วารสาร Mahidol R2R e-Journal
Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

บทบาทและความสำคัญของผู้ตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
The Role and Importance of Internal Auditor for Information Security Management System

กิตติศักดิ์ แก้วบุตรดี[1] อัจฉรา กิจเดช[2*]
KITTISAK KAEWBOODDEE[1], ATCHARA KITDESH[2*]

บทคัดย่อ

ในปัจจุบันเทคโนโลยีสารสนเทศได้มีการพัฒนาไปอย่างรวดเร็วและเข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กรต่าง ๆ ทำให้การรักษาความปลอดภัยของระบบสารสนเทศได้กลายเป็นประเด็นที่สำคัญสำหรับองค์กรต่าง ๆ ในประเทศไทย และในหลาย ๆ ประเทศ เพื่อเป็นการป้องกันการเข้าถึงข้อมูลที่สำคัญต่าง ๆ จึงต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยสารสนเทศ อย่างไรก็ตามองค์กรต้องเผชิญกับปัญหาต่าง ๆ ในปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศให้ได้ตามมาตรฐานข้อกำหนด

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือ ISO/IEC 27001:2013 คือมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ถือเป็นหัวใจหลักในการบริหารจัดการระบบเทคโนโลยีสารสนเทศขององค์กร และได้ถูกนำมาใช้เป็นมาตรฐานในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอย่างแพร่หลาย ซึ่งหนึ่งในกระบวนการที่สำคัญที่ทำให้การดำเนินโครงการดังกล่าวประสบความสำเร็จ คือการตรวจสอบภายใน ซึ่งถือเป็นปัจจัยสำคัญของการควบคุมคุณภาพภายในขององค์กร ทำให้การตรวจประเมินมีความเป็นอิสระ และตรงตามวัตถุประสงค์ของการตรวจสอบภายใน ทำให้การควบคุม ติดตามการดำเนินกิจกรรมต่าง ๆ ให้มีประสิทธิภาพ และประสิทธิผล

ดังนั้น ผู้ตรวจสอบภายในถือเป็นหัวใจสำคัญในการผลักดัน ส่งเสริมการปฏิบัติงานให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กร ที่จะนำระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศมาใช้ เช่น ส่งเสริมให้เกิดกระบวนการกำกับดูแลที่ดี (Good Corporate Governance), ส่งเสริมให้เกิดการรายงานตามหน้าที่ความรับผิดชอบ (Accountability and Responsibility), ส่งเสริมให้เกิดประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน (Efficiency and Effectiveness of Performance), เป็นมาตรการถ่วงดุลแห่งอำนาจ (Check and Balance) และ ให้สัญญาณเตือนภัยล่วงหน้า (Warning Signals) ของการประพฤติมิชอบหรือการทุจริตในองค์กร

[1,2] ตำแหน่งนักวิชาการคอมพิวเตอร์ งานวิเคราะห์และพัฒนาโปรแกรม ฝ่ายสารสนเทศ สำนักงานคณบดี คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

[1,2] Computer Technical Officer Siriraj Information Technology Faculty of Medicine Siriraj Hospital, Mahidol University

* corresponding author : atchara.kit@mahidol.ac.th

วารสาร Mahidol R2R e-Journal
Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

คำสำคัญ : การตรวจสอบภายใน ผู้ตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Abstract

Currently, the information technology had developed rapidly an important role in the operation of various organizations. The Information security had become an important issue for the various business in Thailand and other countries in the world. The information security prevents access to the necessary information. The organizations need to comply with data security requirements. However, the organizations faced many problems in improving the Information Security Management System.

Information Security Management System (ISMS) or ISO27001:2013 is the measures for the security of information systems. It is key to managing an organization's information technology systems and has been widely used as a standard in the management of information security. The key to processes that made the project successful was the internal audit. The internal audit is an important part of quality control within the organization. The internal auditors achieve objectives of the internal audit and internal control of the activities was effectiveness.

Therefore, internal auditors are the key to driving, encourage and promote the implementation of the objectives and goals for instance 1) To encourage good corporate governance. 2) To promote accountability and responsibility for reporting. 3) To encourage efficiency and effectiveness performance of the operation. 4) Check and balance Internal Controls and 5) Warning signals for misconduct or corruption in the organization.

Keywords: Internal audit, Internal auditor, Information Security Management System

บทนำ

ในปัจจุบันเทคโนโลยีสารสนเทศมีการพัฒนาไปอย่างรวดเร็วและเข้ามามีบทบาทสำคัญในการดำเนินงานต่าง ๆ การรักษาความปลอดภัยของข้อมูลในองค์กรจึงกลายเป็นประเด็นที่สำคัญ ซึ่งแต่ละหน่วยงานมีความจำเป็นต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญต่าง ๆ ขององค์กร อย่างไรก็ตามแต่ละองค์กรต้องเผชิญกับปัญหาต่าง ๆ เพื่อเป็นการป้องกันการเข้าถึงข้อมูลที่สำคัญจึงต้องมีการปรับปรุงด้านการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศเพื่อเป็นการป้องกันการเข้าถึงข้อมูลที่สำคัญ ทำให้มีขั้นตอนในการดำเนินงานต่าง ๆ ที่เกี่ยวข้องมากขึ้น นอกจากนี้สิ่งที่สำคัญที่สุดของระบบสารสนเทศต้องมีความน่าเชื่อถือ และข้อมูลที่บันทึกเข้าไปในระบบนั้นต้องเป็นข้อมูลที่ถูกต้องและสมบูรณ์เพื่อประโยชน์ในการนำข้อมูลที่มีการบันทึกเข้าไปกลับมาใช้ประโยชน์ในด้านต่าง ๆ

ความมั่นคงปลอดภัยสารสนเทศถือเป็นเรื่องที่มีสำคัญเป็นอันดับต้น ๆ ขององค์กร เนื่องจากข้อมูลต่าง ๆ ขององค์กร เช่น ข้อมูลทางการเงิน ข้อมูลของการบริการต่าง ๆ ถือเป็นทรัพย์สินที่มีค่ามหาศาล

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

ในปัจจุบันภัยคุกคามทางคอมพิวเตอร์มีการพัฒนาการรูปแบบการโจมตีที่รวดเร็วและหลากหลายมากขึ้น ซึ่งก่อให้เกิดผลกระทบต่อความมั่นคงและการเสถียรภาพการดำเนินงานขององค์กร ดังนั้นจึงมีความจำเป็นต้องมีแนวทางในการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร เช่น จัดให้มีการบริหารจัดการความเสี่ยง จัดสร้างกระบวนการทำงานให้เป็นระบบและสอดคล้องกับมาตรฐานสากล โดยมีการบริหารจัดการและติดตามผลความเสี่ยงอยู่เสมอ รวมถึงการตระหนักและให้ความสำคัญในด้านการป้องกันความเสี่ยงที่จะเกิดขึ้นกับข้อมูล ซึ่งการที่องค์กรมีสารสนเทศที่ดี (Good Information) ทั้งความถูกต้องสมบูรณ์ และความชัดเจนแล้ว ยังต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security) ด้วย รวมถึงการรักษาความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล ระบบฐานข้อมูลและเครือข่ายการสื่อสารข้อมูล การป้องกันทางกายภาพ การวิเคราะห์ความเสี่ยง ประเด็นด้านกฎหมาย มีจรรยาบรรณและความตระหนักด้านความปลอดภัยในระบบคอมพิวเตอร์

การดำเนินการโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) หรือ ISO/IEC 27001:2013 คือ มาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ถือเป็นหัวใจหลักในการบริหารจัดการระบบเทคโนโลยีสารสนเทศขององค์กร และได้ถูกนำมาใช้เป็นมาตรฐานในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอย่างแพร่หลาย และความสำเร็จของการดำเนินการของโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะประสบความสำเร็จไม่ได้ถ้าขาดกระบวนใด ๆ หนึ่งในกระบวนที่สำคัญที่สุดคือการตรวจสอบภายใน ซึ่งเป็นหัวใจสำคัญในการผลักดัน และส่งเสริมการปฏิบัติงานให้บรรลุวัตถุประสงค์และเป้าหมายของ เช่น ส่งเสริมให้เกิดกระบวนการกำกับดูแลที่ดี(Good Corporate Governance) ป้องกันการประพฤติมิชอบหรือการทุจริต และเป็นการลดความเสี่ยงที่อาจเกิดขึ้น จนส่งผลให้ให้การดำเนินงานไม่บรรลุวัตถุประสงค์, ส่งเสริมให้เกิดการรายงานตามหน้าที่ความรับผิดชอบ (Accountability and Responsibility) ทำให้องค์กรได้ข้อมูลหรือรายงานตามหน้าที่ความรับผิดชอบ และเป็นพื้นฐานของหลักความโปร่งใส (Transparency) และสามารถตรวจสอบได้ (Auditability), ส่งเสริมให้เกิดประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน (Efficiency and Effectiveness of Performance) ขององค์กร เนื่องจากการตรวจสอบภายในเป็นการประเมินวิเคราะห์ เปรียบเทียบข้อมูลทุกด้าน การปฏิบัติงานตรวจสอบภายในจึงเป็นส่วนสำคัญที่ช่วยปรับปรุงระบบงานให้รัดกุม ลดขั้นตอนที่ซ้ำซ้อน และเหมาะสมกับสถานการณ์ตลอดเวลา ช่วยลดเวลา และค่าใช้จ่าย เป็นสื่อกลางระหว่างผู้บริหารและผู้ปฏิบัติงานในการประสานงาน ลดปัญหาความไม่เข้าใจในนโยบาย เป็นมาตรการถ่วงดุลแห่งอำนาจ ส่งเสริมให้การจัดสรรการใช้ทรัพยากรขององค์กรเป็นไปอย่างเหมาะสม เพื่อให้ได้ผลงานที่เป็นประโยชน์สูงสุดต่อองค์กร (Check and Balance) และให้สัญญาณเตือนภัยล่วงหน้า (Warning Signals) เช่น การประพฤติมิชอบหรือการทุจริตในองค์กร ลดโอกาสการเกิดความเสี่ยง รวมทั้งเพื่อเพิ่มโอกาสของความสำเร็จของงาน การพัฒนาเหล่านี้ไม่เพียงเป็นจุดเริ่มต้นในการสร้างความมั่นคงปลอดภัยให้ระบบสารสนเทศ และข้อมูลทางสารสนเทศเท่านั้น แต่ยังเป็นจุดเริ่มต้นเพื่อสร้างความเข้มแข็งให้แก่องค์กร สร้างมูลค่า และที่สำคัญสร้างความน่าเชื่อถือให้มีมาตรฐานทัดเทียมนานาประเทศในระดับสากล

ความหมายและความเป็นมาของการตรวจสอบภายใน

ความต้องในการตรวจสอบทั้งภายนอก และภายในจำเป็นต้องมีวิธีการตรวจสอบที่เป็นอิสระเพื่อลดข้อผิดพลาดในการบันทึกข้อมูล การยักยอกทรัพย์สิน และการฉ้อฉลภายในองค์กร การตรวจสอบดังกล่าวข้างต้นเป็นพื้นฐานของการตรวจสอบโดยทั่วไป

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

จุดกำเนิดของการตรวจสอบได้มีขึ้นเมื่อย้อนกลับไปในอดีตของการตรวจสอบทางบัญชี ผู้ที่รับผิดชอบต้องดูแลทรัพย์สินที่เกี่ยวข้องกับการปฏิบัติงาน มีความจำเป็นที่จะต้องถูกตรวจสอบเกี่ยวกับการทำงาน และทรัพย์สินต่าง ๆ (Mautz & Sharaf, 1961; Brown, 2009)

เมื่อย้อนไปเมื่อ 4,000 ปีก่อนคริสตกาล นักประวัติศาสตร์เชื่อว่าระบบการเก็บบันทึกข้อมูลที่เป็นทางการถูกจัดทำขึ้นโดยองค์กรที่มีหน้าที่ในการจัดการ ของรัฐบาลในกลุ่มประเทศที่ตั้งอยู่ในคาบสมุทรบอลข่านเพื่อลดความกังวลต่าง ๆ เกี่ยวกับการจัดทำบัญชีให้ถูกต้องสำหรับใบเสร็จรับเงิน การเบิกจ่าย และการเก็บภาษี ซึ่งคล้ายคลึงกับการพัฒนาเกิดขึ้นในสมัยราชวงศ์จ้าว (Zhao) ของประเทศจีนในช่วง 1,122-1,256 ปีก่อนคริสตกาล ความต้องการในการตรวจสอบระบบการเงินในกรีซ จักรวรรดิโรมัน และเมืองต่างๆ ของอิตาลีในอดีตเป็นต้น ซึ่งทั้งหมดได้มีการพัฒนาอย่างละเอียดและรอบคอบ ซึ่งรัฐบาลเหล่านี้กังวลเกี่ยวกับการทำงานของเจ้าหน้าที่ที่อาจจะเกิดข้อผิดพลาดในการทำบัญชีรวมทั้งความเสียหายต่าง ๆ และอาจจะกระทำการฉ้อโกงเมื่อมีโอกาสเป็นต้น (Ramamoorti, 2003)

การตรวจสอบภายใน ในสมัยเริ่มแรกแตกต่างจากแนวทางที่เป็นอยู่ในปัจจุบันเป็นอย่างมาก สมัยก่อนนั้นคำว่า “ตรวจสอบ” จะหมายถึงตำราลับของฝ่ายบริหารซึ่งมีหน้าที่คอยจับผิดและรายงานให้เสนอฝ่ายบริหารเพื่อพิจารณาลงโทษ ทำให้เกิดปัญหาขึ้นคือ ผู้ตรวจสอบจะมีศัตรูทั่วทุกแห่งในองค์กรเพราะผู้ปฏิบัติงานหรือผู้รับการตรวจสอบไม่ให้ความร่วมมือ แต่ในระยะต่อมาแนวคิดได้เปลี่ยนไปเป็นมุ่งค้นหาข้อบกพร่องของระบบงาน มิใช่ตัวบุคคล แล้วพยายามหาทางแก้ไขให้ดีขึ้น ผู้ตรวจสอบภายในจะวิเคราะห์ถึงจุดอ่อนของระบบงาน และพยายามเข้าใจถึงปัญหาที่กำลังประสบอยู่ แล้วปรึกษาหารือร่วมกับผู้ปฏิบัติงานเพื่อให้ได้ความเห็นร่วมกันที่จะแก้ปัญหาอันจะทำให้การปฏิบัติงานในองค์กรเป็นไปอย่างมีประสิทธิภาพและมีประสิทธิผล เพื่อบรรลุเป้าหมายสูงสุดขององค์กร (Swinkels, 2012)

บทบาทและความสำคัญของผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ผู้ตรวจสอบภายในเป็นส่วนสำคัญของการควบคุมคุณภาพภายในขององค์กร ทำให้การประเมินมีความเป็นอิสระ และตรงตามวัตถุประสงค์ของการตรวจสอบภายใน ทำให้การควบคุมการดำเนินกิจกรรมต่าง ๆ มีประสิทธิภาพ และประสิทธิผล ทั้งนี้ผู้ตรวจสอบภายในยังสามารถให้ข้อเสนอแนะเพื่อเป็นการปรับปรุงคุณภาพอย่างต่อเนื่องในทุก ๆ กิจกรรมของการดำเนินงานภายใต้โครงการต่าง ๆ

ทั้งนี้การตรวจสอบภายในเป็นหัวใจสำคัญของการกำกับดูแลกิจการที่ดี และมีบทบาทสำคัญในการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจสอบภายในเป็นเครื่องมือสำคัญในการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ โดยผู้ตรวจสอบภายในสามารถรายงานเกี่ยวกับประเด็นการประเมินความเสี่ยงที่มีความสำคัญ และรายงานสิ่งที่ต้องปรับปรุงภายในองค์กรให้ผู้บริหารทราบถึงความเสี่ยงต่าง ๆ ให้ผู้บริหารสามารถรับรู้ถึงทิศทางการบริหารจัดการองค์กร นอกจากนี้ผู้ตรวจสอบภายในยังมีส่วนเป็นอย่างมากในการช่วยการปรับปรุงระบบการควบคุมภายใน ความสำคัญดังที่กล่าวมานี้ทำให้ทีมผู้ตรวจสอบภายในสามารถเป็นที่ปรึกษาในองค์กร และเป็นเครื่องมือสำหรับกระตุ้นการปรับปรุงแนวทางการปฏิบัติงานขององค์กรได้เป็นอย่างดี (Pedneault, 2009)

คุณสมบัติของผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

คุณสมบัติที่เหมาะสมของผู้ตรวจสอบภายในตามมาตรฐานการตรวจสอบภายใน ซึ่งเป็นปัจจัยที่จะส่งผลให้การตรวจสอบภายในมีประสิทธิผลในการจัดการความเสี่ยงขององค์กร ดังนั้นผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศจะต้องปฏิบัติหน้าที่อย่างมีประสิทธิภาพ

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

โดยพึงประพฤติปฏิบัติตนภายใต้กรอบความประพฤติที่ดีงามอันที่จะนำมาซึ่งหลักประกันความเชื่อมั่น และให้คำปรึกษาอย่างเที่ยงธรรมเป็นอิสระเปี่ยมด้วยคุณภาพ ซึ่งจะต้องมีความเชี่ยวชาญในด้านต่าง ๆ (Cascarino, 2007) ดังนี้

- มีทักษะเชิงความคิดในการวิเคราะห์และวิจารณ์เรื่องต่าง ๆ ในทางสร้างสรรค์เพื่อให้การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีคุณภาพ

- มีความเข้าใจอย่างเพียงพอในเรื่องที่เกี่ยวกับผู้รับการตรวจสอบในแต่ละหน่วยงาน หรือระบบต่าง ๆ ที่เกี่ยวข้องกับการตรวจสอบภายในระบบความมั่นคงปลอดภัยระบบสารสนเทศ

- มีแนวคิดใหม่ ๆ เกี่ยวกับหลักเกณฑ์ และเทคนิคในการควบคุมการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินการตรวจสอบภายในมีคุณภาพ และมีความน่าเชื่อถือ

- มีความตระหนักและเข้าใจเกี่ยวกับความเสี่ยง และโอกาสเกิดความเสี่ยงที่เกี่ยวข้องต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินโครงการความมั่นคงปลอดภัยระบบสารสนเทศ

- สามารถประยุกต์ใช้วิธีการตรวจสอบที่หลากหลายในการเลือกข้อมูล การรวบรวมข้อมูล การประเมินผล และเอกสารเกี่ยวกับการตรวจสอบต่าง ๆ ได้

- สามารถรายงานผลการตรวจสอบภายในด้วยรูปแบบที่มีความหลากหลาย ต่อผู้รับข้อมูลที่มีความแตกต่างกัน

- มีความซื่อสัตย์ในการปฏิบัติหน้าที่การตรวจสอบภายในด้วยความซื่อสัตย์ ขยันหมั่นเพียร และมีความรับผิดชอบ

- ผู้ตรวจสอบภายในต้องเปิดเผยหรือรายงานข้อเท็จจริงอันเป็นสาระสำคัญทั้งหมดที่ตรวจพบ ซึ่งหากละเว้นไม่เปิดเผยหรือไม่รายงานข้อเท็จจริงดังกล่าวแล้ว อาจจะทำให้รายงานบิดเบือนไปจากข้อเท็จจริง หรือเป็นการปิดบังการกระทำผิดกฎหมาย

- ผู้ตรวจสอบภายในต้องไม่นำข้อมูลต่างๆ ที่ได้รับจากการปฏิบัติงานไปใช้แสวงหา ผลประโยชน์เพื่อตนเอง และจะไม่กระทำการใด ๆ ที่ขัดต่อกฎหมาย

- เมื่อเสร็จสิ้นการตรวจสอบภายใน และพบความไม่สอดคล้อง ผู้ตรวจสอบภายในต้องติดตามผลการตรวจสอบภายใน พร้อมทั้งรายงานเพื่อให้คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้รับทราบถึงผลการดำเนินงาน

นอกจากนี้ผู้ตรวจสอบภายในยังต้องมีความรู้ความเข้าใจในจรรยาบรรณเกี่ยวกับวิชาชีพของผู้ตรวจสอบ เช่น มีความรู้ความเข้าใจ เข้าใจแนวความคิดเกี่ยวกับความเป็นอิสระ และความเที่ยงธรรมของผู้ตรวจสอบภายใน

ประโยชน์ของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นการพัฒนาด้านความมั่นคงปลอดภัยสารสนเทศ และระบบงานอื่น ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ส่งผลให้เกิดการสร้างเพิ่มมูลค่าให้แก่องค์กร มีประโยชน์กับผู้เกี่ยวข้องดังนี้ (Moeller, 2009)

1. ประโยชน์ต่อผู้บริหาร การตรวจสอบภายในถือเป็นการให้ข้อมูลต่าง ๆ แก่ฝ่ายบริหารเพื่อประโยชน์ในการตัดสินใจวางแผนการดำเนินงานต่าง ๆ และให้คำปรึกษากับฝ่ายบริหารในการปรับปรุงประสิทธิภาพการทำงาน ดูแลให้มีการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศให้เกิดประโยชน์สูงสุดต่อองค์กรและผู้บริหารสามารถรับมือกับความเสี่ยงที่อาจจะเกิดขึ้นได้อย่างเหมาะสม

2. ประโยชน์ต่อองค์กร องค์กรมีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศซึ่งสอดคล้องกับข้อกำหนด และระเบียบปฏิบัติให้แก่เจ้าหน้าที่ทุกระดับได้ถือปฏิบัติ มีการตรวจสอบ และประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัย

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

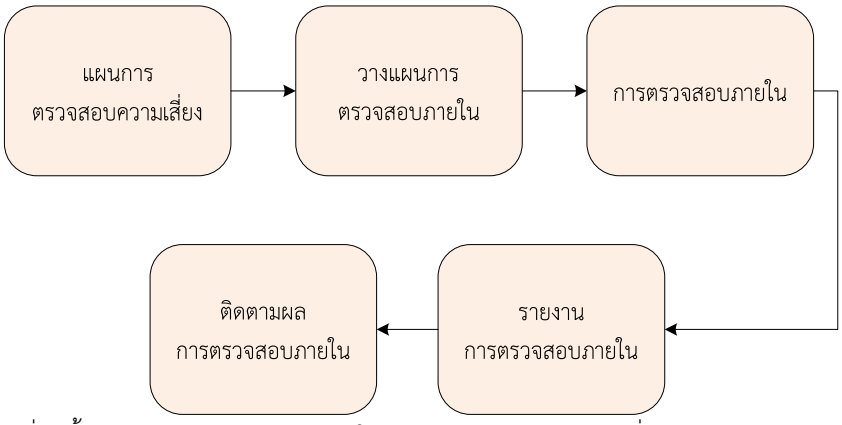
ของระบบเทคโนโลยีสารสนเทศ ผู้บริหารสามารถติดตามประเมินผลการปฏิบัติงานในองค์กรได้อย่างมีประสิทธิภาพ ซึ่งทั้งหมดนี้จะนำมาซึ่งการปรับปรุงคุณภาพอย่างต่อเนื่อง

3. ประโยชน์ต่อบุคลากร สร้างความตระหนักในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และสามารถนำไปประยุกต์ใช้ในชีวิตประจำวันได้ ด้านทรัพยากรบุคคลทำให้พนักงานสามารถเข้าใจถึงความเสี่ยงในฐานะที่เป็นส่วนหนึ่งของการปฏิบัติหน้าที่ประจำวัน

4. ประโยชน์ต่อผู้รับตรวจ การตรวจสอบภายในถูกกำหนดให้มีการทำการตรวจสอบอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการควบคุมคุณภาพภายใน และทำให้การทำงานมีประสิทธิภาพและประสิทธิผล ซึ่งจะส่งผลให้เกิดการปรับปรุงคุณภาพของการทำงานอย่างต่อเนื่อง และเป็นการกระตุ้นให้เจ้าหน้าที่มีความกระตือรือร้นในการปฏิบัติงานในหน้าที่ของตน เอาใจใส่ระมัดระวังรอบคอบ มีผลทำให้ลดความผิดพลาดและก่อให้เกิดประสิทธิภาพในการทำงาน

กระบวนการของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

นับตั้งแต่ปี 2002 ที่มีการประกาศใช้มาตรฐาน ISO 19011 ซึ่งเป็นมาตรฐานเกี่ยวกับแนวทางในการตรวจประเมินเพื่อให้เป็นแนวทางสำหรับการตรวจประเมินระบบบริหารคุณภาพ เพื่อให้สอดคล้องกับขั้นตอนกระบวนการที่เกี่ยวข้องกับการตรวจสอบด้านระบบความมั่นคงปลอดภัยสารสนเทศโดยเฉพาะจึงต้องมีการปรับเปลี่ยนรูปแบบการตรวจประเมิน กระบวนหลักๆ ของการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศดังแสดงในภาพที่ 1 (Gracyalny, 2009; Russell, 2007)



ภาพที่ 1 ขั้นตอนของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1. ขั้นตอนการวางแผนการตรวจสอบความเสี่ยง กระบวนการตรวจสอบภายในเริ่มต้นด้วยแผนการตรวจสอบความเสี่ยง (Risk Based Audit) ซึ่งได้รับการประเมินและปรับปรุงเป็นประจำทุกปี แผนการตรวจสอบความเสี่ยงนี้จะกลายเป็นแนวทางในการดำเนินการตรวจสอบในปีต่อ ๆ ไป นอกเหนือจากการตรวจสอบภายใต้แผนงานแล้วหน่วยตรวจสอบภายในยังมีส่วนร่วมในการดำเนินการประเมินความเสี่ยง และให้คำปรึกษาตามความต้องการต่าง ๆ ของเจ้าหน้าที่ในหน่วยงาน

2. ขั้นตอนการวางแผนการตรวจสอบภายใน ขั้นตอนการวางแผนยังรวมถึงการประชุมเบื้องต้นเพื่อหารือเกี่ยวกับวัตถุประสงค์ระยะเวลาและข้อมูลสำคัญอื่น ๆ ที่สามารถช่วยลดขั้นตอนการตรวจสอบภายในในกระบวนการนี้ผู้ตรวจสอบภายในอาจขอตรวจสอบข้อมูลต่าง ๆ เช่น เอกสารที่เกี่ยวข้องกับการดำเนินโครงการ แผนภูมิองค์กร และรายชื่อผู้ติดต่อต่างๆ ทีม

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

ผู้ตรวจสอบภายในจะต้องเตรียมเอกสารการทำงาน เช่น ใบตรวจสอบ (Checklists) แผนการสุ่มตัวอย่างสำหรับการตรวจสอบภายใน และรูปแบบสำหรับการบันทึก เช่น หลักฐานสนับสนุน สิ่งที่พบจากการตรวจประเมิน และบันทึกการประชุมเป็นต้น

3. ขั้นตอนการดำเนินการตรวจสอบภายในเป็นส่วนที่ใช้เวลานานที่สุดในการตรวจสอบภายใน โดยผู้ตรวจสอบภายในจะรวบรวมข้อมูลเกี่ยวกับการปฏิบัติงานของผู้ตรวจประเมิน ความเข้าใจเกี่ยวกับหน้าที่ของหน่วยงานและระบุจุดแข็งและจุดอ่อน รวมถึงการทบทวนกิจกรรมขั้นตอนเกี่ยวกับการบริหารงานต่าง ๆ และกิจกรรมอื่นๆ ที่เฉพาะเจาะจงสำหรับแต่ละส่วนของหน่วยงาน ผู้ตรวจสอบภายในอาจจะสัมภาษณ์กระบวนการที่มีส่วนสำคัญในการดำเนินงานต่างๆ และตรวจสอบความคืบหน้าของการดำเนินงานกับหัวหน้าหน่วย และบุคลากรของหน่วย ในขั้นตอนสุดท้ายนี้จะทำให้ผู้ตรวจสอบภายในสามารถระบุขอบเขตของความเสี่ยงต่าง ๆ ในการควบคุมภายในขององค์กร

4. ขั้นตอนการจัดทำรายงานการตรวจสอบภายในการรายงานผลการตรวจสอบภายใน เป็นการจัดเตรียมรายงานการตรวจสอบภายในต่อคณะกรรมการบริการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (ISMS Operation Team) และผู้รับตรวจระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตรวจสอบเพื่อพิจารณาผลการตรวจสอบภายใน ที่สำคัญผลการตรวจสอบภายในจะต้องมีความสมบูรณ์ ถูกต้อง เที่ยงตรง และมีความชัดเจน

5. ขั้นตอนการติดตามผลการตรวจสอบภายในเป็นขั้นตอนการติดตามผลการแก้ไข และปรับปรุงความไม่สอดคล้อง หรือข้อเสนอแนะต่าง ๆ ของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ผู้ถูกตรวจสอบภายในจะต้องมีการแจ้งถึงสถานะของการดำเนินการ ให้กับผู้ที่รับผิดชอบการตรวจสอบภายใน ได้รับทราบด้วย

ปัจจัยความสำเร็จของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การตรวจสอบภายในจะประสบความสำเร็จและเป็นประโยชน์ต่อองค์กรในระดับใดนั้นขึ้นอยู่กับปัจจัยพื้นฐานความสำเร็จที่สำคัญ (Alshbiel, 2017) ดังนี้

1. การสนับสนุนของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การตรวจสอบภายในจะพัฒนาไปในทิศทางใดต้องมาจากนโยบายของคณะกรรมการบริหาร โดยต้องกำหนดวัตถุประสงค์และแสดงการสนับสนุนงานตรวจสอบภายในด้านต่าง ๆ ให้ชัดเจน เพื่อแสดงถึงการมีระบบกำกับดูแลและการควบคุมภายในที่ดี

2. วัฒนธรรมองค์กร และความเข้าใจขององค์กร วัฒนธรรมขององค์กรคือพฤติกรรมขององค์กรในการเข้าใจและร่วมมือในงานตรวจสอบภายใน ซึ่งเป็นปัจจัยสำคัญในการเพิ่มความสำเร็จของงานตรวจสอบภายใน

3. ความรู้ ทักษะต่าง ๆ และมนุษยสัมพันธ์ของผู้ตรวจสอบภายใน งานตรวจสอบภายในเป็นการประยุกต์ใช้เทคนิคต่าง ๆ ในการตรวจสอบ เช่น การคิดวิเคราะห์สังเคราะห์ วิธีการประเมิน การบริหารจัดการสมัยใหม่ การประยุกต์ใช้ความรู้ด้านคอมพิวเตอร์ในการตรวจสอบ รวมไปถึงเทคนิคหรือทักษะการสังเกต ทักษะการสื่อสารและมนุษยสัมพันธ์ในการให้คำปรึกษาในด้านต่าง ๆ และผู้ตรวจสอบภายในต้องมีการพัฒนาความรู้ให้ทันสมัยอยู่เสมอ

4. ความพร้อมของระบบงานและสารสนเทศงานตรวจสอบภายในเกี่ยวข้องกับการวิเคราะห์ และประเมินผล ซึ่งต้องอาศัยหลักฐานข้อมูลเพื่อสนับสนุนทั้งข้อมูลในด้านต่าง ๆ และการปฏิบัติงาน ดังนั้นการที่มีระบบงานและข้อมูลสารสนเทศพร้อมกว่าย่อมพัฒนางานตรวจสอบภายในได้เร็วกว่าการที่ไม่มีระบบข้อมูลหรือระบบยังล้าสมัยหรือเชื่อถือไม่ได้

5. การทำงานเป็นทีม มีความสำคัญในทุกองค์กรเป็นสิ่งจำเป็นในการเพิ่มประสิทธิภาพและประสิทธิผล

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

ของการบริหารงาน ความสำเร็จของการปฏิบัติงานต้องอาศัยความร่วมมือของทุกคนในทีมเป็นสิ่งสำคัญ

อุปสรรคของการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การตรวจสอบภายในเพื่อประเมินการปฏิบัติตามนโยบายขั้นตอนระบบและกระบวนการต่าง ๆ จุดมุ่งหมายคือการวิเคราะห์ช่องโหว่ (Gap Analysis) เพื่อให้การปรับปรุงคุณภาพเกิดขึ้น ปัญหาที่พบบ่อยที่สุดเกี่ยวกับการตรวจสอบภายในมีดังนี้ (Moeller, 2009)

1. ปัญหาโครงสร้างหลักขององค์กร ระบบการควบคุมภายในบางครั้งที่ใช้อยู่ล้าสมัยทั้งรูปแบบ และความเชื่อ โดยเน้นเฉพาะส่วนย่อยของกิจกรรมที่จะก่อให้เกิดการควบคุม โดยขาดผู้รับผิดชอบที่แท้จริง
2. ปัญหาความเชื่อและทัศนคติความเชื่อของสังคมโดยรวมยังคงมีทัศนดติเกี่ยวกับการตรวจสอบทุกประเภทคือ เป็นการจับผิด ส่งผลให้ต่างฝ่ายต่างไม่ให้ความไว้วางใจซึ่งกันและกัน
3. ปัญหาเรื่ององค์ความรู้และประสบการณ์ของผู้ตรวจสอบภายใน ถ้าผู้ตรวจสอบภายไม่มีองค์ความรู้ที่เหมาะสม และเพียงพอสำหรับการเป็นผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งถ้าผู้ตรวจสอบภายในขาดความรู้ และประสบการณ์ จะส่งผลต่อการตรวจสอบภายในโดยตรง ดังนั้นผู้บริหารควรให้ความสำคัญกับการเพิ่มพูลทักษะและองค์ความรู้ให้กับทีมผู้ตรวจสอบภายใน
4. ปัญหาต้นทุนและค่าใช้จ่ายในการตรวจสอบถือเป็นปัจจัยที่สำคัญมาก ๆ เพราะว่าในการตรวจสอบภายในแต่ละครั้งถือเป็นต้นทุนที่สูง เมื่อมีค่าดำเนินการค่าเดินทางเข้ามาเกี่ยวข้อง เช่น เวลา และทุนทรัพย์ในการอบรมผู้ตรวจสอบภายใน
5. ขาดอิสรภาพในการตรวจสอบในการปฏิบัติหน้าที่ตรวจสอบภายใน ผู้ตรวจสอบภายในควรมีอิสระภาพไม่ขึ้นตรงกับหน่วยงานใดหน่วยงานหนึ่ง

วิธีการจัดสร้างให้มีผู้ตรวจสอบภายในสำหรับองค์กร

ในการจัดตั้งทีมผู้ตรวจสอบภายในควรเริ่มต้นจากการจัดหาบริษัทจากภายนอกเพื่อร่วมดำเนินการและองค์กรควรแต่งตั้งเจ้าหน้าที่ในหน่วยงานเพื่อเรียนรู้ระบบการดำเนินการตรวจสอบภายในไปพร้อม ๆ กันกับการเริ่มดำเนินโครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะเป็นการผสมผสานการจัดหาทรัพยากรทั้งภายในองค์กรซึ่งมีเจ้าหน้าที่ภายในหน่วยงาน และภายนอกคือบริษัทที่ปรึกษาเพื่อให้คำปรึกษาในการจัดสร้างโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ กระบวนการทำงานของการตรวจสอบภายในที่มีเจ้าหน้าที่ภายในหน่วยงานได้เรียนรู้วิธีการทำงานจากผู้เชี่ยวชาญภายนอกถือว่าเป็นวิธีที่ดีที่สุด โดยใช้ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการในการตรวจสอบภายในจากหน่วยงานภายนอกได้ให้ความรู้กับเจ้าหน้าที่ภายในที่ทำหน้าที่เป็นผู้ตรวจสอบภายในโดยมีข้อกำหนดว่าจะต้องไม่ดำเนินการตรวจสอบในกลุ่มงาน หรือส่วนงานที่ผู้ตรวจสอบภายในสังกัดอยู่

คำแนะนำต่าง ๆ เกี่ยวกับการตรวจสอบภายในของที่ปรึกษาด้านการตรวจสอบภายในที่มีประสบการณ์และมีความความเชี่ยวชาญ จะส่งผลทำให้ผู้ตรวจสอบภายในได้ประสบการณ์ตรงจากการเริ่มทำหน้าที่การตรวจสอบภายในของหน่วยงาน นอกจากนี้สิ่งสำคัญที่สุดผู้ตรวจสอบภายในควรผ่านการอบรมหลักสูตรการตรวจสอบภายในเพื่อเพิ่มขีดความสามารถในการปฏิบัติหน้าที่ที่ได้รับมอบหมาย ซึ่งจะส่งผลต่อต่อความสำเร็จในการดำเนินโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Fountain, 2016)

ข้อดีขององค์กรที่มีผู้ตรวจสอบภายใน

ผู้ตรวจสอบภายในเป็นกลไกสำคัญที่จะทำให้การบริหารจัดการองค์กรเกิดความโปร่งใส ตรวจสอบได้ สนับสนุนให้มีกระบวนการกำกับดูแลที่ดี ทำให้เกิดความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรม เป็นอิสระในการดำเนินงานด้านต่าง ๆ ให้แก่ผู้บริหารตลอดจนผู้มีส่วนได้ส่วนเสียขององค์กร เสริมสร้าง

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

จริยธรรมและคุณค่าและมีการพัฒนาที่เหมาะสมภายในองค์กร สามารถให้ความเชื่อมั่นในเรื่องที่เกี่ยวกับการดำเนินกิจกรรมต่าง ๆ ขององค์กร

ผู้ตรวจสอบภายในมีส่วนสนับสนุนประสิทธิภาพของกระบวนการควบคุมการบริหารความเสี่ยงและเป็นการกำกับดูแลกิจการที่ดี เกิดการประเมินผลและปรับปรุงกระบวนการกำกับดูแลเพื่อให้บรรลุวัตถุประสงค์ของการดำเนินงานต่าง ๆ เป็นหลักประกันการบริหารจัดการภายในองค์กร ผู้ปฏิบัติงานมีความรับผิดชอบในผลงานตามหน้าที่ที่ได้รับมอบหมาย และผู้ตรวจสอบภายในยังเป็นสื่อกลางที่ช่วยในการสื่อสารข้อมูลความเสี่ยงและ ติดตามการดำเนินการตามการควบคุมภายในหน่วยงานไปยังส่วนงานต่าง ๆ เพื่อให้เกิดการปรับปรุงระบบการทำงานขององค์กรที่ดีขึ้น (Berber et al., 2012) เช่น ผู้ตรวจสอบภายในตรวจพบว่ามีข้อบกพร่องในขั้นตอนของการประเมินและติดตามการดำเนินการตามแผนบริหารจัดการความเสี่ยง ของทีมงานต่าง ๆ ในหน่วยงาน ซึ่งหากผู้ตรวจสอบภายในไม่มีการตรวจสอบ และทบทวนการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยแล้ว ความเสี่ยงที่หน่วยงานมีการวิเคราะห์แล้วจะไม่มีการติดตามและไม่ได้นำมาบริหารจัดการอย่างเป็นรูปธรรม ส่งผลทำให้เป็นความเสี่ยงใหญ่ของหน่วยงานและเกิดผลกระทบต่อองค์กรได้ เพราะการวิเคราะห์ความเสี่ยงถือเป็นภารกิจหลัก ๆ ที่สำคัญของการดำเนินการตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อเสียขององค์กรที่ไม่มีผู้ตรวจสอบภายใน

ในกรณีองค์กรไม่มีผู้ตรวจสอบภายในจะส่งผลโดยตรงคือความเสี่ยงที่สำคัญต่าง ๆ ขององค์กรจะไม่ได้รับการประเมินและตรวจติดตามการดำเนินการแก้ไข ทั้งนี้ แต่ในสถานการณ์จริงการตรวจสอบภายในยังไม่สามารถพบความเสี่ยงได้ทั้งหมด และมีส่วนส่งผลให้เกิดการทุจริตในการบริหารจัดการองค์กรไม่สามารถตรวจสอบผลการดำเนินการปฏิบัติงานได้อย่างชัดเจน ทำให้ความเชื่อมั่นจากภายในหรือภายนอกองค์กรลดลง (Obert & Munyunguma, 2014) เช่น ถ้าองค์กรไม่มีผู้ตรวจสอบภายใน หรือกระบวนการตรวจสอบภายในก็จะทำให้การควบคุมกระบวนการในการดำเนินงานภายใต้โครงการความมั่นคงปลอดภัยสารสนเทศ รวมไปถึงการเน้นย้ำให้ผู้บริการทราบถึงผลของการดำเนินงานไม่สามารถเกิดขึ้นได้ ซึ่งเป็นสาเหตุหลักที่ทำให้ไม่สามารถบรรลุวัตถุประสงค์ของการดำเนินโครงการความมั่นคงปลอดภัยสารสนเทศ

ความท้าทายของการตรวจสอบภายในในยุคปัจจุบัน

เพื่อเป็นการเตรียมความพร้อมสำหรับผู้ตรวจสอบภายในในยุคปัจจุบัน ความท้าทายที่ผู้ตรวจสอบภายในต้องคำนึงถึงมีดังนี้ (กรมบัญชีกลาง, 2555; Williams, 2002; Ridley, 2008)

1. กฎระเบียบและกฎหมายต่าง ๆ ที่เกี่ยวข้องกับการตรวจสอบภายใน ผู้ตรวจสอบภายในจะต้องมีความเข้าใจเกี่ยวกับกฎระเบียบและกฎหมายต่าง ๆ ที่เกี่ยวข้องกับหน่วยงานและพิจารณาถึงความสอดคล้องกับกับการดำเนินงานและการปฏิบัติงานว่าเป็นไปตามนโยบายต่าง ๆ ที่ได้วางไว้รวมทั้งสามารถให้ความเห็นแก่ผู้บริหารได้

2. กระบวนการทำงาน ผู้ตรวจสอบภายในจะต้องมีการปรับกระบวนการทำงานตรวจสอบภายในให้มีประสิทธิภาพ และสอดคล้องกับภารกิจขององค์กรเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานให้ดีขึ้น อย่างน้อยผู้ตรวจสอบภายในจำเป็นจะต้องพัฒนา และรักษามาตรฐานการทำงานของตนให้เป็นไปตามมาตรฐานการตรวจสอบภายใน

3. ความรู้เกี่ยวกับระบบงานที่ทำการตรวจสอบ ผู้ตรวจสอบภายในจะต้องทราบถึงระบบงานของหน่วยงานให้มากที่สุด หากผู้ตรวจสอบภายในเข้าใจระบบงานเป็นอย่างดีแล้ว จะส่งผลให้ผู้ตรวจสอบภายในสามารถประเมินความเสี่ยง และการควบคุมการเปลี่ยนแปลงภายในในด้านต่าง ๆ ที่เกิดขึ้นได้อย่างชัดเจนและครอบคลุมยิ่งขึ้น

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

4. ทักษะด้านภาษา ในปัจจุบันภาษาอังกฤษเป็นภาษาต่างประเทศที่มีความสำคัญเป็นอย่างมากสำหรับการติดต่อสื่อสารในรูปแบบต่าง ๆ ดังนั้นในอนาคตอันใกล้จึงจำเป็นอย่างยิ่งที่ผู้ตรวจสอบภายในจะต้องมีการพัฒนาศักยภาพหรือทักษะด้านภาษาให้มีความเชี่ยวชาญมากยิ่งขึ้น

5. วัฒนธรรมขององค์กร ผู้ตรวจสอบภายในอาจต้องมีการติดต่อประสานงานระหว่างหน่วยงาน ส่งผลให้ผู้ตรวจสอบภายในจะต้องมีความเข้าใจในวัฒนธรรมขององค์กร เพื่อให้การติดต่อประสานงานเป็นไปอย่างราบรื่นและมีประสิทธิภาพ

แนวโน้มหน่วยงานที่ได้รับการรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

การออกใบรับรอง (Certification) เป็นวิธีหนึ่งที่จะสามารถรับรองได้ว่าองค์กรมีระบบบริหารความมั่นคงปลอดภัยของข้อมูล และสารสนเทศที่เกี่ยวข้องกับการดำเนินงานต่างๆ ที่มีประสิทธิภาพตามมาตรฐานของความมั่นคงปลอดภัยสารสนเทศ (ISO27001) และมาตรฐานดังกล่าวนี้กำลังได้รับความนิยมมากขึ้นในหลายธุรกิจทุกประเทศทั่วโลก สำหรับประเภทธุรกิจ 10 อันดับแรกที่ขอรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศทั้งหมด เริ่มตั้งแต่ปี พ.ศ. 2549 – พ.ศ. 2560 ดังตารางที่ 1 (International Organization for Standardization, 2018)

ตารางที่ 1 แสดงกลุ่มธุรกิจที่มีการขอรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

ประเภทธุรกิจที่ขอรับรองมาตรฐาน ISO27001	2549	2550	2551	2552	2553	2554	2555	2556	2557	2558	2559	2560	รวม
เทคโนโลยีสารสนเทศ	890	1236	1152	2086	3217	3588	4558	5059	4933	5573	6578	7478	46348
ขนส่งและสื่อสาร	60	70	63	170	184	241	288	322	327	301	401	930	3357
ก่อสร้าง	55	17	12	127	266	350	409	396	454	186	216	193	2681
ไฟฟ้า	38	58	50	135	221	280	342	289	287	296	311	316	2623
วิศวกรรม	25	33	48	173	122	126	189	211	217	201	245	382	1972
การเงิน	47	54	68	148	185	113	138	169	187	197	250	344	1900
ค้าส่งและค้าปลีก	12	38	26	93	164	214	215	224	206	198	202	283	1875
สุขภาพ	14	10	61	102	102	145	201	201	215	231	220	216	1718
การบริการ	23	33	79	181	79	106	155	192	191	212	235	185	1671
การพิมพ์	34	84	30	62	78	101	121	148	126	143	130	187	1244

ที่มา: ดัดแปลงมาจากรายงานการรับรองมาตรฐานระบบการจัดการ องค์การมาตรฐานสากล (ISO)

จากตารางที่ 1 จะพบว่ากลุ่มธุรกิจที่เกี่ยวข้องการเทคโนโลยีสารสนเทศมีการขอรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศตั้งแต่ปี พ.ศ. 2549 – พ.ศ. 2560 มากที่สุดถึง 46,348 และยังพบว่าในกลุ่มธุรกิจอื่น ๆ ทั่วโลกก็ได้มีการขอรับรองในมาตรฐานดังกล่าวส่วนใหญ่มีแนวโน้มมากขึ้นเช่นกัน

ในประเทศแถบเอเชียแปซิฟิคหลาย ๆ ประเทศเริ่มให้ความสำคัญของการขอรับรองมาตรฐาน

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

ความมั่นคงปลอดภัยสารสนทศ ดังจะเห็นได้ว่ามีหลาย ๆ ประเทศมีจำนวนการขอรับรองเพิ่มมากขึ้นทุกปี ดังตารางที่ 2 (International Organization for Standardization, 2018)

ตารางที่ 2 แสดงจำนวนการได้รับการรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศในกลุ่มประเทศเอเชียแปซิฟิค

ประเทศ	2549	2550	2551	2552	2553	2554	2555	2556	2557	2558	2559	2560	รวม
ญี่ปุ่น	3790	4896	4425	5508	6237	6914	7199	7140	7171	8240	8945	9161	79626
ใต้หวัน	159	256	702	934	1028	791	855	918	781	939	1087	994	9444
เกาหลีเหนือ	50	77	94	174	166	191	230	252	288	305	364	369	2560
ออสเตรเลีย	59	55	63	55	82	94	113	138	157	176	531	404	1927
มาเลเซีย	18	23	34	38	60	72	100	181	232	240	260	317	1575
ไทย	7	9	16	34	39	76	96	125	143	189	218	287	1239
ฮ่องกง	29	36	59	72	78	99	110	124	125	141	173	182	1228
สิงคโปร์	7	17	36	41	43	68	65	84	84	93	112	123	773
ฟิลิปปินส์	10	24	27	47	38	59	66	73	47	38	168	174	771
อินโดนีเซีย	2	3	7	13	22	29	35	48	62	65	115	222	623
เวียดนาม	1	2	7	5	21	36	44	39	94	70	64	198	581
มาเก๊า	2	5	2	7	9	12	13	15	16	19	13	14	127
เกาหลีใต้			95		1		1		2	1	1	2	103
นิวซีแลนด์	1	1	4	5	5	5	5	12	1	7	27	28	101
มองโกเลีย								1	1	1	2	2	7
ลาว										1	2	4	7
กัมพูชา				1	1						1	4	7
เมียนมาร์				1	1						1	1	4
ฟิจิ								1			2	1	4
วานูอาตู												1	1
ปาปัวนิวกินี												1	1
ปาเลา												1	1
ไมโครซีเนีย												1	1
หมู่เกาะ													
มาร์แชลล์												1	1
บรูไน												1	1

ที่มา: ดัดแปลงมาจากรายงานการรับรองมาตรฐานระบบการจัดการ องค์การมาตรฐานสากล (ISO)

จากตารางที่ 2 จะเห็นได้ว่าหลาย ๆ หน่วยงานในแต่ละประเทศได้ให้ความสำคัญกับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพิ่มมากขึ้นเรื่อย ๆ เริ่มตั้งแต่ปี พ.ศ. 2549 เป็นต้นมา ซึ่งประเทศที่ได้รับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศมากเป็นอันดับที่หนึ่ง คือ ประเทศญี่ปุ่น มีหน่วยงานที่ได้รับการรับรองตั้งแต่ปี พ.ศ. 2549 ถึง พ.ศ. 2560 มากถึง 79,626 แห่ง ส่วนประเทศไทยมีหน่วยงานที่ได้รับการรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศรวมทั้งสิ้น 1,239 แห่ง และมีแนวโน้มเพิ่มสูงขึ้นทุกปี

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

ในประเทศไทยมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO27001) เริ่มเข้ามามีบทบาทสำคัญ โดยภาครัฐได้ให้ความสำคัญ และสนับสนุนในเรื่องต่าง ๆ เช่น การนำมาตรฐานดังกล่าวมาแปลเป็นภาษาไทย และแนะนำให้หน่วยงานที่มีภารกิจเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศนำเอามาตรฐานดังกล่าวมาประยุกต์ใช้ในองค์กร ประเด็นที่สำคัญที่สุดก็คือ มีการนำมาตรฐานดังกล่าวไปใช้เป็นรากฐานในการพัฒนากฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายด้าน ICT ของประเทศหลายๆ ฉบับ ได้แก่ พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

จากปัจจัยทั้งหลายข้างต้น ทำให้การประยุกต์ใช้ความมั่นคงปลอดภัยสารสนเทศ (ISO27001) ได้กลายเป็นส่วนหนึ่งในแผนแม่บทด้านสารสนเทศของหลาย ๆ องค์กรในทุกประเภทธุรกิจ เพื่อยกระดับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศภายในองค์กรเอง รวมถึงสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียกับองค์กร ตลอดจนช่วยสร้างความมั่นใจว่าองค์กรจะสามารถปฏิบัติภารกิจได้อย่างถูกต้องตามกฎหมายและมีความมั่นคงปลอดภัย

กรณีศึกษาของการตรวจสอบภายในโครงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในสถานพยาบาล

การพัฒนาโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือ ISO/ IEC 27001:2013 ของฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ได้เริ่มดำเนินโครงการเมื่อเดือนตุลาคม พ.ศ. 2558 ทำให้ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้รับการรับรองตามมาตรฐาน ISO27001:2013 เมื่อเดือนกรกฎาคม พ.ศ. 2560 การดำเนินโครงการดังกล่าวส่งผลให้ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาลได้มีการพัฒนามาตรฐานในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศเทียบเท่ามาตรฐานสากล

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล เป็นโรงพยาบาลขนาดใหญ่ในสังกัดมหาวิทยาลัยมหิดล มีผู้ป่วยนอกมารับบริการตลอดทั้งปีจำนวนมากถึง 3.7 ล้านคนต่อปี และผู้ป่วยในจำนวน 8.2 หมื่นคนต่อปี คณะฯ ได้นำเทคโนโลยีต่าง ๆ มาเชื่อมโยงระบบสารสนเทศต่าง ๆ และการเก็บข้อมูลของผู้ป่วยที่มาใช้บริการ ดังนั้นเรื่องของความมั่นคงปลอดภัยสารสนเทศจึงเป็นประเด็นสำคัญอย่างยิ่ง เนื่องจากรูปแบบของภัยคุกคามทางคอมพิวเตอร์ในปัจจุบันมีการพัฒนาอย่างรวดเร็ว ซึ่งภัยคุกคามต่าง ๆ อาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ และอาจจะส่งผลให้การให้บริการผู้ป่วยหยุดชะงัก ผลจากการดำเนินงานดังกล่าวทำให้ผู้ป่วยที่มาใช้บริการได้รับประโยชน์โดยตรง และเกิดความเชื่อมั่นที่มีต่อคณะแพทยศาสตร์ศิริราชมากขึ้น เช่น ข้อมูลทางการแพทย์ ข้อมูลการรักษาพยาบาล ผลการตรวจทางห้องปฏิบัติการของผู้ป่วย รวมไปถึงข้อมูลสารสนเทศที่เกี่ยวข้องกับการดำเนินงาน โดยข้อมูลทั้งหมดจะได้รับการปกป้องควบคุมตามมาตรฐานความปลอดภัยสารสนเทศ

ดังนั้น เมื่อมีผู้ป่วยมาใช้บริการโรงพยาบาลเป็นจำนวนมาก การรักษาความปลอดภัยของข้อมูลต่าง ๆ ได้กลายเป็นประเด็นที่สำคัญ ซึ่งโรงพยาบาลมีความจำเป็นต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อเป็นการป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึงข้อมูลผู้ป่วย และข้อมูลต่างๆ ที่จำเป็นในทางการแพทย์ ข้อมูลทางการแพทย์มักจะเป็นข้อมูลที่เป็นความลับที่ละเอียดอ่อนที่อยู่ในความรับผิดชอบโรงพยาบาลจะต้องดูแลเป็นอย่างดี และตรวจสอบข้อมูลเหล่านี้อย่างระมัดระวัง และโรงพยาบาลควรตรวจสอบให้แน่ใจว่าข้อมูลที่มีการบันทึกเข้าไปในระบบนั้นมีความถูกต้อง และไม่ถูกแก้ไขในระหว่างการบันทึกข้อมูล หรือหลังจากที่มีการบันทึกข้อมูลทางการแพทย์ต่าง ๆ ไปแล้ว อย่างไรก็ตาม

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

โรงพยาบาลต้องเผชิญกับปัญหาต่าง ๆ เมื่อต้องมีการปรับปรุงความมั่นคงปลอดภัยระบบสารสนเทศ เช่น ปัญหาเรื่องบุคลากร และข้อจำกัดด้านงบประมาณที่ใช้ในการพัฒนาโครงการ ประเด็นที่สำคัญที่สุดคือขั้นตอนในการดำเนินงานที่เกี่ยวข้องกับโครงการความมั่นคงปลอดภัยสารสนเทศที่เพิ่มมากขึ้น เป็นสาเหตุที่ทำให้บุคลากรในหน่วยงานมีภาระที่เพิ่มมากขึ้น ต้องอาศัยการบริหารการจัดการเปลี่ยนแปลงที่ชัดเจน ประเด็นที่กล่าวมานี้เป็นความท้าทายในยุคปัจจุบันที่ระบบสารสนเทศได้เข้ามามีบทบาทในการบริหารจัดการองค์กร ดังนั้นองค์กรต่าง ๆ ต้องตระหนักถึงความสำคัญของปัญหาต่าง ๆ ที่อาจจะเกิดขึ้นระหว่างการพัฒนาโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

อีกหนึ่งความสำคัญของผู้ตรวจสอบภายในที่ส่งผลให้โครงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศประสบความสำเร็จได้ คือ ผู้ตรวจสอบภายในต้องมีส่วนร่วมในการทำแผนประเมินและร่วมตรวจสอบความเสี่ยง ซึ่งแผนการตรวจสอบความเสี่ยงกลายเป็นแนวทางในการดำเนินการตรวจสอบในปีต่อ ๆ ไป จึงสามารถกล่าวได้ว่าตรวจสอบภายในมีส่วนอย่างยิ่งในการทำหน้าที่ควบคุม พร้อมทั้งตรวจสอบกระบวนการทำงานต่าง ๆ และผลักดันให้ทุกส่วนในองค์กรทำงานภายใต้กรอบและข้อกำหนดของโครงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อย่างไรก็ตามทุก ๆ หน่วยงานสามารถจัดตั้งโครงการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อพัฒนาระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยตามมาตรฐานสากล แต่ข้อจำกัดที่สำคัญของการพัฒนาโครงการดังกล่าว คือ ด้านงบประมาณ และด้านทรัพยากรทางด้านบุคคล อันเนื่องมาจากข้อจำกัดดังกล่าวทำให้ในปัจจุบันพบว่ามีอีกหลายหน่วยงานที่มีการพัฒนาความปลอดภัยในด้านเทคโนโลยีสารสนเทศแต่ไม่มีการขอรับรองความปลอดภัยของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

สรุป

บทบาทและความสำคัญของผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือการร่วมกิจกรรมการบริหารความเสี่ยงและร่วมทำการตรวจสอบภายใน เพื่อส่งเสริมการสร้างกระบวนการควบคุมภายในขององค์กรให้มีประสิทธิภาพ ที่สำคัญผู้ตรวจสอบภายในยังมีหน้าที่อย่างมืออาชีพในการให้มุมมองที่เป็นกลาง มีความเป็นอิสระจากการปฏิบัติงาน ประเมินและรายงานผลการประเมินแก่คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานความมั่นคงปลอดภัยสารสนเทศ (ISMS Operation Team) ซึ่งบทบาทที่ได้กล่าวมาเหล่านี้เป็นส่วนที่สำคัญในการผลักดันให้องค์กรเกิดการพัฒนาอย่างยั่งยืน

ข้อเสนอแนะ

โลกปัจจุบันอยู่ในยุคกระแสโลกาภิวัตน์ ซึ่งในแต่ละวันมีเหตุการณ์หรือการเปลี่ยนแปลงใหม่ ๆ เกิดขึ้นอยู่ตลอดเวลา ซึ่งผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีความจำเป็นต้องหมั่นศึกษาหาความรู้ และติดตามข่าวสารให้ทันโลกปัจจุบัน พร้อมทั้งทำความเข้าใจในปัจจัยต่าง ๆ ที่มีผลต่อการตรวจสอบภายใน และสภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างต่อเนื่องทั้งจากภายในและภายนอกองค์กร ผู้ตรวจสอบภายในคือกลไกสนับสนุนที่มีประสิทธิภาพ ทำให้องค์กรดำเนินงานไปได้อย่างมีประสิทธิภาพ เพิ่มมูลค่าให้แก่องค์กร และสามารถให้ข้อเสนอแนะ คำปรึกษาแก่ผู้บริหารได้อย่างมีประสิทธิภาพ

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จสมบูรณ์ได้จากการสนับสนุนจากฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ที่ได้

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

เล็งเห็นความสำคัญในการพัฒนาโครงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และให้โอกาสผู้เขียนบทความในการปฏิบัติหน้าที่ผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO27001:2013) คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

เอกสารอ้างอิง

กรมบัญชีกลาง. (2555). AEC (ASEAN Economic Community: AEC) กับงานตรวจสอบภายใน. *จุลสารตรวจสอบภายใน. 16*(88), 1-4.

ALshbiel, S. O. (2017). *Internal Auditing Effectiveness Success Model: A Study on Jordanian Industrial Firms.* Al al-Bayt University, Jordan.

Berber, N., & Vugdelija, V. K. (2012). *Internal Audit of Compensations and Benefits: Tasks and Risks in Production Systems. Inzinerine Ekonomika- Engineering Economics. 23*(4), 414-424.

Brown, R. (2009). *A History of Accounting and Accountants.* Edinburgh: General Books LLC.

Cascarino, R. (2007). *Internal Auditing: An Integrated Approach*. (2nd ed.). Lansdowne, South Africa: Juta and Company Ltd.

Fountain, L. (2016). *Leading the Internal Audit Function: Volume 1 of Internal Audit and IT Audit*. Broken Sound Parkway, NW: CRC Press.

Gracyalny, S. (2009). *Guide to Internal Audit.* (2nd ed.). California, CA: Protiviti Inc.

International Organization for Standardization. (2018). *ISO Survey of certifications to management system standards.* Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

Mautz, R. K. (Robert Kuhn) & Sharaf, Hussein A. (1961). *The philosophy of auditing*. Florida: American Accounting Association.

Moeller, R. R. (2009). *Brink's Modern Internal Auditing: A Common Body of Knowledge*. (7th ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

Obert, S. & Munyunguma, I. N. (2014). Internal Audit Perceptions and Their Impact on Performance of the Internal Audit Function. *IOSR Journal of Business and Management, 16*(5), 81-85.

Pedneault, S. (2009). *Techniques and Strategies for Understanding Fraud*. (3rd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Ramamoorti, S. (2003). *Research Opportunities in Internal Auditing*. Florida: The Institute of Internal Auditors.

Ridley. J. (2008). *Cutting Edge Internal Auditing.* West Sussex, England: John Wiley & Sons.

Russell, J.P. (2007). *The Internal Auditing Pocket Guide, Second Edition: Preparing, Performing, Reporting, and Follow-up.* (2nd ed.). Milwaukee, WI: ASQ Quality Press.

Swinkels, W. H. A. (2012). *Exploration of a theory of internal audit: a study on the*

Received: August 8, 2018 , Reviesed: September 17, 2018 , Accepted: November 6, 2018
http://doi.

theoretical foundations of internal audit in relation to the nature and the control systems of Dutch public listed firms Delft: Published doctoral dissertation, University of Amsterdam, Netherlands.

Williams, E.J. (2002). *The Impact of Globalization on Internal Auditors: The Evolution of Internal Auditing*. Brigham Young University, USA.