กรอบงานการรักษาความปลอดภัยทางไซเบอร์ NIST (CSF) 2.0

National Institute of Standards and Technology

เอกสารนี้สามารถเข้าถึงได้ฟรีจาก: https://doi.org/10.6028/NIST.CSWP.29.tha

February 26, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

บทคัดย่อ

กรอบงานการรักษาความปลอดภัยทางไซเบอร์ของ NIST (CSF) 2.0 ให้คำแนะนำแก่ภาคอุตสาหกรรม หน่วยงานภาครัฐ และองค์กรอื่น ๆ ในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ รายงานดังกล่าวมีการจัดประเภทผลการดำเนินงานด้านการรักษาความปลอดภัยทางไซเบอร์ระดับสูงที่องค์กรใด ๆ จะสามารถนำไปใช้ได้ ไม่ว่าจะมีขนาดเท่าใด อยู่ในภาคส่วนใด หรือมีความครบถ้วนสมบูรณ์เพียงใด เพื่อทำความเข้าใจ ประเมิน กำหนดลำดับความสำคัญ และสื่อสารการดำเนินงานด้านการรักษาความปลอดภัยทางไซเบอร์ได้ดียิ่งขึ้น ทั้งนี้ CSF ไม่กำหนดว่าจะต้องดำเนินการอย่างไรให้บรรลุผล แต่จะเชื่อมโยงไปยังแหล่งข้อมูลออนไลน์ที่ให้คำแนะนำเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติและการควบคุมที่สามารถใช้เพื่อบรรลุผลเหล่านั้นได้ เอกสารนี้จะอธิบายเกี่ยวกับ CSF 2.0 ส่วนต่าง ๆ ของข้อมูล และวิธีการใช้งานบางส่วนจากวิธีการที่มากมายที่สามารถนำไปใช้ได้

คำสำคัญ

การรักษาความปลอดภัยทางไซเบอร์, กรอบการทำงานด้านการรักษาความปลอดภัยทางไซเบอร์ (CSF), การกำกับดูแลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์, การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์, การจัดการความเสี่ยงขององค์กร, โปรไฟล์, ระดับ

กลุ่มเป้าหมาย

บุคคลที่รับผิดชอบในการพัฒนาและนำโปรแกรมการรักษาความปลอดภัยทางไซเบอร์คือกลุ่มเป้าหมายหลักของ CSF นอกจากนี้ บุคคลอื่น ๆ ที่เกี่ยวข้องกับการจัดการความเสี่ยงยังสามารถใช้ CSF ได้ เช่น ผู้บริหาร คณะกรรมการ ผู้เชี่ยวชาญด้านการจัดซื้อ ผู้เชี่ยวชาญด้านเทคโนโลยี ผู้จัดการความเสี่ยง ทนายความ ผู้เชี่ยวชาญด้านทรัพยากรบุคคลและผู้ตรวจสอบด้านการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยง เพื่อเป็นแนวทางในการตัดสินใจที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ นอกจากนี้ CSF ยังมีประโยชน์ต่อผู้ที่กำหนดและมีอิทธิพลต่อนโยบาย (เช่น สมาคม องค์กรวิชาชีพ หน่วยงานกำกับดูแล) ที่กำหนดและสื่อสารความสำคัญของการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

เนื้อหาเพิ่มเติม

NIST จะยังคงสร้างและโฮสต์แหล่งข้อมูลเพิ่มเติมเพื่อช่วยให้องค์กรต่าง ๆ นำ CSF ไปใช้ รวมถึงคู่มือเริ่มต้นแบบเร่งรัดและโปรไฟล์ชุมชน ข้อมูลทั้งหมดได้จัดให้เผยแพร่สู่สาธารณะบน เว็บไซต์ NIST CSF สามารถแจ้งข้อเสนอแนะเกี่ยวกับแหล่งข้อมูลเพิ่มเติมเพื่ออ้างอิงบนเว็บไซต์ NIST CSF กับ NIST ได้ที่ cyberframework@nist.gov

หมายเหตุสำหรับผู้อ่าน

เอกสารที่อ้างอิง กล่าวถึงหรือตัดตอนมาในเอกสารนี้ไม่ใช่ข้อมูลที่คัดมาทั้งหมดเพื่อใช้ในเอกสารนี้ เว้นแต่จะระบุไว้เป็นอย่างอื่น

ในเวอร์ชันก่อน 2.0 กรอบการทำงานด้านการรักษาความปลอดภัยทางไซเบอร์มีชื่อว่า “กรอบการทำงานเพื่อปรับปรุงโครงสร้างพื้นฐานด้านการรักษาความปลอดภัยทางไซเบอร์ที่สำคัญ” และไม่ได้ใช้ชื่อนี้สำหรับ CSF 2.0

กิตติกรรมประกาศ

CSF คือผลจากความพยายามร่วมมือกันหลายปีระหว่างอุตสาหกรรม สถาบันการศึกษา และรัฐบาลในสหรัฐอเมริกาและทั่วโลก NIST ขอขอบคุณและแสดงความขอบคุณทุกท่านที่ร่วมสนับสนุนให้เกิด CSF ฉบับปรับปรุงใหม่นี้ ท่านสามารถดูข้อมูลเกี่ยวกับกระบวนการพัฒนา CSF ได้ที่ เว็บไซต์ NIST CSF และสามารถแบ่งปันสิ่งที่ได้เรียนรู้จากใช้ CSF กับ NIST ได้ที่ cyberframework@nist.gov

สารบัญ

รายการรูปภาพ

คำนำ

Cybersecurity Framework (CSF) 2.0 ได้รับการออกแบบมาเพื่อช่วยเหลือองค์กรทุกขนาดและทุกภาคส่วน รวมถึงภาคอุตสาหกรรม รัฐบาล สถาบันการศึกษาและองค์กรไม่แสวงหากำไรในการจัดการและลดความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ของตน CSF มีประโยชน์ไม่ว่าระดับความสมบูรณ์หรือความซับซ้อนทางเทคนิคของโปรแกรมการรักษาความปลอดภัยทางไซเบอร์ขององค์กรจะเป็นอย่างไร อย่างไรก็ตาม CSF ทราบดีว่าไม่มีแนวทางอย่างใดอย่างหนึ่งที่เหมาะสมกับทุกสถานการณ์ เนื่องจากแต่ละองค์กรมีทั้งความเสี่ยงทั่วไปและความเสี่ยงเฉพาะตัว ตลอดจนการยอมรับความเสี่ยงและการผ่อนระดับความเข้มงวด ตลอดจนภารกิจและวัตถุประสงค์เฉพาะในการบรรลุภารกิจเหล่านั้น ความจำเป็น วิธีที่องค์กรต่าง ๆ จะนำ CSF ไปปฏิบัตินั้นจะแตกต่างกันออกไป

ในทางอุดมคติแล้ว CSF จะถูกใช้เพื่อจัดการกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ควบคู่ไปกับความเสี่ยงอื่น ๆ ขององค์กร รวมถึงความเสี่ยงทางการเงิน ความเป็นส่วนตัว ห่วงโซ่อุปทาน ชื่อเสียง เทคโนโลยีหรือทางกายภาพ

CSF *ขออธิบาย*ถึงผลที่ต้องการว่าองค์กรมีจุดมุ่งหมายให้ผู้คนจำนวนมากเข้าใจ รวมถึงผู้บริหาร ผู้จัดการและผู้ปฏิบัติงาน โดยไม่คำนึงถึงความเชี่ยวชาญด้านการรักษาความปลอดภัยทางไซเบอร์ของพวกเขา เนื่องจากเป้าหมายเหล่านี้ไม่ได้เฉพาะเจาะจงตามภาคส่วน ประเทศ และเทคโนโลยี จึงทำให้มีความยืดหยุ่นตามความจำเป็นสำหรับองค์กรในการจัดการความเสี่ยง เทคโนโลยี และข้อควรพิจารณาเกี่ยวกับภารกิจเฉพาะของตน เป้าหมายจะถูกเชื่อมโยงกับมาตรการควบคุมความปลอดภัยที่มีศักยภาพโดยตรงเพื่อที่จะสามารถพิจารณาการบรรเทาความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ได้โดยทันที

แม้ว่าจะไม่ได้เป็นภาคบังคับ แต่ CSF ก็ช่วยให้ผู้ใช้เรียนรู้และเลือกเป้าหมายอย่างเฉพาะเจาะจง ข้อเสนอแนะเกี่ยวกับวิธีการบรรลุเป้าหมายที่เฉพาะเจาะจงนั้นมีอยู่ในทรัพยากรออนไลน์ที่ขยายตัวขึ้นซึ่งเสริม CSF ซึ่งรวมถึงคู่มือเริ่มต้นฉบับย่อ (QSG) ชุดหนึ่งด้วย นอกจากนี้ เครื่องมือต่าง ๆ ยังมีรูปแบบให้ดาวน์โหลดได้ เพื่อช่วยเหลือองค์กรที่เลือกที่จะทำให้กระบวนการบางส่วนเป็นระบบอัตโนมัติ QSG แนะนำวิธีเบื้องต้นในการใช้ CSF และเชิญชวนผู้อ่านให้สำรวจ CSF และแหล่งข้อมูลที่เกี่ยวข้องในเชิงลึกยิ่งขึ้น CSF และข้อมูลเสริมเหล่านี้จาก NIST และหน่วยงานอื่น ๆ ควรได้รับการพิจารณาในฐานะเป็น "พอร์ตโฟลิโอ CSF" เพื่อช่วยจัดการและลดความเสี่ยง ซึ่งสามารถเข้าถึงได้ผ่านทาง เว็บไซต์ NIST CSF ไม่ว่าจะนำไปใช้ในลักษณะใด CSF จะกระตุ้นให้ผู้ใช้พิจารณาแนวทางการรักษาการรักษาความปลอดภัยทางไซเบอร์ในบริบท และปรับ CSF ให้เหมาะกับความต้องการเฉพาะของตนเอง

การพัฒนาต่อยอดจากเวอร์ชันก่อนหน้า CSF 2.0 ประกอบด้วยฟีเจอร์ใหม่ที่เน้นย้ำถึงความสำคัญของ*การกำกับดูแล* และ *ห่วงโซ่อุปทาน* มีการให้ความสำคัญเป็นพิเศษกับ QSG เพื่อให้แน่ใจว่า CSF มีความเกี่ยวข้องและเข้าถึงได้ง่ายโดยองค์กรขนาดเล็กรวมถึงองค์กรขนาดใหญ่ ปัจจุบัน NIST มี *ตัวอย่างการนำไปใช้* และ *เอกสารอ้างอิงข้อมูล* ซึ่งสามารถดูได้ทางออนไลน์และอัปเดตเป็นประจำ การสร้าง *โปรไฟล์ องค์กร* ในสถานะปัจจุบันและสถานะเป้าหมายจะช่วยให้องค์กรเปรียบเทียบสถานะของตนเองกับสถานะที่ต้องการหรือจำเป็นต้องเป็นได้ และทำให้สามารถดำเนินการและประเมินการควบคุมความปลอดภัยได้รวดเร็วยิ่งขึ้น

ความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพิ่มขึ้นอย่างต่อเนื่อง และการจัดการความเสี่ยงเหล่านั้นจะต้องเป็นกระบวนการต่อเนื่อง เรื่องนี้เป็นจริงโดยไม่คำนึงว่าองค์กรจะเพิ่งเริ่มเผชิญกับความท้าทายด้านการรักษาความปลอดภัยทางไซเบอร์หรือดำเนินกิจการมาหลายปีโดยมีทีมงานด้านการรักษาความปลอดภัยทางไซเบอร์ที่มีความซับซ้อนและมีแหล่งข้อมูลมากมาย CSF ได้รับการออกแบบมาเพื่อให้มีคุณค่าสำหรับองค์กรทุกประเภทและคาดว่าจะให้คำแนะนำที่เหมาะสมเป็นเวลานาน

1. ภาพรวมกรอบการรักษาความปลอดภัยทางไซเบอร์ (CSF)

เอกสารนี้เป็นเวอร์ชัน 2.0 ของ NIST Cybersecurity Framework (*Framework* หรือ *CSF*) ซึ่งมีส่วนประกอบดังต่อไปนี้:

- ***CSF Core*** ซึ่งเป็นแกนหลักของ CSF ซึ่งเป็นอนุกรมวิธานเป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ระดับสูงที่สามารถช่วยให้องค์กรใด ๆ ก็ตามสามารถจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ได้ ส่วนประกอบหลักของ CSF จะมีการจัดลำดับชั้นของฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยที่ให้รายละเอียดเป้าหมายแต่ละรายการ ผู้คนจำนวนมากสามารถเข้าใจเป้าหมายเหล่านี้ได้ รวมถึงผู้บริหาร ผู้จัดการและผู้ปฏิบัติ โดยไม่คำนึงถึงความเชี่ยวชาญด้านการรักษาความปลอดภัยทางไซเบอร์ของพวกเขา เนื่องจากเป้าหมายไม่มีความเฉพาะเจาะจงกับด้านภาคส่วน ประเทศ และเทคโนโลยีใด จึงทำให้มีความยืดหยุ่นสำหรับองค์กรในการจัดการความเสี่ยง เทคโนโลยีและข้อควรพิจารณาเกี่ยวกับภารกิจเฉพาะของตน
- ***โปรไฟล์องค์กร CSF*** ซึ่งเป็นกลไกในการอธิบายสถานะการรักษาความปลอดภัยทางไซเบอร์ปัจจุบันและ/หรือเป้าหมายขององค์กรตามเป้าหมายของ CSF Core
- ***ระดับ CSF*** ซึ่งสามารถนำไปใช้กับโปรไฟล์องค์กร CSF เพื่อกำหนดความเข้มงวดของการกำกับดูแลและแนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ระดับชั้นยังสามารถให้ข้อมูลบริบทเกี่ยวกับวิธีที่องค์กรมองความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และกระบวนการต่าง ๆ ที่มีอยู่เพื่อจัดการความเสี่ยงเหล่านั้น

เอกสารนี้บรรยายถึง*สิ่งที่เป็น* เป้าหมายที่พึงประสงค์ที่องค์กรสามารถที่จะบรรลุได้ เอกสารนี้ไม่ได้ *กำหนด* เป้าหมายหรือ *วิธี* ที่จะบรรลุเป้าหมายเหล่านั้น คำอธิบายเกี่ยวกับ *วิธีที่*องค์กรสามารถบรรลุเป้าหมายเหล่านั้นได้มีอยู่ในชุดแหล่งข้อมูลออนไลน์เสริมของ CSF และมีให้บริการผ่าน เว็บไซต์ NIST CSF ข้อมูลเหล่านี้มีคำแนะนำเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติและการควบคุมที่สามารถใช้เพื่อบรรลุเป้าหมาย และมีจุดมุ่งหมายเพื่อช่วยให้องค์กรเข้าใจ และนำ CSF มาใช้ ซึ่งประกอบด้วย:

- *ข้อมูลอ้างอิง* ที่ให้ข้อมูลชี้ไปยังแหล่งที่มาของคำแนะนำในแต่ละเป้าหมายจากมาตรฐาน แนวปฏิบัติ กรอบงาน กฎระเบียบ นโยบาย ฯลฯ ที่ใช้กันในระดับโลก
- *ตัวอย่างการนำไปใช้* ที่แสดงให้เห็นวิธีการที่เป็นไปได้ในการบรรลุเป้าหมายแต่ละประการ
- *คู่มือเริ่มต้นอย่างรวดเร็ว* ที่ให้คำแนะนำเชิงปฏิบัติเกี่ยวกับการใช้ CSF และแหล่งข้อมูลออนไลน์ รวมถึงการเปลี่ยนจาก CSF เวอร์ชันก่อนหน้าไปเป็นเวอร์ชัน 2.0
- *โปรไฟล์ชุมชน และ เทมเพลต โปรไฟล์องค์กร*ที่ช่วยให้องค์กรนำ CSF ไปปฏิบัติและกำหนดลำดับความสำคัญในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

องค์กรสามารถใช้ CSF Core, Profiles และ Tiers พร้อมกับแหล่งข้อมูลเพิ่มเติมเพื่อทำความเข้าใจ ประเมิน กำหนดลำดับความสำคัญและสื่อสารเรื่องความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

- **ความเข้าใจและประเมิน**: อธิบายสถานะการรักษาความปลอดภัยทางไซเบอร์ปัจจุบันหรือเป้าหมายของส่วนหนึ่งหรือทั้งหมดขององค์กร หาช่องโหว่และประเมินความคืบหน้าในการแก้ไขช่องโหว่เหล่านั้น
- **กำหนดลำดับความสำคัญ**: ระบุ จัดระเบียบและจัดลำดับความสำคัญของการดำเนินการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่สอดคล้องกับภารกิจขององค์กร ข้อกำหนดทางกฎหมายและข้อบังคับ และการจัดการความเสี่ยงและความคาดหวังด้านการกำกับดูแล

- **สื่อสาร**: จัดทำภาษาที่เป็นสื่อกลางในการสื่อสารภายในและภายนอกองค์กรเกี่ยวกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ ความสามารถ ความต้องการ และความคาดหวัง

CSF ได้รับการออกแบบมาเพื่อให้องค์กรทุกขนาดและทุกภาคส่วนได้ใช้งาน ซึ่งประกอบด้วยภาคอุตสาหกรรม รัฐบาล สถาบันการศึกษา และองค์กรไม่แสวงหากำไร โดยไม่คำนึงถึงระดับความพร้อมของโปรแกรมการรักษาความปลอดภัยทางไซเบอร์ขององค์กร CSF เป็นข้อมูลพื้นฐานที่สามารถนำมาใช้ได้ทั้งโดยสมัครใจและนำมาใช้ผ่านนโยบายและคำสั่งของรัฐบาล อนุกรมวิธานและมาตรฐาน แนวปฏิบัติ และแนวทางอ้างอิงของ CSF ไม่ได้มีความจำเพาะเจาะจงสำหรับประเทศใดประเทศหนึ่ง และ CSF เวอร์ชันก่อนหน้านี้ได้ถูกนำไปใช้อย่างประสบความสำเร็จโดยรัฐบาลและองค์กรอื่น ๆ หลายแห่งทั้งภายในและภายนอกสหรัฐอเมริกา

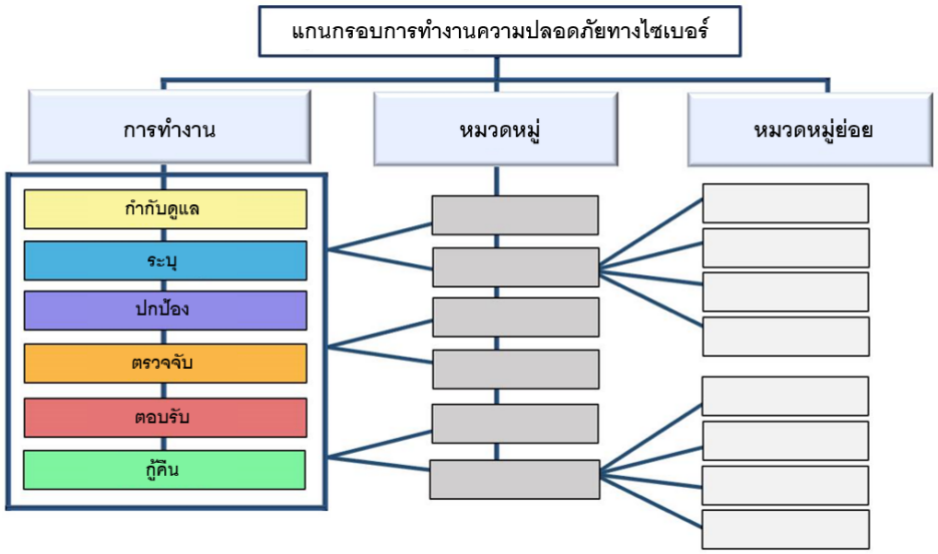
ควรใช้ CSF ร่วมกับแหล่งข้อมูลอื่น ๆ (เช่น กรอบงาน มาตรฐาน แนวปฏิบัติ แนวทางปฏิบัติชั้นนำ) เพื่อจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ให้ดีขึ้น และรายงานภาพรวมในการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ในระดับองค์กร ทั้งนี้ CSF เป็นกรอบงานแบบยืดหยุ่นที่ออกแบบมาเพื่อให้เหมาะกับการใช้งานโดยองค์กรต่าง ๆ ไม่ว่าจะเป็นขนาดใด ทั้งนี้ องค์กรต่าง ๆ จะยังคงมีความเสี่ยงที่แตกต่างกันออกไป รวมถึงภัยคุกคามและจุดอ่อนที่แตกต่างกัน รวมถึงการยอมรับความเสี่ยง ตลอดจนวัตถุประสงค์และข้อกำหนดของภารกิจที่แตกต่างกันไป ดังนั้น แนวทางขององค์กรในการจัดการความเสี่ยงและการนำ CSF ไปใช้จึงแตกต่างกัน

ส่วนที่เหลือของเอกสารนี้มีโครงสร้างดังนี้:

- ส่วนที่ *2* อธิบายพื้นฐานของแกนหลักของ CSF: ฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อย
- ส่วนที่ *3* กำหนดแนวคิดของโปรไฟล์และระดับ CSF
- ส่วนที่ *4* ระบุภาพรวมของส่วนประกอบที่เลือกจากชุดแหล่งข้อมูลออนไลน์ของ CSF: ข้อมูลอ้างอิง ตัวอย่างการนำไปใช้และคู่มือเริ่มต้นแบบเร่งด่วน
- ส่วนที่ *5* หารือถึงวิธีที่องค์กรสามารถบูรณาการ CSF เข้ากับโปรแกรมการจัดการความเสี่ยงอื่น ๆ ได้
- *0* คือ แกนหลักของ CSF
- ภาคผนวก*0* ซึ่งมีภาพประกอบเชิงทฤษฎีของ CSF Tiers
- *0* เป็นรายการคำศัพท์เฉพาะทาง CSF

2. บทนำสู่แกนหลักของ CSF (CSF Core)

0 เป็น CSF Core ซึ่งเป็นชุดเป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ที่จัดเรียงตามฟังก์ชัน จากนั้นเป็นหมวดหมู่ และสุดท้ายคือหมวดหมู่ย่อย ตามที่แสดงใน**ภาพที่** *1* เป้าหมายเหล่านี้ไม่ใช่รายการตรวจสอบการดำเนินการที่จะทำ การดำเนินการที่เฉพาะเจาะจงเพื่อให้องค์กรใดองค์กรหนึ่งบรรลุเป้าหมายนั้นจะแตกต่างกันไปตามองค์กรและกรณีการใช้งาน เช่นเดียวกับบุคคลที่รับผิดชอบในการดำเนินการเหล่านั้น นอกจากนี้ ลำดับและขนาดของฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยในแกนหลักไม่ได้เป็นการเรียงลำดับหรือความสำคัญของการบรรลุผลเหล่านั้น โครงสร้างของแกนหลักได้รับการออกแบบมาเพื่อสะท้อนกับงานของผู้ที่มีหน้าที่ปฏิบัติการด้านการบริหารความเสี่ยงภายในองค์กรมากที่สุด



ภาพที่ *1* **โครงสร้างแกนหลัก** CSF

ฟังก์ชันหลักของ CSF — ควบคุม ระบุ ปกป้อง ตรวจจับ ตอบสนองและกู้คืน — จัดระเบียบเป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ให้อยู่ในระดับสูงสุด

- **การกำกับดูแล** (GV) — *มีการจัดทำ สื่อสารและตรวจสอบกลยุทธ์ ความคาดหวัง และนโยบายการจัดการความเสี่ยงทางไซเบอร์ขององค์กร* ฟังก์ชันการกำกับดูแลมีเพื่อแจ้งให้ทราบว่าองค์กรสามารถทำอะไรได้บ้างเพื่อบรรลุผล และกำหนดลำดับความสำคัญของฟังก์ชันอื่น ๆ ทั้งทั้งห้าด้านของภารกิจและความคาดหวังของผู้มีส่วนได้ส่วนเสีย กิจกรรมการกำกับดูแลถือเป็นสิ่งสำคัญสำหรับการผสานการรักษาการรักษาความปลอดภัยทางไซเบอร์เข้ากับกลยุทธ์การจัดการความเสี่ยงระดับองค์กร (ERM) ที่ครอบคลุมกว้างขึ้น การกำกับดูแลจะช่วยให้เกิดความเข้าใจบริบทขององค์กร รวมทั้งการกำหนดกลยุทธ์ด้านการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยงในห่วงโซ่อุปทานด้านการรักษาความปลอดภัยทางไซเบอร์ บทบาท ความรับผิดชอบและอำนาจ นโยบาย และการกำกับดูแลกลยุทธ์ด้านการรักษาความปลอดภัยทางไซเบอร์
- **ระบุ** (ID) — *ทำให้ความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันขององค์กรเป็นที่เข้าใจของบุคลากร* ความเข้าใจว่าอะไรคือสินทรัพย์ขององค์กร (เช่น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ ระบบ สิ่งอำนวยความสะดวก บริการ บุคลากร) ซัพพลายเออร์ และความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง จะช่วยให้องค์กรสามารถจัดลำดับความสำคัญของการดำเนินงานที่สอดคล้องกับกลยุทธ์การจัดการความเสี่ยงและจุดมุ่งหมายของภารกิจที่ภายใต้การกำกับดูแล ฟังก์ชันนี้ยังรวมถึงการหาโอกาสในการปรับปรุงนโยบาย แผน กระบวนการ ขั้นตอน และแนวปฏิบัติขององค์กรที่สนับสนุนการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อเพื่อการดำเนินงานภายใต้ฟังก์ชันทั้งหกประการ

- **การป้องกัน** (PR) — *ใช้มาตรการป้องกันเพื่อจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร* เมื่อมีการระบุและจัดลำดับความสำคัญของสินทรัพย์และความเสี่ยงแล้ว การปกป้องจะช่วยทำให้เกิดความสามารถในการรักษาความปลอดภัยของสินทรัพย์เหล่านั้นเพื่อป้องกันหรือลดโอกาสและผลกระทบของเหตุการณ์ทางไซเบอร์ที่ไม่พึงประสงค์ ตลอดจนเพิ่มโอกาสและความเป็นไปได้ที่จะใช้ประโยชน์จากโอกาสต่างๆ เป้าหมายที่คาดว่าจะบรรลุได้โดยฟังก์ชันนี้ ได้แก่ การจัดการข้อมูลประจำตัว การรับรองความถูกต้องและการควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล ความปลอดภัยของแพลตฟอร์ม (เช่น การรักษาความปลอดภัยฮาร์ดแวร์ ซอฟต์แวร์ และบริการของแพลตฟอร์มทางกายภาพและแบบเสมือนจริง) และความยืดหยุ่นของโครงสร้างพื้นฐานด้านเทคโนโลยี
- **การตรวจจับ** (DE) — *ค้นหาและวิเคราะห์การโจมตีทางไซเบอร์และช่องโหว่ที่อาจเกิดขึ้น* การตรวจจับจะช่วยให้ค้นพบและวิเคราะห์ความผิดปกติ ตัวบ่งชี้ช่องโหว่ของการรักษาความปลอดภัย และเหตุการณ์ไม่พึงประสงค์อื่นๆ ที่อาจเป็นสัญญาณว่ากำลังเกิดการโจมตีทางไซเบอร์และเหตุการณ์ต่าง ๆ ได้อย่างทันท่วงที ฟังก์ชันนี้สนับสนุนให้เกิดการตอบสนองต่อเหตุการณ์และกิจกรรมการกู้คืนที่ประสบความสำเร็จ
- **การตอบสนอง** (RS) — *ดำเนินการเกี่ยวกับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่ตรวจพบ* การตอบสนองจะช่วยให้เกิดความสามารถในการควบคุมผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ เป้าหมายที่คาดว่าจะเกิดจากฟังก์ชันนี้ได้แก่ การจัดการ การวิเคราะห์ การบรรเทา การรายงานและการสื่อสารเหตุการณ์
- **การกู้คืน** (RC) — *สินทรัพย์และการดำเนินงานที่ได้รับผลกระทบจากเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์จะได้รับการกู้คืน* การกู้คืนจะช่วยให้การดำเนินงานกลับมาเป็นปกติอย่างทันท่วงทีเพื่อลดผลกระทบของเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์และทำให้เกิดช่องทางการสื่อสารที่เหมาะสมระหว่างการกู้คืน

ในขณะที่กิจกรรมการจัดการความเสี่ยงทางไซเบอร์จำนวนมากมุ่งเน้นไปที่การป้องกันไม่ให้เกิดเหตุการณ์เชิงลบ กิจกรรมเหล่านี้อาจสนับสนุนการใช้ประโยชน์จากโอกาสในเชิงบวกด้วยเช่นกัน การดำเนินการเพื่อลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์อาจเป็นประโยชน์ต่อองค์กรในรูปแบบอื่น ๆ เช่น การเพิ่มรายได้ (เช่น เสนอพื้นที่ส่วนเกินให้กับผู้ให้บริการโฮสต์เชิงพาณิชย์เพื่อโฮสต์ศูนย์ข้อมูลของตนเองหรือขององค์กรอื่น จากนั้นจึงย้ายระบบการเงินหลักจากศูนย์ข้อมูลภายในองค์กรไปยังผู้ให้บริการโฮสต์เพื่อลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์)

ภาพที่ 2 แสดงฟังก์ชัน CSF แบบเป็นวงจร เนื่องจากฟังก์ชันทั้งหมดมีความสัมพันธ์กัน ตัวอย่างเช่น องค์กรจะจัดประเภทสินทรัพย์จากฟังก์ชันการระบุและดำเนินการรักษาสินทรัพย์เหล่านั้นจากฟังก์ชันการปกป้อง การลงทุนด้านการวางแผนและการทดสอบจากฟังก์ชันการกำกับดูแล และการระบุจะช่วยให้เกิดการตรวจจับเหตุการณ์ที่ไม่ได้คาดการณ์มาก่อนในฟังก์ชันการตรวจจับได้ทันท่วงที รวมถึงการเปิดใช้ฟังก์ชันการตอบสนองต่อเหตุการณ์และการกู้คืนสำหรับเหตุการณ์ทางไซเบอร์ในฟังก์ชันการตอบรับและการกู้คืน การกำกับดูแลอยู่ตรงศูนย์กลางของวงจร เพราะเป็นการแจ้งให้ทราบว่าองค์กรจะนำฟังก์ชันอีกห้าประการไปใช้อย่างไร

ภาพที่ *2* **ฟังก์ชัน** CSF

ควรจัดการฟังก์ชันต่าง ๆ ในเวลาเดียวกัน การดำเนินการที่สนับสนุน การกำกับดูแล การระบุ การปกป้อง และการตรวจจับ ควรเกิดขึ้นอย่างต่อเนื่อง และการดำเนินการที่สนับสนุน การตอบสนองและการกู้คืน ควรมีความพร้อมตลอดเวลา และดำเนินการเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ขึ้น ฟังก์ชันทั้งหมดมีบทบาทสำคัญที่เกี่ยวข้องกับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ การกำกับดูแล การระบุ และการปกป้องจะช่วยป้องกันและเตรียมพร้อมสำหรับเหตุการณ์ ในขณะที่การควบคุม การตรวจจับ การตอบสนอง และการกู้คืนจะช่วยค้นหาและจัดการเหตุการณ์

ฟังก์ชันแต่ละอย่างได้รับการตั้งชื่อตามคำกริยาที่สรุปหน้าที่ของฟังก์ชันนั้น ฟังก์ชันแต่ละอย่างจะถูกแบ่งออกเป็น *หมวดหมู่* ซึ่งเป็นกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องซึ่งประกอบกันเป็นฟังก์ชันนั้น *หมวดหมู่ย่อย* จะแบ่งหมวดหมู่แต่ละหมวดหมู่ออกเป็นเป้าหมายที่เฉพาะเจาะจงมากขึ้นจากกิจกรรมทางเทคนิคและการจัดการ เนื้อหาไม่ได้ครอบคลุมถึงหมวดหมู่ย่อยโดยละเอียด แต่มีการอธิบายรายละเอียดกิจกรรมที่สนับสนุนแต่ละหมวดหมู่

ฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยจะใช้กับ ICT ทั้งหมดที่องค์กรใช้ รวมถึงเทคโนโลยีสารสนเทศ (IT) อินเทอร์เน็ตของทุกสรรพสิ่ง (IoT) และเทคโนโลยีการดำเนินงาน (OT) สิ่งเหล่านี้ยังสามารถนำไปประยุกต์ใช้กับสภาพแวดล้อมทางเทคโนโลยีทุกประเภท รวมถึงระบบคลาวด์ มือถือ และปัญญาประดิษฐ์อีกด้วย CSF Core เป็นการมองไปยังอนาคตด้วยความตั้งใจที่จะนำไปใช้กับการเปลี่ยนแปลงในด้านเทคโนโลยีและสภาพแวดล้อมต่าง ๆ ในอนาคต

3. บทนำเกี่ยวกับโปรไฟล์และระดับ CSF

หัวข้อนี้จะระบุถึงแนวคิดของโปรไฟล์และระดับ CSF

3.1. โปรไฟล์ CSF

โปรไฟล์องค์กร CSF อธิบายสถานะการรักษาความปลอดภัยทางไซเบอร์ปัจจุบันและ/หรือเป้าหมายขององค์กรในแง่ของเป้าหมายของแกนหลัก โปรไฟล์องค์กร ใช้เพื่อทำความเข้าใจ ปรับแต่ง ประเมิน กำหนดลำดับความสำคัญ และสื่อสารเป้าหมายของแกนหลัก โดยพิจารณาจากวัตถุประสงค์ ภารกิจขององค์กร ความคาดหวังของผู้มีส่วนได้ส่วนเสีย ภาพรวมของภัยคุกคาม และข้อกำหนดต่าง ๆ องค์กรสามารถกำหนดลำดับความสำคัญของการดำเนินการเพื่อให้บรรลุเป้าหมายที่ต้องการอย่างเฉพาะเจาะจง และสื่อสารข้อมูลดังกล่าวไปยังผู้มีส่วนได้ส่วนเสีย

โปรไฟล์องค์กรทุกรายการจะประกอบด้วยสิ่งต่อไปนี้อย่างใดอย่างหนึ่งหรือทั้งสองอย่าง:

1. *โปรไฟล์ปัจจุบัน* จะระบุเป้าหมายหลักที่องค์กรกำลังบรรลุ (หรือพยายามบรรลุ) ในปัจจุบัน และระบุถึงวิธีการหรือขอบเขตในการบรรลุเป้าหมายแต่ละอย่าง
2. *โปรไฟล์เป้าหมาย* ระบุเป้าหมายที่ต้องการที่องค์กรเลือกและกำหนดลำดับความสำคัญเพื่อให้บรรลุวัตถุประสงค์การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ โปรไฟล์เป้าหมายจะพิจารณาการเปลี่ยนแปลงที่คาดว่าจะเกิดขึ้นกับการเปลี่ยนแปลงของการรักษาความปลอดภัยทางไซเบอร์ขององค์กร เช่น ข้อกำหนดใหม่ การนำเทคโนโลยีใหม่มาใช้ และแนวโน้มข้อมูลข่าวกรองด้านภัยคุกคาม

> *โปรไฟล์ชุมชน* เป็นฐานข้อมูลเป้าหมายของ CSF ที่ถูกสร้างขึ้นและเผยแพร่เพื่อตอบสนองความสนใจและเป้าหมายร่วมกันระหว่างองค์กรต่าง ๆ โดยทั่วไป โปรไฟล์ชุมชนจะได้รับการพัฒนาสำหรับภาคส่วนเฉพาะ ภาคส่วนย่อย เทคโนโลยี ประเภทภัยคุกคาม หรือกรณีการใช้งานอื่นโดยเฉพาะ องค์กรสามารถใช้โปรไฟล์ชุมชนเป็นพื้นฐานสำหรับโปรไฟล์เป้าหมายของตนเองได้ ตัวอย่างโปรไฟล์ชุมชนสามารถพบได้ในเว็บไซต์ NIST CSF

ขั้นตอนที่แสดงในภาพที่ 3 และสรุปไว้ด้านล่างแสดงแนวทางหนึ่งที่องค์กรสามารถใช้โปรไฟล์องค์กรเพื่อช่วยปรับปรุงด้านการรักษาความปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

ภาพที่ 3 ขั้นตอนในการสร้างและใช้โปรไฟล์องค์กร CSF

1. **กำหนดขอบเขตโปรไฟล์องค์กร** จัดทำเอกสารข้อเท็จจริงและสมมติฐานระดับสูงที่โปรไฟล์จะอ้างอิงเพื่อกำหนดขอบเขต องค์กรสามารถมีโปรไฟล์องค์กรได้มากเท่าที่ต้องการ โดยแต่ละโปรไฟล์จะมีขอบเขตที่แตกต่างกัน ตัวอย่างเช่น โปรไฟล์สามารถระบุถึงองค์กรทั้งหมดหรือจำกัดเฉพาะระบบการเงินขององค์กร หรือเพื่อต่อต้านภัยคุกคามจากแรนซัมแวร์และจัดการกับเหตุการณ์แรนซัมแวร์ที่เกี่ยวข้องกับระบบการเงินเหล่านั้น
2. **รวบรวมข้อมูลที่จำเป็นในการจัดทำโปรไฟล์องค์กร** ตัวอย่างข้อมูลอาจประกอบด้วย นโยบายขององค์กร ลำดับความสำคัญและแหล่งข้อมูลในการจัดการความเสี่ยง โปรไฟล์ความเสี่ยงขององค์กร บันทึกการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ข้อกำหนดและมาตรฐานด้านการรักษาความปลอดภัยทางไซเบอร์ที่องค์กรได้ปฏิบัติตาม แนวทางปฏิบัติและเครื่องมือ (เช่น ขั้นตอนและการป้องกัน) และบทบาทการทำงาน
3. **สร้างโปรไฟล์องค์กร** กำหนดประเภทข้อมูลที่โปรไฟล์ตามเป้าหมาย CSF ที่เลือก และจัดทำเอกสารข้อมูลที่จำเป็น พิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นจากโปรไฟล์ในปัจจุบัน เพื่อแจ้งให้ทราบถึงการวางแผนและกำหนดลำดับความสำคัญของโปรไฟล์เป้าหมาย นอกจากนี้ ควรพิจารณาใช้โปรไฟล์ชุมชนเป็นพื้นฐานสำหรับโปรไฟล์เป้าหมายด้วย
4. **วิเคราะห์ความแตกต่างระหว่างโปรไฟล์ปัจจุบันและโปรไฟล์เป้าหมาย และสร้างแผนปฏิบัติการ** ดำเนินการวิเคราะห์ความแตกต่างเพื่อระบุและวิเคราะห์ความแตกต่างระหว่างโปรไฟล์ปัจจุบันและโปรไฟล์เป้าหมาย และพัฒนากรอบการดำเนินการตามลำดับความสำคัญ (เช่น บันทึกความเสี่ยง รายงานรายละเอียดความเสี่ยง แผนปฏิบัติการและเหตุการณ์สำคัญ [POA&M]) เพื่อแก้ไขความแตกต่างเหล่านั้น
5. **ดำเนินการตามแผนปฏิบัติการ และอัปเดตโปรไฟล์องค์กร** ปฏิบัติตามแผนดำเนินการเพื่อแก้ไขช่องว่างและนำองค์กรไปสู่เป้าหมาย แผนปฏิบัติการอาจมีการกำหนดระยะเวลาสิ้นสุดของแผนหรือดำเนินการอย่างต่อเนื่อง

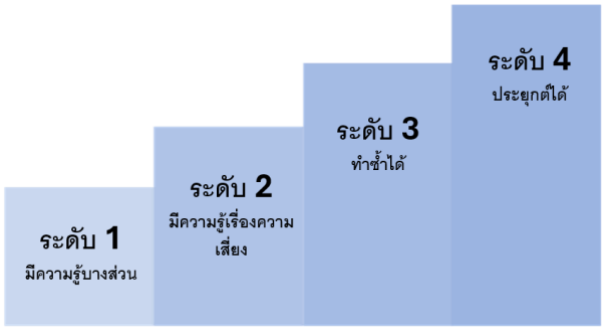
เมื่อพิจารณาถึงความสำคัญของการพัฒนาอย่างต่อเนื่อง องค์กรจึงสามารถดำเนินขั้นตอนเหล่านี้ซ้ำได้บ่อยเท่าที่จำเป็น

ยังสามารถใช้งานอื่น ๆในโปรไฟล์องค์กรได้ ตัวอย่างเช่น สามารถใช้โปรไฟล์ปัจจุบันเพื่อบันทึกและสื่อสารความสามารถด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร และโอกาสในการปรับปรุงที่องค์กรทราบกับผู้มีส่วนได้ส่วนเสียภายนอก เช่น พันธมิตรทางธุรกิจ หรือผู้ที่มีแนวโน้มจะเป็นลูกค้า นอกจากนี้ โปรไฟล์เป้าหมายยังช่วยแสดงความต้องการและความคาดหวังในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรให้ซัพพลายเออร์ พันธมิตร และบุคคลภายนอกอื่น ๆ ทราบเพื่อให้บุคคลภายนอกเหล่านั้นช่วยทำให้บรรลุเป้าหมายได้

3.2. ระดับ CSF

องค์กรสามารถเลือกใช้ระดับเพื่อแจ้งโปรไฟล์ปัจจุบันและเป้าหมายได้ *ระดับต่างๆ* แสดงถึงความเข้มงวดในการกำกับดูแลและจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร และยังเป็นการแสดงว่าองค์กรมองความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์อย่างไร และกระบวนการต่าง ๆ ที่มีอยู่ในการจัดการความเสี่ยงเหล่านั้นเป็นอย่างไร ระดับต่าง ๆ ตามที่แสดงในภาพที่ 4 และที่แสดงเป็นภาพประกอบในเชิงทฤษฎีในภาคผนวก B สะท้อนถึงแนวทางปฏิบัติขององค์กรในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในรูปแบบบางส่วน (ระดับ 1) การมีความรู้เรื่องความเสี่ยง (ระดับ 2) ทำซ้ำได้ (ระดับ 3) และการนำไปประยุกต์ใช้ได้ (ระดับ 4) ระดับต่าง ๆ อธิบายถึงความก้าวหน้าจากการตอบสนองเหตุการณ์ที่ไม่เป็นทางการและเฉพาะหน้า ไปจนถึงวิธีการแก้ปัญหาที่มีความคล่องตัวโดยคำนึงถึงความเสี่ยง

และปรับปรุงอย่างต่อเนื่อง การเลือกระดับจะช่วยกำหนดลักษณะการทำงานโดยรวมว่าองค์กรจะจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์อย่างไร



ภาพที่ *4* CSF Tiers สำหรับการกำกับดูแลและจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

ระดับต่าง ๆ ควรเป็นส่วนเสริมวิธีการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ไม่ใช่นำมาใช้แทนที่วิธีการจัดการ ตัวอย่างเช่น องค์กรสามารถใช้ระดับต่าง ๆเพื่อสื่อสารภายเพื่อใช้เป็นเกณฑ์มาตรฐานสำหรับทั้งองค์กร[1] แนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ ขอแนะนำให้เลื่อนไปสู่ระดับที่สูงขึ้นเมื่อมีความจำเป็นที่ต้องจัดการความเสี่ยงมากขึ้น หรือเมื่อการบ่งชี้ว่าสามารถทำได้และสามารถลดความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่ไม่พึงประสงค์ได้โดยคุ้มกับค่าใช้จ่าย

เว็บไซต์ NIST CSF จะให้ข้อมูลเพิ่มเติมเกี่ยวกับการใช้โปรไฟล์และระดับต่าง ๆ รวมถึงจะนำไปยัง เทมเพลตโปรไฟล์องค์กรที่โฮสต์โดย NIST และที่เก็บ โปรไฟล์ชุมชน ในรูปแบบที่อ่านได้ด้วยคอมพิวเตอร์และมีรูปแบบที่สามารถใช้งานได้หลากหลาย

[1] ในเอกสารนี้ คำว่า "ทั่วทั้งองค์กร" และ "องค์กร" มีความหมายเดียวกัน

4. ข้อมูลเบื้องต้นเกี่ยวกับแหล่งข้อมูลออนไลน์เพิ่มเติมของ CSF

NIST และองค์กรอื่น ๆ ได้จัดทำชุดแหล่งข้อมูลออนไลน์เพื่อช่วยให้องค์กรต่าง ๆ เข้าใจและนำ CSF มาใช้งาน เนื่องจากข้อมูลเหล่านี้ได้รับการโฮสต์ออนไลน์ จึงสามารถอัปเดตได้บ่อยกว่าเอกสารฉบับนี้ซึ่งอัปเดตไม่บ่อยนักเพื่อความเสถียรในการใช้งาน และยังสามารถใช้งานในรูปแบบที่คอมพิวเตอร์อ่านได้ หัวข้อนี้จะระบุภาพรวมของแหล่งข้อมูลออนไลน์สามประเภท ได้แก่ เอกสารอ้างอิงข้อมูล ตัวอย่างการนำไปใช้ และคู่มือเพื่อการเริ่มต้นอย่างรวดเร็ว

ข้อมูลอ้างอิง เป็นการวางเค้าโครงข้อมูลที่ระบุความสัมพันธ์ระหว่างแกนหลักและมาตรฐาน แนวทาง กฎระเบียบ และเนื้อหาอื่นๆ ต่างๆ ข้อมูลอ้างอิงช่วยให้ทราบว่าองค์กรจะบรรลุเป้าหมายหลักได้อย่างไร ข้อมูลอ้างอิงอาจเป็นแบบเฉพาะตามภาคส่วนหรือเทคโนโลยีก็ได้ อาจจัดทำโดย NIST หรือองค์กรอื่น ข้อมูลอ้างอิงบางรายการมีขอบเขตแคบกว่าหมวดหมู่ย่อย ตัวอย่างเช่น การควบคุมเฉพาะด้านตาม SP 800-53 *การควบคุมความปลอดภัยและความเป็นส่วนตัวสำหรับระบบสารสนเทศและองค์กร* อาจเป็นหนึ่งในเอกสารอ้างอิงจำนวนมากที่จำเป็นต่อการบรรลุเป้าหมายที่อธิบายไว้ในหมวดหมู่ย่อยหนึ่ง ข้อมูลอ้างอิงอื่น ๆ อาจมีระดับที่สูงกว่า เช่น ข้อกำหนดจากนโยบายที่ระบุข้อมูลบางส่วนของหมวดหมู่ย่อยหลายประการ เมื่อใช้ CSF องค์กรสามารถระบุข้อมูลอ้างอิงที่มีความเกี่ยวข้องที่สุดได้

ตัวอย่างการนำไปปฏิบัติ จะให้ตัวอย่างเชิงทฤษฎีของขั้นตอนที่กระชับและมุ่งเน้นการดำเนินการเพื่อช่วยให้บรรลุเป้าหมายของหมวดหมู่ย่อย คำกริยาที่ใช้เพื่อแสดงตัวอย่างประกอบด้วยคำว่า แบ่งปัน บันทึก พัฒนา ดำเนินการ ตรวจสอบ วิเคราะห์ ประเมินและการดำเนินการ ตัวอย่างเหล่านี้ไม่ใช่รายการครอบคลุมของการดำเนินการทั้งหมดที่องค์กรสามารถดำเนินการเพื่อให้บรรลุเป้าหมายบางประการและไม่ได้แสดงถึงการดำเนินการที่จำเป็นเพื่อจัดการกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์แต่อย่างใด

คู่มือเพื่อการเริ่มต้นอย่างรวดเร็ว (QSG) เป็นเอกสารโดยย่อเกี่ยวกับหัวข้อเฉพาะที่เกี่ยวข้องกับ CSF และมักจะมีการปรับเนื้อหาให้เหมาะกับกลุ่มเป้าหมายเฉพาะ QSG สามารถช่วยให้องค์กรนำ CSF ไปใช้จริงได้ เนื่องจาก QSG จะสรุปส่วนเฉพาะเจาะจงของ CSF ให้เป็น “ขั้นตอนแรก” ที่สามารถดำเนินการได้จริง ซึ่งองค์กรสามารถพิจารณาเป็นจุดเริ่มต้นของแนวทางสู่การปรับปรุงแนวทางด้านการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยงที่เกี่ยวข้อง คำแนะนำจะได้รับการแก้ไขตามรอบเวลาของตนเอง และจะมีการเพิ่มคำแนะนำใหม่ ๆ ตามความจำเป็น

สามารถแบ่งปันข้อเสนอแนะสำหรับข้อมูลอ้างอิงใหม่ ๆ สำหรับ CSF 2.0 กับ NIST ได้ที่ olir@nist.gov และโปรดส่งข้อเสนอแนะสำหรับแหล่งข้อมูลอื่น ๆ เพื่ออ้างอิงบนเว็บไซต์ NIST CSF รวมถึงหัวข้อ QSG เพิ่มเติมไปที่ cyberframework@nist.gov

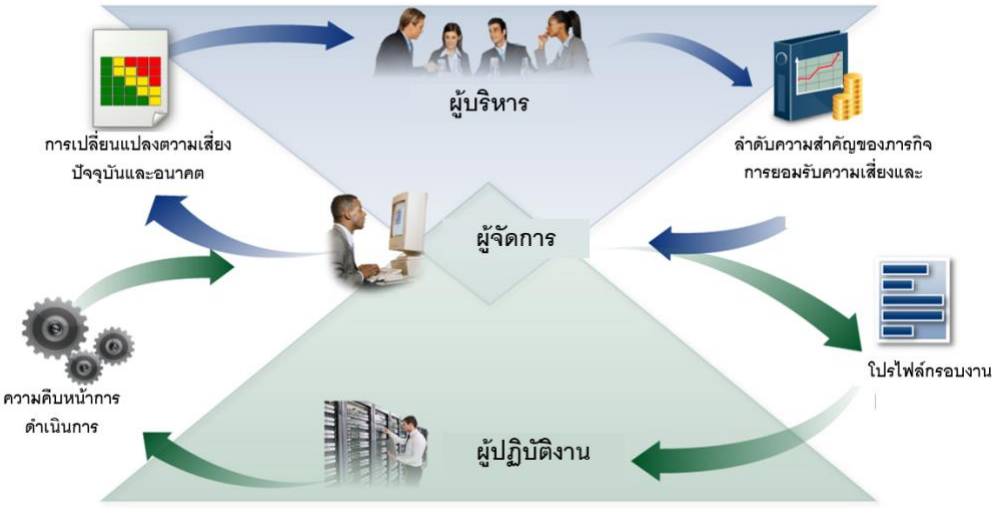
5. การปรับปรุงการสื่อสารและการบูรณาการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

การใช้งาน CSF จะแตกต่างกันไปขึ้นอยู่กับภารกิจและความเสี่ยงเฉพาะขององค์กร ด้วยความเข้าใจถึงความคาดหวังของผู้มีส่วนได้ส่วนเสีย ความเสี่ยงที่ยอมรับได้ (ตามที่ระบุไว้ในฟังก์ชันกำกับดูแล) องค์กรสามารถกำหนดลำดับความสำคัญของกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อตัดสินใจอย่างมีความรู้เกี่ยวกับค่าใช้จ่ายและการดำเนินการด้านการรักษาความปลอดภัยทางไซเบอร์ องค์กรสามารถเลือกจัดการความเสี่ยงได้โดยใช้วิธีใดวิธีหนึ่งหรือหลายวิธี รวมถึงการลดผลกระทบ ถ่ายโอน หลีกเลี่ยง หรือยอมรับความเสี่ยงเชิงลบ และรับรู้ แบ่งปัน เพิ่ม หรือยอมรับความเสี่ยงเชิงบวก ขึ้นอยู่กับผลกระทบและความเป็นไปได้ที่อาจเกิดขึ้น ที่สำคัญ องค์กรสามารถใช้ CSF ได้ทั้งภายในองค์กรเพื่อจัดการความสามารถด้านการรักษาความปลอดภัยทางไซเบอร์และภายนอกองค์กรเพื่อดูแลหรือสื่อสารกับบุคคลที่สาม

หากไม่คำนึงถึงการใช้ CSF องค์กรอาจได้รับประโยชน์จากการใช้ CSF เพื่อเป็นแนวทางเพื่อช่วยให้เข้าใจ ประเมิน กำหนดลำดับความสำคัญและสื่อสารเกี่ยวกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และการดำเนินการที่จะจัดการความเสี่ยงเหล่านั้น สามารถใช้เป้าหมายที่เลือกเพื่อเน้นและดำเนินการตัดสินใจเชิงกลยุทธ์เพื่อปรับปรุงวิธีการรักษาความปลอดภัยทางไซเบอร์และรักษาความต่อเนื่องของฟังก์ชันที่สำคัญต่อภารกิจพร้อมทั้งคำนึงถึงลำดับความสำคัญและแหล่งข้อมูลที่มีอยู่

5.1. การปรับปรุงการสื่อสารเกี่ยวกับการจัดการความเสี่ยง

CSF เป็นพื้นฐานในการพัฒนาการสื่อสารที่เกี่ยวกับสิ่งที่คาดหวัง การวางแผน และแหล่งข้อมูลด้านการรักษาความปลอดภัยทางไซเบอร์ CSF สนับสนุนการสื่อสารแบบสองทิศทาง (ดังที่แสดงในครึ่งบนของ**ภาพที่** *5*) ระหว่างผู้บริหารที่ให้ความสำคัญกับลำดับความสำคัญของงานและทิศทางเชิงกลยุทธ์ขององค์กร และผู้จัดการที่จัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เฉพาะทาง ซึ่งอาจส่งผลต่อการบรรลุเป้าหมายตามลำดับความสำคัญเหล่านั้น CSF ยังสนับสนุนการสื่อสารในลักษณะที่คล้ายกัน (ดังที่แสดงในครึ่งล่างของ**ภาพที่** *5*) ระหว่างผู้จัดการและผู้ปฏิบัติที่นำเทคโนโลยีไปใช้และปฏิบัติงาน ด้านซ้ายของภาพแสดงให้เห็นความสำคัญของผู้ปฏิบัติงานในการแบ่งปันข้อมูลอัปเดต ข้อมูลเชิงลึกและข้อกังวลของตนกับผู้จัดการและผู้บริหาร



ภาพที่ *5* **การใช้** CSF **เพื่อปรับปรุงการสื่อสารการจัดการความเสี่ยง**

การเตรียมการเพื่อสร้างและใช้งานโปรไฟล์องค์กรจะประกอบด้วยการรวบรวมข้อมูลเกี่ยวกับลำดับความสำคัญขององค์กร แหล่งข้อมูล และทิศทางความเสี่ยงจากผู้บริหาร จากนั้น ผู้จัดการจะร่วมมือกับผู้ปฏิบัติงานเพื่อสื่อสารเกี่ยวกับความจำเป็นทางธุรกิจและสร้างโปรไฟล์องค์กรตามข้อมูลความ

เสี่ยง ผู้จัดการและผู้ปฏิบัติงานจะดำเนินการปิดช่องโหว่ใด ๆ ระหว่างโปรไฟล์ปัจจุบันและโปรไฟล์เป้าหมาย และจะให้ข้อมูลสำคัญแก่แผนของระบบ เนื่องจากเป้าหมายจะต้องเกิดขึ้นทั่วทั้งองค์กร รวมถึงผ่านการควบคุมและการติดตามที่ใช้ในระบบ จึงสามารถแบ่งปันเป้าหมายที่อัปเดตได้โดยใช้บันทึกความเสี่ยงและรายงานความคืบหน้า ในส่วนหนึ่งของการประเมินอย่างต่อเนื่อง ผู้จัดการจะได้รับข้อมูลเชิงลึกเพื่อนำไปปรับปรุงและลดอันตรายที่อาจเกิดขึ้นและเพิ่มประโยชน์ที่สามารถทำได้

ฟังก์ชันการกำกับดูแลทำให้เกิดการสื่อสารเกี่ยวกับความเสี่ยงขององค์กรกับ **ผู้บริหาร** ทั้งนี้ การอภิปรายของผู้บริหารว่ากลยุทธ์ โดยเฉพาะอย่างยิ่งความไม่แน่นอนที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์อาจส่งผลต่อการบรรลุวัตถุประสงค์ขององค์กรได้อย่างไร การอภิปรายเรื่องการกำกับดูแลเหล่านี้ทำให้เกิดการสนทนาและข้อตกลงเกี่ยวกับกลยุทธ์การจัดการความเสี่ยง (รวมถึงความเสี่ยงในห่วงโซ่อุปทานการรักษาความปลอดภัยทางไซเบอร์) บทบาท ความรับผิดชอบ และอำนาจ นโยบายและการกำกับดูแล ในขณะที่ผู้บริหารสามารถกำหนดลำดับความสำคัญและวัตถุประสงค์ด้านการรักษาความปลอดภัยทางไซเบอร์ตามความต้องการเหล่านั้น พวกเขาสามารถสื่อสารความคาดหวังเกี่ยวกับการยอมรับความเสี่ยง ความรับผิดชอบและแหล่งข้อมูล ผู้บริหารยังมีความรับผิดชอบในการบูรณาการการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์กับโปรแกรม ERM และโปรแกรมการจัดการความเสี่ยงระดับล่าง (ดูหัวข้อ 5.2) การสื่อสารที่แสดงอยู่ในครึ่งบนของภาพที่ 5 อาจรวมถึงข้อควรพิจารณาสำหรับ ERM และโปรแกรมระดับล่าง และแจ้งให้ผู้จัดการและผู้ปฏิบัติทราบ

เป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ในภาพรวมที่กำหนดโดยผู้บริหารจะได้รับแจ้งและส่งต่อไปยัง **ผู้จัดการ** อนึ่ง สำหรับองค์กรพาณิชย์ สิ่งเหล่านี้อาจนำไปใช้กับสายธุรกิจหรือแผนกปฏิบัติการสำหรับหน่วยงานของรัฐบาล อาจเป็นการพิจารณาในระดับแผนกหรือระดับสาขา เมื่อนำ CSF ไปใช้ ผู้จัดการจะเน้นที่วิธีการบรรลุเป้าหมายความเสี่ยงผ่านทางบริการทั่วไป การควบคุม และความร่วมมือ ตามที่แสดงอยู่ในโปรไฟล์เป้าหมาย และปรับปรุงผ่านการดำเนินการที่ติดตามในแผนปฏิบัติการ (เช่น บันทึกความเสี่ยง รายงานรายละเอียดความเสี่ยง POA&M)

ผู้ปฏิบัติงาน มุ่งเน้นไปที่การนำสถานะเป้าหมายไปปฏิบัติและการวัดการเปลี่ยนแปลงความเสี่ยงด้านปฏิบัติการเพื่อช่วยวางแผน ดำเนินการ และตรวจสอบกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์อย่างเฉพาะเจาะจง ในขณะที่มีการนำการควบคุมมาใช้เพื่อจัดการความเสี่ยงในระดับที่ยอมรับได้ ผู้ปฏิบัติงานจะให้ข้อมูลที่จำเป็นให้กับผู้จัดการและผู้บริหาร (เช่น ตัวชี้วัดประสิทธิภาพที่สำคัญ ตัวชี้วัดความเสี่ยงที่สำคัญ) เพื่อให้พวกเขาเข้าใจถึงวิธีการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ตัดสินใจอย่างมีความรู้และรักษาหรือปรับกลยุทธ์ด้านความเสี่ยงให้เหมาะสม ผู้บริหารยังสามารถรวมข้อมูลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์กับข้อมูลเกี่ยวกับความเสี่ยงประเภทอื่น ๆ ทั่วทั้งองค์กรได้อีกด้วย การอัปเดตความคาดหวังและลำดับความสำคัญจะรวมอยู่ในโปรไฟล์องค์กรที่ได้รับการอัปเดตเมื่อถึงกำหนดเวลา

5.2. การปรับปรุงการบูรณาการกับความเสี่ยงอื่น ๆ โปรแกรมการจัดการ

องค์กรต่าง ๆ เผชิญกับความเสี่ยงด้าน ICT หลายประเภท (เช่น ความเป็นส่วนตัว ห่วงโซ่อุปทาน ปัญญาประดิษฐ์) และอาจใช้กรอบงานและเครื่องมือการจัดการที่เฉพาะกับความเสี่ยงแต่ละประเภท องค์กรบางแห่งบูรณาการ ICT และการจัดการความเสี่ยงอื่น ๆ ทั้งหมดในระดับสูงโดยใช้ ERM ในขณะที่บางแห่งแยกความงานทั้งสองอย่างออกจากกันเพื่อให้แน่ใจว่ามีการให้ความสำคัญอย่างเพียงพอในแต่ละอย่าง

โดยปกติแล้ว องค์กรขนาดเล็กอาจตรวจสอบความเสี่ยงในระดับองค์กร ในขณะที่องค์กรขนาดใหญ่กว่าอาจรักษาความพยายามในการจัดการความเสี่ยงที่แยกจากกันซึ่งรวมเข้าไว้ใน ERM

องค์กรต่าง ๆ สามารถใช้แนวทาง ERM เพื่อสร้างสมดุลให้กับ *พอร์ตโฟลิโอ*การพิจารณาความเสี่ยง รวมถึงการรักษาความปลอดภัยทางไซเบอร์ และตัดสินใจอย่างมีความรู้ ผู้บริหารจะได้รับข้อมูลที่สำคัญเกี่ยวกับกิจกรรมความเสี่ยงในปัจจุบันและที่วางแผนไว้ โดยบูรณาการกลยุทธ์การกำกับดูแลและความเสี่ยงกับเป้าหมายจากการใช้ CSF ก่อนหน้านี้ CSF ช่วยแปลคำศัพท์เฉพาะด้านการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ให้องค์กรต่าง ๆ เพื่อให้เป็นภาษาที่ผู้บริหารจะเข้าใจได้ในเรื่องการจัดการความเสี่ยงทั่วไป

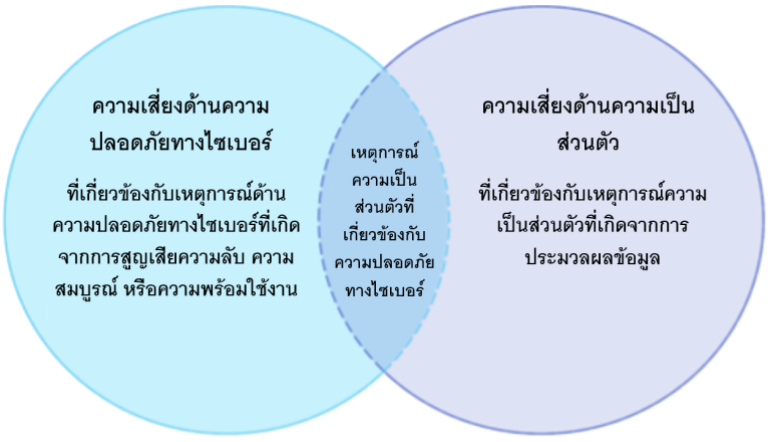
แหล่งข้อมูลของ NIST ที่อธิบายถึงความสัมพันธ์ร่วมกันระหว่างการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และ ERM ได้แก่:

- *NIST Cybersecurity Framework 2.0 – คู่มือเพื่อการเริ่มต้นอย่างรวดเร็วเรื่องการจัดการความเสี่ยงขององค์กร*

- รายงานระหว่างหน่วยงาน NIST (IR) 8286 *การบูรณาการการรักษาการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยงขององค์กร (ERM)*
- IR 8286A, *การระบุและการประเมินความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อการจัดการความเสี่ยงขององค์กร*
- IR 8286B *การจัดลำดับความสำคัญของความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อการจัดการความเสี่ยง*
- IR 8286C *การจัดขั้นตอนดำเนินงานด้านความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อการบริหารความเสี่ยงขององค์กรและการกำกับดูแล*
- IR 8286D *การใช้การวิเคราะห์ผลกระทบทางธุรกิจเพื่อกำหนดลำดับความสำคัญและการตอบสนองต่อความเสี่ยง*
- SP 800-221 *ผลกระทบต่อองค์กรจากความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร: การควบคุมและการจัดการโปรแกรมความเสี่ยงด้าน ICT ในพอร์ตโฟลิโอความเสี่ยงขององค์กร*
- SP 800-221A *เป้าหมายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT): การบูรณาการโปรแกรมการจัดการความเสี่ยงด้าน ICT เข้ากับพอร์ตโฟลิโอความเสี่ยงขององค์กร*

องค์กรอาจพบว่า CSF มีประโยชน์ในการบูรณาการการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์กับโปรแกรมการจัดการความเสี่ยงด้าน ICT แต่ละโปรแกรม เช่น:

- **การจัดการและการประเมินความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์**: CSF สามารถบูรณาการกับโปรแกรมการจัดการและการประเมินความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่จัดตั้งขึ้น เช่น SP 800-37 *กรอบการบริหารความเสี่ยงสำหรับระบบสารสนเทศและองค์กร* และ SP 800-30 *คู่มือสำหรับการประเมินความเสี่ยง* จากกรอบการจัดการความเสี่ยงของ NIST (RMF) สำหรับองค์กรที่ใช้ กรอบการจัดการความเสี่ยงของ NIST รวมทั้งชุดเอกสารที่เผยแพร่ สามารถใช้กรอบการจัดการความเสี่ยงของ NIST เพื่อเสริมแนวทางของกรอบการจัดการความเสี่ยงในการเลือกและกำหนดลำดับความสำคัญในการควบคุมจาก SP 800-53 *การควบคุมความปลอดภัยและความเป็นส่วนตัวสำหรับระบบสารสนเทศและองค์กร*
- **ความเสี่ยงต่อความเป็นส่วนตัว**: แม้ว่าการรักษาความปลอดภัยทางไซเบอร์และความเป็นส่วนตัวจะเป็นงานที่ไม่ขึ้นกับฝ่ายอื่น แต่ในบางสถานการณ์ วัตถุประสงค์ก็ทับซ้อนกับแผนกอื่น ดังที่แสดงใน**ภาพ** *6* -



ภาพ *6* **ความสัมพันธ์ของความเสี่ยงด้านความปลอดภัยไซเบอร์และความเป็นส่วนตัว**

การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์มีความจำเป็นต่อการจัดการความเสี่ยงด้านความเป็นส่วนตัวที่เกี่ยวข้องกับการสูญเสียข้อมูลลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลของบุคคล ตัวอย่างเช่น การละเมิดข้อมูลอาจนำไปสู่การโจรกรรมข้อมูลที่ระบุตัวตนของบุคคล อย่างไรก็ตาม ความเสี่ยงด้านความเป็นส่วนตัวอาจเกิดขึ้นได้จากสิ่งไม่เกี่ยวข้องกับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ด้วยเช่นกัน

องค์กรจะประมวลผลข้อมูลเพื่อบรรลุภารกิจหรือวัตถุประสงค์ทางธุรกิจ ซึ่งบางครั้งอาจทำให้เกิด *เหตุการณ์ที่เกี่ยวกับความเป็นส่วนตัว* ซึ่งบุคคลต่าง ๆ อาจประสบปัญหาอันเป็นผลจากการประมวลผลข้อมูล ปัญหาเหล่านี้สามารถเกิดขึ้นได้หลายแบบ แต่ NIST อธิบายว่าปัญหาเหล่านี้มีตั้งแต่ผลกระทบต่อเกียรติ (เช่น ความอับอายหรือตราบาป) ไปจนถึงอันตรายที่เป็นรูปธรรมมากขึ้น (เช่น การเลือกปฏิบัติ การสูญเสียทางเศรษฐกิจ หรืออันตรายทางกายภาพ) กรอบการทำงานความเป็นส่วนตัวของ NIST และกรอบการทำงานการรักษาความปลอดภัยทางไซเบอร์สามารถใช้ร่วมกันเพื่อจัดการกับประเด็นต่าง ๆ ของความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และความเป็นส่วนตัว นอกจากนี้ วิธีการประเมินความเสี่ยงด้านความเป็นส่วนตัว (PRAM) ของ NIST ยังมีรายการตัวอย่างปัญหาเพื่อใช้ในการประเมินความเสี่ยงด้านความเป็นส่วนตัว

- **ความเสี่ยงในห่วงโซ่อุปทาน**: องค์กรสามารถใช้ CSF เพื่อส่งเสริมการกำกับดูแลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และการสื่อสารกับผู้มีส่วนได้ส่วนเสียในห่วงโซ่อุปทาน เทคโนโลยีทุกประเภทอาศัยระบบนิเวศห่วงโซ่อุปทานที่ซับซ้อน กระจายไปทั่วโลกกว้างขวางและเชื่อมโยงกัน โดยมีเส้นทางที่หลากหลายทางภูมิศาสตร์ และการเอาท์ซอร์สในหลายระดับ ระบบนิเวศนี้ประกอบด้วยหน่วยงานภาครัฐและเอกชน (เช่น ผู้ซื้อ ผู้จัดหา ผู้พัฒนา ผู้รวมระบบ ผู้ให้บริการระบบภายนอก และผู้ให้บริการที่เกี่ยวข้องกับเทคโนโลยีอื่น ๆ) ที่โต้ตอบกันในการวิจัย พัฒนา ออกแบบ ผลิต จัดหา จัดส่ง รวม ดำเนินการ บำรุงรักษา กำจัดและใช้หรือจัดการผลิตภัณฑ์และบริการด้านเทคโนโลยีในลักษณะอื่น ๆ การปฏิสัมพันธ์เหล่านี้เกิดขึ้นและได้รับอิทธิพลจากเทคโนโลยี กฎหมาย นโยบาย ขั้นตอนและการนำไปปฏิบัติ

  เนื่องจากความสัมพันธ์ที่ซับซ้อนและเชื่อมโยงกันในระบบนิเวศนี้ การจัดการความเสี่ยงในห่วงโซ่อุปทาน (SCRM) จึงมีความสำคัญต่อองค์กร Cybersecurity SCRM (C-SCRM) เป็นกระบวนการเชิงระบบสำหรับจัดการกับความเสี่ยงต่อการรักษาความปลอดภัยทางไซเบอร์ตลอดทั้งห่วงโซ่อุปทาน และเป็นการพัฒนากลยุทธ์ นโยบาย กระบวนการ และขั้นตอนการตอบสนองที่เหมาะสม หมวดหมู่ย่อยภายในหมวดหมู่ C-SCRM ของ CSF [GV.SC] ให้ความเชื่อมโยงระหว่างเป้าหมายที่เน้นเฉพาะด้านการรักษาความปลอดภัยทางไซเบอร์และเป้าหมายที่เน้น

  ที่ C-SCRM SP 800-161r1 (แก้ไขครั้งที่ 1) *แนวทางการจัดการความเสี่ยงในห่วงโซ่อุปทานด้านการรักษาความปลอดภัยทางไซเบอร์สำหรับระบบและองค์กร* ซึ่งให้ข้อมูลเชิงลึกเกี่ยวกับ C-SCRM

- **ความเสี่ยงจากเทคโนโลยีที่เกิดใหม่**: เมื่อมีเทคโนโลยีใหม่และการประยุกต์ใช้เทคโนโลยีใหม่ๆ เกิดขึ้น ความเสี่ยงใหม่ ๆ ก็จะชัดเจนขึ้น ตัวอย่างร่วมสมัยคือปัญญาประดิษฐ์ (AI) ซึ่งมีความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และความเป็นส่วนตัว รวมถึงความเสี่ยงประเภทอื่น ๆ อีกมากมาย กรอบการจัดการความเสี่ยงด้านปัญญาประดิษฐ์ของ NIST (AI RMF) ได้รับการพัฒนาเพื่อช่วยจัดการกับความเสี่ยงเหล่านี้ การจัดการความเสี่ยงด้าน AI ร่วมกับความเสี่ยงด้านองค์กรอื่นๆ (เช่น ความเสี่ยงทางการเงิน การรักษาความปลอดภัยทางไซเบอร์ ชื่อเสียง และความเป็นส่วนตัว) จะให้ผลลัพธ์ที่เกิดจากการบูรณาการมากขึ้นและประสิทธิภาพขององค์กร สามารถนำข้อควรพิจารณาและแนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และความเป็นส่วนตัวไปใช้ได้กับการออกแบบ การพัฒนา การปรับใช้ การประเมิน และการใช้งานระบบ AI AI RMF Core ใช้ฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยเพื่ออธิบายเป้าหมายของ AI และช่วยจัดการความเสี่ยงที่เกี่ยวข้องกับ AI ได้

ภาคผนวก A แกนหลัก CSF

ภาคผนวกนี้จะอธิบายเกี่ยวกับฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยของแกนหลัก CSF โดยตารางที่ *1* แสดงรายการชื่อฟังก์ชันหลักและหมวดหมู่ของ CSF 2.0 และตัวระบุตัวอักษรที่ไม่ซ้ำกัน ชื่อฟังก์ชันแต่ละชื่อในตารางจะเชื่อมโยงกับส่วนของฟังก์ชันนั้นในภาคผนวก ลำดับของฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อยของแกนหลักไม่ได้เรียงตามตัวอักษร แต่มีวัตถุประสงค์ให้ผู้ที่มีหน้าที่ในการปฏิบัติงานด้านการบริหารความเสี่ยงภายในองค์กรส่วนใหญ่เข้าใจตรงกัน การกำหนดหมายเลขหมวดหมู่ย่อยไม่ได้ตั้งใจให้เรียงลำดับตามลำดับ ช่องว่างในการกำหนดหมายเลขบ่งชี้ว่าหมวดหมู่ย่อย CSF 1.1 ได้ถูกย้ายไปยัง CSF 2.0

ตารางที่ 1 ชื่อและตัวระบุหมวดหมู่และฟังก์ชันหลักของ CSF 2.0

การทำงาน	หมวดหมู่	ตัวระบุหมวดหมู่
การกำกับดูแล (GV)	บริบทขององค์กร	GV.OC
	กลยุทธ์การบริหารความเสี่ยง	GV.RM
	บทบาท ความรับผิดชอบและอำนาจหน้าที่	GV.RR
	นโยบาย	GV.PO
	การกำกับดูแล	GV.OV
	การจัดการความเสี่ยงห่วงโซ่อุปทานการรักษาความปลอดภัยทางไซเบอร์	GV.SC
การระบุ (ID)	การจัดการสินทรัพย์	ID.AM
	การประเมินความเสี่ยง	ID.RA
	การปรับปรุง	ID.IM
การป้องกัน (PR)	การจัดการข้อมูลประจำตัว การตรวจสอบสิทธิ์และการควบคุมการเข้าถึงข้อมูล	PR.AA
	การตระหนักรู้และการฝึกอบรม	PR.AT
	ความปลอดภัยของข้อมูล	PR.DS
	ความปลอดภัยของแพลตฟอร์ม	PR.PS
	ความยืดหยุ่นของโครงสร้างพื้นฐานด้านเทคโนโลยี	PR.IR
การตรวจจับ (DE)	การตรวจสอบอย่างต่อเนื่อง	DE.CM
	การวิเคราะห์เหตุการณ์ไม่พึงประสงค์	DE.AE
การตอบสนอง (RS)	การจัดการเหตุการณ์	RS.MA
	การวิเคราะห์เหตุการณ์	RS.AN
	การรายงานการตอบสนองต่อเหตุการณ์และการสื่อสาร	RS.CO
	การบรรเทาความรุนแรงของเหตุการณ์	RS.MI
การกู้คืน (RC)	การดำเนินการตามแผนกู้สถานการณ์	RC.RP
	การสื่อสารเพื่อการกู้คืนเหตุการณ์	RC.CO

เอกสารอ้างอิงข้อมูลแกนหลัก CSF และตัวอย่างการนำไปใช้งานมีอยู่ใน เว็บไซต์ CSF 2.0 และผ่านทาง เครื่องมืออ้างอิง CSF 2.0 ซึ่งช่วยให้ผู้ใช้สามารถสำรวจและส่งออกในรูปแบบที่มนุษย์และคอมพิวเตอร์สามารถอ่านได้ CSF 2.0 Core ยังมีให้ใช้งานใน รูปแบบเก่าซึ่งคล้ายกับ CSF 1.1

การกำกับ (GV): มีการจัดทำ สื่อสาร และตรวจสอบกลยุทธ์ ความคาดหวังและนโยบายการจัดการความเสี่ยงทางไซเบอร์ขององค์กร

- **บริบทขององค์กร** (GV.OC): สถานการณ์ต่างๆ เช่น ภารกิจ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย ความสัมพันธ์ และข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญา ที่เกี่ยวข้องกับการตัดสินใจจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรได้รับการเข้าใจ
  - GV.OC-01: ภารกิจขององค์กรเป็นที่เข้าใจและแจ้งให้ทราบถึงการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
  - GV.OC-02: เข้าใจผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก และเข้าใจและพิจารณาความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียเกี่ยวกับการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
  - GV.OC-03: ข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ รวมถึงภาระผูกพันด้านความเป็นส่วนตัวและเสรีภาพพลเมือง เป็นที่เข้าใจและได้รับการจัดการ
  - GV.OC-04: วัตถุประสงค์ ความสามารถ และบริการที่สำคัญที่ผู้มีส่วนได้ส่วนเสียภายนอกพึ่งพาหรือคาดหวังจากองค์กรได้รับการสื่อสารกันจนเป็นที่เข้าใจ
  - GV.OC-05: เป้าหมาย ความสามารถ และบริการที่องค์กรพึ่งพา ได้รับการสื่อสารกันจนเป็นที่เข้าใจ

- **กลยุทธ์การบริหารความเสี่ยง** (GV.RM): ลำดับความสำคัญ ข้อจำกัด การยอมรับความเสี่ยง ตลอดจนข้อสมมติฐานขององค์กรได้รับการจัดทำ สื่อสาร และใช้เพื่อสนับสนุนการตัดสินใจเกี่ยวกับความเสี่ยงด้านปฏิบัติการ
  - GV.RM-01: วัตถุประสงค์การจัดการความเสี่ยงได้รับการกำหนดและตกลงกันโดยผู้มีส่วนได้ส่วนเสียในองค์กร
  - GV.RM-02: การยอมรับความเสี่ยงได้รับการจัดทำเป็นเอกสาร สื่อสารและเก็บรักษา
  - GV.RM-03: กิจกรรมและเป้าหมายของการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์รวมอยู่ในกระบวนการจัดการความเสี่ยงขององค์กร
  - GV.RM-04: กำหนดและสื่อสารทิศทางเชิงกลยุทธ์ที่ระบุทางเลือกในการตอบสนองความเสี่ยงที่เหมาะสม
  - GV.RM-05: มีการจัดทำช่องทางการสื่อสารทั่วทั้งองค์กรเพื่อป้องกันความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ รวมถึงความเสี่ยงจากซัพพลายเออร์และบุคคลภายนอกอื่น ๆ
  - GV.RM-06: มีการจัดทำและสื่อสารวิธีมาตรฐานสำหรับการคำนวณ การบันทึก การจัดหมวดหมู่ และการจัดลำดับความสำคัญของความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
  - GV.RM-07: โอกาสเชิงกลยุทธ์ (เช่น ความเสี่ยงเชิงบวก) ถูกกำหนดลักษณะและรวมอยู่ในข้อหารือเกี่ยวกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร

- **บทบาท ความรับผิดชอบ และอำนาจหน้าที่** (GV.RR): บทบาท ความรับผิดชอบ และอำนาจด้านการรักษาความปลอดภัยทางไซเบอร์ในการส่งเสริมความรับผิดชอบ การประเมินผลการปฏิบัติงาน และการปรับปรุงอย่างต่อเนื่องได้รับการกำหนดและสื่อสาร
  - GV.RR-01: ผู้นำองค์กรมีความรับผิดชอบต่อความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ และส่งเสริมวัฒนธรรมที่ตระหนักถึงความเสี่ยง มีจริยธรรม และปรับปรุงอย่างต่อเนื่อง
  - GV.RR-02: บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ได้รับการกำหนด สื่อสาร ทำความเข้าใจ และบังคับใช้
  - GV.RR-03: จัดสรรทรัพยากรให้เพียงพอตามกลยุทธ์ บทบาท ความรับผิดชอบ และนโยบายด้านความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

- GV.RR-04: การรักษาความปลอดภัยทางไซเบอร์รวมอยู่ในแนวทางปฏิบัติด้านทรัพยากรบุคคล

- **นโยบาย** (GV.PO): มีการกำหนด สื่อสาร และบังคับใช้นโยบายการรักษาความปลอดภัยทางไซเบอร์ขององค์กร
  - GV.PO-01: นโยบายการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ได้รับการจัดทำขึ้นตามบริบทขององค์กร กลยุทธ์ด้านการรักษาความปลอดภัยทางไซเบอร์และการจัดลำดับความสำคัญของงานได้รับการสื่อสารและบังคับใช้
  - GV.PO-02: นโยบายการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์จะได้รับการทบทวน อัปเดต สื่อสาร และบังคับใช้เพื่อสะท้อนถึงการเปลี่ยนแปลงในข้อกำหนด ภัยคุกคาม เทคโนโลยีและภารกิจขององค์กร

- **การกำกับดูแล** (GV.OV): เป้าหมายของกิจกรรมและประสิทธิภาพการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ทั่วทั้งองค์กรจะถูกใช้เพื่อสื่อสาร ตรวจสอบและปรับปรุงกลยุทธ์การจัดการความเสี่ยง
  - GV.OV-01: เป้าหมายของกลยุทธ์การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์จะได้รับการทบทวนเพื่อแจ้งและปรับกลยุทธ์และทิศทาง
  - GV.OV-02: มีการทบทวนและปรับเปลี่ยนกลยุทธ์การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อให้ครอบคลุมข้อกำหนดและความเสี่ยงขององค์กร
  - GV.OV-03: มีการประเมินและตรวจสอบประสิทธิภาพการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรเพื่อปรับเปลี่ยนตามความจำเป็น

- **การจัดการความเสี่ยงในห่วงโซ่อุปทานการรักษาความปลอดภัยทางไซเบอร์** (GV.SC): ผู้มีส่วนได้ส่วนเสียขององค์กรระบุ จัดทำ จัดการ ติดตาม และปรับปรุงกระบวนการจัดการความเสี่ยงในห่วงโซ่อุปทานทางไซเบอร์
  - GV.SC-01: ผู้มีส่วนได้ส่วนเสียในองค์กรจัดทำและตกลงตามโปรแกรม กลยุทธ์ วัตถุประสงค์ นโยบาย และกระบวนการในการจัดการความเสี่ยงในห่วงโซ่อุปทานด้านการรักษาความปลอดภัยทางไซเบอร์
  - GV.SC-02: บทบาทและความรับผิดชอบด้านการรักษาความปลอดภัยทางไซเบอร์สำหรับซัพพลายเออร์ ลูกค้า และพันธมิตรได้รับการกำหนด สื่อสาร และประสานงานภายในและภายนอกองค์กร
  - GV.SC-03: การจัดการความเสี่ยงในห่วงโซ่อุปทานของการรักษาความปลอดภัยทางไซเบอร์ได้รับการบูรณาการเข้ากับกระบวนการจัดการความเสี่ยงทางไซเบอร์และองค์กร รวมทั้งกระบวนการการประเมินความเสี่ยงและการพัฒนา
  - GV.SC-04: **รู้จัก**ซัพพลายเออร์และมีการจัดลำดับตามความสำคัญ
  - GV.SC-05: ข้อกำหนดในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในห่วงโซ่อุปทานได้รับการกำหนด จัดลำดับความสำคัญ และบูรณาการเข้าในสัญญาและข้อตกลงประเภทอื่นกับซัพพลายเออร์และบุคคลที่สามที่เกี่ยวข้อง
  - GV.SC-06: ดำเนินการวางแผนและดำเนินการตามความรอบคอบเพื่อลดความเสี่ยงก่อนที่จะเข้าสู่ความสัมพันธ์อย่างเป็นทางการกับซัพพลายเออร์หรือบุคคลที่สาม
  - GV.SC-07: ความเสี่ยงที่เกิดจากซัพพลายเออร์ ผลิตภัณฑ์และบริการของพวกเขา และบุคคลภายนอกอื่นๆ จะได้รับการทำความเข้าใจ บันทึก จัดลำดับความสำคัญ ประเมิน ตอบสนองและตรวจสอบตลอดระยะเวลาของความสัมพันธ์
  - GV.SC-08: ซัพพลายเออร์ที่เกี่ยวข้องและบุคคลภายนอก จะรวมอยู่ในกิจกรรมการวางแผนเหตุการณ์ การตอบสนองและการกู้คืน
  - GV.SC-09: แนวทางปฏิบัติด้านความปลอดภัยของห่วงโซ่อุปทานถูกบูรณาการเข้าไว้ในโปรแกรมการรักษาความปลอดภัยทางไซเบอร์และการจัดการความเสี่ยงขององค์กร และมีการตรวจสอบประสิทธิภาพการทำงานตลอดทั้งวงจรชีวิตของผลิตภัณฑ์เทคโนโลยีและการให้บริการ

- GV.SC-10: แผนการจัดการความเสี่ยงในห่วงโซ่อุปทานของการรักษาความปลอดภัยทางไซเบอร์ประกอบด้วยข้อกำหนดสำหรับกิจกรรมที่เกิดขึ้นหลังจากการสรุปข้อตกลงหุ้นส่วนหรือบริการ

ระบุ (ID): เข้าใจความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันขององค์กร

- **การจัดการสินทรัพย์** (ID.AM) : สินทรัพย์ (เช่น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ ระบบ สิ่งอำนวยความสะดวก บริการ บุคลากร) ที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจ ได้รับการระบุและจัดการโดยสอดคล้องกับความสำคัญที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กรและกลยุทธ์ด้านความเสี่ยงขององค์กร
  - ID.AM-01: มีการบำรุงรักษาสินค้าคงคลังของฮาร์ดแวร์ที่องค์กรจัดการ
  - ID.AM-02: มีการบำรุงรักษาสินค้าคงคลังของซอฟต์แวร์ บริการและระบบที่จัดการโดยองค์กร
  - ID.AM-03: มีการบำรุงรักษาเครือข่ายการสื่อสารที่ได้รับอนุญาตขององค์กรและการไหลของข้อมูลในเครือข่ายภายในและภายนอก
  - ID.AM-04: มีการบำรุงรักษาสินค้าคงคลังของบริการจากซัพพลายเออร์
  - ID.AM-05: สินทรัพย์จะถูกจัดลำดับความสำคัญตามการจำแนกประเภท ความสำคัญ ทรัพยากรและผลกระทบต่อภารกิจ
  - ID.AM-07: มีการบำรุงรักษาข้อมูลคงคลังและข้อมูลเมตาที่สอดคล้องกันสำหรับประเภทข้อมูลที่กำหนด
  - ID.AM-08: ระบบ ฮาร์ดแวร์ ซอฟต์แวร์ บริการและข้อมูลได้รับการจัดการตลอดอายุการใช้งาน
- **การประเมินความเสี่ยง** (ID.RA): องค์กรเข้าใจถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ต่อองค์กร สินทรัพย์ และบุคคล
  - ID.RA-01: ช่องโหว่ในทรัพย์สินได้รับการระบุ ตรวจสอบและบันทึกไว้
  - ID.RA-02: ข้อมูลภัยคุกคามทางไซเบอร์ได้รับจากกระดานข่าวและแหล่งที่มาของการแชร์ข้อมูล
  - ID.RA-03: ระบุและบันทึกภัยคุกคามภายในและภายนอกต่อองค์กร
  - ID.RA-04: ระบุและบันทึกผลกระทบที่อาจเกิดขึ้นและแนวโน้มของภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่
  - ID.RA-05: ภัยคุกคาม จุดอ่อน โอกาส และผลกระทบใช้เพื่อทำความเข้าใจความเสี่ยงที่จะเกิดขึ้นและแจ้งการกำหนดลำดับความสำคัญในการตอบสนองต่อความเสี่ยง
  - ID.RA-06: เลือกการตอบสนองความเสี่ยง กำหนดลำดับความสำคัญ วางแผน ติดตาม และสื่อสาร
  - ID.RA-07: การเปลี่ยนแปลงและข้อยกเว้นได้รับการจัดการ ประเมินผลกระทบจากความเสี่ยง บันทึก และติดตาม
  - ID.RA-08: มีการจัดตั้งกระบวนการสำหรับการรับ วิเคราะห์ และตอบสนองต่อการเปิดเผยช่องโหว่
  - ID.RA-09: ความถูกต้องและความสมบูรณ์ของฮาร์ดแวร์และซอฟต์แวร์จะได้รับการประเมินก่อนการซื้อและใช้งาน
  - ID.RA-10:ประเมินซัพพลายเออร์ที่สำคัญก่อนการเข้าซื้อกิจการ
- **การปรับปรุง** (ID.IM): มีการระบุการปรับปรุงกระบวนการ ขั้นตอน และกิจกรรมการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรในทุกฟังก์ชันของ CSF
  - ID.IM-01: มีการระบุเรื่องที่ต้องปรับปรุงจากการประเมิน

- ID.IM-02: มีการระบุการปรับปรุงจากการทดสอบและการฝึกซ้อมด้านความปลอดภัย รวมถึงการดำเนินการร่วมกับซัพพลายเออร์และบุคคลที่สามที่เกี่ยวข้อง
- ID.IM-03: พบการปรับปรุงจากการดำเนินการตามกระบวนการปฏิบัติงาน ขั้นตอนและกิจกรรม
- ID.IM-04: แผนการตอบสนองต่อเหตุการณ์และอื่น ๆ แผนการรักษาความปลอดภัยทางไซเบอร์ที่มีผลกระทบต่อการปฏิบัติงานได้รับการจัดทำ สื่อสาร บำรุงรักษาและปรับปรุง

การป้องกัน (PR): ใช้มาตรการป้องกันเพื่อจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร

- **การจัดการข้อมูลประจำตัว การรับรองความถูกต้อง และการควบคุมการเข้าถึง** (PR.AA): การเข้าถึงสินทรัพย์ทางกายภาพและทางคอมพิวเตอร์ได้รับการจำกัดเฉพาะผู้ใช้ที่ได้รับอนุญาต บริการ และฮาร์ดแวร์ และจัดการตามความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาตที่ได้ประเมินไว้
  - PR.AA-01: ข้อมูลที่ระบุตัวตนและข้อมูลเพื่อการเข้าใช้งานสำหรับผู้ใช้ที่ได้รับอนุญาต บริการ และฮาร์ดแวร์จะได้รับการจัดการโดยองค์กร
  - PR.AA-02: ข้อมูลประจำตัวได้รับการตรวจสอบและผูกเข้ากับข้อมูลประจำตัวตามบริบทของการปฏิสัมพันธ์
  - PR.AA-03: ผู้ใช้ บริการต่าง ๆ และฮาร์ดแวร์ได้รับการตรวจสอบ
  - PR.AA-04: การยืนยันตัวตนได้รับการจัดทำขึ้น มีการปกป้องและตรวจสอบความปลอดภัย
  - PR.AA-05: สิทธิ์การเข้าถึง สิทธิต่าง ๆ และการอนุญาตได้รับการกำหนดไว้ในนโยบาย จัดการ บังคับใช้ และตรวจสอบ และระบุถึงหลักการของสิทธิ์ขั้นต่ำและการแบ่งแยกหน้าที่
  - PR.AA-06: การเข้าถึงทรัพย์สินทางกายภาพได้รับการจัดการ ตรวจสอบและบังคับใช้ตามระดับความเสี่ยง
- **ความตระหนักรู้และการฝึกอบรม** (PR.AT): บุคลากรขององค์กรได้รับการสร้างความตระหนักรู้และการฝึกอบรมด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อให้สามารถปฏิบัติหน้าที่ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ได้
  - PR.AT-01: บุคลากรได้รับการสร้างความตระหนักรู้และการฝึกอบรมเพื่อให้มีความรู้และทักษะในการปฏิบัติงานทั่วไปโดยคำนึงถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
  - PR.AT-02: บุคคลที่มีบทบาทเฉพาะทางจะได้รับการสร้างความตระหนักรู้และการฝึกอบรมเพื่อให้พวกเขามีความรู้และทักษะในการปฏิบัติงานที่เกี่ยวข้องโดยคำนึงถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
- **ความปลอดภัยของข้อมูล** (PR.DS): ข้อมูลได้รับการจัดการสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล
  - PR.DS-01: การรักษาความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูลที่เหลือได้รับการคุ้มครอง
  - PR.DS-02: ความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูลระหว่างการขนส่งได้รับการปกป้อง
  - PR.DS-10: การรักษาความลับ ความสมบูรณ์และความพร้อมใช้ของข้อมูลที่ใช้งานได้รับการปกป้อง
  - PR.DS-11: การสำรองข้อมูลจะถูกจัดทำขึ้น และได้รับการป้องกัน บำรุงรักษาและทดสอบ

- **ความปลอดภัยของแพลตฟอร์ม** (PR.PS): ฮาร์ดแวร์ ซอฟต์แวร์ (เช่น เฟิร์มแวร์ ระบบปฏิบัติการ แอปพลิเคชัน) และบริการของแพลตฟอร์มทางกายภาพและเสมือนจริงได้รับการจัดการอย่างสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งาน
  - PR.PS-01: กำหนดและนำแนวทางปฏิบัติในการจัดการการกำหนดค่าไปใช้
  - PR.PS-02: ซอฟต์แวร์ได้รับการบำรุงรักษา เปลี่ยนใหม่และลบออกตามความเสี่ยง
  - PR.PS-03: ฮาร์ดแวร์ได้รับการบำรุงรักษา เปลี่ยนและลบออกตามความเสี่ยง
  - PR.PS-04: บันทึกข้อมูลจะถูกสร้างขึ้นและเปิดให้มีการตรวจสอบอย่างต่อเนื่อง
  - PR.PS-05: การติดตั้งและการทำงานของซอฟต์แวร์ที่ไม่ได้รับอนุญาตจะไม่สามารถทำได้
  - PR.PS-06: แนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัยได้รับการบูรณาการ และมีการตรวจสอบประสิทธิภาพการทำงานตลอดทั้งวงจรการพัฒนาซอฟต์แวร์
- **ความยืดหยุ่นของโครงสร้างพื้นฐานด้านเทคโนโลยี** (PR.IR): สถาปัตยกรรมความปลอดภัยได้รับการจัดการโดยใช้กลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับของทรัพย์สิน ความสมบูรณ์ และความพร้อมใช้งานและความยืดหยุ่นขององค์กร
  - PR.IR-01: เครือข่ายและสภาพแวดล้อมได้รับการปกป้องจากการเข้าถึงและการใช้งานคอมพิวเตอร์ที่ไม่ได้รับอนุญาต
  - PR.IR-02: ทรัพย์สินทางเทคโนโลยีขององค์กรได้รับการปกป้องจากภัยคุกคามด้านสิ่งแวดล้อม
  - PR.IR-03: มีการนำกลไกมาใช้เพื่อบรรลุข้อกำหนดด้านความยืดหยุ่นในสถานการณ์ปกติและสถานการณ์ที่ไม่เอื้ออำนวย
  - PR.IR-04: กำลังการผลิตทรัพยากรที่เพียงพอเพื่อให้แน่ใจว่ามีการรักษาความพร้อมใช้งาน

การตรวจจับ (DE): ค้นหาและวิเคราะห์การโจมตีทางไซเบอร์และช่องโหว่ที่อาจเกิดขึ้น

- **การติดตามอย่างต่อเนื่อง** (DE.CM): มีการตรวจสอบสินทรัพย์เพื่อค้นหาสิ่งผิดปกติ ตัวบ่งชี้ช่องโหว่ และเหตุการณ์ไม่พึงประสงค์อื่น ๆ ที่อาจเกิดขึ้น
  - DE.CM-01: มีการตรวจสอบเครือข่ายและบริการเครือข่ายเพื่อค้นหาเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น
  - DE.CM-02: มีการตรวจสอบสภาพแวดล้อมทางกายภาพเพื่อค้นหาเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น
  - DE.CM-03: มีการติดตามกิจกรรมของบุคลากรและการใช้เทคโนโลยีเพื่อค้นหาเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น
  - DE.CM-06: มีการติดตามกิจกรรมและบริการของผู้ให้บริการภายนอกเพื่อค้นหาเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น
  - DE.CM-09: มีการตรวจสอบฮาร์ดแวร์และซอฟต์แวร์คอมพิวเตอร์ สภาพการรันไทม์และข้อมูลเพื่อค้นหาเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น
- **การวิเคราะห์เหตุการณ์ไม่พึงประสงค์** (DE.AE): ความผิดปกติ ตัวบ่งชี้ช่องโหว่ และเหตุการณ์ไม่พึงประสงค์อื่นๆ ที่อาจเกิดขึ้น จะถูกวิเคราะห์เพื่อระบุลักษณะของเหตุการณ์และตรวจจับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์
  - DE.AE-02: เหตุการณ์ที่อาจเป็นเหตุการณ์ไม่พึงประสงค์จะถูกวิเคราะห์เพื่อให้เข้าใจกิจกรรมที่เกี่ยวข้องได้ดียิ่งขึ้น
  - DE.AE-03: ข้อมูลมีการเชื่อมโยงจากหลายแหล่งข้อมูล

- DE.AE-04: เข้าใจถึงผลกระทบที่คาดว่าจะเกิดขึ้นและขอบเขตของเหตุการณ์ไม่พึงประสงค์
- DE.AE-06: ข้อมูลเกี่ยวกับเหตุการณ์ไม่พึงประสงค์จะถูกจัดเตรียมไว้ให้กับเจ้าหน้าที่และเครื่องมือที่ได้รับอนุญาต
- DE.AE-07: ข้อมูลข่าวกรองด้านภัยคุกคามทางไซเบอร์และข้อมูลบริบทอื่น ๆ จะถูกรวมเข้าไว้ในการวิเคราะห์
- DE.AE-08: มีการแจ้งเมื่อเหตุการณ์ไม่พึงประสงค์ตรงตามเกณฑ์เหตุการณ์ที่กำหนดไว้

การตอบสนอง (RS): ดำเนินการเกี่ยวกับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่ตรวจพบ

- **การจัดการเหตุการณ์** (RS.MA): การจัดการตอบสนองต่อเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่ตรวจพบ
  - RS.MA-01: แผนการตอบสนองต่อเหตุการณ์จะถูกดำเนินการร่วมกับบุคคลที่สามที่เกี่ยวข้องทันทีที่มีการประกาศเหตุการณ์
  - RS.MA-02: รายงานเหตุการณ์ได้รับการคัดแยกและตรวจสอบ
  - RS.MA-03: เหตุการณ์จะถูกจัดหมวดหมู่และจัดลำดับความสำคัญ
  - RS.MA-04: เหตุการณ์จะถูกยกระดับหรือยกระดับตามความจำเป็น
  - RS.MA-05: เกณฑ์การเริ่มดำเนินการกู้สถานการณ์ถูกนำมาใช้
- **การวิเคราะห์เหตุการณ์** (RS.AN): ดำเนินการสอบสวนเพื่อให้มั่นใจว่าตอบสนองและช่วยเหลืองานนิติวิทยาศาสตร์และการกู้คืนได้อย่างมีประสิทธิผล
  - RS.AN-03: การวิเคราะห์จะดำเนินการเพื่อระบุสิ่งที่เกิดขึ้นในระหว่างเหตุการณ์และสาเหตุของเหตุการณ์
  - RS.AN-06: การดำเนินการที่ดำเนินการระหว่างการสอบสวนจะถูกบันทึกไว้ และความสมบูรณ์และที่มาของบันทึกจะถูกเก็บรักษาไว้
  - RS.AN-07: ข้อมูลเหตุการณ์และข้อมูลเมตาจะถูกเก็บรวบรวม และความสมบูรณ์และที่มาของข้อมูลเหล่านั้นจะถูกเก็บรักษาไว้
  - RS.AN-08: ขนาดของเหตุการณ์ได้รับการประมาณการณ์และตรวจสอบความถูกต้อง
- **การรายงานและการสื่อสารการตอบสนองต่อเหตุการณ์** (RS.CO): กิจกรรมการตอบสนองได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียภายในและภายนอกตามที่กฎหมาย ระเบียบหรือแนวนโยบายกำหนด
  - RS.CO-02: ผู้มีส่วนได้ส่วนเสียภายในและภายนอกได้รับแจ้งเหตุการณ์ที่เกิดขึ้น
  - RS.CO-03: ข้อมูลจะถูกแบ่งปันกับผู้มีส่วนได้ส่วนเสียภายในและภายนอกตามที่ได้รับการกำหนด
- **การบรรเทาความรุนแรงของเหตุการณ์** (RS.MI): กิจกรรมต่าง ๆ ดำเนินการเพื่อป้องกันการขยายตัวของเหตุการณ์และบรรเทาผลกระทบ
  - RS.MI-01: เหตุการณ์ถูกจำกัดความรุนแรงไว้
  - RS.MI-02: เหตุการณ์ถูกกำจัด

การกู้คืน (RC): สินทรัพย์และการดำเนินงานที่ได้รับผลกระทบจากเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ได้รับการกู้คืน

- **การดำเนินการตามแผนการกู้สถานการณ์** (RC.RP): กิจกรรมการกู้คืนจะดำเนินการเพื่อให้แน่ใจว่าระบบและบริการที่ได้รับผลกระทบจากเหตุการณ์ทางไซเบอร์สามารถใช้งานได้

- RC.RP-01: ส่วนการกู้คืนของแผนตอบสนองต่อเหตุการณ์จะดำเนินการเมื่อเริ่มต้นจากกระบวนการตอบสนองต่อเหตุการณ์
- RC.RP-02: เลือกการดำเนินการฟื้นฟู กำหนดขอบเขต กำหนดลำดับความสำคัญและดำเนินการ
- RC.RP-03: ตรวจสอบความสมบูรณ์ของข้อมูลสำรองและแหล่งข้อมูลการคืนค่าอื่น ๆ ก่อนนำไปใช้เพื่อการคืนสภาพเดิม
- RC.RP-04: ภารกิจที่สำคัญและการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ถือเป็นบรรทัดฐานการปฏิบัติการหลังเกิดเหตุการณ์
- RC.RP-05: การตรวจสอบความสมบูรณ์ของสินทรัพย์ที่กู้คืน ระบบและบริการได้รับการกู้คืนและยืนยันสถานะการดำเนินงานปกติ
- RC.RP-06: ประกาศสิ้นสุดการกู้สถานการณ์ตามเกณฑ์ที่กำหนด และจัดทำเอกสารที่เกี่ยวข้องกับเหตุการณ์ให้เสร็จสมบูรณ์

- **การสื่อสารการกู้สถานการณ์** (RC.CO): กิจกรรมการกู้สถานการณ์ได้รับการประสานงานกับฝ่ายภายในและภายนอก
  - RC.CO-03: กิจกรรมการฟื้นฟูและความคืบหน้าในการฟื้นฟูความสามารถในการปฏิบัติการจะได้รับการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียภายในและภายนอกที่ได้รับการกำหนด
  - RC.CO-04: มีการอัปเดตต่อสาธารณะเกี่ยวกับการกู้สถานการณ์โดยใช้วิธีการและการส่งข้อความที่ได้รับอนุมัติ

ภาคผนวก B. ระดับ CSF

ตาราง2 มีภาพประกอบของ CSF Tiers ที่ได้ระบุไว้ในหัวข้อที่ *3* ระดับต่าง ๆ แสดงถึงความเข้มงวดของแนวทางการกำกับดูแลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร (กำกับดูแล) และแนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ (ระบุ, ป้องกัน, ตรวจจับ, ตอบสนองและกู้คืน)

ตาราง2 ภาพประกอบเชิงทฤษฎีของระดับ CSF

ระดับ	การกำกับดูแลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์	การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
ระดับที่ 1: บางส่วน	การประยุกต์ใช้กลยุทธ์ความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรได้รับการจัดการในลักษณะเฉพาะกิจ การกำหนดลำดับความสำคัญนั้นเป็นแบบเฉพาะหน้าและไม่ได้ขึ้นอยู่กับวัตถุประสงค์หรือสภาพแวดล้อมภัยคุกคามอย่างเป็นทางการ	ความตระหนักถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในระดับองค์กรยังมีอยู่อย่างจำกัด องค์กรนำการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ไปปฏิบัติเป็นครั้งคราวและเป็นรายกรณีไป องค์กรอาจไม่มีกระบวนการที่ช่วยให้สามารถแบ่งปันข้อมูลการรักษาความปลอดภัยทางไซเบอร์ภายในองค์กรได้ โดยทั่วไปองค์กรจะไม่ตระหนักถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับซัพพลายเออร์และผลิตภัณฑ์และบริการที่องค์กรได้รับและใช้งาน
ระดับที่ 2: มีความรู้เรื่องความเสี่ยง	แนวทางการจัดการความเสี่ยงได้รับการอนุมัติจากฝ่ายบริหาร แต่จะไม่สามารถกำหนดเป็นนโยบายทั่วทั้งองค์กรได้ การกำหนดลำดับความสำคัญของกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์และความต้องการในการป้องกันจะเป็นไปตามวัตถุประสงค์ความเสี่ยงขององค์กร สภาพแวดล้อมของภัยคุกคาม หรือข้อกำหนดทางธุรกิจ/ภารกิจโดยตรง	มีการตระหนักรู้เกี่ยวกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในระดับองค์กร แต่ยังไม่ได้กำหนดแนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในระดับองค์กร การพิจารณาเรื่องการรักษาความปลอดภัยทางไซเบอร์ในวัตถุประสงค์และโปรแกรมขององค์กรอาจเกิดขึ้นได้ในบางระดับแต่ไม่ใช่ทั้งหมดขององค์กร การประเมินความเสี่ยงทางไซเบอร์ของสินทรัพย์ขององค์กรและภายนอกเกิดขึ้นแต่โดยทั่วไปไม่สามารถทำซ้ำหรือเกิดขึ้นซ้ำได้ ข้อมูลเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์มีการแบ่งปันภายในองค์กรอย่างไม่เป็นทางการ องค์กรตระหนักถึงความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับซัพพลายเออร์และผลิตภัณฑ์และบริการที่จัดหาและใช้ แต่ไม่ได้ดำเนินการตอบสนองต่อความเสี่ยงเหล่านั้นอย่างเป็นทางการหรือสม่ำเสมอ
ระดับ 3: ทำซ้ำได้	แนวทางการบริหารความเสี่ยงขององค์กรได้รับการอนุมัติอย่างเป็นทางการและแสดงไว้เป็นนโยบาย นโยบาย กระบวนการ และขั้นตอนที่คำนึงถึงความเสี่ยงจะได้รับการกำหนด นำไปปฏิบัติตามที่ตั้งใจไว้ และได้รับการตรวจสอบ แนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กรได้รับการอัปเดตเป็นประจำตามการนำกระบวนการจัดการความเสี่ยงไปปรับใช้กับการเปลี่ยนแปลงของข้อกำหนดทางธุรกิจ/ภารกิจ ภัยคุกคาม และภูมิทัศน์ทางเทคโนโลยี	มีแนวทางการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์สำหรับทั้งองค์กร ข้อมูลด้านการรักษาความปลอดภัยทางไซเบอร์จะถูกแชร์ไปทั่วทั้งองค์กรเป็นประจำ มีวิธีการในการตอบสนองต่อการเปลี่ยนแปลงความเสี่ยงอย่างมีประสิทธิภาพและสอดคล้องกัน บุคลากรมีความรู้และทักษะในการปฏิบัติหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย องค์กรตรวจสอบความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ของสินทรัพย์อย่างสม่ำเสมอและแม่นยำ ผู้บริหารระดับสูงด้านการรักษาความปลอดภัยทางไซเบอร์และไม่ใช่ด้านการรักษาความปลอดภัยทางไซเบอร์สื่อสารกันเป็นประจำเกี่ยวกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ ผู้บริหารต้องแน่ใจว่าการรักษาความปลอดภัยทางไซเบอร์ได้รับการพิจารณาในทุกสายงานปฏิบัติการขององค์กร กลยุทธ์ด้านความเสี่ยงขององค์กรจะได้รับข้อมูลจากความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับซัพพลายเออร์และผลิตภัณฑ์ และบริการที่องค์กร

ระดับ	การกำกับดูแลความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์	การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์
		ได้รับและใช้ บุคลากรดำเนินการเกี่ยวกับความเสี่ยงเหล่านั้นอย่างเป็นทางการผ่านกลไกต่าง ๆ เช่น ข้อตกลงเป็นลายลักษณ์อักษรเพื่อสื่อสารข้อกำหนดพื้นฐาน โครงสร้างการกำกับดูแล (เช่น สภาพความเสี่ยง) และการดำเนินนโยบายและการติดตามตรวจสอบ การดำเนินการเหล่านี้ได้รับการดำเนินการอย่างสอดคล้องและเป็นไปตามที่ตั้งใจไว้ และมีการติดตามและตรวจสอบอย่างต่อเนื่อง
ระดับ 4: ประยุกต์ใช้ได้	มีแนวทางทั่วทั้งองค์กรในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ โดยใช้นโยบาย กระบวนการ และขั้นตอนที่คำนึงถึงความเสี่ยงเพื่อจัดการกับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น ความสัมพันธ์ระหว่างความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์และวัตถุประสงค์ขององค์กรได้รับการเข้าใจและพิจารณาอย่างชัดเจนเมื่อทำการตัดสินใจ ผู้บริหารติดตามความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ในบริบทเดียวกันกับความเสี่ยงทางการเงินและความเสี่ยงอื่น ๆ ขององค์กร งบประมาณขององค์กรขึ้นอยู่กับความเข้าใจสภาพแวดล้อมความเสี่ยงและการยอมรับความเสี่ยงในปัจจุบันและที่คาดการณ์ไว้ หน่วยธุรกิจนำวิสัยทัศน์ของผู้บริหารไปปฏิบัติและวิเคราะห์ความเสี่ยงในระดับระบบในบริบทของการยอมรับความเสี่ยงขององค์กร การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซ-เบอร์เป็นส่วนหนึ่งของวัฒนธรรมองค์กร เป็นการวิวัฒนาการจากความตระหนักรู้ถึงกิจกรรมที่ผ่านมาและความตระหนักรู้ต่อเนื่องถึงกิจกรรมในระบบและเครือข่ายขององค์กร องค์กรสามารถคำนึงถึงการเปลี่ยนแปลงวัตถุประสงค์ทางธุรกิจ/ภารกิจในวิธีการจัดการและสื่อสารความเสี่ยงได้อย่างรวดเร็วและมีประสิทธิภาพ	องค์กรปรับแนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์โดยอิงตามกิจกรรมด้านการรักษาความปลอดภัยทางไซเบอร์ก่อนหน้าและปัจจุบัน รวมถึงบทเรียนที่ได้รับและตัวบ่งชี้เชิงคาดการณ์ ผ่านกระบวนการปรับปรุงอย่างต่อเนื่องที่ผสมผสานเทคโนโลยีและแนวทางปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์ขั้นสูง องค์กรปรับตัวให้เข้ากับภูมิทัศน์ทางเทคโนโลยีที่เปลี่ยนแปลงอย่างแข็งขัน และตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงและซับซ้อนอย่างทันท่วงทีและมีประสิทธิผล องค์กรใช้ข้อมูลแบบเรียลไทม์หรือเกือบเรียลไทม์เพื่อทำความเข้าใจและดำเนินการตามความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับซัพพลายเออร์และผลิตภัณฑ์และบริการที่จัดหาและใช้อย่างสม่ำเสมอ ข้อมูลเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์จะถูกแบ่งปันอย่างต่อเนื่องทั่วทั้งองค์กรและกับบุคคลที่สามที่ได้รับอนุญาต

ภาคผนวก C. อภิธานศัพท์

หมวดหมู่ CSF
เป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องประเภทหนึ่งซึ่งประกอบกันเป็นฟังก์ชัน CSF

โปรไฟล์ชุมชน CSF
ฐานข้อมูลเป้าหมาย CSF ที่สร้างขึ้นและเผยแพร่เพื่อตอบสนองความสนใจและเป้าหมายร่วมกันระหว่างองค์กรต่าง ๆ โดยทั่วไป โปรไฟล์ชุมชนจะได้รับการพัฒนาสำหรับภาคส่วน ภาคส่วนย่อย เทคโนโลยี ตามประเภทภัยคุกคาม หรือกรณีการใช้งานอย่างอื่นโดยเฉพาะ องค์กรสามารถใช้โปรไฟล์ชุมชนเป็นพื้นฐานสำหรับโปรไฟล์เป้าหมายของตนเองได้

แกนหลัก CSF
อนุกรมวิธานของเป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ระดับสูงที่สามารถช่วยให้องค์กรใด ๆ ก็ตามสามารถจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ได้ ส่วนประกอบของส่วนประกอบเหล่านี้เป็นลำดับชั้นของฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อย ที่ให้รายละเอียดเป้าหมายแต่ละรายการ

โปรไฟล์ปัจจุบันของ CSF
ส่วนหนึ่งของโปรไฟล์องค์กรที่ระบุเป้าหมายหลักที่องค์กรกำลังบรรลุ (หรือพยายามบรรลุ) ในปัจจุบัน และระบุถึงวิธีการหรือขอบเขตในการบรรลุเป้าหมายแต่ละอย่าง

ฟังก์ชัน CSF
ระดับสูงสุดขององค์กรสำหรับเป้าหมายด้านการรักษาความปลอดภัยทางไซเบอร์ มีฟังก์ชัน CSF 6 ประการ ได้แก่ กำกับดูแล ระบุ ปกป้อง ตรวจจับ ตอบสนอง และกู้คืน

ตัวอย่างการนำ CSF ไปใช้งาน
ภาพประกอบเชิงทฤษฎีที่กระชับ เน้นการกระทำเกี่ยวกับวิธีที่จะช่วยให้บรรลุเป้าหมาย CSF Core

ข้อมูลอ้างอิง CSF
การทำแผนที่ที่ระบุความสัมพันธ์ระหว่างเป้าหมาย CSF Core และมาตรฐาน แนวปฏิบัติ กฎระเบียบ หรือเนื้อหาอื่นที่มีอยู่

โปรไฟล์องค์กร CSF
กลไกในการอธิบายสถานะการรักษาความปลอดภัยทางไซเบอร์ปัจจุบันและ/หรือเป้าหมายขององค์กรในส่วนของเป้าหมายของ CSF Core

คู่มือเพื่อการเริ่มต้นอย่างรวดเร็วของ CSF
แหล่งข้อมูลเพิ่มเติมที่ให้คำแนะนำสั้น ๆ ที่สามารถดำเนินการได้เกี่ยวกับหัวข้อที่เกี่ยวข้องกับ CSF อย่างเฉพาะเจาะจง

หมวดหมู่ย่อย CSF
กลุ่มเป้าหมายที่เฉพาะเจาะจงยิ่งขึ้นของกิจกรรมทางเทคนิคและการจัดการด้านการรักษาความปลอดภัยทางไซเบอร์ซึ่งประกอบเป็นหมวดหมู่ CSF

โปรไฟล์เป้าหมาย CSF
ส่วนหนึ่งของโปรไฟล์องค์กรที่ระบุเป้าหมายหลักที่ต้องการซึ่งองค์กรเลือกและกำหนดลำดับความสำคัญเพื่อให้บรรลุวัตถุประสงค์การจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์

ระดับ CSF
ลักษณะเฉพาะของความเข้มงวดในการกำกับดูแลและจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร มี 4 ระดับ: บางส่วน (ระดับ 1) มีความรู้เกี่ยวกับความเสี่ยง (ระดับ 2) ทำซ้ำได้ (ระดับ 3) และประยุกต์ได้ (ระดับ 4)

เอกสารนี้ระบุถึงอุปกรณ์ เครื่องมือ ซอฟต์แวร์ หรือวัสดุเชิงพาณิชย์บางประการ ไม่ว่าจะเป็นเชิงพาณิชย์หรือไม่เชิงพาณิชย์ เพื่อให้สามารถระบุขั้นตอนการทดลองได้อย่างเหมาะสม การระบุดังกล่าวไม่ได้เป็นการแนะนำหรือการรับรองผลิตภัณฑ์หรือบริการใด ๆ โดย NIST และไม่ได้หมายความว่าวัสดุหรืออุปกรณ์ที่ระบุนั้นเป็นวัสดุหรืออุปกรณ์ที่ดีที่สุดสำหรับจุดประสงค์ดังกล่าว

นโยบายชุดเทคนิค NIST
คำชี้แจงเกี่ยวกับลิขสิทธิ์ การใช้งานและการอนุญาต
โครงสร้างตัวระบุเอกสารชุดเทคนิค NIST

วิธีอ้างอิงเอกสารชุดเทคนิค NIST นี้:

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 tha. https://doi.org/10.6028/NIST.CSWP.29.tha

ข้อมูลติดต่อ

cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

ความคิดเห็นทั้งหมดต้องได้รับการเผยแพร่ภายใต้กฎหมายเสรีภาพในการเข้าถึงข้อมูล (FOIA)