

ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management)

ปัจจุบันองค์กรพึ่งพาระบบดิจิทัลและข้อมูลเป็นหลัก ความเสี่ยงด้านไซเบอร์จึงส่งผลกระทบโดยตรงต่อ เช่น ความต่อเนื่องของงาน (Operational Disruption) ความเสียหายทางการเงิน ความเชื่อมั่นของประชาชน หรือลูกค้า ความปลอดภัยของข้อมูลส่วนบุคคล

Cyber Security vs. Information Security เป็นพื้นฐานสำคัญที่สุด” ของการบริหารความเสี่ยงไซเบอร์

- Cyber Security (ความมั่นคงปลอดภัยไซเบอร์) คือ การปกป้อง “ระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบดิจิทัล” จากภัยคุกคามทางไซเบอร์

- Information Security (ความมั่นคงปลอดภัยสารสนเทศ) คือ การปกป้อง “ข้อมูล” ไม่ว่าจะอยู่ใน รูปแบบใดก็ตาม โดยมีเป้าหมายหลักให้ข้อมูลเป็นความลับ มีความถูกต้องและพร้อมใช้งาน

Cyber Security Risk Management คือ กระบวนการบริหารจัดการ “ความเสี่ยงจากภัยคุกคามทางไซเบอร์” อย่างเป็นระบบเพื่อป้องกัน ลดผลกระทบ และทำให้องค์กรดำเนินงานต่อได้ มีองค์ประกอบหลัก ดังนี้

1. Identifying Risk (การระบุความเสี่ยง) คือ การค้นหาและระบุ “อะไรคือสิ่งที่อาจก่อให้เกิดความเสียหายต่อองค์กร”

2. Assess Risk (การประเมินความเสี่ยง) คือ การวิเคราะห์ว่า โอกาสเกิด (Likelihood) ผลกระทบ (Impact) รุนแรงแค่ไหน

3. Control Risk (การควบคุม/ลดความเสี่ยง) คือ การกำหนดมาตรการควบคุม

4. Review Controls (การทบทวนและปรับปรุง)

Frameworks คือ โครงสร้างแนวทางที่ช่วยให้องค์กรทำงานอย่างเป็นระบบ มีมาตรฐาน และควบคุมความเสี่ยงได้ ซึ่งมีหลายวิธี เช่น

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) ใช้สำหรับ Enterprise Risk Management (ERM) เน้นบริหารความเสี่ยงระดับองค์กรทั้งหมด ไม่ใช่เฉพาะ IT

- ISO 27001 มาตรฐานสำหรับ Information Security Management System (ISMS)

- ISO 27032 ISO/IEC 27032 แนวทางด้าน Cybersecurity โดยเฉพาะเน้นการป้องกันภัยไซเบอร์ในโลกออนไลน์

- NIST (National Institute of Standards and Technology) หน่วยงานสหรัฐฯ ที่ออก Framework ด้าน Cybersecurity เป็น Framework ที่นิยมใช้มากที่สุด

- ISO 31000 มาตรฐานด้าน Risk Management ทั่วไปใช้ได้กับทุกอุตสาหกรรม
NIST Cybersecurity Framework (CSF) ประกอบด้วย

- Framework Core คือ “โครงสร้างหลักของกิจกรรมด้าน Cybersecurity” ประกอบด้วย Functions (5 ฟังก์ชันหลัก) คือ 1. Identify 2. Protect 3. Detect 4. Respond 5. Recover

Core บอกว่า “องค์กรควรทำอะไรบ้าง” ในภาพรวม

- Framework Implementation Tiers คือ “ระดับความพร้อม/ความเป็นผู้ใหญ่ (Maturity Level)” ขององค์กร Tier ไม่ได้บอกว่า “ดีหรือไม่ดี” แต่บอกว่าองค์กรอยู่ระดับไหน

- Framework Profiles คือ “การเลือกสิ่งที่เหมาะสมกับองค์กร” องค์กรจะกำหนด: Current Profile (ปัจจุบันทำอะไรอยู่) Target Profile (อยากไปถึงระดับไหน)

Business Continuity Planning (BCP) คือ การวางแผนล่วงหน้าเพื่อให้องค์กรสามารถดำเนินธุรกิจต่อไปได้ แม้เกิดเหตุการณ์ไม่คาดคิด เช่น น้ำท่วม ไฟไหม้ ไฟดับ

ISO 22301: Business Continuity Management คือ ระบบบริหารความต่อเนื่องทางธุรกิจ”

เป้าหมายคือ ทำให้องค์กรเตรียมพร้อม รับมือ และฟื้นตัวจากเหตุการณ์หยุดชะงักได้อย่างเป็นระบบ มีโครงสร้างหลัก ดังนี้

- Context of the Organization วิเคราะห์บริบทองค์กร ผู้มีส่วนได้เสีย และความเสี่ยง
- Leadership ผู้บริหารต้องสนับสนุนและกำหนดนโยบาย BC
- Planning ประเมินความเสี่ยง ทำ BIA (Business Impact Analysis) และกำหนด RTO / RPO
- Support ทรัพยากร บุคลากร การสื่อสาร เอกสาร
- Operation การจัดทำและนำ BCP ไปใช้จริง
- Performance Evaluation ทดสอบแผน ตรวจสอบ ประเมินผล
- Improvement ปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

Wrap Up คือ การสรุปปิดท้ายเนื้อหา การประชุม หรือการเรียน เพื่อทบทวนประเด็นสำคัญก่อนจบ คือ

- องค์กรต้องบริหารความเสี่ยง
- ต้องมี Framework เป็นแนวทาง
- ต้องมีแผน BCP เพื่อรับมือเหตุการณ์
- ต้องทดสอบและปรับปรุงอย่างต่อเนื่อง

Cybersecurity Risk Management เป็น “เครื่องมือเชิงกลยุทธ์” ที่ช่วยให้องค์กรป้องกัน ความเสียหาย รักษาความต่อเนื่องของงาน สร้างความเชื่อมั่น และพัฒนาองค์กรอย่างยั่งยืน

สรุปบทเรียนโดย : นายปิยะพงษ์ วงเวียน ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน

สถานีพัฒนาที่ดินสุรินทร์ สำนักงานพัฒนาที่ดินเขต 3



(นายปิยะพงษ์ วงเวียน)

เจ้าพนักงานการเกษตรปฏิบัติงาน

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ปิยะพงษ์ วงเวียน

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 15 มิถุนายน 2569

A. L.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



aa4c6396

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพว.)
Digital Government Development Agency (Public
Organization) (DGA)
Date: 2026-06-15T09:20:06.787+07:00