การสร้างเกณฑ์วัดสมรรถนะด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรในหน่วยงานภาครัฐของประเทศไทย

INFORMATION SECURITY COMPETENCY STANDARD FOR THE MANPOWER IN THAI PUBLIC SECTOR ORGANIZATIONS

อมรศิริ กลีบผึ้ง [1]

ประสงค์ ปราณีตพลกรัง [2]

พิลาศพงษ์ ทรัพย์เสริมศรี [3]

[1, 3] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาระบบสารสนเทศคอมพิวเตอร์ มหาวิทยาลัยศรีปทุม

[2] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

E-mail : [1]aoamon@gmail.com, [2]prasong.pr@spu.ac.th, [3]pilastpongs@yahoo.com

บทคัดย่อ

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อศึกษาการกำหนดมาตรฐานการรับรองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นมาตรฐานสากลและเพื่อจัดทำแนวทางในการพัฒนามาตรฐานของบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศในหน่วยงานภาครัฐของไทย ซึ่งงานวิจัยในครั้งนี้ผู้วิจัยได้ใช้เครื่องมือที่เป็นแบบสอบ ถาม โดยประยุกต์หลักการที่อ้างอิงตามมาตรฐานหลักที่เป็นที่ยอมรับในระดับสากล เช่น มาตรฐานสำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศของกระทรวงกลาโหมสหรัฐ (DoD) มาตรฐาน ISO/IEC 17799/ 27001 มาตรฐานของยุโรป (EUCIP) มาตรฐานองค์ความรู้ที่จำเป็นทางด้านความมั่นคงปลอดภัยสารสนเทศปี 2008 (EBK2008)

ผู้วิจัยได้นำประเด็นที่สำคัญของแต่ละมาตรฐานมาทำการเปรียบเทียบและสร้างเป็นเกณฑ์วัดสมรรถนะด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรในหน่วยงานภาครัฐจำนวน 2 ร่างมาตรฐาน และทำการประชุมกลุ่มผู้เชี่ยวชาญ (Focus Group) จากหน่วยงานภาครัฐ เพื่อคัดเลือกมาตรฐานและปรับปรุงให้เหมาะสมกับการใช้ในประเทศไทยในลำดับต่อไป

ผลจากการศึกษาวิจัยในครั้งนี้จะได้เกณฑ์วัดสมรรถนะด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรในหน่วยงานภาครัฐ ซึ่งหน่วยงานทั้งภาครัฐและเอกชนสามารถนำไปประยุกต์ใช้ในการกำหนดคุณสมบัติบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานตนเองได้ ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยกับข้อมูลและสารสนเทศอยู่ในระดับที่ยอมรับได้

คำสำคัญ : ความมั่นคงปลอดภัยสารสนเทศ ใบรับรองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย มาตรฐาน ISO27001

ABSTRACT

The purpose of this research is to study the standard of security certificated and propose guidelines for development of the standards of information security professionals in public sector organizations. The questionnaires which based on applying the International Standard such as the standard of information security experts of the U.S. Department of Defense (DoD), ISO/IEC 17799/27001, and european certification of informatics professionals (EUCIP), and information technology (IT) security essential body of knowledge (EBK) 2008 are used.

For comparing 2 capability criterions of information security for the manpower of public sector organizations will be formulated and focus group will be used to determine the qualification of information security personals.

The result of this research can be used to identify the performance for IT security personnel in Thai public sector and can be applied to determine the information security personals qualification of the private organizations.

KEYWORDS : Information security**,** Security certification**,** ISO 27001

1. ความเป็นมาและความสำคัญของปัญหา

การนำเทคโนโลยีสารสนเทศมาใช้ให้เหมาะสมในหน่วยงานหรือองค์กร จะต้องให้ความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อไม่ให้ข้อมูล ความลับ รั่วไหลไปสู่องค์กรหรือบุคคลอื่น โดยเฉพาะอย่างยิ่งในหน่วยงานภาครัฐ เพราะเป็นหน่วยงานขนาดใหญ่ ที่มีความสำคัญต่อประเทศ และมีการเชื่อมโยงข้อมูลถึงกัน ซึ่งผู้ที่มีบทบาทสำคัญคือผู้ที่ดูแลระบบและ/หรือผู้ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กรโดยตรง ดังนั้นจึงจำเป็นที่จะต้องมีการบริหารจัดการบุคลากรทางด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานให้เหมาะสม เช่น หน่วยงานที่เกี่ยวข้องกับความมั่นคงของประเทศ จะต้องเก็บรักษาข้อมูลเป็นความลับขั้นสูงสุด เป็นต้น

ในปัจจุบันหลายหน่วยงานได้ให้ความสำคัญกับการสอบใบรับรองผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งมีจุดมุ่งหมายเพื่อพัฒนาศักยภาพของบุคลากรในหน่วยงานให้เป็นที่ยอมรับและทันต่อภัยคุกคามด้านสารสนเทศใหม่ๆที่เกิดขึ้นรวมทั้งเป็นการสร้างความน่าเชื่อถือให้กับหน่วยงานนั้นๆ

ดังนั้นหน่วยงานภาครัฐของไทยซึ่งเป็นหน่วยงานที่ควรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับสูง ควรมีเกณฑ์การวัดสมรรถนะของบุคลากรด้านไอทีทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ได้บุคลากรที่มีความรู้ความสามารถ

2. วัตถุประสงค์ของการวิจัย

การศึกษาวิจัยครั้งนี้ มีวัตถุประสงค์ ดังต่อไปนี้

1. เพื่อศึกษาการกำหนดมาตรฐานการรับรองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ

2. เพื่อนำเสนอแนวทางของเกณฑ์วัดมาตรฐานของบุคลากรทางด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภาครัฐ

3. แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

มาตรฐานสำหรับผู้เชี่ยวชาญทางด้านความปลอดภัยข้อมูลของกระทรวงกลาโหมสหรัฐฯ (Department of Defense (DoD) Directive 8570.1)

DoD Directive เป็นมาตรฐานข้อกำหนด ของรัฐบาลสหรัฐฯ โดยได้กำหนดแนวทางในการปฏิบัติเกี่ยวกับการคัดสรรบุคลากรในเรื่องของการฝึกอบรมและ การสอบวัดความรู้ความสามารถด้านความปลอดภัย ข้อมูลของบุคคลากร โดยอ้างอิงกับประกาศนียบัตรรับรองความรู้ความสามารถจากหลายสถาบัน ซึ่งได้ มีการแบ่งกลุ่มผู้ปฏิบัติหน้าที่ทางด้านความมั่นคงสารสนเทศออกเป็น 2 กลุ่ม ดังนี้คือ

1. Information Assurance Technical (IAT) คือ ผู้ดูแลระบบคอมพิวเตอร์และระบบเครือข่าย

2. Information Assurance Management (IAM) คือ ผู้ที่กำกับดูแลให้การรักษาความมั่นคงปลอดภัยเป็นไปตามระเบียบข้อบังคับหรือมาตรฐานที่กำหนด หรือเป็นกลุ่มผู้บริหาร

การแบ่งระดับของกลุ่ม IAT และ IAM จะมีลักษณะคล้ายกันคือ ในระดับที่ 1 จะเป็นผู้ปฏิบัติงานขั้นต้น มีประสบการณ์น้อยหรือไม่มีประสบการณ์ แต่จะต้องได้ผ่านการฝึกอบรมมาแล้วและมีประกาศนียบัตรที่เกี่ยวข้อง ในระดับถัดมาจะเป็นระดับหัวหน้างานที่มีประสบการณ์พอสมควร มีประกาศนียบัตรขั้นสูงขึ้น ส่วนในระดับสูงสุดจะเป็นผู้ออกนโยบายและการบริหารจัดการงานของแต่ละกลุ่ม

มาตรฐานองค์ความรู้ที่จำเป็นทางด้านความมั่นคงปลอดภัยสารสนเทศปี 2008 (Information Technology Security Essential Body of Knowledge 2008 : EBK 2008)

เป็นมาตรฐานของหน่วยงานการรักษาความมั่นคงปลอดภัยมาตุภูมิของประเทศสหรัฐอเมริกา (DHS) โดยทำงานร่วมกับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยทั้งของภาครัฐและภาคเอกชน เพื่อพัฒนาขอบข่ายงานในระดับสูงและสร้างเป็นแนวทางระดับชาติ มีการอธิบายถึงองค์ประกอบองค์ความรู้และทักษะทางด้านความมั่นคงปลอดภัยสารสนเทศ โดยแบ่งเป็น 14 ขอบเขตความสามารถ ได้แก่ Data Security, Digital Forensics, Enterprise Continuity, Incident Management , IT Security Training and Awareness, IT Systems Operations and Maintenance, Network and Telecommunications Security , Personnel Security, Physical and Environmental Security, Procurement , Regulatory and Standards Compliance, Security Risk Management, Strategic Security Management, System and Application Security

ซึ่งมาตรฐานนี้เป็นแนวทางปฏิบัติที่กล่าวถึงคุณสมบัติของผู้ที่เกี่ยวข้องทางด้านความมั่นคงปลอดภัยสารสนเทศควรมี ทำให้เป็นที่ยอมรับในระดับสากล

ใบรับรองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Security Certification)

Certified Security เป็นการออกใบประกาศเพื่อรับรองความรู้ด้านความมั่นคงปลอดภัยที่ออกโดยองค์กรหรือบริษัทต่างๆ ที่เกี่ยวข้อง โดยมากจะเป็นบริษัทที่ผลิตฮาร์ดแวร์ และซอฟต์แวร์เกี่ยวกับความมั่นคงปลอดภัย

โดยเฉพาะ เช่น CCSP, CISA, GIAC, Security+, CISSP, SSCP เป็นต้น ซึ่งสามารถแบ่งอย่างกว้างๆได้เป็น 3 กลุ่ม ดังต่อไปนี้ คือ

1. Certified Security โดยตรง จะเป็นกลุ่มที่ผ่านการรับรองขั้นพื้นฐานด้านความมั่นคงปลอดภัย ไม่เจาะลึกด้านฮาร์ดแวร์หรือซอฟต์แวร์ของสถาบันใดสถาบันหนึ่ง แต่เป็นที่ยอมรับของสากลเพราะเป็นการรับรองที่เกี่ยวกับความปลอดภัยโดยตรง

2. Hardware Security เป็นกลุ่มที่ผ่านการรับรองที่ออกโดยบริษัทผู้ผลิตอุปกรณ์ฮาร์ดแวร์

3. Software Security เป็นกลุ่มที่ผ่านการรับรองที่เน้นเฉพาะซอฟต์แวร์ครอบคลุมความรู้ เพียงแค่ซอฟต์แวร์ของผู้ผลิตนั้นๆ โดยเฉพาะ จะเหมาะสำหรับบริษัทที่ทำงานเกี่ยวข้องกับซอฟต์แวร์เหล่านั้นโดยตรง

ปัจจุบันหลายหน่วยงานพยายามร่วมมือกันรณรงค์เพื่อสนับสนุนให้มีการสอบใบรับรองมากขึ้น เพราะเป็นการแสดงให้เห็นถึงศักยภาพของหน่วยงาน และสร้างความน่าเชื่อถือ

มาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 17799:2005

มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงภัยให้กับระบบสารสนเทศขององค์กร โดยมาตรฐาน ISO/IEC17799 เป็นเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยขององค์กร จะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 ซึ่งรายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ

สำหรับมาตรฐาน ISO/IEC 27001 นั้นเป็นมาตรฐานเกี่ยวกับการบริหารการรักษาความมั่นคงปลอดภัยข้อมูล และเป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความมั่นคงปลอดภัยข้อมูล (The Information Security Management System (ISMS)) โดยใช้การบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการสร้างและพัฒนาระบบการรักษาความมั่นคงปลอดภัย และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

4. งานวิจัยที่เกี่ยวข้อง

จากการสืบค้นข้อมูลจากแหล่งต่างๆ พบว่ามีงานวิจัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศจำนวนมากที่ใช้มาตรฐาน ISO27001 และมาตรฐานกรอบความคิดต่างๆทางด้านการความมั่นคงปลอดภัยสารสนเทศอาทิ เช่น

นุชนาฏ รงรอง และ วิเชียร ชุติมาสกุล (2551) ได้ทำการวิจัยเรื่องกรอบแนวคิดการตรวจสอบการพัฒนาและตรวจรับระบบและเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ เพื่อศึกษาวิเคราะห์สาเหตุและแนวทางแก้ไขปัญหาของการพัฒนาระบบและเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ โดยนำเสนอกรอบแนวคิด (Framework) การพัฒนาระบบและเทคโนโลยีสารสนเทศ เพื่อให้เกิดประโยชน์สูงสุดและคุ้มค่าต่อการลงทุน

สมยงค์ สีขาว มนต์ชัย เทียนทอง และ สุพจน์ นิตย์สุวัฒน์ (2551) ได้ทำการวิจัยเรื่องการสร้างเกณฑ์วัดสมรรถนะด้านคอมพิวเตอร์และเทคโนโลยีของบุคลากรองค์การปกครองส่วนท้องถิ่น เพื่อสร้างเกณฑ์วัดสมรรถนะด้านคอมพิวเตอร์และเทคโนโลยีและเพื่อเป็นมาตรฐานในการพัฒนาบุคลากรขององค์กรปกครองส่วน

ท้องถิ่น ผลการวิจัยพบว่าบุคลากรในหน่วยงานภาครัฐส่วนใหญ่มีความรู้ความเข้าใจเชี่ยวชาญทางด้านเทคโนโลยีเกี่ยวกับการพิมพ์งานและการใช้อินเทอร์เน็ตสืบค้นข้อมูล

ยุทธพล พิชัยฌรงค์ และ ประสงค์ ปราณีตพลกรัง (2551) ได้ทำการวิจัยเรื่องการวิเคราะห์และประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับองค์การภาครัฐ เป็นการศึกษาและทำการวิเคราะห์ความเสี่ยงและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับองค์การภาครัฐของประเทศไทย โดยอ้างอิงจากมาตรฐานสากลด้านความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศ ได้แก่ ISO/IEC 17799/27001, ITIL และ COBIT

Jan H. P. Eloff และ Mariki Eloff (2003) ได้ทำการศึกษาวิจัยเรื่องการจัดการความมั่นคงปลอดภัยสารสนเทศแบบใหม่ เพื่อศึกษาการจัดการความมั่นคงปลอดภัยสารสนเทศสำหรับองค์กร (ISMS) โดยรวมมุมมองต่างๆเข้าด้วยกัน เช่น นโยบาย, มาตรฐาน, เทคโนโลยี เป็นต้น ซึ่งการนำไปใช้และการควบคุมจะเป็นไปตามมาตรฐาน ISO/IEC 17799/27001 ผลการวิจัยพบว่าการนำหลักการต่างๆมาประยุกต์ใช้ให้สอดคล้องสามารถทำให้ความมั่นคงปลอดภัยสารสนเทศขององค์กรมีประสิทธิภาพและครอบคลุม

5. ระเบียบวิธีวิจัย

สำหรับระเบียบวิธีวิจัยสามารถแบ่งออกเป็นหัวข้อได้ดังนี้

5.1 ประชากร หรือ กลุ่มตัวอย่างที่เก็บข้อมูล

สำหรับประชากรหรือกลุ่มตัวอย่างที่ใช้ในการเก็บข้อมูลในครั้งนี้ คือ ตัวแทนบุคลากรทั้งระดับบริหารและระดับปฏิบัติการในหน่วยงานภาครัฐที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศเพื่อสอบถามความคิดเห็น และหาข้อสรุปของร่างมาตรฐานและนำมาเปรียบเทียบกับมาตรฐาน EBK2008 เพื่อสรุปผลและข้อเสนอแนะ

5.2 การสร้างเครื่องมือที่ใช้ในการเก็บข้อมูล

การสร้างเครื่องมือที่ใช้ในการเก็บข้อมูลนี้ ผู้วิจัยได้ประยุกต์กรอบวิธีปฏิบัติ (Framework) ตามหลัก ISO27001, CISSP, DoD 8570.1 และ EBK2008 อีกทั้งมาตรฐานต่างๆที่เกี่ยวข้องเพื่อให้เหมาะสมกับระบบสารสนเทศของหน่วยงานภาครัฐของไทย โดยมีขั้นตอนดังนี้

5.2.1 ศึกษาทฤษฎีและมาตรฐานต่างๆ ที่เกี่ยวข้องทางด้านความมั่นคงปลอดภัยสารสนเทศ เช่น มาตรฐานใบรับรองผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ ของสถาบันต่างๆ มาตรฐานสำหรับผู้เชี่ยวชาญทางด้านความปลอดภัยข้อมูลของกระทรวงกลาโหมสหรัฐฯ Department of Defense (DoD), มาตรฐาน ISO/IEC 27001:2005, ISO/IEC 17799, EBK2008 เป็นต้น

5.1.2 สร้างร่างเกณฑ์การวัดสมรรถนะบุคลากรด้านความมั่นคงปลอดภัย

5.1.3 สร้างกรอบงานวิจัยเพื่อให้การออกแบบสอบถามอยู่ในขอบเขตตามวัตถุประสงค์

5.1.4 สร้างแบบสอบถามโดยการเขียนข้อความเพื่อใช้ในการศึกษาถึงความคิดเห็นของบุคลากรที่มีต่อร่างมาตรฐานที่สร้างขึ้นและทำการประชุมกลุ่มผู้เชี่ยวชาญ (Focus groups) เพื่อทดสอบแบบสอบถาม

6. ผลการวิจัย

ผลจากการวิจัยได้ผลเป็นที่น่าพอใจเมื่อเทียบกับวัตถุประสงค์ที่ได้กำหนดเป็นแนวทางในการศึกษาวิจัย ซึ่งตัวแทนบุคลากรในหน่วยงานภาครัฐส่วนใหญ่ (ร้อยละ88.89) ทั้งระดับบริหารและระดับปฏิบัติการเห็นด้วยกับกรอบมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศในร่างที่ 1 ซึ่งมีหัวข้อหลักดังตาราง 1

ตาราง 1 แสดงหัวข้อหลักในร่างมาตรฐานที่ 1 ทั้ง 2 ระดับและเปรียบเทียบกับ EBK2008

Competency Areas	Essential Body of Knowledge (EBK)	ร่างมาตรฐานที่ 1 ระดับ 1	ร่างมาตรฐานที่ 1 ระดับ 2
Data Security	/	/	/
Digital Forensics	/	/	/
Enterprise Continuity	/		/
Incident Management	/	/	
IT Security Training and Awareness	/	/	/
IT Systems Operations and Maintenance	/	/	/
Network and Telecommunications Security	/	/	/
Personnel Security	/	/	/
Physical and Environmental Security	/	/	/
Procurement	/		/
Regulatory and Standards Compliance	/	/	/
Security Risk Management	/		/
Strategic Security Management	/		/
System and Application Security	/		/

จากตาราง 1 จะเห็นได้ว่าเมื่อมีการประชุมกลุ่มผู้เชี่ยวชาญอีกครั้ง โดยที่พิจารณา EBK2008 ประกอบเข้าไปด้วยอาจมีบางหัวข้อที่ควรเพิ่มเติมอีก โดยที่ข้อแนะนำจากการประชุมกลุ่มผู้เชี่ยวชาญ (Focus group) เพิ่มเติมมีดังต่อไปนี้

- Incident Management
- IT Security Training and Awareness
- Physical and Environmental Security
- Regulatory and Standards Compliance

และเพิ่มเติมในร่างมาตรฐานที่ 1 ระดับที่ 2 ดังนี้

- IT Security Training and Awareness
- Physical and Environmental Security
- Regulatory and Standards Compliance
- Strategic Security Management

ส่วนร่างมาตรฐานที่ 2 นั้นเป็นการกำหนดระดับคะแนน ซึ่งประชากรกลุ่มตัวอย่างไม่เห็นด้วยเพราะไม่สะดวกในการนำมาปรับใช้กับระบบราชการ เพราะมีรายละเอียดค่อนข้างมากและซับซ้อน จึงอาจเหมาะสำหรับหน่วยงานอื่น เช่น องค์กรเอกชนที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ

7. สรุปผลการวิจัย

จากการวิจัย สามารถสรุปผลได้ดังนี้

1. ในภาพรวมบุคลากรส่วนใหญ่ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศของหน่วย งานภาครัฐไม่มีการสอบเพื่อรับใบรับรองผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยสารสนเทศ และมีความรู้ความเข้าใจเกี่ยวกับงานด้านความมั่นคงปลอดภัยสารสนเทศเพียงบางส่วน เนื่องจากหน่วยงานไม่มีการสนับสนุนที่เพียงพอ จึงต้องมีการปรับปรุงนโยบาย เช่น สนับสนุนการอบรมทั้งในสถานที่และนอกสถานทีและมีการปรับระดับขั้นเมื่อมีคุณสมบัติผ่านตามเกณฑ์ที่กำหนด

2. ในภาพรวมการจัดการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับหน่วยงานภาครัฐ เป็นการควบคุมดูแลโดยรวม ไม่มีบุคลากรหรือฝ่ายที่ดูแลด้านนี้โดยตรงซึ่งยังเป็นการรวมอยู่ในฝ่ายสารสนเทศ ทำให้เมื่อมีปัญหา หรือภัยคุกคามเกิดขึ้น การตรวจสอบ แก้ไข จะมีความล่าช้าและสามารถส่งผลกระทบต่อหน่วยงานโดยรวมได้

3. ผู้วิจัยได้นำเสนอร่างเกณฑ์วัดสมรรถนะด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรในหน่วยงานภาครัฐดังที่แสดงในร่างมาตรฐานที่ 1 และเป็นที่ยอมรับจากผู้เชี่ยวชาญและบุคลากรในหน่วยงานภาครัฐ

8. ข้อเสนอแนะ

ในงานวิจัยครั้งนี้ ผู้วิจัยมีข้อเสนอแนะดังนี้ คือ

1. ควรให้หน่วยงานหรือองค์กรที่ดูแลด้านสารสนเทศของภาครัฐ เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้นำเกณฑ์ร่างมาตรฐานนี้ไปปรับปรุงและประกาศใช้เป็นนโยบาย เพื่อให้เป็นมาตรฐานเดียวกัน โดยมีการประชุมร่วมกันสำหรับหาข้อสรุปเพื่อปรับกรอบมาตรฐานใช้ให้เหมาะสมกับโครงสร้างของหน่วยงาน และมีการติดตาม ประเมินผลที่ได้จากการนำเกณฑ์นี้ไปใช้

2. สำหรับการทำวิจัยในอนาคต เนื่องจากความก้าวหน้าทางเทคโนโลยีสารสนเทศได้มีการเปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้นเพื่อให้ทันต่อเหตุการณ์และภัยคุกคามใหม่ๆ ที่เกิดขึ้น ผู้สนใจที่จะนำงานวิจัยนี้ไปวิจัยต่อควรจะมีการศึกษาเพิ่มเติม ติดตามการเปลี่ยนแปลงหรือการปรับปรุงมาตรฐานต่างๆ ทางด้านความมั่นคงปลอดภัยสารสนเทศ และงานวิจัยนี้สามารถนำไปอ้างอิงเพื่อทำการศึกษาวิจัยเพื่อออกแบบหลักสูตรการฝึกอบรมสำหรับบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศต่อไปได้

9. รายการอ้างอิง

คณะอนุกรรมการด้านความมั่นคงภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2548. **“มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น 2.5”.** [ออนไลน์] เข้าถึงได้จาก: http://thaicert.nectec.or.th/paper/basic/Book_2.5_FullVersion.pdf

นุชนาฎ รงรอง, วิเชียร ชุติมาสกุล, 2551. “กรอบแนวคิดการตรวจสอบการพัฒนาและตรวจรับระบบและเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ”. **การประชุมทางวิชาการ NCIT2008 ครั้งที่ 2** เรื่อง " การวิจัยเทคโนโลยีสารสนเทศเพื่อการพัฒนาประเทศที่ยั่งยืน", 6-7 พฤศจิกายน, โรงแรมแกรนด์ เมอร์เคียว ฟอร์จูน, กรุงเทพฯ, หน้า 224-233.

บรรจง หะรังสี, 2007. **“ ISO/IEC 27001/17799 Information Security Management Standard”.** [ออนไลน์] เข้าถึงได้จาก: http://www.thaicert.nectec.or.th/isa/ISO27001.pdf

ยุทธพล พิชัยณรงค์**,** ประสงค์ ปราณีตพลกรัง, 2551. “การวิเคราะห์และประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับองค์การภาครัฐ”. **การประชุมทางวิชาการมหาวิทยาลัยศรีปทุม ปีการศึกษา 2551** เรื่อง " ผลงานวิจัยและนวัตกรรมสู่การพัฒนาที่ยั่งยืน", 13 สิงหาคม 2551, อาคาร ดร.สุข พุคยาภรณ์ มหาวิทยาลัยศรีปทุม, กรุงเทพฯ, หน้า 430-437.

สมยงค์ สีขาว, มนต์ชัย เทียน, สุพจน์ นิตย์สุวัฒน์, 2551. “การสร้างเกณฑ์วัดสมรรถนะด้านคอมพิวเตอร์และเทคโนโลยีของบุคลากรองค์การปกครองส่วนท้องถิ่น”. **การประชุมทางวิชาการ NCIT2008 ครั้งที่ 2** เรื่อง " การวิจัยเทคโนโลยีสารสนเทศเพื่อการพัฒนาประเทศที่ยั่งยืน", 6-7 พฤศจิกายน, โรงแรมแกรนด์ เมอร์เคียว ฟอร์จูน, กรุงเทพฯ, หน้า 119-124.

Department of Defense United State of America, 2008. “ Information Assurance Workforce Improvement Program Incorporating Change 1**”.** [Online] Retrieved 2009, March 7 from : http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

Harris, Shon, 2007. **CISSP All-In- One EXAM GUIDE**. 4th ed. New York: McGraw-Hill.

Jan H. P. Eloff**,** Mariki Eloff, 2003. “Information security management: a new paradigm.” Proceedings of the 2003 annual research conference of the South African institute, 2003. pp.130 - 136

“Standards for Information Security Management [Part I].” [Online] Retrieved 2009, April 2, from : http://www.acinfotec.com/viewsecurityarticles.php?ID=6

United States Computer Emergency Readiness Team. “IT Security Essential Body of Knowledge (EBK):A Competency and Functional Framework for IT Security Workforce Development.” [Online] Retrieved 2009, May 10, from : http://www.us-cert.gov/ITSecurityEBK

Wallhoff, John. “The International CISSP Summary**”** [Online] Retrieved 2009, January 10, from : http://www.scillani.se/assets/pdf/The_International_CISSP_Summary.pdf