โดย นายกษิภัท ธนิตรนาคุณ
คณะทำงานศูนย์ความรู้ด้านการสอบบัญชีในธุรกิจที่มีระบบ IT ที่ซับซ้อน ในคณะกรรมการวิชาชีพบัญชีด้านการสอบบัญชี
CISA, CDPSE, ISO 19011:2018 (Internal Auditor), ITIL (V.2, V.3),
IRCA – ISMS Auditor (ISO/IEC 27001:2013) and ISFS (ISO/IEC 27002:2005)

S.M.A.R.T CONTROLS
วัคซีนป้องกันภัยไซเบอร์

ตามที่ทุกท่านทราบปัจจุบันภัยไซเบอร์เพิ่มความรุนแรงขึ้นตลอดเวลาและกระจายไปทุกหย่อมหญ้า โดยเฉพาะภัยที่เกิดขึ้นกับข้อมูลทางการเงิน ซึ่งสร้างความปวดหัวให้กับทั้งนักบัญชีและผู้สอบบัญชีรวมถึงปัจจุบันหน่วยงานกำกับต่าง ๆ ก็มีการออกกฎหมาย ข้อกำหนด และมาตรฐานต่าง ๆ ที่ต้องปฏิบัติตาม เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรฐานการสอบบัญชี ประกาศของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และประกาศของธนาคารแห่งประเทศไทย (ธปท.) เป็นต้น ดังนั้นผู้เขียนได้เขียนบทความนี้เพื่อเป็นวัคซีนป้องกันปัญหาเรื่องดังกล่าว โดยใช้หลักการเกี่ยวกับการควบคุมขั้นพื้นฐานที่หน่วยงานควรมีและถือปฏิบัติ ซึ่งเราเรียกว่า “การควบคุมทั่วไปทางด้านเทคโนโลยีสารสนเทศ (IT General Controls)” หรือบางตำราเรียกว่า “การควบคุมโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ (IT Infrastructure Controls)” ผู้เขียนได้รวบรวมและสรุปเรื่องการควบคุมพื้นฐานฯไว้เพื่อให้ง่ายต่อการเข้าใจและนำไปปฏิบัติไว้ ได้แก่ **“S.M.A.R.T” Controls** โดยที่ (S = Strategy, M = Manage Change, A = Access Control, R = Recovery และ T= Others)

S

S-Strategy (กลยุทธ์)

ผู้บริหารองค์กรควรต้องจัดให้มี นโยบาย (Policy) มาตรฐาน (Standard) และระเบียบการปฏิบัติงาน (Procedure) เช่น นโยบายความมั่นคงปลอดภัยสารสนเทศ ระเบียบเรื่องการบริหารจัดการบัญชีผู้ใช้งาน ระเบียบเรื่องการบริหารการเปลี่ยนแปลงทางด้านสารสนเทศ ระเบียบเรื่องการบริหารจัดการปัญหาคอมพิวเตอร์ และระเบียบเรื่องการสำรองและกู้คืนข้อมูล เป็นต้น โดยต้องได้รับการอนุมัติจากผู้บริหารองค์กร นอกจากนี้ควรประกาศให้ผู้ที่มีส่วนเกี่ยวข้องทราบและปฏิบัติโดยทั่วกันและควรทบทวนให้ทันสมัยอยู่เสมอ

M

M-Manage Change (การบริหารการเปลี่ยนแปลงทางด้านสารสนเทศ)

การควบคุมพื้นฐานที่จำเป็นสำหรับเรื่องการเปลี่ยนแปลงต่าง ๆ ทางด้านสารสนเทศประกอบด้วย

- คำขอต้องได้รับการอนุมัติจากผู้บริหารองค์กร
- ต้องมีการทดสอบเพื่อยอมรับระบบ (UAT = User Acceptance Test)
- ต้องได้รับการอนุมัติก่อนนำระบบขึ้นใช้งานจริง
- ต้องมีการแบ่งแยกหน้าที่ที่เหมาะสม
- ต้องมีการบริหารและติดตามโครงการต่าง ๆ ทางด้านเทคโนโลยีสารสนเทศ
- ต้องมีการจัดการกับ Job Run Batch/Job Schedule
- ต้องมีการควบคุม Source Code
- ต้องมีการควบคุมข้อมูลจริงที่นำมาใช้ทดสอบ
- ต้องมีการควบคุมเรื่องผู้ให้บริการภายนอก (IT Outsource)
- ต้องมีการจัดทำเอกสารที่สำคัญที่ใช้ประกอบการพัฒนาระบบสารสนเทศ เช่น User Manual, Functional Specification, Context/Data Flow Diagram เป็นต้น

A

A-Access Control (การควบคุมการเข้าถึง)

A-Access Control (การควบคุมการเข้าถึง) การควบคุมการเข้าถึงขั้นพื้นฐานประกอบด้วยทั้งด้านลอจิก (Logical Access Control) และด้านกายภาพ (Physical Access Control)

- **ด้านลอจิก (Logical Access Control)**
  - การกำหนดค่าของรหัสผ่าน (Password Parameters Setting) เช่น ความยาว รอบระยะเวลา ความซับซ้อน การใช้รหัสผ่านเก่า และการกรอกรหัสผ่านผิด เป็นต้น
  - การกำหนดค่าความปลอดภัย (Security Configurations) เช่น Firewall Rules, WIFI, BYOD (Bring Your Own Device), Remote Access และการแบ่งโซนเครือข่าย (Network zone) เป็นต้น
  - การบริหารจัดการบัญชีผู้ใช้งาน (User Access Management) เช่น การเพิ่ม การแก้ไข การลบ และการสอบทานบัญชีผู้ใช้งานทั้งบัญชีผู้ใช้งานธรรมดาและบัญชีผู้ใช้งานที่มีสิทธิ์พิเศษ เป็นต้น
  - การสอบทานข้อมูลประวัติการใช้งาน (Log Monitoring) เช่น ต้องมีการเปิดใช้งาน Security Log และการสอบทานข้อมูล Log อย่างสม่ำเสมอ
- **ด้านกายภาพ (Physical Access Control)**
  - การกำหนดสิทธิ์การเข้าถึงห้องหรือศูนย์คอมพิวเตอร์ เช่น การกำหนดสิทธิ์ผู้ถือการ์ด (Access Card) หรือ การกำหนดสิทธิ์ผู้ถือกุญแจ (ให้เฉพาะผู้ที่เกี่ยวข้องและเหมาะสมเท่านั้น) และการบันทึกประวัติการเข้าถึง (Visitor Log) เป็นต้น
  - การควบคุมสภาพแวดล้อมในห้องหรือศูนย์คอมพิวเตอร์ เช่น ไฟฟ้า (UPS/Generator) อุณหภูมิ ความชื้น และอุปกรณ์ดับเพลิง เป็นต้น รวมถึงต้องมีการบำรุงรักษาอุปกรณ์เหล่านั้นอย่างสม่ำเสมอ
  - การเฝ้าติดตามการทำงานของอุปกรณ์คอมพิวเตอร์ (Computer Monitoring) ต้องมีการตรวจติดตามการทำงานของอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เช่น CPU, Disk, Network เป็นต้น

R

R-Recovery (การกู้คืนระบบเมื่อเกิดเหตุฉุกเฉินทางด้านสารสนเทศ)

ผู้บริหารองค์กรควรจัดให้มีการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินทางด้านสารสนเทศ (Disaster Recovery Plan) โดยต้องได้รับการอนุมัติจากผู้บริหารองค์กรและประกาศให้ผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ นอกจากนี้ควรจัดให้มีการทดสอบและทบทวนแผนฯ อย่างสม่ำเสมอ และการสำรองและกู้คืนข้อมูล (Backup and Recovery) ต้องมีการสำรองข้อมูลที่สำคัญขององค์กรและทดสอบกู้คืนอย่างสม่ำเสมอ

T

T-Others (อื่น ๆ)

การควบคุมขั้นพื้นฐานด้านอื่น ๆ ประกอบด้วย

- การบริหารจัดการกับปัญหาด้านเทคโนโลยีสารสนเทศ (Incident and Problem Management) ต้องมีกระบวนการจัดการกับปัญหาทางด้านเทคโนโลยีสารสนเทศให้ทันเวลา
- การบริหารจัดการผู้ให้บริการภายนอก (IT Outsourcing Management) ต้องมีกระบวนการในการคัดเลือก การประเมินความเสี่ยง การจัดทำสัญญา การตรวจสอบการควบคุมภายใน การประเมินผลการปฏิบัติงาน และแนวทางการนำงานกลับมาดำเนินการเอง เป็นต้น
- การป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ต้องมีการติดตั้งโปรแกรม Anti-Virus และปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอ เป็นต้น

สุดท้ายนี้ผู้เขียนหวังเป็นอย่างยิ่งว่า **“S.M.A.R.T” Controls** จะเป็นเครื่องมือเบื้องต้นหรือเป็นวัคซีนที่จะช่วยป้องกันให้องค์กรของท่านพ้นจากภัยทางด้านไซเบอร์ได้ และให้องค์กรสามารถดำเนินการได้อย่างต่อเนื่องและบรรลุเป้าหมายขององค์กรได้อย่างยั่งยืน