ISO/IEC 27001:2013 - Information security management systems

มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) เป็นมาตรฐานการจัดการข้อมูลที่สำคัญ เพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง กำหนดขึ้นโดยองค์การระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย โดยแบ่งเนื้อหาออกเป็น 14 หัวข้อใหญ่ๆ (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 35 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกันรวมแล้ว 114 ข้อ ซึ่งสามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กร

มาตรฐาน ISO/IEC 27001: 2013 ว่าด้วยเรื่องของข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS ให้กับองค์กร ซึ่งมีหัวข้อที่เกี่ยวข้องคือ

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

มาตรฐาน ISO/IEC 27001 นี้ ปัจจุบันได้รับความนิยมอย่างแพร่หลาย เนื่องจากประกอบด้วยวงจร Plan-Do-Check-Act และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

การประยุกต์ใช้ ISMS (Information Security Management System) จะช่วยให้กิจกรรมทางธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง ช่วยป้องกันระบบข้อมูลสารสนเทศขององค์กรจากความเสี่ยงต่อภัยคุกคามต่างๆ เช่น การหลอกลวงทางคอมพิวเตอร์ การจารกรรมข้อมูล ไวรัสจากคอมพิวเตอร์ การเจาะเข้าโปรแกรมคอมพิวเตอร์และการโจมตีเข้าระบบ นอกจากนี้ยังช่วยป้องกันกระบวนการทางธุรกิจจากเกิดการหยุดชะงักอันเกิดจากภัยร้ายแรงต่างๆ เช่น แผ่นดินไหว วาตภัย อัคคีภัย อุทกภัย เป็นต้น

สถานะปัจจุบันของมาตรฐานคือได้ประกาศใช้ตั้งแต่เดือนตุลาคม 2013 โดยสาระสำคัญของการปรับปรุงสามารถสรุปได้ดังนี้

- โครงสร้างมาตรฐานมีการปรับเปลี่ยนให้สอดคล้องกับภาคผนวก SL ของ ISO/IEC Directives เพื่อให้มีโครงสร้างมาตรฐานเป็นไปในทิศทางเดียวกับมาตรฐานระบบการจัดการอื่นๆ (กล่าวคือหัวข้อ 4-10 ในข้างต้นเป็นหัวข้อเดียวกับที่ปรากฏในมาตรฐานระบบการจัดการอื่นๆ)
- ผู้มีส่วนได้เสีย ในมาตรฐานฉบับนี้ มีการกำหนดให้มีการชี้บ่งผู้มีส่วนได้เสีย ซึ่งครอบคลุมถึงผู้ถือหุ้น หน่วยงานผู้มีอำนาจทางกฎหมาย ลูกค้า คู่ค้า เป็นต้น
- ระบบบริหารจัดการเอกสารและบันทึก (Document control and record control) ถูกรวบเข้าเป็นหัวข้อเดียวกัน (เดิมแยกออกจากกัน)
- การประเมินและจัดการความเสี่ยงใช้หลักการประเมินความเสี่ยงที่อ้างอิงไปยังมาตรฐาน ISO/IEC 31000:2009 แต่ยังคงใช้เกณฑ์ในมาตรฐานฉบับเดิมได้
- การกำหนดวัตถุประสงค์ของการดำเนินการและการจัดทำแผนงานเพื่อบรรลุวัตถุประสงค์
- การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน มีการระบุผู้รับผิดชอบ อะไรที่จำเป็นต้องเฝ้าระวังและวัดผล วิธีการในการเฝ้าระวังและวิเคราะห์ผล เมื่อไรต้องดำเนินการ ใครจะเป็นผู้วิเคราะห์และประเมินผล
- การปฏิบัติการแก้ไขความไม่สอดคล้องได้ตัดเนื้อหาส่วนของการปฏิบัติการป้องกัน (Preventive actions) เพราะถือเป็นส่วนหนึ่งของการประเมินและจัดการความเสี่ยงด้วย
- การสื่อสาร ได้กำหนดหัวข้อการสื่อสารอย่างชัดเจน (มาตรฐานเดิมมีแต่ไม่ชัดเจน) กล่าวคือ กำหนดให้มีการสื่อสารข้อมูลที่จำเป็นในระบบ ISMS ได้แก่ อะไรบ้างที่ต้องสื่อสารให้ทราบ เมื่อไรที่ต้องสื่อสารให้ทราบ ใครบ้างที่ต้องสื่อสารให้ทราบ ใครเป็นผู้สื่อสารออกไป และ กระบวนการที่เกี่ยวข้องกับการสื่อสาร

Standard Warning System ของมาตรฐานนี้ คือ

การวิเคราะห์ผลกระทบของมาตรฐานที่จะส่งผลต่อผู้ประกอบการไทย

- สาขาอุตสาหกรรมที่ได้รับผลกระทบ ได้แก่ มาตรฐานนี้สามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภท เช่น ภาคการค้า หน่วยงานภาครัฐ และองค์กรไม่แสวงหากำไร
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้น เมื่อพิจารณาจากปัจจัยต่างๆ ทางธุรกิจและผู้อุปโภคบริโภค พบว่าอยู่ในระดับการเตือนภัยที่ยอมรับได้ ซึ่งเป็นผลมาจาก
  - มาตรฐานนี้ประกาศใช้แล้ว
  - ผลกระทบกับผู้ประกอบการ ยังอยู่ในระดับต่ำ เนื่องจากยังเป็นมาตรฐานภาคสมัครใจ ยังไม่ได้รับแรงกดดันให้ต้องปรับตัวเข้าสู่มาตรฐาน
  - สำหรับการเตรียมความพร้อมของไทยเพื่อการปรับตัวให้เข้าสู่มาตรฐาน ในส่วนของภาครัฐมีการกำหนดให้จัดทำนโยบายความมั่นคงปลอดภัยด้านไอซีที รวมทั้งแผนแม่บทด้านความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติเพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของประเทศ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐาน ISO/IEC 27001 และหน่วยงานภาครัฐบางแห่งได้มีการนำมาตรฐานฉบับนี้มาประยุกต์ใช้ เช่น กสทช.
  - หากผู้ประกอบการจะปรับตัวเข้าสู่มาตรฐาน ในส่วนของหน่วยงานผู้ให้บริการมีครอบคลุมทั้ง หน่วยฝึกอบรมและให้คำปรึกษา และหน่วยรับรองที่สามารถให้บริการได้อย่างเพียงพอ

ผลการประเมินในแต่ละมุมมองผลกระทบมีรายละเอียดดังตาราง

มุมมองผลกระทบ	การวิเคราะห์	ระดับคะแนน (1 – 3)
1. ด้านผลกระทบต่อผู้ประกอบการ	มาตรฐานระบบการจัดการ ISO/IEC 27001 เป็นมาตรฐานประเภทสมัครใจ ดังนั้นหากไม่มีการนำไปใช้ในองค์กรก็ยังสามารถดำเนินธุรกิจต่อไปได้ แต่อย่างไรก็ตาม องค์กรควรมีการกำหนดนโยบายและแผนงานบริหารจัดการความมั่นคงปลอดภัยของข้อมูล เนื่องจากมาตรฐานดังกล่าวมีความจำเป็น เช่น เป็นความต้องการขององค์กรในการบริหารจัดการระบบสารสนเทศให้มีความมั่นคงปลอดภัยต่อการใช้งาน รวมทั้งความคาดหวังของลูกค้าที่ต้องการความเชื่อมั่นต่อระบบการรักษาข้อมูลที่ต้องการทำธุรกรรมผ่านคอมพิวเตอร์	1
2. ด้านระยะเวลา (Time) ที่จะประกาศใช้/บังคับใช้	ประกาศใช้มาตรฐานฉบับใหม่แล้ว เมื่อวันที่ 25/9/2013	3
3. ด้านความพร้อมในการปรับเข้าสู่การเปลี่ยนแปลง **(ประเมินเฉพาะความพร้อมในด้านนโยบายภาครัฐ หรืออุตสาหกรรมภาพรวม)**	เป็นมาตรฐานระบบการจัดการ และมีหน่วยรับรองที่เพียงพอสามารถให้บริการได้ สำหรับจำนวนผู้ได้รับการรับรองเริ่มมีจำนวนผู้ได้รับการรับรองเพิ่มมากขึ้น สำหรับการพัฒนามาตรฐานฉบับใหม่ พบว่าไม่ส่งผลกระทบต่อการปรับตัวเข้าสู่มาตรฐานใหม่ เนื่องจากมีการปรับเปลี่ยนในเชิงข้อกำหนดด้านระบบการจัดการให้สอดคล้องกับมาตรฐานเดิม และมาตรฐานระบบการจัดการอื่น ในส่วนของภาครัฐมีการกำหนดให้จัดทำนโยบายความมั่นคงปลอดภัยด้านไอซีที รวมทั้งแผนแม่บทด้านความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติเพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของประเทศ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐาน ISO/IEC 27001 นอกจากนั้น พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 5 ระบุให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคง	2

มุมมองผลกระทบ	การวิเคราะห์	ระดับคะแนน (1 – 3)
	ปลอดภัยและเชื่อถือได้ ทำให้หน่วยงานภาครัฐต่างต้องเริ่มดำเนินการและเตรียมความพร้อม ตาม พรฎ. ดังกล่าว	