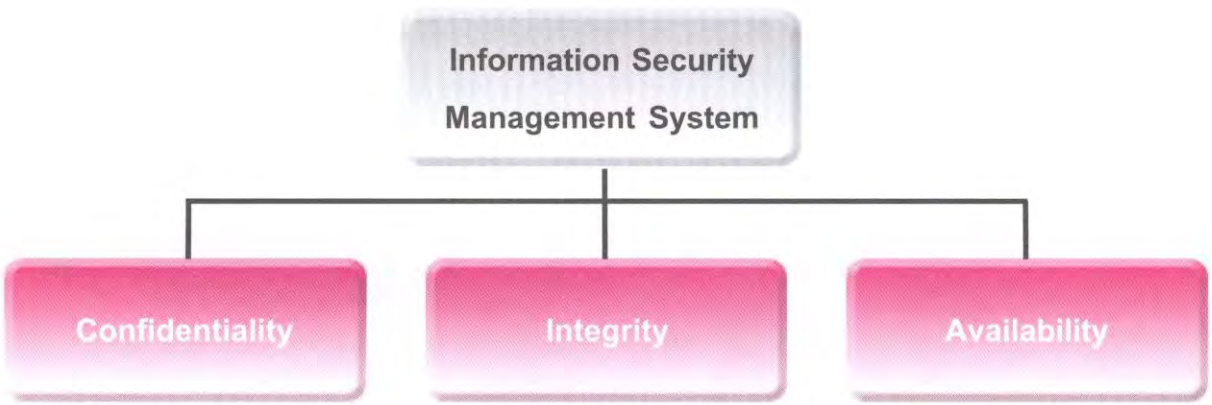
ระบบมาตรฐานบริหารความปลอดภัยของข้อมูลสารสนเทศ

พรพรรณ ปานทิพย์อำพร

ปัจจุบันจะเห็นได้ว่าเรื่องของข้อมูลข่าวสารขององค์กรเป็นเรื่องที่มีความสำคัญมาก และในทุกวันนี้องค์กรต่างๆ ก็ได้นำระบบสารสนเทศมาใช้ในการเก็บรักษาข้อมูลกันเป็นส่วนใหญ่ คงจะเคยได้ยินกันอยู่บ่อยครั้งว่าการสื่อสารระหว่างกันในโลกอิเล็กทรอนิกส์ถูกคุกคามโดยภัยอันตรายต่างๆ มากมาย มีการแฮคหรือการโจรกรรมข้อมูล เพื่อลักลอบดูและนำข้อมูลไปใช้ในทางที่ไม่ดี เพื่อเป็นการแก้ไขปัญหาที่กำลังเกิดขึ้นนี้ให้หมดสิ้นไป จึงจำเป็นที่จะนำมาตรฐาน ISO/IEC 27001:2005 มาปรับและประยุกต์ใช้ซึ่งจะช่วยป้องกันเหตุการณ์ดังกล่าวไม่ให้เกิดขึ้น นอกจากนั้นยังช่วยส่งผลทำให้ระบบงานทางด้านสารสนเทศมีประสิทธิภาพและมีความเป็นสากลมากขึ้น

มาตรฐาน ISO/IEC 27001:2005 (Information Security Management System : ISMS) เป็นมาตรฐานที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ โดยเนื้อหาสาระจะเกี่ยวข้องกับการจัดตั้งระบบการจัดการด้านความปลอดภัยของข้อมูลขึ้นในองค์กร ซึ่งจะมีการกำหนดข้อกำหนดเกี่ยวกับการจัดทำระบบเพื่อให้ข้อมูลมีความมั่นคงปลอดภัย ภายใต้วัตถุประสงค์ในการนำองค์กรไปสู่การเป็นเป็นองค์กรที่มีระบบบริหารจัดการภายในและระบบบริหารความมั่นคงสารสนเทศที่ดี นอกจากนั้นยังนำไปสู่การให้บริการแก่ผู้ใช้บริการได้อย่างมีประสิทธิภาพเป็นที่ยอมรับในระดับสากล

มาตรฐาน ISO/IEC 27001:2005 เป็นระบบการจัดการความปลอดภัยของข้อมูล โดยมีวัตถุประสงค์ในการรักษาไว้ซึ่ง

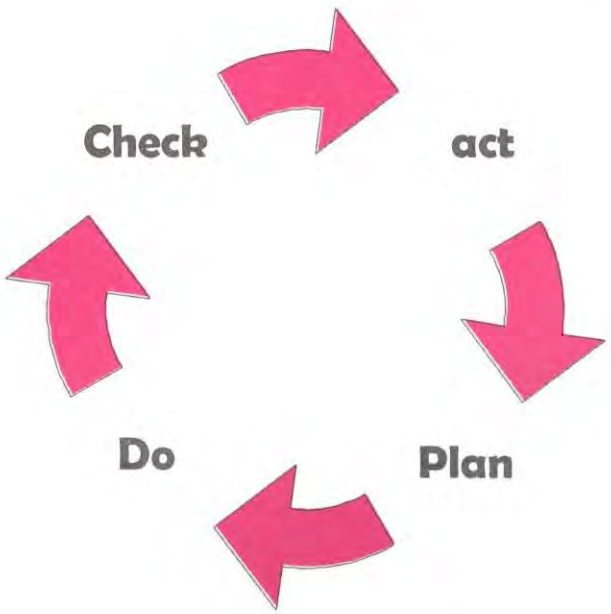


1. ความลับ (Confidentiality) ต้องมีการเก็บรักษาความลับของข้อมูลต่างๆ ที่มีอยู่ภายในองค์กร ซึ่งในทางปฏิบัติมีอยู่หลายวิธีด้วยกัน เช่น มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลต่างๆ ขององค์กร โดยให้ผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลได้

2. ความถูกต้องครบถ้วน (Integrity) ข้อมูลขององค์กรต้องมีความสมบูรณ์และถูกต้องอยู่เสมอ ดังนั้นองค์กรจึงต้องมีการกำหนดมาตรการในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อไม่ให้เกิดความผิดพลาดขึ้นกับข้อมูลขององค์กร

3. ความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ ผู้ที่มีสิทธิ์เข้าถึงข้อมูลต้องสามารถเข้าถึงข้อมูลได้เมื่อต้องการและต้องเป็นไปอย่างต่อเนื่อง

มาตรฐานความมั่นคงและความปลอดภัยทางด้านสารสนเทศมีจุดเริ่มต้นที่กระบวนการประเมินความเสี่ยง การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยภายในองค์กร รวมไปถึงการออกมาตรการเพื่อให้บุคคลในองค์กรตระหนักถึงความสำคัญและนำไปปฏิบัติตาม โดยใช้หลักการ Plan-Do-Check-Act (PDCA Model)



รูปภาพแสดง PDCA Model

1. Plan การจัดทำระบบ ISMS เป็นการจัดทำนโยบายความมั่นคงปลอดภัยของสารสนเทศให้มีเป้าหมาย วัตถุประสงค์ ขั้นตอนที่เกี่ยวข้องกับการบริหารความเสี่ยง

2. Do ประยุกต์ใช้และดำเนินการระบบ ISMS เป็นการดำเนินการและปฏิบัติตามนโยบายที่ได้กำหนดไว้

3. Check เป็นการเฝ้าระวังและตรวจสอบระบบ ISMS พร้อมทั้งการประเมินผล

4. Act รักษาและปรับปรุงระบบ ISMS เป็นการแก้ไขและดำเนินการปรับปรุงเชิงป้องกัน

ระบบการจัดการ ISMS นั้นเป็นระบบการจัดการภายใต้ความเสี่ยงที่ยอมรับได้ในระดับหนึ่ง ไม่ใช่เป็นการทำให้ระบบไม่มีความเสี่ยงเกิดขึ้นเลย โดยส่วนใหญ่มักจะมีการใช้ร่วมกันกับระบบ ISO/IEC 17799:2005 เป็นหลักในการปฏิบัติ เพื่อสร้างความมั่นใจว่าข้อมูลยังถูกเก็บรักษาอยู่อย่างครบถ้วนและอยู่ในสภาพที่ปลอดภัย ทำให้เกิดประสิทธิภาพมากขึ้นในการดำเนินงาน สร้างความน่าเชื่อถือทางด้านความมั่นคงปลอดภัยให้กับการให้บริการและเพิ่มขีดความสามารถให้กับองค์กรได้ต่อไปในอนาคต

เอกสารอ้างอิง

1. ISO 27001 2005 [ออนไลน์] [อ้างถึงวันที่ 17 มกราคม 2551] เข้าถึงได้จาก:
http://www.praxiom.com/iso-27001-intro.htm