จุลสารตรวจสอบภายใน

ปีที่ 3 ฉบับที่ 3 ประจำไตรมาสที่ 3 เดือนเมษายน - มิถุนายน 2558

สวัสดีครับ/ค่ะ...ท่านผู้อ่านจุลสารตรวจสอบภายในทุกท่านในฉบับนี้ทางทีมงานกองบรรณาธิการขอประชาสัมพันธ์เรื่องการเปลี่ยนแปลงตำแหน่งผู้อำนวยการสำนักงานตรวจสอบภายใน โดยมหาวิทยาลัยได้แต่งตั้ง ดร.สุรสิทธิ์ ขวัญบุญบำเพ็ญ อาจารย์ประจำสาขาวิชาวิทยาศาสตร์สิ่งแวดล้อม เข้ามารักษาราชการแทนผู้อำนวยการสำนักงานตรวจสอบภายใน เริ่มปฏิบัติงานตั้งแต่ วันที่ 1 มิถุนายน 2558 เป็นต้นไป

ฉบับนี้กองบรรณาธิการได้นำเสนอเกี่ยวกับการตรวจสอบทางด้านเทคโนโลยีสารสนเทศเพื่อเป็นการเตรียมความพร้อมสำหรับการเข้ารับตรวจทางด้านเทคโนโลยีสารสนเทศตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ 2559 (1 ต.ค. 58 - 30 ก.ย. 59) และเกร็ดความรู้เรื่องวิธีการป้องกันภัยร้ายบนโลกออนไลน์แล้วพบกับสาระดีๆ ในฉบับต่อไปครับ/ค่ะ

ความหมายของเทคโนโลยีสารสนเทศ

สหพันธ์นักบัญชีระหว่างประเทศ หรือ ไอแฟค (International Federation of Accountants : IFAC) ได้ให้ความหมายของเทคโนโลยีสารสนเทศ (Information Technology) ไว้ดังนี้

“เทคโนโลยีสารสนเทศ หมายถึง ผลิตภัณฑ์ฮาร์ดแวร์และซอฟท์แวร์ การปฏิบัติการด้านระบบสารสนเทศ กระบวนการด้านบริหารจัดการ และทรัพยากรมนุษย์รวมทั้งทักษะที่จำเป็นในการที่จะประยุกต์ผลิตภัณฑ์และกระบวนการที่กล่าวมาให้เข้ากับภาระงานการผลิตสารสนเทศ การพัฒนาระบบสารสนเทศ รวมทั้งการจัดการและการควบคุมสารสนเทศ”

ความหมายของการตรวจสอบเทคโนโลยีสารสนเทศ

การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Audit : IT Audit) หมายถึง กระบวนการของการรวบรวมหลักฐานและประเมินหลักฐานที่ได้ เพื่อใช้ในการพิจารณาเกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล การปกป้องดูแลทรัพย์สิน การรักษาความลับ การดำเนินงานเพื่อบรรลุวัตถุประสงค์ขององค์กรอย่างมีประสิทธิผล และการใช้ทรัพยากรอย่างคุ้มค่าและมีประสิทธิภาพ

ความจำเป็นในการควบคุมและตรวจสอบเทคโนโลยีสารสนเทศ

เมื่อองค์กรใช้เทคโนโลยีสารสนเทศ องค์กรมีความจำเป็นในการควบคุมและตรวจสอบเทคโนโลยีสารสนเทศเพื่อวัตถุประสงค์ดังนี้

1. เพื่อป้องกันข้อมูลสูญหาย ข้อมูลที่อยู่ในระบบคอมพิวเตอร์หรือระบบการสื่อสารโทรคมนาคมมีโอกาสสูญหายได้ง่าย องค์กรต้องมีการควบคุมภายในที่ดีเพื่อป้องกัน และแก้ไขกรณีข้อมูลสูญหาย

2. เพื่อความเชื่อถือได้ถูกต้องและครบถ้วนของสารสนเทศ ข้อมูลจากเทคโนโลยีสารสนเทศที่ผิดพลาดย่อมทำให้ผู้บริหารและผู้ใช้สารสนเทศนั้นตัดสินใจแก้ปัญหาต่างๆ อย่างผิดพลาดตามไปด้วย

ที่มา: หนังสือการตรวจสอบภายในและการควบคุมภายใน
โดย จันทนา สาขากร นิพันธ์ เห็นโชคชัยชนะ
และ ศิลปพร ศรีจันเพชร

3. เพื่อป้องกันการใช้คอมพิวเตอร์ในทางที่มิชอบหรือทุจริต องค์กรจะได้รับผลเสียหายจากการใช้คอมพิวเตอร์ในทางที่ไม่ถูกต้อง หรือระบบคอมพิวเตอร์ไม่สามารถทำงานได้ เกิดการหยุดชะงัก

4. เพื่อปกป้องรักษาทรัพย์สินเทคโนโลยีสารสนเทศ เช่น ฮาร์ดแวร์ ซอฟท์แวร์ของบุคลากรด้านคอมพิวเตอร์ให้ปลอดภัย

5. เพื่อรักษาความลับของข้อมูลและสารสนเทศโดยเฉพาะที่สำคัญและเป็นเรื่องลับ

แนวทางการตรวจสอบเทคโนโลยีสารสนเทศ

แนวทางการตรวจสอบ (Audit Guideline) มี 4 ขั้นตอนคือ

1. การศึกษาทำความเข้าใจ (Obtaining an Understanding) เพื่อจดบันทึกกิจกรรมภายใต้วัตถุประสงค์ของการควบคุม และระบุวิธีการหรือมาตรการควบคุมที่กำหนดไว้ว่ามีหรือไม่ โดยการสัมภาษณ์ผู้บริหารและพนักงานเพื่อให้เกิดความเข้าใจ จดบันทึกกระบวนการใช้ทรัพยากรเทคโนโลยีที่สอบถามมา และยืนยันความเข้าใจด้วยการทดสอบแบบติดตามรายการ (Walk-through Test)

2. การประเมินการควบคุม (Evaluating the Control) เพื่อประเมินประสิทธิผลของมาตรการควบคุมที่กำหนดไว้ หรือระดับของการบรรลุวัตถุประสงค์ของการควบคุม

3. การประเมินการปฏิบัติงาน (Assessing Compliance) เพื่อให้แน่ใจว่ามาตรการควบคุมที่กำหนดไว้ หรือระดับของการบรรลุวัตถุประสงค์ของการควบคุม

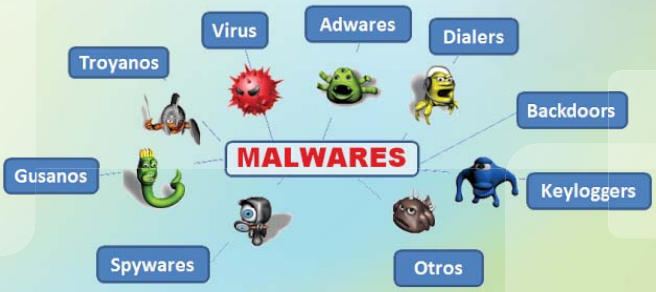
4. การพิสูจน์ยืนยันความเสี่ยง (Substantiating the Risk) เพื่อพิสูจน์หรือยืนยันให้เห็นถึงความเสี่ยงของวัตถุประสงค์ของการควบคุมที่ไม่มีอยู่ โดยการใช้เทคนิคการวิเคราะห์เปรียบเทียบและการปรึกษาหารือกับแหล่งอื่น วัตถุประสงค์คือการสนับสนุนข้อสรุปของผู้ตรวจสอบภายใน และการแจ้งให้ผู้บริหารทราบเพื่อพิจารณาปรับปรุงแก้ไขต่อไป

ที่มา: หนังสือการตรวจสอบภายในและการควบคุมภายใน
โดย จันทนา สาขากร นิพันธ์ เห็นโชคชัยชนะ
และ ศิลปพร ศรีจั่นเพชร

เกร็ดความรู้ เรื่อง วิธีการป้องกันภัยร้ายบนโลกออนไลน์

เมื่อโลกอินเตอร์เน็ตเข้ามามีบทบาทในชีวิตมากขึ้น ภัยร้ายก็มาเยือนถึงตัวได้แบบไม่เว้นวัน จึงนำเสนอเทคนิคป้องกันภัยคุกคามออนไลน์ ที่ใครก็ทำได้ มาให้รับทราบกัน ดังนี้

1. ตั้งสติก่อนเปิดเครื่อง ก่อนเปิดเครื่องคอมพิวเตอร์ ให้รู้ตัวเสมอว่าเราอยู่ที่ไหน ที่บ้าน ที่ทำงาน หรือที่สาธารณะ และระมัดระวังการใช้งานคอมพิวเตอร์ ตั้งแต่เริ่มเปิดเครื่อง คือก่อน Login เข้าใช้งานคอมพิวเตอร์ ต้องมั่นใจว่าไม่มีใครแอบดู Password ของเราได้ เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อคหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า Login ป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ของเราได้อย่างสะดวก อย่าประมาทในการใช้งานอินเตอร์เน็ตควรตระหนักไว้ว่าข้อมูลความลับและความเป็นส่วนตัวของเราอาจถูกเปิดเผยได้เสมอในโลกออนไลน์ แม้เราจะระมัดระวังมากเพียงใดก็ตาม



2. กำหนด Password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษ ไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้น และการใช้งานอินเตอร์เน็ตทั่วไป เช่น การ Login ระบบ E-mail ระบบสนทนาออนไลน์ (Chat) ระบบเว็บไซต์ที่เราเป็นสมาชิกอยู่ ทางที่ดีควรใช้ Password ที่ต่างกันบ้างพอให้จำได้ หรือมีเครื่องมือช่วยจำ Password เข้ามาช่วย

3. สังเกตขณะเปิดเครื่อง ว่ามีโปรแกรมไม่พึงประสงค์รันมาพร้อมๆ กับการเปิดเครื่องหรือไม่ ถ้าดูไม่ทัน ให้สังเกตระยะเวลาบูตเครื่อง หากนานผิดปกติ อาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรืออื่นๆ ได้

4. หมั่นตรวจสอบและอัพเดต OS หรือซอฟต์แวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่อง และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ควรอัพเดตอินเตอร์เน็ตบราวเซอร์ ให้ทันสมัยอยู่เสมอ เนื่องจาก Application Software สมัยใหม่มักพึ่งพาอินเตอร์เน็ตบราวเซอร์ ก่อให้เกิดช่องโหว่ใหม่ๆ ให้ภัยคุกคามเจาะผ่านบราวเซอร์ สร้างปัญหาให้เราได้

5. ไม่ลงซอฟต์แวร์มากเกินจำเป็น จนเกินศักยภาพการทำงานของเครื่องคอมพิวเตอร์ ซอฟต์แวร์ที่จำเป็นต้องลงในเครื่องคอมพิวเตอร์ ได้แก่

– อินเตอร์เน็ตบราวเซอร์ เพื่อใช้เปิดเว็บไซต์ต่างๆ

– E-mail เพื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร

– โปรแกรมสำหรับงานด้านเอกสาร โปรแกรมตกแต่งภาพ เสียง วิดีโอ

– โปรแกรมป้องกันไวรัสคอมพิวเตอร์

หากจำเป็นต้องใช้โปรแกรมอื่น ควรพิจารณาใช้โปรแกรมที่ผ่าน Web Application เช่น Chat VoIP เป็นต้น หรือบันทึกโปรแกรมลงบน Thumb Drive เพื่อรันจากภายนอกเครื่องคอมพิวเตอร์

6. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เว็บไซต์ประเภทนี้ ได้แก่

– เว็บไซต์ลามกอนาจาร

– เว็บไซต์การพนัน

– เว็บไซต์ที่มีหัวเรื่อง “Free” แม้กระทั่ง Free Wi-Fi ที่เราคิดว่าได้เล่นอินเตอร์เน็ตฟรี แต่อาจเป็นแผนของ Hacker ให้เรามาใช้ระบบ Wi-Fi ก็เป็นได้ ให้คิดเสมอว่า “ไม่มีของฟรีในโลก” หากมีการให้ฟรีก็ต้องมีของต่างตอบแทน เช่น โฆษณาแฝง เป็นต้น

7. สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์

8. ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network ชื่อที่ใช้ควรเป็นชื่อเล่นหรือฉายาที่กลุ่มเพื่อนรู้จัก

9. ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเตอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือ ให้คิดถึงใจเขาใจเรา หากเราไม่ชอบสิ่งใด ก็ไม่ควรทำสิ่งนั้นกับผู้อื่น เวลาแสดงความคิดเห็นบนกระดานแสดงความคิดเห็น (Webboard) การรับส่ง E-mail หรือการกระทำใดๆ กับข้อมูลบนอินเตอร์เน็ต

ที่มา : http://www.armamentfairbelgrade.com/

ถาม..ตอบ..กับตรวจสอบภายใน

ถาม : ความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศมีอะไรบ้าง

ตอบ : ในกรณีที่ระบบสารสนเทศใช้คอมพิวเตอร์มีความสำคัญ ผู้ตรวจสอบภายในควรมีความรู้และความเข้าใจเกี่ยวกับสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ซึ่งอาจมีอิทธิพลต่อการประเมินความเสี่ยงและลักษณะของการควบคุมภายใน ในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ รวมถึงสิ่งต่อไปนี้

1. การไม่มีหลักฐานการติดตามรายการหรือขาดร่องรอยการตรวจสอบ ในกรณีที่เป็นระบบงานที่ซับซ้อนซึ่งมีการประมวลผลข้อมูลหลายขั้นตอน ผู้ตรวจสอบภายในไม่สามารถหาหลักฐานที่สมบูรณ์ในการติดตามรายการได้

2. การประมวลผลข้อมูลที่เป็นแบบเดียวกันสำหรับรายการบัญชีที่เหมือนกัน ข้อผิดพลาดในการเขียนโปรแกรม หรือข้อผิดพลาดที่เป็นระบบ โดยปกติแล้วจะทำให้ทุกรายการที่ได้ประมวลผลข้อมูลผิดพลาดเหมือนกันหมด

3. การขาดการแบ่งแยกหน้าที่ บุคคลใดบุคคลหนึ่งซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ การประมวลผลอาจอยู่ในฐานะที่จะปฏิบัติหน้าที่ ซึ่งไม่สมควรปฏิบัติโดยคนเดียว

4. โอกาสที่จะเกิดข้อผิดพลาดและรายการผิดปกติ โอกาสที่จะเกิดข้อผิดพลาดโดยคนเป็นผู้กระทำในการพัฒนา บำรุงรักษา และจัดการประมวลผลในระบบสารสนเทศที่ใช้คอมพิวเตอร์อาจมีมากกว่าในระบบที่ใช้มือ

5. การก่อให้เกิดรายการหรือจัดการประมวลผลรายการอัตโนมัติ การอนุมัติรายการอาจจะไม่มีการบันทึกในลักษณะเดียวกับรายการในระบบที่ใช้มือ การอนุมัติรายการเหล่านี้โดยผู้บริหารอาจถือว่าเกิดขึ้น เมื่อผู้บริหารยอมรับการออกแบบระบบสารสนเทศที่ใช้คอมพิวเตอร์ ตลอดจนการดัดแปลงแก้ไขระบบที่ใช้คอมพิวเตอร์ในภายหลัง

6. การควบคุมอื่นที่ขึ้นอยู่กับการประมวลผลด้วยคอมพิวเตอร์ การประมวลผลด้วยคอมพิวเตอร์อาจมีการจัดทำรายงานและผลลัพธ์อื่นเพื่อนำมาใช้ในการปฏิบัติตามวิธีการควบคุมในระบบที่ใช้มือ ดังนั้นประสิทธิผลของวิธีการควบคุมในระบบที่ใช้มือจะขึ้นอยู่กับประสิทธิผลของการควบคุมเกี่ยวกับความถูกต้องครบถ้วนของการประมวลผลด้วยคอมพิวเตอร์

7. โอกาสที่จะเพิ่มการควบคุมดูแลโดยผู้บริหาร การควบคุมที่เพิ่มขึ้นอาจช่วยให้โครงสร้างการควบคุมภายในโดยรวมของกิจการดีขึ้น

8. โอกาสที่จะใช้เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (Computer-Assisted Audit Tools and Techniques : CAATs) ความเสี่ยงและการควบคุมที่เป็นผลจากการใช้ระบบสารสนเทศที่ใช้คอมพิวเตอร์มีโอกาสที่จะส่งผลกระทบต่อการประเมินความเสี่ยงของผู้ตรวจสอบภายใน ตลอดจนลักษณะ ระยะเวลา และขอบเขตของวิธีการตรวจสอบ

หากท่านมีข้อติชมหรือต้องการแสดงความคิดเห็นหรือมีปัญหาเกี่ยวกับงานตรวจสอบภายใน

ติดต่อได้ที่ : 0-2942-6900 ต่อ 7052

E-mail : cruaudit@gmail.com

Website : http://www.chandra.ac.th/audit/

บรรณาธิการ : ดร.สุรสิทธิ์ ขวัญบุญบำเพ็ญ

กองบรรณาธิการ : นายปฐวี ฉลวย นางสาวเทียมตา พรหมสิทธิ์ นางสาวชยาภา อัตชู นางสาวรัชฎาภรณ์ สนเนตร์ และ นางสาวรัตติกาล มูลศรี