# การสังเคราะห์เนื้อหาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศตามมาตรฐานสากล

# Synthesis of a Security in International Information Technology Standards

จิระ จิตสุภา (Jira Jitsupa)* ปรัชญนันท์ นิลสุข (Prachyanun Nilsook)* และ พัลลภ พิริยะสุรวงศ์ (Pallop Piriyasurawong)*

**บทคัดย่อ**

มาตรฐานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ได้รับความนิยมนำมาใช้ในกระบวนการปกป้องข้อมูลจากภัยคุกคามทั้งจากภายในและภายนอกองค์กร มีด้วยกันหลายมาตรฐาน และแต่ละมาตรฐานมีจุดเน้นหรือการให้ความสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลที่แตกต่างกัน การนำมาตรฐานดังกล่าวมาสังเคราะห์ทำให้เห็นแนวทางการปฏิบัติของแต่ละมาตรฐานที่มีความแตกต่างกันอย่างชัดเจน เพื่อเป็นต้นแบบสำหรับการศึกษาและการนำไปทดลองใช้งาน และทำให้สามารถเลือกใช้มาตรฐานในการป้องกันภัยคุกคามที่มีต่อข้อมูลได้เป็นอย่างดี

**คำสำคัญ:** ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ มาตรฐานสากลด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

**Abstract**

Information technology security standards that were popular in the process used to protect data from threats both inside and outside the organization. There are several standards. Each standard has different focus or emphasis on the security of information. Implementation of such a synthetic approach to the implementation of the standards are clearly different. To be a model for the study and its experimental use and thus can be applied to prevent threats to the data as well.

**Keywords:** Information Technology Security, International Information Technology Security Standard.

## 1. บทนำ

เทคโนโลยีสารสนเทศมีการพัฒนาอย่างต่อเนื่อง เปิดโอกาสให้ประเทศไทยมีทางเลือกและสามารถใช้ประโยชน์จากเทคโนโลยีนี้เพื่อปรับปรุงประสิทธิภาพของโครงสร้างพื้นฐานและลดความเหลื่อมล้ำในการเข้าถึงข้อมูลข่าวสารของประชาชน [1] ช่วยสร้างโอกาสการเรียนรู้ให้คนไทยให้สามารถเข้าถึงข้อมูลข่าวสารและความรู้ได้อย่าง กว้างขวาง รวมทั้งสามารถปรับตัวให้รู้เท่าทันการเปลี่ยนแปลง [2] แต่การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีสารสนเทศเปรียบเสมือนดาบสองคม [3] เพราะสามารถส่งเสริมให้เกิดความก้าวหน้า หรืออาจจะฉุดรั้งให้ตกต่ำลงหรือนิ่งอยู่กับที่ก็ได้ บ่อยครั้งที่เทคโนโลยีสารสนเทศนำมาซึ่งความไม่มั่นคงปลอดภัย เช่น การเพิ่มขึ้นของภัยคุกคาม อย่างไวรัส เวิร์ม การเข้าเจาะระบบสารสนเทศโดยผู้ไม่ประสงค์ดี อาชญากรรมทางคอมพิวเตอร์ [4] หรือเหตุสุดวิสัย [5] ที่คาดไม่ถึงซึ่งอาจเกิดจากความตั้งใจหรือไม่ตั้งใจก็ตาม [6], [7] รวมถึงความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียของเทคโนโลยีสารสนเทศ เช่น ไฟไหม้ ล้วนสร้างความไม่มั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และข้อมูลและสารสนเทศขององค์กรใดๆ ก็ได้ รวมถึงอันตรายที่เกิดขึ้นจากด้านกายภาพและสิ่งแวดล้อม ด้านระบบการบริหารจัดการ [8] เกิดจากศีลธรรม และเกิดจากกฎหมาย [9] อีกด้วย

การบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเป็นการระบุรายละเอียดการดำเนินการของทรัพย์สินด้านความมั่นคงปลอดภัยและการพัฒนาระบบ การจัดทำเอกสาร นโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และแนวปฏิบัติ ซึ่งต้องยึดกรอบดำเนินการที่ประกอบด้วยการเก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality), ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูล

* คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

(Availability) [1], [3], [5], [10], [11], [12] โดยการดำเนินการควรประกอบไปด้วยการแบ่งชั้นความสำคัญและความลับข้อมูล การสร้างความตระหนัก การฝึกอบรมและการให้ความรู้ด้วยการเรียนรู้แก่ผู้มีส่วนได้ส่วนเสีย [3], [13] ซึ่งถือเป็นการบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่มีความสำคัญเป็นอย่างยิ่ง ความเสี่ยงก็เป็นอีกองค์ประกอบหนึ่งที่มีความสำคัญในการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ [14] การวิเคราะห์ความเสี่ยง การบริหารความเสี่ยงสามารถระบุ วัดผล ควบคุม และลดปัญหาต่อความเสียหายที่เกิดขึ้น ซึ่งต้องมีการทบทวนอย่างต่อเนื่องเพื่อหาทางป้องกันและดำเนินการอย่างมีประสิทธิภาพ [3]

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศมีความสำคัญยิ่งในการปกป้องทรัพยากรขององค์กร ซึ่งในความเป็นจริงก็เป็นที่ทราบกันอยู่แล้วว่าไม่มีสิ่งใดที่จะสามารถรับประกันความปลอดภัยได้ 100 เปอร์เซ็นต์ [15] ดังนั้นการจะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยมากที่สุดจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการต่าง ๆ เหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไปหลายมาตรฐานด้วยกัน แต่ละองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจจะเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ [5] มาตรฐานเหล่านี้ช่วยสร้างความมั่นใจในการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้สามารถดำเนินไปได้อย่างต่อเนื่อง มีประสิทธิภาพ และเป็นที่ยอมรับ [15]

ปัจจุบันพัฒนาการของการนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลาย อาจเกิดจากประสบการณ์ในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างไม่ปลอดภัยแล้วก่อให้เกิดผลเสียอันร้ายแรงตามมา หรืออาจเกิดจากนโยบายเชิงรุกของประเทศที่พัฒนาแล้วด้านเทคโนโลยีสารสนเทศได้กำหนดให้ประเทศที่เป็นคู่ค้าของตนต้องจัดทำระบบสารสนเทศที่มีความมั่นคงปลอดภัยเช่นกันจึงจะเป็นที่ยอมรับและเชื่อมั่นในการใช้งาน [16]

มาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศมีหลายมาตรฐานที่องค์กรจากหลายประเทศ เช่น ประเทศญี่ปุ่น ประเทศเกาหลี ประเทศสิงคโปร์ [8], [16] นำไปใช้เป็นแนวทางการปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและประสบความสำเร็จ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ประกอบด้วยมาตรฐาน ISO 27001:2005, COBIT, ITIL, COSO, FIPS PUB 200, NIST 800-14, และ IT BPM [5], [8], [15], [17], [18], [19]

## 2. องค์ประกอบพื้นฐานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเป็นคำใหม่ที่เพิ่งถูกใช้กันมาเมื่อไม่นาน ก่อนหน้านี้คนส่วนมากยังคงเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศว่าเป็นเพียงภัยคุกคามทางกายภาพหรือทางอุปกรณ์เท่านั้น [20] แท้จริงแล้วความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศตั้งอยู่บนองค์ประกอบพื้นฐาน 3 อย่าง [1], [3], [5], [11], [12] เรียกว่า C.I.A. ซึ่งสามารถอธิบายได้ดังนี้

**2.1 ความลับของข้อมูล (Confidentiality)** คือการรักษาหรือการปกปิดเพื่อปกป้องข้อมูลให้เป็นความลับ โดยสามารถเข้าใช้งานได้ เฉพาะผู้ที่ได้รับอนุญาตหรือได้สิทธิ์เท่านั้น

**2.2 ความคงสภาพ หรือความสมบูรณ์ของข้อมูล (Integrity)** เป็นการปกป้อง รักษาข้อมูลไว้ไม่ให้ถูกแก้ไขเปลี่ยนแปลง หรือถูกทำลาย และเป็นการทำให้ข้อมูลมีความน่าเชื่อถือว่าข้อมูลมาจากแหล่งต้นฉบับจริง ไม่ได้ถูกนำไปเปลี่ยนแปลงโดยผู้ที่ไม่ได้รับอนุญาต

**2.3 ความพร้อมใช้งานของข้อมูล (Availability)** คือการดูแล รักษาสภาพของข้อมูลให้สามารถเข้าถึงและเรียกใช้งานได้ตลอดเวลาเมื่อต้องการโดยผู้ที่ได้รับอนุญาตเท่านั้น

แต่ด้วยความก้าวหน้าของเทคโนโลยีสารสนเทศทำให้แนวคิด C.I.A. ไม่เพียงพออีกต่อไป เนื่องจากพบว่ามีภัยคุกคามต่อการปกป้องสารสนเทศให้เป็นความลับ ให้มีสภาพที่สมบูรณ์ และพร้อมใช้มากขึ้น ไม่ว่าจะเป็นภัยคุกคามที่เกิดขึ้นตั้งใจหรือไม่ตั้งใจ เช่น การลักขโมย การแก้ไข เปลี่ยนแปลงโดยไม่ได้รับอนุญาตตลอดจนการนำไปใช้ในทางที่ผิด ดังนั้นจึงได้มีการกำหนดองค์ประกอบของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพิ่มเติม [5], [12] ดังนี้

**2.4 การพิสูจน์ทราบตัวตน (Authentication)** เป็นกระบวนการในการพิสูจน์ว่าผู้ใช้งานบนระบบสารสนเทศเป็นผู้นั้นหรือเป็นเจ้าของสิทธิ์จริงๆ ไม่ได้ถูกแอบอ้างโดยผู้ไม่ประสงค์ดี

**2.5 ระดับสิทธิในการเข้าถึงข้อมูล (Authorization)** ในองค์กรมีบุคลากรมากมาย แต่ละคนก็มีหน้าที่และตำแหน่งที่แตกต่างกันออกไป ดังนั้นจะต้องมีการอนุญาต หรือกำหนดระดับสิทธิ์ในการเข้าถึงข้อมูล ผู้ใดบ้างที่มีสิทธิ์ในการแก้ไขเปลี่ยนแปลงข้อมูลได้ทั้งหมด และผู้ใดที่ไม่มีสิทธิ์แก้ไขเปลี่ยนแปลงข้อมูล

**2.6 ความถูกต้องแม่นยำของข้อมูล (Accuracy)** คือความถูกต้องแม่นยำของข้อมูลและสารสนเทศที่จะต้องไม่ผิดพลาดและต้องมีค่าตรงกับความเป็นจริงเสมอ นอกเสียจากข้อมูลจะถูกเปลี่ยนแปลงโดยผู้ที่ได้รับสิทธิ์ในการเปลี่ยนแปลงเท่านั้น

**2.7 ความเป็นส่วนตัว (Privacy)** ข้อมูลและสารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บ จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเจ้าของสารสนเทศรับทราบ และไม่ถูกละเมิดสิทธิ์โดยผู้ไม่หวังดี

**2.8 การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation)** การเข้าใช้งานระบบสารสนเทศในปัจจุบันมีการกำหนดสิทธิ์ และการอนุญาตให้กับผู้ใช้แต่ละคนที่แตกต่างกันออกไป ซึ่งหากผู้ใช้เหล่านั้นใช้สิทธิ์ที่มีในการเข้าถึงระบบสารสนเทศแล้ว จะไม่สามารถปฏิเสธความรับผิดชอบได้หากทำให้ข้อมูลมีการเปลี่ยนแปลง หรือเสียหาย เนื่องจากระบบสารสนเทศสามารถเก็บหลักฐานจากการเข้าใช้สารสนเทศต่างๆ ได้

## 3. มาตรฐานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ มีความสำคัญต่อการปกป้องข้อมูลและทรัพย์สินขององค์กรซึ่งองค์กรจำเป็นต้องใส่ใจและให้ความสำคัญลำดับแรก [15] วิธีการที่จะทำให้ข้อมูลและทรัพย์สินขององค์กรปลอดภัยนั้นจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการต่างๆ เหล่านี้ได้ถูกกำหนดเอาไว้เป็นมาตรฐานสากลหลายมาตรฐานด้วยกัน องค์กรสามารถเลือกมาตรฐานที่เหมาะสมกับหน่วยงานของตน [5] โดยมาตรฐานเหล่านี้จะระบุรายละเอียดการดำเนินการของทรัพย์สินด้านความมั่นคงปลอดภัย และการพัฒนาระบบ การจัดทำเอกสาร นโยบาย มาตรฐาน ขั้นตอนปฏิบัติและแนวปฏิบัติ ซึ่งต้องยึดตามกรอบการเก็บรักษาข้อมูลไว้เป็นความลับ ความสมบูรณ์ของข้อมูล และความพร้อมใช้ของข้อมูล ประกอบด้วย

**3.1 มาตรฐาน ISO 27001: 2005**

มาตรฐานนี้เป็นมาตรฐานสากลที่ได้รับความนิยมสูงในการนำไปใช้สำหรับเป็นข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร [3] เรียกว่า ISMS หรือ Information Security Management System เป็นมาตรฐานที่มีไว้เพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่องไม่สะดุด ช่วยป้องกันกระบวนการทางธุรกิจจากภัยคุกคามความเสียหายของระบบข้อมูลได้ [5], [22] มาตรฐานนี้เป็นหนึ่งในมาตรฐาน ISO ตระกูล 27000 ที่แบ่งเนื้อหาออกเป็น 11 หัวข้อ แต่ละหัวข้อประกอบด้วยวัตถุประสงค์รวมกันจำนวน 39 วัตถุประสงค์ และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยที่แตกต่างกัน รวมทั้งสิ้น 133 มาตรการ โดยมีหัวข้อสำคัญในมาตรฐานนี้ จำนวน 11 หัวข้อหลัก [5], [23], [24] ดังนี้

1) นโยบายความมั่นคงขององค์กร

2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

3) การบริหารจัดการทรัพย์สินขององค์กร

4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศองค์กร

7) การควบคุมการเข้าถึง

8) การจัดการ การหา และการบำรุงรักษาระบบสารสนเทศ

9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

11) การปฏิบัติตามข้อกำหนด

มาตรฐานนี้ได้ถูกจัดทำขึ้นโดยยึดตามแนวคิดของหลักการ PDCA (Plan-Do-Check-Act) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบ และมีการพัฒนาขึ้นอย่างต่อเนื่อง เริ่มต้นตั้งแต่การจัดตั้ง การนำระบบไปใช้ การดำเนินงาน การติดตามและวัดผล การทบทวน การบำรุงรักษาระบบ และ

การปรับปรุงพัฒนาระบบให้ดียิ่งขึ้น [8]

**3.2 มาตรฐาน ITIL**

ITIL หรือ Information Technology Infrastructure Library เป็นแนวทางปฏิบัติที่ว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยจากประเทศอังกฤษ The British Office of Government Commerce (OGC) มุ่งเน้นการพัฒนากระบวนการเพื่อรองรับการให้บริการต่อลูกค้าและธุรกิจเป็นหลัก เช่นการออกแบบ การติดตั้ง การกระจาย การดูแลรักษาและการปรับปรุง [5], [8], [21] ITIL เป็นแนวทางปฏิบัติที่ดีเยี่ยมในการบริหารจัดการด้าน IT Service ให้แก่ผู้บริโภคอย่างเปี่ยมคุณภาพ แนวทางปฏิบัตินี้เหมาะกับองค์กรไม่ว่าจะขนาดเล็กหรือใหญ่ โดยเฉพาะอย่างยิ่งองค์กรที่เน้นเรื่องของการบริการด้าน IT Service

**3.3 มาตรฐาน FIPS PUB 200**

FIPS PUB 200 หรือ The Federal Information Processing Standards Publication 200 กล่าวถึงเรื่องของข้อกำหนดขั้นต่ำสำหรับความต้องการด้านความมั่นคงปลอดภัย ซึ่งเป็นภาคบังคับขององค์กรบริหารจัดการสารสนเทศและระบบสารสนเทศกลางของประเทศสหรัฐอเมริกา ทุกองค์กรที่เป็นหน่วยงานภาครัฐจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยนี้เป็นอย่างน้อย โดยมาตรฐานนี้ จะมีการระบุประเภทของระบบสารสนเทศต่างๆ และวิธีปฏิบัติที่จำเป็นสำหรับควบคุม เพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศในระบบนั้นๆ โดยมีเนื้อหาโดยสรุปของมาตรฐานนี้ [8] ได้แก่

1) การระบุข้อกำหนดขั้นต่ำของระบบประมวลผลสารสนเทศขององค์กรกลางในประเทศสหรัฐอเมริกา

2) การจัดทำข้อกำหนดนี้เพื่อสนับสนุนการพัฒนา

3) การลงมือปฏิบัติ

4) การดำเนินการ เพื่อสร้างความมั่นคงปลอดภัยระบบสารสนเทศ โดยหน่วยงานสามารถคัดเลือกเฉพาะส่วนที่เกี่ยวข้องกับองค์กรของตนมาปฏิบัติตาม มาตรฐานนี้จึงได้มีการจัดทำแนวทางในการคัดเลือก และกำหนดมาตรการด้านความมั่นคงปลอดภัยที่จำเป็นและเหมาะสมสำหรับระบบประมวลผลสารสนเทศของแต่ละหน่วยงาน

**3.4 มาตรฐาน NIST 800 – 14**

NIST 800-14 หรือ National Institute of Standards and Technology 800-14 เป็นมาตรฐานที่ได้รับการพิมพ์เผยแพร่จากสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา มาตรฐานนี้เป็นเกณฑ์กลางที่ได้รับการจัดทำและเผยแพร่ขึ้นเพื่อเสริมสร้างองค์กรที่ใช้ระบบสารสนเทศให้นำมาตรฐานเทคโนโลยีที่ได้จัดพิมพ์นี้ไปใช้ เพื่อเสริมสร้างความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศขององค์กรหรือหน่วยงานต่างๆ ในประเทศสหรัฐอเมริกาให้มากที่สุด ทั้งนี้เพื่อเป็นการป้องกันภัยคุกคามด้านอาชญากรรมคอมพิวเตอร์และการละเมิดความมั่นคงปลอดภัยข้อมูลสารสนเทศ โดยเฉพาะอย่างยิ่ง สารสนเทศบนระบบโครงสร้างพื้นฐานของประเทศ โดยเนื้อหาของ NIST 800-14 เป็นกฎเกณฑ์พื้นฐานด้านความมั่นคงปลอดภัยคอมพิวเตอร์ มีแนวทางในการปฏิบัติอยู่ด้วยกัน 8 แนวทาง [8], [25]

1) ในพันธกิจขององค์กรต้องให้การสนับสนุนเรื่องความมั่นคงปลอดภัยคอมพิวเตอร์

2) ในการบริหารจัดการขององค์กรต้องผนวกเรื่องของความมั่นคงปลอดภัยปลอดภัยคอมพิวเตอร์ไว้เป็นสาระสำคัญ

3) ควรมีการลงทุนที่เหมาะสมในเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์

4) เจ้าของระบบต้องแสดงรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยของระบบโดยตลอด

5) ความรับผิดชอบและการดูแลเอาใจใส่ในเร่องของความมั่นคงปลอดภัยคอมพิวเตอร์ต้องได้รับการดำเนินการอย่างชัดเจน

6) การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ต้องการแนวทางที่ผสมผสานในวิธีปฏิบัติ

7) ความมั่นคงปลอดภัยคอมพิวเตอร์ต้องได้รับการปรับปรุงให้ดีขึ้นอย่างต่อเนื่องและสม่ำเสมอ

8) ปัจจัยแวดล้อมสามารถส่งผลต่อการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ได้เสมอ

**3.5 มาตรฐาน IT BPM**

IT BPM หรือ Information Technology Baseline Protection Manual เป็นการรักษาความมั่นคงปลอดภัยระบบอย่างมีมาตรฐาน โดยจะจัดทำเฉพาะระบบสารสนเทศที่มีใช้ในองค์กรทั่วไป อาทิ ระบบสารสนเทศเกี่ยวกับบุคลากรขององค์กร ระบบสารสนเทศสำหรับสื่อสารด้วยไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น ซึ่งเนื้อหา IT BPM ประกอบด้วย [8]

1) ระบบต้องมีการบริหารจัดการด้านความมั่นคง

ปลอดภัยตั้งแต่ขั้นการออกแบบ ประสานงานและติดตามสถานะของความมั่นคงปลอดภัยของระบบที่เกี่ยวกับหน้าที่งานนั้น

2) ระบบต้องมีการวิเคราะห์และจัดทำเป็นเอกสารเกี่ยวกับโครงสร้างที่มีอยู่ของทรัพย์สินที่เป็นเทคโนโลยีสารสนเทศในองค์กร

3) ระบบต้องได้รับการประเมินถึงมาตรการและระบบบริหารจัดการด้านความมั่นคงปลอดภัยเดิม ที่ได้จัดทำไว้แล้วนั้น ว่ามีประสิทธิภาพเพียงพอและเหมาะสมแล้วหรือยัง

4) องค์กรต่างๆ สามารถนำโครงสร้างของเครือข่ายที่มีความมั่นคงปลอดภัย ซึ่งได้ออกแบบไว้ เหมาะสมแล้วตามคู่มือนี้มาเป็นแนวทางในการจัดทำเครือข่ายขององค์กร

5) ระบบต้องได้รับการดำเนินการปรับปรุงแก้ไขกรณีที่พบว่ามาตรการหรือแนวทางการรักษา ความมั่นคงปลอดภัยเหล่านั้นไม่เพียงพอ หรือมีการดำเนินการบางอย่างที่ยังไม่รัดกุม

**3.6 มาตรฐาน COBIT**

มาตรฐาน COBIT หรือ Control Objective for Information and related Technology เป็นทั้งแนวคิดและแนวทางการปฏิบัติ เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจแบ่งได้เป็น 4 กระบวนการหลัก ได้แก่

1) การวางแผนและการจัดการองค์กร

2) การจัดหาและติดตั้ง

3) การส่งมอบและบำรุงรักษา

4) การติดตามผล

โดยในแต่ละกระบวนการหลักข้างต้น จะมีวัตถุประสงค์ของการควบคุมหลักถึง 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง รวมถึง 318 หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบสำหรับแต่ละหัวข้ออีกด้วย

**3.7 มาตรฐาน COSO**

COSO หรือ The Committee of Sponsoring of the Treadway Commission เป็นกรอบปฏิบัติที่ช่วยส่งเสริมให้การตรวจสอบกิจการภายในองค์กรมีความเที่ยงตรงและโปร่งใส โดยเฉพาะองค์กรทางด้านการเงิน เพื่อให้เกิดความน่าเชื่อถือ ความถูกต้องเป็นไปตามหลักความเป็นจริง [5] และยังช่วยให้ผู้บริหาร กรรมการ หน่วยงานกำกับดูแลและหน่วยงานศึกษาได้มีข้อมูลความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงขององค์กร ประโยชน์ และข้อจำกัดของการบริหารความเสี่ยงดียิ่งขึ้น [26] โดย COSO มีองค์ประกอบ 5 องค์ประกอบหลัก [27] ดังนี้

1) การควบคุมสภาพแวดล้อม

2) การประเมินความเสี่ยง

3) การควบคุมการดำเนินงานหรือกิจกรรมต่างๆ

4) เทคโนโลยีสารสนเทศและการสื่อสาร

5) การติดตามผล

## 4. ผลการสังเคราะห์เนื้อหาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากมาตรฐานสากล

ตารางที่ 1 เป็นผลจากการสังเคราะห์เนื้อหาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศผ่านการสังเคราะห์และเปรียบเทียบแนวทางปฏิบัติของมาตรฐานสากล 7 มาตรฐาน ได้แนวทางปฏิบัติ 10 แนวทาง ประกอบด้วย

1) การกำหนดแผนกลยุทธ์ พันธกิจ นโยบาย และเป้าหมายการดำเนินงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

2) การกำหนดโครงสร้าง การบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานภายนอก

3) การวางแผน วิเคราะห์การลงทุนและการจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศ

4) การบริหารและพัฒนาทรัพยากรบุคคลด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

5) การระบุและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

6) การป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อมจากภายในและภายนอกองค์กร

7) การจัดหา การพัฒนา และการบำรุงรักษาระบบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

8) การบริหารความต่อเนื่อง การจัดการปัญหาและการเปลี่ยนแปลงด้านความมั่นคงปลอดภัยทางเทคโนโลยี

สารสนเทศ

9) การปฏิบัติตามข้อกำหนด ระเบียบ พระราชบัญญัติ กฎหมาย และบทลงโทษด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

10) การติดตาม ประเมินและรับรองกระบวนการทำงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

**5. บทสรุป**

การสังเคราะห์เนื้อหามาตรฐานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศในครั้งนี้เห็นว่าแต่ละมาตรฐานมีแนวทางการปฏิบัติเพื่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ไม่เหมือนกัน เนื่องจากการให้ความสำคัญและจุดเน้นด้านความมั่นคงปลอดภัยที่แตกต่างกันออกไป

ISO 27001 เป็นมาตรฐานที่มีแนวทางปฏิบัติครบทั้ง 10 แนวทาง เป็นมาตรฐานที่ได้รับการยอมรับและนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในองค์กรทั่วโลก จากรายงานของ ISMS International User Group มีองค์กรมากกว่า 7,346 แห่งนำไปใช้และได้รับการรับรองแล้ว ประเทศไทยมีองค์กรผ่านการรับรองจากมาตรฐานนี้แล้ว 41 แห่ง ในขณะที่ COBIT เป็นมาตรฐานที่มีจำนวนแนวทางปฏิบัติที่ใกล้เคียงกับ ISO 27001 คือ 9 แนวทาง ยกเว้นแนวทางการป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อมจากภายในและภายนอกองค์กร หรือการป้องกันการเขาถึงทางกายภาพโดยไม่ได้รับอนุญาต เช่น การกำหนดและจัดทำบริเวณล้อมรอบเพื่อป้องกันการเกิดความเสียหาย การถูกขโมย การควบคุมการเข้าออกของบุคคล การจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ เช่น ไฟไหม้ แผ่นดินไหว เป็นต้น และมาตรฐานที่มีแนวทางปฏิบัติน้อยที่สุด ได้แก่ มาตรฐาน IT BPM เนื่องจากมาตรฐานนี้เป็นการ

***ตารางที่ 1*** *การสังเคราะห์เนื้อหาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากมาตรฐานสากล*

| แนวทางปฏิบัติ | | มาตรฐานสากล | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ISO/IEC 27001 | COBIT | ITIL | COSO | FIPS PUB200 | NIST 800-14 | IT BPM |
| 1 | กำหนดแผนกลยุทธ์ พันธกิจ นโยบาย และเป้าหมายการดำเนินงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| 2 | กำหนดโครงสร้าง การบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานภายนอก | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| 3 | วางแผน วิเคราะห์การลงทุนและการจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| 4 | การบริหารและพัฒนาทรัพยากรบุคคลด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | ✓ | | ✓ | | |
| 5 | ระบุและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | | ✓ | ✓ | | |
| 6 | การป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อมจากภายในและภายนอกองค์กร | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| 7 | การจัดหา การพัฒนา และการบำรุงรักษาระบบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| 8 | การบริหารความต่อเนื่อง การจัดการปัญหาและการเปลี่ยนแปลงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | ✓ | | | ✓ | |
| 9 | ปฏิบัติตามข้อกำหนด ระเบียบ พระราชบัญญัติ กฎหมาย และบทลงโทษด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | | | | ✓ | |
| 10 | ติดตาม ประเมินและรับรองกระบวนการทำงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ | ✓ | ✓ | | ✓ | | ✓ | ✓ |

กำหนดมาตรฐานขั้นต่ำที่องค์กรควรจะปฏิบัติ โดยเฉพาะระบบสารสนเทศที่มีใช้ในองค์กร เช่น ระบบสารสนเทศบุคลากร ระบบการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์ เป็นต้น แต่อย่างไรก็ตามมาตรฐานนี้มีการปรับปรุงข้อมูลของมาตรฐานใหม่ทุกๆ 6 เดือน ทำให้แนวทางในการปฏิบัติเพิ่มขึ้นตามไปด้วย

ผลจากการสังเคราะห์เนื้อหาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศตามมาตรฐานสากล เป็นอีกแนวทางหนึ่งที่องค์กรสามารถนำมาเป็นข้อมูลในการตัดสินใจได้อย่างรวดเร็วมากขึ้นในการเลือกมาตรฐานที่เหมาะสมตามความจำเป็นเพื่อการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ

**6. เอกสารอ้างอิง**


[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, *แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) พ.ศ. 2552-2556*, 2552.

[2] แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 10 พ.ศ. 2550-2554.

[3] สานนท์ ฉิมมณี และ ภส จันทรศิริ, *เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร ICT ไทยระยะที่ 1 หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ระดับที่ 3*, กรุงเทพฯ: สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2553.

[4] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, *รายงานการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2551*, กรุงเทพฯ, 2552.

[5] ธวัชชัย ชมศิริ, *ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์*, กรุงเทพฯ: บริษัท โปรวิชั่น จำกัด, 2553

[6] P. Jokela and P. Karlsudd, "Learning with Security," *Journal of Information Technology Education*, V.6, 2007.

[7] ยืน ภู่วรวรรณ, *ความสำคัญของการจัดทำแนวนโยบายและแนวปฏิบัติในการรรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภาครัฐ*, เอกสารประกอบการบรรยายสำหรับคณะอนุกรรมการความมั่นคงปลอดภัย.

[8] เศรษฐพงค์ มะลิสุวรรณ, "การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ," [Online]. [cited 22 November 2010] Available from:http://www.our-teacher.com/our-teacher/Military%20Mentorship/20-IT%20Risk%20Management.pdf.

[9] Symantec enterprise security, "Symantec Global Internet Security Threat Report Trends for 2008," 2009. [Online]. [cited 2010 November 22] Available from: http://eval.symantec .co/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008. en-us.pdf.

[10] C. Pfleeger, and S. fleeger, *Security in Computer 4th edition*. Prentice Hall, 2006. [Online]. [cited 22 November 2010] Available from:htttp://www.informit.com/articles/article.aspx?p=680830&seqNum=3.

[11] M. Bishop, *Computer Security Art and Science*, Addison-Wesley Professional, 2002.

[12] พนิดา พานิชกุล, *ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ*, กรุงเทพฯ: บริษัท เคทีพี แอนด์ คอนซัลท์ จำกัด, 2553.

[13] M. Wilson and J. Hash, *Building an Information Technology Security Awareness and Training Program*, Gaithersburg: National Institute of Standards and Technology, 2003.

[14] S. Gary, G. Alice & F. Alexis, "Risk Management Guide for Information Technology Systems," *Gaitherburg & Falls Church: National Institute of Standards and Technology*, 2002.

[15] The Government of the Hong Kong Special Administrative Region, *An Overview of Information Security Standards*, 2008.

[16] บรรจง หะรังสี และ ดวงกมล ทรัพย์พิทยากร, *พัฒนาการมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศในภูมิภาคเอเชียแปซิฟิก*. กรุงเทพฯ: วารสาร NECTEC Security. พฤษภาคม-มิถุนายน 2549, 2549.

[17] ดวงกมล ทรัพย์พิยากร, *มาตรฐาน แนวทางปฏิบัติและกรอบวิธีปฏิบัติต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยี*

*สารสนเทศ*, กรุงเทพฯ: ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2550.

[18] ปริญญา หอมเอนก, "มาตรฐานสากลทางด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ CIO ควรรู้เพื่อนำมาใช้เป็นแนวทางปฏิบัติในองค์กร และ กลยุทธ์ CIO กับการบริหารระบบความปลอดภัยเทคโนโลยีสารสนเทศในองค์กรสมัยใหม่," *วารสาร eLeader Thailand กันยายน* 2548, 2548.

[19] J. Clinch., *ITIL V3 and Information Security*, Clinch Consulting, 2009.

[20] M. Gasser., *Building a Security Computer System*, New York: Van Nostrand Reinhold, 1988.

[21] สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ, *เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร* ICT *ไทย ระยะที่ 2 หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ระดับที่ 3*, ปทุมธานี: สำนักพิมพ์มหาวิทยาลัยกรุงเทพ, 2553.

[22] กิตติพงษ์ เกียรตินิยมรุ่ง, "ระบบมาตรฐานด้านความปลอดภัยของข้อมูล ISO 27001," TUV Rheinland Thailand. [Online]. [cited 2010 November 22] Available from http://www.tuv.com/th/_iso_27001.html

[23] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, *มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550*, กรุงเทพฯ: หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ, 2550.

[24] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, *ร่างแนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ*. กรุงเทพฯ: ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย, 2552.

[25] M. Swanson, and B. Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems. U.S. Department of Commerce*. National Institute of Standards and Technology, 1996.

[26] ตลาดหลักทรัพย์แห่งประเทศไทย, "COSO Enterprise Risk Management Framework".