วิชาองค์การและการจัดการ

(ORGANIZATION &MANAGEMENT)

MPA 6204

CRISIS MANAGEMENT

การจัดการภาวะวิกฤต

รศ.ดร.นัทนิชา โชติพิทยานนท์

ภาวะวิกฤต (Crisis)

- ภาวะวิกฤต (Crisis) คือ สภาวะเหตุการณ์หรือสถานการณ์ชั่วคราวที่ไม่ได้คาดคิด มีความสับสน เกิดขึ้นอย่างกระทันหัน สร้างให้เกิดความตื่นตระหนก ซึ่งโดยส่วนใหญ่นั้นจะไม่ได้มีการเตรียมการเพื่อรับมือ โดยภาวะวิกฤตนั้นจะส่งให้เกิดผลเสียกับหน่วยงานหรือองค์กรต่างๆ ซึ่งจะสร้างให้เกิดความกดดัน ภัยคุกคาม ผลกระทบทางลบต่อคนที่เกี่ยวข้อง เช่น บุคคล องค์กร ตั้งแต่จำนวนเล็กน้อยไปจนถึงคนหมู่มาก และอาจส่งผลถึงชื่อเสียงไปจนถึงผลกำไรในการทำธุรกิจ
- ภาวะวิกฤตโดยส่วนใหญ่จะเกิดขึ้นโดยที่ไม่มีสัญญาแจ้งเตือนล่วงหน้า ฉะนั้นการรู้ถึงความสำคัญและขั้นตอนของการบริหารจัดการกับภาวะวิกฤตนั้น นับเป็นหนึ่งในกลยุทธ์ระดับองค์กรที่จำเป็นต้องให้ความสำคัญ และนำไปอยู่ในแผนงานเชิงกลยุทธ์
- ดังนั้นการเตรียมการล่วงหน้าไว้ก่อนย่อมทำให้เกิดความพร้อมในการรับมือกับสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้นในอนาคตได้

การจัดการภาวะวิกฤต (Crisis Management)

- “การจัดการภาวะวิกฤต (Crisis Management)” คือ กระบวนการบริหารจัดการอย่างเป็นระบบ เพื่อ เตรียมความพร้อม รับมือ ควบคุม และฟื้นฟู สถานการณ์ที่ไม่ปกติหรือคุกคามต่อความมั่นคงขององค์กร
- โดยมีเป้าหมายเพื่อ ลดความสูญเสีย และ ฟื้นฟูความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย (Stakeholders)

ตัวอย่างในภาครัฐ **กรณีสถานการณ์โควิด-19**

- ในปี พ.ศ. 2563 ประเทศไทยเผชิญการแพร่ระบาดของเชื้อไวรัสโควิด-19
- รัฐบาลจึงจัดตั้ง “ศูนย์บริหารสถานการณ์โควิด-19 (ศบค.)” (Center for COVID-19 Situation Administration: CCSA)
- เพื่อเป็นหน่วยงานกลางในการวางแผน บูรณาการ และสื่อสารข้อมูลต่อสาธารณะ
- ผลลัพธ์ : สามารถควบคุมการแพร่ระบาดในระยะแรกได้ดี ได้รับการยอมรับจากองค์การอนามัยโลก (WHO)

ประเภทของวิกฤต

สามารถแบ่งออกได้เป็น 3 กลุ่ม ตามระดับความรับผิดชอบขององค์กร

กลุ่มวิกฤตที่ส่งผลคุกคามต่อองค์กรค่อนข้างน้อย (Victim Cluster)

- องค์กรต้องรับผิดชอบในระดับต่ำ เช่น ภัยธรรมชาติ ข่าวลือ ความรุนแรงในที่ทำงาน การถูกใส่ความต่างๆ

กลุ่มวิกฤตที่เป็นเหตุบังเอิญ (Accidental Cluster)

คือ การที่องค์กรดำเนินธุรกิจแล้วนำไปสู่ภาวะวิกฤต โดยไม่ได้เจตนา ความรับผิดชอบอยู่ในระดับกลาง เช่น การปฏิบัติงานในภาวะยากลำบากจนส่งให้เกิดผลเสียบางอย่าง ความผิดพลาดทางเทคนิคของอุปกรณ์หรือเครื่องจักร ความผิดพลาดจากผลิตภัณฑ์ที่ส่งผลเสียต่อผู้ใช้

กลุ่มวิกฤตที่สามารถป้องกันได้ (Preventable Cluster)

คือ วิกฤตที่เกิดจากการที่พนักงานทำผิดพลาด ส่งผลให้องค์กรต้องรับผิดชอบในระดับสูง มีภัยคุกคามอย่างร้างแรง เช่น ความผิดพลาดของพนักงานที่เกิดจากความประมาทจนนำไปสู่อุบัติเหตุ ความผิดพลาดของฝ่ายบริหาร เช่น การทุจริตในหน้าที่ ทำผิดกฎหมาย การปลอมแปลงเอกสารหรือผลตรวจสอบต่างๆที่ส่งผลต่อความน่าเชื่อถือ

วิกฤตที่ส่งผลคุกคามต่อองค์กรค่อนข้างน้อย (VICTIM CLUSTER)

- เป็นสถานการณ์ที่องค์กรเองก็เป็น “เหยื่อ” (Victim) ของเหตุการณ์เช่นเดียวกับผู้ได้รับผลกระทบอื่น ๆ องค์กร ไม่ได้เป็นต้นเหตุโดยตรงของวิกฤต และ ไม่สามารถควบคุมเหตุการณ์นั้นได้ จึงทำให้ “ระดับความรับผิดชอบขององค์กรในสายตาสาธารณะต่ำ” แต่ยังคงต้องสื่อสารอย่างเหมาะสมเพื่อแสดงความเห็นอกเห็นใจ (Empathy) และรักษาความเชื่อมั่นของสาธารณชน

กรณี: เหตุการณ์ภัยธรรมชาติ – น้ำท่วมใหญ่ พ.ศ. 2554

- หลายหน่วยงานของรัฐ เช่น กระทรวงสาธารณสุข และองค์การบริหารส่วนท้องถิ่น ต้องหยุดการดำเนินงานบางส่วนจากน้ำท่วมรุนแรง หน่วยงานเหล่านี้ ไม่ได้เป็นผู้ก่อเหตุวิกฤต แต่เป็น “เหยื่อร่วม” จึงอยู่ในกลุ่ม Victim Cluster เพราะได้รับผลกระทบจากปัจจัยภายนอก
- แนวทางการจัดการ คือ ออกมาตรการช่วยเหลือผู้ประสบภัย เช่น ศูนย์พักพิง การรักษาพยาบาลฟรี สื่อสารต่อสาธารณะอย่างต่อเนื่อง เพื่อสร้างความเชื่อมั่นในบทบาทของรัฐ เน้นภาพลักษณ์ “รัฐเป็นผู้ช่วย ไม่ใช่ผู้ก่อปัญหา”
- ผลลัพธ์ : ประชาชนมององค์กรในเชิงบวก เห็นความตั้งใจในการช่วยเหลือและฟื้นฟู

สรุปคุณลักษณะของวิกฤตในกลุ่ม VICTIM CLUSTER

ระดับความรุนแรง
ระดับต่ำถึงปานกลาง

ระดับความรับผิดชอบขององค์กร
ระดับต่ำ (องค์กรเป็นผู้ได้รับผลกระทบ ไม่ใช่ผู้ก่อเหตุ)

ตัวอย่างเหตุการณ์
ภัยธรรมชาติ, การก่อการร้าย, การโจมตีทางไซเบอร์, การระบาดของโรค

กลยุทธ์การสื่อสารที่เหมาะสม
แสดงความเห็นใจ (Empathy), ให้ข้อมูลอัปเดต (Information), เน้นการช่วยเหลือ (Corrective Action)

เป้าหมายหลัก
ฟื้นความเชื่อมั่นและภาพลักษณ์องค์กรในฐานะ “ผู้ร่วมเผชิญวิกฤต”

** **Victim Cluster** คือ วิกฤตที่องค์กรเองก็เป็นผู้ประสบภัย ไม่ได้เป็นผู้ก่อปัญหา เช่น ภัยธรรมชาติ การโจมตีทางไซเบอร์ หรือโรคระบาดใหญ่ (โควิด-19 ในระยะแรก) ผู้นำองค์กรต้องแสดง “ความเห็นอกเห็นใจและความรับผิดชอบต่อผู้ได้รับผลกระทบ” เพื่อรักษาความไว้วางใจและภาพลักษณ์เชิงบวกขององค์กร

วิกฤตที่เป็นเหตุบังเอิญ (ACCIDENTAL CLUSTER)

กรณี: โรงงานเคมีรั่วในนิคมอุตสาหกรรมมาบตาพุด)

- บริษัทผู้ผลิตเคมีภัณฑ์รายหนึ่งเกิดเหตุท่อส่งสารเคมีรั่ว ทำให้เกิดกลิ่นและควันกระจายในพื้นที่ใกล้เคียง ตรวจสอบพบว่าเกิดจาก “ความผิดพลาดของระบบควบคุมแรงดัน” ซึ่งไม่ได้เกิดจากความตั้งใจ
- แนวทางการจัดการ คือ หยุดการผลิตทันทีและควบคุมพื้นที่ แถลงข่าวชี้แจงเหตุการณ์อย่างโปร่งใส ชดเชยผู้ได้รับผลกระทบ และตรวจสอบมาตรการความปลอดภัยใหม่

- คือ วิกฤตที่เกิดขึ้นจาก เหตุการณ์ที่ไม่ตั้งใจ หรือเกิดจาก ความผิดพลาดทางเทคนิค มนุษย์ หรือระบบ ซึ่งองค์กรอาจมี “ส่วนเกี่ยวข้องบางส่วน” แต่ไม่ได้เกิดจากเจตนา หรือความประมาทอย่างร้ายแรง
- ดังนั้น ระดับความรับผิดชอบขององค์กรจะอยู่ในระดับ “ปานกลาง (Moderate Responsibility)” แต่สาธารณชนคาดหวังให้องค์กร “แสดงความรับผิดชอบอย่างจริงใจ” และ “แก้ไขปัญหาอย่างโปร่งใส”
- เป้าหมายหลัก: “Restore Trust & Transparency” (ฟื้นความเชื่อมั่นและสร้างความโปร่งใสในการแก้ปัญหา)

กรณี: ระบบเว็บและแอปพลิเคชันล่ม – โครงการ “เที่ยวไทยคนละครึ่ง”

- เมื่อเปิดให้ลงทะเบียน ประชาชนลงทะเบียนพร้อมกันทั่วประเทศ แต่ระบบล่มภายในไม่กี่ชั่วโมง เนื่องจากมีผู้เข้าใช้งานจำนวนมากเกินความคาดหมาย แม้หน่วยงาน ไม่ได้ตั้งใจให้เกิดปัญหา แต่ถือว่ามี “ส่วนเกี่ยวข้องทางเทคนิค” เพราะระบบไม่ได้เตรียมความพร้อมเพียงพอ จึงเข้าข่าย Accidental Cluster
- แนวทางการจัดการ คือ แถลงขอโทษประชาชนทันที ปรับขยายระบบรองรับผู้ใช้งาน และเปิดรอบลงทะเบียนใหม่ให้ทุกคนมีสิทธิ์เท่าเทียม
- ผลลัพธ์ : ลดความไม่พอใจของประชาชน ภาพลักษณ์ของหน่วยงานดีขึ้นจากการสื่อสารอย่างโปร่งใสและรับผิดชอบ

สรุปคุณลักษณะของวิกฤตในกลุ่ม ACCIDENTAL CLUSTER

ระดับความรุนแรง

ระดับปานกลาง

ระดับความรับผิดชอบขององค์กร

ปานกลาง (เกิดจากความผิดพลาดโดยไม่ตั้งใจ)

ตัวอย่างเหตุการณ์

ระบบเทคนิคขัดข้อง, อุบัติเหตุในโรงงาน, ความผิดพลาดของข้อมูล

การรับรู้ของสาธารณะ

เข้าใจว่าองค์กรไม่ได้ตั้งใจ แต่คาดหวังให้ “แสดงความรับผิดชอบ”

กลยุทธ์การสื่อสารที่เหมาะสม

ขอโทษ, อธิบายเหตุผล, แก้ไขและชดเชย, สื่อสารอย่างต่อเนื่องและโปร่งใส

เป้าหมายหลัก

รักษาความเชื่อมั่นของสาธารณะ และฟื้นฟูภาพลักษณ์องค์กร

** **Accidental Cluster** คือ วิกฤตที่เกิดจาก “ความผิดพลาดโดยไม่ตั้งใจ” องค์กรไม่ได้เจตนาทำให้เกิดผลเสีย แต่ต้อง แสดงความรับผิดชอบ โปร่งใส และเร่งแก้ไขทันที เพื่อรักษาความไว้วางใจจากสาธารณชน

วิกฤตที่สามารถป้องกันได้ (PREVENTABLE CLUSTER)

กรณี: บริษัทอาหารรายใหญ่มีการใช้วัตถุดิบไม่ได้มาตรฐาน

- ถูกตรวจพบว่าใช้วัตถุดิบที่ไม่ได้มาตรฐาน GMP โดยมีสารปนเปื้อนและไม่ได้เปิดเผยข้อมูลต่อหน่วยงานกำกับดูแล จนกระทั่งมีผู้บริโภคได้รับอันตรายและเป็นข่าวใหญ่ในสื่อ
- เป็นการกระทำที่ป้องกันได้ หากมีระบบตรวจสอบคุณภาพที่เข้มงวด และองค์กรละเลยความปลอดภัยของผู้บริโภค
- แนวทางจัดการวิกฤต : ยอมรับผิดและเรียกคืนสินค้าทันที แถลงข่าวขอโทษและเปิดเผยแผนฟื้นฟูระบบคุณภาพ ชดเชยลูกค้าและปรับโครงสร้างการควบคุมภายใน

- คือ วิกฤตที่องค์กรเป็นผู้ก่อให้เกิดขึ้นเอง หรือสามารถป้องกันได้แต่ไม่ทำ มาจาก ความประมาทเลินเล่อ การละเมิดจรรยาบรรณ หรือ การตัดสินใจที่ขาดความรับผิดชอบ
- ระดับความรับผิดชอบขององค์กร อยู่ในระดับสูงมาก (High Responsibility) เพราะประชาชนและสื่อจะมองว่า “องค์กรเป็นผู้ผิดโดยตรง”
- จึงต้องยอมรับผิดอย่างเปิดเผย และ ดำเนินการแก้ไขอย่างโปร่งใส

กรณี: การจัดซื้อจัดจ้างไม่โปร่งใส ในองค์กรปกครองส่วนท้องถิ่น

- มีการตรวจสอบพบว่า หน่วยงานท้องถิ่นแห่งหนึ่งอนุมัติโครงการจัดซื้อวัสดุโดยไม่มีการประกวดราคาอย่างเป็นธรรม พบการใช้อำนาจโดยมิชอบและผลประโยชน์ทับซ้อน ส่งผลให้เกิดกระแสวิพากษ์วิจารณ์ในสังคม และถูก สตง. และ ป.ป.ช. ตรวจสอบ
- ลักษณะของวิกฤต เป็นเหตุที่ “สามารถป้องกันได้” หากมีระบบตรวจสอบและธรรมาภิบาล
- แนวทางจัดการวิกฤต คือ ยอมรับข้อผิดพลาดและเปิดเผยข้อมูลต่อสาธารณะ ตั้งคณะกรรมการสอบสวนภายใน ปรับระบบ e-GP (จัดซื้อจัดจ้างอิเล็กทรอนิกส์) ให้ตรวจสอบได้แบบเรียลไทม์
- ผลลัพธ์ที่ดี : ฟื้นความเชื่อมั่นในองค์กร สร้างมาตรฐานการบริหารจัดซื้อโปร่งใสต้นแบบ

สรุปคุณลักษณะของวิกฤตในกลุ่ม PREVENTABLE CLUSTER

ระดับความรุนแรง

ระดับสูง

ระดับความรับผิดชอบขององค์กร

สูงมาก เพราะองค์กรเป็น “ต้นเหตุ” ของปัญหาโดยตรง

ตัวอย่างเหตุการณ์

หน่วยงานรัฐจัดซื้อจัดจ้างไม่โปร่งใส, บริษัทเอกชนปล่อยของเสียลงแม่น้ำ, องค์กรละเลยความปลอดภัยจนเกิดอุบัติเหตุใหญ่, สารปนเปื้อนในสินค้า เป็นต้น

ภาวะผู้นำที่เหมาะสม

มีความรับผิดชอบสูง, จริยธรรมทางการบริหารเพื่อสร้างวัฒนธรรมองค์กรโปร่งใส

กลยุทธ์การสื่อสารที่เหมาะสม

ยอมรับผิดอย่างเป็นทางการ, ขอโทษและชี้แจงความจริง, ชดเชยและเยียวยาผู้เสียหาย, ดำเนินการแก้ไขเชิงระบบ และเปิดเผยผลการสอบสวนอย่างโปร่งใส เป็นต้น

เป้าหมายหลัก

ฟื้นฟูความเชื่อมั่น และป้องกันการเกิดซ้ำ

** **Preventable Cluster** คือ วิกฤตที่องค์กรเป็นผู้ก่อให้เกิดขึ้นเอง หรือสามารถป้องกันได้แต่ไม่ทำ มาจาก ความประมาทเลินเล่อ, การละเมิดจรรยาบรรณ, หรือ การตัดสินใจที่ขาดความรับผิดชอบ ระดับความรับผิดชอบขององค์กร สูงมาก ประชาชนและสื่อจะมองว่า “องค์กรเป็นผู้ผิดโดยตรง” จึงต้อง ยอมรับผิดอย่างเปิดเผย และ ดำเนินการแก้ไขอย่างโปร่งใส

ประเภทของวิกฤต

ตามกรอบแนวคิดของ Peter Bernstein (1996) และ Kaplan & Mikes (2012)

วิกฤตที่ทราบล่วงหน้าว่าจะเกิดแต่ไม่รู้ว่าเมื่อใด (Know-Unknowns)

การที่องค์กรคาดเดาได้ว่าวิกฤตนั้นมีโอกาสจะเกิดขึ้น แต่ไม่สามารถเจาะจงแน่ชัดได้ว่าจะเป็นเมื่อใด ซึ่งหากคาดการณ์ไว้แล้วว่ามีโอกาสเกิดวิกฤตในช่วงเวลาใดเวลาหนึ่ง จึงควรที่จะมีแผนรองรับในอนาคตไว้

วิกฤตที่ไม่ทราบล่วงหน้าว่าจะเกิดและไม่รู้ว่าเมื่อใด (Unknown-Unknown)

การที่องค์กรไม่สามารถคาดเดาหรือไม่รู้ว่าจะมีโอกาสเกิดวิกฤตใดๆขึ้นเลย ซึ่งเป็นการยากที่จะวางแผนป้องกัน เช่น การแพร่ระบาดของโรคโควิด-19, ระบบดิจิทัลล่มทั่วประเทศ ทำให้ข้อมูลหายทั้งระบบ เป็นต้น

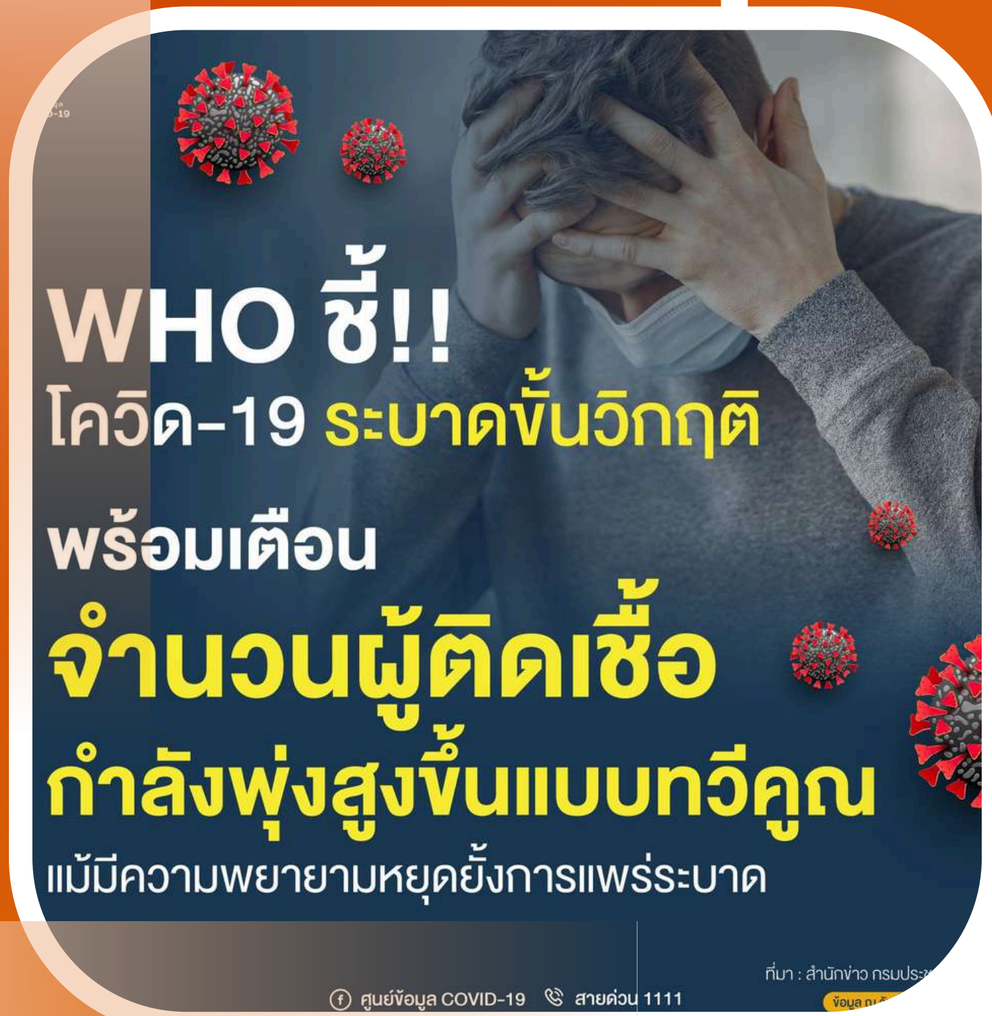
ลักษณะของวิกฤต Know-Unknowns

- คาดเดาได้ (Predictability) รู้ว่าจะเกิดแน่ แต่ไม่รู้ “เมื่อไหร่”
- ระดับความถี่ (Frequency) เกิดเป็นระยะ ๆ (เช่น ทุกปี / ทุกฤดูกาล)
- ผลกระทบ (Impact) ปานกลางถึงสูง ขึ้นอยู่กับการเตรียมพร้อม ความรับผิดชอบขององค์กร ระดับปานกลาง ขึ้นอยู่กับการวางแผนป้องกัน
- แนวทางจัดการ การเตรียมแผนล่วงหน้า และการสื่อสารเตือนภัยอย่างต่อเนื่อง
- เช่น “น้ำท่วม” รู้ว่าเกิดแน่ (Known) เพราะมีสถิติซ้ำซากทุกปี แต่ไม่รู้เวลาแน่ชัด (Unknown) ขึ้นอยู่กับฝน ปริมาณน้ำ และสภาพภูมิอากาศ
- แนวทางจัดการ : จัดทำแผนป้องกันน้ำท่วมประจำปี ฝึกซ้อมอพยพประชาชนในพื้นที่เสี่ยง ใช้ระบบเตือนภัยและข้อมูลเรียลไทม์จากกรมอุตุนิยมวิทยา

ลักษณะของวิกฤต Unknow-Unknowns

- ไม่รู้ว่าเหตุการณ์แบบนี้มีอยู่ในความเป็นไปได้ และ ไม่สามารถคาดการณ์ได้ว่าจะเกิดขึ้นเมื่อใดหรือในรูปแบบใด เป็น “เหตุการณ์ที่ไม่เคยเกิดมาก่อน” หรือ “ไม่มีข้อมูลอ้างอิงในอดีต” จึงไม่สามารถวางแผนรับมือได้ล่วงหน้าอย่างเป็นระบบ
- ความคาดเดาได้ ต่ำมาก ไม่สามารถระบุได้เลยว่าจะเกิดเหตุการณ์ใด
- ผลกระทบ (Impact) สูงมาก มักกระทบวงกว้างทั่วทั้งระบบ
- ระยะเวลาในการตอบสนอง (Response Time) ช่วงแรกจะล่าช้า เพราะองค์กรไม่เคยเตรียมแผนไว้
- ความรับผิดชอบขององค์กร ขึ้นอยู่กับการตอบสนองภายหลังเกิดวิกฤต
- แนวทางจัดการ : ต้องอาศัย “ภาวะผู้นำเชิงพลวัต (Adaptive Leadership)” และ การเรียนรู้ขณะเผชิญเหตุ

บทเรียนสำคัญจากวิกฤตโควิด-19



การเตรียมพร้อม (Preparedness)

ทุกองค์กรต้องมีแผนรับมือเหตุไม่คาดคิด เช่น โรคระบาด ภัยธรรมชาติ หรือ Cyber Crisis

การปรับตัว (Adaptability)

ผู้นำต้องยืดหยุ่นและปรับรูปแบบการทำงาน เช่น Remote Work, Digital Platform

การสื่อสาร (Communication)

การสื่อสารที่ชัดเจน โปร่งใส และต่อเนื่องช่วยลดความตื่นตระหนก

การบูรณาการ (Collaboration)

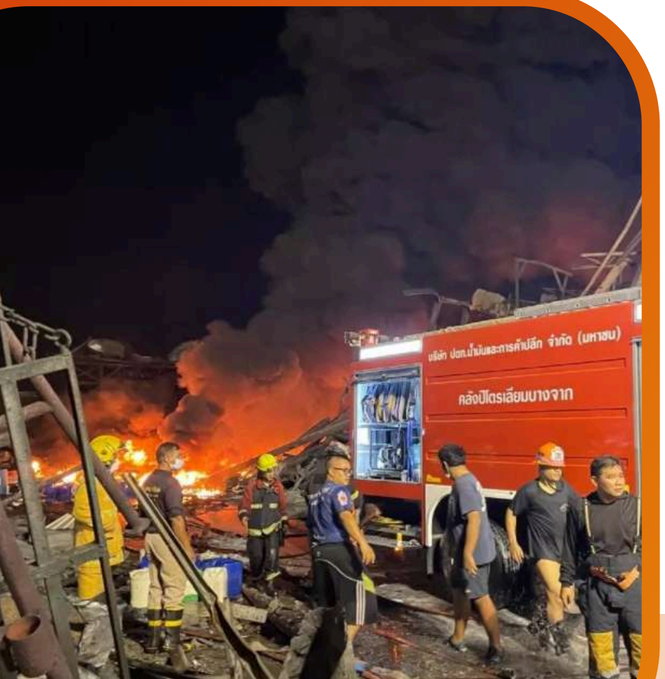
ความร่วมมือระหว่างหน่วยงานรัฐ–เอกชน–ประชาชนคือกุญแจสำคัญ

ภาวะผู้นำในวิกฤต (Leadership in Crisis)

ผู้นำต้องตัดสินใจเด็ดขาด พร้อมรับผิดชอบ และสร้างความมั่นใจแก่สังคม

องค์ประกอบสำคัญของการจัดการภาวะวิกฤต (KEY ELEMENTS)

การจัดการภาวะวิกฤต คือ กระบวนการบริหารสถานการณ์ไม่ปกติอย่างเป็นระบบ
เพื่อป้องกัน ควบคุม และฟื้นฟูองค์กรจากเหตุการณ์ที่ส่งผลกระทบรุนแรง
ผู้นำในภาวะวิกฤตต้องมี ความเด็ดขาด ความยืดหยุ่น และการสื่อสารที่โปร่งใส
เพื่อสร้างความเชื่อมั่นและลดความสูญเสียให้ได้มากที่สุด



- **การวางแผนล่วงหน้า (Crisis Planning)** มีคู่มือและแผนปฏิบัติชัดเจน
- **การสื่อสารในภาวะวิกฤต (Crisis Communication)** สื่อสารโปร่งใส รวดเร็ว และสอดคล้อง
- **การประสานงาน (Coordination)** บูรณาการทุกฝ่ายที่เกี่ยวข้อง
- **ภาวะผู้นำ (Leadership under Pressure)** ผู้นำต้องตัดสินใจรวดเร็ว และสร้างความมั่นใจ
- **การเรียนรู้จากประสบการณ์ (Learning and Adaptation)** สรุปบทเรียนเพื่อปรับปรุงระบบในอนาคต

กระบวนการจัดการภาวะวิกฤต

แนวคิดของ FINK (1986) และ COOMBS (2019) แบ่งเป็น 5 ระยะหลัก ดังนี้

01

ระยะก่อนเกิดวิกฤต (Pre-Crisis)

- เตรียมความพร้อม วางแผนและฝึกซ้อม
- เช่น จัดทำคู่มือรับมือเหตุฉุกเฉิน/แผน BCP

02

ระยะเกิดวิกฤต (Crisis Event)

- ตรวจจับและตอบสนองต่อเหตุการณ์ทันที
- เช่น ตั้งศูนย์บัญชาการ (Crisis Command Center)

03

ระยะควบคุมสถานการณ์ (Crisis Response)

- ดำเนินมาตรการควบคุมและสื่อสารกับผู้เกี่ยวข้อง
- เช่น แถลงข่าวอย่างโปร่งใส ปิดพื้นที่เสี่ยง

04

ระยะฟื้นฟู (Recovery)

- ฟื้นฟูการดำเนินงานและภาพลักษณ์องค์กร
- เช่น ให้ความช่วยเหลือผู้ได้รับผลกระทบ

05

ระยะเรียนรู้ (Learning)

- ประเมินบทเรียนและปรับปรุงแผนเพื่ออนาคต
- เช่น จัดทำรายงานบทเรียน (After Action Review)

ตัวอย่าง กรณี “ไทยแอร์เอเชีย” ในช่วงโควิด-19

- ผู้บริหารจัดตั้ง “ศูนย์บริหารภาวะวิกฤต”
- ปรับแผนการดำเนินธุรกิจ เช่น ลดเที่ยวบิน เพิ่มบริการขนส่งสินค้า และสื่อสารกับลูกค้าอย่างโปร่งใสผ่านโซเชียลมีเดีย
- ผลลัพธ์: องค์กรสามารถรักษาภาพลักษณ์ไว้ได้ และกลับมาเปิดให้บริการได้เร็วหลังวิกฤตคลี่คลาย

ขั้นตอนการจัดการภาวะวิกฤต

- เมื่อเกิดเหตุการณ์ หรือสถานการณ์ที่จะส่งผลเสียหายอย่างรวดเร็ว และรุนแรง ต่อชีวิตและทรัพย์สินของบุคคล ตลอดจนชื่อเสียง และการดำเนินกิจการของบริษัทหรือองค์กรในระยะยาว ซึ่งอาจเกิดจากภัยธรรมชาติ หรือฝีมือมนุษย์ มีผลคุกคามต่อองค์กร เป็นสิ่งที่ไม่คาดคิดมาก่อน ต้องรีบตัดสินใจในระยะเวลาอันสั้น / มีเวลาน้อย องค์กรต้องมีการจัดการภาวะวิกฤตที่เกี่ยวข้องกับการจัดการทั้งก่อน ระหว่าง และหลังที่สิ่งคุกคามที่เกิดขึ้น
- ประกอบด้วย บุคลากรที่มีความรู้ ความชำนาญ กระบวนการและเทคนิคที่จำเป็น เพื่อที่จะบ่งชี้ ประเมิน พร้อมรับมือกับสถานการณ์ โดยเฉพาะอย่างยิ่งในช่วงแรกเริ่มเกิดขึ้นไปจนถึงจุดขั้นตอนของการฟื้นฟู

1. **กำหนดเป้าหมายและวัตถุประสงค์ของการสื่อสารให้ชัดเจน**
2. **เลือกกลยุทธ์ในการตอบโต้วิกฤต**
3. **วางแผนสื่อสารกับผู้มีส่วนได้ส่วนเสีย**
4. **ตั้งหน่วยงานเฉพาะกิจและผู้แถลงการณ์**

ขั้นตอนการจัดการภาวะวิกฤต

1. กำหนดเป้าหมายและวัตถุประสงค์ของการสื่อสารให้ชัดเจน

เมื่อใดก็ตามที่เกิดภาวะวิกฤตขึ้นองค์กรจำเป็นต้องกำหนดแนวทางในการสื่อสาร ทั้งเป้าหมายและวัตถุประสงค์ให้ชัดเจนและมีความเหมาะสมกับเหตุการณ์นั้น ๆ เพื่อเป็นแนวทางในการปฏิบัติในลำดับต่อไป

- ป้องกันการเกิดภาวะวิกฤตใด ๆ แก่บริษัท โดยจัดทำแผนล่วงหน้าพร้อมสื่อสารให้ทุกส่วนที่เกี่ยวข้องได้รับทราบ เข้าใจ สามารถปฏิบัติได้จริงเมื่อเกิดภาวะวิกฤต
- เพื่อกำจัดภาวะวิกฤตนั้นให้หมดไปโดยเร็วที่สุด และจำกัดขอบเขตความเสียหายให้อยู่ในวงจำกัด
- เพื่อรักษาความเชื่อมั่นต่อองค์กร สร้างความน่าเชื่อถือให้เกิดขึ้นกับองค์กรอีกครั้ง
- พื่อลดความตื่นตระหนกของสาธารณชน
- เพื่อให้สามารถกลับมาดำเนินงานได้อย่างรวดเร็ว

ขั้นตอนการจัดการภาวะวิกฤต

กำหนดเป้าหมายและวัตถุประสงค์ของการสื่อสารให้ชัดเจน

ตัวอย่าง ภาครัฐ

- การสื่อสารในสถานการณ์ชายแดนไทย–กัมพูชา ควรกำหนดเป้าหมายการสื่อสาร ให้ประชาชนได้รับข้อมูลที่ถูกต้องและทันท่วงที ร้างความเชื่อมั่นในบทบาทของรัฐบาลและกองทัพ
- ใช้การสื่อสารเชิงรุก โดยข้อมูลทุกชุดต้องผ่านการตรวจสอบและสื่อสารจาก “ศูนย์กลางเดียว” เพื่อป้องกันความสับสน ให้ข้อมูลเชิงข้อเท็จจริง
- ใช้ “โฆษกกองทัพบก” หรือ “โฆษกรัฐบาล” เป็นผู้แถลงเพียงช่องทางเดียว
- ใช้โซเชียลมีเดียทางการ เช่น เพจกรมประชาสัมพันธ์, เพจกองทัพบก เพื่อสื่อสารทันเหตุการณ์

ตัวอย่าง ภาคเอกชน

- “การบินไทย” และ “ไทยแอร์เอเชีย” เมื่อเกิดเหตุเที่ยวบินล่าช้า จากสภาพอากาศไม่ปลอดภัยในการบิน ความหนาแน่นของจราจรทางอากาศ หรือปัญหาทางเทคนิคของเครื่องบิน
- สายการบิน ออกมาขอโทษอย่างเป็นทางการผ่านช่องทางต่าง ๆ โดยให้ข้อมูลที่โปร่งใส พร้อมแจ้งเวลาบินใหม่อย่างชัดเจน
- ดูแลลูกค้า โดยมอบคูปองอาหาร เครื่องดื่ม หรือที่พักระหว่างรอให้แก่ผู้โดยสาร พร้อมจัดเจ้าหน้าที่อำนวยความสะดวกตลอดเวลา
- ใช้การสื่อสารภายใน แจ้งพนักงานประจำสนามบินให้สื่อสารด้วยน้ำเสียงสุภาพและชี้แจงเหตุผลเดียวกันทุกจุด เพื่อให้ “ข้อความสื่อสารเป็นเอกภาพ”

ขั้นตอนการจัดการภาวะวิกฤต

2. เลือกกลยุทธ์ในการตอบโต้วิกฤต

การเลือกกลยุทธ์นั้นก็ต้องเหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น โดยกลยุทธ์นั้นประกอบด้วย 4 กลุ่ม ตามทฤษฎี Situational Crisis Communication Theory (SCCT) ของ Coombs W. T. (2007) ดังนี้

- 1. **กลุ่มปฏิเสธ (Denial Posture)** องค์กรจะปฏิเสธว่าไม่รู้เห็นเกี่ยวกับเรื่องที่เกิดขึ้น ไม่เกี่ยวข้องกับสิ่งที่เกิด และไม่อยู่ในความรับผิดชอบขององค์กร เพื่อที่องค์กรนั้นจะได้ไม่ต้องรับผิดชอบต่อเรื่องราวต่างๆ ซึ่งแบ่งออกได้เป็น
  - **กลยุทธ์โจมตีผู้กล่าวหา** คือ การโต้ตอบว่าข่าวสารหรือข้อกล่าวหาที่ออกมานั้นไม่เป็นความจริง ซึ่งสร้างให้เกิดความเข้าใจผิดต่อองค์กรและจะต้องมีการดำเนินคดีฟ้องร้องกลับ
  - **กลยุทธ์การปฏิเสธ** คือ การที่องค์กรต้องมั่นใจว่าเหตุการณ์วิกฤตที่เกิดขึ้นไม่ได้มีส่วนเกี่ยวข้องกับองค์กร และต้องมีการแจ้งต่อหน้าสาธารณชนอย่างชัดเจนและตรงไปตรงมา
  - **กลยุทธ์แพะรับบาป** คือ การที่องค์กรหาผู้รับผิดชอบที่เป็นกลุ่มที่บริษัทจ้างดำเนินงานแทน เช่น บริษัทคู่สัญญา (Subcontractor) หรือผู้รับเหมาช่วง โดยต้องพิสูจน์ได้ว่าฝ่ายนั้นมีความผิดจริง และไม่ปฏิบัติตามสัญญาโดยต้องพิสูจน์ให้ได้ว่า บริษัทที่รับจ้างนั้นดำเนินการหรือกระทำความผิดจริง ซึ่งเป็นผลจากการละเลยในการทำหน้าที่หรือปฏิบัติตามคำสั่งจึงจะสามารถใช้กลยุทธ์นี้ได้

**** กลยุทธ์การปฏิเสธ (Denial Strategy)** เหมาะสำหรับกรณีที่องค์กร “ไม่ได้มีส่วนเกี่ยวข้องโดยตรง” กับวิกฤต เช่น ข่าวลือ ข้อมูลเท็จ หรือความเข้าใจผิดของสาธารณชน ต้องมี **“ข้อมูลตรวจสอบยืนยันได้”** จากหน่วยงานภายในหรือภายนอก สื่อสารอย่างรวดเร็ว โปร่งใส และสม่ำเสมอ หลีกเลี่ยงการกล่าวโทษผู้อื่นโดยไม่มีหลักฐาน

ขั้นตอนการจัดการภาวะวิกฤต

เลือกกลยุทธ์ในการตอบโต้วิกฤต

- **2. กลุ่มลดความสำคัญ (Diminishment Posture)** การลดระดับความรับผิดชอบต่อวิกฤตให้น้อยลง เพื่อสร้างความน่าเชื่อถือให้กับองค์กรมากขึ้น หรืออีกนัยนึงคือการที่ทำให้ชื่อเสียงขององค์กรเสียหายน้อยลง แบ่งออกได้เป็น
  - **กลยุทธ์การขออภัย** คือ การปฏิเสธถึงความตั้งใจที่จะให้เกิดวิกฤตขึ้น และอัปเดตความคืบหน้าของปัญหาที่ควรแก้ไข พร้อมสร้างความมั่นใจกลับมา
  - **กลยุทธ์การให้เหตุผล** คือ การอธิบายถึงข้อเท็จจริงซึ่งในหลายกรณีผู้ที่เคราะห์ร้ายอาจจะมีส่วนเกี่ยวข้องให้เกิดเหตุการณ์ต่างๆด้วย แต่ต้องมีหลักฐานพิสูจน์ชัดเจนโดยวิธีนี้จะสามารถลดระดับความเลวร้ายที่จะส่งผลกระทบต่อชื่อเสียงขององค์กรได้มากขึ้น

** **กลยุทธ์ลดความสำคัญ (Diminishment Posture)** เหมาะสำหรับกรณีที่องค์กรมีส่วนเกี่ยวข้องบางส่วนแต่ไม่ได้ตั้งใจให้เกิดเหตุ จุดสำคัญคือ ‘**ความโปร่งใส**’ และ ‘**การสื่อสารอย่างเห็นอกเห็นใจ**’ เพื่อเปลี่ยนความไม่พอใจของสาธารณชนให้กลายเป็นความเข้าใจและเห็นใจแทน

ตัวอย่างกลยุทธ์ในการตอบโต้วิกฤต

กลุ่มปฏิเสธ (DENIAL POSTURE)

กลยุทธ์โจมตีผู้กล่าวหา

- **ตัวอย่าง บริษัทผลิตอาหารรายใหญ่** ถูกกล่าวหาว่าใช้วัตถุดิบไม่ได้มาตรฐานในโรงงาน โดยมีผู้ใช้งานในโซเชียลมีเดียโพสต์รูปและกล่าวหาว่า “สินค้าเน่าเสียก่อนหมดอายุ”
- การตอบสนองขององค์กร บริษัทออกแถลงการณ์อย่างเป็นทางการทันทีว่า “ข้อมูลดังกล่าวไม่เป็นความจริง”
- ชี้แจงว่า “รูปภาพที่เผยแพร่ไม่ได้มาจากผลิตภัณฑ์ของบริษัทจริง”
- ประกาศว่าจะดำเนินคดีทางกฎหมายกับผู้โพสต์ข่าวเท็จ ตาม พ.ร.บ.คอมพิวเตอร์
- พร้อมแนบใบรับรองคุณภาพสินค้า (GMP / HACCP) เพื่อยืนยันมาตรฐาน
- เพื่อปกป้องชื่อเสียงของแบรนด์ และหยุดการเผยแพร่ข่าวเท็จที่อาจส่งผลต่อยอดขาย

กลยุทธ์การปฏิเสธ

- **ตัวอย่าง มีข่าวลือว่า “ข้อมูลส่วนบุคคลของประชาชนรั่วไหลจากธนาคาร”** ส่งผลให้ประชาชนเกิดความตื่นตระหนกและไม่มั่นใจในความปลอดภัยของธุรกรรมออนไลน์ เช่น โมบายแบงก์กิ้งและอินเทอร์เน็ตแบงก์กิ้ง
- ธนาคารแห่งประเทศไทยตรวจสอบแล้ว ไม่พบข้อมูลของคนไทยรั่วไหลออกจากระบบของธนาคารพาณิชย์ ภายในประเทศ ระบบธุรกรรมทางการเงินของสถาบันการเงินยังคงมีความปลอดภัยสูง ทุกธุรกรรมบนโมบายแบงก์กิ้งต้องผ่านการยืนยันตัวตนหลายชั้น และมีการยกระดับการเฝ้าระวังร่วมกับหน่วยงานความมั่นคงทางไซเบอร์
- ภาพลักษณ์ของ ธปท. แข็งแกร่งขึ้นในฐานะองค์กรที่ “ตรวจสอบได้และรับผิดชอบ

กลยุทธ์แพะรับบาป

- **ตัวอย่าง บริษัทโทรคมนาคมแห่งหนึ่ง ถูกประชาชนร้องเรียนว่ามีการรั่วไหลของข้อมูลผู้ใช้งานมือถือ** ตรวจสอบแล้วพบว่า บริษัทคู่สัญญาผู้ให้บริการ Call Center ภายนอก เป็นผู้จัดเก็บข้อมูลผิดพลาดและเปิดเผยโดยไม่ได้รับอนุญาต
- การสื่อสารขององค์กร แถลงชัดว่า “การรั่วไหลไม่ได้เกิดจากระบบของบริษัทโดยตรง” เปิดเผยว่าผู้รับเหมาช่วง เป็นผู้ละเมิดเงื่อนไขสัญญา โดยได้ดำเนินการ ยกเลิกสัญญา และ ฟ้องร้องเรียกค่าเสียหายทันที พร้อมประกาศมาตรการตรวจสอบคู่สัญญาทั้งหมดในอนาคต
- เพื่อแยกความรับผิดขององค์กรออกจากคู่สัญญา และแสดงให้เห็นว่าองค์กรมีมาตรการจัดการอย่างเข้มงวด

ขั้นตอนการจัดการภาวะวิกฤต

เลือกกลยุทธ์ในการตอบโต้วิกฤต

- **2. กลุ่มลดความสำคัญ (Diminishment Posture)** การลดระดับความรับผิดชอบต่อวิกฤตให้น้อยลง เพื่อสร้างความน่าเชื่อถือให้กับองค์กรมากขึ้น หรืออีกนัยนึงคือการที่ทำให้ชื่อเสียงขององค์กรเสียหายน้อยลง แบ่งออกได้เป็น
  - **กลยุทธ์การขออภัย** คือ การปฏิเสธถึงความตั้งใจที่จะให้เกิดวิกฤตขึ้น และอัปเดตความคืบหน้าของปัญหาที่ควรแก้ไข พร้อมสร้างความมั่นใจกลับมา
  - **กลยุทธ์การให้เหตุผล** คือ การอธิบายถึงข้อเท็จจริงซึ่งในหลายกรณีผู้ที่เคราะห์ร้ายอาจจะมีส่วนเกี่ยวข้องให้เกิดเหตุการณ์ต่างๆด้วย แต่ต้องมีหลักฐานพิสูจน์ชัดเจนโดยวิธีนี้จะสามารถลดระดับความเลวร้ายที่จะส่งผลกระทบต่อชื่อเสียงขององค์กรได้มากขึ้น

** **กลยุทธ์ลดความสำคัญ (Diminishment Posture)** เหมาะสำหรับกรณีที่องค์กรมีส่วนเกี่ยวข้องบางส่วนแต่ไม่ได้ตั้งใจให้เกิดเหตุ จุดสำคัญคือ ‘**ความโปร่งใส**’ และ ‘**การสื่อสารอย่างเห็นอกเห็นใจ**’ เพื่อเปลี่ยนความไม่พอใจของสาธารณชนให้กลายเป็นความเข้าใจและเห็นใจแทน

ตัวอย่างกลยุทธ์ในการตอบโต้วิกฤต

กลุ่มลดความสำคัญ (DIMINISHMENT POSTURE)

กลยุทธ์การขออภัย

- **ตัวอย่าง สำนักงานประกันสังคม ระบบล่มวันสิ้นเดือน (2566)** ระบบ “ตรวจสอบสิทธิ์ประกันสังคม” และ “ขอรับเงินสงเคราะห์บุตร/ชราภาพ” ไม่สามารถใช้งานได้ในหลายพื้นที่ทั่วประเทศ ทำให้ประชาชนจำนวนมากโพสต์ร้องเรียนผ่านโซเชียลมีเดีย
- สำนักงานประกันสังคม ออกแถลงการณ์ขอโทษทันที ผ่านเพจ Facebook และเว็บไซต์ ระบุว่า “ระบบขัดข้องชั่วคราวจากการอัปเกรดฐานข้อมูลกลาง” ยืนยันว่า “ไม่มีข้อมูลผู้ประกันตนสูญหาย” และจะเร่งแก้ไขให้ระบบกลับมาใช้งานได้ภายใน 24 ชั่วโมง ต่อมาได้รายงานความคืบหน้าแบบเรียลไทม์จนระบบกลับมาใช้งานได้
- ช่วยลดความไม่พอใจของผู้ใช้บริการ สร้างความมั่นใจว่าปัญหาไม่ได้เกิดจากความประมาท แต่เป็นผลจากการพัฒนาระบบ
- ประชาชนเข้าใจสถานการณ์มากขึ้น กระแสโซเชียลที่เคยโจมตีเริ่มลดลง และมีผู้แสดงความคิดเห็นเชิงบวก

กลยุทธ์การให้เหตุผล

- **ตัวอย่าง การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) เหตุไฟดับภาคใต้** ส่งผลให้เกิดเหตุไฟฟ้าดับครั้งใหญ่หลายจังหวัดในภาคใต้ ส่งผลกระทบต่อโรงพยาบาล ร้านค้า และประชาชนจำนวนมาก มีผู้ตั้งคำถามว่า “ทำไมระบบสำรองไฟของ กฟผ. จึงไม่ทำงาน?”
- กฟผ. แถลงข่าวทันทีว่า “เหตุไฟดับเกิดจากอุปกรณ์ส่งไฟฟ้ากำลังแรงสูงขัดข้องในระบบส่ง อธิบายว่า “ไม่ใช่ความผิดของเจ้าหน้าที่” และ “ระบบสำรองทำงานตามขั้นตอน แต่แรงดันไฟตกพร้อมกันในหลายจุด ทำให้ฟื้นระบบช้ากว่าปกติ” ยืนยันว่า “ได้ดำเนินการตรวจสอบจุดขัดข้องและฟื้นระบบได้ภายใน 2 ชั่วโมง” พร้อมประกาศแผนเพิ่มระบบสำรองแรงดันและซ้อมแผนรับมือใหม่
- ทำให้ประชาชนเข้าใจว่าปัญหาเกิดจากเหตุขัดข้องทางเทคนิค ไม่ใช่การละเลย ลดแรงวิพากษ์วิจารณ์ และคงภาพลักษณ์ความเชี่ยวชาญขององค์กรด้านพลังงาน

ขั้นตอนการจัดการภาวะวิกฤต

เลือกกลยุทธ์ในการตอบโต้วิกฤต

- **3. กลุ่มบูรณะ (Rebuilding Posture)** หรือกลยุทธ์ฟื้นฟูชื่อเสียงขององค์กร ถือเป็น ขั้นตอนสำคัญที่สุดในวงจรการสื่อสารภาวะวิกฤต (Crisis Communication) เพราะเป็นช่วงที่องค์กรต้อง “ยอมรับความผิดพลาดอย่างเต็มรูปแบบ” และ “ลงมือเยียวยา” เพื่อฟื้นฟูความเชื่อมั่นของสังคมกลับคืนมา เป้าหมายหลักคือ ฟื้นฟูชื่อเสียงและความไว้วางใจของสาธารณชน หลังจากองค์กร “ยอมรับความผิด” หรือ “มีส่วนรับผิดชอบโดยตรง” ต่อเหตุวิกฤตที่เกิดขึ้น ประกอบด้วย
  - **กลยุทธ์การชดเชย** คือ การที่องค์กรแสดงความรับผิดชอบด้วยการ “ชดเชยความเสียหาย” ทั้งในรูปแบบ เงินสด, บริการ, หรือ สิทธิประโยชน์เพิ่มเติม เพื่อบรรเทาความเดือดร้อนของผู้ได้รับผลกระทบ
  - **กลยุทธ์การขอโทษ** คือ การที่องค์กรออกมาขอโทษรับผิดทุกอย่างและยินดีที่จะช่วยเหลือเยียวยาทุกกรณี เป็นการ “ขอโทษอย่างเป็นทางการ” ยอมรับความผิดพลาดทั้งหมด และประกาศความตั้งใจที่จะแก้ไข และป้องกันไม่ให้เกิดซ้ำ

** **กลยุทธ์ “Rebuilding Posture”** เหมาะสำหรับวิกฤตที่องค์กร มีส่วนรับผิดชอบโดยตรง เช่น ความผิดพลาดจากกระบวนการผลิต การบริการ หรือความประมาทเลินเล่อของบุคลากร หัวใจของกลยุทธ์นี้คือ **“การยอมรับ + การชดเชย + การป้องกันซ้ำ”** ผู้นำต้องกล้าเผชิญหน้า แสดงความรับผิดชอบ และสร้างความเชื่อมั่นด้วยการ “ลงมือทำจริง”

ตัวอย่างกลยุทธ์ในการตอบโต้วิกฤต

กลุ่มบูรณะ (REBUILDING POSTURE)

กลยุทธ์การชดเชย

- **ตัวอย่าง การทางพิเศษแห่งประเทศไทย (กทพ.) เหตุป้ายบอกทางร่วงใส่รถยนต์บนทางด่วน** ป้ายบอกทางขนาดใหญ่บนทางพิเศษศรีรัชหล่นใส่รถยนต์ของประชาชน ส่งผลให้รถได้รับความเสียหายและมีผู้บาดเจ็บเล็กน้อย เหตุการณ์นี้ถูกเผยแพร่ในสื่อออนไลน์อย่างกว้างขวาง และประชาชนตั้งคำถามเรื่อง “มาตรฐานความปลอดภัยของโครงสร้างทางด่วน”
- การทางพิเศษแห่งประเทศไทย ได้ออกมาชี้แจงและดำเนินมาตรการ ชดเชยความเสียหายทันที โดยยอมรับความรับผิดชอบโดยตรง ว่าอุบัติเหตุเกิดในพื้นที่ดูแลของ กทพ. จ่ายค่าชดเชยความเสียหายให้เจ้าของรถยนต์ ที่ได้รับผลกระทบจากเหตุการณ์เต็มจำนวน จัดตั้งคณะกรรมการสอบข้อเท็จจริง และสั่งตรวจสอบป้ายบอกทางทุกจุดทั่วเส้นทาง เสนอปรับปรุงมาตรฐานการตรวจสอบความปลอดภัยเชิงป้องกัน
- ประชาชนที่ได้รับผลกระทบยืนยันว่าได้รับการเยียวยาอย่างรวดเร็ว
- ภาพลักษณ์ของ กทพ. ดีขึ้น เพราะ “ยอมรับผิดทันที และชดเชยอย่างโปร่งใส

กลยุทธ์การขอโทษ

- **ตัวอย่าง โรงพยาบาล กรณีผู้ป่วยเสียชีวิตจากความผิดพลาดทางการแพทย์** โดยครอบครัวของผู้ป่วยโพสต์บนโซเชียลว่า “แพทย์วินิจฉัยโรคผิด” จนผู้ป่วยเสียชีวิตก่อนการรักษาที่ถูกต้อง ทำให้เกิดกระแสโจมตีโรงพยาบาลอย่างรุนแรง
- ผู้บริหารโรงพยาบาล ออกมาแถลงข่าวขอโทษอย่างเป็นทางการ ยอมรับว่า “เกิดความผิดพลาดทางขั้นตอนการรักษาจริง“ ประกาศตั้ง “คณะกรรมการสอบข้อเท็จจริง” ภายในทันที พร้อมเยียวยาครอบครัวผู้เสียชีวิต ทั้งค่าชดเชยทางการเงิน และค่ารักษาพยาบาลที่เกี่ยวข้องทั้งหมด รวมทั้งประกาศมาตรการใหม่ เช่น การตรวจทานผลวินิจฉัยซ้ำ สำหรับโรคเรื้อรัง
- สื่อมวลชนและสังคมให้เครดิตในความกล้าที่ “ขอโทษอย่างเป็นทางการ”
- ช่วยลดแรงกดดันทางสังคม และฟื้นฟูความเชื่อมั่นในระดับหนึ่ง

ขั้นตอนการจัดการภาวะวิกฤต

เลือกกลยุทธ์ในการตอบโต้วิกฤต

- **4. กลุ่มเสริม (Bolstering Posture)** หรือการกล่าวถึงความสัมพันธ์อันดีระหว่างองค์กรกับผู้มีส่วนได้ส่วนเสียต่างๆในเหตุการณ์ภาวะวิกฤตนั้นๆ ซึ่งเป็นกลยุทธ์ที่ใช้เสริมกลุ่มอื่นๆข้างต้น ประกอบด้วย
  - **กลยุทธ์เตือนความจำ** ด้วยการย้ำเตือนความดีขององค์กรเมื่อในอดีต เพื่อให้ผู้คนรู้สึก ไม่ดีกับองค์กรน้อยลง เป็นการ “ย้ำถึงผลงานดีในอดีต” เพื่อให้สังคมเห็นว่าองค์กรมีคุณค่าต่อสังคมมาโดยตลอด และไม่ควรถูกตัดสินจากเหตุการณ์เพียงครั้งเดียว
  - **กลยุทธ์การชื่นชม** เพื่อทำให้กลุ่มผู้มีส่วนได้ส่วนเสียเกิดความรู้สึกทางบวกกับองค์กร เพื่อแสดงให้เห็นว่าองค์กรมีความสัมพันธ์อันดีกับผู้มีส่วนได้ส่วนเสียมาโดยตลอด เพื่อให้สังคมรู้ว่าองค์กรมีความสัมพันธ์ที่ดีและเคารพประชาชน
  - **กลยุทธ์ผู้ตกเป็นเหยื่อ** ด้วยการขอความเห็นใจจากสาธารณชนว่าองค์กรได้รับความเสียหายมากน้อยเพียงใด ใช้ “การขอความเห็นใจ” จากสาธารณชน โดยชี้ว่าองค์กรเองก็ได้รับผลกระทบจากเหตุการณ์นั้นเช่นกันเพื่อให้ได้รับความเห็นใจจากสาธารณชน

** **กลยุทธ์กลุ่มเสริม (Bolstering Posture)** ไม่ได้ใช้เพื่อปฏิเสธหรือชดเชย แต่เพื่อรักษาความสัมพันธ์และศรัทธาของสังคมในระยะยาว โดยองค์กรต้องสื่อสารด้วย “น้ำเสียงแห่งความจริงใจ เห็นอกเห็นใจ และเชื่อมโยงกับคุณค่าที่สังคมจดจำ”

ตัวอย่างกลยุทธ์ในการตอบโต้วิกฤต

กลุ่มเสริม (BOLSTERING POSTURE)

กลยุทธ์เตือนความจำ

- **ตัวอย่าง ปตท. (PTT) เหตุน้ำมันรั่วที่ระยอง** เกิดเหตุท่อน้ำมันรั่วกลางอ่าวไทย ทำให้น้ำมันดิบจำนวนมากลอยเข้าชายฝั่งจังหวัดระยอง กระทบต่อชาวประมงและการท่องเที่ยวอย่างรุนแรง สังคมวิพากษ์วิจารณ์องค์กรอย่างหนัก เรื่อง “ความปลอดภัยและความรับผิดชอบต่อสิ่งแวดล้อม”
- ปตท. ออกแถลงการณ์ขอโทษและเร่งฟื้นฟูพื้นที่ทันที นอกจากการชดเชยและฟื้นฟูชายฝั่งแล้ว ยังสื่อสาร “เตือนความจำ” ถึงบทบาทของ ปตท. ว่าเป็น “องค์กรพลังงานแห่งชาติ” ที่สนับสนุนเศรษฐกิจไทยมายาวนานกว่า 30 ปี ย้ำถึงพันธกิจองค์กรที่มุ่งมั่นพัฒนาประเทศอย่างยั่งยืน
- หลังการสื่อสารต่อเนื่อง 6 เดือน ผลสำรวจภาพลักษณ์องค์กรโดย NIDA Poll พบว่า “ประชาชนกลับมามีความเชื่อมั่นมากขึ้น

กลยุทธ์การชื่นชม

- **ตัวอย่าง กระทรวงสาธารณสุข การสื่อสารขอบคุณบุคลากรทางการแพทย์ในช่วงโควิด-19** บุคลากรทางการแพทย์ต้องทำงานหนักมาก เกิดกระแสข่าว “บุคลากรเหนื่อยล้า ถูกตำหนิ และขาดขวัญกำลังใจ” ในขณะเดียวกันก็มีเสียงวิจารณ์กระทรวงสาธารณสุขว่าบริหารวัคซีนล่าช้า
- กระทรวงสาธารณสุข เน้นการสร้างความรู้สึกทางบวกต่อทุกฝ่าย ผู้บริหารระดับสูง ออกมากล่าวชื่นชมและขอบคุณบุคลากรทางการแพทย์ทั่วประเทศ ว่าเป็น “ด่านหน้าแห่งความเสียสละของชาติ” จัดแคมเปญ “ขอบคุณทีมหมอพยาบาล และอสม. ทั่วไทย” ผ่านสื่อทีวีและสื่อออนไลน์ เพื่อสร้างขวัญกำลังใจ และเชิญประชาชนร่วมแสดง “กำลังใจให้บุคลากรทางการแพทย์” ผ่านกิจกรรมออนไลน์
- กระแสสังคมกลับมาเห็นใจบุคลากรทางการแพทย์

กลยุทธ์ผู้ตกเป็นเหยื่อ

- **ตัวอย่าง การรถไฟแห่งประเทศไทย (รฟท.)** เกิดเหตุรถไฟชนรถบรรทุกตัดหน้าทางข้ามในจังหวัดฉะเชิงเทรา มีผู้เสียชีวิตและบาดเจ็บหลายราย ประชาชนบางส่วนโจมตีว่าการรถไฟ “ขาดมาตรการป้องกันอุบัติเหตุ”
- รฟท. ออกแถลงการณ์ขอโทษและแสดงความเสียใจ ชี้แจงว่า “ทางข้ามดังกล่าวอยู่ในเขตชุมชนที่มีป้ายเตือนและสัญญาณไฟครบถ้วน” แต่คนขับรถบรรทุก “ฝ่าฝืนสัญญาณ” พร้อมกล่าวว่า “เจ้าหน้าที่รถไฟเองก็ได้รับบาดเจ็บจากเหตุการณ์” และย้ำว่า “รฟท. เป็นผู้เสียหายร่วม” และจะเร่งเพิ่มมาตรการป้องกันอุบัติเหตุในอนาคต
- แสดงให้เห็นว่าองค์กรไม่ได้เพิกเฉย แต่เป็น “ผู้เสียหายร่วมในเหตุการณ์” ลดแรงโจมตีจากสาธารณชน และขอความเห็นใจจากประชาชน

ขั้นตอนการจัดการภาวะวิกฤต

3. วางแผนสื่อสารกับผู้มีส่วนได้ส่วนเสีย

ทุก ๆ การเกิดเหตุการณ์วิกฤตขึ้นนั้น องค์กรจำเป็นต้องมีการติดต่อสื่อสารกับทั้งคนภายในองค์กร ผู้ที่มีส่วนเกี่ยวข้องทั้งหมด อาทิ พนักงาน ผู้ที่ตกเป็นเหยื่อในเหตุการณ์วิกฤต คู่ค้า สื่อมวลชน และมีผู้ที่มีส่วนเกี่ยวข้องอื่น ๆ เพื่อสร้างสัมพันธ์อันดี และต้องยึดความคาดหวังของผู้มีส่วนได้ส่วนเสียเป็นที่ตั้ง ซึ่งควรปฏิบัติดังนี้

- **แยกกลุ่มเป้าหมาย** ในการรับข้อมูลข่าวสารให้ชัดเจน การสื่อสารไปยังกลุ่มเป้าหมายแต่ละกลุ่มนั้นจำเป็นต้องแยกประเภทเนื้อหาข่าวสารที่เหมาะสมกับความต้องการในแต่ละกลุ่ม
- **เตรียมเนื้อหา** หรือสิ่งที่จะพูดให้พร้อม ที่ต้องมีความกระชับ ชัดเจน ไม่กำกวม สื่อสารอย่างตรงไปตรงมาให้เหมาะสมกับแต่ละกลุ่มเป้าหมาย
- **เลือกใช้สื่ออย่างเหมาะสม** ที่เข้าถึงกลุ่มเป้าหมายได้อย่างมีประสิทธิภาพ

ตัวอย่าง การวางแผนสื่อสารกับผู้มีส่วนได้ส่วนเสีย กรมควบคุมมลพิษ

เหตุการณ์น้ำเสียในคลองแสนแสบจากโรงงานอุตสาหกรรมรั่วไหล (ปี 2566) มีการร้องเรียนจากประชาชนว่ามีกลิ่นเหม็นและน้ำในคลองกลายเป็นสีดำ ต่อมาพบว่าเกิดจากน้ำเสียรั่วจากโรงงานอุตสาหกรรมในพื้นที่จังหวัดฉะเชิงเทรา ประชาชนเรียกร้องให้หน่วยงานรัฐเร่งดำเนินการตรวจสอบและแก้ไข

1 แยกกลุ่มเป้าหมายการสื่อสารอย่างชัดเจน

แยกผู้รับสารออกเป็น 4 กลุ่มหลัก

- ประชาชนในพื้นที่ : ต้องการรู้สาเหตุ ความปลอดภัย และมาตรการแก้ไข สื่อสารโดยแถลงข่าวชี้แจง, อินโฟกราฟิกออนไลน์, เวทีชี้แจงในพื้นที่
- ผู้ประกอบการ/โรงงาน : ต้องรู้แนวทางตรวจสอบและบทลงโทษ สื่อสารโดยทำหนังสือเวียน, ประชุมร่วมกับสมาคมโรงงาน
- สื่อมวลชน : ต้องการข้อมูลที่ถูกต้องและทันเวลา สื่อสารโดยแถลงข่าวอย่างเป็นทางการ, ศูนย์สื่อเฉพาะกิจ
- หน่วยงานท้องถิ่น : ต้องการแนวทางร่วมมือในการฟื้นฟู สื่อสารโดยประชุมบูรณาการ, ช่องทางไลน์กลุ่มราชการเฉพาะกิจ

2 เตรียมเนื้อหาสื่อสารที่กระชับ ชัดเจน ไม่กำกวม

กรมควบคุมมลพิษจัดทำ “ข้อความหลัก” สำหรับแต่ละกลุ่ม ดังนี้

- ประชาชนในพื้นที่ : “ไม่มีสารพิษรุนแรงในน้ำ – รัฐเร่งฟื้นฟูคุณภาพน้ำใน 7 วัน และตั้งจุดรับร้องเรียนตลอด 24 ชม.”
- ผู้ประกอบการ/โรงงาน : “ตรวจสอบการปล่อยน้ำเสียทุกโรงงานภายใน 48 ชม. หากฝ่าฝืนจะถูกระงับใบอนุญาต”
- สื่อมวลชน : “หน่วยงานพร้อมเปิดข้อมูลตรวจวัดคุณภาพน้ำแบบเรียลไทม์ผ่านเว็บไซต์กรมฯ”
- หน่วยงานท้องถิ่น : “ร่วมกันจัดทีมเคลื่อนที่เร็ว (Environmental Rapid Response Team)”

3 เลือกใช้สื่ออย่างเหมาะสมให้เข้าถึงกลุ่มเป้าหมาย

กรมควบคุมมลพิษเลือกใช้ช่องทางต่าง ๆ ที่เหมาะกับกลุ่มเป้าหมาย เช่น

- ประชาชนในพื้นที่ : ใช้สื่อ “Facebook Page / Line Official / วิทยุชุมชน / เวทีชี้แจงในพื้นที่ เพื่อเน้นความเข้าใจง่ายและเข้าถึงเร็ว
- ผู้ประกอบการ/โรงงาน : ใช้หนังสือราชการ / อีเมล / ระบบ e-Meeting ใช้ช่องทางทางการเพื่อแจ้งแนวปฏิบัติ
- สื่อมวลชน : ใช้ศูนย์ข้อมูลข่าวสารเฉพาะกิจ / แถลงข่าวออนไลน์ เพื่อส่งข้อมูล Fact Sheet และภาพข่าว
- หน่วยงานท้องถิ่น : ใช้กลุ่มไลน์ราชการ / ระบบสารบรรณกลาง / ประชุมร่วม เพื่อให้สื่อสารในแนวเดียวกันและลดความสับสน

ขั้นตอนการจัดการภาวะวิกฤต

4. ตั้งหน่วยงานเฉพาะกิจและผู้แถลงการณ์

การตั้งทีมงานที่เกี่ยวข้องกับการรับมือในภาวะวิกฤตนั้นเป็นสิ่งสำคัญ ที่จะเป็นศูนย์กลางในการปฏิบัติการต่างๆ รวมถึงประสานงานกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง รวมถึงผู้แถลงการณ์ในภาวะวิกฤต ซึ่งจำเป็นต้องมีคุณสมบัติ ดังนี้

- ทีมงานต้องมีอำนาจอย่างเต็มที่ในการจัดการกับภาวะวิกฤต เพราะวิกฤตนั้นเป็นเรื่องที่รอไม่ได้ การให้อำนาจเด็ดขาดในการบริหารจัดการ จะทำให้เกิดความคล่องตัวในการแก้ไขปัญหาต่างๆได้ดีขึ้น
- ผู้แถลงการณ์ต้องมีความเชี่ยวชาญ และความชำนาญในการสื่อสารได้เป็นอย่างดี และมีภาพลักษณ์ที่ดูจริงใจ
- ทีมงานต้องมีสภาวะทางอารมณ์ที่มั่นคง ทำงานภายใต้แรงกดดันอย่างมหาศาลกับสถานการณ์ต่างๆได้ ซึ่งทีมงานต้องมีข้อมูลข้อเท็จจริง และทำความเข้าใจสถานการณ์ที่กำลังเผชิญอยู่ให้ได้อย่างถูกต้องและชัดเจน

ตัวอย่าง การตั้งหน่วยงานเฉพาะกิจและผู้แถลงการณ์

การตั้ง “ศูนย์ปฏิบัติการชายแดนไทย–กัมพูชา” และผู้แถลงการณ์

- ในวิกฤตชายแดน สิ่งสำคัญคือต้องมี ศูนย์กลางการตัดสินใจ (Single Center of Authority) เพื่อให้การตอบสนองรวดเร็วและบูรณาการ
- ผู้แถลงข่าวต้องเป็นตัวแทนที่น่าเชื่อถือ ถ้อยคำต้อง “มีเหตุผล – มีจังหวะ – มีสติมากกว่าอารมณ์”
- การแถลงข่าวควรมีความสม่ำเสมอ (เช้า/เย็น) และยึดข้อมูลจริงเป็นหลัก เพื่อควบคุมข่าวลือ

สถานการณ์ชายแดนไทย-กัมพูชา

โดยอธิบดีกรมสารนิเทศและโฆษกกระทรวงการต่างประเทศ

01 หน่วยงานเฉพาะกิจ / ศูนย์กลาง

- รัฐบาลตั้ง “ศูนย์ตอบโต้สถานการณ์ชายแดนไทย–กัมพูชา” โดยมีคณะกรรมการที่รวมกระทรวงต่างประเทศ, กลาโหม, กองทัพ, กรมประชาสัมพันธ์, และหน่วยงานภาคท้องถิ่นในพื้นที่ชายแดน

02 อำนาจในการตัดสินใจ

- ศูนย์นี้มีอำนาจสั่งปิดด่าน, ย้ายประชาชน, ควบคุมข้อมูล และประสานกับหน่วยงานทหารอย่างรวดเร็วโดยไม่ต้องรอขั้นตอนปกติ

03 ผู้แถลงการณ์หลัก

- โฆษกกระทรวงการต่างประเทศ หรือโฆษกกองทัพบก, โฆษกทัพภาคที่ 2 สามารถทำหน้าที่แถลงสถานการณ์อย่างเป็นทางการ

04 คุณสมบัติผู้แถลงข่าว

- มีความรู้เชิงการต่างประเทศ / ความมั่นคง
- ใช้ถ้อยคำกลาง ไม่ก้าวร้าว
- มีภาพลักษณ์แน่วแน่และเป็นธรรม
- สามารถสื่อสารกับสื่อมวลชนทั้งในและต่างประเทศ

05 หน้าที่และกิจกรรม

- แถลงสถานการณ์ชายแดนรายเช้า / รายค่ำ ผ่านสื่อแห่งทางการ
- ตอบคำถามสื่อมวลชน / ชี้แจงข้อเท็จจริง
- ประสานข้อมูลระหว่างหน่วยงานในประเทศและเอกชน / ชาวบ้านชายแดน
- ตรวจสอบและเผยแพร่ข้อมูล real-time ผ่านเว็บไซต์ราชการ / แพลตฟอร์มโซเชียลของรัฐ

กรณีศึกษา การใช้กลยุทธ์การจัดการภาวะวิกฤต

KFC ลงโฆษณาว่าตัวเองเป็น FCK เพราะไม่มีไก่ให้ขาย

- เหตุการณ์นี้เป็นวิกฤตของ KFC ที่เกิดขึ้นในประเทศอังกฤษในปี 2561 วิกฤตครั้งนี้เกิดจาก KFC เปลี่ยนสายส่งวัตถุดิบของ KFC การจัดการด้านขนส่งที่ผิดพลาด ทำให้ KFC 700 สาขาไม่มีไก่ที่เป็นวัตถุดิบมาให้บริการลูกค้า
- KFC ออกมาน้อมรับความผิดพลาดด้วยการลงโฆษณาขอโทษลูกค้าผ่านหนังสือพิมพ์ Metro 1 หน้าเต็ม ในโฆษณานั้น KFC ยังออกมาว่าตัวเองด้วยการเปลี่ยนโลโก้ KFC เป็น FCK อยู่บนถังใส่ไก่ที่ไม่มีไก่ ซึ่งคำว่า FCK เป็นการล้อเลียนกับคำว่า F_CK
- พร้อมข้อความที่กล่าวว่าตัวเองว่า ร้านขายไก่ทอดไม่มีขายไก่ เป็นสิ่งที่ไม่สมควร และขออภัยลูกค้าที่เดินทางมาร้านและไม่มีไก่ให้กิน และสัญญาว่าจะเร่งส่งไก่ไปที่สาขาให้เร็วที่สุด
- โฆษณาของ KFC ที่ออกมาขอโทษในวิกฤตไม่มีไก่ นอกจากจะสร้างความรู้สึกให้อภัยจากลูกค้าและรัก KFC มากขึ้นจากการมองว่า KFC ยังกล้ายอมรับความผิดพลาดและว่าตัวเองถึงเหตุการณ์ดังกล่าวอีกด้วย

กรณีศึกษา โออิชิ กับ สิ่งแปลกปลอมในขวด

- เมื่อปี 2548 ขาเขียวโออิชิถูกผู้บริโภคร้องเรียนถึง 2 ครั้งในเวลาใกล้เคียงกัน ครั้งแรกร้องเรียนว่าชาเขียวโออิชิที่ดื่มมีกรดเกลือเจือปน ทำให้รู้สึกแสบปากและลำคอจนต้องเข้ารับการรักษาที่โรงพยาบาล และเรื่องที่สองคือพบสิ่งแปลกปลอมในชาเขียวที่มีลักษณะเหมือนเชื้อราทำให้เกิดท้องเสียอย่างรุนแรงหลังดื่มขาเขียวไป
- ตัน ภาสกรนที ประธานกรรมการ ในเวลานั้น ออกมาแก้ไขวิกฤตในครั้งนั้นด้วยการออกมาขอโทษและเดินทางไปเยี่ยมลูกค้าที่ได้รับผลกระทบจากการดื่มชาเขียวโออิชิด้วยตัวเอง พร้อมกับออกค่ารักษาพยาบาลให้ทั้งหมด
- ได้ออกมาขอโทษสังคมและชี้แจงยืนยันถึงกระบวนการผลิตที่รัดกุม และสร้างความมั่นใจด้วยการเปิดโรงงานให้สำนักงานสาธารณสุขจังหวัดปทุมธานี เข้าตรวจสอบระบบการผลิตภายในโรงงาน และเก็บชาเขียวล็อตที่มีปัญหาออกจากตลาดทั้งหมด และนำนักข่าวเข้าไปทำข่าวที่โรงงานดูขั้นตอนการผลิต เพื่อสร้างความเชื่อมั่นแก่ผู้ผู้บริโภค
- สร้างแคมเปญรวยฟ้าผ่า พลิกฝาโออิชิ กรีนที ลุ้นรางวัลเงินสด 1 ล้านบาททันที ใต้ฝาขวด ขึ้นเป็นครั้งแรก

กรณีศึกษา อิชิตัน หมดสต๊อก ไม่มีขาย

- เพจเฟซบุ๊ก ตัน ภาสกรนที ได้โพสต์ระบุว่า “ขอโทษลูกค้าและคู่ค้าทุกท่านที่อิชิตันผลิตสินค้าส่งไม่ทัน หมดสต็อกชั่วคราว แม้จะเพิ่มกำลังการผลิตเป็น 100 ล้านขวดต่อเดือน แต่ของก็ยังไม่ทันส่ง เรากำลังเร่งมือทั้งวันทั้งคืนเพื่อส่งมอบสินค้าให้ทุกท่านเร็วที่สุด”
- กลุ่มลูกค้ามาแสดงตัวในคอมเมนท์เป็นวัยรุ่นสายเขียว หลายคนมาชี้เป้าถึงประโยชน์ของขวดรุ่นนี้ เช่น รุ่นปากขวดกว้าง ที่หลายคนกลับเอาไปทำเป็นบ้องกัญชา บางคนบอกว่าขวดรุ่นนี้ใช้งานดีมาก บางคนเอาไปผสมในสูตรต้มน้ำกระท่อม จึงทำให้ขายดีจนสินค้าขาดตลาด

กรณีศึกษา โรงพยาบาลโดนแฮกข้อมูล

- ข้อมูลคนไข้ของโรงพยาบาลถูกแฮกและนำมาเรียกค่าไถ่
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร แถลงข่าวกรณีการแฮกข้อมูลผู้ป่วยของกระทรวงสาธารณสุข ถูกแฮกข้อมูลผู้ป่วยไปโพสต์ขายบนเว็บไซต์ เมื่อวันที่ 5 กันยายน 2564 จึงร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ลงตรวจสอบข้อเท็จจริงและประเมินความเสียหายทันที และเร่งแก้ไขเหตุการณ์ที่เกิดขึ้น โดยการกู้คืนข้อมูล และจัดการการเข้าถึงระบบ

กรณีศึกษา ข้าว 10 ปี

การพลิกฟื้น หลังวิกฤต

- เมื่อเหตุการณ์วิกฤตผ่านพ้นไป หรือสามารถจัดการกับปัญหาต่าง ๆ ได้สำเร็จ คณะกรรมการเฉพาะกิจบริหารภาวะวิกฤต จะต้องประสานแผนการพลิกฟื้นองค์การ (Disaster Recovery Plan : DRP) เพื่อให้การผ่านพ้นจากภาวะวิกฤตเป็นไปอย่างมีเสถียรภาพ
- จัดการสรุปบทเรียน (Lesson Learn) ประเด็นความเสี่ยง การควบคุม และข้อเสนอแนะอื่น ๆ เพื่อการบริหารความเสี่ยงที่มีประสิทธิภาพยิ่งขึ้น
- แผนการพลิกฟื้นธุรกิจ (Disaster Recovery Plan : DRP) เป็นขั้นตอนเพื่อทำให้องค์การกลับเข้าสู่ภาวะของการดำเนินงานปกติภายหลังจากที่ได้เผชิญกับสถานการณ์วิกฤตต่าง ๆ ด้วยการจัดการกับสิ่งคุกคามและผลกระทบที่เกิดขึ้น ฟื้นฟูความเสียหาย สร้างความเชื่อมั่นแก่ ลูกค้า พนักงาน สังคม และผู้มีส่วนได้เสียทุกกลุ่ม

การพลิกฟื้น หลังวิฤต

1 การก่อร่างแผน / จัดทำแผนฟื้นฟู (Assemble Plan)

- การประเมินความพร้อมทางด้านโครงสร้างพื้นฐานขององค์การ
- การบริหารความเสี่ยงในทุกด้าน จะต้องพิจารณาในเรื่องของแผนการพลิกฟื้นองค์การด้วยเสมอ
- แผนการพลิกฟื้นองค์การ จะต้องได้รับการทดสอบ และทบทวนเป็นประจำ เพื่อสร้างความเชื่อมั่นที่มีต่อแผน
- จะต้องมีการสื่อสารแผนการพลิกฟื้นองค์การ ให้พนักงานได้เรียนรู้ รับทราบ และตื่นตัวอยู่เสมอ
- โดยมีวัตถุประสงค์
  - เพื่อจัดทำเอกสารแผนการพลิกฟื้นองค์การ สำหรับผู้บริหารหน่วยงานและพนักงานใช้เป็นแนวทางการปฏิบัติงาน
  - เพื่อให้กระบวนการพลิกฟื้นองค์การจากเหตุการณ์วิกฤต เป็นกระบวนการที่ดี มีประสิทธิภาพ
  - เพื่อให้มีกระบวนการตอบสนองสถานการณ์วิกฤตอย่างเป็นระบบ สามารถควบคุมเหตุการณ์ได้อย่างรวดเร็ว ส่งผลกระทบในวงจำกัด และพลิกฟื้นสู่ภาวะปกติได้อย่างมีประสิทธิภาพ
  - เพื่อให้พนักงานและบุคคลที่เกี่ยวข้อง มีความเข้าใจตรงกันในการดำเนินการพลิกฟื้นองค์การด้านต่าง ๆ เพื่อประสิทธิภาพของการสื่อสาร

การพลิกฟื้น หลังวิกฤต

2 การระบุขอบเขตผลกระทบ (Identify Scope)

- การกำหนดขอบเขตของการดำเนินการฟื้นฟูองค์การ ภายหลังเหตุการณ์วิกฤตนั้น มีการประเมินเหตุการณ์วิกฤตที่อาจเกิดขึ้น ความเสี่ยงหรือผลกระทบที่อาจจะเกิดขึ้น ซึ่งจะเกี่ยวข้องกับความเสียหายต่าง ๆ หลังวิกฤต เช่น

Crisis	Disaster / Possible Loss	Scope of Recovery	Priority
1.ไฟไหม้สำนักงาน	1.1 อาคารสำนักงานเสียหายทั้งหมด	1.1 การสำรวจความเสียหายและการ Claim ประกัน	1
	1.2.อุปกรณ์เครื่องมือเครื่องใช้เสียหาย	1.2 การจัดหาสำนักงานชั่วคราว	1
		1.3 การจัดสรรงบประมาณเพื่อฟื้นฟู	1
	1.3 เอกสารทางบัญชีการเงิน เสียหาย	1.4การจัดทำสำเนาเอกสารจากระบบสำรอง	2
		1.5การจัดหาแบบสำรองจากหน่วยงานอื่น ๆ	2
	1.4 เอกสารแบบไฟฟ้า และก่อสร้างเสียหาย	1.6 การจัดหาสำนักงานถาวร (ใหม่)	2

การพลิกฟื้น หลังวิกฤต

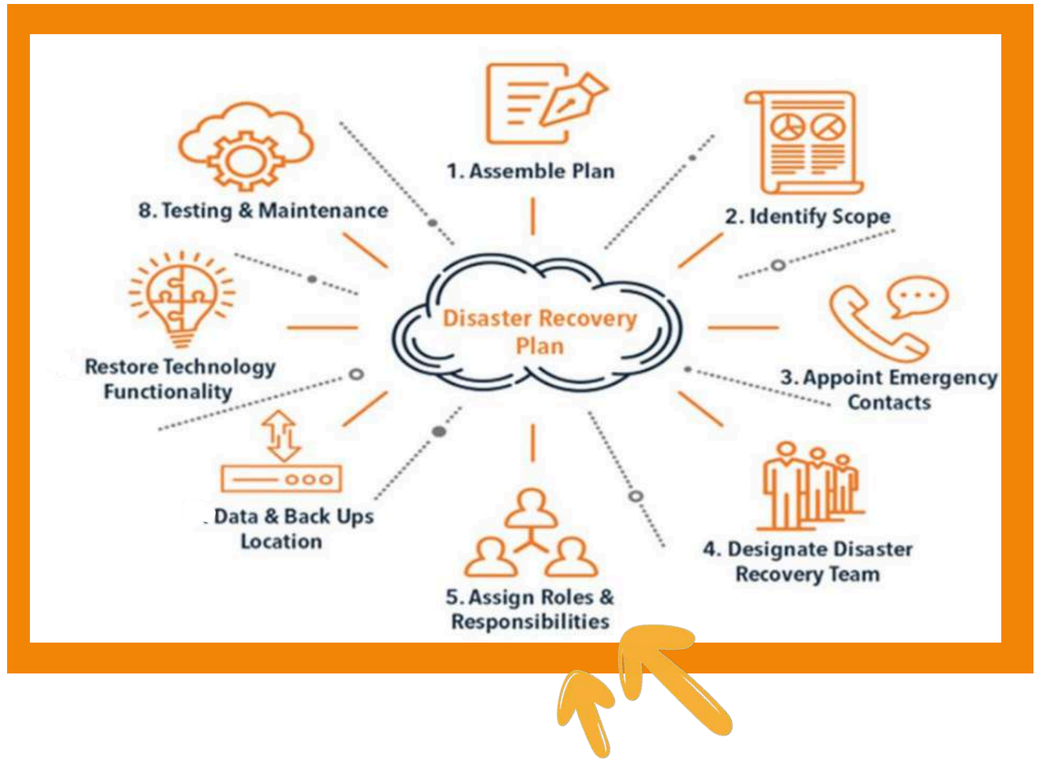
3 กำหนดหมายเลข/ช่องทางติดต่อฉุกเฉิน (Appoint Emergency Contacts)

- เลขหมายโทรศัพท์ในด้านต่าง ๆ เพื่อใช้ในการติดต่อ ประสานงานที่สำคัญในแต่ละด้านภายหลังเหตุการณ์วิกฤต เพื่อให้การพลิกฟื้นการดำเนินงานเป็นไปอย่างมีระบบ เป็นเอกภาพ ไม่สับสน
- มักจะเป็นเลขหมายโทรศัพท์ของทีมงานเฉพาะกิจ หรือ หน่วยงานสนับสนุนด้านต่าง ๆ เช่น ฝ่ายบุคคล บัญชี การเงิน อำนวยการ กลาง และ IT เป็นต้น รวมถึงเลขหมายหน่วยงานภายนอกในกรณีวิกฤตฉุกเฉิน

4 การกำหนดทีมงานฟื้นฟูการดำเนินงาน (Designate Disaster Recovery Team)

- โดยคณะกรรมการเฉพาะกิจบริหารภาวะวิกฤต เป็นผู้กำหนดบุคคล ซึ่งเป็นตัวแทนของหน่วยงานต่าง ๆ ทำหน้าที่ในคณะทำงานเฉพาะกิจ เพื่อการฟื้นฟูการดำเนินงาน ให้กลับเข้าสู่ภาวะปกติ

การพลิกฟื้น หลังวิกฤต



5 การกำหนดบทบาท หน้าที่ของทีม (Assign Roles ard Responsibilities)

- หน้าที่อำนวยการ และจัดหาทรัพยากรที่จำเป็น เพื่อให้หน่วยงานต่าง ๆ สามารถเพิ่มขีดความสามารถในการปฏิบัติงานได้ในระดับปกติ
- หน้าประสานงานกับคณะทำงานเหตุการณ์วิกฤต (Crisis Working Team - CWT) ในการประเมินความเสียหายและเสนอแนวทางการฟื้นฟู ตรวจสอบ กำกับ การดำเนินงาน และติดตั้งระบบงานเพิ่มเติมให้มีความสมบูรณ์ เพื่อให้สามารถบริการลูกค้าประชาชน และผู้ปฏิบัติงานได้เช่นเดิม
- ให้ความช่วยเหลือหน่วยงานต่าง ๆ ในการเพิ่มขีดความสามารถในการปฏิบัติงาน ให้ได้ในระดับปกติ

การพลิกฟื้น หลังวิกฤต

6 ข้อมูลและสถานที่สำรอง (Data and Back-up Location)

- ตรวจสอบฐานข้อมูลประเภทต่าง ๆ สถานที่ใช้เก็บสำรองข้อมูล สถานที่สำรองเพื่อรองรับการปฏิบัติงาน สถานที่สำรองเพื่อจัดเก็บสินค้า เครื่องมือ เครื่องจักรกล เป็นต้น
- เพื่อให้สามารถนำมาใช้ได้ทันทีภายหลังวิกฤต รวมถึงพัฒนา ปรับปรุง เพิ่มขีดความสามารถในด้านต่าง ๆ ให้ได้เทียบเท่าระดับการปฏิบัติงานปกติ

7 การติดตั้งระบบงาน และการเริ่มทำงานใหม่ (Restore Technology and Functionality)

- เมื่อมีความพร้อมทางด้านสถานที่ ข้อมูล เครื่องมือเครื่องใช้ บุคลากร และทรัพยากรอื่น ๆ ที่จำเป็นแล้ว การติดตั้งระบบงาน Applications และโปรแกรมการปฏิบัติงาน เพื่อเริ่มปฏิบัติงานจริง หลังจากต้องหยุดชะงักจากเหตุการณ์วิกฤต และหน่วยงานแต่ละส่วนร่วมกันดำเนินการ

การพลิกฟื้น หลังวิฤต

8 การทดสอบและรักษาสถานภาพ (Testing and Maintenance)

- เป็นการทดสอบกระบวนการปฏิบัติงาน และ ระบบงานว่าสามารถปฏิบัติงานได้อย่างสม่ำเสมอ ถูกต้อง และต่อเนื่องเช่นเดิมหรือไม่ มีส่วนใดบกพร่องต้องปรับปรุง มีกระบวนการปฏิบัติงานใด ๆ ที่จำเป็นต้องเปลี่ยนแปลง แตกต่างไปจากเดิม หรือไม่
- จะต้องจัดทำคู่มือการปฏิบัติงานใด ๆ เพิ่มเติมอีกบ้าง การรักษามาตรฐาน และ ความสม่ำเสมอในการปฏิบัติงาน และพัฒนาปรับปรุงให้มีประสิทธิภาพดียิ่งขึ้น

** สรุป Disaster Recovery Plan (DRP) เป็น “เครื่องมือหลังวิกฤต” ที่ช่วยให้องค์กรฟื้นฟูระบบงานได้อย่างรวดเร็วและมีประสิทธิภาพ โดยหัวใจสำคัญคือการเตรียมทีมที่พร้อม, มีข้อมูลสำรองที่ปลอดภัย, และฝึกซ้อมอย่างต่อเนื่อง

ตัวอย่างกรณีศึกษา

ระบบฐานข้อมูลประชาชนของหน่วยงานภาครัฐถูกโจมตีทางไซเบอร์ ทำให้ระบบล่มทั่วประเทศเป็นเวลา 12 ชั่วโมง

เป้าหมายของแผนฟื้นฟู : ฟื้นฟูระบบบริการภาครัฐให้กลับมาใช้งานได้ภายใน 24 ชั่วโมง โดยไม่กระทบต่อข้อมูลประชาชนและความเชื่อมั่นของสังคม

01

Assemble Plan
จัดทำแผนฟื้นฟู

- เริ่มจากการวางแผนอย่างเป็นระบบ โดยระบุเป้าหมายหลักของการฟื้นฟู เช่น เวลากู้คืนระบบ และระดับข้อมูลที่ต้องกู้คืน
- ตัวอย่าง กระทรวงดิจิทัลฯ ร่วมกับสำนักงานพัฒนารัฐบาลดิจิทัล (DGA) จัดทำ “แผนฟื้นฟูระบบฐานข้อมูลภาครัฐ” โดยตั้งเป้าให้ระบบกลับมาใช้งานได้ภายใน 24 ชม. และข้อมูลไม่สูญหายเกิน 30 นาที

02

Identify Scope
ระบุขอบเขตของผลกระทบ

- กำหนดว่าระบบใดบ้างที่ต้องกู้คืนก่อน–หลัง เพื่อให้ทราบลำดับความสำคัญ
- ตัวอย่าง ทีม IT ระบุว่า ระบบที่ต้องกู้คืนเร่งด่วน 3 อันดับแรก คือ
  - 1. ระบบลงทะเบียนบัตรประชาชน
  - 2. ระบบโอนข้อมูลบริการภาครัฐ (Gov Data Exchange)
  - 3. ระบบติดต่อหน่วยงานจังหวัด

03

Appoint Emergency Contacts
กำหนดหมายเลข/ช่องทางติดต่อฉุกเฉิน

- ระบุผู้ที่ต้องติดต่อทันทีเมื่อเกิดเหตุ เช่น ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ, ผู้ประสานกับศูนย์ความมั่นคงไซเบอร์, และผู้แถลงข่าว
- ตัวอย่าง มีการตั้ง “สายด่วนฟื้นฟูระบบ” และ “กลุ่ม LINE Crisis Command”
- เพื่อให้ผู้บริหาร, เจ้าหน้าที่ IT, และสื่อสารองค์กรติดต่อกันได้ทันที

04

Designate Disaster Recovery Team
แต่งตั้งทีมเฉพาะกิจฟื้นฟูระบบ

- แต่งตั้งทีมงานที่มีหน้าที่ชัดเจนในการดำเนินการ เช่น ทีมกู้ข้อมูล, ทีมระบบเครือข่าย, ทีมสื่อสารภายใน และทีมโฆษกองค์กร
- ตัวอย่าง สำนักงานพัฒนารัฐบาลดิจิทัล (DGA) ตั้ง “ทีมฟื้นฟูระบบและป้องกันข้อมูลรั่วไหลอย่างเร่งด่วน (Disaster Recovery Plan Team for Government: DRP)” นำโดย CIO และผู้แทนจาก สกมช. (สำนักงานความมั่นคงไซเบอร์แห่งชาติ)
- เพื่อรับผิดชอบฟื้นฟูเซิร์ฟเวอร์หลักและตรวจสอบการรั่วไหลของข้อมูล

ตัวอย่างกรณีศึกษา

ระบบฐานข้อมูลประชาชนของหน่วยงานภาครัฐถูกโจมตีทางไซเบอร์ ทำให้ระบบล่มทั่วประเทศเป็นเวลา 12 ชั่วโมง

เป้าหมายของแผนฟื้นฟู : ฟื้นฟูระบบบริการภาครัฐให้กลับมาใช้งานได้ภายใน 24 ชั่วโมง โดยไม่กระทบต่อข้อมูลประชาชนและความเชื่อมั่นของสังคม

5

Assign Roles & Responsibilities
กำหนดบทบาทหน้าที่ของแต่ละฝ่าย

- ระบุว่าใครต้องทำอะไร ระหว่างวิกฤต เช่น ใครเป็นผู้อนุมัติการกู้คืนระบบ ใครรับผิดชอบสื่อสารต่อสาธารณะ
- ตัวอย่าง
  - ทีมเทคนิค กู้คืนระบบและตรวจสอบความปลอดภัย
  - ทีมสื่อสารองค์กร แถลงข่าวต่อประชาชน
  - ทีมบริหาร อนุมัติการเปิดระบบใหม่
  - ทีมกฎหมาย ตรวจสอบผลกระทบด้านข้อมูลส่วนบุคคล (PDPA)

6

Data & Backups Location
ระบุแหล่งเก็บข้อมูลสำรอง

- จัดเก็บข้อมูลสำรอง (Backup) ไว้ในพื้นที่ที่ปลอดภัย เช่น Cloud สำรอง หรือศูนย์ข้อมูลสำรอง (Data Center Backup Site)
- ตัวอย่าง หน่วยงานใช้ระบบ “Government Cloud” และมี Backup Site ที่จังหวัดเชียงใหม่
- เพื่อให้กู้ข้อมูลได้แม้ระบบส่วนกลางในกรุงเทพฯ ถูกโจมตี

7

Restore Technology Functionality
ฟื้นฟูระบบเทคโนโลยี

- เมื่อระบบพร้อม ต้องดำเนินการฟื้นฟูเซิร์ฟเวอร์ โปรแกรม และเครือข่าย ให้กลับมาทำงานตามลำดับความสำคัญที่กำหนด
- ตัวอย่าง ทีมเทคนิคเริ่มเปิดระบบ Gov Data Exchange ก่อน เพื่อให้หน่วยงานต่าง ๆ สามารถเชื่อมข้อมูลกันได้
- จากนั้นค่อยฟื้นฟูระบบบริการประชาชนอื่น ๆ เช่น ระบบ Smart ID และ e-Services

8

Testing & Maintenance
ทดสอบและปรับปรุงแผน

- หลังจากฟื้นฟูระบบ ต้องมีการทดสอบการทำงานของระบบและปรับปรุงแผนฟื้นฟู (DRP) เพื่อให้มีประสิทธิภาพมากขึ้นในอนาคต
- ตัวอย่าง หลังวิกฤต ทีมฟื้นฟู (DRP) จัด “Simulated Cyber Attack Test” ทุก 6 เดือน และปรับปรุงคู่มือการฟื้นฟู (Recovery Playbook) ให้ครอบคลุมภัยไซเบอร์ยุคใหม่ เช่น Ransomware และ AI Threat เป็นต้น

การบริหารความเสี่ยงองค์กร

Enterprise Risk management

Enterprise Risk Management

ประเทศไทยมีการบริหารจัดการหลายภาคส่วน
เพื่อพัฒนาประเทศชาติให้เจริญก้าวหน้าในทุกด้าน
เหมือนกับอารยะประเทศ ในการบริหารจัดการ
ทั้งภาครัฐและเอกชน ย่อมต้องมีความเสี่ยงองค์กร
การบริหารความเสี่ยง ผู้บริหารองค์กร เจ้าหน้าที่ผู้ปฏิบัติงาน
พนักงานทุกคนในองค์กร ควรจะต้องเข้าใจในพื้นฐานของ
แนวความคิดของการบริหารความเสี่ยง
ที่ทุกคนในองค์กรต้องทำความเข้าใจร่วมกัน เพื่อให้การ
บริหารความเสี่ยงบรรลุเป้าประสงค์
วิสัยทัศน์ และพันธกิจขององค์กร

ความเสี่ยง

ความหมาย

- คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่
- ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา เกิดจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จ ตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ
- ความเสี่ยง คือ เหตุการณ์การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบสร้างความเสียหายความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ทั้งในระดับองค์การระดับหน่วยงานและระดับบุคคลได้

ความเสี่ยง

นิยาม

- โอกาสที่เกิดขึ้นแล้วธุรกิจจะเกิดความเสียหาย (Chance of Loss)
- ความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ (Possibility of Loss)
- ความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event)
- การคลาดเคลื่อนของการคาดการณ์ (Dispersion of Actual Result)
- ความไม่แน่นอนของเหตุการณ์ ซึ่งไม่สามารถคาดเดาได้ว่าจะเกิดขึ้นเมื่อใด แต่ความเสี่ยงนั้น ๆ จะมีแนวโน้มที่เกิดขึ้นไม่มากก็น้อยในองค์กร

ความเสี่ยง

ศัพท์ทางเทคนิค ที่เกี่ยวข้อง

- **ภัย (Peril)** คือ สาเหตุของความเสียหาย ซึ่งภัยสามารถเกิดขึ้นได้จากภัยธรรมชาติ เช่น เกิดพายุ สึนามิ น้ำท่วม แผ่นดินไหว เป็นต้น ภัยนอกจากจะเกิดขึ้นได้จากภัยธรรมชาติแล้ว ภัยนั้นยังเกิดขึ้นจากการกระทำของมนุษย์ เช่น อัคคีภัย จลาจล ฆาตกรรม เป็นต้น สำหรับสาเหตุสุดท้ายที่จะเกิดภัยได้นั้นคือภัยที่เกิดขึ้นจากภาวะเศรษฐกิจ เพราะภัยที่เกิดจากภาวะเศรษฐกิจ เป็นอีกสาเหตุที่สำคัญ เพราะเมื่อเกิดขึ้นแล้วคนทั้งประเทศ หรือทั้งภูมิภาคจะได้รับผลกระทบอย่างกว้างขวาง
- **สภาวะที่จะทำให้เกิดความเสียหาย (Hazard)** คือ สภาพเงื่อนไขที่เป็นสาเหตุที่ทำให้ ความเสียหายเพิ่มสูงขึ้น โดยสภาวะต่าง ๆ นี้สามารถแบ่งออกได้เป็น สภาวะทางด้านกายภาพ คือ สภาวะของโอกาสที่จะเกิดความเสียหาย เช่น ชนิดและทำเล ที่ตั้ง ของสิ่งปลูกสร้าง อาจเอื้อต่อการเกิดเพลิงไหม้ สภาวะทางด้านศีลธรรม (Moral) คือ สภาวะของโอกาสที่จะเกิดขึ้นจากความไม่ซื่อสัตย์ต่อหน้าที่การงาน เช่น การฉ้อโกงของพนักงาน และสภาวะด้านจิตสำนึกในการป้องกันความเสี่ยง (Morale) คือ สภาวะที่ไม่ประมาทและเลินเล่อ หรือการไม่เอาใจใส่ในการป้องกันความเสี่ยง เช่น การที่พนักงานปล่อยให้เครื่องจักรทำงานโดยไม่ควบคุม

การบริหารความเสี่ยง

Risk Management

- กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด
- เป็นการประกอบกันอย่างลงตัวของวัฒนธรรมองค์กร กระบวนการและโครงสร้างองค์กร ซึ่งมีผลโดยตรงต่อประสิทธิภาพการบริหาร และผลได้ผลเสียขององค์กร

Enterprise Wide Risk Management

- การบริหารความเสี่ยงขององค์กรโดยรวม คือ การบริหารความเสี่ยงโดยมีโครงสร้างองค์กร กระบวนการ และวัฒนธรรมองค์กร
- เป็นกลไกส่วนหนึ่งของการขับเคลื่อนไปสู่การกำกับดูแลกิจการที่ดี ซึ่งต้องสอดคล้องกับแผนการดำเนินงานต่าง ๆ ขององค์กร เพื่อบรรลุวัตถุประสงค์และการเติบโตอย่างยั่งยืนขององค์กร

ประเภทของความเสี่ยง

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานที่นำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก ส่งผลกระทบต่อการบรรลุวิสัยทัศน์ พันธกิจ หรือสถานะขององค์กร ทำให้องค์กร สูญเสียโอกาสทางธุรกิจ, เสียเปรียบเชิงการแข่งขัน, หรือ ไม่บรรลุเป้าหมายระยะยาว

- ตัวอย่าง กระทรวงท่องเที่ยวฯ มุ่งส่งเสริม "ท่องเที่ยวเชิงสุขภาพ" หลังโควิด ผลักดันนโยบาย “Thailand Wellness Hub” เพื่อดึงดูดนักท่องเที่ยวเชิงสุขภาพ
- ความเสี่ยงเชิงกลยุทธ์ คือ ขาดบุคลากรทางการแพทย์และบริการสุขภาพที่ได้มาตรฐานสากล คู่แข่งในภูมิภาค (มาเลเซีย–สิงคโปร์) มีชื่อเสียงและระบบการแพทย์ดีกว่า
- ผลกระทบ: แผนไม่สามารถสร้างรายได้ตามเป้าหมาย และงบประมาณส่งเสริมถูกใช้ไปโดยไม่เกิดผลลัพธ์เชิงเศรษฐกิจจริง
- แนวทางจัดการ วิเคราะห์แนวโน้มภายนอก (PESTEL) ประเมินจุดแข็ง–จุดอ่อนขององค์กร (SWOT) และจัดระบบติดตาม (KPI เพื่อปรับกลยุทธ์ได้ทันท่วงที

ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)

ความเสี่ยงที่เกิดจากการกำหนดการดำเนินการในการปฏิบัติงานของบุคลากร ซึ่งส่งผลต่อการปฏิบัติงานต่าง ๆ ขององค์กรทำให้ไม่บรรลุวัตถุประสงค์และเป้าหมายที่กำหนด เกิดความล่าช้า สูญเสีย หรือหยุดชะงัก

- ตัวอย่าง สำนักทะเบียนอำเภอ ระบบบัตรประชาชนล่ม เซิร์ฟเวอร์หลักในศูนย์ข้อมูลเสียหายจากไฟฟ้าขัดข้อง และไม่มีระบบสำรองอัตโนมัติ
- ลักษณะความเสี่ยง ระบบเทคโนโลยีสารสนเทศขัดข้อง (IT System Failure)
- ผลกระทบ : ประชาชนไม่สามารถทำบัตรประชาชนใหม่ได้หลายชั่วโมง ประชาชนร้องเรียนเรื่องความล่าช้า
- แนวทางจัดการ จัดทำระบบสำรองข้อมูล กำหนดคู่มือปฏิบัติกรณีระบบล่ม ฝึกอบรมเจ้าหน้าที่ให้มีทักษะรับมือเหตุขัดข้องทางเทคนิค

ประเภทของความเสี่ยง

ความเสี่ยงด้านนโยบาย / กฎหมาย/ระเบียบ/ข้อบังคับ (Policy & Compliance Risk)

ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามนโยบาย กฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องได้ หรือ นโยบาย กฎหมาย ระเบียบ ข้อบังคับที่มีอยู่ไม่เหมาะสมเป็นอุปสรรคต่อการปฏิบัติงาน อาจส่งผลให้เกิดโทษทางกฎหมาย ความเสียหายทางชื่อเสียง หรือการสูญเสียสิทธิประโยชน์ขององค์กร

- ตัวอย่าง หน่วยงานภาครัฐจัดซื้อจัดจ้างไม่เป็นไปตามระเบียบพัสดุ / ระเบียบราชการ
- สาเหตุจากเจ้าหน้าที่ขาดความเข้าใจในระเบียบพัสดุ พ.ศ. 2560 หรือมีการเร่งรัดจัดซื้อโดยไม่มีการประกาศราคากลาง
- ผลกระทบ ถูกสำนักงานการตรวจเงินแผ่นดิน (สตง.) ตรวจสอบ โครงการถูกระงับหรือยกเลิก ผู้บริหารถูกลงโทษทางวินัยหรือทางอาญา
- แนวทางจัดการ จัดอบรมเจ้าหน้าที่เรื่องกฎหมายจัดซื้อจัดจ้าง ตั้งคณะกรรมการตรวจสอบภายใน ใช้ระบบ e-GP เพื่อเพิ่มความโปร่งใส

ความเสี่ยงด้านการเงิน (Financial Risk)

ความเสี่ยงที่เกิดจากการที่การเบิกจ่ายงบประมาณไม่เป็นไปตามแผน งบประมาณถูกตัด งบประมาณที่ได้รับไม่สอดคล้องกับสถานการณ์ของภารกิจที่เปลี่ยนแปลงไปทำให้การจัดสรรไม่พอเพียง

- ตัวอย่าง โครงการลงทุนโครงสร้างพื้นฐานของรัฐ เช่น รถไฟความเร็วสูง มีความเสี่ยงจากการกู้เงินและภาระหนี้สาธารณะ
- สาเหตุจากการคาดการณ์รายได้จากการใช้บริการสูงเกินจริง ทำให้การชำระคืนเงินกู้ใช้เวลานาน
- ผลกระทบ ภาระหนี้ของภาครัฐเพิ่มขึ้น ต้องใช้งบประมาณแผ่นดินชำระหนี้แทนรายได้จากโครงการ เสี่ยงต่อการถูกวิพากษ์วิจารณ์ทางการเมือง
- แนวทางจัดการ จัดทำการวิเคราะห์ความคุ้มค่าทางเศรษฐกิจ ใช้รูปแบบการร่วมทุน PPP (Public-Private Partnership)จัดระบบติดตามผลตอบแทนการลงทุนอย่างต่อเนื่อง

ประเภทของความเสี่ยง

ความเสี่ยงด้านสุขภาพ (Healthy Risk)

ความเสี่ยงหรือความเสียหายที่ส่งผลต่อชีวิตและความปลอดภัยของบุคลากร กำลังพล รวมถึงบุคคลภายนอก ที่เกิดจากปัจจัยทางกายภาพ เคมี ชีวภาพ หรือพฤติกรรมการทำงาน ที่ส่งผลกระทบต่อสุขภาพร่างกาย และจิตใจของบุคลากรในองค์กร ทำให้คนทำงานไม่ปลอดภัย ไม่สุขภาพดี และไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

- ตัวอย่าง เจ้าหน้าที่ภาคสนามของกรมป่าไม้ทำงานในพื้นที่เสี่ยง เสี่ยงต่อสุขภาพจากสภาพแวดล้อมและสัตว์มีพิษ
- สาเหตุจากปฏิบัติงานในป่าลึก ขาดอุปกรณ์สื่อสารและปฐมพยาบาล
- ผลกระทบ อุบัติเหตุ / การเจ็บป่วยเฉียบพลัน / ขวัญกำลังใจลดลง / อัตราการลาออกเพิ่มขึ้น
- แนวทางจัดการ จัดสวัสดิการตรวจสุขภาพก่อน-หลังปฏิบัติงาน มีระบบรายงานอุบัติเหตุและช่วยเหลือฉุกเฉิน ฝึกอบรมการปฐมพยาบาลขั้นพื้นฐาน

ความเสี่ยงด้านสิ่งแวดล้อม (Environment Risk)

การดำเนินงานขององค์กรที่มีผลทำให้เกิดผลกระทบหรือเกิดการเปลี่ยนแปลงต่อสภาพแวดล้อมทั้งภายในและภายนอกองค์กร อาจกระทบต่อ ทรัพยากรธรรมชาติ ชุมชน สุขภาพของประชาชน หรือความยั่งยืนขององค์กร

- ตัวอย่าง โรงไฟฟ้าชีวมวลของรัฐถูกร้องเรียนเรื่องมลพิษ ความเสี่ยงจากมลพิษทางอากาศ
- สาเหตุ จากการปล่อยควันเกินค่ามาตรฐาน / ไม่มีระบบกรองฝุ่น PM2.5
- ผลกระทบ ถูกชุมชนรอบข้างคัดค้านและร้องเรียน สูญเสียความน่าเชื่อถือของหน่วยงาน ต้องหยุดดำเนินการและปรับปรุงระบบกรองอากาศ
- แนวทางจัดการ ติดตั้งระบบ “Real-Time Air Quality Monitoring” ประชาสัมพันธ์ข้อมูลคุณภาพอากาศแบบโปร่งใส ทำรายงานผลกระทบสิ่งแวดล้อม (EIA) และเผยแพร่ต่อสาธารณะ

ประเภทของความเสี่ยง

ความเสี่ยงด้านชุมชน (Community Risk)

ความเสี่ยงหรือความเสียหายอันเนื่องมาจากการดำเนินงานขององค์กรที่ทำให้เกิดผลกระทบต่อชุมชนโดยรอบทั้งทางตรงและอ้อม ทั้งในด้านเศรษฐกิจ สังคม วัฒนธรรม และสิ่งแวดล้อม ซึ่งอาจทำให้เกิดความขัดแย้ง สูญเสียความเชื่อมั่น หรือกระทบต่อความต่อเนื่องของโครงการ

- ตัวอย่าง โครงการก่อสร้างเขื่อนของกรมชลประทานถูกชุมชนคัดค้าน เป็นความขัดแย้งระหว่างรัฐกับชุมชน (Conflict Risk)
- สาเหตุจากชุมชนไม่ได้รับฟังข้อมูลล่วงหน้า กังวลว่าจะสูญเสียที่ดินทำกินและผลกระทบสิ่งแวดล้อม
- ผลกระทบ โครงการต้องหยุดชั่วคราว หน่วยงานรัฐเสียภาพลักษณ์และความน่าเชื่อถือ ต้องใช้งบประมาณเพิ่มเติมเพื่อฟื้นฟูความสัมพันธ์
- แนวทางจัดการ จัดเวทีรับฟังความคิดเห็น (Public Hearing) อย่างโปร่งใส ทำรายงานผลกระทบสิ่งแวดล้อมและชุมชน (EIA/EHIA) ตั้งคณะกรรมการร่วมรัฐ–ชุมชนเพื่อติดตามโครงการ

ความเสี่ยงด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk)

ความเสี่ยงหรือความเสียหายที่ส่งผลต่อชื่อเสียงไม่ว่าจะเป็นผลจากการดำเนินงานทั้งทางตรงและทางอ้อม ส่งผลต่อภาพพจน์และความน่าเชื่อถือขององค์กร ซึ่งอาจเกิดจากเหตุการณ์จริง ความเข้าใจผิด หรือข่าวสารที่ถูกบิดเบือน

- ตัวอย่าง ธนาคารพาณิชย์ถูกโจมตีข้อมูลลูกค้ารั่วไหล
- สาเหตุจากระบบฐานข้อมูลถูกแฮก / พนักงานขาดความเข้าใจด้าน Data Privacy
- ผลกระทบ ลูกค้าสูญเสียความเชื่อมั่นในความปลอดภัยของข้อมูล ถูกสื่อวิจารณ์
- แนวทางจัดการ ตั้งทีมเฉพาะกิจ “Cyber Incident Response” แถลงชี้แจงอย่างโปร่งใส / แจ้งลูกค้าทันที / ชดเชยค่าเสียหาย ลงทุนเพิ่มเติมในระบบ Cybersecurity & Data Protection

กระบวนการจัดการความเสี่ยง

1 การระบุความเสี่ยง (Identification)

ขั้นตอนการวิเคราะห์และระบุความเสี่ยงเป็นขั้นตอนที่สำคัญมาก เป็นการทำความเข้าใจกับสาเหตุของการเกิดความเสี่ยง ระบุถึงเหตุการณ์หรือกิจกรรมของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาดความเสียหายและการไม่บรรลุวัตถุประสงค์ที่กำหนด

ขั้นตอนหลักของการระบุความเสี่ยง

- **1. กำหนดวัตถุประสงค์ขององค์กร** : เช่น “ลดระยะเวลาบริการประชาชนลง 30% ภายในปีงบประมาณ”
- **2. วิเคราะห์บริบท (Context Analysis)** : พิจารณาสภาพแวดล้อมทั้งภายใน–ภายนอกที่อาจส่งผลต่อความเสี่ยง เช่น โครงสร้างองค์กร บุคลากร กฎหมาย นโยบาย เทคโนโลยี
- **3. ระบุเหตุการณ์ความเสี่ยง (Identify Risk Events)** : เช่น ระบบล่ม, บุคลากรขาดทักษะ, งบประมาณไม่พอ
- **4. ระบุสาเหตุของความเสี่ยง (Causes)** : เช่น ขาดการวางแผน / การอบรม / การควบคุมภายในไม่เพียงพอ
- **5. ระบุผลกระทบของความเสี่ยง (Consequences)** : เช่น งานล่าช้า, ประชาชนไม่พอใจ, เสียชื่อเสียง
- **6. บันทึกในทะเบียนความเสี่ยง (Risk Register)** : จัดทำเอกสารรวบรวมความเสี่ยงทั้งหมดเพื่อใช้ประเมิน บันทึก “เหตุการณ์–สาเหตุ–ผลกระทบ–เจ้าของความเสี่ยง”

กระบวนการจัดการความเสี่ยง

2 ประเมินและวิเคราะห์ความเสี่ยง (Assessment & Analysis)

เป็นการประเมินเพื่อวัดความเป็นไปได้ของโอกาสเกิด (Likelihood Score) และผลกระทบ/ความรุนแรง (Impact Score) ของปัจจัยเสี่ยงทั้ง 8 ด้าน โดยนำความเสี่ยงที่ระบุไว้แล้วทั้งหมดมาพิจารณาเพื่อจัดลำดับความเสี่ยงและการประเมินความเสี่ยงมักจะทำ 2 มิติ คือ

- โอกาส/ความถี่ที่จะเกิด (Probability) หมายถึงความน่าจะเป็นที่จะเกิดเหตุการณ์ที่นำมาพิจารณาเกิดขึ้นมากน้อยเพียงใด
- ระดับผลกระทบ/ความรุนแรง (Severity/Impact) หรือผลกระทบที่เกิดจากเหตุการณ์นั้นๆ หรือคาดคะเนว่าจะเกิดเหตุการณ์นั้นๆ และเมื่อเกิดขึ้นแล้วจะเกิดความรุนแรงหรือผลกระทบกับสิ่งต่าง ๆ และความเสียหายที่เกิดขึ้นในด้านต่างๆ อย่างไรบ้าง

กระบวนการจัดการความเสี่ยง

2 ประเมินและวิเคราะห์ความเสี่ยง (Assessment & Analysis)

ขั้นตอนการประเมินและวิเคราะห์ความเสี่ยง

- **1. ระบุความเสี่ยงที่ต้องประเมิน** : ใช้ข้อมูลจากขั้นตอน “Risk Identification” เช่น ความเสี่ยงระบบล่ม, บุคลากรลาออกสูง, งบประมาณล่าช้า
- **2. วิเคราะห์สาเหตุและปัจจัยเสี่ยง (Risk Cause Analysis)** : เช่น ขาดการสำรองข้อมูล, ระบบล้าสมัย, การฝึกอบรมไม่เพียงพอ
- **3. ประเมินโอกาสเกิด (Likelihood)** : ประมาณความถี่หรือความน่าจะเป็นที่เหตุการณ์จะเกิด เช่น 1 = แทบไม่เกิดเลย, 5 = เกิดบ่อยทุกปี
- **4. ประเมินผลกระทบ (Impact / Consequence)** : ประเมินความรุนแรงหากเกิดเหตุการณ์ขึ้นจริง เช่น 1 = กระทบเล็กน้อย, 5 = กระทบต่อองค์กรทั้งระบบ
- **5. คำนวณระดับความเสี่ยง (Risk Level)** : คำนวณจากสูตร: Risk Level = Likelihood × Impact เช่น 3 (โอกาส) × 4 (ผลกระทบ) = 12 = ระดับ “สูง”
- **6. จัดลำดับความเสี่ยง (Risk Ranking)** : เรียงลำดับความเสี่ยงจากสูงสุดไปต่ำสุด เพื่อวางแผนควบคุมหรือลดผลกระทบก่อน
- **7. สรุปในตารางประเมินความเสี่ยง (Risk Matrix)** : แสดงภาพรวมระดับความเสี่ยงในองค์กร ใช้เป็นแผนภาพ Heat Map แดง–เหลือง–เขียว

🔴 **สูงมาก – ต้องจัดการทันที**
🔶 **สูง – ต้องควบคุมและติดตามใกล้ชิด**
🟡 **ปานกลาง – ต้องวางแผนลดความเสี่ยง**
🟢 **ต่ำ – เฝ้าระวัง**

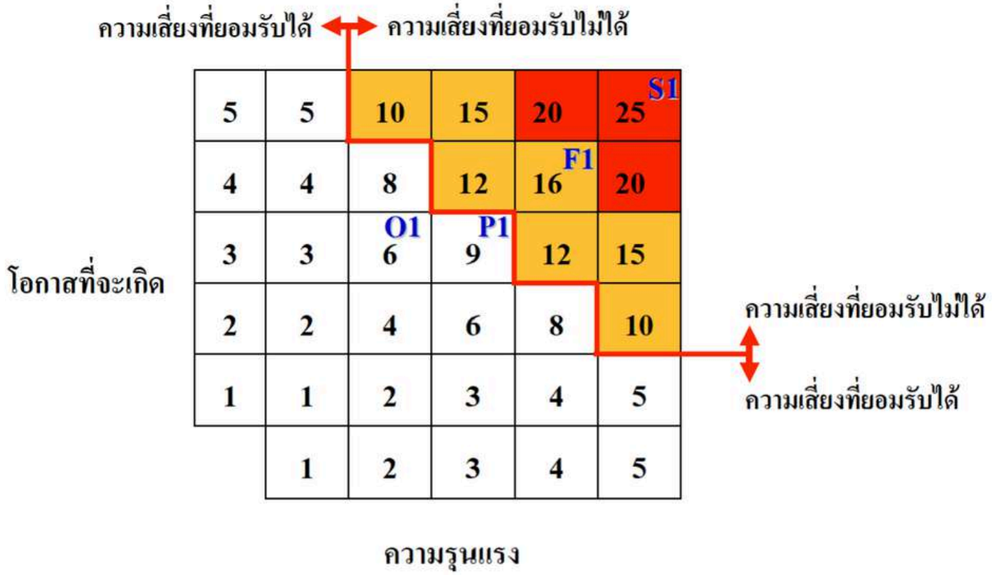
ตัวอย่าง การประเมินและวิเคราะห์ความเสี่ยงของกรมทางหลวง

ความเสี่ยง	โอกาสเกิด (L)	ผลกระทบ (I)	ระดับความเสี่ยง (L×I)	การจัดการ
โครงการก่อสร้างล่าช้า	4	5	20 🔴	ติดตามแผนทุกเดือน / ตรวจสอบผู้รับเหมา
งบประมาณเบิกจ่ายล่าช้า	3	4	12 🔶	วางระบบเบิกออนไลน์ / อบรมเจ้าหน้าที่
อุบัติเหตุในพื้นที่ก่อสร้าง	2	5	10 🟡	ตรวจสอบความปลอดภัย / จัดอุปกรณ์ป้องกัน
ขาดบุคลากรช่างผู้เชี่ยวชาญ	3	3	9 🟡	พัฒนาศักยภาพ / จ้างที่ปรึกษาภายนอก

กระบวนการจัดการความเสี่ยง

พิจารณาและจัดลำดับความเสี่ยง

หลังจากประเมินความเป็นไปได้ของโอกาสที่เกิด (Likelihood Score) และผลกระทบ/ความรุนแรง (Impact Score) ของปัจจัยเสี่ยงต่าง ๆ โดยนำความเสี่ยงที่ระบุไว้แล้วทั้งหมดมาพิจารณาความเสี่ยง ดังนี้



	3	ระดับความเสี่ยงสูงมาก มีค่าระหว่าง 20 -25	ความเสี่ยงยอมรับไม่ได้
	2	ระดับความเสี่ยงสูง มีค่าระหว่าง 10 - 19	ความเสี่ยงสูง
	1	ระดับต่ำหรือปานกลาง มีค่าระหว่าง 1 - 9	ความเสี่ยงที่ยอมรับได้

ตัวอย่างภาพ Heat Map (แผนภาพระดับความเสี่ยง)

	ผลกระทบสูง (5)	4	3	2	1 (ต่ำ)
5 (เกิดบ่อย)	สูงมาก	สูง	ปานกลาง	ต่ำ	ต่ำมาก
4	สูง	ปานกลาง	ต่ำ	ต่ำ	ต่ำมาก
3	ปานกลาง	ต่ำ	ต่ำ	ต่ำมาก	ต่ำมาก
2	ต่ำ	ต่ำ	ต่ำมาก	ต่ำมาก	ต่ำมาก
1 (แทบไม่เกิด)	ต่ำมาก	ต่ำมาก	ต่ำมาก	ต่ำมาก	ต่ำมาก

- พื้นที่สีแดง : ความเสี่ยงสูงมาก ต้องบริหารเร่งด่วน
- พื้นที่สีเหลือง : ความเสี่ยงปานกลาง ต้องติดตามและควบคุม
- พื้นที่สีเขียว : ความเสี่ยงต่ำ ยอมรับได้

กระบวนการจัดการความเสี่ยง

3

กิจกรรมควบคุมความเสี่ยง (Mitigation)

กิจกรรมควบคุมความเสี่ยง เป็นกระบวนการปฏิบัติงานที่ทุกคนทุกระดับในองค์กรร่วมกันกำหนดขึ้น เพื่อสร้างความมั่นใจในการดำเนินการอย่างสมเหตุสมผล ในการบรรลุวัตถุประสงค์ขององค์กรหรือหน่วยงาน ซึ่งกิจกรรมควบคุมความเสี่ยงมีการประเมิน ดังนี้

- การดำเนินการควบคุมเพื่อป้องกัน เป็นการกำหนดกิจกรรมที่นำมาใช้ในควบคุมความเสี่ยง
- การควบคุมที่มีอยู่แล้ว เป็นกิจกรรมที่จะนำมาใช้ในควบคุมความเสี่ยง ที่มีอยู่และยังไม่มีหรือมีแต่ยังไม่สมบูรณ์
- โดยใช้เครื่องหมาย / หมายถึง มีอยู่แล้ว X หมายถึงไม่มี และ O หมายถึง มีแต่ไม่สมบูรณ์
- แสดงผลของการควบคุมที่มีอยู่แล้ว ที่ทำกิจกรรมในการควบคุมความเสี่ยง

รูปแบบของการประเมินกิจกรรมควบคุมความเสี่ยง

เมื่อองค์กรได้ระบุและประเมินความเสี่ยงแล้ว ขั้นต่อมาคือการตรวจสอบว่า “มีการควบคุมอยู่แล้วหรือไม่” และ “มีประสิทธิภาพเพียงใด” โดยสามารถใช้การประเมินดังนี้

สัญลักษณ์	ความหมาย	การตีความ
/	มีการควบคุมอยู่แล้ว	มีระบบ มาตรการ หรือกิจกรรมที่ชัดเจนและดำเนินการอย่างต่อเนื่อง
O	มีการควบคุมแต่ยังไม่สมบูรณ์	มีกิจกรรมบางส่วน แต่ยังขาดการดำเนินการครบวงจรหรือประสิทธิภาพไม่เพียงพอ
X	ยังไม่มีการควบคุม	ยังไม่มีมาตรการใด ๆ ควบคุมความเสี่ยง ต้องจัดทำกิจกรรมใหม่

วัตถุประสงค์ของกิจกรรมควบคุมความเสี่ยง

- เพื่อสร้างความมั่นใจว่ากระบวนการทำงานดำเนินไปตามแผนที่กำหนด
- เพื่อป้องกันหรือลดโอกาสการเกิดเหตุการณ์ที่ไม่คาดคิด
- เพื่อให้มั่นใจว่าผลการดำเนินงานเป็นไปตามวัตถุประสงค์เชิงกลยุทธ์ขององค์กร
- เพื่อให้หน่วยงานสามารถตรวจสอบ ติดตาม และปรับปรุงระบบควบคุมได้อย่างต่อเนื่อง

ขั้นตอนการประเมินกิจกรรมควบคุมความเสี่ยง

1. ตรวจสอบกิจกรรมควบคุมที่มีอยู่

- สำรวจว่าหน่วยงานได้ดำเนินการใดแล้วบ้างในการป้องกันความเสี่ยง

2. ประเมินความเพียงพอและประสิทธิผล

- สำรวจว่าพิจารณาว่ากิจกรรมดังกล่าวเพียงพอในการลดโอกาสหรือผลกระทบของความเสี่ยงหรือไม่หน่วยงานได้ดำเนินการใดแล้วบ้างในการป้องกันความเสี่ยง

3. ใช้สัญลักษณ์ / O X แสดงสถานะ

- เพื่อแสดงให้เห็นภาพรวมของระดับความพร้อมในการควบคุม

4. สรุปผลเพื่อวางแผนปรับปรุง

- หากพบว่ากิจกรรมควบคุมไม่สมบูรณ์หรือไม่มี ต้องจัดทำแผนปรับปรุงเพิ่มเติม

ตัวอย่าง ตารางกิจกรรมควบคุมความเสี่ยงของหน่วยงานภาครัฐ

ความเสี่ยง	กิจกรรมควบคุมความเสี่ยง	มีอยู่แล้ว (/)	ไม่มี (X)	มีแต่ไม่สมบูรณ์ (O)	หมายเหตุ
ระบบบริการประชาชนล่ม	จัดตั้งระบบสำรองข้อมูล (Backup Server)	/			มีการสำรองทุก 3 เดือน
ข้อมูลประชาชนรั่วไหล	กำหนดสิทธิ์การเข้าถึงข้อมูลเฉพาะระดับ			O	ยังไม่มีระบบบันทึก Log การเข้าใช้งาน
การเบิกจ่ายงบประมาณล่าช้า	พัฒนาโปรแกรมติดตามสถานะเบิกจ่าย	X			อยู่ระหว่างพัฒนาโดยสำนักงบประมาณ
บุคลากรขาดทักษะดิจิทัล	จัดอบรมหลักสูตร Digital Literacy	/			อบรมปีละ 2 ครั้ง
เอกสารราชการสูญหาย	ใช้ระบบ e-Document แทนกระดาษ			O	ยังไม่ครอบคลุมทุกหน่วยย่อย

การแสดงผลของการควบคุมที่มีอยู่แล้ว (EXISTING CONTROL EFFECTIVENESS)

เพื่อให้เห็นระดับความพร้อมขององค์กรในภาพรวม อาจจัดทำในรูปแบบ “กราฟเรดาร์ (RADAR CHART)” หรือ “ตารางคะแนนภาพรวม” โดยคิดคะแนน เช่น

/ = 2 คะแนน
O = 1 คะแนน
X = 0 คะแนน

ตัวอย่างผลรวม

หมวดความเสี่ยง	คะแนนเฉลี่ย	ระดับความพร้อม	แนวทางพัฒนา
การดำเนินงาน (Operational Risk)	1.8	สูง	รักษามาตรการที่ดี
การเงิน (Financial Risk)	1.0	ปานกลาง	ปรับปรุงระบบควบคุมงบประมาณ
เทคโนโลยีสารสนเทศ (IT Risk)	0.7	ต่ำ	จัดทำระบบควบคุมใหม่ / สำรองข้อมูล
บุคลากร (HR Risk)	1.5	สูง	เพิ่มการพัฒนา Soft Skills
ชื่อเสียงองค์กร (Reputation Risk)	0.9	ต่ำ	สร้างแผน Crisis Communication

กระบวนการจัดการความเสี่ยง

4

การตรวจสอบ (Monitoring)

- การรวบรวมข้อมูลเกี่ยวกับการป้องกันภัยคุกคามและการตอบสนองต่อเหตุการณ์เพื่อประเมินว่ากลยุทธ์การจัดการความเสี่ยงขององค์กรว่ามีประสิทธิภาพเพียงใด นอกจากนี้ยังรวมถึงการวิจัยแนวโน้มความเสี่ยงที่เกิดขึ้นใหม่เพื่อพิจารณาว่ากรอบการจัดการความเสี่ยงขององค์กรว่าจำเป็นต้องปรับปรุงหรือไม่ หรือจะต้องปรับปรุงในอนาคต
- สรุปผลกิจกรรมที่ใช้ในการจัดการความเสี่ยง ประกอบด้วย ความเสี่ยงที่เกิดขึ้น การควบคุม ระดับความเสี่ยง การจัดการความเสี่ยง กิจกรรมที่ควบคุม ระยะเวลาการดำเนินงาน เพื่อให้แต่ละหน่วยงานดำเนินการจัดการความเสี่ยงตามกิจกรรมและระยะเวลาที่กำหนดไว้

กระบวนการจัดการความเสี่ยง

5

การประสานงาน (Cooperation)

การสร้างความสัมพันธ์ระหว่างความเสี่ยงและกลยุทธ์การบรรเทาความเสี่ยงในพื้นที่ต่าง ๆ ของการดำเนินงานขององค์กร เพื่อสร้างระบบตอบสนองต่อภัยคุกคามที่มีการรวมศูนย์และประสานงานมากขึ้น

6

การรายงาน (Reporting)

การบันทึกและตรวจสอบข้อมูลที่เกี่ยวข้องกับความพยายามในการจัดการความเสี่ยงขององค์กร เพื่อประเมินประสิทธิภาพ และติดตามผลเพื่อให้เกิดความมั่นใจว่าความเสี่ยงได้มีการควบคุมและจัดการอย่างมีประสิทธิผล โดยพิจารณาจากผลลัพธ์ของการทำกิจกรรม ระยะเวลาการดำเนินงาน ความคืบหน้า ปัญหาและอุปสรรค มีการตรวจสอบเพื่อแนะนำให้ปรับปรุงข้อบกพร่องให้เหมาะสมกับเวลา และมีการรายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงขององค์กร

กลยุทธ์ที่ใช้ในการบริหารความเสี่ยง

การนำกระบวนการบริหารความเสี่ยงมาใช้ในองค์กรจะมีการดำเนินการให้บรรลุเป้าหมายที่วางไว้ เนื่องจากการบริหารความเสี่ยงเป็นการทำนายอนาคตอย่างมีเหตุผล มีหลักการและหาทางลดหรือป้องกันความเสียหายในการทำงานแต่ละขั้นตอนไว้ล่วงหน้า ดังนั้นจึงควรเลือกใช้กลยุทธ์บริหารความเสี่ยงที่เหมาะสม

การยอมรับความเสี่ยง (Take)

ความเสี่ยงที่เหลืออยู่ในปัจจุบันอยู่ภายในระดับที่ต้องการและยอมรับได้แล้ว โดยไม่ต้องมีการดำเนินการเพิ่มเติมเพื่อลดโอกาสหรือความรุนแรงที่อาจเกิดขึ้นได้อีก

การลดหรือควบคุม (Treat)

การดำเนินการเพิ่มเติมเพื่อลดโอกาสที่อาจเกิดขึ้นหรือความรุนแรงของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เป็นการออกแบบระบบควบคุม การแก้ไขปรับปรุงการทำงานเพื่อป้องกันหรือ จำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

การถ่ายโอนหรือกระจาย (Transfer)

การโอนหรือการกระจายความรับผิดชอบกับผู้อื่นในการจัดการความเสี่ยง เช่นการประกันทรัพย์สินเพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

การหยุดหรือการหลีกเลี่ยง (Terminate)

การหยุดหรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบ การทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

กลยุทธ์การยอมรับความเสี่ยง

(Take / Accept Strategy)

- การที่องค์กรตัดสินใจ “ยอมรับ” ความเสี่ยงที่เหลืออยู่ โดยไม่ดำเนินมาตรการใดเพิ่มเติม เพื่อควบคุมหรือถ่ายโอน เนื่องจากเห็นว่าความเสี่ยงนั้นมีโอกาสเกิดต่ำ ผลกระทบไม่รุนแรง หรือการลงทุนในการลดความเสี่ยง “ไม่คุ้มค่า” กับผลลัพธ์ที่จะได้
- องค์กรเลือกจะอยู่กับความเสี่ยงนั้น โดยเตรียมแผนสำรอง (Contingency Plan) เพื่อรองรับผลกระทบ หากเหตุเกิดขึ้นจริง

หลักการของการยอมรับความเสี่ยง

- ต้องเป็นความเสี่ยงที่อยู่ในระดับ Low หรือ Acceptable Level
- ต้องมี เหตุผลรองรับทางเศรษฐกิจหรือเชิงนโยบาย
- ต้องมี แผนเผชิญเหตุ (Contingency Plan) หรือ งบสำรองฉุกเฉิน (Reserve Fund) เพื่อรองรับผลกระทบ
- ต้องได้รับการอนุมัติจาก ผู้บริหารระดับสูง / คณะกรรมการบริหารความเสี่ยง

ตัวอย่าง กรมอุตุนิยมวิทยา

- ความเสี่ยง: ระบบเซิร์ฟเวอร์สำรองสำหรับศูนย์ข้อมูลภูมิภาคยังไม่เชื่อมโยง 100%
- การประเมิน: โอกาสเกิดต่ำ / ผลกระทบจำกัดในระดับภูมิภาค
- กลยุทธ์: ยอมรับความเสี่ยง (Take) โดย
  - ยังไม่ลงทุนระบบสำรองใหม่ทันที เนื่องจากงบประมาณสูง
  - ใช้มาตรการชั่วคราว เช่น การสื่อสารผ่านเครือข่ายกลาง
  - จัดทำแผนฉุกเฉิน หากระบบล่ม
- ผลลัพธ์ ประหยัดงบประมาณ และสามารถควบคุมผลกระทบได้ด้วยมาตรการสำรอง

กลยุทธ์การถ่ายโอนหรือกระจายความเสี่ยง

(Transfer / Sharing Strategy)

- กลยุทธ์ที่องค์กร “โอนความเสี่ยง” ทั้งหมดหรือบางส่วน ไปยังบุคคลหรือองค์กรอื่นที่มีความสามารถในการจัดการความเสี่ยงนั้นได้ดีกว่า เพื่อลดภาระหรือผลกระทบที่อาจเกิดขึ้นกับองค์กร
- องค์กรไม่ได้ “หลีกเลี่ยง” ความเสี่ยง แต่ “แบ่งปัน” ภาระหรือ “ส่งต่อ” ความรับผิดชอบบางส่วน ให้กับหน่วยงานภายนอก เช่น บริษัทประกันภัย ผู้รับจ้าง หรือพันธมิตรทางธุรกิจ

หลักการของการถ่ายโอนความเสี่ยง

- ต้องเป็นความเสี่ยงที่สามารถระบุและประเมินค่าได้ เป็นตัวเงิน หรือประเมินโอกาสเกิดได้อย่างชัดเจน เช่น ความเสียหายต่อทรัพย์สิน หรือความล่าช้าในโครงการ
- ต้องถ่ายโอนให้กับบุคคลหรือองค์กรที่มีศักยภาพ คู่สัญญาหรือหน่วยงานที่รับโอนต้องมีขีดความสามารถทางการเงิน กฎหมาย หรือเทคนิคเพียงพอ เช่น บริษัทประกันภัย บริษัทคู่สัญญา หรือพันธมิตรทางธุรกิจ
- ต้องมีข้อตกลงหรือสัญญาเป็นลายลักษณ์อักษร เช่น สัญญา Outsource, สัญญา Joint Venture, หรือกรมธรรม์ประกันภัย
- ต้องคุ้มค่าทางเศรษฐกิจ ต้นทุนของการโอนความเสี่ยง (เช่น ค่าประกันภัย หรือค่าจ้าง) ต้องไม่สูงเกินกว่าผลประโยชน์ที่ได้รับจากการลดผลกระทบ
- ต้องมีการติดตามและประเมินผลภายหลังการถ่ายโอน ต้องมีการติดตามและประเมินผลภายหลังการถ่ายโอน
- ต้องสอดคล้องกับกฎหมายและนโยบายขององค์กร ไม่ขัดต่อระเบียบราชการ มติคณะรัฐมนตรี หรือแนวนโยบายขององค์กร โดยเฉพาะในภาครัฐ

ตัวอย่างในภาครัฐ

- โครงการก่อสร้างอาคารราชการ : จ้างผู้รับเหมาภายนอกและกำหนด “สัญญาความรับผิด” หากส่งงานล่าช้า
- การจัดนิทรรศการระดับชาติ : ทำประกันภัยความเสียหายของทรัพย์สินหรืออุบัติเหตุภายในงาน
- การจัดการขยะในเขตเทศบาล : จ้างเอกชนบริหารจัดการ (Outsource) ภายใต้สัญญารับผิดชอบผลกระทบสิ่งแวดล้อม
- ระบบสารสนเทศของกรมราชการ : ทำสัญญา Cloud Service กับผู้ให้บริการภายนอก

กลยุทธ์การลดหรือควบคุมความเสี่ยง

(Treat / Reduce Strategy)

- การดำเนินการเพื่อ “ลดโอกาสเกิด” หรือ “ลดผลกระทบ” ของความเสี่ยง โดยการปรับปรุงกระบวนการ ระบบ บุคลากร หรือเทคโนโลยี เพื่อให้ความเสี่ยงนั้น อยู่ในระดับที่องค์กรยอมรับได้ (Acceptable Level)
- องค์กรยังยอมทำกิจกรรมนั้นอยู่ แต่จะบริหารจัดการให้เกิดความเสียหายน้อยที่สุด

หลักการของกลยุทธ์การลดหรือควบคุมความเสี่ยง

- ลดโอกาสการเกิดความเสี่ยง (Reduce Probability) ใช้มาตรการป้องกันล่วงหน้า เช่น การอบรม การใช้เทคโนโลยีควบคุม การเพิ่มระบบตรวจสอบ
- ลดผลกระทบเมื่อความเสี่ยงเกิดขึ้น (Reduce Impact) เตรียมแผนรองรับเหตุการณ์ เช่น ระบบสำรอง (Backup System) หรือทีมตอบสนองฉุกเฉิน
- มุ่งพัฒนาอย่างต่อเนื่อง (Continuous Improvement) ปรับปรุงกระบวนการให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น
- กำหนดเจ้าของความเสี่ยง (Risk Owner) ให้หน่วยงานหรือบุคคลรับผิดชอบโดยตรงในการควบคุมและติดตาม

ตัวอย่างในภาครัฐ

ความเสี่ยงจากระบบบริการประชาชนล่มในช่วงลงทะเบียนสิทธิ์รัฐ

- กลยุทธ์การลด / ควบคุม โดยจัดตั้งศูนย์ข้อมูลสำรอง และทดสอบระบบ ก่อนเปิดใช้งานจริง
- ช่วยลดโอกาสระบบล่ม เพิ่มความเชื่อมั่นของประชาชน

ความเสี่ยงจากภัยพิบัติในพื้นที่เทศบาล

- กลยุทธ์การลด / ควบคุม โดยจัดตั้งศูนย์ป้องกันและบรรเทาสาธารณภัยประจำเขต จัดอบรมเจ้าหน้าที่ด้านการอพยพและการกู้ภัย
- ช่วยลดผลกระทบต่อชีวิตและทรัพย์สินของประชาชน

ความเสี่ยงจากการทุจริตจัดซื้อจัดจ้าง

- กลยุทธ์การลด / ควบคุม โดยใช้ระบบ e-Bidding และ e-Procurement เพื่อความโปร่งใส ตรวจสอบโดยคณะกรรมการภายนอก
- ช่วยลดความเสี่ยงการทุจริต เพิ่มความโปร่งใส

กลยุทธ์การหยุดหรือหลีกเลี่ยงความเสี่ยง

(erminate / Avoid Strategy)

- การยุติ (Terminate) หรือ ไม่ดำเนินกิจกรรมใด ๆ ที่มีความเสี่ยงสูงเกินระดับที่องค์กรยอมรับได้ เพื่อป้องกันไม่ให้ความเสี่ยงนั้นเกิดขึ้นตั้งแต่ต้น
- เป็นการตัดไฟตั้งแต่ต้นลม ถ้ากิจกรรมหนึ่งเสี่ยงเกินไปและไม่คุ้มกับผลตอบแทน องค์กรจะ เลือกไม่ทำ หรือเปลี่ยนแนวทางดำเนินงานใหม่ แทน

หลักการของกลยุทธ์การหยุดหรือหลีกเลี่ยงความเสี่ยง

- ป้องกันเหตุไม่ให้เกิดตั้งแต่ต้นทาง หลีกเลี่ยงกิจกรรมที่มีความเสี่ยงสูง หรือยกเลิกโครงการที่อาจสร้างผลกระทบรุนแรง
- พิจารณาความคุ้มค่า (Cost–Benefit) หากต้นทุนการควบคุมหรือผลกระทบสูงเกินประโยชน์ที่ได้รับ ควรยุติการดำเนินการ
- เลือกทางเลือกใหม่ที่ปลอดภัยกว่า เปลี่ยนกระบวนการ วิธีการ หรือเครื่องมือ เพื่อให้เกิดความเสี่ยงต่ำลง
- ตัดสินใจเชิงนโยบายอย่างชัดเจน ต้องมีการอนุมัติจากผู้บริหารระดับสูง หรือคณะกรรมการความเสี่ยง
- สื่อสารและประเมินผลกระทบจากการยุติ แจ้งผู้มีส่วนได้ส่วนเสียและจัดทำรายงานผลกระทบจากการหยุดกิจกรรม

ตัวอย่างในภาครัฐ

โครงการก่อสร้างในพื้นที่ป่าสงวนแห่งชาติ

- กลยุทธ์การหยุด/หลีกเลี่ยง โดยยกเลิกโครงการ เนื่องจากเสี่ยงต่อการละเมิดกฎหมายสิ่งแวดล้อม
- เพื่อป้องกันความเสียหายทางกฎหมายและชื่อเสียงของรัฐ

โครงการจัดซื้ออุปกรณ์เทคโนโลยีจากต่างประเทศที่มีปัญหาด้านความมั่นคงข้อมูล

- กลยุทธ์การหยุด/หลีกเลี่ยง โดยเปลี่ยนไปใช้ผู้ผลิตในประเทศหรือประเทศพันธมิตรที่ได้รับการรับรอง
- เพื่อลดความเสี่ยงด้านความมั่นคงไซเบอร์

โครงการพัฒนาในพื้นที่เสี่ยงภัยพิบัติ (ดินถล่ม/น้ำท่วม)

- กลยุทธ์การหยุด/หลีกเลี่ยง ยกเลิกแผนก่อสร้างและปรับพื้นที่ให้เป็นเขตปลอดภัย
- เพื่อลดความเสียหายต่อชีวิตและทรัพย์สิน

ประโยชน์ที่ได้จากการบริหารความเสี่ยง

- ตระหนักถึงภัยคุกคามที่ยังมาไม่ถึง
- ปรับปรุงระบบงานและการวางแผน
- ลดการสูญเสียที่อาจเกิดขึ้นได้
- สร้างโอกาส
- สร้างคุณค่าให้การทำงาน
- สนับสนุนการตัดสินใจของผู้บริหาร
- สร้างภาพลักษณ์ที่ดีให้องค์กร
- ปกป้องการปฏิบัติงาน
- เป็นส่วนหนึ่งของการบริหารงาน
- มองเป้าหมายในภาพรวม

Thank You