การสัมภาษณ์เชิงลึกและประเมินระบบจากผู้เชี่ยวชาญ

เรื่อง

การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม

(The Development of Cyber-Resilient Capability Maturity Model of Digital Supply Chains for Managing the Digital Business Continuity in Small and Medium-sized Enterprises)

ชื่อผู้เชี่ยวชาญ.....

ตำแหน่ง .....

หน่วยงาน .....

วันที่สัมภาษณ์.....**สถานที่**.....

ผู้วิจัย

นายนริส อุไรพันธ์

นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการจัดการโลจิสติกส์และโซ่อุปทาน

วิทยาลัยโลจิสติกส์และซัพพลายเชน มหาวิทยาลัยศรีปทุม

โทรศัพท์ : 062-807-5550 อีเมล : naris080515@yahoo.com

วัตถุประสงค์ของการวิจัย

1. เพื่อทำการศึกษาและวิเคราะห์ระดับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล
2. เพื่อทำการวิเคราะห์ปัจจัยสำคัญที่มีผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
3. เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
4. เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
5. เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
6. เพื่อพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม

กรอบแนวคิดในการวิจัย

<u>คำชี้แจง</u> ขอความกรุณาผู้เชี่ยวชาญได้โปรดพิจารณา/ตรวจสอบ แนวทางการดำเนินงานวิจัยพร้อมทั้งข้อแนะนำ “**การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม**” อย่างอิสระ ทั้งนี้ในกรณีที่ท่านมีความเห็นหรือข้อเสนอแนะในการปรับปรุงแต่ละประเด็นโปรดเขียนข้อเสนอแนะหรืออาจให้ข้อแนะนำโดยตรงแก่ผู้วิจัย จักขอบพระคุณเป็นอย่างยิ่ง

รายการพิจารณา/ตรวจสอบ		**หมายเหตุ**
ส่วนที่ 1	แนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)	
ส่วนที่ 2	แนวทางการกำหนดตัวชี้วัดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)	
ส่วนที่ 3	แนวทางการกำหนดระดับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่ อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains)	
ส่วนที่ 4	แนวทางการประเมินระดับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล	

ส่วนที่ 1 แนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

(Cyber Resilience Supply Chain Model)

การพัฒนา **“ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม (The Development of Cyber-Resilient Capability Maturity Model of Digital Supply Chains for Managing the Digital Business Continuity in Small and Medium-sized Enterprises)”** ที่ผู้วิจัยนำเสนอนั้น ได้ทำการศึกษาทฤษฎี และงานวิจัยที่เกี่ยวข้อง รวมทั้งอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST), มาตรฐาน CMMI, CCS CSC (Council on Cybersecurity: 20 Critical Security Controls), COBIT 5, ISA 62443-2-1:2009 และมาตรฐาน ISO ประกอบด้วย

ISO/IEC 27001:2013 มาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

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

ISO/IEC 27005:2018 มาตรฐานด้านการบริหารจัดการความเสี่ยงด้านไซเบอร์ ที่ประกอบด้วย Information technology, Security techniques, Information security management systems

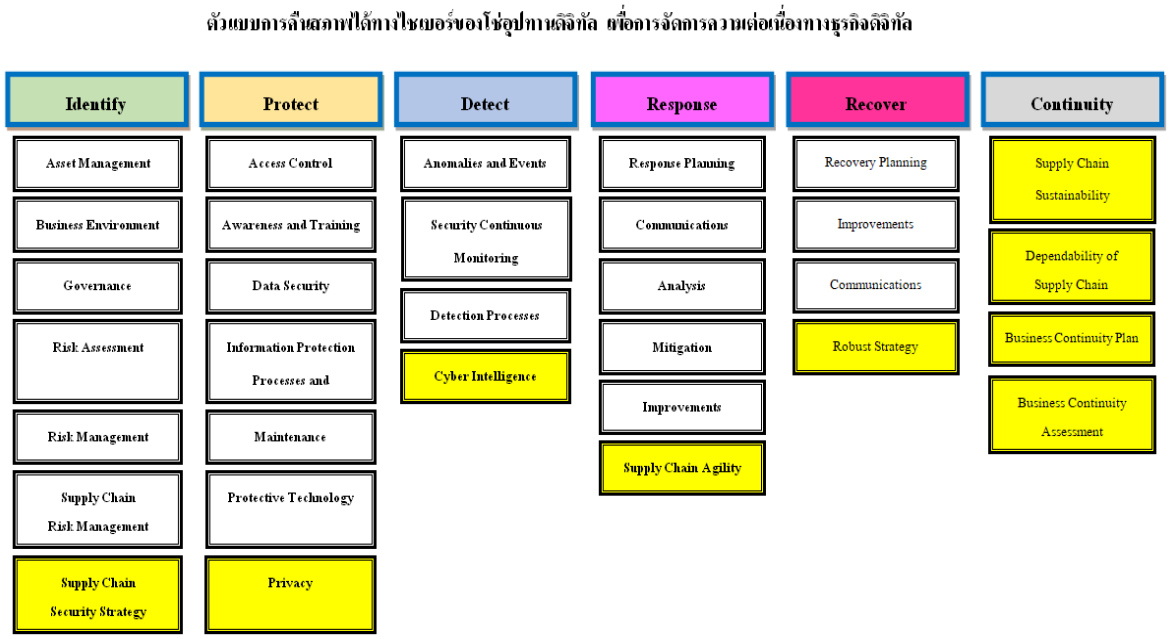
ISO 22301:2012 มาตรฐานด้านการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) เป็นมาตรฐานที่ช่วยให้แต่ละองค์กรสามารถวางแผนรับมือกับภัยพิบัติรูปแบบต่างๆ ได้อย่างเป็นระบบ โดยเฉพาะอย่างยิ่ง การโจมตีไซเบอร์

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

IS/IEC 28000 เป็นมาตรฐานที่กำหนดข้อกำหนดของระบบการจัดการความปลอดภัยของโซ่อุปทานและจัดเตรียมรูปแบบการจัดการให้กับองค์กรที่ต้องการนำระบบนี้ไปใช้ มีจุดมุ่งหมายในการจัดการความเสี่ยงอย่างมีประสิทธิภาพโดยจัดกิจกรรมขององค์กรด้านความมั่นคงปลอดภัยของโซ่อุปทานภายใต้ระบบเดียวกับระบบการจัดการอื่น ๆ

ISO 31000:2009 มาตรฐานด้านการบริหารจัดการความเสี่ยงระดับองค์กร

มาตรฐานต่าง ๆ ที่ใช้ ในการศึกษานี้ คือ เป็นมาตรฐานสากลที่ใช้สำหรับระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลทำให้กระบวนการทำงานขององค์กรภายใต้โซ่อุปทานสามารถที่จะทำงานได้อย่างมีความปลอดภัยจากสภาพแวดล้อมทางดิจทัลที่เป็นอยู่ในปัจจุบัน ด้วยการทำงานที่มีขั้นตอนชัดเจน และมีความพร้อมในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ในโซ่อุปทานได้อย่างมีประสิทธิภาพ สร้างความเชื่อถือคู่ค้าที่อยู่ภายใต้โซ่อุปทาน จากการศึกษาข้อมูลดังกล่าวข้างต้นทำให้ผู้วิจัยสามารถนำเสนอตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model) ที่ได้พัฒนาขึ้น โดยแสดงไว้ในรูปที่ 1



รูปที่ 1 ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

รายละเอียดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล สามารถแบ่งออกได้เป็น 6 หมวด 32 มิติการดำเนินการ โดยสามารถอธิบายได้ดังต่อไปนี้

หมวดที่ 1 การระบุ (Identify) – เป็นการระบุและเข้าใจถึงบริบทต่าง ๆ ของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีรายละเอียดมิติในการดำเนินการจะประกอบด้วย

มิติที่ 1 การจัดการทรัพยากรขององค์กร (Asset Management) ข้อมูล บุคลากร อุปกรณ์ ระบบ และสิ่งอำนวยความสะดวกที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจ จะต้องได้รับการระบุและจัดการให้สอดคล้องกับความสำคัญเชิงสัมพันธ์กับ วัตถุประสงค์ทางธุรกิจและกลยุทธ์ความเสี่ยงทางไซเบอร์ขององค์กร

มิติที่ 2 สภาวะแวดล้อมทางธุรกิจ (Business Environment) สร้างความเข้าใจในภารกิจขององค์กร วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสียและกิจกรรมขององค์กร และจัดลำดับความสำคัญข้อมูลเหล่านี้ เพื่อกำหนดบทบาทความรับผิดชอบ และการตัดสินใจในการจัดการความเสี่ยงทางไซเบอร์

มิติที่ 3 การกำกับดูแล (Governance) นโยบายขั้นตอนและกระบวนการในการจัดการและตรวจสอบความต้องการด้านกฎระเบียบ กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการ

ดำเนินงานขององค์กรและแจ้งให้ทราบถึงการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

มิติที่ 4 การประเมินความเสี่ยง (Risk Assessment) การทำความเข้าใจขององค์กรต่อความเสี่ยงทางไซเบอร์ ที่มีผลการดำเนินงานขององค์กร (รวมถึงภารกิจหน้าที่ ภาพลักษณ์หรือชื่อเสียง) ทรัพย์สินขององค์กร และบุคลากร

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

มิติที่ 6 การจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management) ลำดับความสำคัญขององค์กร ข้อจำกัด การยอมรับความเสี่ยงและข้อสมมติฐานถูกกำหนดขึ้นและใช้เพื่อสนับสนุนการตัดสินใจความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในโซ่อุปทาน รวมทั้งองค์กรได้กำหนดและดำเนินการตามกระบวนการเพื่อระบุประเมินและจัดการความเสี่ยงของโซ่อุปทาน

มิติที่ 7 กลยุทธ์การจัดการความมั่นคงปลอดภัยของโซ่อุปทาน (Supply Chain Security Strategy) เพื่อเป็นการกำหนดกลยุทธ์ที่ใช้ในการจัดการความมั่นคงปลอดภัยของโซ่อุปทานเพื่อสร้างความเชื่อมั่นให้กับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียต่อโซ่อุปทาน

หมวดที่ 2 การป้องกัน (Protect) – เป็นการวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กรต่อความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีรายละเอียดของกลุ่มงานในหมวดนี้คือ

มิติที่ 1 การควบคุมการเข้าถึง (Access Control) การจำกัดการเข้าถึงสินทรัพย์และสิ่งอำนวยความสะดวกที่เกี่ยวข้อง เฉพาะผู้ใช้งาน กระบวนการและอุปกรณ์ที่ได้รับอนุญาต และมีการจัดการที่สอดคล้องกับความเสี่ยงที่ประเมินจากการเข้าถึงกิจกรรมและธุรกรรมที่ไม่ได้รับอนุญาต

มิติที่ 2 การตระหนักและการฝึกอบรม (Awareness and Training) ต้องมีการให้ศึกษาเรื่องความมั่นคงปลอดภัยทางไซเบอร์ต่อบุคลากร รวมถึงการต้องฝึกอบรมอย่างเพียงพอในการปฏิบัติหน้าที่และความรับผิดชอบด้านความปลอดภัยของข้อมูลที่สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

มิติที่ 3 ความมั่นคงปลอดภัยของข้อมูล (Data Security) ข้อมูลและการบันทึก (ข้อมูล) ได้รับการจัดการให้สอดคล้องกับกลยุทธ์ความเสี่ยงทางไซเบอร์ขององค์กร เพื่อปกป้องความลับความถูกต้อง และความพร้อมของข้อมูล

มิติที่ 4 ขั้นตอนและกระบวนการ การป้องกันข้อมูล (Information Protection Processes and Procedures) นโยบายความปลอดภัย (วัตถุประสงค์ ขอบเขต บทบาทความรับผิดชอบ ข้อผูกพันการจัดการและการประสานงานระหว่างหน่วยงานองค์กร) กระบวนการและขั้นตอนและการบำรุงรักษาและใช้ในการจัดการป้องกันระบบ ข้อมูล และสินทรัพย์

มิติที่ 5 การบำรุงรักษา (Maintenance) การบำรุงรักษาและซ่อมแซม การควบคุมระบบงานที่เกี่ยวข้อง และส่วนประกอบของระบบสารสนเทศให้มีการดำเนินการที่สอดคล้องกับนโยบายและขั้นตอน

มิติที่ 6 เทคโนโลยีการป้องกัน (Protective Technology) โซลูชันด้านความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อรับรองความมั่นคงปลอดภัย และการคืนสภาพได้ของระบบ และสินทรัพย์ให้สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

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 (Response Planing) กระบวนการและขั้นตอนการรับมือต้องได้รับการดำเนินการ และบำรุงรักษาอยู่อย่างตลอด เพื่อให้มั่นใจว่ามีการตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบทันเวลา

มิติที่ 2 การสื่อสารเกี่ยวกับการรับมือ (Communications) กิจกรรมการตอบสนองมีการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกตามความเหมาะสมเพื่อรวมการสนับสนุนจากหน่วยงานบังคับใช้กฎหมาย

มิติที่ 3 การวิเคราะห์เพื่อการรับมือ (Analysis) มีการวิเคราะห์เพื่อให้มั่นใจว่ามีการตอบสนองที่เพียงพอและสนับสนุนกิจกรรมการกู้คืน

มิติที่ 4 การบรรเทาสถานการณ์ (Mitigation) มีการดำเนินกิจกรรมเพื่อการป้องกันรวมถึงกิจกรรมการบรรเทาสถานการณ์ ผลกระทบและกำจัดเหตุการณ์

มิติที่ 5 การพัฒนาแนวทางการรับมือ (Improvements) กิจกรรมการรับมือเพื่อตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ต้องมีการปรับปรุงโดยการรวมบทเรียนที่ได้เรียนรู้จากกิจกรรมการตรวจจับ / ตอบสนองในปัจจุบันและก่อนหน้า

มิติที่ 6 ความคล่องตัวของโซ่อุปทาน (Supply Chain Agility) ความสามารถของโซ่อุปทานที่ให้ความสนใจต่อการปรับตัวของระบบอย่างรวดเร็วในสถานการณ์ที่ต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่สามารถคาดเดาได้ ด้วยการแสดงปฏิกิริยาตอบโต้(React) การตอบสนอง (Respond) การปรับตัว (Adapt) รวมไปถึงการกำหนด ค่าใหม่ (Re-Cnfigure)

หมวดที่ 5 การฟื้นฟู (Recover) – เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ ฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม รายละเอียดของกลุ่มงานในหมวดนี้มีดังนี้

มิติที่ 1 การวางแผนการฟื้นฟูระบบ (Recovery Planning) กระบวนการและขั้นตอนการกู้คืนจะถูกดำเนินการและบำรุงรักษาเพื่อให้แน่ใจว่าระบบหรือทรัพย์สินจะได้รับผลกระทบจากเหตุการณ์ความปลอดภัยทางไซเบอร์ในเวลาที่เหมาะสม

มิติที่ 2 การพัฒนาแนวทางการฟื้นฟูระบบ (Improvements) การวางแผนและกระบวนการกู้คืนจะได้รับการปรับปรุงโดยผสมผสานบทเรียนที่เรียนรู้เข้ากับกิจกรรมในอนาคต

มิติที่ 3 การสื่อสารเกี่ยวกับการฟื้นฟูระบบ (Communications) กิจกรรมการฟื้นฟูจะได้รับการประสานงานกับฝ่ายภายในและภายนอก เช่นศูนย์ประสานงานผู้ให้บริการอินเทอร์เน็ต เจ้าของระบบที่ถูกโจมตี ผู้ที่ตกเป็นเหยื่อ และผู้ขาย

มิติที่ 4 กลยุทธ์ความคงทน (Robust Strategy) เป็นความสามารถของโซ่อุปทานที่จะดำเนินงานตามหน้าที่ต่อไปแม่ว่าจะมีความเสียหายบางอย่างเกิดขึ้นต่อโซ่อุปทาน โดยยังจะต้องสามารถรักษาสถานะของโซ่อุปทานให้มีความเสถียรได้เหมือนกับก่อนที่มีการเปลี่ยนแปลง และจะต้องสามารถทนทานได้มากกว่าการตอบสนอง

หมวดที่ 6 การจัดการความต่อเนื่อง (Continuity) – เป็นการดำเนินการตามขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง

มิติที่ 1 ความยั่งยืนของโซ่อุปทาน (Supply Chain Sustainability) การจัดการต่อผลกระทบด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม รวมถึงการส่งเสริมการกำกับดูแลกิจการที่ดีตลอดวัฏจักรชีวิตของสินค้าและบริการ

มิติที่ 2 ความเชื่อได้ของโซ่อุปทาน (Dependability of Supply Chain) ความสามารถในการให้บริการที่เชื่อถือได้อย่างสมเหตุสมผล ที่สามารถส่งมอบโดยระบบซึ่งเป็นพฤติกรรมที่สามารถรับรู้ได้โดยผู้ใช้งาน โดยความเชื่อถือได้ของโซ่อุปทานจะมีคุณลักษณะ (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

ข้อเสนอแนะ / ข้อคิดเห็น จากผู้เชี่ยวชาญ สำหรับส่วนที่ 1

ส่วนที่ 1 แนวทางการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

.....

.....

.....

.....

.....

ส่วนที่ 2 แนวทางการกำหนดตัวชี้วัดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)

หลักในการกำหนดตัวชี้วัดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ในการกำหนดตัวชี้วัดเพื่อใช้เป็นแนวทางในการบรรลุถึงระดับความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ใช้หลักการทำงานของวงล้อเดมิ่ง (The Deming Cycle) หรือ วัฏจักรวางแผน-ทำ-ตรวจสอบ-ปฏิบัติ (Plan-Do-Check-Act Cycle) อ้างใน ณัฏพันธ์ เขจรนันท์ (2549) ซึ่งวงล้อเดมิ่ง จะช่วยให้ การทำงานสามารถพัฒนาคุณภาพของงานอย่างต่อเนื่องโดยพิจารณาลดหรือกำจัดกิจกรรมที่ไม่ก่อให้เกิดประโยชน์ออกจากการปฏิบัติงาน โดยแยกงานที่ไม่ก่อให้เกิดคุณค่า (No Value) ออกจากงานที่สร้างคุณค่าให้แก่ผลิตภัณฑ์หรือบริการ ซึ่งจะช่วยให้กระบวนการปฏิบัติงานมีความกระชับและพัฒนาขึ้นอย่างต่อเนื่อง โดยแนวทางสำหรับการทำงานของวงจรเดมิ่งประกอบด้วย

1. การวางแผน (Plan) เป็นการกำหนดแผนงานที่สามารถประเมินความก้าวหน้าของงานได้อย่างเป็นรูปธรรม

2. การทำ า (Do) เป็นการดำเนินการตามแผนติดตาม และตรวจสอบความก้าวหน้าของกระบวนการ โดยเก็บรวบรวมข้อมูลตามระยะเวลาที่กำหนดเพื่อเป็นหลักฐานในการวิเคราะห์

3. การตรวจสอบ (Check) เป็นการตรวจสอบข้อมูลการดำเนินงานว่าจะสามารถบรรลุตามแผนที่กำหนดไว้หรือไม่ เพื่อพิจารณาปรับแผนหรือหยุดโครงการถ้าเกิดความไม่สอดคล้องระหว่างความเป็นจริงกับความต้องการ

4. การปฏิบัติ (Act) เป็นการตรวจสอบกระบวนการและจัดทำเอกสาร เพื่อนำแผนงานทีที่พัฒนาจนประสบความสำเร็จ ไปเป็นแนวทางและมาตรฐานในการปฏิบัติงานต่อไป ทำให้มีการพัฒนาคุณภาพของงานอย่างต่อเนื่อง

ดังนั้นผู้วิจัยได้ทำการกำหนดตัวชี้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยได้พิจารณาจากการนำเอากลุ่มงาน (Category) ของแต่ละหน้าที่งาน (Function) ไปทำการทบทวนวรรณกรรม เพื่อดำเนินการในการจัดทำตัวชี้วัดในแต่ละกลุ่มงาน จากผลของการดำเนินการดังกล่าวทำให้ผู้วิจัยสามารถกำหนดตัวชี้วัด ได้ตามกลุ่มงานแต่ละตัว สามารถสรุปได้ตารางที่ 1 และ ตารางที่ 2 ตามลำดับ

ตารางที่ 1 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	

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 2 : ตัวชี้วัดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล

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
	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 และมีการประเมินความเสี่ยงจากกระบวนการในการพิจารณาและอนุมัติการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศ ในทุกๆ ขั้นตอน

Category	ตัวชี้วัด	
Business Environment	6	มีการวางระบบการทำงานรวมไปถึงบทบาทหน้าที่ความรับผิดชอบทั้งในองค์กร ภาคธุรกิจ ตลอดจนเครือข่ายในโซ่อุปทานภายใต้โครงสร้างพื้นฐานที่สำคัญร่วมกันอย่างมีประสิทธิภาพและเหมาะสมกับงาน
	7	มีการสื่อสารในประเด็นของภารกิจ วัตถุประสงค์ และกิจกรรมขององค์กร ให้กับเครือข่ายในโซ่อุปทานภายใต้โครงสร้างพื้นฐานที่สำคัญให้รับทราบ และสามารถทำงานร่วมกันได้
	8	มีการกำหนดฟังก์ชั่นการพึ่งพาและฟังก์ชั่นที่สำคัญ (Dependencies and critical functions) เพื่อการคืนสภาพได้เพื่อรองรับการส่งมอบบริการที่สำคัญในทุก ๆ สถานะการทำงานทั้งหมดไม่ว่าจะอยู่ภายใต้การโจมตี ระหว่างการกู้คืน หรือในสภาวะปกติ
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
	16	มีการกำหนดให้มีการประเมินความเสี่ยงทางไซเบอร์ ด้านที่อาจส่งผลกระทบต่อข้อมูลลูกค้าอย่างสม่ำเสมอ โดยให้มีครอบคลุมถึงความเสี่ยงที่เกิดขึ้นจากการติดตั้งและการนำเทคโนโลยีใหม่มาใช้การออกผลิตภัณฑ์และบริการใหม่ 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 เพื่อให้สามารถระบุภัยคุกคามทางไซเบอร์ที่มี

Category	ตัวชี้วัด	
		โอกาสสร้างความเสียหายที่อาจเกิดขึ้นตลอดจนความเพียงพอของนโยบาย 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
Supply Chain Risk Management	24	มีการวางแผนในการจัดการความเสี่ยงของโซ่อุปทาน ที่ได้จัดทำไว้เป็นระเบียบวิธีการในการปฏิบัติ แต่ยังไม่ได้มีการวางแผนในขั้นตอนของการดำเนินการ
	25	มีการร่วมมือกันในการกำหนด จัดตั้ง ประเมิน จัดการ และตกลงร่วมกันต่อ กระบวนการในการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน จากผู้ที่มีส่วนได้ส่วนเสียขององค์กร
	26	มีการกำหนด และจัดลำดับความสำคัญในระบบสารสนเทศ องค์ประกอบ และบริการของซัพพลายเออร์และคู่ค้าที่เป็นบุคคลที่สาม และมีการประเมินโดยใช้กระบวนการในการประเมินความเสี่ยงทางไซเบอร์ของโซ่อุปทาน
	27	มีการออกแบบสัญญากับซัพพลายเออร์และคู่ค้าที่เป็นบุคคลที่สาม ด้วยการวัดผลที่เหมาะสมเพื่อให้บรรลุต่อวัตถุประสงค์ต่อการรักษาความปลอดภัยทางไซเบอร์และแผนในการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน
	28	มีการประเมินซัพพลายเออร์และคู่ค้าบุคคลที่สามอยู่เป็นประจำ โดยใช้การตรวจสอบ หรือการประเมินรูปแบบอื่น ๆ รวมถึงผลการทดสอบ เพื่อยืนยันว่าถึงการปฏิบัติตามภาระผูกพันตามสัญญา
	29	มีการวางแผนและทดสอบต่อการตอบสนองและการกู้คืน ที่นำไปใช้กับซัพพลายเออร์และผู้ให้บริการบุคคลที่สาม
Supply Chain Security Strategy	30	บริษัทได้มีการกำหนดให้มีกลยุทธ์ในการรักษาความปลอดภัยไซเบอร์ของโซ่อุปทาน รวมทั้งจัดให้มีการทบทวนกลยุทธ์ ที่ครอบคลุมถึงเทคโนโลยี นโยบาย และระเบียบวิธีปฏิบัติ ที่อยู่ภายใต้กลยุทธ์การจัดการความเสี่ยงขององค์กร
	31	บริษัทมีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ที่ครอบคลุมในเรื่องของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน การบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามไซเบอร์ และการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ที่สอดคล้องกับมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับกันทั่วไป
	32	บริษัทมีการกำหนดโครงการที่สนับสนุนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโซ่อุปทาน ที่สอดคล้องกับทิศทางของเทคโนโลยี หรือมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับโดยทั่วไป
	33	การกำหนดนโยบายรักษาความมั่นปลอดภัยทางด้านเทคโนโลยีของบริษัท มีการคำนึงถึงผลการวิเคราะห์หรือข้อมูลที่ได้มาจากองค์ความรู้ด้านภัยคุกคามไซเบอร์ของโซ่อุปทาน รวมถึงกระบวนการในการเชื่อมโยง ปรับปรุง และทบทวนนโยบายต้องเกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ทั้งหมดของบริษัท

Category	ตัวชี้วัด	
PROTECT		
Identity Management, Authentication and Access Control	34	บริษัทมีการกำหนดวิธีการเข้าถึงข้อมูลของพนักงานไว้ โดยแยกตามระดับหน้าที่ความรับผิดชอบของพนักงานแต่ละคน ซึ่งจะยังไม่ได้พิจารณาว่า ลำดับความสำคัญของข้อมูลเหมาะสมกับพนักงานในระดับใดมากนัก
	35	บริษัทมีการใช้วิธีการในการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากลในการพิสูจน์ตัวตนและการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สายและมีการเปลี่ยน Encryption Key สำหรับการเข้ารหัสอย่างสม่ำเสมอ และมีการออกแบบ และแบ่งระบบเครือข่ายภายในไว้เป็นโซนต่างๆ รวมถึงการวางมาตรการป้องกันตามระดับของความเสี่ยงจากการถูกโจมตีทางไซเบอร์
	36	บริษัทมีกระบวนการควบคุมและติดตามการเปลี่ยนแปลงการตั้งค่าอุปกรณ์คอมพิวเตอร์ รวมถึงการมีมาตรการในการควบคุม เพื่อป้องกันไม่ให้มีการติดตั้งโปรแกรมจากผู้ใช้งานที่ไม่ได้รับอนุญาต
	37	บริษัทมีการกำหนดสิทธิ์การเข้าถึงระบบงานและข้อมูลสลับให้พนักงาน โดยเป็นไปตามหลักการการแบ่งแยกหน้าที่ที่ดี โดยกำหนดขอบเขตหน้าที่ความรับผิดชอบตามความจำเป็น โดยมอบหมายให้ผู้มีอำนาจทำการอนุมัติ การเปลี่ยนแปลง การยกเลิก และการสอบทานสิทธิ์ ซึ่งต้องสอดคล้องกับระดับความเสี่ยงที่บริษัทได้กำหนดไว้
	38	บริษัทมีการแยกบัญชีผู้ใช้งานของผู้ดูแลระบบ เป็น 2 บัญชีผู้ใช้งาน คือ สำหรับการใช้งานทั่วไป และสำหรับการบริหารจัดการระบบที่จำเป็นต้องใช้สิทธิสูง หรือมีการอนุญาตให้ใช้งานสิทธิสูงตามความจำเป็น
	39	บริษัท มีการกำหนดมาตรการควบคุมในการพิสูจน์ตัวตนลูกค้าผู้ใช้งานผลิตภัณฑ์และบริการทางการเงินผ่านระบบ Internet ที่สอดคล้องตามระดับความเสี่ยง
	40	บริษัทมีมาตรการควบคุมการรักษาความมั่นคงปลอดภัยทางกายภาพเพื่อป้องกันการเข้าถึงอุปกรณ์เทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารของบริษัท 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 แต่ยังไม่มีแบบแผนใด ๆ โดยส่วนมากจะเป็นการอบรมเพื่อให้บุคลากรตระหนักถึงความสำคัญ รู้จัก และสามารถแก้ไขสถานการณ์ได้ในเบื้องต้น เมื่อต้องประสบกับเหตุการณ์การโจมตี หรือเมื่ออุปกรณ์ที่ใช้งาน

Category	ตัวชี้วัด	
		เกิดอาการผิดปกติจากภัยคุกคามทางไซเบอร์ 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 รวมทั้งยังมีเครื่องมือที่ใช้ในการป้องกันการเข้าถึง หรือนำข้อมูลลับออกจากบริษัท
	50	บริษัทมีการปกปิดหรือลบข้อมูลในส่วนสำคัญของลูกค้าก่อนนำไปใช้งาน เพื่อให้เป็นไปตามกฎหมาย หลักเกณฑ์ของทางการ และนโยบายของบริษัทที่ได้กำหนดไว้
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	บริษัทได้มาตรการให้มีการปฏิบัติตามนโยบายและข้อบังคับเกี่ยวกับสภาพแวดล้อมการทำงานจริง

Category	ตัวชี้วัด	
		สำหรับสินทรัพย์ขององค์กร
	57	บริษัทกำหนดระเบียบวิธีปฏิบัติการทำลายข้อมูลสารสนเทศ (Information Disposal) ครอบคลุมขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลให้สอดคล้องกับระดับความสำคัญของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การควบคุมการทำลายในลักษณะ Dual Control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดให้มีการจัดทำทะเบียนการทำลายข้อมูลสำคัญ 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 ไปที่พบว่าสินทรัพย์ดังกล่าวมีการสูญเสีย หรือหมดอายุการใช้งาน
	63	บริษัทมีมาตรการในการการบำรุงรักษาและซ่อมแซมสินทรัพย์ขององค์กร โดยจะต้องถูกดำเนินการและบันทึกด้วยเครื่องมือที่ได้รับการอนุมัติและควบคุม
	64	บริษัทมีมาตรการสำหรับการบำรุงรักษาสินทรัพย์องค์กรโดยระยะไกล โดยจะต้องได้รับการอนุมัติบันทึกและดำเนินการในลักษณะที่ต้องสามารถป้องกันต่อการเข้าถึงที่ไม่ได้รับอนุญาต
Protective Technology	65	บริษัทมีการป้องกันภัยคุกคามทางไซเบอร์ โดยในเบื้องต้นได้ใช้โปรแกรม Anti-Virus ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ในบริษัท แต่ยังไม่ได้มีการจัดการไปถึงอุปกรณ์ที่พนักงานนำมาใช้งานเอง รวมไปถึงเครือข่ายต่างๆ ที่ยังไม่สามารถดำเนินการป้องกันได้อย่างทั่วถึง
	66	บริษัทมีขอบเขตการตรวจสอบการประเมินความมั่นคงปลอดภัย การจัดเก็บ และรับส่งข้อมูลที่มีความสำคัญของบริษัท ความเพียงพอของระบบการบริหารจัดการและควบคุมความเสี่ยงทางไซเบอร์ การแลกเปลี่ยนข้อมูล รวมไปถึงความสามารถในการรับมือต่อเหตุการณ์ผิดปกติทางไซเบอร์ว่ามีความสอดคล้องกับระดับความเสี่ยงทางไซเบอร์ที่กำหนดไว้ในระดับบริษัท
	67	บริษัทมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลแบบพกพา ให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น รวมทั้งมีมาตรการควบคุมเพื่อป้องกันการถ่ายโอนข้อมูลที่เป็นความลับ การรั่วไหลของข้อมูลจากอุปกรณ์ที่สูญหายหรือถูกโจรกรรม และยังมีกระบวนการในการทำลายข้อมูลจากอุปกรณ์ที่ไม่ได้ใช้งานแล้ว

Category	ตัวชี้วัด	
	68	บริษัทมีมาตรการเชิงเทคนิคหรือเครื่องมือเพื่อใช้ป้องกันการเชื่อมต่อ หรือการเข้าถึงระบบเครือข่ายภายในของบริษัท โดยอุปกรณ์ที่ไม่ได้รับอนุญาต
	69	บริษัทแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกออกจากระบบเครือข่ายภายในบริษัท ออกจากกันอย่างชัดเจน
	70	บริษัทมีอุปกรณ์ป้องกันเครือข่ายติดตั้งไว้ในระบบเครือข่ายไร้สายเพื่อป้องกันการเข้าถึงเครือข่ายภายใน และจำกัดการติดต่อสื่อสารที่ไม่ได้รับอนุญาต (Unauthorized Traffic)
	71	บริษัทใช้วิธีการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากลในการพิสูจน์ตัวตนและการรับส่งข้อมูลผ่านระบบเครือข่ายไร้สาย
	72	บริษัทแบ่งระบบเครือข่ายภายในเป็นโซนต่างๆ (Network Segmentation) และวางมาตรการการป้องกันตามระดับความเสี่ยงจากการถูกโจมตีทางไซเบอร์
Privacy	73	บริษัทมีการวางแผนในเรื่องการใช้งานระบบ สำหรับพนักงานและบุคลากรโดยจัดตามลำดับความสำคัญของการดำเนินงาน 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	บริษัทมีมาตรการควบคุมการป้องกัน Malware และ Man-in-the-Middle ในขั้นตอนการพิสูจน์ตัวตนของลูกค้าในการทำธุรกรรมที่มีความเสี่ยงสูงตามที่บริษัทกำหนดว่าเป็นธุรกรรมที่มีความเสี่ยงสูงผ่านเครือข่าย Internet
DETECT		
Anomalies and Events	79	บริษัทมีการดำเนินการต่อเหตุการณ์ผิดปกติที่เกิดขึ้น แบบแก้ไขสถานการณ์เป็นกรณี ๆ ไป และยังไม่มีการวางแผนไว้อย่างเป็นระบบ และยังไม่มีบุคลากรที่คอยเฝ้าระวังหรือตรวจสอบความผิดปกติจากภัยคุกคามทางไซเบอร์
	80	บริษัทมีกระบวนการหรือระบบที่สามารถเฝ้าระวังหรือติดตามพฤติกรรมการเข้าใช้งานระบบที่น่าสงสัย หรือเข้าข่ายเป็นการทุจริตในขั้นตอนการพิสูจน์ตัวตนพนักงาน และบุคคลภายนอก และแจ้งเตือนผู้ที่รับมอบอำนาจอัตโนมัติเพื่อดำเนินการแก้ไขอย่างทันท่วงที
	81	บริษัทจัดให้มีการเก็บบันทึกเหตุการณ์อย่างมั่นคงปลอดภัย ถึงการบันทึกการเข้าถึง (Access Log) การบันทึกการดำเนินงาน (Activity Log) ที่สำคัญ บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log) และบันทึกด้านการรักษาความปลอดภัย (Security Event Log) โดยสามารถดู

Category	ตัวชี้วัด	
		ย้อนหลังได้ด้วยวิธีการที่ปลอดภัย
	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
	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	บริษัทมีกระบวนการหรือมาตรการแจ้งเตือนเมื่อพบเหตุการณ์ที่มีโอกาสเป็นการโจมตีทางไซเบอร์เพื่อให้หน่วยงาน ผู้รับผิดชอบในการเฝ้าระวัง การรักษาความมั่นคงปลอดภัยทราบอย่างทันการณ์
	90	บริษัทมีเครื่องมือและกระบวนการในการตรวจจับและแจ้งเตือน เมื่อตรวจพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ เพื่อรายงานให้หน่วยงานหรือผู้ที่มีหน้าที่รับผิดชอบในการรับมือเหตุการณ์ผิดปกติทางไซเบอร์ทราบและดำเนินการแก้ไข
	91	บริษัทมีเครื่องมือหรือกระบวนการในการตรวจจับการพยายามบุกรุกเครือข่าย มีเครื่องมือตรวจจับเหตุการณ์ผิดปกติ (Incident) มีเครื่องมือที่สามารถตรวจจับเมื่อมีการเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ และมีเครื่องมือตรวจจับและแจ้งเตือนเหตุการณ์ตามความเสี่ยงของทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยสามารถแจ้งเตือนไปยังหน่วยงานหรือผู้รับผิดชอบที่เกี่ยวข้องทันทีให้สามารถดำเนินการรับมือได้อย่างรวดเร็ว (Proactive)
	92	บริษัทมีเครื่องมือเพื่อวิเคราะห์เชื่อมโยงข้อมูลเหตุการณ์ผิดปกติจากแหล่งต่างๆ ของบริษัท แบบ Real Time จากอุปกรณ์เครือข่าย หรืออุปกรณ์รักษาความปลอดภัยเครือข่ายของระบบที่สำคัญ และมีเครื่องมือที่สามารถตรวจจับภัยคุกคามจากภายในและภายนอกที่เชื่อมโยงในระดับองค์กร รวมถึงแจ้งเตือนหน่วยงานที่รับผิดชอบ และหน่วยงานที่เกี่ยวข้อง
Cyber Intelligence	93	บริษัทมีการมอบหมายให้มี ผู้ทำหน้าที่บริหารจัดการเหตุการณ์ผิดปกติเมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์ของโซ่อุปทานเกิดขึ้น และผู้ทำหน้าที่ติดตามและวิเคราะห์ Cyber Threat Intelligence ต้องมีการทำงานอย่างใกล้ชิดและมีบูรณาการ

Category	ตัวชี้วัด	
	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
	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 และติดตามเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้นและมีกระบวนการติดต่อผู้รับผิดชอบในการวิเคราะห์ รับมือภัยคุกคาม และตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

Category	ตัวชี้วัด	
Mitigation	106	บริษัทยังมีมาตรการที่ใช้ในการบรรเทาต่อภัยคุกคามทางไซเบอร์ที่ยังมีความไม่ชัดเจน ส่วนใหญ่จะเป็นการดำเนินการเมื่อเกิดเหตุการณ์ผิดปกติขึ้น
	107	บริษัทจัดให้มีกระบวนการการจำกัดการเข้าถึง ยกเลิกการใช้งาน ทำลาย หรือทดแทนทรัพย์สินด้านเทคโนโลยีสารสนเทศ ที่มีผลกระทบจากเหตุการณ์ผิดปกติทางไซเบอร์ รวมถึงการวิเคราะห์เหตุการณ์ผิดปกติทางด้านความมั่นคงปลอดภัยตั้งแต่ช่วงแรกเมื่อตรวจพบเหตุการณ์บุกรุก เพื่อตอบสนองและลดผลกระทบต่อเหตุการณ์ดังกล่าวที่อาจเกิดขึ้น
	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 ที่จะสามารถเกิดขึ้นได้ในโซ่อุปทานด้วยความรวดเร็ว
	112	บริษัทมีขั้นตอนในการตัดสินใจที่จะกระทำการใด ๆ เมื่อพบกับภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานด้วยความรวดเร็ว
	113	บริษัทมีความสามารถในการตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานด้วยความรวดเร็ว
	114	บริษัทมีกระบวนการที่สามารถจะปรับเปลี่ยนวิธีการในการดำเนินธุรกรรมต่าง ๆ ภายในโซ่อุปทานได้อย่างรวดเร็ว เมื่อเผชิญกับภัยคุกคามที่เข้ามาโจมตีการทำงานในบริษัท
RECOVER		
Recovery Planning	115	มีแผนการกู้คืนต่อเหตุการณ์ผิดปกติที่ดำเนินการอยู่ยังสามารถจัดการต่อภัยคุกคามทางไซเบอร์ได้อยู่ในระดับหนึ่ง
	116	บริษัทมีแผนการกู้คืนต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยการจัดทำต้องครอบคลุมกระบวนการดังนี้ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) การประเมินความเสี่ยง (Risk Analysis) การวางกลยุทธ์สำหรับแผนฉุกเฉิน การจัดทำแผนฉุกเฉิน การสื่อสารและฝึกอบรมให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก การทดสอบปรับปรุงและสอบทานแผนฉุกเฉิน โดยการจัดการแผนฉุกเฉินดังกล่าว ต้องสามารถดำเนินการได้ทั้งในระหว่างและหลังจากที่ถูกโจมตี
Improvements	117	บริษัทได้มีการนำสิ่งที่ได้เรียนรู้ (Lessons Learned) จากการถูกโจมตีหรือเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น ทั้งภายในและภายนอกบริษัท มาปรับปรุงแผนการกู้คืนต่อเหตุการณ์ผิดปกติทางไซเบอร์
Communications	118	บริษัทจัดให้มีการสื่อสารเรื่องความปลอดภัยเพื่อสร้างความมั่นใจต่อการดำเนินงานให้แก่บุคลากร

Category	ตัวชี้วัด	
		ภายในรับทราบ
	119	บริษัทจัดให้มีการประชาสัมพันธ์ในมาตรการ และกิจกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้แก่หน่วยงานภายในและภายนอกบริษัท ลูกค้า ซัพพลายเออร์ และผู้มีส่วนได้เสียเพื่อสร้างความเชื่อมั่น และน่าเชื่อถือ
	120	บริษัทมีกระบวนการในการเรียกชื่อเสียงของบริษัทกลับคืนมาหลังจากที่ได้รับผลจากเหตุการณ์ผิดปกติทางไซเบอร์ไว้อย่างชัดเจน
Robust Strategy	121	บริษัทมีกระบวนการในการกลับเข้าสู่สภาวะปกติได้อย่างรวดเร็วเมื่อถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานในโซ่อุปทานเกิดการหยุดชะงัก
	122	บริษัทมีความสามารถที่จะปรับเปลี่ยนกระบวนการไปสู่สภาวะการทำงานใหม่ ๆ หลังจากการถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานเกิดการหยุดชะงัก
	123	บริษัทมีมาตรการเกี่ยวกับการเตรียมความพร้อมด้านการจัดการทางการเงินไว้เป็นอย่างดี ต่อการถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำการดำเนินงานเกิดการหยุดชะงัก
	124	บริษัทสามารถที่จะดำเนินธุรกรรมกับคู่ค้าในโซ่อุปทานต่อไปได้ แม้จะถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำให้การดำเนินงานเกิดการชะงัก
	125	บริษัทสามารถที่จะรักษา ควบคุม หน้าที่ต่าง ๆ ในโซ่อุปทาน หลังจากที่ถูกโจมตีจากภัยคุกคามทางไซเบอร์ ที่ทำให้การดำเนินงานเกิดการชะงัก
CONTINUITY		
Supply Chain Sustainability	126	บริษัทได้มีการตั้งคณะกรรมการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดยมีบทบาทหน้าที่ในการกำหนดกลยุทธ์ นโยบาย และแผนงานเทคโนโลยีสารสนเทศ ให้ครอบคลุมความมั่นคงปลอดภัยไซเบอร์และสอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัท ตลอดทั้งโซ่อุปทาน รวมทั้งดูแลติดตามการดำเนินงาน ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์
	127	บริษัทมีผู้บริหารที่เห็นความสำคัญและจำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยได้เข้ามามีบทบาทและหน้าที่ความรับผิดชอบในการกำหนดและอนุมัติกลยุทธ์ นโยบาย รวมทั้งกำกับดูแล และติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้สอดคล้องกับการดำเนินธุรกรรมในโซ่อุปทาน
	128	บริษัทมีการจัดสรรงบประมาณที่เพียงพอ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน ที่ครอบคลุม ถึงระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐาน (Infratructure) รวมทั้งบุคลากร เครื่องมือและบริการที่เกี่ยวข้อง
Dependability of Supply Chain	129	บริษัทมีการกำหนดถึงความพร้อมต่อกระบวนการการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน โดยระบบจะต้องสามารถเปิดใช้งานได้ทันทีเมื่อมีการร้องขอจากผู้ใช้งาน
	130	บริษัทมีการกำหนดความน่าเชื่อถือต่อการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน โดยระบบจะต้องสามารถจัดการได้ตามความคาดหวังหรือความต้องการของผู้ใช้งาน
	131	บริษัทมีการกำหนดถึงความปลอดภัยต่อการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน โดยระบบจะต้อง สามารถแสดงให้เห็นได้ถึงความเสี่ยหายที่อาจจะเกิดขึ้น
	132	บริษัทมีการกำหนดถึงความสามารถในการป้องกันตัวเองจากการโจมตีที่จะส่งผลถึงความมั่นคง

Category	ตัวชี้วัด	
		ปลอดภัยทางไซเบอร์ของโซ่อุปทาน จากผู้บุกรุกที่เจตนาจะเข้ามาโจมตีหรือโดยไม่ได้ตั้งใจ
	133	บริษัทมีการกำหนดถึงความสามารถในการต่อต้าน และกู้คืนจากเหตุการณ์ที่เกิดจากการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้หน่วยงานเสียหาย ต่อโซ่อุปทาน โดยเมื่อถูกโจมตีแล้วระบบจะยังต้องสามารถดำเนินการต่อไปได้
	134	บริษัทมีการกำหนดถึงความสามารถการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทาน ที่จะต้องแสดงให้เห็นถึงขอบเขตที่ระบบสามารถปรับให้เข้ากับความต้องการใหม่
Business Continuity Plan	135	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถทำให้บริษัทรวมไปถึงผู้ถือหุ้นมีความเข้าในถึงระดับของความเสี่ยงที่สามารถทำให้กิจการดำเนินต่อไปได้
	136	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถนำมาใช้จัดการธุรกรรมต่าง ๆ ในโซ่อุปทานได้อย่างมีประสิทธิภาพ
	137	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถสร้างความเชื่อถือให้กับผู้ถือหุ้นที่มีต่อบริษัทได้
	138	บริษัทมีแผนความต่อเนื่องทางธุรกิจสามารถที่ทำให้เกิดแผนในการบริหารธุรกิจ และจะสามารถช่วยป้องกันทรัพย์สินของบริษัท รวมไปถึงข้อมูลที่สำคัญของบริษัทพร้อมทั้งยังสามารถที่จะฟื้นฟูปัญหาที่เกิดขึ้นให้กลับมาทำงานได้อย่างมีประสิทธิภาพตามเดิม
	139	บริษัทมีแผนความต่อเนื่องทางธุรกิจทำให้เกิดความสามารถทางการแข่งขันได้
Business Continuity Assessment	140	บริษัทได้ดำเนินการจัดให้มีการประเมินความต่อเนื่องทางธุรกิจ โดยทำการตรวจสอบด้านการรักษาความมั่นคงความปลอดภัยไซเบอร์ โดยดำเนินการติดตามอย่างสม่ำเสมอเพื่อป้องกันและรับมือต่อภัยคุกคามไซเบอร์ได้อย่างทันท่วงที
	141	บริษัทได้จัดให้มีหน่วยงานที่มีหน้าที่และความรับผิดชอบในการประเมินความต่อเนื่องทางธุรกิจและจัดการความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องกับการปฏิบัติงานประจำ และงานที่ได้รับมอบหมาย รวมทั้งติดตาม จัดทำรายงาน เฝ้าระวังภัยคุกคาม และศึกษาแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการจัดการความต่อเนื่องทางธุรกิจ โดยนำเสนอรายงานต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง
	142	บริษัทมีขอบเขตการตรวจสอบกระบวนการการจัดทำการประเมินความต่อเนื่องทางธุรกิจที่บริษัทยอมรับได้ โดยมีความเหมาะสมกับขนาดและความซับซ้อนของการดำเนินธุรกิจ รวมไปถึงการสอบทานระดับความของต่อเนื่องทางธุรกิจกับผลที่ได้ควบคู่กับประเมินความพร้อมด้าน Cyber Resilience

ข้อเสนอแนะ / ข้อคิดเห็น จากผู้เชี่ยวชาญ สำหรับส่วนที่ 2

ส่วนที่ 2 แนวทางการกำหนดตัวชี้วัดของตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)

.....

.....

.....

.....

.....

.....

ส่วนที่ 3 แนวทางการกำหนดระดับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains)

การกำหนดระดับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ทำการนิยามระดับของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลไว้ โดยทำการนิยามไว้ดังตารางที่ 3

ตารางที่ 3 นิยามของระดับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

Level	Description	Characteristics
1	**ระดับเริ่มต้น (Initial Level)** เป็นระดับที่บริษัทต่าง ๆ ต้องจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยอาศัยความสามารถของบุคลากรเพียงอย่างเดียว ซึ่งมีลักษณะของการทำงานที่ยังไม่เป็นทางการมากนัก ยังไม่มีการควบคุมที่ดี ไม่มีการ	1. มีหลักฐานเอกสารที่บ่งบอกว่า องค์กรหรือบริษัทมีการกล่าวถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล และความต้องการที่จะมีอยู่ แต่ยังไม่มีการนำเอามาตรฐานใด ๆ มาใช้ในกระบวนการ 2. ไม่มีกฎเกณฑ์และการสื่อสารภายในบริษัทในด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่เป็นกระบวนการที่เป็นมาตรฐาน 3. เมื่อเกิดปัญหา ก็จะดำเนินการแก้ปัญหาเฉพาะกรณี ๆ ไป จะเป็นการประชุมกันภายในองค์กร เพื่อดำเนินการจัดการ

Level	Description	Characteristics
	วางแผนงานที่เป็นระบบ จึงทำให้ไม่สามารถประเมินคุณภาพในการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่เกิดขึ้นว่าจะมีคุณภาพดีหรือไม่	4. มีกระบวนการที่จัดการต่อความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ไม่สามารถคาดเดาได้ (unpredictable process) 5. ไม่มีการกำหนดขั้นตอนในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลในองค์กร 6. ยังไม่มีระบบสารสนเทศที่ใช้ในการจัดการที่ดีพอในองค์กร 7. การอบรมพนักงานยังไม่มีประสิทธิภาพ หรือบางทีก็ยังไม่มีการอบรมใด ๆ เลย
2	**ระดับจัดการเบื้องต้น (Repeatable Level)** ในระดับนี้มีแนวทางในการจัดการต่อภัยคุกคามทางไซเบอร์**ของโซ่อุปทานดิจิทัล**เบื้องต้น มีการวางแผนการทำงานอย่างเป็นระบบ มีการจัดทำเอกสาร สามารถตรวจสอบ และนำไปปฏิบัติได้ บริษัทต่าง ๆ สามารถเข้าสู่ระดับนี้ได้ จะสามารถจัดการต่อปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีลักษณะแบบเดียวกันให้ประสบผลสำเร็จได้เช่นเดียวกับภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่สามารถจัดการได้สำเร็จไปแล้ว	1. เริ่มมีการทำความเข้าใจในบริบทขององค์กร และมีความตระหนัก ต่อความสำคัญในการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 2. มีการกำหนดความจำเป็นและความคาดหวังขององค์กรต่อการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 3. มีการนำเอาระบบสารสนเทศ การพยากรณ์ และตัวชี้วัดเบื้องต้นมาใช้สำหรับการจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 4. เริ่มต้นการพัฒนาในการกำหนดมาตรฐาน กิจกรรมและตัวชี้วัดด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล 5. มีการดำเนินการในด้านการวางแผน การส่งมอบ การตรวจสอบ รวมไปถึงการจัดทำเอกสาร ที่เกี่ยวกับกระบวนการ นโยบาย และขั้นตอนในการดำเนินงานในด้านการจัดการต่อปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 6. มีการนำเอานโยบาย แผนการไปใช้ปฏิบัติ เพื่อให้บรรลุผลของการจัดการปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 7. มีการตรวจสอบ และกำกับดูแล แนวทางในการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล 8. มีการให้ความสำคัญต่อปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยกิจกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลได้มีการกำหนดขึ้นอย่างเป็นทางการ ซึ่งอาจจะต้องมีการเปลี่ยนแปลงกระบวนการในการดำเนินงานขององค์กร ที่ดำเนินการโดยฝ่ายผู้บริหารขององค์กร 9. การเลือกกระบวนการด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลถูกกำหนดเพื่อ ปรับปรุง และ ควบคุมกระบวนการหลักขององค์กร และจะมีการวางแผนการตรวจสอบ

Level	Description	Characteristics
		การลงทุนอย่างมีประสิทธิภาพ โดยจะทำการดำเนินการในบริบทตามกรอบแนวคิดโครงสร้างพื้นฐานทางด้านไอทีขององค์กรหรือบริษัทนั้น ๆ 10. มีการกำหนดขั้นพื้นฐานเกณฑ์ในการวัดความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล รวมถึงเทคนิควิธีสำหรับการประเมิน แต่อย่างไรก็ตามวิธีการดังกล่าวก็ยังไม่ได้ถูกปรับใช้ทั่วทั้งองค์กรหรือบริษัท 11. องค์กรยังไม่มีการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลอย่างเป็นรูปแบบ รวมถึงไม่มีการสื่อสารเกี่ยวกับการกำกับดูแลและแบ่งความรับผิดชอบให้แต่ละบุคคล 12. เครื่องมือที่จะนำมาใช้สำหรับการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล จะยังมีข้อจำกัดในการถูกเลือกและนำไปใช้ เนื่องจากยังขาดผู้เชี่ยวชาญ โดยจะสามารถทำได้เพียงการนำมาใช้วัดในเรื่องความมั่นคงปลอดภัยได้เท่านั้น แต่อาจจะยังไม่ได้ถูกนำมาใช้แบบสมบูรณ์
3	**ระดับที่มีการกำหนดกระบวนการขึ้นอย่างชัดเจน (Defined Level)** ในระดับนี้เป็นการพัฒนาเพิ่มขึ้นจาก Repeatable Level การเข้าสู่ระดับบริษัทต่าง ๆ จะต้องมีการกำหนดแนวทางในการปฏิบัติงานด้านการจัดทำเอกสารและกำหนดมาตรฐานในการปฏิบัติงาน ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลได้อย่างเหมาะสม โดยมาตรฐานดังกล่าวต้องมีแนวปฏิบัติแบบเดียวกันทั้งองค์กร นั้นคือ องค์กรเริ่มมีระเบียบวิธีการปฏิบัติงานเป็นมาตรฐานของตนเอง	1. มีการยอมรับในความสำคัญของการป้องกันภัยคุกคามทางไซเบอร์ ของโซ่อุปทานดิจิทัล มีการกำหนดค่าพื้นฐานของตัวชี้วัด มีการเชื่อมโยงระหว่างผลลัพธ์กับสิ่งที่มีอยู่ โดยได้ทำการกำหนดไว้ให้เป็นเอกสารที่ชัดเจนมากขึ้น 2. มีการบูรณาการในนโยบาย กระบวนการ ระบบสารสนเทศ หน่วยงาน รวมไปถึงกิจกรรมที่เป็นแนวทางในการปฏิบัติให้มีรูปแบบ หรือมีมาตรฐานมากขึ้น โดยกำหนดเป็นกลยุทธ์ การวางแผนการดำเนินงาน รวมไปถึงกระบวนการตรวจสอบ ขั้นตอนของกระบวนการให้มีความเป็นมาตรฐานมากขึ้น มีการสื่อสารที่เป็นขั้นตอนและการอบรมที่มีแบบแผน 3. มีการพัฒนาระบบงานในการรักษาความมั่นคงปลอดภัยให้มีมาตรฐานในการปฏิบัติงาน โดยอาจจะมีการนำหลักการที่เป็นมาตรฐาน เช่น ISO ต่าง ๆ เข้ามาใช้ในการปฏิบัติการ 4. มีการกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล และแผนการในการบรรลุวัตถุประสงค์นั้น 5. มีการกำหนดถึงบทบาทหน้าที่ความรับผิดชอบของหน่วยงานและตัวบุคคล 6. ตัวชี้วัดของกิจกรรมทั้งหมดจะถูกบันทึก และติดตาม ซึ่งจะ

Level	Description	Characteristics
		นำไปสู่การปรับปรุงต่อไป การวัดต่าง ๆ มีแบบแผนมีมาตรฐาน แต่การนำปฏิบัตินั้นยังไม่มีความชำนาญนัก บุคคลจะได้รับการฝึกอบรมเพื่อเรียนรู้การใช้เครื่องมือในการวัดตามมาตรฐาน จะยังไม่มีการวิเคราะห์รากฐานของปัญหา โดยจะทำเป็นครั้งคราวเท่านั้น
4	**ระดับมีการจัดการ (Managed Level)** เป็นการพัฒนาเพิ่มขึ้นจาก Defined Level ลักษณะการปฏิบัติในระดับนี้ผู้จัดทำต้องมีการรวบรวมข้อมูลรายละเอียดการปฏิบัติงานต่างๆ ที่เกิดขึ้นไว้ในรูปของสถิติ (Statistical Process Control) เพื่อนำข้อมูลนั้นมาใช้ในการศึกษาวิเคราะห์ผลการทำงาน สามารถวัดผล และควบคุมกระบวนการในการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล	1. มีการมีความเข้าใจเรื่องของความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยเกิดจากการอบรมอย่างมีแบบแผน ทำให้มีความเข้าใจที่ชัดเจน มีการกำหนดความรับผิดชอบ และการตรวจสอบที่มีมาตรฐาน 2. กระบวนการทางด้านการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล มีความสอดคล้องกับกลยุทธ์ขององค์กร การปรับปรุงกระบวนการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลเป็นไปตามหลักความเข้าใจในเชิงปริมาณ มีการนำหลักการทางสถิติมาใช้ในการวิเคราะห์ผลการทำงาน โดยสามารถประเมิน วัดผลและควบคุมกระบวนการในการดำเนินงาน และมีความเป็นไปได้ที่จะตรวจสอบหรือวัดผลการปฏิบัติงาน 3. ผู้มีส่วนได้ส่วนเสียในทุก ๆ กระบวนการจะมีความตระหนักในความเสี่ยงรวมถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ในเชิงคุณค่าที่จะได้รับการจัดการรวมทั้งมีการกำหนดเกณฑ์ความคลาดเคลื่อนของกระบวนการที่ต้องดำเนินการ 4. มีกระบวนการมากมายที่ต้องทำแต่ไม่ใช่ว่าทุกกระบวนการจะเป็นการทำงานที่ประสิทธิภาพเสมอไป บางครั้งกระบวนการอาจจะต้องปรับปรุงมีการวิเคราะห์รากของปัญหาเป็นไปตามมาตรฐาน 5. เริ่มเห็นความสำคัญของกระบวนการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) และมีการปฏิบัติในประเด็นนี้ผู้เชี่ยวชาญภายในองค์กรมีส่วนร่วมเพื่อแลกเปลี่ยนเรียนรู้ถึงความต้องการต่าง ๆ
5	**ระดับปรับปรุงให้เหมาะสมที่สุด (Optimizing Level)** เป็นระดับที่ได้นำเอาหลักการจัดการคุณภาพ (Continuous Process Improvement) มาใช้เพื่อป้องกันไม่ให้เกิด	1. มีการนำเอาหลักการของการจัดการคุณภาพมาใช้ในการกระบวนการด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลในองค์กร โดยพัฒนาให้อยู่ในระดับที่เป็นการปฏิบัติที่ดีที่สุด ด้วยพื้นฐานที่มาจากการปรับปรุงอย่างต่อเนื่องและเป็นตัวแบบให้กับองค์กรอื่น 2. การฝึกอบรมและการสื่อสารได้รับการสนับสนุน จากผู้บริหาร

Level	Description	Characteristics
	ข้อบกพร่องในการปฏิบัติงานและนำไปสู่การพัฒนาอย่างต่อเนื่อง รวมถึงเพื่อให้บริษัทต่าง ๆ สามารถปรับเปลี่ยนตัวเองให้สอดคล้องกับการเปลี่ยนแปลงทางด้านเทคโนโลยีได้	มากขึ้น 3. นโยบายต่าง ๆ ที่นำไปใช้ในองค์กรมีการปรับใช้ได้อย่างรวดเร็วและสนับสนุนต่อความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลอย่างเต็มที่ 4. ปัญหาและความเบี่ยงเบนที่เกิดขึ้นถูกวิเคราะห์จากรากของปัญหาทั้งหมด โดยการปฏิบัติที่มีประสิทธิภาพ ในระดับนี้จะได้มีการนำเอาเทคโนโลยี สารสนเทศมาใช้เพื่อขยาย บูรณาการ และปรับให้เป็นการทำงานที่เป็นอัตโนมัติ รวมถึงมีเครื่องมือหลาย ๆ เครื่องมือเพื่อปรับปรุงคุณภาพและประสิทธิภาพ 5. มีการกำหนดความเสี่ยง และผลลัพธ์ที่เกิดขึ้นว่ามีอะไรบ้าง รวมถึงความสมดุลของการสื่อสารระหว่างองค์กร 6. มีการกำหนดผู้เชี่ยวชาญจากภายนอกเพื่อใช้ในการตรวจสอบการประเมินตนเองและมีการสื่อสารเกี่ยวกับความคาดหวังด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ถูกขยายภายในองค์กร 7. มีเทคโนโลยีที่เหมาะสมเพื่อที่จะสนับสนุนการวัด การวิเคราะห์ การติดต่อสื่อสารและการอบรมในด้านความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลขององค์กรและมีการเชื่อมโยงอย่างมีกลยุทธ์

เมื่อได้ทำการวิเคราะห์และสังเคราะห์ “ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Cyber-Resilient Supply Chain Model)” ตามรูปที่ 1 เพื่อพัฒนาให้เป็น “ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Capability Maturity Model for Cyber-Resilient Supply Chain)” ตามในรูปที่ 2

Capability Maturity Model for Cyber-Resilient Supply Chain

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

รูปที่ 2_ ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ในการจัดการความต่อเนื่องทางธุรกิจดิจิทัลของโซ่อุปทานดิจิทัลนั้น จะมีองค์ประกอบและตัวชี้วัดภายในที่แสดงถึงระดับวุฒิภาวะความสามารถของวิสาหกิจขนาดกลางและขนาดย่อม ในการตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีและความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งคะแนนที่ได้รับจากการประเมินผลของบุคลากรของวิสาหกิจขนาดกลางและขนาดย่อมในฐานะตัวแทนองค์กร ที่ผ่านทั้ง 32 มิติการดำเนินงาน ทำให้สามารถแสดงถึงระดับวุฒิภาวะความสามารถสำหรับการคืนสภาพได้ด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลได้ดังตารางที่ 4 นี้

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

ตารางที่ 4 ระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

ระดับวุฒิภาวะความสามารถ Capability Maturity Level	**ตัวชี้วัดระดับวุฒิภาวะความสามารถ Maturity Indicator Level**
Level 1 : Initial	MIL1: มีการกำหนดนโยบาย / จัดทำแผน วัตถุประสงค์และแผนการดำเนินงาน MIL2: มีเอกสาร กระบวนการ ขั้นตอน เครื่องมือที่เป็นรูปแบบมากขึ้น MIL3: มีการประกาศ/สื่อสาร/อบรม ทั้งภายในและภายนอกองค์กร
Level 2 : Repeatable	MIL4: มีการนำเอานโยบาย/แผนที่ได้วางไว้ไปสู่การปฏิบัติ 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

<u>ข้อเสนอแนะ / ข้อคิดเห็น จากผู้เชี่ยวชาญ สำหรับส่วนที่ 3</u>

ส่วนที่ 3 แนวทางการกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains)

.....

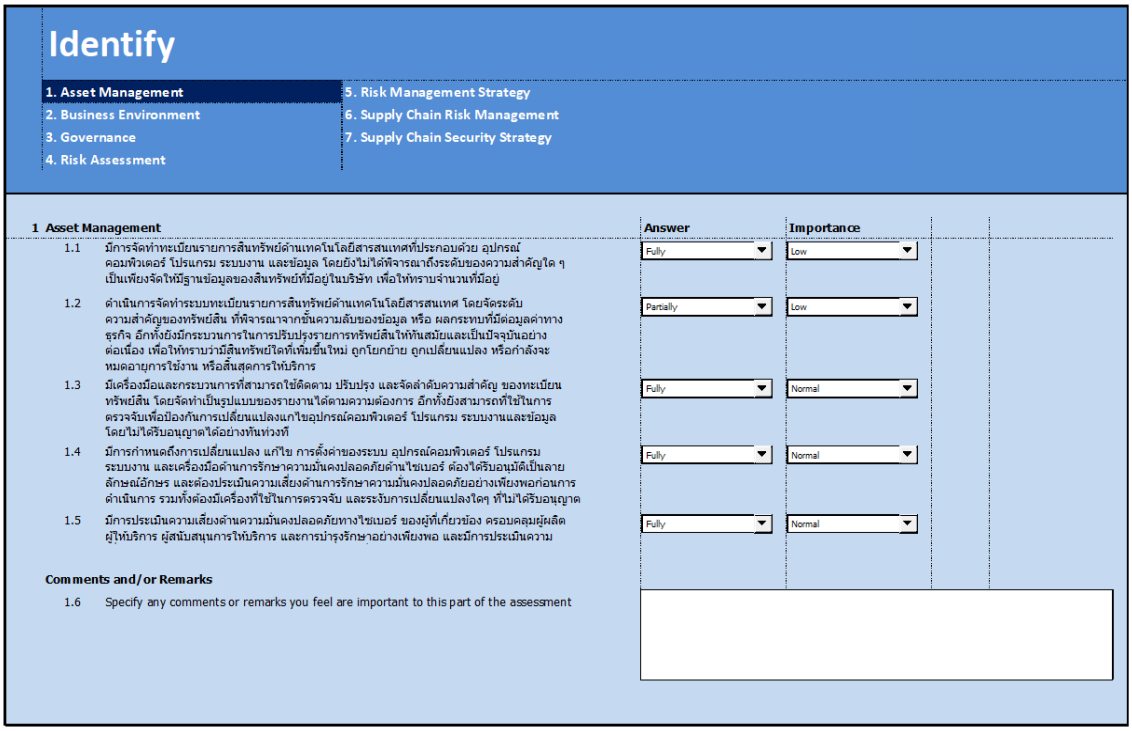
.....

.....

.....

ส่วนที่ 4 แนวทางการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

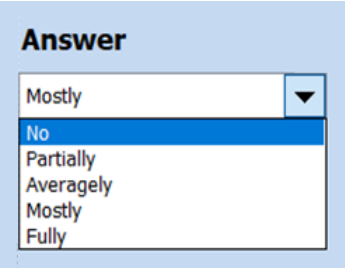
การประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้กำหนดให้ผู้ประเมินทำการประเมินประเมินให้เป็นไปตามตัวชี้วัดแต่ละตัว ตัวอย่างของการประเมินผู้วิจัยเสนอแนวทาง โดยแสดงดังรูปที่ 3



รูปที่ 3 การประเมินระดับวุฒิภาวะของตัวชี้วัด

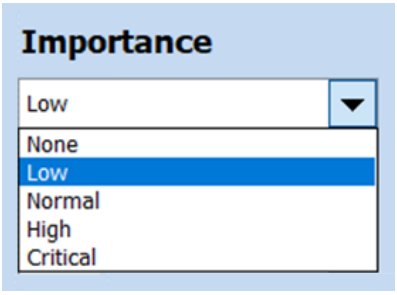
เกณฑ์การประเมินตัวชี้วัด ผู้วิจัยได้มีเกณฑ์ในการกำหนดการตอบของผู้ที่จะทำการประเมินดังต่อไปนี้

1. Answer การประเมินตามตัวชี้วัดในแต่ละมิติ โดยแต่ละตัวชี้วัดจะให้ผู้ประเมินพิจารณาคะแนน 5 ระดับ โดยแต่ละระดับจะใช้เกณฑ์การให้คะแนนระดับการปฏิบัติ ตามตัวชี้วัดตามมาตรฐาน ISO/IEC 15504 โดยมี รายละเอียดระดับความสำเร็จ ในการปฏิบัติตามตัวชี้วัด โดยจะหมายถึง การประเมินว่า องค์กรได้มีการปฏิบัติตามตัวชี้วัดในแต่ละข้อมากน้อยเพียงใด โดยแบ่งระดับการตอบดังต่อไปนี้



- 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)

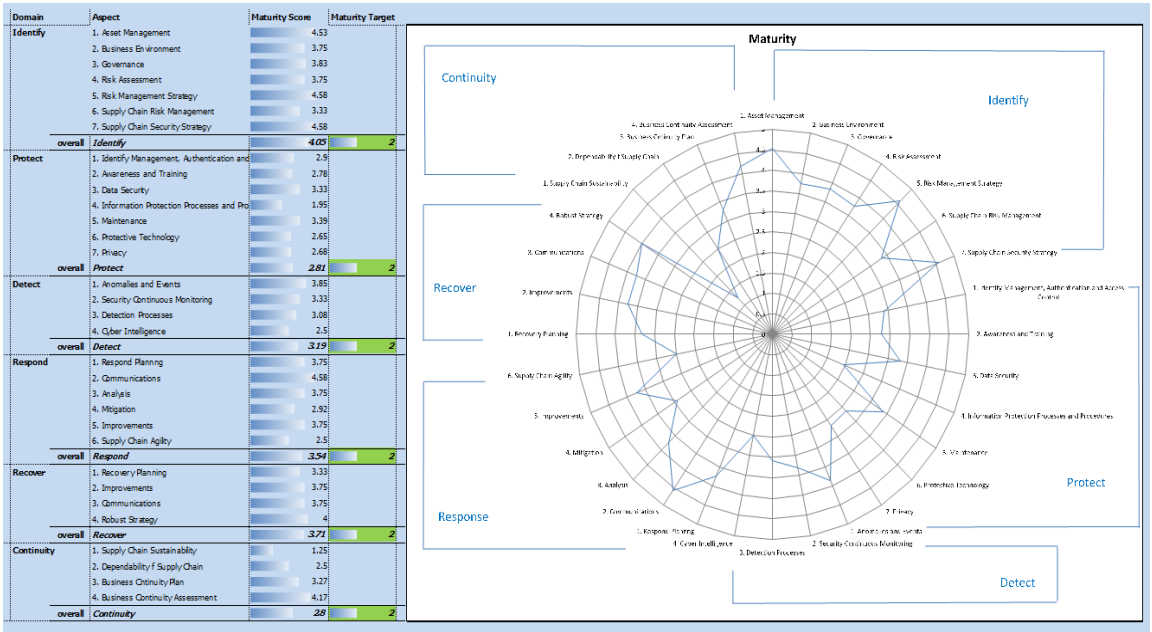
2. Importance เป็นค่าน้ำหนักในการประเมินตัวชี้วัดแต่ละตัว โดยผู้วิจัยมองว่า ในการกำหนดระดับความสำเร็จของตัวชี้วัดแต่ละตัวในข้อที่ 1 Answer นั้น ยังควรจะต้องมีการกำหนดระดับความสำคัญของระดับคะแนนที่ระบุลงไปด้วย โดยค่าน้ำหนักที่กำหนดนั้นจะมีค่าดังต่อไปนี้



- 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)

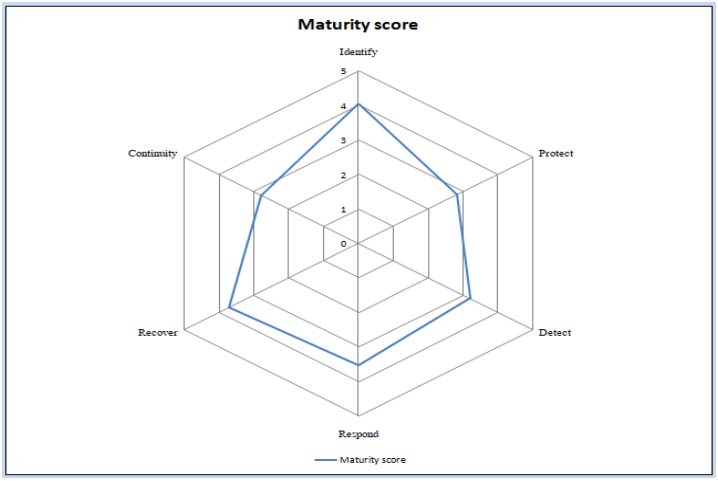
การรายงานผลการประเมินระดับวุฒิภาวะ ผู้วิจัยได้ทำการรายงานผลระดับวุฒิภาวะใน 2 ลักษณะ

1. การรายงานผลในระดับมิติทั้ง 32 มิติ



Domain	Aspect	Maturity Score	Maturity Target
Identify	1. Asset Management	4.53	
	2. Business Environment	3.75	
	3. Governance	3.83	
	4. Risk Assessment	3.75	
	5. Risk Management Strategy	4.58	
	6. Supply Chain Risk Management	3.33	
	7. Supply Chain Security Strategy	4.58	
overall	*Identify*	*4.05*	*2*
Protect	1. Identify Management, Authentication and	2.5	
	2. Awareness and Training	2.78	
	3. Data Security	3.33	
	4. Information Protection Processes and Pro	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 Ontinuity Plan	3.27	
	4. Business Continuity Assessment	4.17	
overall	*Continuity*	*2.8*	*2*

2. การรายงานผลในระดับหน้าที่งานตามหมวดต่าง ๆ ทั้ง 6 หมวด



ข้อเสนอแนะ / ข้อคิดเห็น จากผู้เชี่ยวชาญ สำหรับส่วนที่ 4

ส่วนที่ 4 แนวทางการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของ โซ่อุปทาน

<u>ระดับความคิดเห็นโดยรวมของผู้เชี่ยวชาญต่อตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล</u>

1. “ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล” ตามใน**<u>รูปที่ 1</u>** **<u>มีความเหมาะสมหรือไม่ อย่างไร หรือควรต้องทำการปรับปรุงอย่างไร</u>**

.....

.....

.....

.....

.....

2. “ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล” ตามใน **<u>รูปที่ 2</u>**
<u>มีความเหมาะสม อยู่ในระดับใด (□ 5 ----- □ 4----- □ 3---- □ 2 -----□1)</u> เพราะเหตุใด

.....

.....

.....

.....

.....

3. “ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล” ตาม ใน**<u>รูปที่ 2</u>**
มีระดับการยอมรับ อยู่ในระดับใด <u>(□ 5 ----- □ 4----- □ 3---- □ 2 -----□1)</u> เพราะเหตุใด

.....

.....

.....

.....

.....

4. ข้อเสนอแนะโดยรวมต่อสิ่งที่ควรปรับปรุงใน “ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล” ใน**รูปที่ 2** มีอะไรบ้าง

.....

.....

.....

.....

.....

ลงชื่อ

.....

(.....)

วันที่..... เดือน..... พ.ศ.....

ผู้เชี่ยวชาญ