

ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์

ศูนย์ส่งเสริมและพัฒนาอุตสาหกรรมดิจิทัล กรุงเทพมหานคร

INFORMATION SECURITY (INFOSEC) VS. CYBERSECURITY



InfoSec

มุ่งเน้นการปกป้องข้อมูลในรูปแบบ (กระดาษ ดิจิทัล) ตามหลัก Traid



Cybersecurity

เน้นเฉพาะการปกป้องระบบเครือข่ายและข้อมูลดิจิทัลที่เชื่อมต่อกับระบบไซเบอร์

CYBERSECURITY RISK MANAGEMENT

กระบวนการเชิงระบบในการระบุภัยสินสารสนเทศ วิเคราะห์ภัยคุกคามและช่องโหว่ ประเมินโอกาสและผลกระทบ ตลอดจนกำหนดมาตรการรับมือที่เหมาะสม

ระบุทรัพย์สิน (Identify Assets)

วิเคราะห์ภัยคุกคาม (Analyze Threats)

ประเมินผลกระทบ (Assess Impact)

กำหนดมาตรการ (Determine Measures)



กรอบการทำงานมาตรฐาน (FRAMEWORKS)

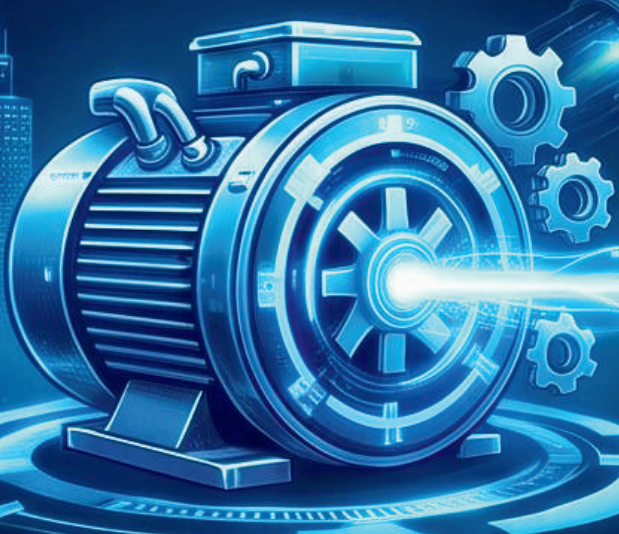
บรรทัดฐานเพื่อความปลอดภัยสากล

คือแนวทาง ที่ใช้เป็นบรรทัดฐานในการออกแบบ พัฒนาและประเมินระบบช่วยให้การตรวจสอบช่องโหว่ เป็นไปอย่างมีประสิทธิภาพ



NIST CSF: แนวทางการบริหารความเสี่ยงที่ครอบคลุม

ประกอบด้วย 5 ฟังก์ชันหลัก ได้แก่ การระบุตัวตน (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการกู้คืน (Recover)



BUSINESS CONTINUITY PLAN (BCP)

แนวทางปฏิบัติที่องค์กรจัดทำขึ้นเพื่อเตรียมความพร้อมรับมือกับเหตุการณ์ฉุกเฉินหรือภัยพิบัติ



ISO 22301: มาตรฐานการจัดการความต่อเนื่อง

มาตรฐานสากลสำหรับ BCMS ที่เน้นการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) และสร้างความเชื่อมั่น