จดหมายข่าว

เพื่อการเตือนภัยด้านมาตรฐาน

ภายใต้โครงการสร้างระบบข้อมูล และองค์ความรู้ด้านมาตรฐานระบบการจัดการและการเตือนภัย

ปีที่ 5 ฉบับที่ 38 เดือนมกราคม 2558

มาตรฐานการใช้บริการจากภายนอกองค์กร

ISO เชื่อมั่นในการปกป้องความเป็นส่วนตัวของคลาวด์ ตอนที่ 1

มาตรฐานระบบการจัดการในการต่อต้านการติดสินบน

ดัชนีเศรษฐกิจสีเขียวของโลก ปี 2014

ISSN 2228-9925

จดหมายข่าวเพื่อการเตือนภัยด้านมาตรฐาน

ภายใต้โครงการสร้างระบบข้อมูล และองค์ความรู้ด้านมาตรฐานระบบการจัดการและการเตือนภัย

ปีที่ 5 ฉบับที่ 38 เดือนมกราคม 2558

Management System Certification Institute (Thailand): MASCI
1025, 2nd 11th 18th Floor, Yakult Building,
Phaholyothin Road, Samsen Nai, Phayathai, Bangkok
10400, Thailand
Tel. (+662) 617-1727-36 Fax. (+662) 617-1708
www.masci.or.th

กอง บก. ขอกล่าวสวัสดีท่านผู้อ่าน "จดหมายข่าวเพื่อการเตือนภัยด้านมาตรฐาน" สำหรับบทความที่น่าสนใจประจำเดือนมกราคม 2558 ทีมงาน Intelligence Unit ได้สรุปบทความเกี่ยวกับมาตรฐานการใช้บริการจากภายนอกองค์กร และ ISO เชื่อมั่นในการปกป้องความเป็นส่วนตัวของคลาวด์ ตอนที่ 1 รวมถึง Standard Warning เกี่ยวกับ มาตรฐานระบบการจัดการในการต่อต้านการติดสินบน และบทวิเคราะห์เรื่อง ดัชนีเศรษฐกิจสีเขียวของโลก ปี 2014

สุดท้ายนี้ ขอขอบคุณสำนักงานเศรษฐกิจอุตสาหกรรมที่ให้การสนับสนุนงบประมาณดำเนินการโครงการสร้างระบบข้อมูลและองค์ความรู้ ด้านมาตรฐานระบบการจัดการ และการเตือนภัย หรือ Intelligence Unit

กอง บก.

มาตรฐานการใช้บริการจากภายนอกองค์กร (Outsourcing)

หลายๆ องค์กร มีการพัฒนาและปรับเปลี่ยนกลยุทธ์และแนวทางการบริหารจัดการธุรกิจเพื่อให้มีผลการดำเนินงานที่มีประสิทธิภาพและประสิทธิผลดีขึ้น ซึ่งแนวทางการดำเนินงานหนึ่งที่ถูกนำมาใช้มากขึ้น คือ การใช้บริการจากภายนอกองค์กร (Outsourcing) ในลักษณะการจัดหาจัดจ้างหน่วยงานภายนอกให้ดำเนินกิจกรรมใดกิจกรรมหนึ่งขององค์กร (อาจไม่ใช่กิจกรรมหลักขององค์กร หรือผู้รับจ้างมีความเชี่ยวชาญมากกว่า) หรืออีกนัยหนึ่ง คือ การขยายหรือย้ายฐานการผลิตและดำเนินการไปยังต่างประเทศที่มีต้นทุนต่ำกว่า

การใช้บริการจากภายนอกองค์กร (Outsourcing) มีข้อดี คือ ลดค่าใช้จ่ายจากการโอนงานให้ผู้เชี่ยวชาญที่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพมากกว่าไปดำเนินการแทน ทำให้สามารถใช้ทรัพยากรที่มีอยู่อย่างจำกัดไปพัฒนากิจกรรมหลักขององค์กร ไม่ต้องลงทุนในการจ้างบุคลากร ให้การฝึกอบรม จัดหาอุปกรณ์เทคโนโลยีสารสนเทศในการปฏิบัติงานสนับสนุนต่าง ๆ (Back Office Operations) และเป็นการบริหารความเสี่ยงขององค์กรด้วย

Deloitte ซึ่งเป็นบริษัทบัญชีและที่ปรึกษา ได้ทำการสำรวจเกี่ยวกับการใช้บริการจากภายนอกองค์กรและการดำเนินงานเองโดยบุคลากรภายในองค์กรทั่วโลก ปี 2014 (2014 Global Outsourcing and Insourcing Survey) พบว่า การใช้บริการจากภายนอกองค์กรและธุรกิจที่เกี่ยวข้องมีการขยายตัวและเติบโตมากขึ้น (Deloitte คาดการณ์ว่าการใช้บริการจากภายนอกองค์กรทั่วโลกจะขยายตัว 12% - 26%) โดยกิจกรรมที่มักจะใช้การบริการจากภายนอก เช่น เทคโนโลยีสารสนเทศ (Information Technology) งานด้านบุคลากร (Human Resource) การเงินและการบัญชี (Finance and Accounting) และการจัดซื้อจัดหา (Procurement)

คณะกรรมการวิชาการ ISO/PC 259 ของ ISO ได้พัฒนามาตรฐาน ISO 37500: 2014 ขึ้น ซึ่งเป็นแนวทางการใช้บริการจากภายนอกองค์กร เพื่อให้องค์กรทุกประเภท ทุกขนาด ได้นำไปใช้ ซึ่งประกอบด้วย คำศัพท์และคำนิยามที่เกี่ยวข้อง แนวคิดและรูปแบบของการใช้บริการจากภายนอกองค์กร ขอบข่ายการกำกับดูแลการใช้บริการจากภายนอกองค์กร และวงจรของการใช้บริการจากภายนอกองค์กร (ประกอบด้วย การวิเคราะห์กลยุทธ์การใช้บริการจากภายนอกองค์กร กระบวนการเริ่มต้นและการคัดเลือก รูปแบบการเปลี่ยนแปลง จากการดำเนินการเองไปสู่การใช้บริการจากภายนอกองค์กร (Transition) และการส่งมอบคุณค่าของการใช้บริการจากภายนอกองค์กร)

ที่มา : www.iso.org , www.deloitte.com , http://standardsforum.com/new-iso-37500-guidance-outsourcing/ และ http://cgbusinessconsulting.com/new-iso-standard-iso-375002014-outsourcing/

ISO เชื่อมั่นในการปกป้องความเป็นส่วนตัวของคลาวด์ ตอนที่ 1

แม้ว่ามีการใช้บริการเพิ่มมากขึ้น แต่ก็มีคนบางกลุ่มยังไม่มั่นใจที่จะใช้บริการคลาวด์ บางคนแย่ไปกว่านั้นอีก คือ ไม่ยอมใช้บริการคลาวด์เลย กลุ่มนี้จะอ้างว่าไม่มั่นใจในเรื่องของความปลอดภัยและการปกป้องความเป็นส่วนตัว ทั้งนี้ จากการสำรวจในระดับโลกของบีทีเมื่อปีที่แล้ว พบว่าความปลอดภัยด้านข้อมูลและความเชื่อถือในบริการที่ใช้คลาวด์ เป็นสาเหตุของความไม่สบายใจเป็นอย่างมากสำหรับผู้ที่ทำหน้าที่ตัดสินใจในองค์กรใหญ่ๆ มีผู้ตอบแบบสำรวจถึง 76 % ที่ตอบว่าให้ความสนใจหลักในเรื่องความปลอดภัยเมื่อใช้บริการที่ใช้คลาวด์

ถึงแม้ว่าผู้ตอบแบบสำรวจ 79 % ในสหรัฐอเมริกายังคงใช้บริการจัดเก็บข้อมูลบนคลาวด์และเว็บแอพพลิเคชั่นกับธุรกิจของตนเอง แต่ก็เป็นที่เห็นได้อย่างชัดเจนว่าความเชื่อมั่นในความปลอดภัยบนคลาวด์อยู่ในระดับต่ำมาก

ความกังวลดังกล่าวเป็นที่เข้าใจได้ แต่ก็มีการกล่าวกันจนเกินจริงไปบ้าง มาเรีย-มาร์ตินา ยาลาโมว่า (Maria-Martina Yamalova) ผู้เชี่ยวชาญด้านกฎหมายเกี่ยวกับคลาวด์คอมพิวติ้งของบริษัทโควิงตั้นแอนด์ เบอร์ลิ่ง (Covington & Burling) กล่าวว่า บ่อยครั้ง ผู้ให้บริการคลาวด์ที่มีชื่อเสียงได้ยื่นข้อเสนอด้านความปลอดภัยให้มากเกินกว่าที่บุคคลหรือองค์กรและบริษัทต่างๆ จะสามารถทำได้ด้วยตนเอง ผู้ให้บริการเหล่านี้ลงทุนในทรัพยากรที่สำคัญในการสร้างความมั่นใจว่าระบบของพวกเขาจะสามารถใช้ประโยชน์ในการวัดด้านความปลอดภัยได้สูงสุด โดยมีการทำการทดสอบแบบสุดโต่ง และทำให้ระบบมีความเข้มแข็งอยู่เป็นประจำอย่างสม่ำเสมอ หลายบริษัทได้ปฏิบัติตามมาตรฐานความปลอดภัยในระดับสากลและต้องปฏิบัติตามกฎหมายเพื่อให้สามารถดูแลความปลอดภัยและความเป็นส่วนตัวในเรื่องข้อมูล นอกจากนี้ บริษัทเหล่านี้ยังยื่นข้อเสนอให้ลูกค้าสามารถควบคุมระดับความเป็นส่วนตัว เพื่อปกป้องข้อมูลอีกด้วย ความจริงแล้ว เรื่องราวของคลาวด์ตอนนี้ก็เหมือนกับเรื่องราวของคอมพิวเตอร์พีซีในอดีตที่เคยมีความวิตกกังวลกันว่าระบบความปลอดภัยของมันจะทนทานกับสิ่งต่างๆ ที่ต้องเผชิญได้หรือไม่

ข้อเท็จจริงก็คือคลาวด์ถูกสร้างขึ้นมาอย่างเท่าเทียมกันและคุณภาพของการบริการและการสนับสนุนก็แตกต่างกันออกไปในผู้ให้บริการแต่ละผู้ให้บริการ

ปัญหาที่เกิดขึ้นกับคลาวด์ คือ ความเชื่อมั่น ดังนั้นการปรับปรุงให้เกิดความน่าเชื่อถือการพัฒนาคนและธุรกิจ จะช่วยให้มองเห็นถึงประโยชน์ของคลาวด์ คอมพิวติ้งมากขึ้น เช่น ค่าใช้จ่ายที่ถูกลง การปรับปรุงที่ดีขึ้นในเรื่องความสามารถในการขยายระบบเพื่อรองรับการใช้งานและเวลาที่ใช้ในการปฏิบัติงาน ระดับความเชื่อมั่นในลักษณะดังกล่าวจะเกิดขึ้นได้ก็ต่อเมื่อมีการพิจารณาในเรื่องชนิดของข้อมูลในตอนที่มีการวางแผนที่จะนำคลาวด์มาใช้

ศาสตราจารย์เอ็ดเวิร์ด ฮัมฟรีส์ ผู้วางแผนและเตรียมการในกลุ่มปฏิบัติงานขององค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) ซึ่งรับผิดชอบมาตรฐานการบริหารจัดการความปลอดภัยของข้อมูล ซึ่งรวมถึงมาตรฐาน ISO/IEC 27001 (Information technology-Security techniques-Information security management systems-Requirement) และ ISO/IEC 27002 (Information technology-Security techniques-Code of practice for information security controls) และร่างมาตรฐาน ISO/IEC DIS 27017 (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services) ศาสตราจารย์เอ็ดเวิร์ดเชื่อว่าการสร้างบรรยากาศของความเชื่อถือเป็นสิ่งแรกที่สำคัญมากและจำเป็นต้องทำเมื่อจะทำการจ้างคนภายนอกเข้ามาดูแลระบบเทคโนโลยีสารสนเทศ และยังกล่าวว่า “บริษัทจำเป็นต้องมีความมั่นใจในการว่าจ้างผู้ให้บริการคลาวด์”

ผู้ใช้บริการบางรายอาจไม่เข้าใจว่าพวกเขาจำเป็นต้องเลือกผู้ให้บริการคลาวด์ที่มีธรรมาภิบาลที่ดีต่อกระบวนการในเรื่องข้อมูลส่วนบุคคลแต่ก็รู้ว่าการตรวจสอบนี้ไม่ใช่เรื่องง่ายนัก สถานการณ์นี้อาจนำไปสู่ความเสี่ยงที่เพิ่มขึ้นในการปกป้องข้อมูลส่วนบุคคล

ถ้าเป็นเช่นนั้นแล้ว เราจะทำอย่างไรดี ผู้ให้บริการคลาวด์ควรจะทำอย่างไร โปรดติดตาม ISO เชื่อมั่นในการปกป้องความเป็นส่วนตัวของคลาวด์ ตอนที่ 2 ซึ่งเป็นตอนจบ ในฉบับต่อไป

ที่มา: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref1921

Standard Warning

มาตรฐานระบบการจัดการในการต่อต้านการติดสินบน

ข้อมูลจากธนาคารโลก (World Bank) ประเมินว่ามีการจ่ายเงินเพื่อการติดสินบนกันสูงถึง 1 ล้านล้านเหรียญสหรัฐฯ ในแต่ละปี และประมาณการว่ามีองค์กรธุรกิจจำนวนกว่า 50% ที่มีการจ่ายเงินติดสินบนเพื่อรักษาธุรกิจของตนเอง ซึ่งการคอร์รัปชั่นหรือการติดสินบนนี้ถือเป็นภัยคุกคามที่มีนัยสำคัญต่อธุรกิจในหลายๆ ประเทศ และในหลายๆ อุตสาหกรรม ที่จะส่งผลกระทบต่อการเติบโตทางเศรษฐกิจและการลงทุนที่ลดลง อีกทั้งยังก่อให้เกิดความยากจนและความไม่เท่าเทียมกันในสังคมได้

สำหรับมาตรฐานระบบการจัดการ สามารถใช้เป็นเครื่องมือหนึ่งที่จะช่วยในการบริหารจัดการการต่อต้านคอร์รัปชั่น เช่น BS 10500:2011 Specification for an anti-bribery management system (ABMS) ซึ่งเป็นมาตรฐานของฝั่งสหราชอาณาจักร (UK) ที่พัฒนาขึ้นเพื่อให้สอดรับกับกฎหมาย คือ The UK Bribery Act 2010 ซึ่งเป็นกฎหมายว่าด้วยการป้องกันและปราบปรามการทุจริตคอร์รัปชั่น โดยมุมมองที่สำคัญของ BS 10500 มีดังนี้

- นโยบายการต่อต้านการติดสินบน (Anti-bribery policy)
- การสื่อสาร (Communication)
- การให้ความรู้ การฝึกอบรม และการแนะแนว (Education, training and guidance)
- ความรับผิดชอบในการปฏิบัติตาม (Responsibility for compliance)
- ทรัพยากรในการต่อสู้กับการติดสินบน (Resources to combat bribery)
- การประเมินความเสี่ยง (Risk assessment)
- การตรวจสอบวิเคราะห์สถานะธุรกิจ (Due diligence)
- ขั้นตอนการจ้างงาน (Employment procedures)
- นโยบายการให้ของขวัญ การต้อนรับ และการบริจาค (Gifts, hospitality, donations policies)
- การจ่ายเงินค่าอำนวยความสะดวก (Facilitation payments)
- การมอบหมายการตัดสินใจ (Delegated decision-making)
- การควบคุมสัญญา (Contractual controls)
- การควบคุมทางการเงิน (Financial controls)
- การควบคุมการจัดซื้อจัดจ้างและการค้า (Procurement and commercial controls)
- การเพิ่มความระมัดระวังให้มากขึ้น (Raising concerns: whistle-blowing arrangements)
- ขั้นตอนการสืบสวน (Investigation procedures)
- กระบวนการทางวินัย (Disciplinary procedures)

โดย Intelligence Team

- การตรวจสอบภายใน (Internal audit)
- การทบทวนของฝ่ายบริหาร (Top management overview and tone)

ส่วนมาตรฐานสากลที่อยู่ระหว่างการพัฒนา ISO 37001 Anti-bribery management systems ซึ่งน่าจะต่อยอดหรือมีบางส่วนที่สอดคล้องกับ BS 10500 โดย ISO 37001 เป็นมาตรฐานระบบการจัดการที่จะแสดงถึงแนวทางการปฏิบัติที่ดีเพื่อต่อต้านคอร์รัปชั่นที่สามารถนำไปประยุกต์ใช้ได้กับทุกองค์กร ซึ่งมาตรฐานนี้ถูกพัฒนาขึ้นโดยมีโครงสร้างสอดคล้องตามมาตรฐานระบบการจัดการอื่นๆ เช่น ISO 9001 และ ISO 14001

สถานะล่าสุดของ ISO 37001 ณ วันที่ 29 ตุลาคม 2557 คือ มาตรฐานฉบับร่างกรรมาธิการ (Committee Draft ; ISO/CD 37001) โดยคาดว่าน่าจะประกาศเป็นมาตรฐานสากลภายในปี 2559

ประโยชน์ของมาตรฐานทั้ง 2 ฉบับนี้ คือ จะช่วยแสดงให้เห็นว่าองค์กรมีการดำเนินงานตามตัวชี้วัดที่สมเหตุสมผลและเหมาะสมต่อการป้องกันการติดสินบน

ภาพจาก : www.iso.org

ที่มา :

- http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1916
- http://www.bsigroup.com/LocalFiles/en-GB/bs-10500/resources/BS-10500-Whitepaper-UK-EN.pdf
- http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030238856

ดัชนีเศรษฐกิจสีเขียวของโลก ปี 2014

รายงานเรื่องดัชนีชี้วัดเศรษฐกิจสีเขียว หรือ The Global Green Economy Index (GGEI) ได้เผยแพร่ครั้งแรกในปี 2010 เพื่อต้องการใช้เป็นเครื่องมือในการสื่อสาร เพื่อช่วยผู้กำหนดนโยบาย องค์กรระหว่างประเทศ และภาคเอกชนมีจุดอ้างอิงสำหรับผลการดำเนินงานของประเทศด้านเศรษฐกิจสีเขียว และการจัดอันดับผลการดำเนินงานในช่วงเวลาดังกล่าว ซึ่งจัดทำและเผยแพร่โดย Dual Citizen LLC ซึ่งเป็นหน่วยงานที่ปรึกษาด้านการพัฒนาองค์กรสากล

GGEI 2014 ครอบคลุมการสำรวจใน 60 ประเทศ (รวมถึงประเทศไทย) และ 70 เมือง โดยวัดจากผลการดำเนินงาน (Performance) ตามดัชนีชี้วัดใน 4 มิติ ดังภาพ และวัดจากการสำรวจความเห็นของผู้เชี่ยวชาญและผู้ที่เกี่ยวข้องในอุตสาหกรรม (Perception)

ผลการสำรวจดัชนีชี้วัดเศรษฐกิจสีเขียว สรุปผลที่น่าสนใจ คือ

- ประเทศที่มีอยู่ที่มีคะแนนดัชนีชี้วัดเศรษฐกิจสีเขียว (GGEI) สูงที่สุด คือ เยอรมัน (Performance) และสวีเดน (Perspective)
- อันดับเมืองสีเขียวที่มีคะแนนสูงสุด คือ โคเปนเฮเกน ซึ่งยังคงมีผลการดำเนินงานที่แข็งแกร่งอย่างต่อเนื่อง (เหมือนปี 2012) ส่วนอันดับรองลงมา คือ แวนคูเวอร์ และสิงคโปร์
- สำหรับการเข้าร่วมการสำรวจปี 2014 เป็นปีแรก คือ คอสตาริกา มีผลการดำเนินงาน (Performance) เป็นอย่างดีอยู่ในลำดับที่ 3 ถัดจากสวีเดนและนอร์เวย์ และได้รับการยอมรับอย่างมากในการสำรวจความเห็นของผู้เชี่ยวชาญฯ (Perception) ซึ่งเป็นที่น่าประทับใจสำหรับประเทศเล็กๆ นี้

ดัชนีชี้วัดเศรษฐกิจสีเขียวนี้ ถือเป็นข้อมูลพื้นฐานสำหรับประเทศต่างๆ ในการวางแผนและกำหนดนโยบายเพื่อการพัฒนาผลการดำเนินงานของประเทศและเศรษฐกิจให้มีระดับคะแนนสูงขึ้น ซึ่งเป็นส่วนหนึ่งของการพัฒนาประเทศไปสู่ความยั่งยืน

ที่มา:

- The Global Green Economy Index 2014, Dual Citizen LLC
- http://www.dualcitizeninc.com