ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

Factors influencing IT Risks for Securities Companies in Thailand

สาริยา นุชอนงค์
อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ธุรกิจ
คณะบริหารธุรกิจ มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

บทคัดย่อ

ปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการดำเนินธุรกิจของบริษัทหลักทรัพย์ ซึ่งมีความเสี่ยงหลายด้านที่ควรคำนึงถึง โดยหากขาดการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพียงพอ อาจส่งผลกระทบต่อการดำเนินธุรกิจหรืออาจสร้างความเสียหายทั้งต่อบริษัทหลักทรัพย์และความเชื่อมั่นจากลูกค้าได้ การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาถึงระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยและปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย เครื่องมือที่ใช้ในการวิจัยคือ แบบสอบถามโดยสถิติที่ใช้ในการวิเคราะห์ข้อมูล ประกอบด้วยการหาความถี่ ร้อยละ (%) ค่าเฉลี่ย (Mean) ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) การวิเคราะห์ความแตกต่างระหว่างกลุ่มใช้การทดสอบแบบกลุ่มตัวอย่างไม่สัมพันธ์กัน (t-test Independent Group) การทดสอบความแปรปรวนทางเดียว (One-way Anova) การวิเคราะห์สัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson Product Moment Correlation) และวิธีการถดถอยพหุคูณ (Multiple Regression Analysis)

ผลการวิจัยพบว่า 1) ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับต่ำโดยพบความเสี่ยงที่เกิดจากการว่าจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ อยู่ในระดับสูงสุด 2) ปัจจัยด้านนโยบายการควบคุมความปลอดภัย ปัจจัยด้านเครื่องมือที่ใช้ในการบริหารความเสี่ยง ปัจจัยด้านการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ ปัจจัยด้านการสื่อสารเรื่องความเสี่ยง ปัจจัยด้านองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ และปัจจัยด้านผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

คำสำคัญ : ความเสี่ยง เทคโนโลยีสารสนเทศ บริษัทหลักทรัพย์

ABSTRACT

In recent years, IT has played a vital role in running a business for Securities companies. Moreover, there are many IT risks that these companies should consider. As a result, the lacking of good IT risk management could damage the businesses and the trust of customers. The research aims to study the level of IT Risks for Securities Companies in Thailand and factors influencing IT Risks for Securities Companies in Thailand. Questionnaires were distributed to respondents to collect data. Data were analyzed by statistical tools such as percentage, frequency, mean, standard deviation, t-test, Anova, Pearson's Correlation, and Multiple Regression Analysis.

The results found were as follows: 1) IT Risks for Securities Companies in Thailand were at the low level. Outsourcing IT applications or information was the highest risk among other IT Risks. 2) The factors affecting IT Risks for Securities Companies in Thailand were Security control policies, risk management tools, knowledge transfer on security policies and best practices, IT Risks communication, IT infrastructure, and people who involve in IT Risks.

Keywords: Risk, Information Technology, Securities Companies

บทนำ

ปัจจุบันองค์กรต่าง ๆ ล้วนต้องอาศัยโลกไซเบอร์อันเป็นที่มาของข้อมูลอิเล็กทรอนิกส์ เพื่อความสะดวกรวดเร็วและมีประสิทธิภาพในการทำงาน แต่ยิ่งวิทยาการเหล่านี้มีความสะดวกรวดเร็วมากเท่าไร ก็ยิ่งมีโอกาสเกิดความเสี่ยงมากขึ้นเท่านั้น นอกจากนี้ระบบสารสนเทศยังมีความสำคัญอย่างยิ่ง เพราะเป็นโครงสร้างพื้นฐานของการดำเนินธุรกิจต่าง ๆ ซึ่งจำเป็นต้องมีการบริหารจัดการที่ดีเพื่อรองรับความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้น ความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรนั้นจากการศึกษาของ IT Policy Compliance Group (2008) พบว่าไม่ได้มาจากทางด้านเทคนิคเทคโนโลยีหรือบุคลากรฝ่ายปฏิบัติการ แต่มาจากความล้มเหลวจากการละเลยขององค์กรและความผิดพลาดจากกระบวนการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (IT Governance) ซึ่งความล้มเหลวเหล่านี้นำไปสู่การตัดสินใจที่ผิดพลาดและโครงสร้างทางเทคโนโลยีสารสนเทศที่ไม่ถูกต้อง นอกจากนี้จากการเปิดเผยข้อมูลผลสำรวจเกี่ยวกับผลประทบที่เกิดจากเทคโนโลยีสารสนเทศทั่วโลกของซิสโก้ ก็เป็นเครื่องยืนยันถึงความเสี่ยงที่เกิดขึ้นได้ ทั้งนี้เพราะฝ่าย IT มีการปรับใช้เทคโนโลยีใหม่ ๆ ในการปรับปรุงธุรกิจมากขึ้น บริษัทต่าง ๆ มีการติดตั้งโปรแกรมประยุกต์ทางคอมพิวเตอร์ใหม่ ๆ มากขึ้น รวมทั้งการขยายเครือข่าย ปรับเปลี่ยนกลยุทธ์ระบบเครือข่ายให้สอดคล้องกับความต้องการทางธุรกิจ จะเห็นได้ว่าความเสี่ยงเป็นเรื่องที่ควรคำนึงถึงแต่หลายบริษัทไม่ได้ตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ (Cisco Global IT Impact Survey, 2013) จากการศึกษาของ IT Policy Compliance Group (2010) พบว่าบางบริษัทไม่สามารถอธิบายเกี่ยวกับความเสี่ยงที่เกิดขึ้นในบริษัท หรือต้องใช้เวลาในการค้นหาคำตอบ โดยเฉพาะกลุ่มสถาบันการเงินทั้งที่ประกอบกิจการธนาคารและที่ไม่ประกอบกิจการธนาคาร ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ โดยจะต้องทุ่มเทในเรื่องนี้อย่างหนัก โดยเฉพาะอย่างยิ่งในเรื่องข้อมูลของลูกค้า เพราะข้อมูลนั้นมีความสำคัญมากและมีความเสี่ยงที่จะสูญหายหรือถูกขโมย เพราะฉะนั้นทุกองค์กรควรตระหนักอย่างยิ่งว่า ความไม่มีประสิทธิภาพของการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (Ineffective IT Governance) เป็นปัจจัยที่สำคัญที่ทำให้เกิดความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร

การศึกษาในครั้งนี้มุ่งความสำคัญไปที่สถาบันการเงินที่ไม่ประกอบกิจการธนาคารคือ บริษัทที่ประกอบธุรกิจหลักทรัพย์ซึ่งเป็นธุรกิจที่เติบโตไปตามทิศทางเดียวกับภาวะของตลาดหุ้นหรือตลาดทุน และมีธุรกรรมที่เกี่ยวข้องกับระบบสารสนเทศอย่างแพร่หลาย ดังจะเห็นได้จากนักลงทุนผ่านอินเทอร์เน็ตมีแนวโน้มเพิ่มขึ้นโดยตลอด อันเป็นผลสืบเนื่องมาจากมาตรการส่งเสริมการลงทุนของภาครัฐและตลาดหลักทรัพย์แห่งประเทศไทย ในช่วงสิ้นปี 2555 มีนักลงทุนเปิดบัญชีซื้อขายหุ้นกับบริษัทหลักทรัพย์ผ่านอินเทอร์เน็ต เพิ่มขึ้นถึง 446,870 ราย มีมูลค่าการซื้อขายผ่านระบบอินเทอร์เน็ตสูงถึง 415,368 ล้านบาท คิดเป็นมูลค่าซื้อขายผ่านระบบอินเทอร์เน็ตต่อมูลค่าการซื้อขายรวมในตลาดหลักทรัพย์เท่ากับร้อยละ 30 เมื่อเทียบกับช่วงสิ้นปี 2551 ซึ่งมีนักลงทุนเปิดบัญชีซื้อขายหุ้นกับบริษัทหลักทรัพย์ผ่านอินเทอร์เน็ต เท่ากับ 189,348 ราย มีมูลค่าการซื้อขายผ่านระบบอินเทอร์เน็ตเพียง 98,395 ล้านบาท คิดเป็นมูลค่าซื้อขายผ่านระบบอินเทอร์เน็ตต่อมูลค่าการซื้อขายรวมในตลาดหลักทรัพย์เท่ากับร้อยละ 19 (ตลาดหลักทรัพย์แห่งประเทศไทย, 2555) และจากการศึกษาของ ThreatTrack security (2014) พบว่าบริษัทให้บริการทางด้านการเงินเป็นหนึ่งในสองอุตสาหกรรมที่ตกเป็นเป้าหมายของอาชญากรรมทางคอมพิวเตอร์มากที่สุด ดังจะเห็นได้จากเหตุการณ์ที่มีการขู่จากแฮกเกอร์เพื่อเจาะระบบ/เว็บไซต์ สถาบันการเงินทั่วโลก นอกจากนี้ยังพบความเสี่ยงจากความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ดังเช่นที่เคยมีกรณีระบบส่งคำซื้อขายหลักทรัพย์ของบริษัทหลักทรัพย์ของไทยจำนวน 16 บริษัท เกิดความขัดข้องไม่สามารถส่งคำสั่งซื้อขายได้ และเหตุการณ์ระบบซื้อขายหุ้นทางอินเทอร์เน็ตของตลาดหลักทรัพย์แห่งประเทศไทยล่มเนื่องมาจากปัญหาทางด้านฮาร์ดแวร์ ซึ่งส่งผลต่อความเชื่อมั่นของนักลงทุน

จากเหตุผลข้างต้นบริษัทหลักทรัพย์ในประเทศไทยจึงได้ให้ความสำคัญต่อความเสี่ยงนี้โดยมีการระบุความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศเป็นหนึ่งในปัจจัยความเสี่ยงของบริษัทไว้ในรายงานประจำปีของบริษัท ทั้งนี้เพราะการดำเนินธุรกิจของบริษัทหลักทรัพย์จำเป็นต้องพึ่งพาระบบคอมพิวเตอร์เป็นหลัก หากระบบเกิดความขัดข้องหรือเสียหายจะกระทบต่อการดำเนินงานและความน่าเชื่อถือของบริษัท ดังนั้นจึงมีความจำเป็นที่ต้องทำการศึกษาว่าระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้และปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศในบริษัทหลักทรัพย์ในประเทศไทยเพราะการที่ทราบความเสี่ยงและปัจจัยความเสี่ยงจะช่วยให้เราสามารถป้องกันความเสี่ยงที่จะเกิดขึ้นได้ นอกจากนี้ยังสามารถนำข้อมูลที่ได้ไปใช้ในการปรับปรุงการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี ทำให้ผลการดำเนินธุรกิจดีขึ้นและมีความเสี่ยงทางด้านการเงินน้อยลง

ทบทวนวรรณกรรม

1. ความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบ IT และการบริหารจัดการความเสี่ยงที่เกิดขึ้น

ปัจจุบันระบบ IT ได้เข้าไปมีบทบาทในกระบวนการทางธุรกิจเพิ่มมากขึ้น ความล้มเหลวหรือความขัดข้องของระบบสามารถสร้างความเสียหายให้กับองค์กรได้ จากการศึกษาของ Goldstein, Chernobai, and Benaroch (2011) พบว่าความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศเป็นอันตรายที่สำคัญและไม่ควรมองข้ามหรือเพิกเฉย โดยบริษัทที่พบความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ เป็นต้นว่า การบุกรุกจากภายใน เช่น พนักงานนำข้อมูลไปขาย พนักงานดำเนินการซื้อขายหุ้นโดยไม่ได้รับอนุญาต (Rouge Trader) การบุกรุกจากภายนอก เช่น การถูกเจาะระบบเพื่อขโมยข้อมูลลูกค้า ความเสียหายทรัพย์สินทางกายภาพ เช่น การสูญเสียจากภัยพิบัติ การหยุดชะงักทางธุรกิจและความล้มเหลวของระบบคอมพิวเตอร์ ความขัดข้องในการประมวลผลระบบงาน โดยความเสี่ยงที่เกิดขึ้นเหล่านี้จะส่งผลกระทบทางลบต่อความมั่งคั่งทางทรัพย์สินของบริษัท (Wealth Effect) และยังส่งผลให้มูลค่าทางการตลาดลดลงอีกด้วย นอกจากนี้ IT Policy Compliance Group (2010) ได้ทำการศึกษาถึงความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศที่เกิดขึ้น พบว่าในองค์กรที่มีแนวปฏิบัติที่ดีนั้นเกิดความเสี่ยงในเรื่องของข้อมูลที่สำคัญสูญหายหรือถูกขโมยถึงร้อยละ 85 รองลงมาเป็นการถูกคุกคามในเรื่องความปลอดภัยบนอินเทอร์เน็ต ร้อยละ 70 การหยุดชะงักทางธุรกิจเนื่องมาจากเทคโนโลยีสารสนเทศ ร้อยละ 61 สูญเสียรายได้ ทรัพย์สิน ร้อยละ 56 ต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ ร้อยละ 42 และการขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศ ร้อยละ 28 นอกจากนี้ ปริญญา หอมเอนก (2553) ยังกล่าวถึงปัญหาที่พบบ่อยจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรโดยแบ่งเป็นปัญหาใหญ่ ๆ ดังนี้คือ การให้บริการขององค์กรหยุดชะงักในกรณีที่ระบบสารสนเทศเกิดปัญหา เช่น ระบบล่ม ความคุ้มค่าหรือคุณค่าที่รับกลับมาจากการลงทุนด้าน IT ว่าคุ้มค่าหรือไม่ การควบคุมการลงทุนเกี่ยวกับเทคโนโลยีสารสนเทศ การควบคุมและบริหารจัดการระบบสารสนเทศ การนำเทคโนโลยีสารสนเทศมาใช้แล้วไม่สอดคล้องกับการดำเนินธุรกิจขององค์กรและไม่สามารถตอบโจทย์ของผู้บริหารระดับสูง ผู้ใช้งานระบบสารสนเทศ ลูกค้าและผู้ถือหุ้น กฎหมายและกฎข้อบังคับที่ทยอยออกมาบังคับใช้ เช่น กฎหมายธุรกรรมอิเล็กทรอนิกส์และกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ การป้องกันความปลอดภัยของข้อมูลและสารสนเทศที่จะส่งผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจขององค์กร

Bandyopadhyay, Mykytyn P., and Mykytyn K. (1999) กล่าวว่าเพื่อที่จะลดความเสี่ยงที่เกิดจากการใช้สารสนเทศในองค์กรจึงได้มีการพัฒนากรอบสำหรับการบูรณาการการบริหารจัดการความเสี่ยงเข้ากับเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วย 4 องค์ประกอบที่สำคัญคือ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) มาตรการการลดความเสี่ยง (Risk-Reducing Measures) และการตรวจสอบติดตามความเสี่ยง (Risk Monitoring)

ซึ่งความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศนั้นแบ่งออกได้หลายระดับดังนี้คือ ระดับ Application ในที่นี้คือ ความผิดพลาดทางเทคนิคหรือความล้มเหลวในการติดตั้งโปรแกรมหรือระบบสารสนเทศ ซึ่งอาจเกิดจากความเสี่ยงจากภัยธรรมชาติ การกระทำของคู่แข่ง จากแฮกเกอร์ และไวรัสคอมพิวเตอร์ ระดับที่สองคือ 1) ระดับ Organization ซึ่งก็คือ ผลกระทบที่เกิดจากการใช้สารสนเทศต่อการทำงานทั่วทั้งองค์กร ตัวอย่างเช่น ความเสี่ยงทางด้านกลยุทธ์เป็นต้นว่าการขาดความต่อเนื่องของการลงทุนทางด้าน IT และ 2) ระดับ Interorganizational ความเสี่ยงที่เกิดขึ้นจากการแลกเปลี่ยนเปลี่ยนข้อมูลระหว่างองค์กร นอกจากนี้จากการศึกษาของ Smith and McKeen (2009) พบว่าในยุคปัจจุบันที่บริษัทต้องพึ่งพาเทคโนโลยีสารสนเทศในการทำงานมากขึ้น การก่อกวนการให้บริการและแนวปฏิบัติในด้านการรักษาความปลอดภัยที่ไม่เพียงพอมีจำนวนเพิ่มขึ้นด้วย ดังนั้นการบริหารจัดการความเสี่ยงที่เกิดจากใช้เทคโนโลยีสารสนเทศนั้นขยายขอบเขตมากขึ้นและซับซ้อนขึ้น การรักษาความปลอดภัยเพียงทางกายภาพหรือเทคโนโลยี เช่น การใส่กุญแจห้องและการตรวจจับไวรัส อย่างที่บริษัทใช้ในอดีตนั้นไม่เพียงพอ การบริหารจัดการความเสี่ยงในปัจจุบันจะต้องมีวางกลยุทธ์และทำในแบบองค์รวม ทั้งนี้เพราะการเปลี่ยนแปลงความเสี่ยงมาได้จากทั้งภายใน เช่น จากการดำเนินงานและจากพนักงาน และจากภายนอก เช่น จากภัยพิบัติและจากผู้บุกรุก ด้วยการพัฒนากรอบแนวทางในการบริหารความเสี่ยง (Risk Management Framework) และนำมาใช้ จะสร้างความเข้าใจร่วมกันที่ถูกต้องเกี่ยวกับความเสี่ยง ระดับความเสี่ยง และผู้มีส่วนเกี่ยวข้องในเรื่องความเสี่ยง ดังนั้นองค์กรที่มีประสิทธิภาพในการบริหารจัดการความเสี่ยงจะช่วยลดผลกระทบที่เกิดจากความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศลงได้ ซึ่งก็สอดคล้องกับการศึกษาของ Carcary (2012) ที่ได้นำเอาการกำหนดมาตรฐานคุณภาพ (Capability Maturity Framework) มาใช้ในการบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ โดย IT-CMF ประกอบไปด้วย 4 กลยุทธ์ที่มีการบูรณาการเพื่อใช้ในการบริหารจัดการเทคโนโลยีสารสนเทศคือ การบริหารเทคโนโลยีสารสนเทศเหมือนว่าเป็นธุรกิจ การบริหารงบประมาณ การบริหารความสามารถและความพร้อมขององค์กรในการใช้เทคโนโลยีสารสนเทศ และการบริหารเทคโนโลยีสารสนเทศเพื่อมูลค่าทางธุรกิจ จากโมเดลนี้จะช่วยให้ผู้บริหาร (CEO/CIO) เข้าใจและพยายามปรับปรุงความพร้อมขององค์กรและบุคลากรในการใช้เทคโนโลยีสารสนเทศผ่านเกณฑ์ 5 ระดับ เพื่อให้เกิดผลประโยชน์ทางธุรกิจคุ้มค่ากับการลงทุนทางด้านเทคโนโลยีสารสนเทศ นอกจากหลักการบริหารจัดการความเสี่ยงที่กล่าวมา IT Policy Compliance Group (2008) ยังพบว่า บริษัทที่มีแนวทางการปฏิบัติที่เหมาะสมในเรื่องของการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ทางด้าน IT (IT Governance, Risk, and Compliance- IT GRC) จะช่วยให้ผลการดำเนินการทางธุรกิจดีขึ้น องค์กรที่มีการกำกับดูแล IT GRC ที่ดีกว่าจะมีสมรรถนะในการทำงานที่ดีกว่าองค์กรอื่นทั้งในด้านความพึงพอใจของลูกค้า การรักษาฐานลูกค้า และการเพิ่มขึ้นของรายได้และผลกำไร นอกจากนี้ยังช่วยลดความเสี่ยงที่เกิดจากระบบเทคโนโลยีสารสนเทศโดยช่วยลดโอกาสจากข้อมูลลูกค้าสูญหายหรือถูกขโมยลงกว่า 50 เท่า และลดความเสียหายด้านการเงินอันเกิดจากข้อมูลลูกค้าสูญหายหรือถูกขโมยกว่า 96%

2. ความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศกับอุตสาหกรรมการเงินการธนาคารและบริษัทหลักทรัพย์

ในปัจจุบันระบบเทคโนโลยีสารสนเทศมีความจำเป็นสำหรับองค์กรในการดำเนินธุรกิจ ในอุตสาหกรรมการเงินการธนาคารก็เช่นกัน เพื่อที่จะสามารถแข่งขันกับคู่แข่งและเพิ่มขีดความสามารถในการขับเคลื่อนธุรกิจ จากที่ ISACA (2009) ระบุไว้ว่าความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศในบริษัทการเงินนั้น ถือเป็นส่วนหนึ่งในความเสี่ยงอื่น ๆ ไม่ว่าจะเป็นความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ หรือความเสี่ยงด้านเครดิต อีกทั้งโครงสร้างหลักเทคโนโลยีสารสนเทศ (IT Infrastructure) ในปัจจุบัน ซึ่งตามคำจำกัดความของ K. Laudon and J. Laudon (2006) คือ ทรัพยากรเทคโนโลยีสารสนเทศที่สามาถนำมาแบ่งปันใช้งานร่วมกันได้ ซึ่งจะช่วยจัดเตรียมโครงสร้างพื้นฐานสำหรับระบบสารสนเทศขององค์กร โดยโครงสร้างหลักเทคโนโลยีสารสนเทศประกอบไปด้วย 7 ส่วนหลักที่จะต้องมีการประสานงานกันเพื่อประกอบการเป็นโครงสร้างหลักเทคโนโลยีสารสนเทศให้แก่องค์กรธุรกิจ ซึ่งประกอบไปด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์ (Computer

Hardware Platforms) โครงสร้างพื้นฐานระบบปฏิบัติการ (Operating System Platforms) โปรแกรมประยุกต์สำหรับวิสาหกิจ (Enterprise Software Application) การบริหารจัดการระบบฐานข้อมูล (Data Management and Storage) ระบบเครือข่ายและการสื่อสารระยะไกล (Networking/Telecommunications Platforms) ระบบอินเทอร์เน็ต (Internet Platforms) และบริการที่ปรึกษาและการบูรณาการ (Consulting and System Integration Service) โดยองค์กรในปัจจุบันสร้างโครงสร้างหลักเทคโนโลยีสารสนเทศด้วยการเลือกผสมผสานจากตัวแทนจำหน่าย คน และเทคโนโลยีจากหลายแหล่ง และทำให้ส่วนประกอบต่าง ๆ สามารถทำงานร่วมกันได้เป็นระบบงานเดียวกันและเนื่องจากส่วนประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศถูกขับดันด้วยการสนับสนุนจากแหล่งที่มาต่างกัน การทำให้ระบบสามารถทำงานร่วมกันเป็นหนึ่งเดียวจึงเป็นเรื่องที่ท้าทายความสามารถ องค์กรจำเป็นต้องบูรณาการข่าวสารที่ถูกจัดเก็บไว้ในโปรแกรมประยุกต์ต่าง ๆ จากระบบงานดั้งเดิม อินทราเน็ต อินเทอร์เน็ต และเว็บไซต์ รวมทั้งต้องบูรณาการข้อมูลข่าวสารที่เก็บอยู่ในเครื่องมือต่างชนิดกัน เช่น โทรศัพท์และอุปกรณ์มือถือต่าง ๆ เครื่อง PC และเครื่องโน๊ตบุ๊ค จากการศึกษาของ Fheili (2011) ก็ยังช่วยยืนยันว่าธุรกิจการธนาคารนั้นมีการเปลี่ยนแปลงจากแบบดั้งเดิมที่ให้ลูกค้ามาเข้าคิวใช้บริการ ไปเป็นแบบสมัยใหม่ที่ลูกค้าสามารถเข้าถึงได้ทุกที่ทุกเวลาของการให้บริการ โดยอุตสาหกรรมการธนาคารถือเป็นหัวใจของการปฏิวัติทางด้าน IT โดยสารสนเทศจะเข้ามาช่วยในส่วนของการพัฒนาสินค้าและบริการ พัฒนาระบบโครงสร้างของธนาคารให้ดีขึ้น ซึ่งตรงนี้ส่งผลให้เกิดความเสี่ยงที่เกี่ยวข้องการใช้เทคโนโลยีสารสนเทศขึ้น ในขณะที่ Aguilar (2011) มีความเห็นว่าบริษัทด้านการเงินจะต้องทำงานหนักขึ้นในเรื่องของความเสี่ยงไม่ว่าจะเป็นการพัฒนากรอบความเสี่ยงที่ยอมรับได้ (Risk Appetite Framework) และสร้างโครงสร้างหลักเทคโนโลยีสารสนเทศ ในสภาวะที่มีวิกฤตทางการเงินเกิดขึ้น โดยเฉพาะในเรื่องความปลอดภัยของข้อมูลถือเป็นงานท้าทายสถาบันการเงินที่จะต้องทำ นอกจากนี้จากการศึกษาของ Bakshi (2012) พบว่ากระบวนการทำงานของตลาดหลักทรัพย์ในประเทศอินเดียขึ้นอยู่กับ IT ทำให้ตลาดหลักทรัพย์ของอินเดียต้องให้ความสำคัญกับการบริหารความเสี่ยง นอกจากนี้ความผันแปรของสภาพทางธุรกิจได้เปลี่ยนโครงสร้างหลักพื้นฐานทางเทคโนโลยีสารสนเทศไม่แต่เฉพาะฮาร์ดแวร์แต่รวมถึงโปรแกรมประยุกต์และการบริการทางเทคโนโลยีสารสนเทศ ดังนั้นการใช้กรอบแนวคิดในการบริหารความเสี่ยงช่วยให้ตลาดหลักทรัพย์ของประเทศอินเดียมีโครงสร้างที่มีแบบแผนและทราบถึงความเสี่ยงเกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศที่มีอยู่ในองค์กร สามารถกำหนดกระบวนการในการตรวจสอบความเสี่ยงได้อย่างต่อเนื่อง เช่นเดียวกันกับการศึกษาของ Reinhold, Doherty, and Higgins (2011) ที่กล่าวไว้อย่างสอดคล้องว่า ในภาวะที่ต้องเผชิญกับวิกฤตทางการเงินสถาบันเงินต่าง ๆ ได้พัฒนากรอบของระดับความเสี่ยงที่องค์กรยอมรับได้และสร้างโครงสร้างพื้นฐานของระบบสารสนเทศ โดยเฉพาะความเสี่ยงทางด้านข้อมูล ดังนั้นสถาบันการเงินจะต้องกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้อย่างชัดเจน และต้องคอยติดตามความเสี่ยงนั้นอย่างมีประสิทธิภาพผ่านการเข้าถึงสารสนเทศที่ที่ถูกต้อง เชื่อถือได้ นอกจากนี้ทั้งกรอบของระดับความเสี่ยงที่องค์กรยอมรับได้และโครงสร้างพื้นฐานของระบบสารสนเทศ ยังมีความสัมพันธ์กัน ซึ่งผู้บริหารระดับสูงจำเป็นต้องพิจารณาหรือประเมินการบริหารความเสี่ยงนี้อย่างดีและยังต้องมองอนาคตข้างหน้าของกลยุทธ์ทางธุรกิจด้วยความเข้มแข็ง และความมีพลังของผู้บริหารระดับสูงมีความสำคัญมากในการที่จะแสดงให้เห็นถึงความสำคัญของกรอบของระดับความเสี่ยงที่องค์กรยอมรับได้ และความเสี่ยงทางด้านข้อมูลนั้นสามารถส่งผลกระทบต่อองค์กรได้

กลุ่มอุตสาหกรรมการเงินนั้น (ร้อยละ 31) มีความเสี่ยงที่จะเกิดจากการใช้เทคโนโลยีสารสนเทศ ดังจะเห็นจากการตกเป็นเป้าหมายของอาชญากรรมทางคอมพิวเตอร์มากเป็นอันดับสองรองจากกลุ่มอุตสาหกรรมทางด้านพลังงาน (ร้อยละ 37) (Threat Track Security, 2014) สำหรับบริษัทหลักทรัพย์ในประเทศไทยจำเป็นต้องพึ่งพาระบบคอมพิวเตอร์เป็นหลักในการทำงานตั้งแต่การใช้ระบบซื้อขายหลักทรัพย์ (Front Office System) และระบบปฏิบัติการหลักทรัพย์ (Back Office System) รวมถึงการปรับปรุงคุณภาพของการบริการทางเทคโนโลยีสารสนเทศในการซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารถูกนำมาใช้ในธุรกิจเพิ่มมากขึ้น ทั้งนี้เพราะคนส่วนใหญ่สามารถเข้าถึงข้อมูล

ไม่เฉพาะผ่านเครื่องคอมพิวเตอร์ แต่สามารถเข้าถึงผ่านสมาร์ทโฟน หรือแท็บเล็ตได้ทุกที่ทุกเวลา เพื่อรองรับกลุ่มลูกค้าที่มีความประสงค์จะส่งคำสั่งซื้อขายด้วยตนเองในยุคที่จำนวนผู้ใช้อินเทอร์เน็ตเพิ่มขึ้น โดยจำนวนผู้ใช้อินเทอร์เน็ตในประเทศไทยมีอยู่ถึง 23.8 ล้านคน คิดเป็นร้อยละ 35 ของประชากรทั้งประเทศ (Social, Digital & Mobile in APAC, 2014) ถึงแม้การนำเอาระบบสารสนเทศมาใช้ในการดำเนินงานของบริษัทหลักทรัพย์ จะมีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสแข่งขันในทางธุรกิจได้ อย่างไรก็ตามการใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง จากการศึกษาค้นคว้าประกอบกับการตรวจสอบบริษัทหลักทรัพย์ของสำนักงานคณะกรรมการการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (2552) พบว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัทหลักทรัพย์ สามารถแบ่งออกเป็น 4 ประเภท 1) Access Risk: เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ 2) Integrity Risk: เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ 3) Availability Risk: เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ 4) Infrastructure Risk: เป็นความเสี่ยงเกี่ยวกับการที่บริษัทหลักทรัพย์มิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ ความเสี่ยงที่เกิดจากใช้เทคโนโลยีสารสนเทศนั้นหากบริษัทหลักทรัพย์ไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อบริษัทหลักทรัพย์ ลูกค้า และยังส่งกระทบทางลบต่อความมั่งคั่งทางทรัพย์สินของบริษัทโดยเฉพาะบริษัทที่ให้บริการทางด้านการเงิน (Goldstein et al. , 2011)

ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร

จากการสำรวจเอกสารเรื่องปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ ส่วนใหญ่จะเป็นการศึกษาของต่างประเทศ โดยสามารถสรุปปัจจัยที่มีผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรได้ดังนี้

ปัจจัยที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ จากการศึกษาของ IT Policy Compliance Group (2008) คณะกรรมการที่กำกับดูแลระบบเทคโนโลยีสารสนเทศควรประกอบไปด้วยบุคคลจากหลายฝ่าย ซึ่งก็สอดคล้องกับงานวิจัยทั้ง 2 ชิ้น เรื่อง How the Master of IT Deliver More Value and Less Risk และ What Color is Your Information Risk - Today? ของ IT Policy Compliance Group (2010) ที่ยืนยันในลักษณะเดียวกันเรื่องบุคคลที่เกี่ยวข้องในการบริหารจัดการคุณค่า ความเสี่ยง และกำกับดูแลสำหรับ IT เพื่อให้ได้ผลลัพธ์ที่ดีผู้ที่มีส่วนเกี่ยวข้องในการบริหารจัดการความเสี่ยงควรประกอบไปด้วยบุคคลต่าง ๆ จากหลายแผนกดังนี้ ผู้จัดการฝ่าย IT ผู้ตรวจสอบภายใน ผู้บริหารระดับสูง เช่น CEO COO ผู้จัดการฝ่ายธุรกิจต่าง ๆ ผู้จัดการฝ่ายกำกับดูแลความเสี่ยง ผู้จัดการฝ่ายความปลอดภัยของระบบสารสนเทศ เช่น CISO CSO และผู้จัดการฝ่ายกฎหมายและกำกับดูแลการทำงาน และจากศึกษาของ ISACA (2009) ก็แสดงผลสอดคล้องกันว่า ผู้บริหารระดับสูงจะต้องเข้ามามีส่วนร่วมและไม่มองว่าความเสี่ยงเป็นงานของฝ่ายเทคโนโลยีสารสนเทศหรือเป็นเรื่องทางเทคนิคอย่างเดียว นอกจากนี้จากงานวิจัยของ Smith and McKeen (2009) ได้แสดงว่าการบริหารจัดการความเสี่ยงทางด้าน IT มิใช่เป็นงานเฉพาะของกลุ่มคนทางด้าน IT เท่านั้นแต่ต้องได้รับความร่วมมือจากทุกคนในแบบองค์รวม จึงสามารถนำเสนอสมมติฐานที่ 1 ได้ดังนี้

สมมติฐานที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ปัจจัยที่ 2 การควบคุมความปลอดภัยของงานสารสนเทศ การควบคุมความปลอดภัยของระบบสารสนเทศคือการนำวิธีการหรือเทคนิคต่าง ๆ มาใช้ในการป้องกันและรักษาความปลอดภัยหรือลดความเสี่ยงความเสียหายที่จะเกิดกับทรัพย์สินในระบบสารสนเทศสามารถแบ่งได้เป็น การควบคุมความปลอดภัยทางด้านกายภาพ (ไฟ น้ำ ระบบไฟฟ้า ฝุ่น และผู้บุกรุก) การควบคุมความปลอดภัยทางด้านตรรกะ (การควบคุมการเข้าถึงระบบสารสนเทศและการควบคุมป้องกันไวรัสคอมพิวเตอร์และเวิร์ม) และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ (มีแผนในการฟื้นสภาพระบบจากภัยพิบัติและมีการทำประกันภัย) (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2545) และจากการศึกษาของ IT Policy Compliance Group (2010) เรื่อง What Color is Your Information Risk - Today? พบว่าการควบคุมความปลอดภัยของสารสนเทศ จะช่วยป้องกันการรั่วไหลของข้อมูลที่สำคัญได้ ซึ่งสอดคล้องกับการศึกษาของ Bandyopadhyay et al. (1999) ที่พบว่าการมีนโยบายหรือแผนควบคุมความปลอดภัยของงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพจะช่วยลดความเสี่ยงลงได้ นอกจากนี้จากการศึกษาของ Fern (2009) พบว่าองค์กรในยุคศตวรรษที่ 21 นั้นล้วนแต่พึ่งพาเทคโนโลยีสารสนเทศ จึงจำเป็นที่จะต้องตรวจสอบความปลอดภัยทางด้านกายภาพของทรัพย์สินทางด้าน IT เช่น ผู้บุกรุก ไฟและความร้อน น้ำและความชื้น และความเสียหายของอุปกรณ์ต่าง ๆ นอกจากนี้ยังต้องควบคุมความปลอดภัยทางด้านซอฟต์แวร์จากการถูกขโมยข้อมูล โดยมีการกำหนดสิทธิการเข้าถึงข้อมูล เพราะความล้มเหลวของซอฟต์แวร์ส่งผลให้ข้อมูลเสียหายและไม่สามารถเข้าถึงได้ ดังนั้นการไม่มีนโยบายทางด้านความปลอดภัยที่เป็นลายลักษณ์อักษรและการบังคับใช้ การควบคุมรักษาความปลอดภัยที่ไม่เข้มแข็ง การบริหารจัดการที่ไม่มีประสิทธิภาพเกี่ยวกับสิทธิและการเข้าถึงข้อมูล และการไม่มีการแบ่งแยกอำนาจหน้าที่และความรับผิดชอบอย่างชัดเจน เป็นปัจจัยที่เพิ่มความเสี่ยงของการถูกคุกคาม (Maxim, 2011) จึงสามารถนำเสนอสมมติฐานที่ 2

สมมติฐานที่ 2 นโยบายการควบคุมความปลอดภัยงานสารสนเทศ ส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ปัจจัยที่ 3 งบประมาณ จากงานศึกษาของ IT Policy Compliance Group (2010) พบว่าการใช้งบประมาณทางด้าน IT ความปลอดภัยของข้อมูล และการตรวจสอบมีผลโดยตรงต่อผลลัพธ์การดำเนินงาน คือ ถ้าต้องการผลลัพธ์ที่ดีเยี่ยมการใช้งบประมาณก็ต้องสูงขึ้นด้วย ถ้าใช้งบประมาณในส่วนของความปลอดภัยและการตรวจสอบน้อย ความเสี่ยงในเรื่องของการหยุดชะงักทางธุรกิจ การสูญหายของข้อมูลหรือโดนขโมย และปัญหาในตรวจสอบก็จะมากขึ้นด้วย และงานวิจัยอีกชิ้นหนึ่งของ IT Policy Compliance Group (2011) เรื่อง How High Performance Organization Manage IT พบว่าองค์กรที่มีการใช้งบประมาณสูงกว่าโดยเฉพาะการใช้งบประมาณทางด้าน IT งบประมาณในการตรวจสอบและงบประมาณในการรักษาความปลอดภัยของข้อมูลจะมีผลลัพธ์ที่ดีกว่าในเรื่องของการลดความเสี่ยง จึงสามารถนำเสนอสมมติฐานที่ 3

สมมติฐานที่ 3 งบประมาณส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ปัจจัยที่ 4 เครื่องมือที่ใช้ในการบริหารจัดการความเสี่ยง ดังที่การศึกษาของ Bandyopadhyay, et al. (1999) กล่าวไว้ว่าการบริหารจัดการความเสี่ยงที่ดีตามขั้นตอนอันประกอบไปด้วย การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง มาตรการการลดความเสี่ยง และการตรวจสอบติดตามความเสี่ยงจะเป็นการป้องกันทรัพย์สินทางด้าน IT เป็นต้นว่าข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากรและสิ่งอำนวยความสะดวกต่าง ๆ จากการคุกคาม ภัยธรรมชาติ ความผิดพลาดทางเทคนิค การก่อวินาศกรรม และการเข้าถึงระบบโดยไม่ได้รับอนุญาต นอกจากนี้งานของ IT Policy Compliance Group (2010) เรื่อง How the Master of IT Deliver More Value and Less Risk ยังพบว่าเครื่องมือทางการบริหารสำคัญ 5 ตัวที่ถูกใช้ภายในองค์กรที่ช่วยให้ความเสี่ยงนั้นลดลงประกอบไปด้วย ISO 27001, CIS benchmarks, COBIT, IT Portfolio Management และ Balanced Scorecards โดยเครื่องมือที่นิยมใช้มากที่สุดในกรณีที่ต้องการผลลัพธ์ที่ดีที่สุดคือ ISO

27001, CIS benchmarks, COBIT ตามลำดับ ในขณะที่จากการสำรวจองค์กรที่อยู่ในอุตสาหกรรมทางการเงินทั่วโลกของ Ernst & Young (2008) พบว่าเครื่องมือที่ใช้คือ COBIT, ITIL, ISO17799, SOX และ COSO ตามลำดับ จึงสามารถนำเสนอสมมติฐานที่ 4

สมมติฐานที่ 4 เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่าง ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ปัจจัยที่ 5 ขนาดขององค์กร จากการศึกษาเรื่อง How the Master of IT Deliver More Value and Less Risk ของ IT Policy Compliance Group (2010) พบว่าบริษัทที่มีขนาดเล็ก (วัดจากผลประกอบการทั้งปี) ส่วนใหญ่จะเผชิญกับปัญหาของการหยุดชะงักทางธุรกิจอันเกิดมาจาการใช้ระบบสารสนเทศ ปัญหาในการตรวจสอบ และการสูญหายและถูกขโมยของข้อมูล ซึ่งบริษัทขนาดเล็กเหล่านี้เป็นบริษัทที่ลดค่าใช้จ่ายทางด้าน IT ในทางกลับกันบริษัทที่มีขนาดกลางและขนาดใหญ่จะพบกับปัญหาเหล่านี้น้อยกว่า โดยบริษัทขนาดใหญ่จะพบน้อยที่สุด จึงสามารถนำเสนอสมมติฐานที่ 5

สมมติฐานที่ 5 ขนาดของบริษัทที่แตกต่างกัน ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ปัจจัยที่ 6 การสื่อสารในเรื่องของความเสี่ยง การสื่อสารถือเป็นส่วนหนึ่งของระบบสารสนเทศ บุคลากรต้องสามารถสื่อสารสารสนเทศที่เกี่ยวกับความเสี่ยงข้ามหน่วยงานได้ รวมทั้งไปตามสายบังคับบัญชา ซึ่งจำเป็นต้องมีการสื่อสารที่เหมาะสมแบบเปิดเผย ตรงไปตรงมา การพัฒนาช่องทางในการสื่อสารเรื่องความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ และการใช้ภาษาที่ตรงไปตรงมา ชัดเจน ระหว่างพนักงานในองค์กรจะช่วยทำให้ความเสี่ยงลดน้อยลง (Gill, 2012) จากการเรียบเรียงของ นวพร เรืองสกุล (2553) พบว่าวิธีการสื่อสารอาจมาได้หลายรูปแบบเช่นในรูปของคู่มือนโยบาย บันทึก จดหมายอิเล็กทรอนิกส์ บอร์ดติดประกาศ การสื่อสารทางเว็บไซต์ และการสื่อสารด้วยวาจา งานวิจัยของ IT Policy Compliance Group (2010) เรื่อง How the Master of IT Deliver More Value and Less Risk ยังพบว่าการสื่อสารและการแบ่งปันของมูลเกี่ยวกับคุณค่า ความเสี่ยงและการกำกับดูแลที่เกี่ยวกับการใช้ IT เพื่อให้ได้ผลลัพธ์ที่ดีควรจะใช้วิธีต่าง ๆ ดังนี้ เช่น อีเมล์ การพูดจา รายงานในรูปแบบของการแสดงข้อมูลภาพรวมหรือข้อมูลที่ได้จากการประมวลผลร่วมกันทั้งระบบโดยนำแสดงในรูปแบบของแผนภาพ (Dashboard) รายงานที่แสดงประสิทธิภาพโดยเปรียบเทียบผลลัพธ์ตามจริงกับผลลัพธ์เป้าหมาย (Scorecard) และรายงานและข้อสรุปที่ได้จากฐานข้อมูล การใช้เพียงการโทรศัพท์ อีเมล์ และเอกสารอิเล็กทรอนิกส์แล้วเน้นการแจ้งเฉพาะเวลามีเหตุร้ายนั้นจะทำให้ผลลัพธ์ที่ออกมาไม่ดี ดังนั้นการสื่อสารเรื่องความเสี่ยงจะช่วยให้เข้าใจความเสี่ยงและสามารถจัดการความเสี่ยงได้อย่างมั่นใจ (Smith and McKeen, 2009) จึงสามารถนำเสนอดังสมมติฐานที่ 6

สมมติฐานที่ 6 การสื่อสารเรื่องความเสี่ยง ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ปัจจัยที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศ รูปแบบของการจัดโครงสร้างแผนก IT ภายในองค์กร สามารถแบ่งได้เป็น 3 โครงสร้างหลักคือ 1) Centralization คือ การรวมศูนย์ทรัพยากรที่เกี่ยวข้องกับ IT ทั้งหมดมาที่ส่วนกลาง 2) Decentralization คือ แบบกระจายศูนย์ โดยในแผนกต่าง ๆ มี IT เป็นผู้ดูแลในหน่วยงานของตน และ 3) Federalism คือ การผสมผสาน ระหว่างแบบรวมศูนย์และแบบกระจายศูนย์เข้าด้วยกัน (Luftman and Bullen, 2004) โดยแบบรวมศูนย์ทำให้การควบคุมจากฝ่ายบริหารระดับสูงในงานด้านเทคโนโลยีสารสนเทศเป็นไปโดยอัตโนมัติการใช้งานด้านฮาร์ดแวร์ ซอฟต์แวร์ และบุคลากรเป็นอย่างประหยัด และแบบกระจายศูนย์จะช่วยปรับปรุงความสามารถขององค์กร เนื่องจากมีกระจายโอกาสในการใช้งานด้านระบบสารสนเทศออกไป และช่วยลดค่าใช้จ่ายในการติดต่อสาร

เกี่ยวกับกิจกรรมด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามแบบกระจายศูนย์นั้นอาจเกิดปัญหาในการควบคุมมาตรฐาน ส่งผลให้ประสิทธิภาพและประสิทธิผลของการทำงานระบบสารสนเทศอาจต่ำกว่าที่คาดไว้ รวมถึงการรักษาทรัพย์สินและความปลอดภัยของข้อมูลอาจได้รับผลกระทบได้ (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2545) จากการศึกษาของ Co and Fink (2010) พบว่าโครงสร้างแบบกระจายศูนย์จะมีความเสี่ยงสูงกว่าเนื่องจากการควบคุมด้าน IT เป็นไปได้ยาก ในขณะที่องค์กรที่ใช้แบบผสมต้องมีการบริหารจัดการ IT ที่ดี เพื่อที่จะได้รับประโยชน์และข้อดีของแบบรวมศูนย์และแบบกระจายศูนย์ จึงสามารถนำเสนอผลดังสมมติฐานที่ 7

สมมติฐานที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกัน ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ปัจจัยที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ โครงสร้างเทคโนโลยีสารสนเทศ (IT Infrastructure) ตามคำจำกัดความของ K. Laudon and J. Laudon (2006) คือ ทรัพยากรเทคโนโลยีสารสนเทศที่สามารถนำมาแบ่งปันใช้งานร่วมกันได้ซึ่งจะช่วยจัดเตรียมโครงสร้างพื้นฐานสำหรับระบบสารสนเทศขององค์กร โดยโครงสร้างหลักเทคโนโลยีสารสนเทศประกอบไปด้วย 7 ส่วนหลักที่จะต้องมีการประสานงานกันเพื่อประกอบการเป็นโครงสร้างหลักเทคโนโลยีสารสนเทศให้แก่องค์กรธุรกิจ ซึ่งประกอบไปด้วยโครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์ โครงสร้างพื้นฐานระบบปฏิบัติการ โปรแกรมประยุกต์สำหรับวิสาหกิจ การบริหารจัดการระบบฐานข้อมูล ระบบเครือข่ายและการสื่อสารระยะไกล ระบบอินเทอร์เน็ต และบริการที่ปรึกษาและการบูรณาการ จากการศึกษาของ Fheili (2011) พบว่าในปัจจุบัน IT เป็นสิ่งจำเป็นมากสำหรับองค์กรโดยเฉพาะธนาคารและเพื่อให้องค์กรมีระบบ IT ที่ทันสมัยจำเป็นต้องมีการ Outsource บริการทางด้าน IT เพิ่มขึ้น ซึ่งนำมาสู่ความเสี่ยงทางด้าน IT ได้ นอกจากนี้การอยู่รอดของธุรกิจในปัจจุบันยังขึ้นกับโครงสร้างหลักด้านเทคโนโลยีสารสนเทศ โดยจะต้องเป็นโครงสร้างที่ปลอดภัย รวดเร็ว และพร้อมใช้ เพราะถ้าเกิดความล้มเหลวจะส่งผลให้องค์กรมีความเสี่ยงเพิ่มขึ้น ซึ่งสอดคล้องกับงานวิจัยของ Barshi (2012) ที่แสดงว่าการเปลี่ยนแปลงโครงสร้างเทคโนโลยีสารสนเทศ เป็นต้นว่า ฮาร์ดแวร์ การปรับปรุงโปรแกรมประยุกต์ใหม่ และการบริการทางเทคโนโลยีสารสนเทศ ทำให้องค์กรจะต้องระมัดระวังและกลับไปพิจารณาการจัดการบริหารความเสี่ยงอีกครั้ง การศึกษาของ Bandyopadhyay et al. (1999) ยังช่วยยืนยันว่าโครงสร้างหลักเทคโนโลยีสารสนเทศมีผลต่อความเสี่ยงทางด้าน IT โดยเฉพาะถ้าองค์กรมีระบบเครือข่ายและการสื่อสารระยะไกลและการใช้งานผ่านเว็บไซต์ จึงสามารถนำเสนอผลดังสมมติฐานที่ 8

สมมติฐานที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ปัจจัยที่ 9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี พนักงานทุกคนต้องได้รับรู้มีความเข้าใจในเรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องรู้ว่าใช้อย่างไรจึงจะปลอดภัย พนักงานต้องเล็งเห็นถึงความสำคัญของกฎเกณฑ์ นโยบาย ข้อบังคับที่องค์กรตั้งขึ้น เพื่อลดหรือหลีกเลี่ยงความเสี่ยงการฝึกอบรมและการสื่อสารให้พนักงานมีความรู้มีความเข้าใจเป็นปัจจัยช่วยลดความเสี่ยงในองค์กร (พลพธู ปียวรรณ และ สุภาพร เชิงเอี่ยม, 2552) และจากการศึกษาของ IT Policy Compliance Group (2010) พบว่าพฤติกรรมของคน เช่น ความผิดพลาด การละเลยไม่ปฏิบัติตามขั้นตอน การใช้งานอย่างไม่ถูกต้อง และการทุจริตการขโมยข้อมูล ก่อให้เกิดอันตรายต่อการใช้ระบบเทคโนโลยีสารสนเทศ ดังนั้นการให้การอบรม และเอกสารรายงานแก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ ที่เพียงพอก็จะได้ผลลัพธ์ที่ดีลดปัญหาและอันตรายทีเกิดจากการใช้ IT ให้น้อยลง ซึ่งสอดคล้องกับงานวิจัยของ Smith and McKeen (2009) ที่แสดงไว้ว่าการให้ความรู้เกี่ยวกับความเสี่ยงแก่พนักงานในองค์กร ทำให้บริษัทได้ประโยชน์เพราะพนักงานจะเข้าใจและรับรู้ถึงความเสี่ยง ทำให้สามารถจัดการความเสี่ยงได้อย่างมั่นใจ จึงสามารถนำผลดังสมมติฐานที่ 9

สมมติฐานที่ 9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

วิธีการวิจัย

1. กลุ่มประชากร และกลุ่มตัวอย่าง

ผู้บริหารฝ่าย IT หรือเทียบเท่าของบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศไทย ที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตกับนักลงทุนทุกบริษัทจำนวนทั้งสิ้น 26 บริษัท (ตลาดหลักทรัพย์แห่งประเทศไทย, 2555)

2. เครื่องมือที่ใช้ในการเก็บข้อมูล

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในครั้งนี้คือ แบบสอบถาม 3 ตอน ที่ถามถึงข้อมูลเกี่ยวกับ

2.1 ข้อมูลทั่วไปของฝ่าย IT ของบริษัท (ตำแหน่งงาน วุฒิการศึกษา อายุ และเพศ ของผู้ตอบแบบสอบถาม / จำนวนบุคลากรในบริษัทและในฝ่าย IT / ศูนย์ข้อมูลเทคโนโลยีสารสนเทศ / ศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิดจากภัยพิบัติ / โครงสร้างการจัดแผนกหรือฝ่าย IT) โดยเป็นแบบสอบถามแบบเขียนคำตอบและให้เลือกเพียง 1 คำตอบ จำนวน 11 ข้อ

2.2 ข้อมูลเรื่องการบริหารจัดการความเสี่ยง (ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงเกิดจากการใช้เทคโนโลยีสารสนเทศ / รูปแบบการกำหนดความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ / การจัดทำแผนงานระบบเทคโนโลยีสารสนเทศ / การควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพ ทางตรรกะ และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ / การจัดสรรงบประมาณทางด้าน IT งบประมาณด้านการรักษาความปลอดภัยทางด้าน IT และงบประมาณด้านการตรวจสอบด้าน IT / วิธีการในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยง / รูปแบบโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ / การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำในบริษัท) โดยเป็นแบบสอบถามแบบเขียนคำตอบ แบบให้เลือกเพียง 1 คำตอบ และแบบให้เลือกตอบได้มากกว่า 1 ข้อ จำนวน 10 ข้อ

2.3 ข้อมูลเกี่ยวกับระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ที่เกิดขึ้นในบริษัท (ระดับความเสี่ยงของข้อมูลที่สำคัญสูญหายหรือถูกขโมย / การถูกคุกคามในเรื่องความปลอดภัยบนอินเทอร์เน็ต / การหยุดชะงักทางธุรกิจเนื่องมาจาก IT เช่นการเกิดช่วงเวลาที่ไม่สามารถใช้งานได้ (Downtime) / การสูญเสียรายได้ ทรัพย์สิน / การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ / การขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT) โดยเป็นแบบสอบถามแบบมาตราส่วนประมาณค่า จำนวน 7 ข้อ

3. การเก็บรวบรวมข้อมูล

การเก็บข้อมูลในครั้งนี้ผู้วิจัยได้รวบรวมข้อมูลจากผู้บริหารฝ่าย IT หรือเทียบซึ่งเป็นผู้ที่สามารถให้ข้อมูลที่มีความถูกต้องและน่าเชื่อถือสอดคล้องกับการทำการวิจัยในครั้งนี้ จากบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตทั้ง 26 บริษัท จำนวนบริษัทละ 1 คน โดยผู้วิจัยส่งจดหมายเพื่อขออนุญาตและขอความร่วมมือในการเก็บข้อมูล รวมทั้งการนัดหมายวันเวลาที่สะดวกในการเข้าไปเก็บข้อมูล โดยผู้วิจัยได้รับความร่วมมือในการให้ข้อมูลที่มีความสมบูรณ์กลับจำนวน 21 บริษัท คิดเป็นร้อยละ 80.77

4. การวิเคราะห์ข้อมูล

ผู้วิจัยใช้สถิติพรรณนาในการบรรยายลักษณะของข้อมูลทั่วไปของกลุ่มตัวอย่างและใช้ วิธีการวิเคราะห์ความถดถอยเชิงพหุคูณ (Multiple Regression Analysis) วิธีการใช้ค่าสถิติทดสอบทีแบบกลุ่มตัวอย่างไม่สัมพันธ์กัน (t-test Independent Group) วิธีการใช้ค่าสถิติวิเคราะห์ความแปรปรวนแบบทางเดียว (One–Way Anova) และการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson Product Moment Correlation) ในการวิเคราะห์อิทธิพลและความสัมพันธ์ที่ส่งผลต่อความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

ผลการศึกษา

การวิจัยในครั้งนี้แบ่งผลการวิเคราะห์ข้อมูลเป็น 3 ส่วน ดังรายละเอียดต่อไปนี้

1. การวิเคราะห์ข้อมูลฝ่าย IT ในบริษัทหลักทรัพย์

พบว่า ทุกบริษัทหลักทรัพย์ในประเทศไทยมีศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลาง (Data Center) ที่บริษัทเอง โดยบริษัทที่ให้ข้อมูลรายละเอียดของศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางจำนวน 16 บริษัท คิดเป็นร้อยละ 76.19 มีศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางอยู่สูงกว่าชั้น 1 ทุกบริษัท ในส่วนของศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิดจากภัยพิบัติ (Disaster Recovery Site) พบว่าบริษัทหลักทรัพย์ร้อยละ 90.75 มีการจัดตั้งศูนย์นี้ โดยร้อยละ 89.47 ของบริษัทที่มีศูนย์นี้มีศูนย์อยู่ที่สาขาอื่นหรืออาคารอื่น รองลงมาร้อยละ 5.26 มีอยู่ที่บริษัทเอง และ Cyber World ในส่วนของบุคลากรพบว่าจำนวนบุคลากรในบริษัทหลักทรัพย์ที่เป็นบุคลากรในฝ่าย/แผนก IT มากกว่า 15 คน คิดเป็นร้อยละ 57.10 รองลงมาเป็นบุคลากรในฝ่าย/แผนก IT จำนวน 12–15 คน และจำนวน 6–8 คน คิดเป็นร้อยละ 23.80 และ 9.50 ตามลำดับ ลำดับสุดท้ายคือ บุคลากรจำนวน 3–5 คน และน้อยกว่า 3 คน เท่ากันคือ คิดเป็นร้อยละ 4.80

นอกจากนี้ยังพบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีการจัดรูปแบบโครงสร้างฝ่าย/แผนก IT แบบรวมศูนย์ คิดเป็นร้อยละ 76.20 รองลงมาคือ มีการจัดแบบผสม และแบบกระจายศูนย์ คิดเป็นร้อยละ 19.00 และ 4.80 ตามลำดับ และยังพบอีกว่าบริษัทหลักทรัพย์มีการใช้ระบบสารสนเทศอื่นนอกจากระบบซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ต โดยมีการใช้ระบบ Back Office e-finance ASPEN Bloomberg บัญชี ความเสี่ยงลูกค้า คิดคำนวณชำระราคา ระบบของธุรกิจกองทุนรวมหลักทรัพย์ ระบบซื้อขายที่ไม่ใช้อินเทอร์เน็ตหรือการโทรขาย การโอนเงิน และ Lotus Note

2. การวิเคราะห์ข้อมูลเรื่องการบริหารจัดการความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัท

2.1 สำหรับผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์พบว่า ผู้บริหารระดับสูงทางด้าน IT เช่น CIO เป็นผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศมากที่สุดคิดเป็นร้อยละ 18.7 รองลงมาคือ ผู้บริหารระดับสูง เช่น CEO และ COO และผู้ตรวจสอบภายใน มีอัตราส่วนเท่ากันคือ ร้อยละ 15.4 ตามด้วยตำแหน่งผู้จัดการฝ่ายบริหารความเสี่ยง คิดเป็นร้อยละ 14.3 ส่วนตำแหน่งผู้จัดการฝ่ายปฏิบัติการ IT และผู้จัดการฝ่ายความมั่นคงปลอดภัยของสารสนเทศ มีอัตราส่วนเท่ากันคือ ร้อยละ 12.1 ลำดับสุดท้ายคือ ผู้จัดการฝ่ายกฎหมายและการกำกับดูแลการปฏิบัติงาน คือ ร้อยละ 8.80 นอกจากนี้ยังมีตำแหน่งอื่น ๆ อีก คิดเป็นร้อยละ 3.3 โดยระบุว่าคือ ตำแหน่งผู้จัดการการบริหารความเสี่ยงด้านปฏิบัติการ และผู้ช่วยผู้อำนวยการฝ่าย

2.2 ในเรื่องการควบคุมความปลอดภัยทางกายภาพในด้านแรกอัคคีภัย พบว่าบริษัทหลักทรัพย์ทั้ง 21 บริษัทมีระบบแจ้งเตือนภัย รองลงมาคือ มีอุปกรณ์ฉีดดับเพลิง เช่น น้ำ สารคาร์บอนไดออกไซด์ หรือแก๊ซฮาลอน และมีการฝึกซ้อมระบบป้องกันอัคคีภัยจำนวน 20 บริษัท ลำดับถัดมาคือ บริษัทมีแผนผังแสดงจุดที่ตั้งของระบบดับเพลิงและสายไฟมีฉนวนหุ้มป้องกันคือ 14 บริษัท ในส่วนของการควบคุมความปลอดภัยทางกายภาพด้านน้ำ พบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีการเก็บทรัพย์สินระบบสารสนเทศอยู่ในชั้นที่น้ำท่วมไม่ถึงจำนวน 17 บริษัท รองลงมาคือ บริษัทมีการติดตั้งสัญญาณเตือนภัยเชื่อมต่อกับเครื่องตรวจจับ (Water Sensor) 16 บริษัท ลำดับถัดมาคือ บริษัทมีหลังคา ผนัง พื้นป้องกันการรั่วซึมจำนวน 15 บริษัท มีทางระบายน้ำที่เหมาะสม และมีข้อห้ามพนักงานนำเครื่องดื่มเข้าใกล้คอมพิวเตอร์และอุปกรณ์ จำนวน 14 และ 11 บริษัท ตามลำดับ ในเรื่องการควบคุมความปลอดภัยทางกายภาพด้านระบบไฟฟ้า พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการติดตั้งอุปกรณ์สำรองไฟหรือ UPS รองลงมาคือ มีการติดตั้งอุปกรณ์ตัดไฟ (Circuit Breaker) หรืออุปกรณ์ควบคุมแรงดันกระแสไฟ (Voltage Regulator) ส่วนการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพด้านฝุ่นพบว่ามีบริษัทหลักทรัพย์ส่วนใหญ่มีการดูดฝุ่นอยู่เสมอจำนวน 19 บริษัท รองลงมาคือ บริษัทมีพื้นห้องและพรมแบบกันฝุ่น จำนวน 11 บริษัท มาตรการสุดท้ายคือ การควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพจากผู้บุกรุกที่ไม่ได้รับอนุญาต พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการจำกัดการเข้าออก รองลงมาคือ ศูนย์คอมพิวเตอร์ของบริษัทมีประตูแข็งแรงและมีสัญญาณเตือนภัย รองลงมาคือ บริษัทเก็บดิสก์หรือเทปที่บันทึกข้อมูลเข้าตู้ล็อกกุญแจ นอกจากนี้ยังมีบริษัทที่มีการป้องกันผู้บุกรุกที่ไม่ได้รับอนุญาตด้วยวิธีอื่น ๆ เช่น เก็บดิสก์หรือเทปไว้ข้างนอกบริษัท การเอาเข้าไปเก็บที่ธนาคาร และติดตั้ง CCTV

เรื่องการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะด้านการควบคุมการเข้าถึงระบบสารสนเทศพบว่า บริษัทหลักทรัพย์ทุกบริษัทมีการกำหนดนโยบายการใช้ Password เช่น ไม่อนุญาตให้ใช้รหัสผ่านที่มีลักษณะมีจุดอ่อน รองลงมาคือ บริษัทมีการกำหนดสิทธิอำนาจการใช้งานของผู้ใช้แต่ละคน มีการบันทึกข้อมูลการใช้งาน เช่น เก็บข้อมูล Log File มีระเบียบกำหนดเกี่ยวกับการให้ เปลี่ยนแปลง และยกเลิกรหัส จำนวน 20 บริษัท รองลงมาคือ บริษัทมีการระบุผู้ใช้และพิสูจน์ผู้ใช้ที่แท้จริง จำนวน 18 บริษัท นอกจากนี้ยังมีบริษัทที่มีการป้องกันการควบคุมการเข้าถึงระบบสารสนเทศด้วยวิธีอื่น ๆ เช่น รีวิวสิทธิ์ประจำปี จำนวน 1 บริษัท ส่วนในเรื่องการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะด้วยการควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์ม พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการมีการป้องกันไวรัส รองลงมาคือ บริษัทมีการแก้ไขเมื่อตรวจเจอไวรัส จำนวน 20 บริษัท รองลงมาคือ บริษัทมีมีการตรวจหาไวรัสอย่างสม่ำเสมอ และมีการให้ความรู้แก่ผู้ใช้เกี่ยวกับอันตรายของไวรัสและการป้องกัน จำนวน 19 บริษัท ลำดับถัดมา คือ บริษัทมีการให้แต่ละหน่วยงานร่วมกันกำหนดวิธีการควบคุมการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ในเครือข่าย เช่น การเข้ารหัสข้อมูลตั้งแต่จุดเริ่มต้นถึงปลายทาง (End-to-End Encryption) จำนวน 18 บริษัท นอกจากนี้ยังมีบริษัทที่มีการควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์มด้วยวิธีอื่น ๆ เช่น กำหนดห้ามเอาไฟล์หนัง เพลง มาลงในเครื่องคอมพิวเตอร์ จำนวน 1 บริษัท

เรื่องการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีแผนในการฟื้นสภาพระบบจากภัยพิบัติ (Disaster Recovery Plan) รองลงมาคือ บริษัทมีการทำประกันภัย พบว่ามีเพียงบริษัทเดียวที่ไม่มีการทำประกันภัย โดยแผนที่บริษัทส่วนใหญ่มีคือ แผนฉุกเฉิน (Emergency Plan) รองลงมาคือ แผนสำรอง (Backup Plan) และแผนทดสอบ (Test Plan) ส่วนแผนฟื้นสภาพ (Recovery Plan) พบว่ามีบริษัทหลักทรัพย์ใช้น้อยที่สุด ในส่วนของการประกันภัยบริษัทส่วนใหญ่มีการทำประกันอุปกรณ์ฮาร์ดแวร์ รองลงมาคือ ทำประกันที่เก็บสื่อ และอื่น ๆ เช่น ทำประกันทุกสิ่งทั้งหมดในบริษัท จำนวน 5 บริษัท ลำดับถัดมาคือ การทำประกันเอกสารสำคัญและพบว่ามีบริษัทที่ทำประกันความหยุดชะงักทางธุรกิจน้อยที่สุดพบเพียง 3 บริษัท

2.3 ในเรื่องของงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 พบว่าบริษัทที่ยินยอมเปิดเผยข้อมูลทั้งสิ้น 12 บริษัท โดยมีงบประมาณทางด้าน IT ต่ำสุดอยู่ที่ 2,000,000.00 บาท สูงสุดอยู่ที่ 400,000,000.00 บาท และมีค่า

เฉลี่ยอยู่ที่ 56,000,000.00 บาท ในเรื่องของงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 พบว่าบริษัทที่มีการจัดสรรงบประมาณด้านนี้ยินยอมเปิดเผยข้อมูลทั้งสิ้น 8 บริษัท โดยมีค่างบประมาณด้านการรักษาความปลอดภัยทางด้าน IT ต่ำสุดอยู่ที่ 100,000.00 บาท สูงสุดอยู่ที่ 50,000,000.00 บาท และมีค่าเฉลี่ยอยู่ที่ 7,218,750.00 บาท ส่วนในเรื่องของงบประมาณทางด้านการตรวจสอบทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 พบว่าบริษัทที่มีการจัดสรรงบประมาณด้านนี้ยินยอมเปิดเผยข้อมูลทั้งสิ้น 2 บริษัท โดยมีค่างบประมาณด้านการตรวจสอบทางด้าน IT ต่ำสุดอยู่ที่ 300,000.00 บาท สูงสุดอยู่ที่ 1,000,000.00 บาท และมีค่าเฉลี่ยอยู่ที่ 650,000.00 บาท

ในเรื่องของอัตราการจัดสรรงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 พบว่ามีบริษัทหลักทรัพย์ที่ยินยอมให้ข้อมูลจำนวน 17 บริษัท โดยส่วนใหญ่บริษัทมีอัตราการจัดสรรงบประมาณทางด้าน IT ในปี 2012 เพิ่มขึ้นจากปี 2011 คิดเป็นร้อยละ 66.70 โดยเมื่อเปรียบเทียบกับปี 2011 แล้วมีอัตราการเพิ่มขึ้นเฉลี่ยอยู่ที่ร้อยละ 17.33 ในทางกลับกันพบว่ามีบริษัทที่มีอัตราการจัดสรรงบประมาณทางด้าน IT ในปี 2012 ลดลงจากปี 2011 คิดเป็นร้อยละ 4.80 โดยเมื่อเปรียบเทียบกับปี 2011 แล้วมีอัตราการลดลงเฉลี่ยอยู่ที่ร้อยละ 10.00 นอกจากนี้มีบริษัทคิดเป็นร้อยละ 9.50 ที่มีอัตราการการจัดสรรงบประมาณทางด้าน IT ในปี 2012 ไม่เปลี่ยนแปลงเมื่อเทียบกับปี 2011 ในส่วนของข้อมูลอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 พบว่ามีบริษัทหลักทรัพย์ที่มีการจัดสรรงบประมาณด้านนี้ที่ยินยอมให้ข้อมูลจำนวน 11 บริษัท โดยส่วนใหญ่บริษัทมีอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ในปี 2012 ไม่เปลี่ยนแปลงจากปี 2011 คิดเป็นร้อยละ 38.10 โดยมีบริษัทคิดเป็นร้อยละ 14.29 ที่มีอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ในปี 2012 เพิ่มขึ้นจากปี 2011 โดยเมื่อเปรียบเทียบกับปี 2011 พบว่ามีอัตราการเพิ่มขึ้นเฉลี่ยอยู่ที่ร้อยละ 10.00

2.4 ในเรื่องเครื่องมือที่ช่วยบริหารจัดการความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พบว่าบริษัทหลักทรัพย์มีการใช้เครื่องมือ COBIT มากที่สุด คิดเป็นร้อยละ 24.00 รองลงมาคือ มีการใช้ ISO27001 คิดเป็นร้อยละ 16.00 ลำดับถัดไปคือ IT Portfolio Management, Balanced Scorecard, ITIL, ISO17799 และเครื่องมืออื่น ๆ เช่น IT POLICY เท่ากันคิดเป็นร้อยละ 4.00

2.5 ในเรื่องวิธีการแบบต่าง ๆ ในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ พบว่า โดยส่วนใหญ่บริษัทหลักทรัพย์ติดต่อสื่อสารด้วยอีเมล์ และการใช้คู่มือนโยบายเท่ากัน คิดเป็นร้อยละ 17.89 รองลงมาคือ มีการใช้การประกาศ คิดเป็นร้อยละ 14.74 ลำดับถัดไปคือ การใช้รายงาน คิดเป็นร้อยละ 12.63 โดยจำแนกเป็น Exception Report ร้อยละ 5.26 Web-Dashboard และ Priority Report ร้อยละ 1.05 และแบบอื่น ๆ เช่น บทความร้อยละ 2.11 รูปแบบการสื่อสารลำดับถัดไปคือ การใช้โทรศัพท์ คิดเป็นร้อยละ 10.53 ลำดับถัดมาคือ การใช้เอกสารอิเล็กทรอนิกส์ และการสื่อสารด้วยวาจา คิดเป็นร้อยละ 8.42 และ 7.37 ตามลำดับ นอกจากนี้ยังมีการใช้วิธีอื่น ๆ เช่น การใช้เว็บไซต์ คิดเป็นร้อยละ 1.05

2.6 ในเรื่องโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ พบว่าเรื่องโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วย 1) ด้านฮาร์ดแวร์คอมพิวเตอร์ที่บริษัทหลักทรัพย์ใช้มากที่สุดคือ การใช้เครื่อง PC โดยทุกบริษัททั้ง 21 บริษัท มีการใช้ รองลงมาคือ โน๊ตบุ๊ค 17 บริษัท เครื่องมินิ 14 บริษัท แท็บเล็ต 8 บริษัท เครื่อง Mac 6 บริษัท เครื่องเมนเฟรม 2 บริษัท และ Power PC 2 บริษัท 2) ด้านระบบปฏิบัติการที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการใช้ระบบปฏิบัติการ Windows รองลงมาคือ Linux และ Unix คือ มีบริษัทที่ใช้ 18 และ 16 บริษัท ส่วน Solaris และ Mac OS มีใช้ 5 และ 3 บริษัท นอกจากนี้ยังมีบริษัทที่ใช้ระบบปฏิบัติการแบบอื่น ๆ เช่น VMS โอซีรี่ Jbunto Oracle Linux

Aix ระบบปฏิบัติการบน risc 6000 3) ด้านซอฟต์แวร์ประยุกต์วิสาหกิจที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์จำนวน 5 บริษัทมีการใช้ซอฟต์แวร์ประยุกต์วิสาหกิจ SON และซอฟต์แวร์ของไทย รองลงมาคือ มีการใช้ Oracle Application จำนวน 2 บริษัท SAP และ J.D. Edwards อย่างละ 1 บริษัท 4) ด้านซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูลที่บริษัทหลักทรัพย์ใช้พบว่าบริษัทหลักทรัพย์มีการใช้ซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูล SQL Server และ MS Access มากที่สุดคือ 13 บริษัท รองลงมาคือ My SQL 12 บริษัท DB2 และ Informix 8 บริษัท Oracle 4 บริษัท และ Sybase 1 บริษัท 5) ด้านการใช้บริการ Outsource ทางด้าน IT พบว่า ร้อยละ 71.43 ของบริษัทหลักทรัพย์มีการใช้บริการ Outsource ทางด้าน IT โดยพบบริษัทร้อยละ 28.57 ที่ไม่มีการใช้บริการ Outsource ทางด้าน IT โดยการใช้บริการ Outsource ที่บริษัทหลักทรัพย์ใช้บริการคือ การพัฒนาระบบสารสนเทศ ระบบเครือข่าย การติดตั้งเดินสายระบบกล้องวงจรปิด PC Support และฮาร์ดแวร์

2.7 ในเรื่องการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ พบว่า ร้อยละ 95.20 ของบริษัทหลักทรัพย์มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ มีเพียงร้อยละ 4.80 ที่ไม่มีการให้ความรู้แก่พนักงาน และยังพบอีกว่ารูปแบบของการให้ความรู้แก่พนักงานส่วนใหญ่จะเป็นการอบรมและการแจกเอกสารคู่มือ คิดเป็นร้อยละ 32 รองลงมาจะเป็นรูปแบบอื่น ๆ เช่น ผ่านระบบ e-Learning อินทราเน็ต การประชุม และการปฐมนิเทศพนักงานใหม่ คิดเป็นร้อยละ 22 และการจัดสัมมนา คิดเป็นร้อยละ 14

3. การวิเคราะห์ปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

3.1 ระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศโดยวัดจากการตอบแบบสอบถาม พบว่าระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้มี 2 ระดับ คือ ระดับต่ำ และปานกลาง โดยความเสี่ยงที่มีค่าเฉลี่ยสูงสุดคือ การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำให้ คือ มีค่าเฉลี่ย 2.38 มีส่วนเบี่ยงเบนมาตรฐาน 1.071 โดยค่าเฉลี่ยความเสี่ยงมีค่าเท่ากับ 1.95 มีส่วนเบี่ยงเบนมาตรฐาน 0.480 โดยแสดงผลในตารางที่ 1

ตารางที่ 1: ระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้

ความเสี่ยง	$\bar{X}$	S.D.	ระดับ	ลำดับ
1. ข้อมูลที่สำคัญสูญหายหรือถูกขโมย	1.65	0.933	ต่ำ	6
2. การถูกคุกคามในเรื่องความปลอดภัยบนอินเทอร์เน็ตสารสนเทศ	1.90	0.539	ต่ำ	3
3. การหยุดชะงักทางธุรกิจเนื่องมาจาก IT เช่นการเกิดช่วงเวลาที่ไม่สามารถใช้งานได้ (Downtime)	1.81	0.402	ต่ำ	4
4. การสูญเสียรายได้ ทรัพย์สิน	1.71	0.561	ต่ำ	5
5. การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้	2.38	1.071	ปานกลาง	1
6. การขาดแคลนบุคลากรที่ความเชี่ยวชาญทางด้าน IT	2.24	0.889	ปานกลาง	2
เฉลี่ย	**1.95**	**0.480**	**ต่ำ**	

3.2 การทดสอบสมมติฐาน ผลการทดสอบสมมติฐานปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์พบว่าสมมติฐาน ที่ 1, 2, 4, 6, 8 และ 9 เป็นไปตามที่ผู้วิจัยตั้งสมมติฐานไว้อย่างมีนัยสำคัญที่ระดับ 0.05 ดังนี้

สมมติฐานที่ 1 ปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ มีความสัมพันธ์ในทิศทางตรงข้ามกับความเสี่ยงเกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ กล่าวคือ ถ้าจำนวนผู้มีส่วนเกี่ยวข้องประกอบไปด้วยหลายฝ่ายความเสี่ยงก็จะลดลง โดยมีความสัมพันธ์ ร้อยละ 48.3 โดยแสดงผลในตารางที่ 2

ตารางที่ 2: การวิเคราะห์ปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยง

ความสัมพันธ์ระหว่าง	ค่าสัมประสิทธิ์สหสัมพันธ์
จำนวนผู้เกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้	–0.483*

สมมติฐานที่ 2 ปัจจัยนโยบายการควบคุมความปลอดภัยมีผลกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยประกอบไปด้วยการควบคุมทางกายภาพ การควบคุมทางตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ ส่งผลในทิศทางตรงข้ามต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ นั่นคือ ถ้ามีการความคุมความปลอดภัยงานสารสนเทศทางด้านกายภาพ ทางด้านตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติอย่างครบถ้วนความเสี่ยงก็จะลดลง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณเท่ากับ 0.887 สามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 78.70 โดยแสดงผลในตารางที่ 3

ตารางที่ 3: การวิเคราะห์ปัจจัยนโยบายการควบคุมความปลอดภัยงานสารสนเทศ

ตัวแปรพยากรณ์	b	S.E.	Beta	อันดับที่	t	sig
วิธีการควบคุมทางกายภาพ	–0.235	0.098	–0.323	3	–2.407	0.028*
วิธีการควบคุมทางตรรกะ	–0.170	0.067	–0.348	2	–2.558	0.020*
วิธีการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ	–0.330	0.092	–0.452	1	–3.582	0.002*
R = 0.887	R square = 0.787 Adjust R square = 0.749 F = 20.897					

สมมติฐานที่ 4 ปัจจัยเครื่องมือที่ใช้ในการบริหารความเสี่ยง พบว่าความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในบริษัทที่ไม่ใช้เครื่องมือในการบริหารความเสี่ยงสูงกว่าบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยง โดยบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยงมีค่าเฉลี่ยความเสี่ยงอยู่ที่ 1.62 และบริษัทที่ไม่ใช้มีค่าเฉลี่ยอยู่ที่ 2.30 โดยแสดงผลในตารางที่ 4

ตารางที่ 4: การวิเคราะห์ปัจจัยเครื่องมือที่ใช้ในการบริหารความเสี่ยง

	N	$\bar{X}$	S.D.	t-test	Sig.
ใช้เครื่องมือ	11	1.62	0.401	–4.647	0.000*
ไม่ใช้เครื่องมือ	10	2.30	0.258		

สมมติฐานที่ 6 ปัจจัยการสื่อสารเรื่องความเสี่ยง มีความสัมพันธ์ในทิศทางตรงข้ามกับความเสี่ยงที่เกี่ยงข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์นั่นคือ ถ้าจำนวนวิธีการสื่อสารเรื่องความเสี่ยงหลากหลายขึ้นค่าความเสี่ยงก็จะลดลงโดยมีความสัมพันธ์ร้อยละ 58.9 โดยแสดงผลในตารางที่ 5

ตารางที่ 5: การวิเคราะห์ปัจจัยการสื่อสารเรื่องความเสี่ยง

ความสัมพันธ์ระหว่าง	ค่าสัมประสิทธิ์สหสัมพันธ์
จำนวนวิธีการสื่อสารเรื่องความเสี่ยงกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้	–0.0589*

สมมติฐานที่ 8 ปัจจัยองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศอันประกอบด้วยโครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์ โครงสร้างพื้นฐานระบบปฏิบัติการ โปรแกรมประยุกต์สำหรับวิสาหกิจ การบริหารจัดการระบบฐานข้อมูล ระบบเครือข่ายและการสื่อสารระยะไกล ระบบอินเทอร์เน็ต และบริการที่ปรึกษาและการบูรณาการระบบงาน พบว่าส่วนประกอบของโครงสร้างเทคโนโลยีสารสนเทศที่แตกต่างกัน ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ที่แตกต่างกัน โดยแสดงผลในตารางที่ 6

ตารางที่ 6: การวิเคราะห์ปัจจัยการสื่อสารเรื่องความเสี่ยง

แหล่งความแปรปรวน	Sum of Squares	df	Mean Square	F	Sig.
ระหว่างกลุ่ม	1.747	2	0.874	5.485	0.014*
ภายในกลุ่ม	2.867	18	0.154		

สมมติฐานที่ 9 ปัจจัยการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ พบว่าการให้ความรู้แก่พนักงานในวิธีที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ที่แตกต่างกัน โดยแสดงผลในตารางที่ 7

ตารางที่ 7: การวิเคราะห์ปัจจัยการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ

แหล่งความแปรปรวน	Sum of Squares	df	Mean Square	F	Sig.
ระหว่างกลุ่ม	1.783	2	0.891	5.667	0.012*
ภายในกลุ่ม	2.831	18	0.157		

สมมติฐานที่ไม่เป็นไปตามที่ผู้วิจัยตั้งไว้มีดังนี้

สมมติฐานที่ 3 ปัจจัยด้านงบประมาณ เนื่องจากว่ามีข้อจำกัดของการเปิดเผยข้อมูลในเรื่องงบประมาณทางด้าน IT งบประมาณทางด้านความปลอดภัย และงบประมาณทางด้านการตรวจสอบของบริษัทหลักทรัพย์ ทำให้ข้อมูลที่เก็บมาได้ไม่เพียงพอต่อการการประมวลผล กล่าวคือ มีบริษัทที่ยอมเปิดเผยข้อมูลเรื่องงบประมาณน้อยกว่า 15 บริษัท

สมมติฐานที่ 5 ปัจจัยด้านขนาดของบริษัทซึ่งจัดขนาดโดยใช้ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 พบว่าบริษัทที่มีขนาดที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน โดยบริษัทที่มีขนาดใหญ่จะมีค่าเฉลี่ยของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้สูงที่สุดคือ มีค่าเฉลี่ย 2.00 โดยบริษัทขนาดเล็กและขนาดกลางจะมีค่าเฉลี่ยของความเสี่ยง 1.95 และ 1.92 ตามลำดับ

สมมติฐานที่ 7 ปัจจัยการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศพบว่าบริษัทที่มีรูปแบบที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกันโดยพบค่าเฉลี่ยความเสี่ยงเกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ของบริษัทที่จัดโครงสร้างแผนกเทคโนโลยีสารสนเทศแบบกระจายศูนย์ มีค่าเฉลี่ยของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้สูงที่สุดอยู่ที่ 2.00 บริษัทที่มีรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศแบบผสมมีค่าเฉลี่ยของความเสี่ยงอยู่ที่ 1.86 และบริษัทที่จัดโครงแผนกเทคโนโลยีสารสนเทศแบบรวมศูนย์ มีค่าเฉลี่ยของความเสี่ยงอยู่ที่ 1.96

จึงสามารถสรุปผลการวิเคราะห์ตามสมมติฐานการศึกษาได้ดังตารางที่ 8

ตารางที่ 8: ผลการทดสอบสมมติฐาน

สมมติฐาน	ผลการทดสอบ	สถิติที่ใช้
สมมติฐานที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Pearson Product Moment Correlation
สมมติฐานที่ 2 นโยบายการควบคุมความปลอดภัยงานสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Multiple Regression Analysis
สมมติฐานที่ 3 งบประมาณส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	ไม่สามารถทดสอบได้เนื่องจากข้อจำกัดในการเปิดเผยข้อมูลด้านงบประมาณของบริษัท	
สมมติฐานที่ 4 เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่างส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน	สอดคล้องกับสมมติฐาน	t-test Independent Group
สมมติฐานที่ 5 ขนาดของบริษัทที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน	ไม่สอดคล้องกับสมมติฐาน	One–Way Anova
สมมติฐานที่ 6 การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Pearson Product Moment Correlation
สมมติฐานที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน	ไม่สอดคล้องกับสมมติฐาน	One–Way Anova
สมมติฐานที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	One–Way Anova
สมมติฐานที่ 9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	One–Way Anova

อภิปรายผลและข้อเสนอแนะ

1. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย

จากการวิเคราะห์ค่าความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย พบว่าอยู่ในระดับต่ำ ทั้งนี้อาจเป็นเพราะบริษัทหลักทรัพย์ในประเทศไทยมีความตระหนักถึงความสำคัญของการรักษาความปลอดภัย รวมทั้งการปฏิบัติตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ/น. 32/2552 เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ดังจะเห็นได้จากข้อมูลที่สำรวจได้พบว่าทุกบริษัทมีศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลาง และส่วนใหญ่อยู่ชั้น 2 ขึ้นไป เพื่อความปลอดภัยจากอุทกภัย (Cisco, 2004) มีการควบคุมความปลอดภัยทางกายภาพด้าน IT และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ เป็นต้น อย่างไรก็ตามยังพบบริษัทที่ไม่มีศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิดจากภัยพิบัติ เพื่อสำรองข้อมูลและกู้คืนข้อมูลหลังภัยพิบัติ ซึ่งในประเทศไทยแม้มีแนวทางการกำกับดูแลจากคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ แต่เป็นเพียงนโยบายไม่ได้มีการบังคับใช้และบทลงโทษ รวมทั้งอาจมองว่าประเทศไทยมีอัตราการเกิดภัยพิบัติต่ำ แต่ในปัจจุบันประเทศไทยได้เผชิญกับภัยพิบัติเพิ่มขึ้นทั้งแผ่นดินไหว คลื่นสึนามิ และน้ำท่วม เป็นต้น ดังนั้นบริษัทไม่ควรละเลยและควรนำไปปฏิบัติอย่างจริงจังเพื่อจะได้ช่วยลดความเสี่ยงและทำให้บริษัทสามารถดำเนินงานได้อย่างต่อเนื่อง แม้ในยามที่ประสบภัยพิบัติ นอกจากนี้จากผลการศึกษาการพบว่าความเสี่ยงอันเกิดจากการต้องว่าจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้อยู่ในระดับสูงสุด โดยร้อยละของบริษัทที่มีการใช้บริการมีถึงร้อยละ 71.43 ถึงแม้การจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้จะมีข้อดีหลายประการเป็นต้นว่าช่วยลดต้นทุน เพราะอาจไม่คุ้มค่าที่บริษัทจะลงทุนเอง เพราะการดำเนินการโดยใช้เทคโนโลยีสารสนเทศเข้าช่วยในองค์กรเป็นการลงทุนที่สูง อีกทั้งบริษัทให้บริการมักจะมีความรู้ที่เกิดจากประสบการณ์ในการให้บริการกับลูกค้าหลายราย และมีบุคลากรที่มีความรู้เฉพาะทางในด้าน IT ทำให้สามารถดำเนินงานได้อย่างมีมาตรฐานและมีคุณภาพสูงกว่าการที่บริษัทจะทำเองรวมทั้งยังช่วยแก้ปัญหาการขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT ของบริษัท แต่ในขณะเดียวกันบริษัทอาจต้องเผชิญความเสี่ยงในเรื่องการเปิดเผยข้อมูลสำคัญบางอย่างให้แก่บริษัทให้บริการ เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน นอกจากนี้ยังอาจมีความเสี่ยงที่ผลงานของบริษัทให้บริการจะไม่เป็นไปตามที่ต้องการ ทำให้ต้องเสียเวลาในการแก้ไข ซึ่งอาจส่งผลเสียหายต่องานโดยรวมของบริษัทได้ ดังนั้นบริษัทจะต้องคำนึงถึงคือ ผู้ให้บริการควรเป็นบริษัทที่มีความชำนาญและมีประสบการณ์ในการให้บริการต้องเป็นบริษัทที่น่าเชื่อถือ เคยมีผลงานปรากฏเด่นชัด และควรพิจารณาถึงขอบเขตและระดับการให้บริการอย่างรอบคอบ

2. แนวทางการป้องกันเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

จากผลสรุปที่ได้จากการวิจัยสามารถนำเสนอแนวทางในการป้องกันและบริหารความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับมาตรฐาน COBIT ซึ่งคือ แนวปฏิบัติเพื่อให้การควบคุมภายในด้านเทคโนโลยีสารสนเทศสามารถดำเนินไปได้อย่างมีประสิทธิภาพดังตารางที่ 9

ตารางที่ 9: แนวทางการป้องกันและบริหารความเสี่ยงที่ได้จากการวิจัยเชื่อมโยงเข้ากับมาตรฐาน COBIT

การเชื่อมโยงกับกระบวนการหลักของ COBIT		แนวทางการป้องกันและบริหารความเสี่ยง
การวางแผนและการจัดการองค์กร (PO : Planning and Organization)	PO6 PO6 PO1 PO3	1. จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทที่เป็นลายลักษณ์อักษร 2. สื่อสารด้วยรูปแบบที่หลากหลายวิธีเพื่อสร้างความตระหนักถึงการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแก่ผู้เกี่ยวข้อง 3. จัดทำแผนกลยุทธ์และแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศ 4. กำหนดทิศทางด้านเทคโนโลยีด้วยการวางแผนพื้นฐานโครงสร้างเทคโนโลยีสารสนเทศ 5. จัดให้มีคณะกรรมการกำกับดูแลหรือวางแผนด้านเทคโนโลยีสารสนเทศที่มาจากหลายฝ่ายที่เกี่ยวข้อง
การจัดหาและติดตั้ง (AI : Acquisition and Implementation)	AI3	1. จัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีเพื่อให้องค์กรมีรูปแบบด้าน IT ที่เหมาะสมกับระบบงาน ลดความหลากหลายของประเภทการใช้งานลงโดยเฉพาะการใช้ฮาร์ดแวร์คอมพิวเตอร์ ระบบปฏิบัติการ และซอฟแวร์สำหรับบริหารจัดการฐานข้อมูล
การส่งมอบและบำรุงรักษา (DS : Delivery and Support)	DS2 DS12 DS5 DS4 DS7	1. มีการบริหารจัดการที่ดีในการใช้บริการจากบุคคลภายนอกเพื่อให้มั่นใจว่าผู้ให้บริการจะปฏิบัติหน้าที่ด้วยความรับผิดชอบถูกต้อง และต่อเนื่อง 2. จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ 3. จัดให้มีระบบการรักษาความปลอดภัยทางตรรกะที่เพียงพอเพื่อปกป้องข้อมูลจากการถูกใช้ เปิดเผย แก้ไข ทำลาย โดยไม่ได้รับอนุมัติหรือการสูญหาย รวมทั้งการบริหารจัดการให้ข้อมูลมีความสมบูรณ์ ถูกต้อง และน่าเชื่อถือ 4. จัดให้มีการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติเพื่อให้สามารถดำเนินธุรกิจอย่างต่อเนื่องหากมีเหตุการณ์สำคัญทำให้ต้องหยุดชะงัก เช่น การจัดให้มีศูนย์สำรองข้อมูลและการจัดเก็บสื่อข้อมูลสำรองไว้นอกสถานที่ 5. จัดให้มีการฝึกอบรมให้ความรู้แก่พนักงานอย่างเพียงพอเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพและเข้าใจถึงความเสี่ยง

(ISACA, 2009 and IT Governance Institute, 2008)

บทสรุป

ความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับต่ำ อีกทั้งผู้บริหารฝ่าย IT ของบริษัทหลักทรัพย์ทุกบริษัททราบถึงระดับความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศของบริษัทตัวเอง โดยพบว่าปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ นโยบายการควบคุมความปลอดภัย เครื่องมือที่ใช้ในการบริหารความเสี่ยง การสื่อสารเรื่องความเสี่ยง องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศและการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ เป็นตัวแปรที่ส่งผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ดังนั้นบริษัทหลักทรัพย์ควรตระหนักและให้ความสำคัญต่อปัจจัยเหล่านี้รวมทั้งมีการจัดการบริหารความเสี่ยง สร้างมาตรฐานทางด้านเทคโนโลยีสารสนเทศ เพื่อก้าวให้ทันต่อการเปลี่ยนแปลงที่อาจเกิดขึ้นได้ในการดำเนินธุรกิจ โดยต้องสร้างทัศนคติจากผู้บริหารระดับสูงจนถึงทุกฝ่ายที่เกี่ยวข้อง ให้มีจิตสำนึกถึงความสำคัญต่อการรักษาความปลอดภัยและสร้างมาตรฐานทางด้านเทคโนโลยีสารสนเทศ จะได้เป็นเครื่องยืนยันถึงความน่าเชื่อถือและความมีประสิทธิภาพในการบริหารจัดการความเสี่ยงของบริษัท ตลอดจนสร้างความเชื่อมั่นไว้ใจให้กับลูกค้าได้อย่างชัดเจน อย่างไรก็ตามการศึกษาในครั้งนี้มุ่งเน้นการวิจัยเชิงปริมาณ ดังนั้นข้อเสนอแนะสำหรับการต่อยอดงานวิจัยนี้คือทำการวิจัยเชิงคุณภาพถึงปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ เพื่อให้ได้ข้อมูลอีกรูปแบบหนึ่งประกอบการพิจารณา รวมทั้งจะได้ทราบแนวทางในการรับมือแก้ไขและแนวทางปฏิบัติที่ดีของบริษัท ในการบริหารและจัดการความเสี่ยงที่เกิดขึ้น

เอกสารอ้างอิง

ภาษาไทย

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2552). *ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์เรื่องแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์*. สืบค้นเมื่อ 1 สิงหาคม 2555, จาก http://capital.sec.or.th/webapp//nrs/data/4853s.pdf

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2552). *แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ*. สืบค้นเมื่อ 25 ตุลาคม 2557, จาก http://www.theiiat.or.th/km/newsdesc.php?n=90210161729

ตลาดหลักทรัพย์แห่งประเทศไทย. (2555). *รายชื่อบริษัทสมาชิกตลาดหลักทรัพย์แห่งประเทศไทย*. สืบค้นเมื่อ 20 มิถุนายน 2555, จาก http://www.set.or.th/set/memberlist.do?language=th&country=TH

ตลาดหลักทรัพย์แห่งประเทศไทย. (2555). *ข้อมูลสถิติทางธุรกิจหลักทรัพย์*. สืบค้นเมื่อ 25 ตุลาคม 255, จาก http://www.set.or.th/th/market/securities_company_statistics55.html

ตลาดหลักทรัพย์แห่งประเทศไทย. (2555). *SETSMART (SET Market Analysis and Reporting Tool)*. สืบค้นเมื่อ 1 กรกฎาคม 2555, จาก http://www.setsmart.com/ism/login.jsp

ไทยเซิร์ต, NECTEC. (2007). *มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั้น 2.5) ประจำปี 2550*. สืบค้นเมื่อ 20 สิงหาคม 2555, จาก http://www.nstda.or.th/pub/2009/20090206-e-comm-security-std.pdf

นวพร เรืองสกุล. (2551). *กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ: บทสรุปสำหรับผู้บริหารกรอบโครงสร้าง*. กรุงเทพฯ : อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง จำกัด.

Recall, Inc. (ไม่ปรากฏปีพิมพ์). *บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูล*. สืบค้นเมื่อ 12 ธันวาคม 2555, จาก http://www.th.recall.com/data-protection/~/media/files/Solutions/recall-data-protection-legislation-en.sdhx

บรรจง หะรังสี และ ภัทราวดี เหมทานนท์. (2555). *COBIT 5 กับการนำไปใช้งาน*. สืบค้นเมื่อ 12 ธันวาคม 2555, จาก http://www.tnetsecurity.com/content_audit/cobit5_implementtation_step.php

ประชาชาติธุรกิจ. (2546). *การควบคุมภายใน...สิ่งที่เลี่ยงไม่ได้*. สืบค้นเมื่อ 22 มกราคม 2555, จาก http://www.nidambe11.net/ekonomiz/2003q2/article2003april24p2.htm

ปริญญา หอมเอนก. (2551). *IT Service Management (ITSM), IT Infrastructure Library (ITIL V2 & V3) และมาตรฐาน ISO/IEC 20000*. สืบค้นเมื่อ 22 มกราคม 2555, จาก http://www.acisonline.net/article_prinya_eEnterprise_oct_08.htm

ปริญญา หอมเอนก. (2553). *เจาะลึก IT Governance Implementation และบทวิเคราะห์ Cobit 5.0 "Enterprise Governance of IT Framework" และ IT Governance Implementation Guide ล่าสุดจาก ISACA*. สืบค้นเมื่อ 22 มกราคม 2555, จาก http://www.theiiat.or.th/media/km/thumbnail/18/111125151018/ITGovernanceImplementation.pdf

ปริญญา หอมเอนก. (2556). *การประเมินตนเองเพื่อควบคุมความเสี่ยง-CSA/Controls self assessment ตอนที่ 8 COSO (Committee of Sponsoring Organization)*. สืบค้นเมื่อ 22 มกราคม 2556, จาก http://www.itgthailand.com/tag/องค์ประกอบของการควบคุม/

พลพธู ปียวรรณ และ สุภาพร เชิงเอี่ยม. (2552). *ระบบสารสนเทศเพื่อการจัดการ*. กรุงเทพฯ: วิทยพัฒน์.

พสุ เดชะรินทร์. (2545). *ประมวลจากกลยุทธ์สู่การปฏิบัติด้วย Balanced Scorecard และ Key Performance Indicators*. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2545). *เอกสารการสอนชุดวิชาการตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายในหน่วยที่ 1–7*. กรุงเทพฯ: มหาวิทยาลัยสุโขทัยธรรมาธิราช.

วชิราพร ปัญญาพินิจนุกูร. (2552). *มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC27001 และ ISO/IEC 1799 ฉบับประเทศไทย*. สืบค้นเมื่อ 22 ธันวาคม 2555, จาก http://www.oknation.net/blog/print1.php?id=404278

English

Aguilar, M. (2011). *Financial firms have more work on Risk, IT*. Retrieved November 22, 2011, from http://www.complianceweek.com

Bandyopandhyay, K., Mykytyn, P. P. and Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437–444.

Barksi, S. (2012). Risk IT Framework for IT Risk Management: A Case Study of National Stock Exchange of India Limited. *COBIT Focus*, *1*, 5–10.

Carcary, M. (2012). Developing a Framework for Maturing IT Risk Management Capabilities. *Proceedings of the European Conference on Information Management & Evaluation*, 33–40.

Center for Internet Security. (2009). *CIS benchmarks*. Retrieved November 22, 2011, from http:// benchmarks. cisecurity.org/downloads/benchmarks/

Cisco. (2013). *Cisco Global IT Impact Survey*. Retrieved August 12, 2013, from http://www.cisco.com/en/US/ solutions/collateral/ns1015/Cisco_IT_Impact_Survey_Results_2013.pdf

Cisco. (2004). *Data Center best practices for security and performance*. Retrieved October 25, 2014, from http://www.echomountain.com/pdfs/CiscoBestPractices.pdf

Ernst & Young. (2008). *Management Information Technology Risk A Global survey for the financial services industry*. Retrieved August 2, 2012, from http://www.ey.com

Fern, G. (2009). Don't risk IT. *British Journal of Administrative Management*, 67, 13–13.

Fheili, M. L. (2011). Information technology at the forefront of operational risk: banks are at a greater risk. *The Journal of Operational Risk, 6*(2), 47–67.

Gawenda, S. (2008). *IT Portfolio Management*. Retrieved December 22, 2011, from http://citebm.business.illinois.edu/TWC%20Class/Project_reports_Fall2008/Project%20and%20Risk%20Management/Sebastian%20Gawenda/OT%20Portfolio%20Management%20Paperx.pdf

Gill, M. (2012). IT Risk is Business Risk. *COBIT Focus*, 2, 10–12.

Goldstein, J., Chernobai, A. and Benaroch, M., (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information System, 12*(9), 606–631.

ISACA. (2009). *The risk IT Framework*. Retrieved July 20, 2012, from http://www.isaca.org/riskitfw

ISACA. (2009). *COBIT 4.1 Framework for IT Governance and Control*. Retrieved October 27, 2014, from http://isaca.org Knowledge-Center/COBIT/Pages/Overview.aspx

IT Governance Institute. *COBIT MAPPING*. Retrieved October 27, 2014, from http://www.itsm.hr/baza%20znanja/Mapping% 20ITILV3%20COBIT41.pdf

IT Policy Compliance Group. (2008). *Annual Report: IT Governance, Risk and Compliance- Improving Business Results and mitigating Financial risk*. Retrieved December 22, 2011, from http://www.itpolicycompliance.com/research-reports/2008-annual-report-it-governance-risk-and-compliance-%e2%80%93-improving-business-results-and-mitigating-financial-risk

IT Policy Compliance Group. (2010). *What Color is Your Information Risk—Today?*. Retrieved December 22, 2011, from http://www.itpolicycompliance.com/research-reports/what-color-is-your-information-risk-%e2%80%93-today

IT Policy Compliance Group. (2010). *How the Master of IT Deliver More Value and Less Risk*. Retrieved December 22, 2011, from http://www.itpolicycompliance.com/research-reports/how-the-master-of-it-deliver-more-value-and-less-risk

IT Policy Compliance Group. (2011). *How High Performance Organization Manage IT*. Retrieved December 22, 2011, from http://www.itpolicycompliance.com/research-reports/how-high-performance-organizations-manage-it

Ko, D. and Fink, D. (2010). Information technology governance: an evaluation of the theory-practice gap. *Corporate Governance, 10*(5), 662–674.

Laudon, K. C. and Laudon, J. P. (2006). *Management Information Systems*. Pearson Education Indochina Ltd.

Luftman, N. J. and Bullen, C. F. (2004). *Managing the Information Technology Resource*. Pearson Prentice Hall.

Maxim, M. (2011). *Defending against insider threats to reduce your IT risk. White Paper Security and Compliance*, Retrieved October 25, 2014, from http://www.informationweek.com/whitepaper/Security/Vulnerabilities-and-Threats/defending-against-insider-threats-to-reduce-your-i-wp1310136646?articleID=191702534

Reinhold, B., Doherty, J. and Higgins, D. (2011). Rethink risk, rethink technology. *ABA Banking Journal, 103* (4), 27–30.

Smith, H. A. and McKeen, J. D. (2009). Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk. *Communications of the Association for Information Systems*, *25*, 519–530.

Social, Digital & Mobile in APAC (2014). *2014 Asia-Pacific Digital Overview*. Retrieved October 22, 2014, from http://www.slideshare.net/wearesocialsg/social-digital-mobile-in-apac

TreatTrack Security. (2014). *Energy Company and Financial Service Firms Remain Vulnerable to Data-Breaching Malware*. Retrieved October 25, 2014, from http://www.threattracksecurity.com/resources/white-papers/data-breaching-malware-threatens-energy-and-finance-firms.aspx

Westerman, G. and Hunter, R. (2007). *IT Risk turning business threats into competitive advantage*. Boston: Harvard Business School Publishing.

Translated Thai References (ส่วนที่แปลรายการอ้างอิงภาษาไทย)

The Securities and Exchange Commission. (2009). *Announcement of the securities and exchange commission: Information Technology security regulation and monitoring for Securities Companies*. Retrieved August 1, 2012, from http://capital.sec.or.th/webapp//nrs/data/4853s.pdf

The Securities and Exchange Commission. (2009). *Information Technology security regulation and monitoring*. Retrieved October 25, 2014, from http://www.theiiat.or.th/km/newsdesc.php?n=90210161729

The Stock Exchange of Thailand. (2012). *Listed Securities Companies in Thailand*. Retrieved June 20, 2012, from http://www.set.or.th/set/memberlist.do?language=th&country=TH

The Stock Exchange of Thailand. (2012). *SETSMART (SET Market Analysis and Reporting Tool)*. Retrieved July 1, 2012, from http://www.setsmart.com/ism/login.jsp

ThaiCERT, NECTEC. (2007). *Information Security Standard for Electronic Transactions (version 2.5) 2007*. Retrieved August 20, 2012, from http://www.nstda.or.th/pub/2009/20090206-e-comm-security-std.pdf

Navaporn Ruangsakul. (2008). *Enterprise Risk Management – Integrated Framework: Executive Summary*. Bangkok: Amarin Printing and Publishing.

Recall, Inc. (no date). *Data Protection Legislation*. Retrieved December 12, 2012, from http://www.th.recall.com/data-protection/~/media/files/Solutions/recall-data-protection-legislation-en.sdhx

Banjong Harangsee and Patravadee Hemtanon. (2012). *Use of COBOT 5*. Retrieved December 12, 2012, from http://www.tnetsecurity.com/content_audit/cobit5_implementtation_step.php

Prachachat Business Newspaper. (2003). *Internal Control...Inevitable*. Retrieved January 22, 2012, from http://www.nidambe11.net/ekonomiz/2003q2/article2003april24p2.htm

Prinya Hom-anek. (2008). *IT Service Management (ITSM), IT Infrastructure Library (ITIL V2 & V3) and ISO/IEC 2000 Standard*. Retrieved January 22, 2012, from http://www.acisonline.net/article_prinya_eEnterprise_oct_08.htm

Prinya Hom-anek. (2010). *Delve into IT Governance Implementation and Cobit 5.0 Enterprise Governance of IT Framework and Latest IT Governance Implementation Guide from ISACA*. Retrieved January 22, 2012, from http://www.theiiat.or.th/media/km/thumbnail/18/111125151018/ITGovernanceImplementation.pdf

Prinya Hom-anek. (2013). *Controls Self Assessment - CSA Chapter 8 COSO (Committee of Sponsoring Organization)*. Retrieved January 22, 2012, from http://www.itgthailand.com/tag/องค์ประกอบของการควบคุม/

Polpatoo Piyawan and Supaporn Choeng. (2009). *Management Information System*. Bangkok: Wittayapat.

Pasu Decharin. (2002). *Strategy to Action with Balanced Scorecard และ Key Performance Indicators*. Bangkok: Chulalongkorn University Publishing.

Sukhothaitammatirat University. (2002). Computer Audit and Internal Control Unit 1–7 Material. Bangkok: Sukhothaitammatirat University.

Wachiraporn Panyapinitkukul. (2009). *ISO/IEC 27001 and ISO/IEC 17999 Information Security Standard (Thailand version)*. Retrieved December 22, 2012, from http://www.oknation.net/blog/print1.php?id=404278