บันทึกข้อความ

ส่วนราชการ สถานีพัฒนาที่ดินกรุงเทพมหานคร โทร ๐-๒๔๕๓-๒๒๑๗

ที่ กษ ๐๘๐๘.๑๙/๑๖๘ **วันที่** ๑๖ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งแบบรายงานผลการพัฒนาความรู้ของข้าราชการ รอบการประเมินที่ ๑/๒๕๖๙

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร

ตามที่ กรมพัฒนาที่ดิน กำหนดกรอบตัวชี้วัดระดับความสำเร็จของการส่งเสริมการพัฒนาความรู้ของบุคลากรในหน่วยงาน ในรอบการประเมินที่ ๑/๒๕๖๙ ให้ข้าราชการมีการพัฒนาความรู้ โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่องส่งให้ผู้บังคับบัญชาทราบนั้น

ข้าพเจ้า ได้ทำการเรียนรู้ผ่านสื่อการเรียนการสอนจำนวน ๒ หลักสูตร ได้แก่

๑. โครงการฝึกอบรมออนไลน์ในระบบ (TDGA e-Learning) เรื่อง "ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management)"

๒. โครงการฝึกอบรมออนไลน์ในระบบ (TDGA e-Learning) เรื่อง "ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะที่จำเป็นสำหรับการปฏิบัติงานแบบออนไลน์ (Digital Literacy : Essential Skills for Working Online"

ในการนี้ จึงขอส่งแบบรายงานผลการพัฒนาความรู้ ๑ เรื่อง "ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management)" พร้อมแนบหลักฐานการเรียนมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและพิจารณา

(นางสาวจุฑารัตน์ วิจิตรปัญญา)
เจ้าพนักงานธุรการปฏิบัติงาน

(นางสาวนัทฐา ทักษ์รัตนศรัณย์)
ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จุฑารัตน์ วิจิตรปัญญา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 5 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-05T21:14:24.456+07:00
7e6ce106

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จุฑารัตน์ วิจิตรปัญญา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะที่จำเป็นสำหรับการปฏิบัติงานแบบออนไลน์

(Digital Literacy : Essential Skills for Working Online)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

95c58dd0

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สบร.)
Date: 2026-02-04T20:34:11.794+07:00

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ
สถานีพัฒนาที่ดินกรุงเทพมหานคร สำนักงานพัฒนาที่ดินเขต ๑
รอบการประเมินที่.....๑/๒๕๖๙.....ตั้งแต่วันที่....๑ ต.ค. ๒๕๖๘ – ๓๑ มี.ค. ๒๕๖๙.....
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางสาวจุฑารัตน์ วิจิตรปัญญา **ตำแหน่ง** เจ้าพนักงานธุรการปฏิบัติงาน
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินกรุงเทพมหานคร สำนักงานพัฒนาที่ดินเขต ๑
หัวข้อการพัฒนา โครงการฝึกอบรมออนไลน์ (TDGA e-Learning) "ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management)"
สถานที่ สถานีพัฒนาที่ดินกรุงเทพมหานคร สำนักงานพัฒนาที่ดินเขต ๑ **วันที่** ๕ กุมภาพันธ์ ๒๕๖๙
วิทยากร/ผู้ให้ความรู้ ผศ.พิเศษ สันติพัฒน์ อรุณธารี มหาวิทยาลัยหอการค้าไทย
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy

คำอธิบายบทเรียน

เรียนรู้ความหมายและความสำคัญของ Cybersecurity และ Cybersecurity Risk กระบวนการของ Cybersecurity Risk ความรู้เบื้องต้นของ Risk Assessment และ Risk Management แนวทางการวางแผนความต่อเนื่องทางธุรกิจ Business Continuity Planning (BCP)

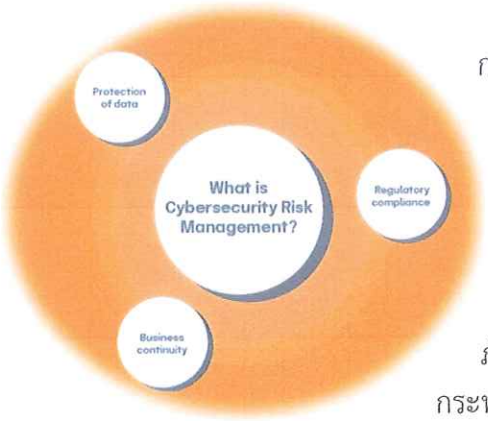
วัตถุประสงค์

๑. เพื่อให้ผู้เรียนเข้าใจความหมายและกระบวนการของ Cybersecurity Risk Management
๒. เพื่อให้ผู้เรียนเข้าใจหลักการพื้นฐานของ Risk Management
๓. เพื่อให้ผู้เรียนเข้าใจแนวทางการจัดทำแผน Business Continuity Planning

หัวข้อในบทเรียน

- ☐ Cyber Security vs. Information Security เรียนรู้ความหมายของ Cyber Security และ Information Security
- ☐ Cyber Security Risk Management ความเข้าใจเบื้องต้นของ Cyber Security Risk Management
- ☐ Frameworks กรอบการดำเนินงานและมาตรฐานที่เกี่ยวข้อง
- ☐ NIST Cybersecurity Framework ความเข้าใจเบื้องต้นของ NIST Cybersecurity Framework
- ☐ Business Continuity Planning (BCP) เรียนรู้การวางแผนความต่อเนื่องทางธุรกิจ
- ☐ ISO ๒๒๓๐๑ Business Continuity Management เรียนรู้มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO ๒๒๓๐๑ (BCM)

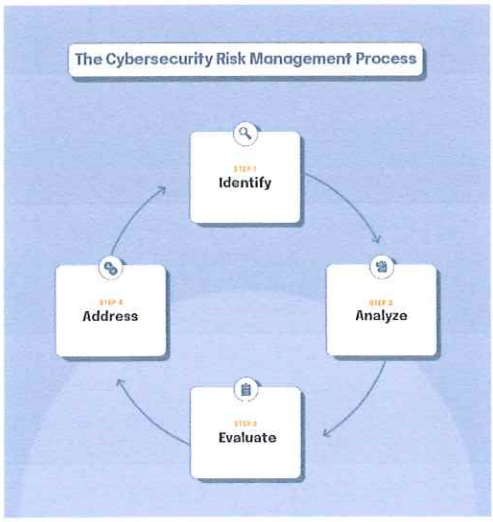
การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์คืออะไร?



การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นกระบวนการต่อเนื่องในการระบุ วิเคราะห์ ประเมิน และแก้ไขภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรของคุณ ซึ่งเริ่มต้นด้วยความเข้าใจร่วมกันเกี่ยวกับนิยามของความเสี่ยงด้านไซเบอร์ (หรือเรียกว่าความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์) ความเสี่ยงด้านไซเบอร์คือความน่าจะเป็นที่ภัยคุกคาม จุดอ่อนของระบบ หรือการกระทำของมนุษย์จะส่งผลกระทบต่อความลับ ความสมบูรณ์ หรือความพร้อม ใช้งานของระบบสารสนเทศ ส่งผลให้เกิดผลกระทบทางการเงิน การดำเนินงาน หรือชื่อเสียง ในองค์กรหลายแห่ง การบริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์ระดับองค์กรเป็นศาสตร์ที่เชื่อมโยงการควบคุมความปลอดภัยทางเทคนิค วัตถุประสงค์ทางธุรกิจ และการกำกับดูแลในระดับคณะกรรมการเข้าด้วยกันเป็นโปรแกรมที่ประสานงานกัน ในทางปฏิบัติ การวิเคราะห์ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ (บางครั้งเรียกว่าการวิเคราะห์ความเสี่ยงด้านความปลอดภัยทางไซเบอร์) คือการเปลี่ยนภัยคุกคามและช่องโหว่ให้เป็นความเสี่ยงที่จัดลำดับความสำคัญและพร้อมสำหรับการตัดสินใจ

กระบวนการบริหารจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

NIST SP ๘๐๐-๓๐ เป็นวิธีการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ใช้กันอย่างแพร่หลาย สำหรับการวางโครงสร้างการเตรียมการ การประเมิน การสื่อสาร และการบำรุงรักษาอย่างต่อเนื่อง



โดยทั่วไปจะปฏิบัติตามกระบวนการรักษาความปลอดภัยทางไซเบอร์ที่เป็นระบบ เริ่มต้นด้วยการกำหนดขอบเขตและวัตถุประสงค์ของการจัดการความเสี่ยง จากนั้นจึงระบุความเสี่ยงที่อาจส่งผลกระทบต่อวัตถุประสงค์ขององค์กร ต่อมาคือการประเมินความเสี่ยงเพื่อทำความเข้าใจความเป็นไปได้และผลกระทบที่อาจเกิดขึ้น ในขั้นตอนการประเมินความเสี่ยง จะมีการเปรียบเทียบความเสี่ยงกับค่าความคลาดเคลื่อนที่องค์กรกำหนดไว้ เพื่อจัดลำดับความสำคัญของความเสี่ยงสำหรับการตัดสินใจ

จัดทำแผนบริหารจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ระบุความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ในการระบุความเสี่ยง จำเป็นอย่างยิ่งที่จะต้องเริ่มต้นด้วยการทำความเข้าใจภัยคุกคาม จุดอ่อน และผลที่ตามมาจากการบรรจบกันของสิ่งเหล่านี้

ภัยคุกคาม คือ สถานการณ์หรือเหตุการณ์ที่มีศักยภาพที่จะส่งผลกระทบในทางลบต่อการดำเนินงานหรือทรัพย์สินขององค์กรผ่านการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต ภัยคุกคามสามารถเกิดขึ้นได้ในหลายรูปแบบ รวมถึงการโจมตีที่เป็นปรปักษ์ ความผิดพลาดของมนุษย์ ความล้มเหลวของโครงสร้างหรือการกำหนดค่า และแม้แต่ภัยพิบัติทางธรรมชาติ

ช่องโหว่ สามารถนิยามได้ว่าเป็นจุดอ่อนในระบบสารสนเทศ ขั้นตอนการรักษาความปลอดภัย การควบคุมภายใน หรือการดำเนินการที่แหล่งที่มาของภัยคุกคามสามารถใช้ประโยชน์ได้ บ่อยครั้งที่ช่องโหว่เกิดจากความไม่เพียงพอของฟังก์ชันภายใน เช่น การรักษาความปลอดภัย และยังสามารถพบได้จากภายนอกในห่วงโซ่อุปทานหรือความสัมพันธ์กับผู้ขาย

ผลที่ตามมา คือผลลัพธ์ที่ไม่พึงประสงค์ที่เกิดขึ้นเมื่อภัยคุกคามใช้ประโยชน์จากช่องโหว่ ผลกระทบจะวัดความรุนแรงของผลที่ตามมา และองค์กรของคุณจะต้องประเมินต้นทุนดังกล่าวเมื่อประเมินความเสี่ยง โปรดจำไว้ว่าต้นทุนเหล่านี้มักมาจากการสูญหายหรือถูกทำลายของข้อมูล การหยุดชะงักของบริการ และบทลงโทษทางกฎหมายหรือข้อบังคับ ซึ่งอาจเป็นอุปสรรคสำคัญต่อธุรกิจขององค์กรใดๆ ก็ตาม

ประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์

การประเมินความเสี่ยงเป็นโอกาสอันมีค่าในการเน้นย้ำถึงความสำคัญของความปลอดภัยทั่วทั้งองค์กร การประเมินความเสี่ยงช่วยให้ทีมของคุณสามารถฝึกฝนการสื่อสารและความร่วมมือที่มีประสิทธิภาพ ซึ่งมีบทบาทสำคัญในการบริหารความเสี่ยงในอนาคต

ระบุมาตรการลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่เป็นไปได้

การระบุและประเมินความเสี่ยงเป็นเพียงจุดเริ่มต้นเท่านั้น จะดำเนินการอย่างไรกับความเสี่ยงที่พบ มาตรการบรรเทาผลกระทบเพื่อจัดการความเสี่ยงของจะเป็นอย่างไร จะจัดการกับความเสี่ยงที่เหลืออยู่ได้อย่างไร ประวัติศาสตร์บอกเราว่าทีมบริหารความเสี่ยงที่ประสบความสำเร็จมากที่สุดมักมีแผนการที่รอบคอบเพื่อเป็นแนวทางในการวางกลยุทธ์การตอบสนองต่อความเสี่ยงที่สูงกว่าระดับความเสี่ยงที่องค์กรยอมรับได้

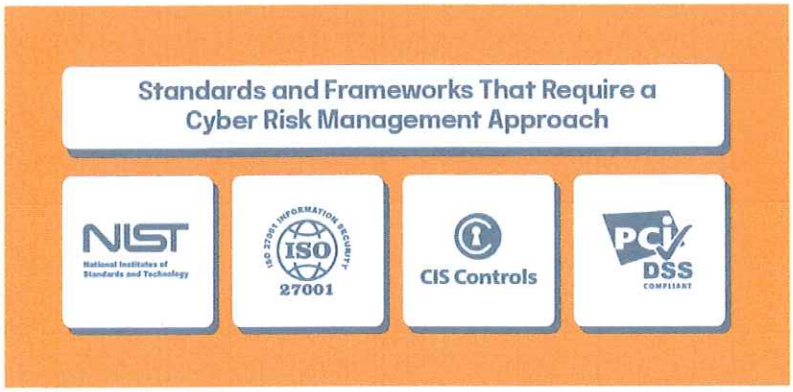
องค์กรต่างๆ สามารถลดความเสี่ยงได้โดยการเลือกและนำมาตรการควบคุมมาใช้ ซึ่งรวมถึงบุคลากร กระบวนการ หรือเทคโนโลยี เช่น

- ☐ โปรแกรมฝึกอบรมด้านความปลอดภัยทางไซเบอร์
- ☐ กำลังอัปเดตซอฟต์แวร์
- ☐ โซลูชันการจัดการสิทธิ์การเข้าถึงระดับสูง (PAM)
- ☐ การตรวจสอบสิทธิ์การเข้าถึงแบบหลายปัจจัย
- ☐ การสำรองข้อมูลแบบไดนามิก

สิ่งที่หน่วยงานควรตรวจสอบ

- ☐ **การเปลี่ยนแปลงด้านกฎระเบียบ** : การติดตามกฎระเบียบและข้อเปลี่ยนแปลงต่างๆ อย่างสม่ำเสมอจะช่วยให้ระบบควบคุมภายในสอดคล้องกับความคาดหวังจากภายนอก
- ☐ **ความเสี่ยงจากผู้ขาย** : ตรวจสอบและจัดทำเอกสารเกี่ยวกับการรักษาความปลอดภัยและการปฏิบัติตามกฎระเบียบเมื่อร่วมงานกับผู้ขายรายใหม่ จำไว้ว่าข้อบกพร่องของพวกเขาอาจกลายเป็นปัญหาใหญ่
- ☐ **การใช้งานไอทีภายในองค์กร** : ทำความเข้าใจว่าทีมงานภายในองค์กรใช้เทคโนโลยีอะไรบ้าง และพวกเขาใช้งานอย่างไร เพื่อเตรียมพร้อมรับมือกับช่องโหว่ที่อาจเกิดขึ้น

มาตรฐานและกรอบการทำงานที่กำหนดให้ต้องใช้แนวทางการบริหารความเสี่ยงทางไซเบอร์



นอกจาก NIST SP ๘๐๐-๕๓ แล้ว ยังมีมาตรฐาน/กรอบการปฏิบัติตามข้อกำหนดด้านความปลอดภัยทางไซเบอร์อื่นๆ อีกหลายฉบับที่ประกอบด้วยแนวทางปฏิบัติที่ดีที่สุดและข้อกำหนดสำหรับการจัดการความเสี่ยงทางไซเบอร์ มาตรฐานเหล่านี้ให้ภาษาและโครงสร้างที่ใช้ร่วมกันสำหรับโครงการริเริ่มด้านความปลอดภัยทางไซเบอร์ในการบริหารความเสี่ยงขององค์กร ช่วยให้ทีมต่างๆ สามารถปรับการควบคุม การประเมิน และการรายงานให้สอดคล้องกันทั่วทั้งองค์กร ส่วนใหญ่เลือกใช้กรอบการบริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์อย่างน้อยหนึ่งกรอบเพื่อกำหนดมาตรฐานการประเมิน การควบคุม และการรายงาน ด้านล่างนี้คือกรอบการทำงานที่เป็นที่รู้จักมากที่สุด:

<u>ไอโซ/อีอีซี ๒๗๐๐๑</u>

มาตรฐานสากลสำหรับการจัดการความปลอดภัยของข้อมูล “มาตรฐาน ISO ใดที่มีข้อกำหนดสำหรับการจัดการและควบคุมความเสี่ยง” คำตอบหลักคือ ISO/IEC ๒๗๐๐๑ (โดย ISO/IEC ๒๗๐๐๒ ให้คำแนะนำการควบคุมที่ละเอียดกว่า) กำหนดและรักษาระดับเกณฑ์ความเสี่ยงด้านความปลอดภัยของข้อมูล

กรอบงานความปลอดภัยทางไซเบอร์ของ NIST เวอร์ชัน ๒.๐

กรอบงานความปลอดภัยทางไซเบอร์ (CSF) ๒.๐ ของ NIST นำเสนอชุดผลลัพธ์ด้านความปลอดภัยทางไซเบอร์ที่ครอบคลุม ซึ่งออกแบบมาเพื่อช่วยให้องค์กรทุกขนาดและทุกภาคส่วนสามารถจัดการและลดความเสี่ยงทางไซเบอร์ได้ ประกอบด้วยการจำแนกประเภทของการดำเนินการด้านความปลอดภัยทางไซเบอร์ระดับสูงในหกหน้าที่สำคัญด้านความปลอดภัย ได้แก่ การกำกับดูแล การระบุ การปกป้อง การตรวจจับ การตอบสนอง และการกู้คืน หน้าที่เหล่านี้มุ่งเน้นที่จะจัดการกับภัยคุกคามทางไซเบอร์ที่หลากหลาย รวมถึงมัลแวร์ การขโมยรหัสผ่าน การโจมตีแบบฟิชชิ่ง การโจมตีแบบ DDoS การดักฟังข้อมูล การหลอกลวงทางสังคม และอื่นๆ ในขณะเดียวกันก็ขยายไปถึงเทคโนโลยีเกิดใหม่ ความเสี่ยงด้านความเป็นส่วนตัว และความเสี่ยงในห่วงโซ่อุปทานด้วย โดยเฉพาะอย่างยิ่ง แนะนำให้องค์กรดำเนินการตามขั้นตอนต่อไปนี้

- ☐ ระบุและบันทึกจุดอ่อนของสินทรัพย์
- ☐ ติดตามข่าวสารล่าสุดเกี่ยวกับภัยคุกคามทางไซเบอร์จากฟอรัมแลกเปลี่ยนข้อมูลต่างๆ
- ☐ ระบุและบันทึกภัยคุกคามทั้งภายในและภายนอกองค์กร
- ☐ ระบุผลกระทบทางธุรกิจที่อาจเกิดขึ้นและความน่าจะเป็นของเหตุการณ์เสี่ยง
- ☐ ใช้ปัจจัยคุกคาม จุดอ่อน ความเป็นไปได้ และผลกระทบในการประเมินความเสี่ยง
- ☐ ระบุและจัดลำดับความสำคัญของการตอบสนองต่อความเสี่ยง

ขั้นตอน	วัตถุประสงค์
เตรียมตัว	กิจกรรมสำคัญเพื่อเตรียมความพร้อมให้องค์กรสามารถจัดการกับความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวได้
จัดหมวดหมู่	แจ้งให้ทราบถึงกระบวนการและภารกิจการบริหารความเสี่ยงขององค์กร โดยพิจารณาถึงผลกระทบเชิงลบที่เกี่ยวข้องกับการสูญเสียความลับ ความสมบูรณ์ และความพร้อมใช้งานของระบบและข้อมูลที่ประมวลผล จัดเก็บ และส่งผ่านโดยระบบเหล่านั้น
เลือก	เลือก ปรับแต่ง และจัดทำเอกสารเกี่ยวกับมาตรการควบคุมที่จำเป็นเพื่อปกป้องระบบและองค์กรให้สอดคล้องกับระดับความเสี่ยง
ดำเนินการ	ดำเนินการตามมาตรการควบคุมในแผนรักษาความปลอดภัยและความเป็นส่วนตัวสำหรับระบบและองค์กร
ประเมิน	ตรวจสอบว่ามีการนำระบบควบคุมไปใช้อย่างถูกต้อง ทำงานได้ตามที่ตั้งใจไว้ และก่อให้เกิดผลลัพธ์ที่ต้องการในแง่ของการตอบสนองความต้องการด้านความปลอดภัยและความเป็นส่วนตัวของระบบและองค์กรหรือไม่
อนุญาต	สร้างความรับผิดชอบโดยกำหนดให้เจ้าหน้าที่ระดับสูงเป็นผู้พิจารณาว่าความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวที่เกิดจากการทำงานของระบบหรือการใช้มาตรการควบคุมทั่วไปนั้นอยู่ในระดับที่ยอมรับได้หรือไม่
เฝ้าสังเกต	รักษาความตระหนักรู้เกี่ยวกับสถานการณ์ด้านความปลอดภัยและความเป็นส่วนตัวของระบบและองค์กรอย่างต่อเนื่อง เพื่อสนับสนุนการตัดสินใจด้านการบริหารความเสี่ยง

มาตรฐาน NIST CSF ๒.๐ ให้คำแนะนำโดยละเอียดเกี่ยวกับการจัดการความเสี่ยงในห่วงโซ่อุปทานผ่านกระบวนการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในห่วงโซ่อุปทาน (C-SCRM) โดยเรียกร้องให้องค์กรต่างๆ สร้างและนำวิธีการที่เป็นระบบมาใช้เพื่อระบุ ประเมิน และจัดการความเสี่ยงในห่วงโซ่อุปทานด้วยการกำหนดกลยุทธ์ จัดลำดับซัพพลายเออร์ตามความสำคัญ กำหนดข้อกำหนดด้านความปลอดภัย และบูรณาการความพยายามเหล่านี้เข้ากับกรอบการบริหารความเสี่ยงและการตอบสนองต่อเหตุการณ์ในวงกว้าง

กรอบการบริหารความเสี่ยงของ NIST

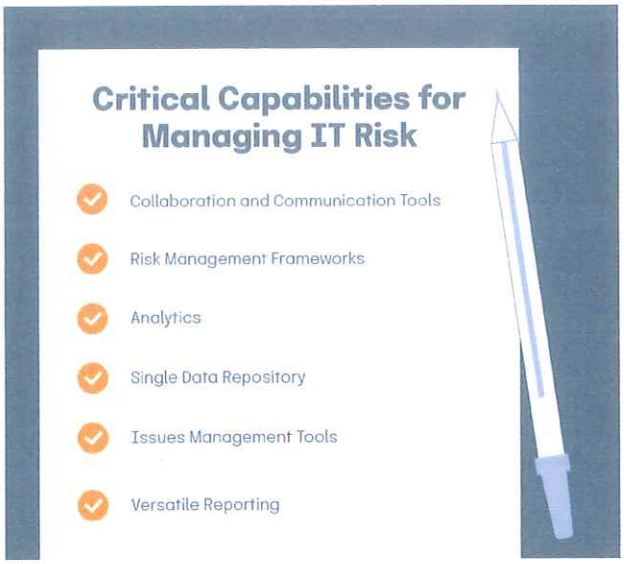
นำเสนอขั้นตอนที่บูรณาการกิจกรรมการบริหารความเสี่ยงด้านความปลอดภัย ความเป็นส่วนตัว และห่วงโซ่อุปทานไซเบอร์ เข้ากับวงจรชีวิตการพัฒนาระบบ แนวทางการบริหารความเสี่ยงนี้สามารถนำไปใช้กับระบบใหม่และระบบเดิม ระบบหรือเทคโนโลยีทุกประเภท (เช่น IoT ระบบควบคุม) และภายในองค์กรทุกประเภท ไม่ว่าจะมีขนาดหรือภาคส่วนใดก็ตาม ขั้นตอนสำคัญในกรอบการทำงานประกอบด้วยดังต่อไปนี้

บทบาทของทีมงานด้านการปฏิบัติตามกฎระเบียบภายในและการตรวจสอบในการบริหารความเสี่ยง

ในองค์กรที่มีความพร้อมแล้ว การบริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์ขององค์กรขึ้นอยู่กับทีมงานด้านการปฏิบัติตามกฎระเบียบและการตรวจสอบภายใน เพื่อให้การประเมินความเสี่ยง การควบคุม การทดสอบ และการแก้ไขปัญหาดำเนินไปอย่างต่อเนื่อง การบริหารความเสี่ยงเป็นกระบวนการต่อเนื่องที่ควรมีการประเมินใหม่ การทดสอบใหม่ และการลดความเสี่ยงอย่างต่อเนื่องเสมอ ด้านล่างนี้คือ ๘ วิธีที่สามารถช่วยได้

๑. ระบุและประเมินความเสี่ยง
๒. วางแผน กำหนดขอบเขต และทดสอบความเครียดของความเสี่ยงระดับจุลภาค
๓. ระบุการควบคุม
๔. ประเมินประสิทธิผลของการควบคุม
๕. เชื่อมโยงการควบคุมกับข้อกำหนด
๖. ตรวจสอบและทดสอบระบบควบคุมอัตโนมัติ
๗. บันทึก ติดตาม และรายงานข้อบกพร่อง

ความสามารถที่สำคัญสำหรับการบริหารความเสี่ยง



การวิเคราะห์

ความสามารถอเนกประสงค์นี้เป็นหัวใจสำคัญของการวิเคราะห์ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ช่วยในการวิเคราะห์สาเหตุที่แท้จริง การตรวจจับแนวโน้ม และการวิเคราะห์เชิงคาดการณ์ความเสี่ยงที่เกิดขึ้นใหม่ เพื่อให้คุณสามารถจัดลำดับความสำคัญในการลดความเสี่ยงโดยอิงจากข้อมูลจริง แทนที่จะใช้ความรู้สึกเพียงอย่างเดียว

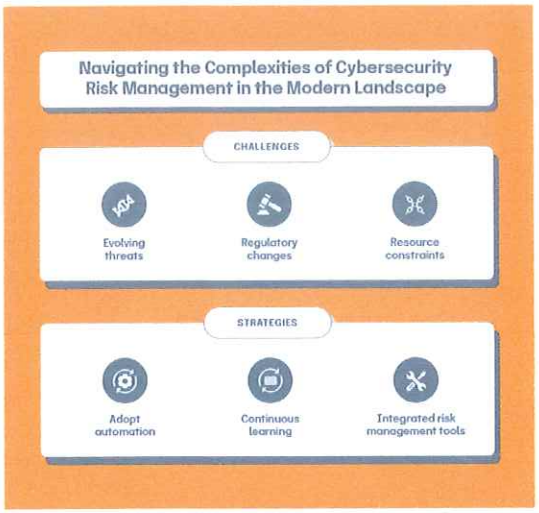
เครื่องมือจัดการปัญหา

เครื่องมือเหล่านี้จะจัดระเบียบการมอบหมายขั้นตอนการบรรเทาผลกระทบเฉพาะเจาะจง และตั้งระบบเตือนอัตโนมัติเพื่อให้ดำเนินการตามภารกิจให้เสร็จสิ้นโดยเร็ว นอกจากนี้ยังแจ้งเตือนผู้บริหารระดับสูงหากภารกิจไม่แล้วเสร็จ

การรายงานที่หลากหลาย

ความยืดหยุ่นในการนำเสนอ รายงาน การบริหารความเสี่ยงด้านไอทีแก่ผู้นำหน่วยธุรกิจและผู้บริหารระดับสูงในรูปแบบที่ต้องการและใช้งานได้ง่ายที่สุด

การรับมือกับความซับซ้อนของการบริหารจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในยุคปัจจุบัน



การจัดการความเสี่ยงทั่วทั้งองค์กรมีความซับซ้อนกว่าที่เคยเป็นมาในปัจจุบัน สภาพแวดล้อมด้านความปลอดภัยสมัยใหม่เปลี่ยนแปลงอยู่บ่อยครั้ง และการเพิ่มขึ้นอย่างรวดเร็วของผู้ให้บริการภายนอก เทคโนโลยีที่พัฒนาขึ้น และกฎระเบียบที่ขยายตัวอย่างต่อเนื่อง ล้วนเป็นความท้าทายสำหรับองค์กรต่างๆ

จากสถานการณ์ดังกล่าว การนำกระบวนการบริหารความเสี่ยงมาใช้จึงมีความสำคัญอย่างยิ่งต่อองค์กร เริ่มจากการระบุและประเมินความเสี่ยงเพื่อสร้างแบบจำลองความเสี่ยง จากนั้นเลือกกลยุทธ์การลดความเสี่ยงและตรวจสอบการควบคุมภายในอย่างต่อเนื่องเพื่อให้สอดคล้องกับความเสี่ยง การประเมินใหม่ การทดสอบใหม่ และการลดความเสี่ยงอย่างต่อเนื่อง ควรมีบทบาทสำคัญในทุกโครงการบริหารความเสี่ยงเสมอ

ในท้ายที่สุดแล้ว การบริหารความเสี่ยงในยุคปัจจุบันนั้นไม่มีวันหยุดพัก สภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างต่อเนื่องและไม่เคยมีมาก่อน โดยมีภัยคุกคามและช่องโหว่เพิ่มขึ้นทุกนาที อย่างไรก็ตาม ด้วยความช่วยเหลือจากเครื่องมือวิเคราะห์ เครื่องมือการทำงานร่วมกัน/การสื่อสาร/การจัดการปัญหา และกรอบการบริหารความเสี่ยงจากภายนอก องค์กรที่สร้างสรรค์และประสบความสำเร็จจะยังคงสามารถยืนหยัดในการต่อสู้เพื่อบริหารความเสี่ยงด้านไอทีและรักษาความปลอดภัยทั่วทั้งองค์กรต่อไปได้

ประโยชน์ที่ได้รับจากการอบรม

จากที่ได้รับการอบรม ออนไลน์ (TDGA e-Learning) เรื่อง “ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management) ทำให้มีความรู้ ความเข้าใจในเรื่องของการประเมินความเสี่ยง การรับมือภัยคุกคามทางไซเบอร์ ซึ่งในปัจจุบันหน่วยงานราชการปรับเปลี่ยนเป็นรัฐบาลยุคดิจิทัลแล้วนั้น เพื่อให้การรักษาความ มั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐ และประชาชนที่ใช้บริการ ช่วยปกป้องข้อมูลสำคัญ ระบุภัยคุกคาม และลดผลกระทบทางการเงินหรือชื่อเสียงจากการถูกโจมตีได้ทันท่วงที ประโยชน์หลักคือการสร้างความมั่นคงในระบบดิจิทัล ทำให้สามารถจัดสรรทรัพยากรเพื่อป้องกันจุดอ่อนที่สำคัญที่สุดได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

.....

(ลงนาม).....

(นางสาวจุฑารัตน์ วิจิตรปัญญา)

ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน

(ลงนาม).....

(นางสาวนัทฐา ทักษ์รัตนศรัณย์)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร

ผู้รับรองผลการพัฒนาความรู้