บทคัดย่อ

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 เพื่อวิเคราะห์เปรียบเทียบผลการศึกษาและจัดทำเป็นข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตที่เหมาะสมสำหรับธนาคารที่ใช้เป็นกรณีศึกษาต่อไป

ผลการศึกษาวิจัย พบว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นมีมาตรการในการควบคุมที่สอดคล้องกับแนวทางและข้อกำหนดในการป้องกันความปลอดภัยข้อมูลสารสนเทศที่ระบุอยู่ในมาตรฐาน ISO/IEC 17799:2005 เป็นอย่างมาก โดยความสอดคล้องนั้นสามารถแบ่งออกได้เป็น 2 ลักษณะ ได้แก่ ความสอดคล้องโดยตรง ซึ่งหมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นมีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศในระดับต่างๆเป็นของตนเอง และมาตรการดังกล่าวนั้นก็สอดคล้องกับข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน และความสอดคล้องโดยอ้อม ซึ่งหมายความว่า บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษานั้นไม่มีมาตรการในการจัดการความปลอดภัยข้อมูลสารสนเทศตามที่ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อย่างชัดเจน แต่มีความสอดคล้องกับนโยบายด้านความปลอดภัยข้อมูลสารสนเทศในภาพรวมของธนาคารซึ่งอ้างอิงมาจากข้อกำหนดที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 17799:2005 อยู่แล้ว นอกจากนี้ ธนาคารยังได้นำหลักการของ PDCA ที่ได้ระบุไว้ในมาตรฐาน ISO/IEC 27001:2005 เข้ามาประยุกต์ใช้ในการบริหารจัดการบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคาร เพื่อให้การปฏิบัติงานในทุกขั้นตอนที่เกี่ยวข้องกับบริการดังกล่าวมีขั้นตอนการทำงานที่ชัดเจน เป็นระเบียบแบบแผน สามารถตรวจสอบได้ อันจะนำไปสู่การพัฒนาบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารอย่างต่อเนื่อง (Continuous Improvement) ในที่สุด

Abstract

This independent study is a study of an information security system for internet banking using a case study of a commercial bank in Thailand. The objective is to compare an information security policy of internet banking with two international standards of information security, which are ISO/IEC 17799:2005 and ISO/IEC 27001:2005. This study uses data collection methods such as Ethnographic Delphi Futures Research (EDFR) and In-Depth Interview, as well as related documents, articles, and internet research. Then, a Gap Analysis is done in order to analyze and compare the results, which can use to give recommendations on proper information security policy for internet banking for the bank of a case study.

The result is that the information security policy of internet banking complies with the information security controls specified in ISO/IEC 17799:2005 in two ways. In one aspect, internet banking has its own management levels and controls, which is similar to the ones defined in the standard. In the other aspect, internet banking does not have its own management levels and controls, but it aligns with the bank's information security policy which also refers to ISO/IEC 17799:2005. Moreover, internet banking also applies PDCA principle to the management of information security controls, which will lead to continuous improvement of internet banking in the future.