



## แบบสอบถามสำหรับการหาค่านำหนักของปัจจัย

สำหรับงานวิจัย

เรื่อง

การพัฒนาตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทาน เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม

(Development of Capability Maturity Model for Cyber-Resilient Supply Chains

in Order to Manage the Digital Business Continuity in Small and Medium-sized Enterprises)

ชื่อผู้ประเมินระบบ : .....

ตำแหน่ง : .....

บริษัท / องค์กร : .....

วันที่ทำการประเมิน : .....

ผู้วิจัย

นายนิริศ อุไรพันธ์

นักศึกษาลัทธิศาสตรปรัชญาคุณวุฒิบัณฑิต สาขาวิชาการจัดการโลจิสติกส์และโซ่อุปทาน

วิทยาลัยโลจิสติกส์และซัพพลายเชน มหาวิทยาลัยศรีปทุม

โทรศัพท์ : 062-807-5550 อีเมล : [naris080515@yahoo.com](mailto:naris080515@yahoo.com)

**คำชี้แจง** แบบสอบถามนี้เป็นส่วนหนึ่งในการทำวิทยานิพนธ์ของหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการจัดการ โลจิสติกส์และโซ่อุปทาน โดยมีวัตถุประสงค์เพื่อศึกษาถึงความสำคัญของปัจจัยในการพิจารณาตัดสินใจเลือกผลของการประเมินระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม โดยจุดมุ่งหมายของแบบสอบถามนี้เพื่อสำรวจความคิดเห็นของผู้บริหารระดับสูง ผู้บริหาร เจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ที่มีประสบการณ์ในการพิจารณาปัจจัยต่าง ๆ ที่มีความสำคัญต่อการตัดสินใจเลือกระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน และจะได้นำข้อมูลที่รวบรวมได้จากการสำรวจความคิดเห็นนี้มาศึกษาจัดเป็นระบบตัดสินใจเลือกระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อจัดการความต่อเนื่องของธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม ที่ใช้ในการศึกษาต่อไป

#### **ขั้นตอนในการตอบแบบสอบถาม**

1. อ่านและทำความเข้าใจความหมายของปัจจัยต่าง ๆ ที่ใช้เป็นเกณฑ์ในการตัดสินใจเลือกระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานที่อธิบายไว้ในหน้าแบบสอบถาม ก่อนที่จะตอบแบบสอบถาม
2. การตอบแบบสอบถามครั้งนี้เป็นการให้ผู้ตอบแบบสอบถามแสดงความคิดเห็นของตนเองในการให้ความสำคัญของปัจจัยแต่ละตัวที่ใช้พิจารณาเลือกระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน โดยพิจารณาเปรียบเทียบเป็นคู่ ๆ ไป ทั้งนี้ การพิจารณาเปรียบเทียบจะพิจารณาเปรียบเทียบเป็นคู่ ๆ ที่ละคู่จะกว่าจะครบทุกปัจจัย
3. เพื่อเป็นแนวทางเดียวกัน จึงได้กำหนดค่ามาตรฐานที่ใช้ในการเปรียบเทียบให้ความสำคัญของปัจจัย รายละเอียดค่าต่าง ๆ แสดงไว้ในหน้าถัดไป
4. ในการพิจารณาเปรียบเทียบค่าความสำคัญของปัจจัยจากตารางแบบสอบถามที่ให้มา จะพิจารณาให้ค่าความสำคัญของปัจจัยที่อยู่ทางด้านซ้ายของแถว เมื่อเปรียบเทียบกับปัจจัยที่อยู่ทางด้านขวาของบรรทัดเดียวกัน

## คำอธิบายและความหมายของปัจจัยแต่ละตัว

ข้อเสนอแนะคำอธิบายและความหมายที่เกี่ยวข้องกับปัจจัยแต่ละตัว ที่จะนำมาใช้ในการพิจารณาเปรียบเทียบค่าความสำคัญในการตัดสินใจเลือกระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน มีดังต่อไปนี้

**1. ปัจจัยด้านการระบุ (Identify)** – เป็นการระบุและเข้าใจถึงบริบทต่าง ๆ ของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน ซึ่งประกอบไปด้วย

**1.1 การจัดการทรัพยากรขององค์กร (Asset Management)** ข้อมูล บุคลากร อุปกรณ์ ระบบและสิ่งอำนวยความสะดวกที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจ ได้รับการระบุและจัดการให้สอดคล้องกับความสำคัญเชิงสัมพันธ์กับ วัตถุประสงค์ทางธุรกิจและกลยุทธ์ความเสี่ยงขององค์กร

**1.2 สภาพแวดล้อมทางธุรกิจ (Business Environment)** สร้างความเข้าใจในภารกิจขององค์กร วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสียและกิจกรรมขององค์กร และจัดลำดับความสำคัญ ข้อมูลเหล่านี้ เพื่อกำหนดบทบาทความรับผิดชอบและการตัดสินใจในการจัดการความเสี่ยงทางไซเบอร์

**1.3 การกำกับดูแล (Governance)** นโยบายขั้นตอนและกระบวนการในการจัดการและตรวจสอบความต้องการด้านกฎระเบียบ กฎหมาย ความเสี่ยง สิ่งแวดล้อมและการดำเนินงานขององค์กรและแจ้งให้ทราบถึงการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

**1.4 การประเมินความเสี่ยง (Risk Assessment)** การทำความเข้าใจขององค์กรต่อความเสี่ยงในโลกไซเบอร์ที่มีผลการดำเนินงานขององค์กร (รวมถึงภารกิจหน้าที่ ภาพลักษณ์หรือชื่อเสียง) ทรัพย์สินขององค์กรและบุคลากร

**1.5 กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)** มีการกำหนดลำดับความสำคัญขององค์กร ข้อจำกัด การยอมรับความเสี่ยงและข้อสมมติฐาน ที่ต้องได้รับการจัดทำขึ้นมา และใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงในการดำเนินงาน

**1.6 การจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management)** ลำดับความสำคัญขององค์กร ข้อจำกัด การยอมรับความเสี่ยงและข้อสมมติฐานถูกกำหนดขึ้นและใช้เพื่อสนับสนุนการตัดสินใจความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในโซ่อุปทาน องค์กรได้กำหนดและดำเนินการตามกระบวนการเพื่อระบุประเมินและจัดการความเสี่ยงของโซ่อุปทาน

**1.7 กลยุทธ์การจัดการความปลอดภัยของโซ่อุปทาน (Supply Chain Security Strategy)** เพื่อเป็นการกำหนดกลยุทธ์ที่ใช้ในการจัดการความปลอดภัยของโซ่อุปทาน เพื่อสร้างความเชื่อมั่นให้กับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียต่อโซ่อุปทาน

**2. ปัจจัยด้านการป้องกัน (Protect)** – เป็นการวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร ต่อความเสี่ยงทางไซเบอร์ของโซลูชัน ประกอบด้วย

**2.1 การควบคุมการเข้าถึง (Access Control)** การจำกัดการเข้าถึงสินทรัพย์และสิ่งอำนวยความสะดวกที่เกี่ยวข้อง เฉพาะผู้ใช้งาน กระบวนการและอุปกรณ์ที่ได้รับอนุญาต และมีการจัดการที่สอดคล้องกับความเสี่ยงที่ประเมินจากการเข้าถึงกิจกรรมและธุรกรรมที่ไม่ได้รับอนุญาต

**2.2 การตระหนักรู้และการฝึกอบรม (Awareness and Training)** ต้องมีการให้ศึกษาเรื่องความปลอดภัยในโลกไซเบอร์ต่อบุคลากร รวมถึงการต้องฝึกอบรมอย่างเพียงพอในการปฏิบัติหน้าที่และความรับผิดชอบด้านความปลอดภัยของข้อมูลที่สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

**2.3 ความปลอดภัยของข้อมูล (Data Security)** ข้อมูลและบันทึก (ข้อมูล) ได้รับการจัดการสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับความซื่อสัตย์และความพร้อมของข้อมูล

**2.4 ขั้นตอนและกระบวนการการป้องกันข้อมูล (Information Protection Processes and Procedures)** นโยบายความปลอดภัย (วัตถุประสงค์ ขอบเขต บทบาทความรับผิดชอบ ข้อผูกพัน การจัดการและการประสานงานระหว่างหน่วยงานองค์กร) กระบวนการและขั้นตอนและการบำรุงรักษาและใช้ในการจัดการป้องกันระบบข้อมูลและสินทรัพย์

**2.5 การบำรุงรักษา (Maintenance)** การบำรุงรักษาและซ่อมแซมการควบคุมระบบงานที่เกี่ยวข้อง และส่วนประกอบของระบบสารสนเทศนั้นดำเนินการสอดคล้องกับนโยบายและขั้นตอน

**2.6 เทคโนโลยีการป้องกัน (Protective Technology)** โซลูชันด้านความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อรับรองความปลอดภัยและการคืนสภาพได้ของระบบและสินทรัพย์ให้สอดคล้องกับนโยบายขั้นตอนและข้อตกลงที่เกี่ยวข้อง

**2.7 ความเป็นส่วนตัว (Privacy)** เพื่อช่วยให้องค์กรกำหนดมาตรการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้องกับข้อมูลที่ระบุตัวตนของลูกค้า, คู่ค้า ได้ภายในสภาพแวดล้อมทางดิจิทัลและบทบาทหน้าที่ในการประมวลผลข้อมูลบุคคลตามหลักการจัดการข้อมูลบุคคล

**3. ปัจจัยด้านการตรวจจับ (Detect)** – เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ มีรายละเอียดของกลุ่มงานในหมวดนี้ดังนี้

**3.1 สถานการณ์และเหตุการณ์ที่มีความผิดปกติ (Anomalies and Events)** การตรวจหากิจกรรมที่ผิดปกติในเวลาที่เหมาะสมและเข้าใจถึงผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ดังกล่าว

### 3.2 การตรวจสอบความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)

ระบบข้อมูลและสินทรัพย์จะถูกตรวจสอบเป็นระยะ ๆ เพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์และตรวจสอบประสิทธิภาพของมาตรการป้องกัน

### 3.3 กระบวนการการตรวจสอบ (Detection Processes) กระบวนการและขั้นตอนการ

ตรวจจับนั้นต้องได้รับการบำรุงรักษาและทดสอบเพื่อให้แน่ใจว่ามีการรับรู้เหตุการณ์ที่ผิดปกติอย่างทันเวลาและเพียงพอ

### 3.4 ข่าวกรองทางไซเบอร์ (Cyber Intelligence) กระบวนการในการสืบค้น ตรวจสอบ

วิเคราะห์ และพิสูจน์ว่า ข่าวที่ได้รับทางไซเบอร์นั้นมีความน่าเชื่อถือ และทำการจัดทำรายงานส่งต่อให้กับผู้ที่เกี่ยวข้อง

**4. ปักจ้ยด้านการรับมือ (Respond) –** เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น รายละเอียดของกลุ่มงานในหมวดนี้มีดังนี้

#### 4.1 การวางแผนการรับมือ (Response Planing) กระบวนการและขั้นตอนการรับมือ ต้อง

ได้รับการดำเนินการ และบำรุงรักษาอยู่อย่างตลอด เพื่อให้มั่นใจว่ามีการตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบทันเวลา

#### 4.2 การสื่อสารเกี่ยวกับการรับมือ (Communications) กิจกรรมการตอบสนองมีการ

ประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกตามความเหมาะสมเพื่อรวมการสนับสนุนจากหน่วยงานบังคับใช้กฎหมาย

#### 4.3 การวิเคราะห์เพื่อการรับมือ (Analysis) มีการวิเคราะห์เพื่อให้มั่นใจว่ามีการตอบสนอง

ที่เพียงพอและสนับสนุนกิจกรรมการกู้คืน

#### 4.4 การบรรเทาสถานการณ์ (Mitigation) มีการดำเนินกิจกรรมเพื่อการป้องกัน รวมถึง

กิจกรรมการบรรเทาสถานการณ์ ผลกระทบและกำจัดเหตุการณ์

#### 4.5 การพัฒนาแนวทางการรับมือ (Improvements) กิจกรรมการรับมือเพื่อตอบสนองต่อ

เหตุการณ์ผิดปกติทางไซเบอร์ต้องมีการปรับปรุงโดยการรวมบทเรียนที่ได้เรียนรู้จากกิจกรรมการตรวจจับ / ตอบสนองในปัจจุบันและก่อนหน้า

#### 4.6 ความคล่องตัวของโซ่อุปทาน (Supply Chain Agility) ความสามารถของโซ่อุปทานที่

ให้ความสนใจต่อการปรับตัวของระบบอย่างรวดเร็วในสถานการณ์ที่ต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่สามารถคาดเดาได้ ด้วยการแสดงปฏิกิริยาตอบโต้ (React) การตอบสนอง (Respond) การปรับตัว (Adapt) รวมไปถึงการกำหนด ค่าใหม่ (Re-Configure)

5. **ปัจจัยด้านการฟื้นฟู (Recover)** – เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ ฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม รายละเอียดของกลุ่มงานในหมวดนี้มีดังนี้

5.1 **การวางแผนการฟื้นฟูระบบ (Recovery Planning)** กระบวนการและขั้นตอนการกู้คืนจะถูกดำเนินการและบำรุงรักษาเพื่อให้แน่ใจว่าระบบหรือทรัพย์สินจะได้รับผลกระทบจากเหตุการณ์ความปลอดภัยทางไซเบอร์ในเวลาที่เหมาะสม

5.2 **การพัฒนาแนวทางการฟื้นฟูระบบ (Improvements)** การวางแผนและกระบวนการกู้คืนจะได้รับการปรับปรุงโดยผสมผสานบทเรียนที่เรียนรู้เข้ากับกิจกรรมในอนาคต

5.3 **การสื่อสารเกี่ยวกับการฟื้นฟูระบบ (Communications)** กิจกรรมการฟื้นฟูจะได้รับการประสานงานกับฝ่ายภายในและภายนอก เช่น ศูนย์ประสานงานผู้ให้บริการอินเทอร์เน็ตเจ้าของระบบที่ถูกโจมตี ผู้ที่ตกเป็นเหยื่อ และผู้ขาย

5.4 **กลยุทธ์ความคงทน (Robust Strategy)** เป็นความสามารถของโซ่อุปทานที่จะดำเนินงานตามหน้าที่ต่อไปแม้ว่าจะมีความเสียหายบางอย่างเกิดขึ้นต่อโซ่อุปทาน โดยยังจะต้องสามารถรักษาสถานะของโซ่อุปทานให้มีความเสถียรได้เหมือนกับก่อนที่มีการเปลี่ยนแปลง และจะต้องสามารถทนทานได้มากกว่าการตอบสนอง

6. **ปัจจัยด้านการจัดการความต่อเนื่อง (Continuity)** – เป็นการดำเนินการตามขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง

6.1 **ความยั่งยืนของโซ่อุปทาน (Supply Chain Sustainability)** การจัดการต่อผลกระทบด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม รวมถึงการส่งเสริมการกำกับดูแลกิจการที่ดี ตลอดวัฏจักรชีวิตของสินค้าและบริการ

6.2 **ความเชื่อถือได้ของโซ่อุปทาน (Dependability of Supply Chain)** ความสามารถในการให้บริการที่เชื่อถือได้อย่างสมเหตุสมผล ที่สามารถส่งมอบโดยระบบซึ่งเป็นพฤติกรรมที่สามารถรับรู้ได้โดยผู้ใช้งาน โดยความเชื่อถือได้ของโซ่อุปทานจะมีคุณลักษณะ (attributes) ที่ประกอบด้วยความพร้อมใช้งาน (availability), ความน่าเชื่อถือ (reliability), ความปลอดภัย (safety), การรักษาความลับ (confidentiality), ความสมบูรณ์ (integrity), ความสามารถในการบำรุงรักษา (maintainability) และความมั่นคงปลอดภัย (security)

6.3 **แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)** การวางแผนการต่อการจัดการธุรกิจเพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องเหตุการณ์ที่ไม่คาดคิดที่อาจเกิดขึ้นได้ โดยมีบทบาทที่สำคัญนอกเหนือไปจากที่จะช่วยป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นได้ต่อทรัพย์สิน ข้อมูลขององค์กร โอกาสในการสร้างรายได้ รวมไปถึงการเสริมสร้างภาพลักษณ์ขององค์กรในด้านการจัดการที่ดีเพื่อสร้างความมั่นใจต่อผู้ลงทุนและผู้ลูกค้า โดยต้องสามารถดำเนินการ

ได้อย่างต่อเนื่องพร้อมทั้งสามารถบ่งบอกถึงสาเหตุของผลกระทบและความเสียหายทำให้สามารถแก้ไขปัญหาดังกล่าวได้อย่างถูกต้องและรวดเร็ว และเหมาะสมกับสถานการณ์ได้

**6.4 การประเมินความต่อเนื่องทางธุรกิจ (Business Continuity Assessment)** ศึกษาผลกระทบจากสถานการณ์ภายในและภายนอกที่จะส่งผลกระทบต่อ การดำเนินธุรกิจเพื่อใช้ในการจัดความสำคัญของแต่ละกิจกรรมในธุรกิจว่าได้รับผลกระทบอย่างไรจากแต่ละเหตุการณ์ ทั้งในด้านสินค้าและบริการ พร้อมทั้งสามารถที่จะระบุไปถึงความเร่งด่วนในแต่ละขั้นตอนเพื่อใช้ในการออกแบบแผนการป้องกันต่อไป

#### เกณฑ์มาตรฐานที่ใช้ในการเปรียบเทียบความสำคัญ

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

### ตัวอย่างการกรอกแบบสอบถาม

จากแบบสอบถามที่แสดงไว้เป็นตัวอย่างด้านล่างนี้ ผู้ตอบแบบสอบถามจะต้องพิจารณาให้ค่าความสำคัญของปัจจัยเมื่อเปรียบเทียบกับปัจจัยตัวอื่นในแต่ละแถวของตาราง ท่านจะต้องพิจารณาว่า ปัจจัย A มีความสำคัญมากกว่า ปัจจัย B มากน้อยเพียงใด

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

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

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



**แบบสอบถาม :** การพิจารณาเปรียบเทียบความสำคัญของปัจจัยที่มีผลต่อการตัดสินใจระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม

ปัจจัย	ค่ามาตรฐานของการเปรียบเทียบ												ปัจจัย					
	มากกว่า								เท่ากัน	น้อยกว่า								
การระบุ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การป้องกัน
การระบุ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การตรวจจับ
การระบุ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การรับมือ
การระบุ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การฟื้นฟู
การระบุ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การจัดการ ความต่อเนื่อง
การป้องกัน	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การตรวจจับ
การป้องกัน	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การรับมือ
การป้องกัน	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การฟื้นฟู
การป้องกัน	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การจัดการ ความต่อเนื่อง
การตรวจจับ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การรับมือ
การตรวจจับ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การฟื้นฟู
การตรวจจับ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การจัดการ ความต่อเนื่อง
การรับมือ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การฟื้นฟู
การรับมือ	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การจัดการ ความต่อเนื่อง
การฟื้นฟู	9	8	7	6	5	4	3	2	1	9	8	7	6	5	4	3	2	การจัดการ ความต่อเนื่อง

ผู้ประเมิน .....

( ..... )

วันที่ .....