หัวข้อการค้นคว้าอิสระ	การศึกษาระบบความมั่นคงปลอดภัยด้านสารสนเทศสำหรับบริการทางการเงินผ่านอินเทอร์เน็ต กรณีศึกษา: ธนาคารพาณิชย์แห่งหนึ่ง A Study of Information Security System for Internet Banking Case Study: A Commercial Bank in Thailand
ชื่อผู้เขียน	นางสาวหนึ่งฤทัย เตชะรัตนประเสริฐ Miss Nuengruethai Techaratanaprasert
แผนกวิชา/คณะ	สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ	ดร.สมิทธ์ ตุงคะสมิต
ปีการศึกษา	2551

บทสรุป

ในปัจจุบัน เป็นที่ยอมรับกันว่าอินเทอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันของบุคคลทั่วไปเป็นอย่างมาก ไม่ว่าจะเป็นการสืบค้นข้อมูล การซื้อขายสินค้า การรับส่งจดหมายอิเล็กทรอนิกส์ การเล่นเกมออนไลน์ การเข้าไปเยี่ยมชมเว็บไซต์ต่างๆ เช่น เว็บไซต์ข่าว เว็บไซต์เพื่อความบันเทิง นอกจากนี้ อินเทอร์เน็ตยังถูกใช้เป็นช่องทางในการดำเนินธุรกิจขององค์กรต่างๆ ไม่ว่าจะเป็นการซื้อขายสินค้าและการประมูลสินค้าออนไลน์ตามเว็บไซต์ต่างๆ การเรียกดูและการซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตของตลาดหลักทรัพย์แห่งประเทศไทย การจองตั๋วเครื่องบินผ่านอินเทอร์เน็ตของสายการบินต่างๆ รวมไปถึงการให้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารพาณิชย์หลายๆแห่ง ไม่ว่าจะเป็นการสอบถามยอดคงเหลือในบัญชี การโอนเงิน การชำระค่าสินค้าและบริการ การซื้อขายและแลกเปลี่ยนกองทุน เป็นต้น แต่ในขณะเดียวกัน การกระทำอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตได้เพิ่มจำนวนขึ้นและมีความซับซ้อนขึ้นเป็นอย่างมากเช่นกัน และได้ส่งผลกระทบอย่างร้ายแรงต่อทั้งบุคคลทั่วไปที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตไปจนถึงองค์กรต่างๆที่ใช้อินเทอร์เน็ตเป็นช่องทางในการดำเนินธุรกิจ โดยเฉพาะอย่างยิ่งธนาคารพาณิชย์ต่างๆ ดังเช่นในเรื่องของการส่งจดหมายอิเล็กทรอนิกส์หลอกลวงเพื่อสอบถามรหัสส่วนตัวและหมายเลขบัตรเครดิตจากลูกค้าโดยแอบอ้างว่าเป็นจดหมายอิเล็กทรอนิกส์ที่ส่งมาจากธนาคาร

หรือการติดอุปกรณ์บางอย่างที่ตู้กดเงินอัตโนมัติของธนาคารเพื่อทำการคัดลอกหมายเลขบัตรเอทีเอ็มและรหัสส่วนตัวเพื่อนำไปใช้ทำบัตรเอทีเอ็มปลอม เป็นต้น

ปัญหาดังกล่าวส่งผลให้องค์กรต่างๆโดยเฉพาะอย่างยิ่งธนาคารพาณิชย์จำเป็นต้องปรับตัวและทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของตนเองใหม่ โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ต โดยอาจจะอ้างอิงมาจากมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศในปัจจุบันซึ่งมีหลายมาตรฐานและเป็นที่ยอมรับว่าเป็นมาตรฐานที่มีความน่าเชื่อถือ เช่น มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005 เป็นต้น หรืออาจจะใช้มาตรการเสริมอื่นๆ ไม่ว่าจะเป็นการเพิ่มระดับของการรักษาความปลอดภัยในการเข้าใช้งานระบบให้กับลูกค้า การติดตั้งอุปกรณ์ตรวจจับความผิดปกติที่เกิดขึ้นกับระบบการให้บริการ หรือการให้ความรู้ทางด้านความปลอดภัยข้อมูลสารสนเทศแก่พนักงานอย่างเพียงพอ โดยมีจุดมุ่งหมายเพื่อให้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีการบริหารจัดการที่สอดคล้องกับมาตรฐานสากลที่เป็นที่ยอมรับและสอดคล้องกับข้อบังคับที่ได้ประกาศไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และยังเป็นการสร้างความน่าเชื่อถือให้แก่ธนาคารและสร้างความมั่นใจให้แก่ลูกค้าของธนาคารอีกด้วย

การศึกษาวิจัยเรื่องนี้ เป็นการศึกษานโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษา เปรียบเทียบกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากล 2 แบบ ได้แก่ มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005 โดยใช้วิธีการรวบรวมข้อมูลแบบปฐมภูมิ ได้แก่ การวิจัยด้วยเทคนิคเดลฟายแบบปรับปรุง (Ethnographic Delphi Futures Research: EDFR) และการสัมภาษณ์เชิงลึก (In-Depth Interview) และวิธีการรวบรวมข้อมูลแบบทุติยภูมิ ได้แก่ การค้นคว้าจากเอกสาร บทความ งานวิจัยที่เกี่ยวข้อง และการค้นคว้าทางอินเทอร์เน็ต แล้วจึงจัดทำ Gap Analysis เพื่อวิเคราะห์เปรียบเทียบผลการศึกษาและจัดทำเป็นข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตที่เหมาะสมสำหรับธนาคารที่ใช้เป็นกรณีศึกษา

ทั้งนี้ มาตรฐาน ISO/IEC 17799:2005 นั้นเป็นมาตรฐานการจัดการด้านความปลอดภัยของข้อมูล ที่เน้นที่ระบบการบริหารจัดการภายในองค์กรเพื่อรักษาความปลอดภัยของข้อมูล โดยมีข้อกำหนดต่างๆตั้งแต่กระบวนการนำข้อมูลมาใช้และการจัดเก็บข้อมูล ตลอดจนการมีแผนรับมือเมื่อเกิดเหตุฉุกเฉินขึ้นกับข้อมูล เพื่อให้องค์กรสามารถปฏิบัติตัวได้อย่างถูกต้อง และ

สามารถกู้ข้อมูลกลับขึ้นมาเพื่อทำให้องค์กรสามารถดำเนินกิจกรรมของตนต่อไปตามปกติได้อย่างรวดเร็วที่สุด โดยโครงสร้างของมาตรฐานจะประกอบไปด้วยหัวข้อ (Domain) และวัตถุประสงค์ (Control Objectives) ที่ใช้ในการควบคุมทางด้านการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศทั้งหมด 11 หัวข้อ ใน 39 วัตถุประสงค์ รวมเป็นมาตรการ (Controls) ทั้งสิ้น 133 มาตรการ ในขณะที่มาตรฐาน ISO/IEC 17799:2005 นั้นเป็นมาตรฐานเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management Systems: ISMS) ซึ่งจะกำหนดความต้องการ (Set of Requirements) ในการจัดทำระบบ ISMS เพื่อช่วยให้องค์กรสามารถสร้างระบบ ISMS ขึ้นมาได้อย่างมีประสิทธิภาพ ซึ่งระบบ ISMS นี้ถือเป็นส่วนหนึ่งของระบบบริหารจัดการขององค์กรที่มีพื้นฐานมาจากแนวทางการบริหารจัดการความเสี่ยงของธุรกิจ (Business Risk Approach) โดยมีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศและทรัพย์สินอื่นๆขององค์กร เพื่อให้องค์กรสามารถรอดพ้นจากภัยคุกคามต่างๆได้ โดยเนื้อหาของมาตรฐานนั้นจะว่าด้วยเรื่องของการจัดตั้งระบบ ISMS ขึ้นภายในองค์กร โดยประยุกต์เข้ากับหลักการของ Plan-Do-Check-Act (PDCA) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาอย่างต่อเนื่อง (Continuous Improvement) และได้มีการอ้างอิงมาตรการของการควบคุมทางด้านการจัดการความปลอดภัยของข้อมูลทั้ง 133 มาตรการตามมาตรฐาน ISO/IEC 17799:2005 โดยระบุไว้ในส่วนของ Annex A นอกจากนี้ มาตรฐาน ISO/IEC 27001:2005 ยังมีเนื้อหาครอบคลุมถึงการออกใบรับรองให้กับองค์กร (Organization Certification) เพื่อเป็นการรับรองว่าองค์กรดังกล่าวมีระบบ ISMS ที่มีประสิทธิภาพ และการออกใบรับรองให้กับบุคคล (Individual Certification) ที่ทำหน้าที่เป็นผู้ตรวจรับรองระบบว่าบุคคลนั้นเป็นผู้ที่มีความรู้ ความชำนาญในระบบ ISMS เป็นอย่างดี และมีคุณสมบัติเพียงพอที่จะทำหน้าที่ตรวจรับรองระบบ ISMS ได้อีกด้วย

ผลการศึกษาวิจัย พบว่า ในระดับองค์กร ธนาคารมีการวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารที่มีความสอดคล้องกับมาตรฐาน ISO/IEC 17799:2005 อยู่แล้ว อีกทั้งธนาคารก็ได้มีการวางแผนงานในการสื่อสารเนื้อหาโดยรวมของนโยบายออกไปให้พนักงานรับทราบ โดยให้ความสำคัญกับการสร้างความเข้าใจที่ถูกต้องในเรื่องของความแตกต่างระหว่างคำว่านโยบายกับมาตรฐานและระเบียบวิธีในการปฏิบัติงาน เพื่อหลีกเลี่ยงไม่ให้พนักงานเกิดความสับสน และยังได้ให้ความสำคัญกับการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงานทุกคนในธนาคาร นอกจากนี้ ธนาคารยังได้มีการวางกลไกต่างๆ

เพื่อช่วยให้ธนาคารรับทราบปัญหาที่เกิดขึ้นจากการนำนโยบายไปปฏิบัติจริง เพื่อที่จะได้พิจารณาปรับปรุงแก้ไขนโยบายดังกล่าวให้มีความเหมาะสมกับการทำงานมากที่สุด ซึ่งจะเห็นได้ว่า การวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศของธนาคารนั้น ไม่ได้เป็นเพียงการนำหัวข้อในการควบคุมทั้งหมดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 มาปรับใช้ภายในธนาคารเท่านั้น แต่นโยบายดังกล่าวยังได้ผ่านการพิจารณาในหลายๆแง่มุม ไม่ว่าจะเป็นในเรื่องของวัฒนธรรมองค์กร ลักษณะการดำเนินงานของธนาคาร และที่สำคัญคือ ลักษณะการทำงานรวมถึงความรู้สึกนึกคิดของพนักงาน เพื่อให้แน่ใจว่านโยบายที่ออกมานั้นจะประสบผลสำเร็จตามที่ธนาคารคาดหวัง ส่วนในเรื่องของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นก็มีมาตรการในการควบคุมที่สอดคล้องกับแนวทางและข้อกำหนดในการป้องกันความปลอดภัยข้อมูลสารสนเทศที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 เป็นอย่างมาก โดยความสอดคล้องนั้นสามารถแบ่งออกได้เป็น 2 ลักษณะ ได้แก่ ความสอดคล้องโดยตรง ซึ่งหมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นมีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศในระดับต่างๆเป็นของตนเอง และมาตรการดังกล่าวนั้นก็สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน ซึ่งได้แก่ ข้อกำหนดที่อยู่ในหัวข้อ A.7 Asset Management, A.10 Communications and Operations Management, A.11 Access Control, A.12 Information Systems Acquisition, Development, and Maintenance, A.13 Information Security Incident Management, A.14 Business Continuity Management, และ A.15 Compliance และความสอดคล้องโดยอ้อม ซึ่งหมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นไม่มีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศตามที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน แต่เนื่องจากบริการทางการเงินผ่านอินเทอร์เน็ตนั้นถือเป็นส่วนหนึ่งของการบริหารจัดการภายในธนาคาร ดังนั้น ถ้าหากในภาพรวมแล้วธนาคารมีการวางนโยบายด้านความปลอดภัยข้อมูลสารสนเทศที่สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 แล้ว ก็สามารถกล่าวได้ว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศที่สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 ด้วยเช่นกัน ซึ่งหัวข้อของการควบคุมที่มีความสอดคล้องในลักษณะดังกล่าวประกอบด้วย A.5 Security Policy, A.6 Organizational of Information Security, A.8 Human Resource Security และ A.9 Physical and Environmental Security นอกจากนี้ ธนาคารยังได้นำหลักการของ PDCA ที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 27001:2005 เข้ามาประยุกต์ใช้ในการบริหารจัดการบริการทางการเงินผ่าน

อินเทอร์เน็ตของธนาคาร เพื่อให้การปฏิบัติงานในทุกขั้นตอนที่เกี่ยวข้องกับบริการดังกล่าว ตั้งแต่การเริ่มต้นสร้างระบบ การดูแลรักษาระบบ จนกระทั่งการปรับปรุงและพัฒนาระบบให้มีประสิทธิภาพและมีความปลอดภัยสูงขึ้น มีขั้นตอนการทำงานที่ชัดเจน เป็นระเบียบแบบแผน สามารถตรวจสอบได้ อันจะนำไปสู่การพัฒนาบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอย่างต่อเนื่อง (Continuous Improvement) ในที่สุด

ในส่วนของข้อเสนอแนะจากการวิจัยนั้น ผู้วิจัยมีความเห็นว่า นอกจากการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงานของธนาคารแล้ว ปัจจัยส่วนหนึ่งที่จะช่วยให้พนักงานของธนาคารปฏิบัติตามนโยบายด้านความปลอดภัยข้อมูลสารสนเทศอย่างจริงจังก็คือ การให้รางวัลและการกำหนดบทลงโทษที่เหมาะสม และเนื่องจากธนาคารมีการวางแผนที่จะประกาศนโยบายให้พนักงานรับทราบไปพร้อมๆกับการสร้างความตระหนักรู้ในเรื่องของความปลอดภัยข้อมูลสารสนเทศให้กับพนักงาน ผู้วิจัยจึงมีความเห็นว่า การสร้างฐานข้อมูลความรู้ในเรื่องของนโยบายความปลอดภัยข้อมูลสารสนเทศของธนาคาร โดยอาศัยแนวความคิดของการบริหารจัดการองค์ความรู้ (Knowledge Management) ภายในองค์กร น่าจะเป็นวิธีการที่เหมาะสม ส่วนข้อเสนอแนะสำหรับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารนั้น เนื่องจากผลสรุปจากการทำ Gap Analysis ดังกล่าวเป็นเพียงการสรุปว่าบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีหรือไม่มีมาตรการที่สอดคล้องกับหัวข้อของการควบคุมที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 ซึ่งการมีอยู่ของมาตรการดังกล่าวอาจไม่ได้หมายถึงการนำมาใช้อย่างมีประสิทธิภาพก็เป็นได้ ดังนั้น ผู้วิจัยจึงมีความเห็นว่า ธนาคารควรจะได้มีการจัดทำเอกสารที่แสดงถึงรายละเอียดของมาตรการต่างๆที่ธนาคารนำมาใช้เพื่อป้องกันความปลอดภัยข้อมูลสารสนเทศของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร โดยกำหนดหัวข้อตามหัวข้อของการควบคุมที่ระบุในมาตรฐาน ISO/IEC 17799:2005 เพื่อช่วยให้ผู้ที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารทราบว่า มาตรการที่ธนาคารนำมาใช้นั้นมีระดับของการควบคุมอยู่ในระดับใด ผู้ที่มีหน้าที่เกี่ยวข้องกับมาตรการนั้นๆได้รับทราบและมีการปฏิบัติตามมาตรการเหล่านั้นหรือไม่ เพื่อประโยชน์ในการทบทวนและปรับปรุงมาตรการต่างๆให้มีความเหมาะสมกับการบริหารจัดการความปลอดภัยข้อมูลสารสนเทศของบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมากที่สุด และหลังจากที่ได้มีการจัดทำเอกสารดังกล่าวขึ้นมาแล้วนั้น หากธนาคารเห็นว่าบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารมีมาตรการในการป้องกันความปลอดภัยข้อมูลสารสนเทศที่มีประสิทธิภาพและสอดคล้องกับหัวข้อของการควบคุมที่ระบุในมาตรฐาน ISO/IEC 17799:2005 ทุกประการแล้วนั้น ผู้วิจัยเห็นว่า ธนาคารควรพิจารณานำบริการ

ทางการเงินผ่านอินเทอร์เน็ตของธนาคารเข้ารับการตรวจรับรองระบบเพื่อให้ได้ใบรับรองตามมาตรฐาน ISO/IEC 27001:2005 ทั้งนี้ เพื่อช่วยสร้างความมั่นใจให้กับลูกค้าที่ใช้และกำลังจะตัดสินใจใช้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร และเป็นตัวอย่างให้กับระบบงานอื่นๆ ของธนาคารในการยกระดับของการป้องกันความปลอดภัยข้อมูลสารสนเทศของตนให้มีประสิทธิภาพมากขึ้น อันจะส่งผลให้เกิดความตื่นตัวในเรื่องของการป้องกันความปลอดภัยข้อมูลสารสนเทศทั่วทั้งธนาคาร

สำหรับข้อเสนอแนะในการวิจัยครั้งต่อไปนั้น ผู้วิจัยมีความเห็นว่า แนวทางในการศึกษาวิจัยครั้งต่อไปนั้นอาจจะเป็นลักษณะของการศึกษาถึงความพร้อมในการนำบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษาเข้ารับการตรวจรับรองระบบเพื่อขอใบรับรองตามมาตรฐาน ISO/IEC 27001:2005 หรือการศึกษาถึงปัจจัยด้านการบริหารโครงการที่มีผลต่อการนำบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษาเข้ารับการตรวจรับรองระบบเพื่อขอใบรับรองตามมาตรฐาน ISO/IEC 27001:2005 หรือการศึกษาถึงความเป็นไปได้ในการนำแนวความคิดของการบริหารจัดการองค์ความรู้ (Knowledge Management) เข้ามาใช้กับการสื่อสารนโยบายความปลอดภัยข้อมูลสารสนเทศขององค์กร เป็นต้น