อมทั้งให้ผู้เชี่ยวชาญทำการประเมินระบบ ซึ่งได้ทำการพัฒนาแบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structure Interview) ซึ่งมีการกำหนดประเด็นคำถามตามกรอบแนวคิด สำหรับการสัมภาษณ์จะเป็นลักษณะซักไซ้ไล่เลียงเพื่อให้ทราบข้อมูลในเรื่องนั้นให้มากที่สุด

จากการสัมภาษณ์เชิงลึกทำให้ผู้วิจัยได้หลักการและแนวทางในการปฏิบัติ จากประสบการณ์จริงจากผู้เชี่ยวชาญ ในมุมมองในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ทำให้ผู้วิจัยได้กรอบแนวปฏิบัติ ตัวชี้วัด พร้อมเกณฑ์ในการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อมที่ชัดเจนมากขึ้น พร้อมกันนี้ผู้วิจัยได้นำผลจากการสัมภาษณ์เชิงลึกมาดำเนินการวิเคราะห์เนื้อหา (Content Analysis) (เอื้อมพร หลินเจริญ, 2555; อมาวสี อัมพันศิริรัตน์, 2557) โดยแนวทางที่ใช้ในการสัมภาษณ์ จะแสดงรายละเอียดอยู่ในภาคผนวก จะประกอบไปด้วยประเด็นของการสอบถาม โดยมีรายละเอียดดังต่อไปนี้

1. แนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

2. แนวทางการกำหนดตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicator)

3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chain)

4. แนวทางการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

5. ระดับความคิดเห็นโดยรวมต่อตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

5.1 การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีความเหมาะสมหรือไม่

5.2 ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีความเหมาะสมอยู่ในระดับใด (5,4,3,2,1)

5.3 ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับอยู่ในระดับใด (5,4,3,2,1)

5.4 ข้อเสนอแนะโดยรวมต่อสิ่งที่ควรปรับปรุงใน ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

5.5 ข้อเสนอแนะต่อปัจจัยความสำเร็จของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม (Digital SME Business)

5.6 ข้อเสนอแนะต่อการคืนสภาพได้อย่างยั่งยืนของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม (Sustainable Resilient Digital SME Business)

ผลการวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกด้วยการวิเคราะห์เชิงเนื้อหา (Content Analysis)

โดยผลสรุปการสัมภาษณ์ของแนวทางในแต่ละข้อนั้น ผู้วิจัยได้ทำการสรุปผลของการสัมภาษณ์ตามแนวทางต่าง ๆ ซึ่งมีรายละเอียดดังต่อไปนี้

1. แนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model) ดังรายละเอียดในตารางที่ 4.41

ตารางที่ 4.41 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับแนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	1. Supply Chain ในที่นี้ กำหนด Industry ด้านไหน หรือใช้ได้กับทุก Industry ให้เหตุผลด้วย
		2. ขาดตัวอย่างการประยุกต์ใช้งานจริง กับธุรกิจ SME ควรยกมาสัก 1-2 ราย
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	1. ถูกต้องตามหลักวิชาการ
		2. คลอบคลุมประเด็น/เนื้อหาที่เกี่ยวข้อง
		3. น่าจะมีวิธีการในการแสดงความ สัมพันธ์ระหว่าง 6 หมวด 32 มิติ ไม่ใช่ลอย ๆ
3	ดร.มงคล กลิ่นกระจาย	1. ปรับความชัดเจนของตัวอักษรในภาพประกอบที่ 1 และอาจจะทำการหมุนแกนของภาพประกอบที่1 ให้เป็นตามแนวนอนแล้วทำการขยายภาพ
		2. หมวดที่ 4 ในมิติที่ 2 ให้ปรับคำอธิบายตาม comment โดยเพิ่มคำอธิบายของมิติที่ 2 เข้าไปจากเดิม คือ กิจกรรมการตอบสนองมีการประสานงานกับ ให้เพิ่มเป็น กิจกรรมการตอบสนองมีการประสานงานข้อมูลหรือเหตุการณ์ผิดปกติกับ
		3. หมวดที่ 5 ในมิติที่ 2,3,4 ขอแนะนำให้ปรับตาม comment โดย มิติที่ 2 เพิ่มข้อความจาก การวางแผนและกระบวนการกู้คืนจะได้รับการปรับปรุงโดยผสมผสาน ปรับเป็น การวางแผนและกระบวนการกู้คืนจะได้รับการปรับปรุงแก้ไขให้กลับเข้าสู่สภาวะปกติโดยผสมผสาน มิติที่ 3 เปลี่ยนจากคำว่า ฝ่าย เป็น หน่วยงาน มิติที่ 4 เพิ่มคำขยายความ

ตารางที่ 4.41 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
		4. หมวดที่ 6 มิติที่ 1-4 แนะนำให้เพิ่มรายละเอียดตามความหมายของแต่ละมิติ
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	1. เห็นชอบในส่วนนี้ แต่ขอให้ Re-Confirm เรื่องหัวข้อที่เพิ่มมา (กรอบสีเหลือง) ว่าเป็น Sub-Category หรือไม่ อาจจะหางานวิจัยหรือบทความมายืนยัน
5	ดร.ชาลี วรกุลพิพัฒ์	1. มีความเหมาะสมในภาพรวม แต่ในแต่ละ block ที่เสริมเข้ามาควรที่จะสามารถอธิบายรายละเอียดได้และควร link ให้เข้ากับ keyword ที่สำคัญเช่น AI, Privacy Act, Data Government, ISM-Benchmark เป็นต้น
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	-
7	ผศ.ดร.อัศม์เดช วานิชชินชัย	1. มีความเหมาะสม เนื่องจากอ้างอิงและประยุกต์จากกรอบของ NIST ซึ่งเป็นองค์กรที่ได้รับความเชื่อถือในระดับนานาชาติ และปรับปรุงเพิ่มเติมจากงานวิจัยอื่นที่เกี่ยวข้อง โดยเพิ่มองค์ประกอบ (Category) ไปในแต่ละ Functions
8	ดร.ศักดิ์ เสกขุนทด	1. เหมาะสม
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	1. ยังไม่เห็นข้อแตกต่างระหว่างสิ่งที่เพิ่มเข้าไปในกรอบฯ ต้องสามารถบอกได้ถึงสิ่งที่มีอยู่ สิ่งที่เพิ่มเข้าไป
10	ผศ.ดร.ณฐพร อุตกฤษฏ์	1. ควรมีการจัดทำ Matrix Assessment และ Metha Synthesis เพื่อใช้เปรียบเทียบ the generic standard กับตัวที่ผู้วิจัยนำเสนอ เพื่อให้ชัดเจนถึงวัตถุประสงค์การนำไปใช้ที่แตกต่าง
11	คุณนพพร เทพสิทธา	-

ตารางที่ 4.41 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
12	คุณสุเมธ อักษรกิตติ์	1. ISO 22301 : 2012 และที่ออกใหม่ ISO 22301 : 2019 ตีพิมพ์เมื่อ ตค. 2019 มีอะไรเพิ่มเติมบ้าง 2. การจัดมิติต่างๆ ตรงกับหมวดหมู่อย่างเหมาะสมหรือไม่ ลองดู
13	ดร.อดิศักดิ์ ศรีนครินทร์	1. I'am OK with the framework
14	คุณทัชนันท์ กังวานตระกูล	-
15	ดร.มนู อรดีดลเชษฐ์	-

2. แนวทางการกำหนดตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicator)

ตารางที่ 4.42 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับแนวทางการกำหนดตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	1. No Comment (ดีแล้ว)
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	1. คลอบคลุมเรื่อง กระบวนการ (Process) คน (People) และเครื่องมือ (Tools & Equipment)
		2. ข้อสังเกต เป็นไปได้หรือไม่ที่ยุบรวม category ที่สัมพันธ์กันค่อนข้างมาก เช่น Risk Assessment, Risk Management Strategy, Supply Chain Risk Management
3	ดร.มงคล กลิ่นกระจาย	1. ขอพิจารณาให้ปรับปรุงข้อมูลของแนวทางจาก Plan-Do-Check-Act มาเป็น Plan-Do-Check-Verify กล่าวคือ เปลี่ยนจากคำว่า Act ที่ใช้ความหมายว่าการปฏิบัติ มาเป็น Verify ที่มีความหมายว่า การตรวจรับรอง

ตารางที่ 4.42 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
		2. ขอให้ปรับคำว่า “บริษัท” ที่ปรากฏในตัวชี้วัดในทุก ๆ ข้อให้เป็น “องค์กร” แทน เพราะเป็นคำกลาง ๆ ที่ในบางครั้งการเข้าไปประเมินไม่ได้เข้าไปประเมินในบริษัท แต่เป็นหน่วยงานใดหน่วยงานหนึ่ง
		3. ปรับลำดับข้อของตัวชี้วัด ในแต่ละ category ให้มีจำนวนข้อเป็น 120 ข้อจาก 142 ข้อ ตามคำแนะนำเพื่อเป็นการรวมกลุ่มของตัวชี้วัด ไม่ให้ซ้ำซ้อน
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	1. เนื่องจากตัวชี้วัดมีจำนวนมากจึงอยากให้หาจำนวนที่เหมาะสม สำหรับแบบประเมิน (อาจจะใช้ได้ทั้งหมด ถ้าผู้ตอบสามารถตอบได้)
5	ดร.ชาลี วรกุลพิพัฒ์	1. มีความเหมาะสม แต่ควรอธิบายได้ว่าที่มาของการได้ตัวแบบแต่ละส่วนเป็นอย่างไร - Qualitative --> Quantitative - ศึกษา CMMI ให้ลึก - ศึกษา Self-Assessment ใน ISM-Benchmark และแนวปฏิบัติของการตรวจ Security Policy ของกระทรวง DE
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	
7	ผศ.ดร.อัศม์เดช วานิชชินชัย	1. มีความเหมาะสม กับบริบทของ SME ไทย ทั้งนี้อาจพิจารณาลดจำนวนตัวชี้วัดในบาง Category และเพิ่มในบาง Category (ที่มีตัวชี้วัดเดียว) และทดสอบในบริษัทตัวอย่าง
8	ดร.ศักดิ์ เสกขุนทด	1. เหมาะสม

ตารางที่ 4.42 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	1. ควรอ้างอิง Best Practice, Standards, Framework ที่เกี่ยวข้อง
		2. ตัวชี้วัดที่ทำ เป็นการเพิ่มเข้ามา หรือ adapt จากสิ่งที่เป็นอยู่ต้องอธิบายให้ชัดเจน
10	ผศ.ดร.ณฐพร อุตกฤษฏ์	1. ทำ Matrix Assessment โดยใช้รูปแบบแนวคิด Risk Management มาประยุกต์
11	คุณนพพร เทพสิทธา	-
12	คุณสุเมธ อักษรกิตติ์	1. ตัวชี้วัด (KPI) ควรเป็นรูปธรรม และเห็นได้ชัดเจน เช่น จะวัดแบบไหนด้วยผลลัพธ์อย่างไร (Action Plan) 2. Business Continuity Strategy and Solutions 3. ลองดู ISO 22301 : 2013 Business Continuity Management (Oct 2019)
13	ดร.อดิศักดิ์ ศรีนครินทร์	1. Most indicators must be more specific than this. Example : from 34-43 you should use the standards frm ETDA (to indicate the level of IAL and AAL)
14	คุณทัชนันท์ กังวานตระกูล	-
15	ดร.มนู อรดีดลเชษฐ์	-

3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chain)

ตารางที่ 4.43 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับแนวทางการกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	1. No comment
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	1. ระดับ 2 นิยามและ Characteristics ขาดคำสำคัญ (Keyword) Repeatable
		2. ตารางที่ 3 และ 4 เรียก MIL 1-10 ว่า เป็นตัวชี้วัด ไม่น่าจะถูก เพราะไม่มีลักษณะเป็นตัวชี้วัด (เป็นนามธรรม) และไม่เห็นความสัมพันธ์ระหว่าง 32 มิติ 142 ตัวชี้วัด ในแต่ละ MIL
3	ดร.มงคล กลิ่นกระจาย	1. ปรับเพิ่มเติมความหมายของ Maturity ในแต่ละ level ทั้งในส่วนของ Description และ Characteristics ตามคำแนะนำ
		2. ในภาพประกอบที่2 เน้นใส่สีในแต่ละ Level เพื่อแยกความแตกต่างในแต่ละระดับของตัวแบบวุฒิภาวะ
		3. อธิบายให้เห็นความแตกต่างของตารางที่ 4 และภาพประกอบที่2
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	1. มีความเหมาะสม
5	ดร.ชาลี วรกุลพิพัฒ์	1. ความเห็นเป็นไปได้ในแนวทางเดียวกับส่วนที่ 2 กล่าวคือ ต้องสามารถหาที่มาของการประเมินคะแนนให้ได้และให้เป็นมาตรฐาน คล้ายกับการตรวจ CMMI หรือ Audit ISO/IEC27001
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	-

ตารางที่ 4.43 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
7	ผศ.ดร.อัศฆ์เดช วานิชชินชัย	1. มีการอ้างอิงระดับ Maturity Level จากหน่วยงาน/งานวิจัยที่เชื่อถือได้ ทั้งนี้อาจพิจารณาลำดับขั้นตอนในแต่ละ Level เพื่อให้มีความเข้าใจที่ตรงกันมากขึ้น และให้ User เป็นผู้ทดสอบระบบจริง
8	ดร.ศักดิ์ เสกขุนทด	1. เหมาะสม
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	1. ควรอ้างอิงวิธีการวัดระดับวุฒิภาวะความสามารถอื่น ๆ ด้วย
10	ผศ.ดร.ณฐพร อุตกฤษฏ์	1. ข้อ Assessment รายย่อยบางข้อที่ยังคลุมเครือ ไม่ชัดเจนในการกำหนดระดับวุฒิภาวะ ควรมีการจำแนก should/have to/must เพื่อใช้ในการกำหนดกรอบให้ชัดเจน
11	คุณนพพร เทพสิทธา	-
12	คุณสุเมธ อักษรกิตติ์	1. OK 2. ดู Reactive Supply Chain Management , Dynamic Supply Chain Flexibility
13	ดร.อดิศักดิ์ ศรีนครินทร์	1. I'am OK with the framework
14	คุณทัชนันท์ กังวานตระกูล	1. ให้เน้นอธิบายลักษณะของ maturity ด้วยรูปภาพ
15	ดร.มนู อรดีดลเชษฐ์	-

4. แนวทางการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ตารางที่ 4.44 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับแนวทางการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	1. การพัฒนาโดยใช้ Excel Spreedsheet ช่วยอธิบายให้เห็นภาพชัดเจนกว่านี้
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	1. การให้คะแนน (Answer) 1-5 มีหลักเกณฑ์อย่างไร เป็น Subjective หรือ Objective
		2. Important (weighted factor) การให้ค่าน้ำหนักเช่นเดียวกันกับ Answer คือ มีหลักเกณฑ์อย่างไร
3	ดร.มงคล กลิ่นกระจาย	1. ปรับขยายและวางในแนวนอนให้เต็มหน้าของรายงานในระดับมิติ
		2. เพิ่มคำอธิบายในแต่ละหมวด ที่ท้ายรูปที่เกิดขึ้น
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	1. แนวทางมีความเหมาะสม แต่ควรจะทำการยืนยันในเรื่อง Weighted factor ว่ามีแหล่งอ้างอิงที่เชื่อถือได้หรือไม่
5	ดร.ชาลี วรกุลพิพัฒ์	1. ศึกษาและเทียบการประเมินกับ ISM-Benchmark และนักวิจัยควรหาโอกาสพัฒนาระบบ Self-Assessment ด้วย
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	-
7	ผศ.ดร.อัศม์เดช วานิชชินชัย	1. มีความเหมาะสม อาจให้ user เป็นผู้ประเมินความยากง่ายในการใช้งาน การนำข้อมูลมาสรุป/วิเคราะห์
		2. ในส่วน Important อาจให้ผู้เชี่ยวชาญเป็นผู้ให้น้ำหนักความสำคัญ

ตารางที่ 4.44 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
8	ดร.ศักดิ์ เสกขุนทด	1. เหมาะสม
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	-
10	ผศ.ดร.ณฐพร อุตกฤษฎ์	-
11	คุณนพพร เทพสิทธา	-
12	คุณสุเมธ อักษรกิตติ์	1. OK
		2. รายงานผลในระดับมิติทั้ง 32 มิติ มีกี่ระดับ ดูในรูปไม่ชัดเจน
13	ดร.อดิศักดิ์ ศรีนครินทร์	1. The idea is sound. However "How to do it" needs to be clarified.
14	คุณทัชนันท์ กังวานตระกูล	-
15	ดร.มนู อรดีดลเชษฐ์	-

5. ระดับความคิดเห็นโดยรวมต่อตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

   5.1 ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีความเหมาะสมหรือไม่

ตารางที่ 4.45 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับระดับความคิดเห็นถึงความเหมาะสมของตัวแบบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	Supply Chain ใน Industry อะไรที่เหมาะสมกับ Model นี้
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	มีความเหมาะสม แต่ให้ดูข้อเสนอแนะ/ข้อคิดเห็นในส่วนที่ 1

ตารางที่ 4.45 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
3	ดร.มงคล กลิ่นกระจาย	มีความเหมาะสมดี เพียงแต่สีที่ใช้แสดงผลกรอบความสามารถในแต่ละส่วนควรใช้สีที่แตกต่างกับสีของหมวด เช่นสีเขียว
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	เหมาะสม (แต่ขอให้ยืนยันว่าตรงกับ Category หรือไม่)
5	ดร.ชาลี วรกุลพิพัฒ์	เหมาะสมแล้ว แต่ต้องการรายละเอียดในแต่ละ Block
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	มีความเหมาะสม และมีความเข้าใจตามรูปแบบที่นำเสนอ
7	ผศ.ดร.อัศม์เดช วานิชชินชัย	มีความเหมาะสม โดยดูเหตุผลในส่วนที่ 1 (หน้าที่ 5) เพิ่มเติม
8	ดร.ศักดิ์ เสกขุนทด	เหมาะสม
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	อธิบายความแตกต่างระหว่าง Framework ตั้งต้น
10	ผศ.ดร.ณฐพร อุตกฤษฏ์	แม้ว่าในภาพรวมอาจจะยังไม่แสดงถึงแนวทางและรูปแบบที่ต้องการพัฒนา แต่ยังมีความซ้ำซ้อน
11	คุณนพพร เทพสิทธา	มีความเหมาะสมในระดับหนึ่ง เพราะได้ผ่านการศึกษามาอย่างดี และนำมา Integrate กันได้เหมาะสม แต่ขอให้มองภาพของ Supply Chain Process หลัก ๆ เข้ามาประกอบด้วย เช่น Sourcing, People รวมทั้งหาวิธีที่จะทำให้ Practical มากขึ้น เหมาะกับ SME นำไปใช้ด้วยตนเอง
12	คุณสุเมธ อักษรกิตติ์	1. เหมาะสม 2. Dependability of Supply Chain เกี่ยวข้องกับ Continuity อย่างไรบ้าง
13	ดร.อดิศักดิ์ ศรีนครินทร์	want to see the example frm the real work.
14	คุณทัชนันท์ กังวานตระกูล	เหมาะสมดีแล้ว
15	ดร.มนู อรดีดลเชษฐ์	เหมาะสม

5.2 ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีความหมาะสมอยู่ในระดับใด (5,4,3,2,1)

ตารางที่ 4.46 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับระดับความคิดเห็นถึงความเหมาะสมของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ลำดับ	ผู้ประเมิน	ระดับ	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	4	-
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	3	ให้ดูข้อเสนอแนะ/ข้อคิดเห็นในส่วนที่ 3
3	ดร.มงคล กลิ่นกระจาย	4	เนื่องด้วยครอบคลุมในเกือบทุกมิติ เพียงขาดคำอธิบายด้านท้ายรูปที่แสดง จึงแนะนำให้ขยายรูปในแนวนอนให้เห็นได้ชัด แล้วมีคำอธิบายใต้รูป โดยทำตัวอย่างระดับหน้าที่ในแต่ละหมวดด้วยสีให้แยกชัดเจน
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	5	
5	ดร.ชาลี วรกุลพิพัฒ์	5	เหมาะสมแล้ว แต่ว่าในแต่ละข้ออาจ weight ต่างกัน คล้ายกับการ Audit ISO/IEC27001 เช่น หากข้อใดไม่ผ่านถือว่าไม่ผ่านทั้งหมด เป็นต้น
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	4	สมควรที่จะต้องปรับข้อความบางส่วนให้มีความเข้าใจมากยิ่งขึ้น
7	ผศ.ดร.อัศม์เดช วานิชชินชัย		มีความเหมาะสมเบื้องต้น พิจารณาลำดับ Maturity Level เพิ่มเติมในส่วนที่ 3 หน้า 23
8	ดร.ศักดิ์ เสกขุนทด		เหมาะสม

ตารางที่ 4.46 (ต่อ)

ลำดับ	ผู้ประเมิน	ระดับ	ข้อเสนอแนะ/ข้อคิดเห็น
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	3	ควรเปรียบเทียบกับ Model อื่นๆ ด้วยก่อนสรุปถึง maturity ทั้ง 5 ระดับ
10	ผศ.ดร.ณฐพร อุตกฤษฎ์	4	ถ้ามีการปรับตัวแบบตามที่แนะนำจะทำให้ตัวแบบนี้มีความน่าสนใจมากขึ้น
11	คุณนพพร เทพสิทธา	5	มีความเหมาะสมและชัดเจนดีแล้ว
12	คุณสุเมธ อักษรกิตติ์	4	Level 3 มีการอ้างอิงมาตรฐานอะไรหรือไม่ลองค้นดู
13	ดร.อดิศักดิ์ ศรีนครินทร์		เหมาะสม
14	คุณทัชนันท์ กังวานตระกูล	4	มีความเหมาะสม แต่ให้เขียนหลักเกณฑ์ในการ Satisfied Maturity Level ให้เป็นนิยาม
15	ดร.มนู อรดีดลเชษฐ์		เหมาะสม
ค่าเฉลี่ยของระดับความเหมาะสม		**4.09**	

ดังนั้นจากระดับความเหมาะสมของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับความเหมาะที่ระดับมาก โดยค่าเฉลี่ยที่ได้มีค่าอยู่ที่ 4.09

5.3 ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับอยู่ในระดับใด (5,4,3,2,1)

ตารางที่ 4.47 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับระดับความคิดเห็นถึงการยอมรับของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ลำดับ	ผู้ประเมิน	ระดับ	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	4	
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	3	ให้ดูข้อเสนอแนะ/ข้อคิดเห็นในส่วนที่ 3

ตารางที่ 4.47 (ต่อ)

ลำดับ	ผู้ประเมิน	ระดับ	ข้อเสนอแนะ/ข้อคิดเห็น
3	ดร.มงคล กลิ่นกระจาย	5	สามารถยอมรับได้ เนื่องจากมีการแบ่งตัวชี้วัดในแต่ละระดับ โดยมีการเน้นตัวชี้วัดเฉพาะของแต่ละมิติออกมาชัดเจน
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	5	
5	ดร.ชาลี วรกุลพิพัฒ์	4	เห็นด้วย เหตุผลด้วยกันครับข้อที่แล้ว
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์		เสนอให้ปรับข้อความบางส่วนให้มีความชัดเจนมากยิ่งขึ้น
7	ผศ.ดร.อัศฆ์เดช วานิชชินชัย		มีความเหมาะสมเบื้องต้น ควรนำไปทำการทดสอบเชิงประจักษ์จริง
8	ดร.ศักดิ์ เสกขุนทด		เหมาะสม
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	3	ปรับแก้ตามข้อ2
10	ผศ.ดร.ณฐพร อุตกฤษฎ์	4	ยอมรับได้แต่ควรเพิ่มเติมตามที่แนะนำไป
11	คุณนพพร เทพสิทธา	5	รายละเอียดคลอบคลุม โดยจุดสำคัญอยู่ที่การอธิบายให้ผู้ประกอบการได้เข้าใจและนำไปใช้การประเมินธุรกิจของตนเองอย่างจริงจัง
12	คุณสุเมธ อักษรกิตติ์	4	
13	ดร.อดิศักดิ์ ศรีนครินทร์		เหมาะสม
14	คุณทัชนันท์ กังวานตระกูล	4	
15	ดร.มนู อรดีดลเชษฐ์		เหมาะสม
ค่าเฉลี่ยของระดับการยอมรับ		**4.10**	

ดังนั้นจากระดับความเหมาะสมของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับที่ระดับมาก โดยค่าเฉลี่ยที่ได้มีค่าอยู่ที่ 4.10

4.4.1 ผลการวิเคราะห์เพื่อตอบข้อสมมติฐานการวิจัย (ข้อ 7-8)

ข้อที่	สมมติฐาน	ผลการทดสอบ
7	ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีระดับความเหมาะสมอยู่ในระดับมาก	ยอมรับสมมติฐาน
8	ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีระดับการยอมรับอยู่ในระดับมาก	ยอมรับสมมติฐาน

5.4 ข้อเสนอแนะโดยรวมต่อสิ่งที่ควรปรับปรุงใน ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ตารางที่ 4.48 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับระดับความคิดเห็นถึงข้อเสนอแนะของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	ความชัดเจนของพัฒนา Model ด้วย tools อะไร และควรจะต้องมีการ prove โดย users
2	ผศ.ดร.ประณต บุญไชยอภิสิทธิ์	ให้ดูข้อเสนอแนะ/ข้อคิดเห็นในส่วนที่ 3
3	ดร.มงคล กลิ่นกระจาย	ควรมีการยกตัวอย่าง อย่างน้อย 1 มิติ ในแต่ละระดับ
4	รศ.ดร.เรืองศักดิ์ แก้วธรรมชัย	-
5	ดร.ชาลี วรกุลพิพัฒ์	ควรศึกษาร่วมกับ CMMI ให้ลงลึก และศึกษา Data Governance Maturity Model ของ DGA
6	คุณยิ่งศักดิ์ ศรีสุขสวัสดิ์	ข้อเสนอแนะคือควรปรับปรุงคำให้มีความหมายชัดเจนยิ่งขึ้น
7	ผศ.ดร.อัศม์เดช วานิชชินชัย	มีความเหมาะสม ทั้งนี้อาจจะเขียนนิยามของ Level ต่างๆ พร้อมยกตัวอย่างให้ชัดเจนมากขึ้น

ตารางที่ 4.48 (ต่อ)

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
8	ดร.ศักดิ์ เสกขุนทด	ขอให้เพิ่มเรื่อง Data Governance
9	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	ต้องไปเทียบกับตัวอื่นมาก่อน
10	ผศ.ดร.ณฐพร อุตกฤษฎ์	ทำให้เกิดความชัดเจนและความแตกต่างจากของที่มีอยู่และการนำไปใช้งาน
11	คุณนพพร เทพสิทธา	1. แยกให้ชัดเจนระหว่าง Cyber Business Resilience และ Cyber Supply Chain Resilience 2. ทำให้ผู้ประกอบตระหนัก เข้าใจ และสามารถประเมินตนเอง เพื่อจะนำไปพัฒนาต่อยอดธุรกิจของตนเองได้อย่างสะดวก (Simplification)
12	คุณสุเมธ อักษรกิตติ์	ดี และลอง Update ISO 22301 : 2019 ว่ามีการเปลี่ยนแปลง แตกต่างจาก ISO 22301 : 2012 อย่างไรบ้าง
13	ดร.อดิศักดิ์ ศรีนครินทร์	-
14	คุณทัชนันท์ กังวานตระกูล	1. การจัดข้อมูลให้เป็น diagram เพื่อให้เข้าใจง่าย 2. นิยาม ตัวชี้วัด ให้มีความสอดคล้อง และมี keywords 3. การกำหนดหลักเกณฑ์การตัดสินใจว่า จะผ่าน ML ระดับใด โดยมีข้อพิจารณาหรือบ่งชี้อะไรได้บ้าง ให้ความยืดหยุ่นทาง model
15	ดร.มนู อรดีดลเชษฐ์	1. ควรมองในลักษณะของ Extra Success 2. งานที่ทำจะเหมาะกับ SME หรือไม่ ให้ไปลองพิจารณาดูอีกที หรือมองในมุมที่จะเหมาะกับ SME ต่อไป

5.5 ข้อเสนอแนะต่อปัจจัยความสำเร็จของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม (Digital SME Business)

ตารางที่ 4.49 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับข้อเสนอแนะต่อปัจจัยความสำเร็จของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	คุณนพพร เทพสิทธา	1. สร้างความสามารถในการวางแผนและ Strategic Thinking 2. มองสภาพแวดล้อมให้ออกว่าเป็น Opportunity หรือ Threat 3. Transform ตนเองสู่ Digital Transformation และพัฒนาตนเองสู่ Global Supply Chain Management

5.6 ข้อเสนอแนะต่อการคืนสภาพได้อย่างยั่งยืนของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม (Sustainable Resilient Digital SME Business)

ตารางที่ 4.50 ผลการสัมภาษณ์ผู้เชี่ยวชาญสำหรับข้อเสนอแนะต่อการคืนสภาพได้อย่างยั่งยืนของวิสาหกิจดิจิทัลขนาดกลางและขนาดย่อม

ลำดับ	ผู้ประเมิน	ข้อเสนอแนะ/ข้อคิดเห็น
1	คุณนพพร เทพสิทธา	Data Management สู่ Big Data และใช้ IoT/AI เป็นหัวใจ โดยจะต้องเตรียมพร้อมเพื่อให้ปรับตัว ให้เข้าใจ และค่อยๆ พัฒนาตนเองสู่ Digital Transformation หาก Data ไม่สมบูรณ์ ถูกต้อง รวดเร็ว ก็ไม่มีทางที่จะทำ Resilience ได้ดี

6. ประเด็นแนะนำเพิ่มเติมจากผู้เชี่ยวชาญ

ตารางที่ 4.51 ประเด็นข้อแนะนำเพิ่มที่ได้จากการสัมภาษณ์ผู้เชี่ยวชาญที่มีการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ลำดับ	ผู้ประเมิน	ประเด็น/ข้อแนะนำ
1	ดร.พิลาศพงษ์ ทรัพย์เสริมศรี	1. ประเด็นของ Security ต้องพิจารณาให้ลึกลงไปในงาน ในแต่ละ transaction ที่เกิดขึ้นภายใต้กิจกรรมทางด้านโลจิสติกส์และโซ่อุปทานดิจิทัล
		2. ควรจะพิจารณาไปตามกลุ่มอุตสาหกรรมของ SME เพราะถ้าทำรวมทั้งหมดใน SME ตัวแบบที่พัฒนาอาจจะไม่สามารถตอบโจทย์ได้อย่างแท้จริง
		3. ในมุมมองของท่านอาจารย์มองว่าเรื่องSecurity เป็นเรื่องของการจัดความต่อเนื่องของภาคธุรกิจ (Continuity) ได้เพราะปัจจุบันเทคโนโลยีได้เข้ามาบทบาทต่อการดำเนินงานในภาคธุรกิจมากขึ้น ทุกอย่างทำงานได้อย่างอัตโนมัติ (Automation) มากขึ้น 4. ในปัจจุบันงานทุกอย่างต้องเข้าไปเกี่ยวข้องกับความมั่นคงปลอดภัย (Security) มากขึ้น อย่างเช่น Smart distribution center ที่แจ๊คหม่าได้นำมาใช้งานนั้นสามารถทำให้ธุรกิจอาลีบาบา สามารถส่งของได้ทั่วโลก Security จึงเข้ามามีบทบาทเป็นอย่างมาก
		5. อาจารย์ท่านเป็นห่วงว่า แนวคิดในการทำงานวิจัยจะไม่สามารถเป็น General ได้ ควรจะ Specific หรือให้เกิดชำนาญและเชี่ยวชาญเฉพาะด้านเฉพาะกลุ่ม Industry ไปเลย

ตารางที่ 4.51 (ต่อ)

ลำดับ	ผู้ประเมิน	ประเด็น/ข้อแนะนำ
		6. คำแนะนำเล็กๆ น้อยๆ สำหรับการจะส่งบทความต่างประเทศ ถ้างานนั้นเป็นงานที่ทำเฉพาะในประเทศไทย หรือเป็นสินค้าของประเทศนั้นๆ มาดำเนินการและจัดการในประเทศไทย บทความจะมีความสนใจเป็นอย่างมาก เพราะว่า ถ้าเป็นเรื่องที่กว้างๆ อาจารย์ท่านบอกว่า peer review ทั้งหลายเค้าอ่านบทความมาเยอะ เค้าอาจจะมองว่างานของเราก็ซ้ำๆ กับที่ผ่านๆ มาจะทำให้ไม่เป็นที่สนใจต่อ peer review เหล่านั้นและอาจจะตีงานให้ตกได้
		7. เมื่อได้ Software หรือ Application ควรนำไปปฏิบัติสำหรับใช้งานจริงๆ โดยทดลองกับบริษัทบางบริษัทเพื่อให้ได้ผลตอบรับกลับมาเกี่ยวกับงานที่เราจะทำให้วิทยานิพนธ์มีความน่าเชื่อถือมากขึ้น
2	ดร.ชาลี วรกุลพิพัฒ์	1. ต้องชี้ให้เห็นถึงข้อแตกต่างระหว่าง Cyber Resilience , BCP , DRP ให้ชัด โดยจะต้องแม่นในแนวคิดต่างๆ เหล่านี้
		2. ต้องทำการ Validate กรอบแนวคิดที่เพิ่มขึ้น (สีเหลือง) ซึ่งอาจจะมาจากการทำ Review Literature และ/หรือ จากการ Survey ที่อาจจะมาจากการ Interview, questionaire, field test
		3. อาจจะต้องมีการเตรียมทำ slide เพิ่มเติมไว้อธิบายกรรมการตอน defense ในเรื่องของ AI , Privacy ที่อาจจะไม่เกี่ยวข้องกับเรื่องที่ศึกษาเลยก็เป็นได้
		4. อาจารย์อธิบายถึงหลักการของ Respond ว่าจะต้องทำให้ถูกคน และถูกเวลา โดยการ respond ก็สามารถทำได้ด้วยทั้งระบบ IT หรือผ่านสื่อต่างๆ ได้

ตารางที่ 4.51 (ต่อ)

ลำดับ	ผู้ประเมิน	ประเด็น/ข้อแนะนำ
		5. อาจารย์ท่านอยากให้พูดถึงประเด็นในการวิเคราะห์ความเสี่ยงให้มีความเข้าใจมากขึ้น ให้เข้าใจในความสำคัญของการวิเคราะห์ความเสี่ยงในส่วนงานต่างๆ ว่าทำไมถึงต้องไม่เท่ากันในแต่ละส่วนงาน และแนวทางในการแก้ปัญหาที่เกิดขึ้น จากการวิเคราะห์ความเสี่ยง ที่ทำให้เราทราบว่า งานส่วนไหนสำคัญมากน้อยแค่ไหน เมื่อเกิดปัญหาจะได้มีแนวทางในการแก้ปัญหาในส่วนงานที่สำคัญมากกว่าก่อน ตามลำดับลงไป
		6. แนะนำให้ศึกษาเพิ่มเติมเกี่ยวกับ แนวคิดของ Robust โดยอาจาย์ให้หลักการ ACID สำหรับระบบฐานข้อมูล
		7. แนวทางสำหรับการประเมินตัวแบบ อาจารย์แนะนำ ISM-Benchmark
		8. แนะนำให้ศึกษาเรื่อง Data Governance
		9. อาจารย์บอกว่า การทำ Self Assessment ถึงว่าเป็นสุดยอดของสุดยอดในเรื่องของการประเมิน เพราะถ้าสามารถผลักดันให้ทุกองค์กรสามารถทำการประเมินตนเองได้นั้นจะเป็นเรื่องที่ดีที่สุด
3	ดร.อดิศักดิ์ ศรีนครินทร์	1. งานที่ทำควรจะต้องหาให้ได้ว่า เคยมี tools หรือ mechanism อะไรบ้างที่ทำไว้ก่อนหน้า และงานที่ทำจะมีการพัฒนา tools และ mechnism อย่างไร
4	ดร.ศักดิ์ เสกขุนทด	1. ความสำคัญของงาน logistics ในปัจจุบันคือ ต้องมีเรื่อง traceability
		2. Data Security ก็มีส่วนสำคัญ โดยเฉพาะความสำคัญในส่วนของ Data Security Sharing

ตารางที่ 4.51 (ต่อ)

ลำดับ	ผู้ประเมิน	ประเด็น/ข้อแนะนำ
		3. ท่านให้ศึกษาถึงความสำคัญของ identity management เพราะจะมีความสำคัญต่อกระบวนการสำหรับงานด้าน security
		4. ศึกษาความเสี่ยงจากการเกิดขึ้นของเทคโนโลยีใหม่ๆ ท่ะจมีผลต่อการดำเนินธุรกรรมในปัจจุบัน เช่น Blockchain, IoT, Big data
		5. แนวทางในอนาคตเอกสารต่างๆ จะเป็น digital ทั้งหมด ดังนั้นความสำคัญในเรื่องของ digital document security จึงเป็นอีกสิ่งที่ต้องคำนึงถึง
		6. แนวทางในการจัดการข้อมูลส่วนบุคคลPrivacy ก็จะเป็นประเด็นสำคัญต่อการรักษาความมั่นคงปลอดภัยด้วยเช่นเดียวกัน ซึ่งโดยปกติแล้วPrivacy กับSecurity จะสวนทางกันจะทำอย่างไรที่จะทำให้2สิ่งนี้Balanceกันได้
5	รศ.ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ	1. ตัวชี้วัดที่พัฒนาขึ้นมานั้น ต้องชี้ให้ได้ว่า ตัวใดเพิ่มขึ้นมา ตัวใดเป็นการ Adapt จากสิ่งที่มีอยู่ และถ้า Adapt มาแล้วนั้นให้บอกถึงแหล่งที่มาให้ได้ว่าอ้างอิงมาจากไหน
		2. Maturity ทั้ง 5 Level ต้องบอกให้ได้ว่า เอามาจากไหน
		3. ตัวชี้วัดที่เพิ่มเติมเข้ามา ควรทำตารางให้ชัดเจนเลยว่า เป็นการเพิ่มเข้ามา
		4. การพัฒนา MIL ให้สามารถบอกถึงแหล่งอ้างอิงให้ได้ว่าพัฒนามาจากไหน
		5. ตัวชี้วัด ประเด็นพิจารณาร่วมกัน เ ช่นในข้อ 128 "บริษัทมีการจัดสรรงบประมาณที่เพียงพอ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ครอบคลุมถึงระบบงาน

ตารางที่ 4.51 (ต่อ)

ลำดับ	ผู้ประเมิน	ประเด็น/ข้อแนะนำ
		(Application) ข้อมูล (information) โครงสร้างพื้นฐาน (Infrastructure) รวมทั้งบุคลากร เครื่องมือและบริการที่เกี่ยวข้อง" ควรจะแบ่งเป็นข้อย่อยๆ ดีหรือไม่ เพราะการตอบต้องเลือกตอบแต่ถ้าบางตัวมี บางตัวไม่มี จะทำให้ผู้ตอบสับสนได้ว่าควรจะตอบอย่างไร
		6. ในตัวชี้วัดที่มีคำว่า และ/หรือ ควรเช็คดูให้ดีว่าจะทำให้ผู้ตอบทำการตอบแบบประเมินยากหรือไม่
		7. ต้องสร้างตารางที่อธิบายให้ชัดเจนว่า ตัวชี้วัดแต่ละตัวมีที่มา หรืออ้างอิงจากข้อมูลจากแหล่งใด
6	รศ.ดร.สุดสงวน งามสุริยโรจน์	1. ตัวชี้วัดในแต่ละตัว จะต้องสามารถระบุได้ว่าควรอยู่ใน level ที่เท่าไหร่
		2. การกำหนดเกณฑ์ เป็นเรื่อง Serious ควรจะต้องบอกได้ว่า minimum requirement ควรอยู่ตรงไหน

4.4.2 ผลการวิเคราะห์ข้อมูลด้วยการวิเคราะห์เชิงเนื้อหา

ข้อมูลที่ได้รับการจากการสัมภาษณ์ ผู้วิจัยได้รับความอนุเคราะห์ข้อมูลจากผู้เชี่ยวชาญ จากกลุ่มสาขา 4 กลุ่มสาขา ได้แก่ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จำนวน 4 ท่าน ด้านตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model: CMM) จำนวน 4 ท่าน ด้านเทคโนโลยีดิจิทัล (Digital Technology) จำนวน 5 ท่าน และด้านโลจิสติกส์และโซ่อุปทานดิจิทัล จำนวน 4 ท่าน รวมจำนวนผู้เชี่ยวชาญทั้งสิ้น 17 ท่าน โดยมีวัตถุประสงค์เพื่อตรวจสอบตัวแบบ ตัวชี้วัด รวมไปถึงเกณฑ์ที่จะนำมาใช้ในการประเมินระบบระดับวุฒิภาวะความสามารถการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อมว่าเป็นไปตามที่ได้ศึกษาหรือไม่ และเพื่อรับทราบถึงประสบการณ์ ตลอดจนแนวปฏิบัติในการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ ในบริบทของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อมต่อไป

ผู้วิจัยได้นำผลการสัมภาษณ์ของผู้เชี่ยวชาญทั้งหมดไปทำการตรวจสอบความเหมาะสมและความสอดคล้อง จากผู้เชี่ยวชาญทั้ง 4 กลุ่มสาขา เพื่อวินิจฉัยถึงความเหมาะสมของแนวทางของตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล และเกณฑ์ในการประเมินระดับวุฒิภาวะที่ได้พัฒนาขึ้น โดยผู้เชี่ยวชาญทั้ง 4 กลุ่มสาขา ผู้วิจัยได้ทำการแบ่งกลุ่มความเชี่ยวชาญไว้ดังต่อไปนี้

1. ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์นั้นคัดเลือกมาจากผู้ทรงคุณวุฒิที่มีประสบการณ์ และมีบทบาทสำคัญในการกำหนดนโยบาย รวมถึงการกำหนด ทิศทางการเติบโตของการรักษาความมั่นคงปลอดภัยในระดับประเทศ

2. ผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ ที่คัดเลือกจากผู้ทรงคุณวุฒิที่มีประสบการณ์ด้านการจัดทำมาตรฐาน และประเมินระดับวุฒิภาวะความสามารถให้กับองค์กรต่าง ๆ โดยผู้เชี่ยวชาญในกลุ่มที่ 1 และ 2 นี้จะได้ช่วยพิจารณาถึงความสอดคล้องต่อแนวทางในการพัฒนาต่อมุมมองทางด้านการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลหรือไม่

3. ผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล คัดเลือกจากผู้ทรงคุณวุฒิที่มีความประสบการณ์และความเชี่ยวชาญต่อเทคโนโลยีที่มีการเปลี่ยนแปลงไปในโลกปัจจุบัน ซึ่งผู้เชี่ยวชาญกลุ่มนี้จะช่วยพิจารณาถึงความสอดคล้องต่อแนวทางในการพัฒนาว่ามีความเหมาะสมและสอดคล้องต่อบริบทของการเป็นโซ่อุปทานดิจิทัลหรือไม่

4. ผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทานดิจิทัล ผู้เชี่ยวชาญกลุ่มนี้จะช่วยพิจารณาความสอดคล้องของแนวทางที่พัฒนาขึ้นว่ามีความสอดคล้องต่อหลักการในการจัดการโลจิสติกส์และซ่อุปทานดิจิทัลหรือไม่

โดยหากผู้เชี่ยวชาญเห็นด้วยกับแนวทางในการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์ในการประเมินที่ผู้วิจัยได้นำเสนอ จะทำเครื่องหมาย ✓ เมื่อผู้เชี่ยวชาญไม่เห็นด้วยผู้วิจัยจะใช้เครื่องหมาย ✗ ผลการศึกษาดังตารางที่ 4.52 – 4.55

ตารางที่ 4.52 ผลการวินิจฉัยความสอดคล้องและเหมาะสมของแนวทางการกำหนดตัวแบบตัวชี้วัดวุฒิภาวะความสามารถและเกณฑ์การประเมิน จากผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ

ความสอดคล้องของแนวทางในการกำหนดตัวแบบ ตัวชี้วัดระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมินสำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
1. แนวทางการกำหนดกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
2. แนวทางการกำหนดตัวชี้วัดของกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
4. แนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓

ข้อเสนอแนะเพิ่มเติม

1. ควรจะมีวิธีการในการแสดงความสัมพันธ์ระหว่าง 6 หมวด 32 มิติ ให้ชัดเจนมากกว่านี้
2. งานที่ทำได้ครอบคลุมเรื่อง กระบวนการ (process) คน (people) และเครื่องมือ (Tools & Equipment)
3. เป็นไปได้หรือไม่ที่ยุบรวม category ที่สัมพันธ์กันค่อนข้างมาก เช่น Risk Assessment, Risk Management Strategy, Supply Chain Risk Management
4. การที่เรียก MIL 1-10 ว่า เป็นตัวชี้วัด ไม่น่าจะถูก เพราะไม่มีลักษณะเป็นตัวชี้วัด (เป็นนามธรรม) และไม่เห็นความสัมพันธ์ระหว่าง 32 มิติ 142 ตัวชี้วัด ในแต่ละ MIL
5. เกณฑ์การให้คะแนน (Answer) รวมถึงค่าน้ำหนัก (Weighted Factor) 1-5 มีหลักเกณฑ์อย่างไร เป็น Subjective หรือ Objective
6. การอธิบายลักษณะของ Maturity Model ควรที่จะอธิบายด้วยรูปภาพเพื่อความเข้าใจของผู้อื่นที่จะศึกษางานได้เข้าใจได้ง่ายขึ้น
7. ผลของการศึกษาวิจัยควรมองในลักษณะของ Extra Success ผลที่เกิดขึ้นที่จะเป็นประโยชน์กับ SME จริง ๆ
8. งานที่ทำจะเหมาะกับSMEหรือไม่ ให้ไปลองพิจารณาดูอีกที หรือมองในมุมที่จะเหมาะกับSMEต่อไป

ตารางที่ 4.53 ผลการวินิจฉัยความสอดคล้องและเหมาะสมของแนวทางการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน จากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ความสอดคล้องของแนวทางในการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน สำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านตัวความมั่นคงปลอดภัยไซเบอร์			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
1. แนวทางการกำหนดกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
2. แนวทางการกำหนดตัวชี้วัดของกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
4. แนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓

ข้อเสนอแนะเพิ่มเติม

1. ต้องชี้ให้เห็นถึงข้อแตกต่างระหว่าง Cyber Resilience , BCP , DRP ให้ชัด โดยจะต้องแม่นในแนวคิดต่างๆ เหล่านี้
2. ต้องทำการ Validate กรอบแนวคิดที่เพิ่มขึ้น (สีเหลือง) ซึ่งอาจจะมาจากการทำ Review Literature และ/หรือ จากการ Survey ที่อาจจะมาจากการ Interview, Questionaire, Field Test
3. อาจจะต้องมีการเตรียมทำ Slide เพิ่มเติมไว้อธิบายกรรมการตอน Defense ในเรื่องของ AI , Privacy ที่อาจจะไม่เกี่ยวข้องกับเรื่องที่ศึกษาเลยก็เป็นได้
4. หลักการของ Respond ควรจะต้องทำให้ถูกคน และถูกเวลา โดยการ Respond ก็สามารถทำได้ด้วยทั้งระบบ IT หรือผ่านสื่อต่าง ๆ ได้
5. ควรอธิบายถึงประเด็นในการวิเคราะห์ความเสี่ยงให้มีความเข้าใจมากขึ้น ให้เข้าใจในความสำคัญของการวิเคราะห์ความเสี่ยง ในส่วนงานต่าง ๆ ว่าทำไมถึงต้องไม่เท่ากันในแต่ละส่วนงาน และแนวทางในการแก้ปัญหาที่เกิดขึ้น จากการวิเคราะห์ความเสี่ยง ที่ทำให้เราทราบว่า งานส่วนไหนสำคัญมากน้อยแค่ไหน เมื่อเกิดปัญหาจะได้มีแนวทางใน

ตารางที่ 4.53 (ต่อ)

ข้อเสนอแนะเพิ่มเติม

การแก้ปัญหาในส่วนงานที่สำคัญมากกว่าก่อน ตามลำดับลงไป

6. ศึกษาเพิ่มเติมเกี่ยวกับ แนวคิดของ Robust ด้วยหลักการ ACID สำหรับระบบฐานข้อมูล
7. ศึกษาแนวทางสำหรับการประเมินตัวแบบ โดยเฉพาะในเรื่อง ISM-Benchmark
8. ศึกษาเพิ่มเติมในประเด็นของ Data Governance
9. การทำ Self Assessment ถึงว่าเป็นสุดยอดของสุดยอดในเรื่องของการประเมิน เพราะถ้าสามารถผลักดันให้ทุกองค์กรสามารถทำการประเมินตนเองได้นั้นจะเป็นเรื่องที่ดีที่สุด
10. Data Security ก็มีส่วนสำคัญ โดยเฉพาะความสำคัญในส่วนของ Data Security Sharing
11. ศึกษาถึงความสำคัญของ Identity Management เพราะจะมีความสำคัญต่อกระบวนการสำหรับงานด้าน Security
12. ศึกษาความเสี่ยงจากการเกิดขึ้นของเทคโนโลยีใหม่ๆ ที่จะมีผลต่อการดำเนินธุรกรรมในปัจจุบันเช่น Blockchain, IoT, Big data
13. แนวทางในอนาคตเอกสารต่าง ๆ จะเป็น Digital ทั้งหมด ดังนั้นความสำคัญในเรื่องของ Digital Document Security จึงเป็นอีกสิ่งที่ต้องคำนึงถึง
14. แนวทางในการจัดการข้อมูลส่วนบุคคล Privacy ก็จะเป็นประเด็นสำคัญต่อการรักษาความมั่นคงปลอดภัยด้วยเช่นเดียวกัน ซึ่งโดยปกติแล้ว Privacy กับ Security จะสวนทางกัน จะทำอย่างไรที่จะทำให้ 2 สิ่งนี้ Balance กันได้
15. ตัวชี้วัดที่พัฒนาขึ้นมานั้น ต้องชี้ให้ได้ว่า ตัวใดเพิ่มขึ้นมา ตัวใดเป็นการ Adapt จากสิ่งที่มีอยู่ และถ้า Adapt มาแล้วนั้นให้บอกถึงแหล่งที่มาให้ได้ว่าอ้างอิงมาจากไหน
16. ตัวชี้วัดในแต่ละตัว จะต้องสามารถระบุได้ว่าควรอยู่ใน Level ที่เท่าไหร่
17. การกำหนดเกณฑ์ เป็นเรื่อง Serious ควรจะต้องบอกได้ว่า Minimum Requirement ควรอยู่ตรงไหน

ตารางที่ 4.54 ผลการวินิจฉัยความสอดคล้องและเหมาะสมของแนวทางการกำหนดตัวแบบตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน จากผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล

ความสอดคล้องของแนวทางในการกำหนดกรอบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน สำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล				
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4	ท่านที่ 5
1. แนวทางการกำหนดกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓	✓
2. แนวทางการกำหนดตัวชี้วัดของกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓	✓
3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓	✓
4. แนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓	✓

ข้อเสนอแนะเพิ่มเติม

1. Maturity ทั้ง 5 Level ต้องบอกให้ได้ว่า เอามาจากไหน
2. ตัวชี้วัดที่เพิ่มเติมเข้ามา ควรทำตารางให้ชัดเจนเลยว่า เป็นการเพิ่มเข้ามา
3. การพัฒนา MIL ให้สามารถบอกถึงแหล่งอ้างอิงให้ได้ว่าพัฒนามาจากไหน
4. ตัวชี้วัด ประเด็นพิจารณาร่วมกัน เช่นในข้อ 128 “บริษัทมีการจัดสรรงบประมาณที่เพียงพอในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ครอบคลุมถึงระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐาน (Infrastructure) รวมทั้งบุคลากร เครื่องมือและบริการที่เกี่ยวข้อง” ควรจะแบ่งเป็นข้อย่อย ดีหรือไม่ เพราะการตอบต้องเลือกตอบแต่ถ้าบางตัวมี บางตัวไม่มี จะทำให้ผู้ตอบสับสนได้ว่าควรจะตอบอย่างไร
5. ในตัวชี้วัดที่มีคำว่า และ/หรือ ควรเช็คดูให้ดีว่าจะทำให้ผู้ตอบทำการตอบแบบประเมินยากหรือไม่

ตารางที่ 4.54 (ต่อ)

ข้อเสนอแนะเพิ่มเติม

6. ต้องสร้างตารางที่อธิบายให้ชัดเจนว่า ตัวชี้วัดแต่ละตัวมีที่มา หรืออ้างอิงจากข้อมูลจากแหล่งใด
7. เกณฑ์การให้คะแนนเป็นอย่างไร ควรจะระบุให้ชัดเจนว่าเป็น Subjective หรือ Objective
8. ตัวชี้วัด (KPI) ควรเป็นรูปธรรม และเห็นได้ชัดเจน เช่น จะวัดแบบไหนด้วยผลลัพธ์อย่างไร (Action Plan)
9. ควรจะศึกษาในประเด็นของ Business Continuity Strategy and Solutions ให้มากยิ่งขึ้น
10. ให้ศึกษาถึง ISO 22301 : 2019 Business Continuity Management (Oct 2019)
11. ศึกษาในเรื่อง Reactive Supply Chain Management และ Dynamic Supply Chain Flexibility เพิ่มเติม
12. ควรมีการจัดทำ Matrix Assessment และ Meta Synthesis เพื่อใช้เปรียบเทียบ the generic standard กับตัวที่ผู้วิจัยนำเสนอ เพื่อให้ชัดเจนถึงวัตถุประสงค์การนำไปใช้ที่แตกต่าง
13. ควรจัดทำ ทำ Matrix Assessment โดยใช้รูปแบบแนวคิด Risk Management มาประยุกต์
14. ข้อ Assessment รายย่อยบางข้อที่ยังคลุมเครือ ไม่ชัดเจนในการกำหนดระดับวุฒิภาวะ ควรมีการจำแนก should/have to/must เพื่อใช้ในการกำหนดกรอบให้ชัดเจน
15. ควรจะต้องหาให้ได้ว่า เคยมี tools หรือ mechanism อะไรบ้างที่ทำไว้ก่อนหน้า และงานที่ทำจะมีการพัฒนา tools และ mechnism อย่างไร

ตารางที่ 4.55 ผลการวินิจฉัยความสอดคล้องและเหมาะสมของแนวทางการกำหนดตัวแบบตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน จากผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทานดิจิทัล

ความสอดคล้องของแนวทางในการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน สำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทานดิจิทัล			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
1. แนวทางการกำหนดกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓

ตารางที่ 4.55 (ต่อ)

ความสอดคล้องของแนวทางในการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมิน สำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทาน			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
2. แนวทางการกำหนดตัวชี้วัดของกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
3. แนวทางการกำหนดระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
4. แนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	✓	✓	✓	✓
ข้อเสนอแนะเพิ่มเติม 1. ประเด็นของ Security ต้องพิจารณาให้ลึกลงไปในงาน ในแต่ละ Transaction ที่เกิดขึ้นภายใต้กิจกรรมทางด้านโลจิสติกส์และโซ่อุปทานดิจิทัล 2. ควรจะพิจารณาไปตามกลุ่มอุตสาหกรรมของ SME เพราะถ้าทำรวมทั้งหมดใน SME ตัวแบบที่พัฒนาอาจจะไม่สามารถตอบโจทย์ได้อย่างแท้จริง 3. ปัจจุบันไม่อาจปฏิเสธได้ว่า เรื่อง Security เป็นเรื่องของการจัดความต่อเนื่องของภาคธุรกิจ (Continuity) ได้ เพราะปัจจุบันเทคโนโลยีได้เข้ามาบทบาทต่อการดำเนินงานในภาคธุรกิจมากขึ้น ทุกอย่างทำงานได้อย่างอัตโนมัติ (Automation) มากขึ้น 4. ความสำคัญของงาน Logistics ในปัจจุบันคือ ต้องมีเรื่อง Traceability 5. ในปัจจุบันงานทุกอย่างต้องเข้าไปเกี่ยวข้องกับความมั่นคงปลอดภัย (Security) มากขึ้น อย่างเช่น Smart Distribution Center ที่แจ๊คหม่าได้นำมาใช้งานนั้นสามารถทำให้ธุรกิจอาลีบาบา สามารถส่งของได้ทั่วโลก Security จึงเข้ามามีบทบาทเป็นอย่างมาก 6. แนวคิดในการทำงานวิจัยจะไม่สามารถเป็น General ได้ การทำวิจัยควรจะ Specific หรือให้เกิดชำนาญและเชี่ยวชาญเฉพาะด้าน เฉพาะกลุ่ม Industry				

ตารางที่ 4.55 (ต่อ)

ข้อเสนอแนะเพิ่มเติม
7. การจะส่งบทความต่างประเทศ ถ้างานนั้นเป็นงานที่ทำเฉพาะในประเทศไทย หรือเป็นสินค้าของประเทศนั้น ๆ มาดำเนินการและจัดการในประเทศไทย บทความจะมีความสนใจเป็นอย่างมาก เพราะว่า ถ้าเป็นเรื่องที่กว้างๆ อาจารย์ท่านบอกว่า Peer Review ทั้งหลาย เค้าอ่านบทความมาเยอะ เค้าอาจจะมองว่างานของเราก็ซ้ำ ๆ กับที่ผ่าน ๆ มาจะทำให้ไม่เป็นที่สนใจต่อ Peer Review เหล่านั้นและอาจจะตีงานให้ตกได้
8. เมื่อได้ Software หรือ Application ควรนำไปปฏิบัติสำหรับใช้งานจริง ๆ โดยทดลองกับบริษัทบางบริษัทเพื่อให้ได้ผลตอบรับกลับมาเกี่ยวกับงานที่เรา จะทำให้วิทยานิพนธ์มีความน่าเชื่อถือมากขึ้น

ผลการสอบถามถึงระดับความคิดเห็นโดยรวมต่อตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยพิจารณาถึงความเหมาะสมและการยอมรับของกรอบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล โดยหากผู้เชี่ยวชาญเห็นด้วยกับแนวทางในการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ที่ผู้วิจัยได้นำเสนอว่ามีความเหมาะสมจะทำเครื่องหมาย ✓ เมื่อผู้เชี่ยวชาญไม่เห็นด้วยผู้วิจัยจะใช้เครื่องหมาย ✗ ผลการศึกษาแสดงได้ดังในตารางที่ 4.56 – 4.59

ตารางที่ 4.56 ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล จากผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ

ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีความเหมาะสมหรือไม่	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับความเหมาะสมหรือไม่	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับหรือไม่	✓	✓	✓	✓

ตารางที่ 4.57 ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล จากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีความเหมาะสมหรือไม่	✓	✓	✓	✓

ตารางที่ 4.57 (ต่อ)

ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับความเหมาะสมหรือไม่	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับหรือไม่	✓	✓	✓	✓

ตารางที่ 4.58 ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล จากผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล

ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล				
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4	ท่านที่ 5
การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลมีความเหมาะสมหรือไม่	✓	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับความเหมาะสมหรือไม่	✓	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับหรือไม่	✓	✓	✓	✓	✓

ตารางที่ 4.59 ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของตัวแบบและระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล จากผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทานดิจิทัล

ระดับความคิดเห็นโดยรวมต่อความเหมาะสมของกรอบและระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล	ผู้เชี่ยวชาญด้านโลจิสติกส์และโซ่อุปทาน			
	ท่านที่ 1	ท่านที่ 2	ท่านที่ 3	ท่านที่ 4
การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีความเหมาะสมหรือไม่	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับความเหมาะสมหรือไม่	✓	✓	✓	✓
ตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล มีระดับการยอมรับหรือไม่	✓	✓	✓	✓

จากการสัมภาษณ์ ผลการวินิจฉัยความสอดคล้องและระดับความคิดเห็นโดยรวมต่อเหมาะสมของแนวทางการกำหนดตัวแบบการคืนสภาพได้ ตัวชี้วัด ระดับวุฒิภาวะความสามารถและเกณฑ์การประเมินที่ผู้วิจัยได้นำเสนอในการศึกษาในครั้งนี้ ทำให้ผู้วิจัยสามารถสรุปได้ว่า ตัวแบบการคืนสภาพได้ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์การประเมินสำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ที่ผ่านกระบวนการวิเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึก รวมถึงการตรวจสอบความเหมาะสมและความสอดคล้องจากผู้เชี่ยวชาญด้านวุฒิภาวะความสามารถ ด้านความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีดิจิทัล และด้านโลจิสติกส์และโซ่อุปทานดิจิทัล ทำให้ผู้วิจัยสามารถยืนยันได้ถึงผลของการศึกษา ตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถ และเกณฑ์ที่ใช้ในการประเมิน สำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

4.4.3 ผลการวิเคราะห์การสนทนากลุ่ม (Focus Group)

ถึงแม้ว่าการวิเคราะห์เชิงเนื้อหาที่ได้ดำเนินการไปก่อนหน้านั้น จะเป็นการวิเคราะห์ข้อมูลเพื่อยืนยันถึงแนวทางในการกำหนดตัวแบบ ตัวชี้วัด ระดับวุฒิภาวะความสามารถและเกณฑ์ในการประเมิน วุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจ โดยผลที่ได้จากการวิเคราะห์ทำให้สามารถยืนยันได้ถึงสิ่งที่ผู้วิจัยได้นำเสนอสำหรับงานวิจัยในครั้งนี้ แต่ยังมีบางประเด็นสำหรับการศึกษาที่ยังต้องการยืนยันเพื่อให้ผลของการนำเสนอสำหรับการวิจัยนี้มีความเป็นรูปธรรมมากขึ้น ดังนั้นผู้วิจัยจึงได้ดำเนินการจัดการสนทนากลุ่มโดยได้รับความอนุเคราะห์จากผู้ทรงคุณวุฒิจำนวน 6 ท่าน เพื่อทำการตรวจสอบและยืนยันถึงแนวทางที่ผู้วิจัยได้นำเสนอสำหรับงานวิจัยในครั้งนี้ โดยผลจากการสนทนากลุ่มทำให้ได้ข้อมูลเชิงคุณภาพดังนี้

4.4.3.1 แนวทางในการยุบรวมตัวชี้วัดที่มีมากเกินไป (จาก 142 ข้อ) ที่ผู้วิจัยได้นำเสนอ จะมีผลทำให้ผู้ที่จะประเมินทำการประเมินได้อย่างไม่เบื่อหน่าย และให้ง่ายต่อผู้ประเมิน (Simplify)

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “การยุบรวมตัวชี้วัดที่มามากเกินไป จนอาจจะทำให้ผู้ประเมินเบื่อหน่าย และยากลำบากต่อผู้ประเมิน” ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า ให้คงตัวชี้วัดจำนวนเท่าเดิมไว้ก่อน เพราะผู้วิจัยเองก็ได้ดำเนินการในการทบทวนวรรณกรรมมาในระดับหนึ่ง แต่สิ่งที่อยากจะ ควรระบุให้ได้ว่าตัวชี้วัดเพิ่มเข้ามาใหม่ หรือเป็นการ Adapt จากของเดิมที่มีอยู่ และต้องอ้างอิงให้ได้ถึงที่มาของตัวชี้วัดให้ได้ กับประเด็นในตัวชี้วัดบางตัวที่ต้องมีการพิจารณาร่วมกัน ที่มีทางเลือกของตัวชี้วัดเป็นจำนวนมาก เช่น บริษัทมีการดำเนินการ A, B, และ C ถ้าผู้ประเมินพิจารณาว่าบริษัทมี A และ C แต่ไม่มี B จะทำให้ผู้ประเมินสับสนว่าควรจะต้องตอบอย่างไร แนวทางควรจะต้องแยกเป็นข้อย่อยหรือไม่ และในบางตัวชี้วัดที่มีคำว่า และ/หรือ อาจจะทำให้ผู้ประเมินสับสนได้เช่นเดียวกัน

4.4.3.2 การที่เรียก MIL 1-10 ว่า เป็นตัวชี้วัด ไม่น่าจะถูก เพราะไม่มีลักษณะเป็นตัวชี้วัด (เป็นนามธรรม) และไม่เห็นความสัมพันธ์ระหว่าง 32 มิติ 142 ตัวชี้วัด ในแต่ละ MIL

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “การที่เรียก MIL 1-10 ว่าเป็นตัวชี้วัด ไม่น่าจะถูก เพราะไม่มีลักษณะเป็นตัวชี้วัด (เป็นนามธรรม) และไม่เห็นความสัมพันธ์ระหว่าง 32 มิติ 142 ตัวชี้วัด ในแต่ละ MIL” สำหรับประเด็นนี้ผู้วิจัยได้ชี้แจงให้กับผู้ทรงคุณวุฒิทราบว่า การกำหนดตัวชี้วัด MIL 1-10 นั้น ได้อ้างอิงมาจากหลักการของ CYBERSECURITY

CAPABILITY MATURITY MODEL (C2M2) ที่ถูกพัฒนาโดย The Department of Energy (DOE) ซึ่งร่วมมือกับ Department of Homeland Security (DHS) สหรัฐอเมริกา แต่สิ่งที่ต่างกันระหว่างแนวทางของ C2M2 คือ ใน C2M2 ในทุก ๆ domain จะมีการระบุตัวชี้วัดได้ในทุกระดับ (ตั้งแต่ MIL0 – MIL3) แต่ในงานวิจัยที่ผู้วิจัยนำเสนอนี้ จะจัดระดับวุฒิภาวะความสามารถตาม Maturity Level ตามที่นำเสนอไว้ในขั้นตอนที่ 3 ของวัตถุประสงค์ข้อที่ 3 และในส่วนของความสัมพันธ์ระหว่างตัวชี้วัดกับ MIL เนื่องจากเกณฑ์ในการให้คะแนนผู้วิจัยได้มีการนำเสนอเอาไว้สำหรับตัวชี้วัดในแต่ละข้อ โดยพิจารณาตามระดับวุฒิภาวะตามภาพประกอบที่4.13 โดยรายละเอียดก็ได้อธิบายตามข้อที่ 4.3.2.3 ต่อไป ด้วยเหตุผลที่ผู้วิจัยได้นำเสนอให้กับผู้ทรงคุณวุฒิให้รับทราบ จึงทำให้ผู้ทรงคุณวุฒิสรุปร่วมกันว่า แนวทางที่ผู้วิจัยได้นำเสนอมานั้นมีความเหมาะสมทั้งในส่วนการนิยามถึง MIL และความสัมพันธ์ระหว่างตัวชี้วัด กับ MIL แต่อยากให้ตัดคำว่า “ตัวชี้วัด” ที่ปรากฏในตาราง 4.40 ออก เพราะตัวชี้วัดที่ผู้วิจัยได้นำเสนอในงานวิจัยจะเป็นตัวชี้วัดที่นำมาประเมินระดับวุฒิภาวะความสามารถฯ แล้ว ซึ่งจะทำให้สับสนได้

4.4.3.3 เกณฑ์การให้คะแนน (Answer) รวมถึงค่าน้ำหนัก (Weighted Factor) 1-5 มีหลักเกณฑ์อย่างไร เป็น Subjective หรือ Objective

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “เกณฑ์การให้คะแนน (Answer) รวมถึงค่าน้ำหนัก (Weighted Factor) 1-5 มีหลักเกณฑ์อย่างไร เป็น Subjective หรือ Objective” ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า ควรจะเป็น Subjective เพราะการประเมินเป็นแบบ Subjective คือการให้ความเห็นในมุมมองของตัวเองเป็นหลัก “ความจริง” ที่เกิดขึ้นนั้นเป็นความจริงแบบที่เจ้าตัวคนวิจารณ์ตีความ คิด หรือรู้สึก หรือพูดง่าย ๆ คือเป็นความเห็นและประสบการณ์ที่เกิดขึ้นกับตัวเอง ความเห็นลักษณะนี้ เช่น “เท่าที่ผมรู้สึกนั้น ผมว่า….” “ในมุมมองของผมนั้น ผมเห็นว่า…..” เพราะผู้วิจัยกำหนดเกณฑ์ในการประเมินตัวชี้วัดแต่ละตัวเอาไว้ตามภาพประกอบที่ 4.13 อย่างเช่นใน Level ที่ 2 ที่มีเกณฑ์ในการประเมิน 5 ข้อ คือ MIL1 – MIL5 ถ้าเกิดผู้ประเมินกำลังประเมินในตัวชี้วัดหนึ่ง ๆ ซึ่งมีแค่ 4 ข้อ (กล่าวคือ มี MIL1, MIL2, MIL4 และ MIL5) ซึ่งไม่มี MIL3 ด้วยประเด็นดังกล่าวนี้ผู้ประเมินควรจะเลือกตอบในข้อ Answer เป็น 1 หรือ 2 ทั้งนี้ก็ขึ้นอยู่กับตัวผู้ประเมิน แต่ผู้วิจัยได้นำเสนอให้กับผู้ทรงว่า ถ้าเป็นเช่นนี้จะให้ผู้ประเมินเลือกตอบ Answer = 2 แต่ยังมีค่า Weighted Factor เป็นตัวกำหนดอีกทางหนึ่ง ที่สามารถเลือกตอบค่า Weighted Factor ได้ตั้งแต่ None จนถึง Critical ซึ่งจะมีผลทำให้คำตอบของผู้ประเมินในข้อนี้มีค่าตั้งแต่ 1 จนถึง 2 ได้ เพราะระบบจะทำการ Weighted ระดับของคะแนนตามไปด้วย (จะไม่ได้ 2 เต็ม) ซึ่งเป็นผลให้ผู้ทรงคุณวุฒิ เห็นด้วยในหลักการที่ผู้วิจัยได้นำเสนอในงานวิจัยนี้

4.4.3.4 งานที่ทำจะเหมาะกับ SME หรือไม่ ให้ไปลองพิจารณาดูอีกที หรือมองในมุมที่จะเหมาะกับ SME ต่อไป

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “งานที่ทำจะเหมาะกับ SME หรือไม่ ให้ไปลองพิจารณาดูอีกที หรือมองในมุมที่จะเหมาะกับ SME ต่อไป” ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า มีความเหมาะสมในเบื้องต้น แต่ต้องนำไปสู่การปฏิบัติจริง นำเอาสิ่งที่ผู้วิจัยนำเสนอไปทดลองให้ผู้ประกอบการทำการประเมินถึงสิ่งที่ผู้วิจัยได้นำเสนอ ซึ่ง ณ เวลานั้น จะได้คำตอบที่ชัดเจนมากที่สุด แต่เนื่องจากงานที่วิจัยนำเสนอนี้ เป็นเรื่องใหม่ จึงอาจจะยังไม่สามารถสรุปให้ชัดเจนไปเลยว่า มีความเหมาะสมมากน้อยเพียงใด

4.4.3.5 ตัวชี้วัดในแต่ละตัว จะต้องสามารถระบุได้ว่าควรอยู่ใน Level ที่เท่าไหร่

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “ตัวชี้วัดแต่ละตัวจะต้องสามารถระบุได้ว่าควรอยู่ใน Level ที่เท่าไหร่” สำหรับประเด็นนี้ผู้วิจัยได้อธิบายให้ผู้ทรงทราบถึงเกณฑ์การประเมินที่ได้อธิบายไปแล้วในข้อ 4.3.2.3 ถึงสาเหตุที่ไม่ได้จัดว่าตัวชี้วัดแต่ละตัวอยู่ใน level ที่เท่าไหร่ เพราะข้อคำถามที่เป็นตัวชี้วัดไม่ได้บอกถึงระดับของวุฒิภาวะและการประเมินเป็นลักษณะ subjective ดังนั้นจึงให้ผู้ประเมินทำการประเมินเป็นรายข้อด้วยเกณฑ์ของระดับวุฒิภาวะที่แสดงดังภาพประกอบที่4.13 โดยเกณฑ์ที่นำมาพิจารณาได้อ้างอิงจากหลักการของ SOC-CMM และ ISM Benchmark ที่ตัวชี้วัดแต่ละตัวก็ไม่ได้ระบุว่าอยู่ใน Level ไหนเช่นเดียวกัน ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า จากการที่ผู้วิจัยออกแบบตัวชี้วัดและเกณฑ์ในการประเมินมีหลักการและวิธีการที่อ้างอิงจากแหล่งข้อมูลที่น่าเชื่อถือ งานของผู้วิจัยจึงไม่จำเป็นต้องระบุว่าตัวชี้วัดตัวไหน อยู่ใน maturity ที่ level เท่าไหร่ เหมือนใน CMMI

4.4.3.6 การกำหนดเกณฑ์ เป็นเรื่อง Serious ควรจะต้องบอกได้ว่า Minimum Requirement ควรอยู่ตรงไหน

จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “การกำหนดเกณฑ์ เป็นเรื่องที่ Serious ควรจะต้องบอกได้ว่า Minimum Requirement ควรอยู่ตรงไหน” ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า พิจารณาจากข้อที่ผ่าน ๆ มาของผู้วิจัยสำหรับงานวิจัยที่ผู้วิจัยนำเสนอนั้น จึงไม่จำเป็นที่จะต้องกำหนดในเรื่องของ Minimum Requirement ที่จะต้องใช้ในสำหรับงานวิจัยในตอนนี้ เพราะผู้วิจัยมีการกำหนดเกณฑ์ กับหลักวิธีการประเมินที่ขึ้นอยู่กับผู้ประเมินจะเป็นผู้พิจารณาอยู่แล้ว

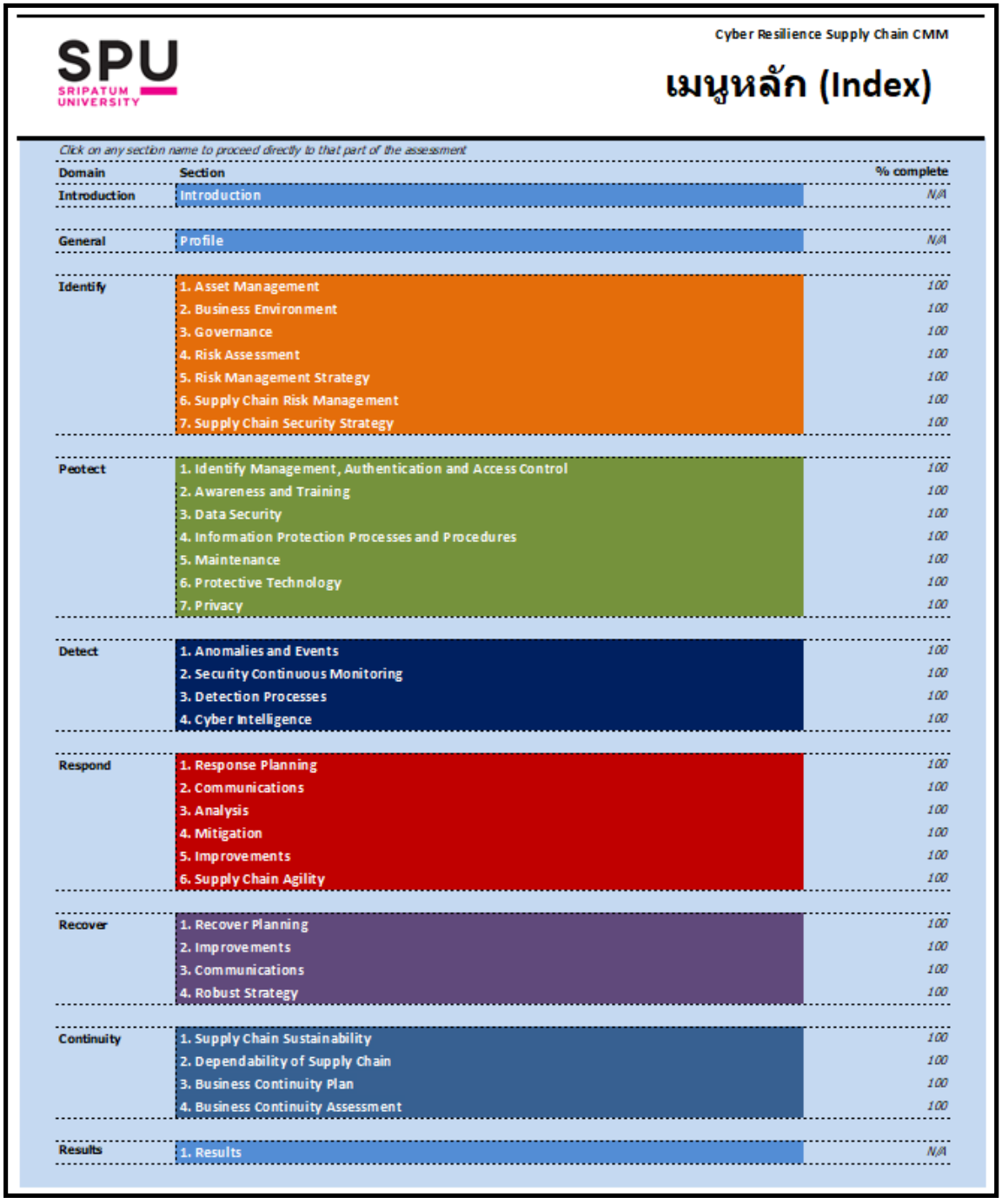
จากการสนทนากลุ่มของผู้ทรงคุณวุฒิในประเด็น “แนวคิดในการทำงานวิจัยไม่สามารถเป็น General ได้ การทำวิจัยควรจะ Specific หรือให้เกิดความชำนาญและเชี่ยวชาญเฉพาะด้าน เฉพาะกลุ่ม Industry ไปเลย” ผู้ทรงคุณวุฒิได้สรุปร่วมกันว่า ในเบื้องต้นมีความเหมาะสมสำหรับงานของผู้วิจัย พิจารณาในภาพใหญ่ ที่มองจากปัญหาการโจมตีทางไซเบอร์ที่อาจจะมีต่อ SME ดังนั้นการจะพิจารณาให้เฉพาะด้าน หรือเฉพาะกลุ่ม Industry นั้น อาจจะทำได้แต่เป็นงานวิจัย ที่สามารถต่อยอด เพื่อให้เกิดประโยชน์กับกลุ่ม Industry ในแต่ละกลุ่มของ SME รวมไปถึงกลุ่มอุตสาหกรรมขนาดใหญ่ต่อไปได้

4.5 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 5

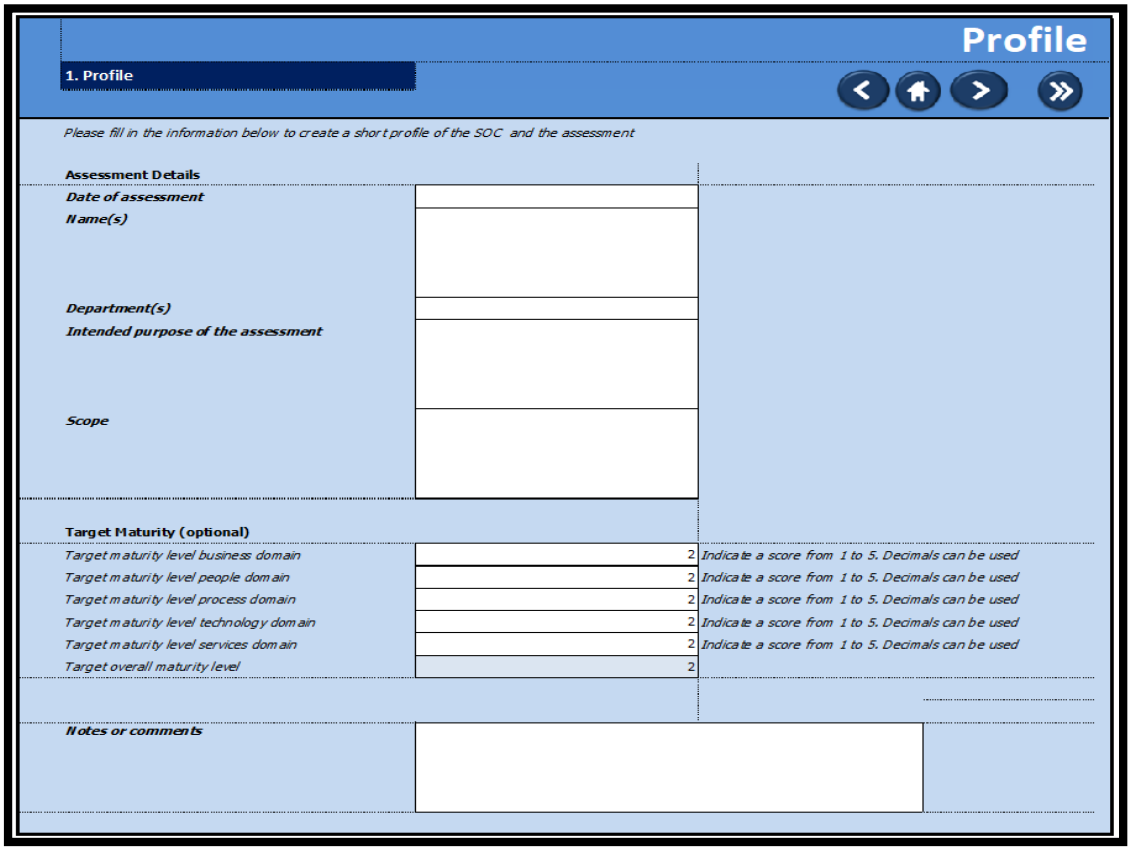
ผลการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 5 เพื่อพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม เมื่อผู้วิจัยได้กำหนดกรอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ประกอบไปด้วย 6 หมวด 32 มิติ ซึ่งทำให้สามารถกำหนดถึงตัวชี้วัดต่าง ๆ ได้ถึง 142 ตัวชี้วัด ตามวัตถุประสงค์ในข้อที่ 3-5 แล้วนั้น ผู้วิจัยจึงได้นำความรู้ที่ได้ค้นพบนี้ มาต่อยอดเพื่อให้สามารถประยุกต์ใช้ความรู้จากงานวิจัยฉบับนี้ได้อย่างเป็นรูปธรรม โดยการพัฒนาระบบประเมินในรูปแบบมาโคร (Macro) บนโปรแกรมไมโครซอฟท์เอ็กซ์เซล (Microsoft Excel) เพื่อให้เกิดความสะดวกในการประเมิน และยังจะสามารถวิเคราะห์ช่องว่าง (Gap Analysis) ในแต่ละมิติ รวมไปถึงภาพรวมของแต่ละหมวด เพื่อให้ผู้บริหารได้เห็นถึงช่องว่างของจุดแข็งและจุดที่ควรพัฒนาของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล เพื่อเป็นส่วนสนับสนุนในการตัดสินใจในการลงทุนด้านไอทีขององค์กร/หน่วยงาน เพื่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลต่อไป นอกจากนี้ระบบยังจะสามารถให้คำแนะนำสำหรับมิติที่เป็นจุดที่ควรพัฒนาแก่ผู้บริหาร เพื่อเป็นแนวทางในการปรับปรุงระบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลขององค์กร/หน่วยงานได้อย่างมีทิศทาง มีเป้าหมาย และมีประสิทธิภาพ ผู้วิจัยได้แสดงรูปหน้าจอส่วนที่สำคัญเพื่อให้เห็นภาพการทำงานของระบบดังภาพประกอบที่ 4.14 – 4.16

ภาพประกอบที่ 4.14 ผู้ประเมินสามารถทำการประเมินได้ทีละมิติของแต่ละหมวด โดยเมื่อทำการประเมินในมิติที่ 1 สามารถที่จะเลือกประเมินในมิติที่ 2 หรือมิติอื่น ๆ ที่อยู่ภายใต้หมวดนั้น ๆ ได้ โดยถ้าต้องการที่จะทำการประเมินในหมวดถัดไป ก็สามารถเข้าไปที่เมนูหลัก และเลือกหมวดที่ต้องการจะเข้าไปทำการประเมินได้ โดยที่หน้าเมนูหลักจะมีตัวเลขบอกให้ผู้ประเมินทราบว่า ได้ทำ

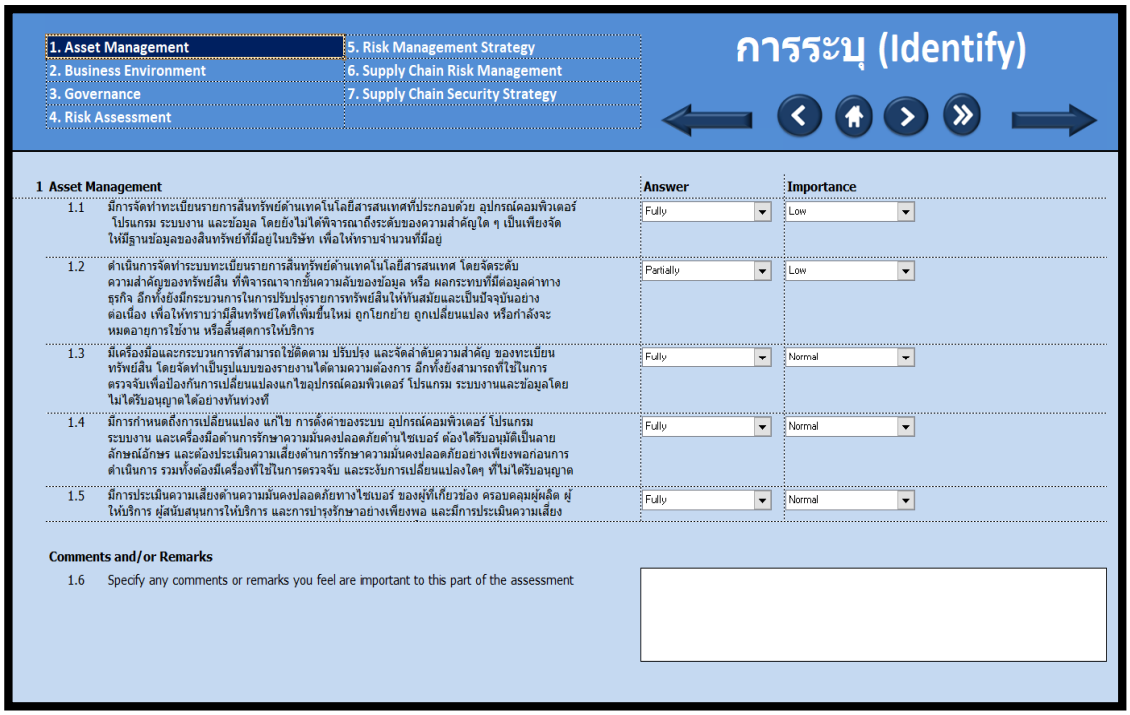
การประเมินในแต่ละมิติครบถ้วนแล้วหรือยัง โดยตัวเลขจะอยู่ทางด้านขวาของแต่ละมิติ ถ้าตัวเลขอยู่ที่ 100 หมายถึงว่าในมิตินั้น ๆ ผู้ประเมินได้ทำการประเมินครบในทุกข้อเป็นที่เรียบร้อยแล้ว



ภาพประกอบที่ 4.14 หน้าจอหลักของระบบประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของห่วงโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล

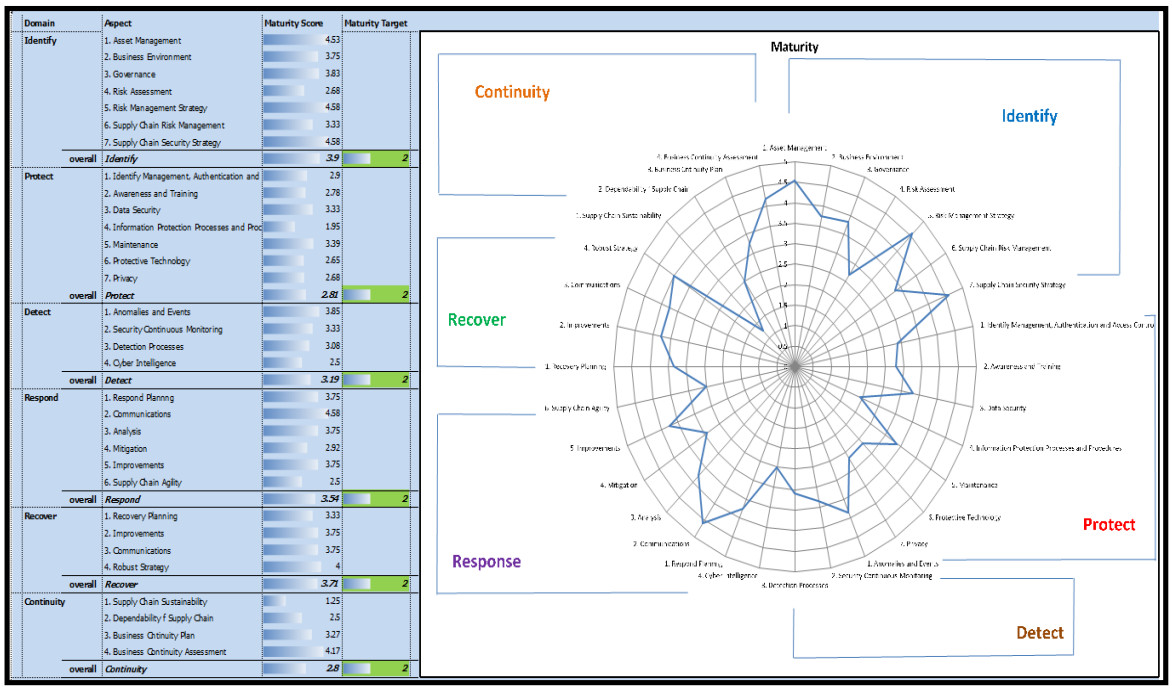


ภาพประกอบที่ 4.15 หน้าจอระบุรายละเอียดของผู้ประเมิน



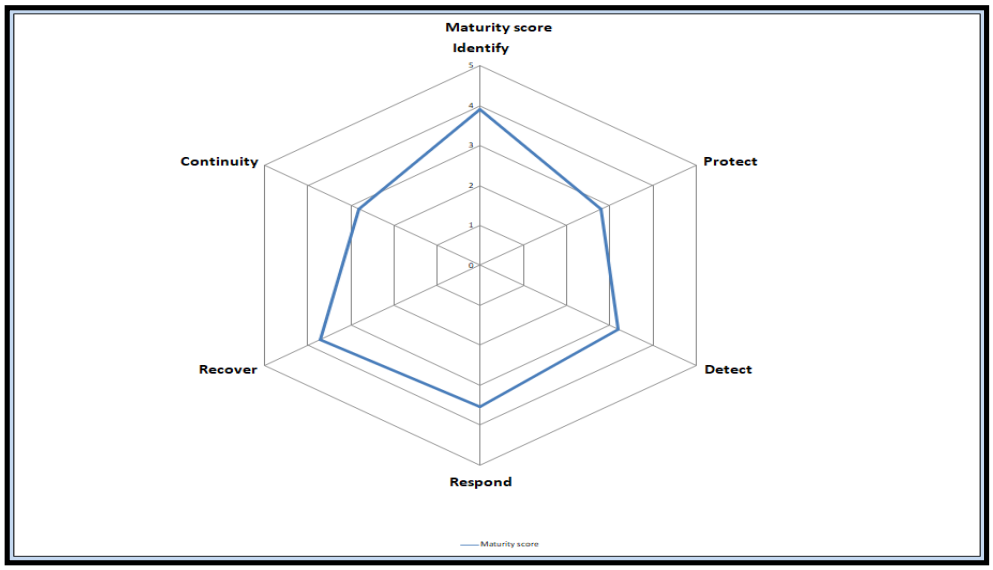
ภาพประกอบที่ 4.16 หน้าจอเมนูการประเมินการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

เมื่อผู้ประเมินการประเมินครบทุกมิติ และทุกหมวดเป็นที่เรียบร้อยแล้ว ผู้ประเมินสามารถที่จะเรียกดูการรายงานผลได้ที่เมนู Results โดยเมื่อกดเข้าไป ผู้ประเมินจะเห็นการายงาผลดังภาพประกอบที่ 4.17 – 4.18 ดังต่อไปนี้



Domain	Aspect	Maturity Score	Maturity Target
Identify	1. Asset Management	4.53	
	2. Business Environment	3.75	
	3. Governance	3.83	
	4. Risk Assessment	2.68	
	5. Risk Management Strategy	4.58	
	6. Supply Chain Risk Management	3.33	
	7. Supply Chain Security Strategy	4.58	
overall	*Identify*	*3.9*	*2*
Protect	1. Identify Management, Authentication and	2.9	
	2. Awareness and Training	2.78	
	3. Data Security	3.33	
	4. Information Protection Processes and Proc	1.95	
	5. Maintenance	3.39	
	6. Protective Technology	2.65	
	7. Privacy	2.68	
overall	*Protect*	*2.81*	*2*
Detect	1. Anomalies and Events	3.85	
	2. Security Continuous Monitoring	3.33	
	3. Detection Processes	3.08	
	4. Cyber Intelligence	2.5	
overall	*Detect*	*3.19*	*2*
Respond	1. Respond Planning	3.75	
	2. Communications	4.58	
	3. Analysis	3.75	
	4. Mitigation	2.92	
	5. Improvements	3.75	
	6. Supply Chain Agility	2.5	
overall	*Respond*	*3.54*	*2*
Recover	1. Recovery Planning	3.33	
	2. Improvements	3.75	
	3. Communications	3.75	
	4. Robust Strategy	4	
overall	*Recover*	*3.71*	*2*
Continuity	1. Supply Chain Sustainability	1.25	
	2. Dependability f Supply Chain	2.5	
	3. Business Ctinuity Plan	3.27	
	4. Business Continuity Assessment	4.17	
overall	*Continuity*	*2.8*	*2*

ภาพประกอบที่ 4.17 การรายงานผลการประเมินคะแนนแต่ละมิติ



ภาพประกอบที่ 4.18 การรายงานผลการประเมินคะแนนแต่ละหมวด

4.5.1 ผลการวิเคราะห์ข้อมูลโดยเทคนิคกระบวนการตัดสินใจเชิงลำดับชั้น (Analytic Hierarchy Process: AHP**)**

ในกรณีที่บริษัท/องค์กร/หน่วยงาน ที่มีผู้ทำการประเมินมากกว่า 1 คนขึ้นไป ผู้วิจัยจึงได้นำเอาเทคนิคกระบวนการตัดสินใจเชิงลำดับชั้น (Analytic Hierarchy Process: AHP) ซึ่งเป็นกระบวนการตัดสินใจที่มีประสิทธิภาพ โดยแบ่งองค์ประกอบของปัญหาออกเป็น ส่วน ๆ ในรูปของแผนภูมิตามลำดับชั้นแล้วกำหนดค่าของการวินิจฉัยเปรียบเทียบปัจจัยต่าง ๆ และนำค่าเหล่านั้นมาคำนวณเพื่อดูว่าปัจจัยและทางเลือกอะไรมีค่าลำดับความสำคัญสูงที่สุด

4.5.1.1 โครงสร้างเชิงลำดับชั้นของเกณฑ์การตัดสินใจที่ใช้ในการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

จากผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 ถึงข้อที่ 4 เกี่ยวกับระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของห่วงโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ผู้วิจัยสามารถนำมาสร้างเป็นโครงสร้างลำดับชั้นในการประเมินระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลจากผู้ประเมินหลายราย โดยแสดงดังภาพประกอบที่4.19

กำหนดให้

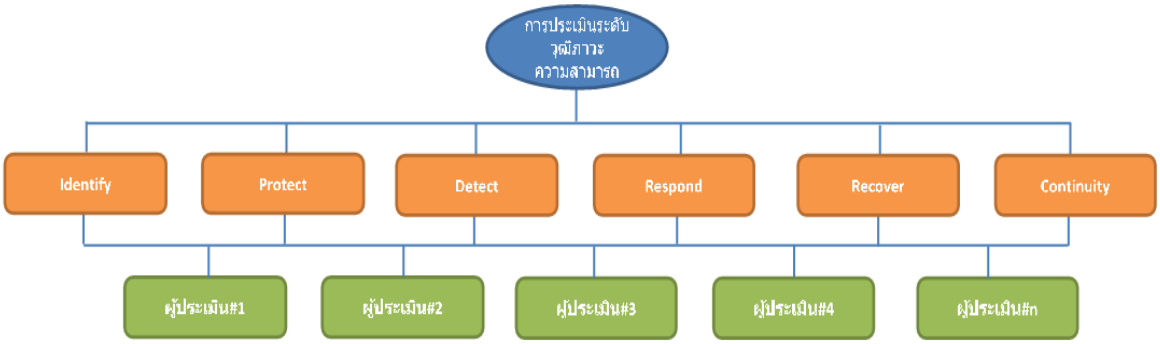
X_j โดยที่ j = 1,2,3,...

1 = ผู้ประเมินรายที่ 1

2 = ผู้ประเมินรายที่ 2

⋮

n = ผู้ประเมินรายที่ n



ภาพประกอบที่ 4.19 โครงสร้างลำดับชั้นของการประเมินระดับวุฒิภาวะความสามารถของผู้ประเมิน

4.5.1.2 รายละเอียดของผู้ตอบแบบสอบถาม

จากผลการวิจัยที่ได้ตามวัตถุประสงค์ข้อ 3-5 นั้น ซึ่งผู้วิจัยได้พัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม ตามวัตถุประสงค์ในข้อที่ 5 โดยนำเอาระบบการประเมินดังกล่าวนี้ไปทดลองใช้กับบริษัทต่าง ๆ จำนวน 12 บริษัท โดยมีผู้ร่วมประเมินจำนวน 15 ท่าน เพื่อทดสอบดูว่า ระบบการประเมินระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลนั้น มีความเป็นไปได้ในการนำไปใช้งานเพื่อให้เกิดประโยชน์ให้มากที่สุด โดยในการนำเอาระบบการประเมินนี้ไปทดสอบกับบริษัทต่าง ๆ ผู้วิจัยได้ให้ผู้ร่วมทดสอบทำการประเมินเพื่อหาค่าน้ำหนักของปัจจัย เพื่อจะได้นำมาใช้ในการวิเคราะห์ข้อมูลตามกระบวนการตัดสินใจเชิงลำดับชั้นต่อไป โดยรายละเอียดของผู้ตอบแบบสอบถามแสดงดังตารางที่ 4.60

ตารางที่ 4.60 รายละเอียดของผู้ตอบแบบสอบถามประเมินค่าน้ำหนักของปัจจัย

ลำดับ	บริษัท	ตำแหน่ง
1	1	กรรมการผู้จัดการ
2	2	Project Manager
3	3	Digital Marketing Manager
4	4	Business Consult Manager
5	5	IT Senior Officer
6	6	Senior IT Support
7	7	Assistant IT Section Manager
8	8	IT Manager
9	9	Sales and Marketing Manager
10	10	Operation Merchandising Parcel & Support Manager
11	11	Human Resource Manager
12	12	Account Manager
13	12	Senior Programmer
14	12	Application Support Manager
15	12	Programmer

4.5.1.3 การวิเคราะห์ความสำคัญค่าน้ำหนักของปัจจัย

ในการวิเคราะห์ความสำคัญค่าน้ำหนักของปัจจัย ผู้วิจัยได้ออกแบบแบบสอบถามสำหรับการหาค่าน้ำหนักของปัจจัย โดยรายละเอียดแสดงในภาคผนวก ซึ่งได้มีผู้ตอบแบบสอบถามมาจำนวนทั้งสิ้น 15 ท่าน จาก 12 บริษัท โดยผู้วิจัยได้กำหนดเกณฑ์สำหรับผู้ตอบแบบสอบถามในเรื่องค่าน้ำหนักโดยมีรายละเอียดดังตารางที่ 4.61

ตารางที่ 4.61 เกณฑ์มาตรฐานที่ใช้ในการเปรียบเทียบความสำคัญ

ค่าความสำคัญ	นิยาม	คำอธิบาย
1	มีความสำคัญเท่ากัน	ปัจจัยทั้งสองที่กำลังพิจารณาเปรียบเทียบมีความสำคัญเท่าเทียมกัน
3	มีความสำคัญมากกว่าพอประมาณ	ปัจจัยที่กำลังพิจารณาเปรียบเทียบมีความสำคัญมากกว่าปัจจัยตัวหนึ่งพอประมาณ
5	มีความสำคัญมากกว่าอย่างเด่นชัด	ปัจจัยที่กำลังพิจารณาเปรียบเทียบมีความสำคัญมากกว่าปัจจัยอีกตัวหนึ่งอย่างเด่นชัด
7	มีความสำคัญมากกว่าอย่างเด่นชัดมาก	ปัจจัยที่กำลังพิจารณาเปรียบเทียบมีความสำคัญมากกว่าปัจจัยอีกตัวหนึ่งอย่างเด่นชัดมาก
9	มีความสำคัญมากอย่างยิ่ง	ค่าความสำคัญสูงสุดที่จะเป็นไปได้ในการพิจารณาเปรียบเทียบปัจจัยทั้งสอง
2,4,6,8	เป็นค่าความสำคัญระหว่างกลางของค่าที่กล่าวไว้ข้างต้น	ค่าความสำคัญในการเปรียบเทียบปัจจัยถูกพิจารณาว่าควรเป็นค่าระหว่างกลางของค่าที่กล่าวไว้ข้างต้น

ในการตอบแบบสอบถาม ผู้วิจัยได้กำหนดให้ผู้ตอบแบบสอบถามเลือกที่จะประเมินค่าน้ำหนักของปัจจัย ซึ่งจะต้องนำปัจจัยมาเปรียบเทียบเป็นคู่ ๆ จนครบทุกคู่ โดยเริ่มต้นจากบนลงล่างของแผนภูมิ โดยจำนวนคู่ที่จะใช้ในการเปรียบเทียบจะเท่ากับ

$$\text{จำนวนคู่ในการเปรียบเทียบ} = \frac{n^2-n}{2}$$

โดยที่ n = จำนวนปัจจัยที่ถูกนำมาเปรียบเทียบ

ดังนั้นในงานวิจัยนี้จากโครงสร้างลำดับชั้นของการประเมินระดับวุฒิภาวะความสามารถของผู้ประเมิน ที่แสดงในภาพประกอบที่4.19 นั้น ซึ่งมีจำนวนปัจจัยทั้งสิ้น 6 ปัจจัย จึงสามารถหาจำนวนคู่ในการเปรียบเทียบได้ดังนี้

$$\text{จำนวนคู่ในการเปรียบเทียบ} = \frac{6^2-6}{2}$$
$$= 15 \text{ คู่}$$

ในการตอบแบบสอบถาม ผู้วิจัยได้แสดงตัวอย่างในการตอบแบบสอบถามไว้ตามรายละเอียดด้านล่างนี้ โดยที่ผู้ตอบแบบสอบถามจะต้องพิจารณาให้ค่าความสำคัญของปัจจัยเมื่อเปรียบเทียบกับปัจจัยตัวอื่นในแต่ละแถวของตาราง ท่านจะต้องพิจารณาดูว่า ปัจจัย A มีความสำคัญมากกว่า ปัจจัย B มากน้อยเพียงใด

ทียบปัจจัยในการเปรียบเA กับ B ถ้าท่านมีความเห็นว่า A “มีความสำคัญมากกว่าอย่างเด่นชัด” มากกว่า B แล้ว คำตอบของท่านจะเป็น ”5” ทางด้านมากกว่า ในตารางแบบสอบถาม หรือ

ในการเปรียบเทียบปัจจัยA กับ B ถ้าท่านมีความเห็นว่า A “มีความสำคัญน้อยกว่าอย่างเด่นชัด” มากกว่า B แล้ว คำตอบของท่านจะเป็น ”5” ทางด้านน้อยกว่า ในตารางแบบสอบถาม

จากตัวอย่างข้างต้นสามารถกรอกข้อมูลในการพิจารณาได้ดังตารางที่ 4.62

ตารางที่ 4.62 ตัวอย่างการกรอกแบบสอบถามสำหรับหาค่าน้ำหนักของปัจจัย

ปัจจัย	ค่ามาตรฐานของการเปรียบเทียบ																ปัจจัย
	มากกว่า								เท่ากัน	น้อยกว่า							
A	9	8	7	6	(5)	4	3	2	1	9	8	7	6	5	4	3	2	B
A	9	8	7	6	5	4	3	2	1	9	8	7	6	(5)	4	3	2	B

4.1.5.4 ผลการวิเคราะห์ข้อมูลสำหรับการหาค่าน้ำหนักของปัจจัย

หลังจากที่ได้ให้ผู้ทำการประเมินระบบในแต่ละบริษัท ตอบแบบสอบถามสำหรับการหาค่าน้ำหนักของปัจจัยแล้วนั้น ผู้วิจัยได้ทำการรวบรวมข้อมูลและนำมาทำการคำนวณหาค่าคะแนนเฉลี่ยของปัจจัยในแต่ละคู่เปรียบเทียบ โดยผลที่ได้แสดงดังตารางที่ 4.63

ตารางที่ 4.63 ผลคะแนนในเรื่องการเปรียบเทียบความสำคัญของปัจจัยของผู้ตอบแบบสอบถาม

ผู้ตอบแบบสอบถาม	I	I	I	I	I	P	P	P	P	D	D	D	R1	R1	R2
	P	D	R1	R2	C	D	R1	R2	C	R1	R2	C	R2	C	C
1	6	1	3	8	8	1	7	2	7	3	4	5	1	2	1
2	9	-7	8	8	-8	9	8	8	9	-9	-9	-8	9	8	-9
3	8	8	9	5	8	6	4	1	1	1	9	1	-9	1	-9
4	7	6	-8	-8	7	8	-8	-8	6	7	7	-8	-9	8	-9
5	-5	1	-7	-5	-5	1	1	1	1	5	5	1	3	1	1
6	4	6	5	6	-6	7	-7	6	5	6	6	5	8	6	5
7	4	4	4	4	4	1	2	2	2	2	2	2	1	1	1
8	7	1	1	7	-6	1	4	8	8	1	1	8	5	1	1
9	2	6	1	-4	1	2	1	4	7	6	6	5	5	-6	-6
10	1	7	1	-5	1	1	1	5	8	5	5	5	5	-7	-7
11	5	5	5	5	1	5	5	5	1	5	1	-5	5	-5	-5
12	5	5	5	7	5	-5	-6	2	-5	-5	-7	9	6	7	7
13	-6	-5	-7	-8	-8	8	1	1	8	-8	1	-8	1	1	1
14	-5	5	5	5	7	5	4	5	1	5	5	-5	-4	-5	5
15	6	-8	5	5	8	1	1	7	-4	-5	1	5	6	6	8
คะแนนรวม	48	35	30	30	17	51	18	49	55	19	37	12	33	19	-15
ผลคะแนนเฉลี่ย	**3**	**2**	**2**	**2**	**1**	**3**	**1**	**3**	**4**	**1**	**2**	**1**	**2**	**1**	**-1**

จากตารางที่ 4.63 ผลที่ได้สามารถสรุปผลที่ได้ดังต่อไปนี้

เพื่อให้บรรลุเป้าหมายที่ต้องการ

- เกณฑ์ Identify มีความสำคัญมากกว่าเกณฑ์ Protect ในระดับปานกลาง

ดังนั้น $I = 3P$ หรือ $P = (1/3)I$

- เกณฑ์ Identify มีความสำคัญมากกว่าเกณฑ์ Detect ในระดับน้อยกว่าปานกลาง

  ดังนั้น $I = 2D$ หรือ $D = (1/2)I$

- เกณฑ์ Identify มีความสำคัญมากกว่าเกณฑ์ Respond ในระดับน้อยกว่าปานกลาง

  ดังนั้น $I = 2R_1$ หรือ $R_1 = (1/2)I$

- เกณฑ์ Identify มีความสำคัญมากกว่าเกณฑ์ Recover ในระดับน้อยกว่าปานกลาง

  ดังนั้น $I = 2R_2$ หรือ $R_2 = (1/2)I$

- เกณฑ์ Identify มีความสำคัญเท่ากันกับเกณฑ์ Continuity

  ดังนั้น $I = C$ หรือ $C = I$

- เกณฑ์ Protect มีความสำคัญมากกว่าเกณฑ์ Detect ในระดับปานกลาง

  ดังนั้น $P = 3D$ หรือ $D = (1/3)P$

- เกณฑ์ Protect มีความสำคัญเท่ากันกับเกณฑ์ Respond

  ดังนั้น $P = R_1$ หรือ $R_1 = P$

- เกณฑ์ Protect มีความสำคัญมากกว่าเกณฑ์ Recover ในระดับปานกลาง

  ดังนั้น $P = 3R_2$ หรือ $R_2 = (1/3)P$

- เกณฑ์ Protect มีความสำคัญมากกว่าเกณฑ์ Continuity ในระดับปานกลางถึงมาก

  ดังนั้น $P = 4C$ หรือ $C = (1/4)P$

- เกณฑ์ Detect มีความสำคัญเท่ากันกับเกณฑ์ Respond

  ดังนั้น $D = R_1$ หรือ $R_1 = D$

- เกณฑ์ Detect มีความสำคัญมากกว่าเกณฑ์ Recover ในระดับน้อยกว่าปานกลาง

  ดังนั้น $D = 2R_2$ หรือ $R_2 = (1/2)D$

- เกณฑ์ Detect มีความสำคัญเท่ากันกับเกณฑ์ Continuity

  ดังนั้น $D = C$ หรือ $C = D$

- เกณฑ์ Respond มีความสำคัญมากกว่าเกณฑ์ Recover ในระดับน้อยกว่าปานกลาง

  ดังนั้น $R_1 = 2R_2$ หรือ $R_2 = (1/2)R_1$

- เกณฑ์ Respond มีความสำคัญเท่ากันกับเกณฑ์ Continuity

  ดังนั้น $R_1 = C$ หรือ $C = R_1$

- เกณฑ์ Recover มีความสำคัญเท่ากันกับเกณฑ์ Continuity

  ดังนั้น $R_2 = C$ หรือ $C = R_2$

สามารถสรุปผลของการเปรียบเทียบปัจจัยเป็นคู่ได้ผลตามตารางที่ 4.64

ตารางที่ 4.64 คะแนนเฉลี่ยการเปรียบเทียบปัจจัยเป็นคู่

ปัจจัย	ค่ามาตรฐานของการเปรียบเทียบ			ปัจจัย
	มากกว่า	เท่ากัน	น้อยกว่า	
การระบุ	3			การป้องกัน
การระบุ	2			การตรวจจับ
การระบุ	2			การรับมือ
การระบุ	2			การฟื้นฟู
การระบุ		1		ความต่อเนื่อง
การป้องกัน	3			การตรวจจับ
การป้องกัน		1		การรับมือ
การป้องกัน	3			การฟื้นฟู
การป้องกัน	4			ความต่อเนื่อง
การตรวจจับ		1		การรับมือ
การตรวจจับ	2			การฟื้นฟู
การตรวจจับ		1		ความต่อเนื่อง
การรับมือ	2			การฟื้นฟู
การรับมือ		1		ความต่อเนื่อง
การฟื้นฟู		1		ความต่อเนื่อง

จากนั้นทำการคำนวณเพื่อหาค่าน้ำหนักของปัจจัยแต่ละตัว ซึ่งได้ผลตาม ตารางที่ 4.65 – 4.67

ตารางที่ 4.65 แสดงผลค่าการวินิจฉัยเปรียบเทียบในตารางเมทริกซ์

เป้าหมาย	Identify	Protect	Detect	Respond	Recover	Continuity
Identify	1	3	2	2	2	1
Protect	1/3	1	3	1	3	4
Detect	1/2	1/3	1	1	2	1
Respond	1/2	1	1	1	2	1
Recover	1/2	1/3	1/2	1/2	1	1
Continuity	1	1/4	1	1	1	1

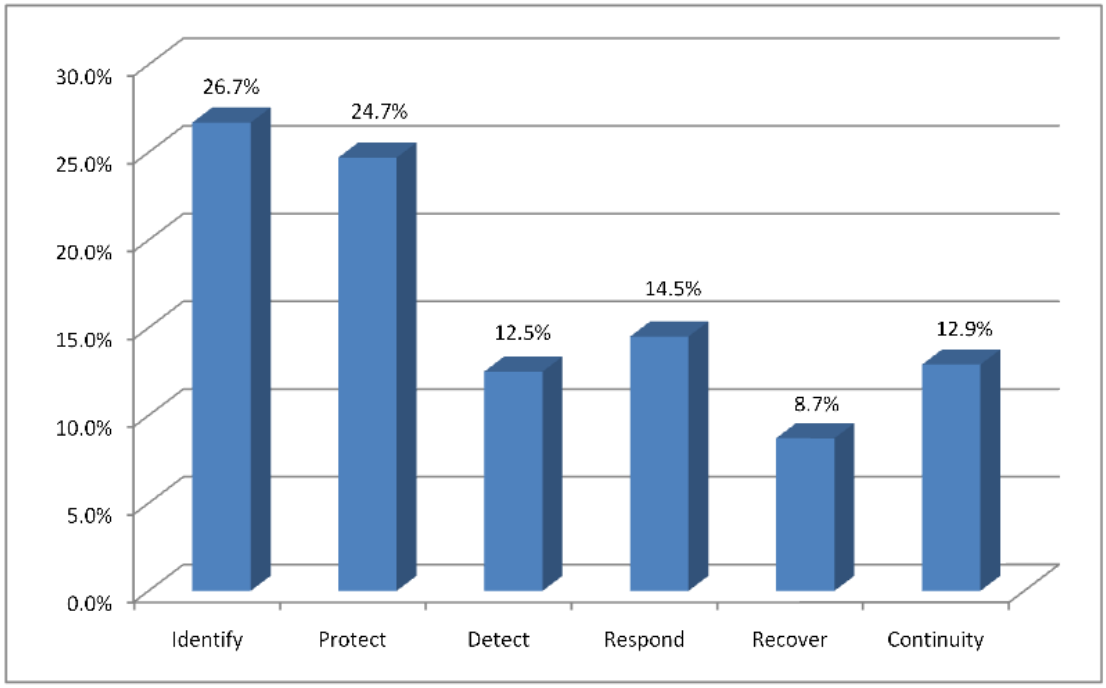
ตารางที่ 4.66 ผลรวมในแนวตั้งของตารางเมทริกซ์

เป้าหมาย	Identify	Protect	Detect	Respond	Recover	Continuity
Identify	1	3	2	2	2	1
Protect	1/3	1	3	1	3	4
Detect	1/2	1/3	1	1	2	1
Respond	1/2	1	1	1	2	1
Recover	1/2	1/3	1/2	1/2	1	1
Continuity	1	1/4	1	1	1	1
ผลรวมในแนวตั้ง	**3 5/6**	**6**	**8 1/2**	**6 1/2**	**11**	**9**

ตารางที่ 4.67 หาอัตราส่วนที่ได้จากผลรวมในแนวตั้ง

เป้าหมาย	Identify	Protect	Detect	Respond	Recover	Continuity	ลำดับความสำคัญ	
Identify	1/4	1/2	1/4	1/3	1/5	1/9	0.267	1.00
Protect	2/23	1/6	1/3	1/6	1/4	4/9	0.247	
Detect	1/8	4/71	1/8	1/6	1/5	1/9	0.125	
Respond	1/8	1/6	1/8	1/6	1/5	1/9	0.145	
Recover	1/8	4/71	1/17	1/13	1/11	1/9	0.087	
Continuity	1/4	3/71	1/8	2/13	1/11	1/9	0.129	

จากตารางที่ 4.67 ได้ผลลัพธ์จากการเปรียบเทียบความสัมพันธ์ของปัจจัยต่าง ๆ ทั้ง 6 ปัจจัย พบว่าผู้ตอบแบบสอบถามทั้ง 15 ท่าน ให้ความสำคัญกับปัจจัย Identify เป็นอันดับแรก รองลงมาเป็น Protect, Respond, Continuity, Detect และ Recover ตามลำดับ ดังแสดงในภาพประกอบที่ 4.20



ภาพประกอบที่ 4.20 ค่าน้ำหนักของปัจจัย

4.1.5.5 ตัวอย่างการวิเคราะห์ผลข้อมูลที่บริษัทมีการประเมินหลายคนด้วย AHP

ผลที่ได้จากการนำเอาระบบประเมินไปใช้กับบริษัทต่างๆ จำนวน 12 บริษัท โดยเฉพาะบริษัทที่ 12 ที่มีผู้ประเมิน 4 ท่าน โดยผู้ประเมินมีตำแหน่งต่าง ๆ ดังนี้

ผู้ประเมินท่านที่ 1	Account Manager
ผู้ประเมินท่านที่ 2	Senior Manager
ผู้ประเมินท่านที่ 3	Application Support Manager
ผู้ประเมินท่านที่ 4	Programmer

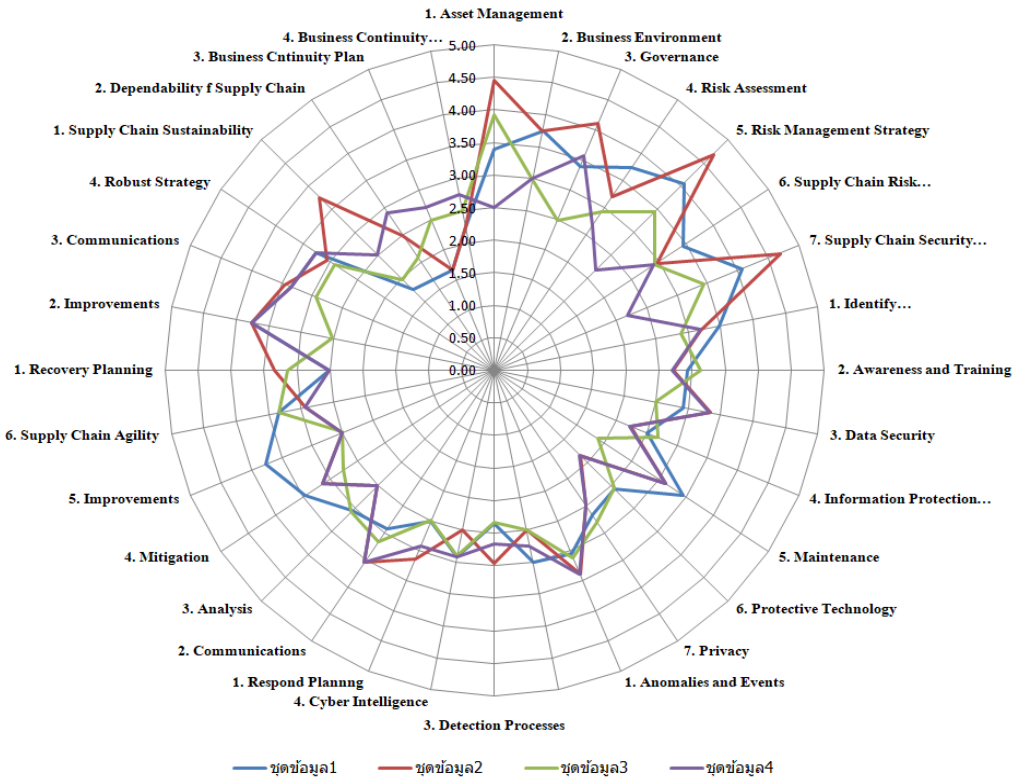
โดยได้ผลจากการประเมินออกมาดังตารางที่ 4.68 ภาพประกอบที่ 4.21 – 4.22

ตารางที่ 4.68 ผลการประเมินของผู้ประเมิน 4 ท่านจากบริษัทที่ 12

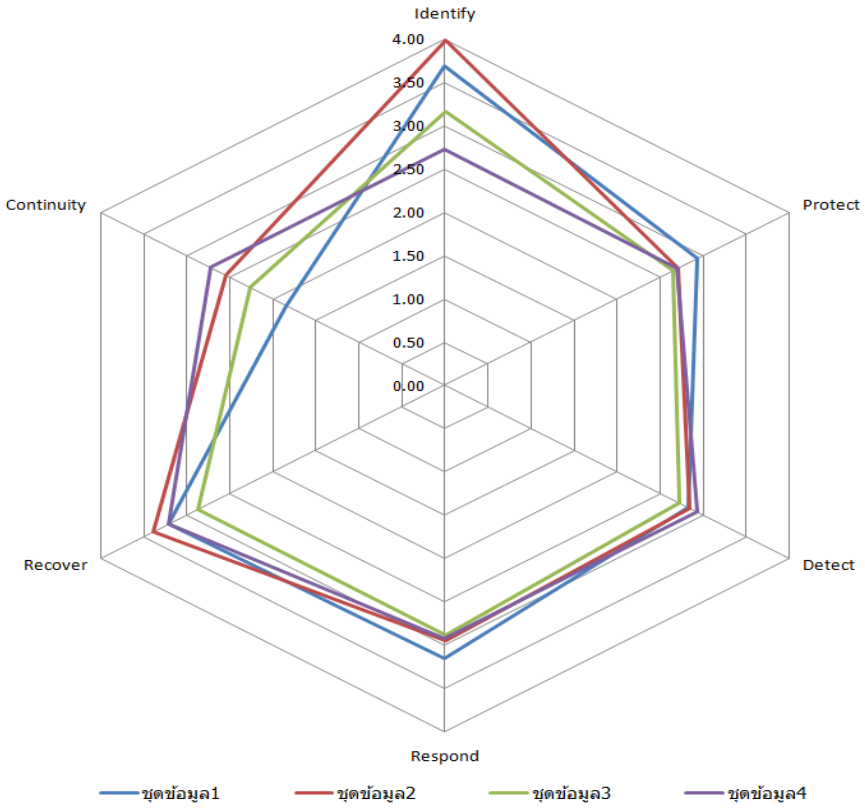
Aspect	Maturity Score			
	#1	#2	#3	#4
1. Asset Management	3.39	4.46	3.93	2.50
2. Business Environment	3.75	3.75	3.00	3.00
3. Governance	3.39	4.11	2.50	3.57
4. Risk Assessment	3.75	3.21	2.92	2.68
5. Risk Management Strategy	4.06	4.69	3.44	2.19
6. Supply Chain Risk Management	3.44	2.97	2.92	2.92
7. Supply Chain Security Strategy	4.06	4.69	3.44	2.19
Identify	**3.69**	**3.98**	**3.16**	**2.72**
8. Identify Management, Authentication and Access Control	3.47	3.19	2.89	3.19
9. Awareness and Training	2.92	2.71	3.13	2.71
10. Data Security	2.92	3.33	2.50	3.33
11. Information Protection Processes and Procedures	2.50	2.23	2.68	2.23
12. Maintenance	3.44	3.13	1.88	3.13
13. Protective Technology	2.57	1.84	2.57	1.84
14. Privacy	2.66	2.50	2.81	2.50
Protect	**2.93**	**2.70**	**2.64**	**2.70**
15. Anomalies and Events	3.04	3.39	3.13	3.39
16. Security Continuous Monitoring	3.00	2.50	2.50	2.75
17. Detection Processes	2.34	2.97	2.34	2.66
18. Cyber Intelligence	2.92	2.50	2.92	2.92
Detect	**2.83**	**2.84**	**2.72**	**2.93**
19. Respond Plannng	2.50	3.13	2.50	2.92
20. Communications	2.92	3.54	3.18	3.54
21. Analysis	3.04	2.50	3.08	2.50
22. Mitigation	3.44	3.13	2.75	3.13
23. Improvements	3.75	2.50	2.50	2.50

ตารางที่ 4.68 (ต่อ)

Aspect	Maturity Score			
	#1	#2	#3	#4
24. Supply Chain Agility	3.33	2.92	3.33	2.92
Respond	**3.16**	**2.95**	**2.89**	**2.92**
25. Recovery Planning	2.50	3.33	3.13	2.50
26. Improvements	3.75	3.75	2.50	3.75
27. Communications	3.33	3.44	2.92	3.33
28. Robust Strategy	3.25	3.04	2.92	3.25
Recover	**3.21**	**3.39**	**2.87**	**3.21**
29. Supply Chain Sustainability	1.75	3.75	1.96	2.50
30. Dependability f Supply Chain	1.67	2.50	2.08	2.92
31. Business Cntinuity Plan	1.67	1.67	2.50	2.71
32. Business Continuity Assessment	2.25	2.25	2.50	2.75
Continuity	**1.84**	**2.54**	**2.26**	**2.72**



ภาพประกอบที่ 4.21 ระดับวุฒิภาวะความสามารถของผู้ประเมินทั้ง 4 ท่านในแต่ละมิติ



ภาพประกอบที่ 4.22 ระดับวุฒิภาวะความสามารถของผู้ประเมินทั้ง 4 ท่านในแต่ละหมวด

จากค่าน้ำหนักของปัจจัยที่หาตามข้อ 4.4.1.4 นั้น สามารถนำมาคำนวณหาได้ว่า ผลการประเมินจะเลือกตามผู้ประเมินท่านใน สามารถแสดงได้ดังตารางที่ 4.69 – 4.70

ตารางที่ 4.69 ค่าน้ำหนักของปัจจัยในแต่ละหมวด

หมวด	ค่าน้ำหนักปัจจัย
Identify	0.267
Protect	0.247
Detect	0.125
Respond	0.144
Recover	0.087
Continuity	0.129

ตารางที่ 4.70 ผลการประเมินระดับวุฒิภาวะความสามารถของผู้ประเมินด้วย AHP

หมวด	ผู้ประเมิน			
	#1	**#2**	**#3**	**#4**
Identify	0.99	1.06	0.84	0.73
Protect	0.72	0.67	0.65	0.67
Detect	0.35	0.36	0.34	0.37
Respond	0.45	0.42	0.42	0.42
Recover	0.28	0.30	0.25	0.28
Continuity	0.24	0.33	0.29	0.35
ผลลัพธ์	**3.04**	**3.14**	**2.80**	**2.81**

จากผลลัพธ์ที่ได้ จะเห็นว่าผู้ประเมินท่านที่ 2 จะมีค่าผลการคำนวณผลรวมของปัจจัยในแต่ละหมวดมากที่สุด ดังนั้นจึงสรุปได้ว่า การประเมินของบริษัทที่ 12 นี้จะเป็นระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาไดต่อไป

4.4 สรุป

ในบทนี้เป็นการวิเคราะห์ และนำเสนอผลการวิจัย โดยผู้วิจัยได้แบ่งการนำเสนอตามลำดับของวัตถุประสงค์ในงานวิจัย ได้แก่ ผลการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 1&2 เพื่อทำการวิเคราะห์ปัจจัยสำคัญที่มีผลต่อความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ในการจัดการความต่อเนื่องของธุรกิจดิจิทัล ใช้ระเบียบวิธีวิจัยเชิงปริมาณ (Quantitative Research) และใช้แบบสอบถาม (Questionnaires) เป็นเครื่องในงานวิจัย โดยผลการวิจัยพบว่า 1) ความร่วมมือกันของโซ่อุปทานดิจิทัล การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล 2) ความร่วมมือกันของโซ่อุปทานดิจิทัล และการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจทัล มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผ่านการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล 3) ความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวก

ต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และ 4) ความร่วมมือกันของโซ่อุปทานดิจิทัล การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ผ่านความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 3&4 เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ในขั้นนี้ได้ดำเนินการศึกษาจากเอกสารและงานวิจัยที่เกี่ยวข้องเพื่อนำมาใช้ในการพัฒนากรอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ตัวชี้วัด และเกณฑ์ในการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ผลการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 5 เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการสร้างคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ในขั้นนี้เป็นการใช้ระเบียบวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยวิธีการสัมภาษณ์เชิงลึก (In-depth Interview) โดยพัฒนาแบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structure Interview) จากผู้เชี่ยวชาญ 17 ท่าน โดยแบ่งเป็นผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จำนวน 4 ท่าน ด้านตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model: CMM) จำนวน 4 ท่าน ด้านเทคโนโลยีดิจิทัล (Digital Technology) จำนวน 5 ท่าน และด้านโลจิสติกส์และโซ่อุปทานดิจิทัล จำนวน 4 ท่าน และได้ทำการการตรวจสอบความเหมาะสมและความสอดคล้องของกรอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ตัวชี้วัดและเกณฑ์ในการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ด้วยการวิเคราะห์เชิงเนื้อหา (Content Analysis) และยืนยันผลการวิจัยที่ได้ด้วยการสนทนากลุ่ม (Focus Group) โดยผู้เชี่ยวชาญ 6 ท่าน ซึ่งทำให้งานวิจัยสามารถเห็นผลได้อย่างเป็นรูปธรรม รวมถึงสามารถใช้เป็นฐานความรู้ด้านวิชาการที่สามารถนำไปขยายผลต่อยอดแก่นักวิจัยที่สนใจในอนาคต

ผลการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ 6 เพื่อพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของห่วงโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม จากผลการศึกษาที่ได้ตามวัตถุประสงค์ในข้อที่ 2 และ 3 ผู้วิจัยได้นำผลการศึกษาที่ค้นพบไปพัฒนาเป็นระบบประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม โดยการสร้างมาโคร (Macro) ในไมโครซอฟต์ เอกซ์เซล (Micrsoft Excel) และได้นำไปทดลองใช้งานกับ 12 บริษัท

โดยมีจำนวนผู้ประเมิน 15 ท่าน โดยผู้วิจัยได้ทดลองให้ 1 บริษัททำการประเมิน 4 ท่าน และใช้เทคนิคกระบวนการตัดสินใจเชิงลำดับชั้น (Analytic Hierarchy Process: AHP) มาใช้ในการตัดสินใจเลือกผลการประเมินที่ได้จากบริษัทดังกล่าว ซึ่งช่วยให้ผลการวิจัยสามารถนำไปใช้งานได้อย่างเป็นรูปธรรมมากขึ้น