ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

Factors influencing IT Risks for Securities Companies in Thailand

สาริยา นุชอนงค์

การวิจัยนี้ได้รับทุนอุดหนุนจากมหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ
ปีการศึกษา 2555

ชื่อเรื่อง : ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย
ผู้วิจัย : สาริยา นุชอนงค์
สถาบัน : มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ
ปีที่พิมพ์ : 2557
สถานที่พิมพ์ : มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ
แหล่งที่เก็บรายงานฉบับสมบูรณ์ : มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ
จำนวนหน้างานวิจัย : 107 หน้า
คำสำคัญ : ความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ
ลิขสิทธิ์ : มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาถึงระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย 2) ศึกษาปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย และ 3) สำรวจข้อมูลรวมทั้งการบริหารจัดการความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย โดยมีวิธีดำเนินการกับกลุ่มเป้าหมายคือบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศ ไทยที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตจำนวนทั้งสิ้น 21 บริษัท สถิติที่ใช้ในการวิเคราะห์ข้อมูลประกอบด้วย หาความถี่ ร้อยละ(%) หาค่าเฉลี่ย (Mean) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) วิเคราะห์ความแตกต่างระหว่างกลุ่มใช้การทดสอบแบบกลุ่มตัวอย่างไม่สัมพันธ์กัน (t-test Independent Group) การทดสอบความแปรปรวนทางเดียว (One-way Anova) วิเคราะห์ตัวแปรอิสระที่ส่งผลต่อต่อตัวแปรตามโดยใช้วิธีการถดถ่อยอย่างง่าย (Simple Regression Analysis) และ วิธีการถดถอยพหุคูณ (Multiple Regression Analysis)

ผลการวิจัยพบว่า

1. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับต่ำ โดยพบความเสี่ยงอันเกิดจากการต้องว่าจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ (outsource) อยู่ในระดับสูงสุด

2. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์เมื่อจำแนกตามเครื่องมือที่ใช้ในการบริหารความเสี่ยง แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ส่วนการจำแนกตามขนาดของบริษัท และรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศ ไม่แตกต่างกัน

3. ปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 23.80 ปัจจัยนโยบายการควบคุมความปลอดภัยส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 78.70 ปัจจัยการสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 34.70 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 28.00 และ ปัจจัยการให้ความรู้แก่พนักงานในเรื่อง

นโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 63.40 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

4. บริษัทหลักทรัพย์ส่วนใหญ่มีโครงสร้างและการบริหารจัดการ รวมทั้งการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ดีสอดคล้องกับประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

Research Title	: Factors influencing IT Risks for Securities Companies in Thailand
Researcher (s)	: Sariya Nuchanong
Institution	: Huachiew Chalermprekiet University
Year of Publication	: 2014
Publisher	: Huachiew Chalermprekiet University
Source	: Huachiew Chalermprekiet University
No. of Pages	: 107 pages
Keywords	: IT Risk
Copyright	: Huachiew Chalermprekiet University

Abstract

The purpose of this research were 1) to study the level of IT Risks for Securities Companies in Thailand, 2) to study factors influencing IT Risks for Securities Companies in Thailand, and 3) to survey IT professionals from all Securities Companies in Thailand to understand how well the companies can organize and manage IT Risks. Samples were 21 IT managers from Securities Companies in Thailand. Tools used to collect data were questionnaires developed by the researcher. Data were analyzed by percentage, frequency, mean, standard deviation, t-test Independent Group, One-way Anova, Simple Regression Analysis, 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. IT Risk as classified by risk management tools was statistically significant different at 0.05, while there were no statistical difference of IT Risks as classified by company sizes and IT department structures.

3. People who involve in IT Risks, security control policies, IT Risks communication, IT infrastructure and providing employees the knowledge of security policies and best practices were the factors affecting IT Risks for Securities Companies in Thailand, accounted for 78.70, 34.70, 28.00 and 63.40 percent of total variance repectively with the statistically significant difference at 0.05.

4. Most of all Securities Companies in Thailand are well structured and organized as well as strictly operational control and IT security according to the announcement of The office of Thai Securities and Exchange Commission in terms of Operational control and IT security.

กิตติกรรมประกาศ

รายงานการวิจัยฉบับนี้สำเร็จอย่างสมบูรณ์ ได้ด้วยความช่วยเหลืออย่างดียิ่งจาก อาจารย์ ดร. ธิดารัตน์ โชคสุชาติ ที่ได้กรุณาให้คำแนะนำปรึกษา และข้อมูลต่างๆ และเป็นกำลังใจที่สำคัญยิ่งมาโดยตลอด ขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอขอบพระคุณ รศ.ดร. ดนยพฤทธ์ ไกรฤทธิ์ Professor & Acting Dean School of Management , Asian Institute of Technology(AIT) ที่เสียสละเวลาอันมีค่าให้คำแนะนำทำให้งานวิจัยนี้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณ ผศ. ดร.ณัฐธนนท์ หงส์วริทธิ์ธร อาจารย์ประจำภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ คุณเขมรินทร์ อัมฤทธิ์ Head of IT บริษัทหลักทรัพย์ แมคควอรี่ (ประเทศไทย) และ คุณขนิฐา หล่อลักษณ์ Business Risk Management Director บริษัท Diageo Moet Hennessy (Thailand) Ltd. ที่ได้กรุณาให้คำแนะนำตลอดจนช่วยตรวจสอบเครื่องมือที่ใช้ในการวิจัย

ขอขอบคุณผู้บริหารฝ่าย IT ของบริษัทหลักทรัพย์ทุกท่าน ที่ให้ความร่วมมือและอำนวยความสะดวกในการเก็บข้อมูลเป็นอย่างดี

และที่ขาดไม่ได้ขอขอบคุณอาจารย์ ดร. วนิดา พฤทธิวิทยา อาจารย์ประจำภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ รุ่นน้องที่แสนดีที่ช่วยติดต่อประสานงาน ทำให้งานวิจัยชิ้นนี้ดำเนินลุล่วงไปอย่างราบรื่น

ท้ายที่สุดผู้วิจัยขอน้อมบูชาพระคุณบิดามารดาและอาจารย์ทุกท่านที่ได้อบรมสั่งสอนวิชาความรู้และให้ความเมตตาแก่ผู้วิจัยมาโดยตลอด เป็นกำลังใจสำคัญที่ทำให้การศึกษาวิจัยฉบับนี้สำเร็จลุล่วงได้ด้วยดี

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญตาราง(ต่อ)

ตารางที่ **หน้า**

สารบัญรูปภาพ

ภาพที่ **หน้า**

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

จากเหตุการณ์ภัยพิบัติต่างๆที่เกิดขึ้นไม่ว่าจะเป็นภัยพิบัติจาก tsunami ที่ญี่ปุ่น หรือที่เหตุการณ์น้ำท่วมครั้งใหญ่ในประเทศไทยปี 2554 ทำให้เราทราบว่าความเสี่ยงนั้นสามารถเกิดขึ้นได้ตลอดเวลาและทำให้เกิดความเสียหายอย่างมากมายและถ้าขาดการป้องกันและวางแผนที่ดีก็ทำให้เกิดความเสียหายร้ายแรงได้ เช่นเดียวกันกับเทคโนโลยีสารสนเทศซึ่งปัจจุบันได้มีการนำมาใช้ในการขับเคลื่อนองค์กรอย่างกว้างขวาง และในโลกปัจจุบันองค์กรต่างๆมุ่งสู่โลกไซเบอร์ที่อาศัยข้อมูลอิเล็กทรอนิกส์เพื่อความสะดวกลื่นไหลในการใช้ข้อมูลแต่ยิ่งสะดวกลื่นไหลมากเท่าไรก็ยิ่งมีความเสี่ยงสูงขึ้น นอกจากนี้ระบบสารสนเทศยังเป็นโครงสร้างพื้นฐานของการดำเนินธุรกิจต่างๆจำเป็นที่ต้องมีการบริหารจัดกา รที่ดีเพื่อรองรับความเสี่ยงต่างๆที่อาจเกิดขึ้นความเสี่ยงที่เกี่ยว ข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรนั้นจากการศึกษาของ IT Policy Compliance Group (2008) พบว่าไม่ได้มาจากทางด้านเทคนิคเทคโนโลยี หรือบุคลากรฝ่ายปฏิบัติการแต่ว่ามาจาก ความล้มเหลวจากการละเลยขององค์กรและความผิดพลาดจากกระบวนการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (IT Governance) ซึ่งความล้มเหลวเหล่านี้นำไปสู่การตัดสินใจที่ผิดพลาดและโครงสร้างทาง IT ที่ไม่ถูกต้อง นอกจากนี้ การมองว่าความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรอยู่แต่เฉพาะในฝ่าย IT เป็นสิ่งที่ไม่ถูกต้อง เพราะว่า IT Risk ก็คือ Business Risk ดังนั้นมุมมองที่ใช้เทคโนโลยีในการขับเคลื่อนและการแตกมุมมองทางด้าน IT Risk จำเป็นต้องถูกแทนที่ด้วยการมองแบบบูรณาการโดยเริ่มจากการเข้าใจ Business Risk และผลที่ตามมาจากการตัดสินใจทาง IT การบริหารจัดการด้วยการบูรณาการมุมมองทางธุรกิจของIT riskโดยผ่านองค์ประกอบที่สำคัญ 3 ประการอันได้แก่ Foundation (Foundation of IT assets คือระบบโครงสร้างพื้นฐานและเทคโนโลยีโปรแกรมประยุกต์ต่างๆรวมทั้งการกำหนดหน้าที่ความรับผิดชอบของบุคลากรและกระบวนการการทำงาน) Process (Risk governance process คือการกำหนดมุมมองของความเสี่ยงระดับ enterprise level เพื่อให้ผู้บริหารระดับสูงสามารถลำดับความสำคัญและตัดสินใจจัดการกับความเสี่ยงได้อย่างเหมาะสม ขณะเดียวกันก็ยังให้โอกาสผู้บริหารระดับล่างสามารถที่จะบริหารจัดการความเสี่ยงส่วนของตนเองได้อิสระ) และ Awareness (Risk aware culture คือการสร้างวัฒนธรรมในองค์กรทำให้ทุกคนตระหนักและรับรู้ถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้น) ซึ่งการบริหารจัดการความเสี่ยงผ่านทาง 3 องค์ประกอบที่กล่าวมาแล้วนั้นมีความสำคัญต่อทุกองค์กรมากโดยจะช่วยลดภัยคุกคามทางด้านITขณะเดียวกันจะช่วยเพิ่มมูลค่าทางธุรกิจจากการใช้ IT อีกด้วย (Westerman and Hunter. 2007)

นอกจากนี้การเปิดเผยข้อมูลผลสำรวจเกี่ยวกับผลประทบทางด้าน IT ทั่วโลกของซิสโก้ (Cisco Global IT Impact Survey. 2013) ก็เป็นเครื่องยืนยันถึงความเสี่ยงที่เกิดขึ้นได้ทั้งนี้เพราะฝ่าย IT มีการปรับใช้เทคโนโลยีใหม่ๆในการปรับปรุงธุรกิจมากขึ้น บริษัทต่างๆมีการติดตั้งโปรแกรมประยุกต์ทางคอมพิวเตอร์ใหม่ๆมากขึ้น รวมทั้งการขยายเครือข่ายปรับเปลี่ยนกลยุทธ์ระบบเครือข่ายให้สอดคล้องกับความต้องการทางธุรกิจ ซึ่งจากรายงานพบว่ามีการติดตั้งโปรแกรมประยุกต์ทางคอมพิวเตอร์เพิ่มขึ้นจากปีที่แล้ว และยังแสดงว่ามีการดำเนินงานทางธุรกิจใหม่ๆโดยที่ไม่ได้ปรึกษาฝ่าย IT ซึ่งอาจส่งผลกระทบต่อระบบเครือข่ายในการรองรับโปรแกรมประยุกต์ทางคอมพิวเตอร์ใหม่ๆ ผลสำรวจยังเปิดเผยอีกว่าประสิทธิภาพของระบบเครือข่ายส่งผลกระทบต่อโปรแกรมประยุกต์ทางคอมพิวเตอร์ นอกจากนี้ประเด็นด้านความปลอดภัยยังถูกระบุว่าเป็นอุปสรรคอันดับหนึ่งที่ขัดขวางการความสำเร็จการปรับใช้ระบบเครือข่าย cloud

จะเห็นได้ว่าความเสี่ยงมีความสำคัญมากแต่หลายๆบริษัทไม่ได้ตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ จากการศึกษาของ IT Policy Compliance Group (2010) พบว่าบางบริษัทไม่สามารถตอบได้ถึงความเสี่ยงที่เกิดขึ้นในบริษัท หรือตอบได้แต่ใช้เวลาในการค้นหาคำตอบ โดยเฉพาะสถาบันการเงินซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงในเรื่อง IT อย่างมีประสิทธิภาพโดยจะต้องทำงานอย่างหนักโดยเฉพาะอย่างยิ่งในเรื่องของข้อมูลสำคัญรวมถึงข้อมูลของลูกค้า เพราะข้อมูลนั้นมีความสำคัญมากและมีความเสี่ยงที่จะสูญหายหรือถูกขโมย อีกทั้งในปัจจุบันการทำงาน ธุรกรรมต่างๆล้วนผ่านทางอินเตอร์เน็ต ดังนั้นการป้องกันควบคุมความปลอดภัยนั้นมีความสำคัญมากเพราะถ้ามีปัญหาจะนำไปสู่การหยุดชะงักทางธุรกิจซึ่งหมายถึงการสูญเสียรายได้และทรัพย์สิน นอกจากนี้ความเสี่ยงจากภัยธรรมชาติก็เป็นประเด็นที่ต้องไม่ละเลยและให้ความสำคัญด้วยเช่นกันเพราะในปัจจุบันเกิดภัยธรรมชาติบ่อยครั้งซึ่งแต่ละครั้งก็ก่อให้เกิดความเสียหายอย่างมาก นอกจากความเสี่ยงที่กล่าวมาแล้วความไม่มีประสิทธิภาพของการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (Ineffective IT Governance) เป็นปัจจัยที่สำคัญที่ทำให้เกิดความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร คือการขาดโครงสร้างและกระบวนการที่เหมาะสมสำหรับความเชื่อมโยงทางธุรกิจในการลงทุนทาง IT และการตัดสินใจ ความซับซ้อนที่ยากต่อการควบคุม และความละเลยเพิกเฉยต่อความเสี่ยง ซึ่งส่วนใหญ่มีสาเหตุมาจากการไม่รู้ การบริหารจัดการโครงสร้างพื้นฐานที่ไม่ดี การละเลยเพิกเฉยหรือการทุจริตของพนักงาน และ การมีระบบที่ไม่ปลอดภัยผู้ที่มีส่วนเกี่ยวข้อง หรือมีบทบาทรวมทั้งหน่วยงาน ในการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรนั้นก็มีความสำคัญมากเพราะการที่องค์กรมีพนักงานที่มีความรู้ความสามารถทางด้าน IT อย่างดีไม่ได้หมายหมายว่าจะสามารถควบคุมความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรได้ ดังนั้นการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรและ การกำกับดูแลให้การปฏิบัติงานและการดำเนินธุรกรรมขององค์กรให้เป็นไปตามกฎเกณฑ์ นั้นจำเป็นต้องอาศัยความร่วมมือจากหลายคนหลายฝ่ายมาเกี่ยวข้องร่วมกันผู้บริหารเทคโนโลยีระดับสูง (CIO) จะต้องชัดเจนในเรื่องของผลทางธุรกิจที่จะเกิดขึ้นจากความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรและต้องมีการบริหารจัดการความเสี่ยงเพื่อเป็นการสร้างสภาพแวดล้อมในการตัดสินใจเพื่อให้ผู้บริหารขององค์กรสามารถตัดสินใจเกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรในเชิงธุรกิจได้เพื่อให้เกิดประสิทธิภาพและประสิทธิผลดีที่สุดและเพื่อที่จะลดความเสี่ยงลงการนำเครื่องมือมาช่วยในการบริหารจัดการก็มีความจำเป็นด้วยเช่นกัน ปัจจุบันมีเครื่องมือจำนวนมากให้เลือกใช้ไม่ว่าจะเป็น IT Balanced Scorecard, Strategic IT map, COBIT, ISO, IT GRC system(Governance, risk, compliance), หรือ IT Portfolio management เป็นต้น (IT Policy Compliance Group. 2010)

ทุกองค์กรต้องเผชิญกับความไม่แน่นอนและด้วยการใช้ IT ในองค์กรมีความเสี่ยงโดยเฉพาะสถาบันทางการเงินที่ซึ่งมีการใช้ระบบสารสนเทศจำนวนมากในการประกอบธุรกิจอย่างแพร่หลาย มีแรงจูงใจจากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์หรือความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์หรือการที่ไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการตลอดจนการบริหารจัดการ ระบบคอมพิวเตอร์และบุคลากรด้านคอมพิวเตอร์ ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจจำเป็นต้องมีการบริหารจัดการเพื่อลดความเสี่ยง และให้ความสำคัญกับระบบป้องกันความปลอดภัย นอกเหนือจากการลงทุนทางด้านฮาร์ดแวร์และซอฟต์แวร์ ปัจจุบันสถาบันการเงินและธนาคารเริ่มตื่นตัวมากขึ้นเพื่อปรับตัวตามระเบียบข้อบังคับด้านความปลอดภัย จึงจำเป็นต้องมีการศึกษาว่ามีความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้

ใดบ้างที่เกิดขึ้นและปัจจัยที่มีผลต่อความเสี่ยงทางด้าน IT เพราะการที่ทราบความเสี่ยงและปัจจัยความเสี่ยงจะช่วยให้เราสามารถป้องกันความเสี่ยงทางด้าน IT ที่จะเกิดขึ้นได้นอกจากนี้ยังนำข้อมูลที่ได้ไปใช้ในการปรับปรุงการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีทำให้ผลการดำเนินธุรกิจดีขึ้นและมีความเสี่ยงทางด้านการเงินน้อยลง

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาถึงระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย
2. เพื่อศึกษาปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย
3. เพื่อสำรวจข้อมูล รวมทั้งการบริหารจัดการความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

คำถามในการวิจัย

1. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับใด
2. มีปัจจัยใดบ้างที่ส่งผลต่อเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย
3. โครงสร้างของฝ่ายเทคโนโลยีสารสนเทศ และ การบริหารจัดการความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทยเป็นอย่างไร

สมมติฐานของการวิจัย

1. ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศขององค์กรส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
2. นโยบายการควบคุมความปลอดภัยส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
3. งบประมาณส่งผลต่อความเสี่ยงที่ที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
4. เครื่องมือที่ใช้ในการบริหารความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
5. ขนาดของบริษัทที่แตกต่างกันส่งผลต่อกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
6. การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
7. รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
8. องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงเกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร

ขอบเขตของการวิจัย

บริษัทหลักทรัพย์ต่างๆที่ใช้ในงานวิจัยนี้เป็นบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศไทยไม่รวม Sub-broker และเปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตในปี 2555 จำนวนทั้งสิ้น 26 บริษัท (ดูรายละเอียดในภาคผนวก จ)

นิยามศัพท์เฉพาะ

1. ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงหมายถึงบุคคลในบริษัทหลักทรัพย์ที่มีหน้าที่ในเรื่องของการกำหนดและบริหารจัดการความเสี่ยง, บริหารจัดการคุณค่า, และกำกับดูแลในเรื่องการบริหารความเสี่ยง
2. นโยบายการควบคุมความปลอดภัยของงานสารสนเทศ คือ การควบคุมทางกายภาพ การควบคุมทางตรรกะ และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ
3. งบประมาณคือจำนวนงบประมาณทางด้านเทคโนโลยีสารสนเทศ, จำนวนงบประมาณด้านการรักษาความปลอดภัย, จำนวนงบประมาณด้านการตรวจสอบ
4. เครื่องมือที่ใช้ในการบริหารความเสี่ยงคือรูปแบบของเครื่องที่ใช้ในการบริหารความเสี่ยงอันประกอบไปด้วยเครื่องมือดังต่อไปนี้ ISO 27001, CIS benchmarks, COBIT, IT portfolio management, Balanced Scorecard, ITIL, ISO17799, SOX และ COSO
5. ขนาดขององค์กรแบ่งเป็น องค์กรขนาดเล็กคือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 44,684,048,523 ถึง 523,381,373,618 บาท, องค์กรขนาดกลางคือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 523,381,373,619 ถึง 1,002,078,698,712 บาท และ องค์กรขนาดใหญ่คือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 1,002,078,698,712 บาทขึ้นไป
6. การสื่อสารเรื่องของความเสี่ยงคือวิธีในการสื่อสารทั้งภายในและภายนอกอันประกอบไปด้วย รูปแบบรายงาน ซึ่งแบ่งเป็น Exception report, Priority report, Web-dashboard, Email, การพูดจา, โทรศัพท์,เอกสารอิเล็กโทรนิกส์, คู่มือนโยบายและประกาศ
7. รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีคือ รูปแบบของการจัดโครงสร้างแผนก IT ภายในองค์กร ได้แก่ แบบรวมศูนย์ (Centralization), แบบกระจายศูนย์ (Decentralization) และ แบบผสม (Federalism)
8. องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศคือ โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต และ บริการที่ปรึกษาและการบูรณาการระบบงาน
9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำหรือไม่ ได้แก่ การสัมมนา, การอบรม, การแจกเอกสารคู่มือ

ประโยชน์ที่คาดว่าจะได้รับ

1. บริษัทหลักทรัพย์หรือบริษัทในรูปแบบธุรกิจอื่น ๆ เข้าใจและตระหนักถึงความเสี่ยงที่เกี่ยวกับการใช้เทคโนโลยีสารสนเทศรวมทั้งผลกระทบที่เกิดขึ้นจากต้นเหตุเพื่อใช้เป็นแนวทางในการบริหารความเสี่ยงที่มีประสิทธิภาพ
2. ก่อให้เกิดการพัฒนาความรู้เกี่ยวกับปัจจัยต่าง ๆ ที่ส่งผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร
3. ผู้บริหารบริษัทหลักทรัพย์หรือบริษัทในรูปแบบธุรกิจอื่นๆสามารถนำผลการวิจัยไปใช้ในการวางแผนกำหนดนโยบาย และปรับปรุงแนวปฏิบัติด้านเทคโนโลยีสารสนเทศให้มีการบริหารจัดการเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีและเหมาะสมซึ่งจะส่งผลให้การดำเนินธุรกิจดีขึ้นการลดความเสี่ยงที่เกี่ยวกับการใช้เทคโนโลยีสารสนเทศในการดำเนินงานของบริษัท

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องผู้วิจัยมีวัตถุประสงค์เพื่อสรุปสาระสำคัญเพื่อนำไปสู่กรอบแนวคิดในการวิจัย โดยการวิเคราะห์ปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ใน ประเทศไทย โดยได้ศึกษาสาระสำคัญในประเด็นต่อไปนี้ 1) แนวคิด IT Risk และความสำคัญของ IT Risk 2) The Risk IT Framework 3) ความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบ IT และการบริหารจัดการความเสี่ยงที่เกิดขึ้น 4) IT Risk กับอุตสาหกรรมการเงินและการธนาคาร 5) ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร โดยมีสาระต่างๆที่สรุปได้ในแต่ละประเด็นดังนี้

1. แนวคิด IT Risk และความสำคัญของ IT Risk

Westerman and Hunter (2007) กล่าวไว้ว่ากว่า 50 ปีที่มีการนำเทคโนโลยีสารสนเทศมาใช้งานอย่างแพร่หลาย จำนวนองค์กรที่การทำงานต้องขึ้นอยู่กับเทคโนโลยีสนเทศมีจำนวนเพิ่มขึ้น เมื่อการใช้งานเพิ่มขึ้นความเสี่ยงที่เกิดจาการใช้งานระบบสารสนเทศก็เพิ่มขึ้นด้วย โดย Waterman and Hunter ได้ให้คำจำกัดความของ IT Risk ไว้ว่าคือ การเกิดเหตุการณ์ที่ไม่ได้คาดไว้ที่ทำให้เกิดความล้มเหลวของระบบสารสนเทศหรือการใช้งานที่ไม่ถูกต้องของระบบสารสนเทศที่ส่งผลคุกคามต่อองค์กร โดยความเสี่ยงนั้นไม่ได้ส่งผลอยู่เฉพาะในผ่าน IT หรือ ศูนย์ข้อมูลเท่านั้น แต่ส่งผลถึงผลการดำเนินงานทางธุรกิจขององค์กรนั้นอีกด้วย ทำให้การบริหารจัดการ IT Risk เป็นสิ่งจำเป็นที่ผู้บริหารระดับสูงต้องให้ความสำคัญ ในทำนองเดียวกัน K. Laudon and J. Laudon (2008) ได้ให้เหตุผลความอ่อนไหวต่อการถูกโจมตีและการใช้งานในทางที่ไม่ถูกต้องของระบบเทคโนโลยีสารสนเทศไว้ว่า ก่อนที่จะมีระบบเทคโนโลยีสารสนเทศที่ทำงานโดยอัตโนมัติ ข้อมูลต่างๆขององค์กรถูกเก็บและรักษาความปลอดภัยเป็นเอกสาร และเมื่อข้อมูลมีปริมาณมากถูกจัดเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ ข้อมูลเหล่านี้จะมีความอ่อนไหวต่อภัยคุกคามในรูปแบบต่างๆมากกว่าเมื่ออยู่ในรูปแบบกระดาษเอกสาร นอกจากนี้ระบบสารสนเทศสามารถเชื่อมโยงเข้าด้วยกันผ่านระบบเครือข่ายการสื่อสารความเป็นไปได้ในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้งานอย่างไม่ถูกต้องสามารถเกิดขึ้นจากจุดเชื่อมต่อใดๆบนระบบเครือข่ายก็ได จะเห็นได้ว่าระบบคอมพิวเตอร์มีบทบาทสำคัญอย่างมากในทางธุรกิจ หน่วยงานของรัฐ และในชีวิตประจำวันขององค์กร และเมื่อองค์กรได้เริ่มมาพึ่งพาระบบเทคโนโลยีสารสนเทศมากขึ้นในการหารายได้และการปฏิบัติงาน องค์กรเหล่านี้จำเป็นที่จะต้องมีมาตรการเพื่อให้แน่ใจว่าระบบเทคโนโลยีสารสนเทศของตนจะมีความพร้อมใช้อยู่เสมอ ไม่เกิดความล้มเหลวหรือเกิดช่วงเวลาที่ไม่สามารถใช้งานได้ (downtime) เพราะนั่นก่อให้เกิดความเสียหายไม่ว่าจะเป็นสร้างความไม่พอใจให้ลูกค้า การสูญเสียยอดขาย และไม่สามารถทำธุรกรรมที่มีความวิกฤติต่อการปฏิบัติงานภายในองค์กรได้

จากการศึกษาของ ISACA (2009) ยังพบว่า IT Risk ถือเป็นส่วนหนึ่งของความเสี่ยงในองค์กรนอกเหนือจาก ความเสี่ยงด้านกลยุทธ์, ความเสี่ยงด้านสิ่งแวดล้อม, ความเสี่ยงทางการตลาด, ความเสี่ยงด้านเครดิต, ความเสี่ยงด้านปฏิบัติการ และ ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับและกฎหมาย อย่างไรก็ตาม IT Risk ในหลายๆองค์กรยังถือเป็นส่วนหนึ่งในความเสี่ยงเหล่านี้ด้วย เป็นต้นว่า IT Risk เป็นส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการ อาจกล่าวได้ว่า IT Risk ก็คือ Business Risk ดังนั้นเป็นเรื่องจำเป็นที่ต้องสามารถระบุและบริหารจัดการ IT Risk ให้ดี มิฉะนั้นแล้วจะเกิดความเสียหายตามมา

2. The Risk IT Framework

ความเสี่ยงที่เกี่ยวข้องกับการใช้ IT นั้นเกิดขึ้นเสมอไม่ว่าจะมีการประเมินความเสี่ยงหรือไม่ดังนั้นองค์กรจำเป็นต้องมีกระบวนการ หรือกรอบโครงสร้างที่ใช้ในการบริหารจัดการความเสี่ยงที่เกิดขึ้น จากข้อมูลของ ISACA (2009) สามารถแบ่งโครงสร้างของ Risk IT Framework ได้เป็น 3 ส่วนหลัก คือ Risk Governance, Risk Response และ Risk Evaluation โดย Risk Governance เป็นส่วนที่มีความสำคัญมากที่สุด มีวัตถุประสงค์เพื่อให้การบริหารจัดการความเสี่ยงกลายเป็นส่วนหนึ่งของวัฒนธรรมองค์กร โดยเชื่อมโยงกับหลักการบริหารความเสี่ยงในองค์กร (Enterprise Risk Management) ทำให้ทุกคนในองค์กรตระหนักถึงความเสี่ยง (Risk Aware) โดยเฉพาะผู้บริหารระดับสูง ต้องให้การสนับสนุนในเรื่องการบริหารจัดการความเสี่ยงในภาพรวม ในส่วนที่สอง Risk Evaluation มีเพื่อกำหนด วิเคราะห์ และนำเสนอความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ โดยนำเสนอในภาษาที่เข้าใจง่ายแทนการนำเสนอในรูปแบบทางเทคนิค นั่นคือการนำเสนอผลประเมินความเสี่ยงให้ผู้เกี่ยวข้องได้รับรู้ในภาษาทางธุรกิจที่เข้าใจได้ง่ายและชัดเจน และในส่วนสุดท้ายคือ Risk Response มีวัตถุประสงค์เพื่อตอบสนองความเสี่ยง โดยการกำหนดค่า KPI (Key Risk Indicator) และจัดลำดับความสำคัญของความเสี่ยง กล่าวโดยสรุป การพัฒนา Risk IT Framework ของ ISACA เพื่อปิดช่องว่างระหว่างการบริหารความเสี่ยงในองค์กรและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศลง โดยให้มีการเชื่อมโยงเข้าด้วยกันเพื่อเกิดประสิทธิภาพในการบริหารจัดการความเสี่ยง

3. ความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบ IT และการบริหารจัดการความเสี่ยงที่เกิดขึ้น

IT Policy Compliance Group (2010) ได้ทำการศึกษาถึงความเสี่ยงที่เกี่ยวข้องกับการใช้ IT ที่เกิดขึ้น พบว่าในองค์กรที่มีแนวปฏิบัติที่ดีนั้นเกิดความเสี่ยงในเรื่องของข้อมูลที่สำคัญสูญหายหรือถูกขโมยถึง 85 % รองลงมาเป็น การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ต 70% การหยุดชะงักทางธุรกิจเนื่องมาจากเทคโนโลยีสารสนเทศ 61 % สูญเสียรายได้ ทรัพย์สิน 56% ต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ 42% และการขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน เทคโนโลยีสารสนเทศ 28% นอกจากนี้ ปริญญา หอมเอนก (2553) ยังกล่าวถึงปัญหาที่พบบ่อยจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรโดยแบ่งเป็นปัญหาใหญ่ๆดังนี้คือ การให้บริการขององค์กรหยุดชะงักในกรณีที่ระบบสารสนเทศเกิดปัญหาเช่นระบบล่ม, ความคุ้มค่าหรือคุณค่าที่รับกลับมาจากการลงทุนด้าน IT ว่าคุ้มค่าหรือไม่ การควบคุมการลงทุนเกี่ยวกับเทคโนโลยีสารสนเทศ, การควบคุมและบริหารจัดการระบบสารสนเทศ, การนำเทคโนโลยีสารสนเทศมาใช้แล้วไม่สอดคล้องกับการดำเนินธุรกิจขององค์กรและไม่สามารถตอบโจทย์ของผู้บริหารระดับสูง ผู้ใช้งานระบบสารสนเทศ ลูกค้าและผู้ถือหุ้น, กฎหมายและกฎข้อบังคับที่ทยอยออกมาบังคับใช้เช่นกฎหมายธุรกรรม, อิเล็คทรอนิกส์ และกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์, การป้องกันความปลอดภัยของข้อมูลและสารสนเทศที่จะส่งผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจขององค์กร

Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) กล่าวว่าเพื่อที่จะลดความเสี่ยงที่เกิดจากการใช้สารสนเทศในองค์กรจึงได้มีการพัฒนากรอบสำหรับการบูรณาการการบริหารจัดการความเสี่ยงเข้ากับ IT ซึ่งประกอบไปด้วย 4 องค์ประกอบที่สำคัญคือ การระบุความเสี่ยง(Risk Identification), การวิเคราะห์ความเสี่ยง(Risk Analysis), มาตรการการลดความเสี่ยง(Risk-reducing measures) และ การตรวจสอบติดตามความเสี่ยง(Risk Monitoring) ซึ่งความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศนั้นแบ่งออกได้หลายระดับดังนี้คือ ระดับ Application ในที่นี้คือความผิดพลาดทางเทคนิคหรือความล้มเหลวในการติดตั้งโปรแกรมหรือระบบสารสนเทศ ซึ่งอาจเกิดจากความเสี่ยงจากภัยธรรมชาติ, การกระทำของคู่แข่ง, จากแฮกเกอร์ และไวรัสคอมพิวเตอร์ ระดับที่สองคือระดับ Organization ซึ่งก็คือผลกระทบที่เกิดจากการใช้สารสนเทศต่อการทำงานทั่วทั้งองค์กร ตัวอย่างเช่นความเสี่ยงทางด้านกลยุทธ์เป็นต้นว่าการขาดความต่อเนื่องของ

การลงทุนทางด้าน IT และระดับ Interorganizational มีความเสี่ยงเกิดขึ้นจากการแลกเปลี่ยนเปลี่ยนข้อมูลระหว่างองค์กร

นอกจากนี้ Westerman and Hunter กล่าวว่าหลักสำคัญ 3 ประการในการบริหารจัดการความเสี่ยง อันได้แก่ Foundation คือระบบโครงสร้างพื้นฐานและเทคโนโลยีโปรแกรมประยุกต์ต่างๆรวมทั้งการกำหนดหน้าที่ความรับผิดชอบของบุคลากรและกระบวนการการทำงาน, Process นั่นก็คือการกำหนดมุมมองของความเสี่ยงระดับ enterprise level เพื่อให้ผู้บริหารระดับสูงสามารถลำดับความสำคัญและตัดสินใจจัดการกับความเสี่ยงได้อย่างเหมาะสม ขณะเดียวกันก็ยังให้โอกาสผู้บริหารระดับล่างสามารถที่จะบริหารจัดการความเสี่ยงส่วนของตนเองได้อิสระ, และ Awareness นั่นก็คือการสร้างวัฒนธรรมในองค์กรทำให้ทุกคนตระหนักและรับรู้ถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้น ซึ่งการบริหารจัดการความเสี่ยงผ่านทาง 3 องค์ประกอบที่กล่าวมาแล้วนั้นมีความสำคัญต่อทุกองค์กรมากโดยจะช่วยลดภัยคุกคามทางด้าน IT ขณะเดียวกันก็จะช่วยเพิ่มมูลค่าทางธุรกิจจากการใช้ IT อีกด้วย และเพื่อให้ IT Risk เป็นที่เข้าใจในทางธุรกิจจึงเกิดการพัฒนา 4A framework ขึ้นมาเป็นเครื่องมือในการบริหารจัดการ ความเสี่ยงที่เกิดจากการใช้ระบบสารสนเทศ อันประกอบไปด้วย Availability (การทำให้ระบบสามารถทำงานได้ตลอดรวมทั้งเวลาที่มีปัญหาขัดข้อง), Access (การเข้าถึงข้อมูลและระบบอย่างเหมาะสมเพื่อให้คนที่มีสิทธิเข้าถึงเท่านั้นที่เข้าระบบได้), Accuracy (ให้ข้อมูลที่มีความถูกต้องครบถ้วนตรงตามความต้องการของผู้บริหาร พนักงาน ลูกค้า คู่ค้า และผู้มีอำนาจควบคุม), Agility (ความรวดเร็วว่องไวในการแก้ไข ปรับตัวกับสถานการณ์ที่เกิดขึ้น) ด้วยการใช้ระเบียบข้อบังคับทั้ง 3 ข้อ อันได้แก่ Foundation, Process, และ Awareness จะช่วยทำให้การบริหารจัดการ 4A framework เกิดความสมบูรณ์ ช่วยให้สามารถบริหารความเสี่ยงที่เกิดจากการใช้สารสนเทศได้และยังช่วยให้ข้อมูลสำหรับการอภิปรายและการตัดสินใจในทุกระดับขององค์กร และที่สำคัญยังทำให้ผู้บริหารเกิดความมั่นใจ ซึ่งเมื่อผู้บริหารมั่นใจแล้วว่าอะไรที่เป็นความเสี่ยงที่สำคัญที่สุดก็จะทำให้กระบวนการในการตัดสินใจและบริหารจัดการความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล นวพร เรืองสกุล (2551) ยังได้เรียบเรียงไว้ว่าการควบคุมระบบสารสนเทศถือเป็นหนึ่งในแปดขององค์ประกอบที่เชื่อมโยงกันของการบริหารความเสี่ยงขององค์กร สารสนเทศจะต้องได้รับการระบุ จัดเก็บและนำไปสื่อสารในรูปแบบและกรอบเวลาที่เอื้อให้บุคลากรสามารถนำไปใช้ในการปฏิบัติหน้าที่ตามความรับผิดชอบได้ การดูแลรักษาให้สารสนเทศสอดคล้องกับความต้องการเป็นสิ่งสำคัญโดยเฉพาะเมื่อองค์กรต้องพบการเปลี่ยนแปลง คู่แข่งที่มีการเคลื่อนไหวอย่างรวดเร็ว หรือการเปลี่ยนแปลงในความต้องการของลูกค้า ซึ่งข้อมูลจะช่วยให้องค์กรตัดสินได้ว่าความเสี่ยงขององค์กรนั้นเป็นอย่างไร ช่วยให้ผู้บริหารเห็นภาพความเสี่ยงที่มีอยู่ในกระบวนการทำงานหรือหน่วยงาน ซึ่งระบบสารสนเทศทำให้หลายองค์กรมีความสามารถในการวัดและติดตามประเมินผลงานและนำเสนอข้อมูลเชิงวิเคราะห์ในระดับองค์กรได้ดีขึ้น ความซับซ้อนและการเชื่อมต่อของระบบยังคงดำเนินไปพร้อมๆกับการที่องค์กรต่างๆใช้ความสามารถในทางเทคโนโลยีใหม่ๆ ที่เกิดขึ้นให้เป็นประโยชน์ไปพร้อมๆกันอย่างไรก็ตามการพึ่งพาระบบสารสนเทศที่เพิ่มมากขึ้นเรื่อยๆย่อมนำมาซึ่งความเสี่ยงใหม่ๆ เช่นการฝ่าฝืนกฎระเบียบเกี่ยวกับความปลอดภัยของข้อมูลหรือ อาชญากรรมไซเบอร์ ซึ่งความเสี่ยงเหล่านี้จะต้องถูกผนวกเข้าไปในการบริหารความเสี่ยงขององค์กรด้วย

นอกจากหลักการบริหารจัดการความเสี่ยงที่กล่าวมา IT Policy Compliance Group(2008) ยังพบว่า บริษัทที่มีแนวทางการปฏิบัติที่เหมาะสมในเรื่องของ IT Governance, Risk, and Compliance- IT GRC จะช่วยให้ผลการดำเนินการทางธุรกิจดีขึ้น องค์กรที่มีการกำกับดูแล IT GRC ที่ดีกว่าจะมีสมรรถนะในการทำงานที่ดีกว่าองค์กรอื่นทั้งในด้านความพึงพอใจของลูกค้า การรักษาฐานลูกค้า และการเพิ่มขึ้นของรายได้และผลกำไร นอกจากนี้ยังช่วยลดความเสี่ยงที่เกิดจากระบบเทคโนโลยีสารสนเทศ โดยช่วยลดโอกาสจากข้อมูลลูกค้าสูญหายหรือถูกขโมยลงกว่า 50 เท่า และลดความเสียหายด้านการเงินอันเกิดจากข้อมูลลูกค้าสูญหายหรือถูกขโมย กว่า 96 เปอร์เซ็นต์

4. IT Risk กับ อุตสาหกรรมการเงินและการธนาคาร

ในปัจจุบันระบบเทคโนโลยีสารสนเทศ มีความจำเป็นสำหรับองค์กรในการดำเนินธุรกิจ ในอุตสาหกรรมการเงินการธนาคารก็เช่นกัน เพื่อที่จะสามารถแข่งขันกับคู่แข่งและเพิ่มขีดความสามารถในการขับเคลื่อนธุรกิจ จากที่ ISACA ระบุไว้ว่า IT Risk ในบริษัทการเงินนั้นถือเป็นส่วนหนึ่งในความเสี่ยงอื่นๆ ไม่ว่าจะเป็นความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านปฏิบัติการ หรือความเสี่ยงด้านเครดิต อีกทั้ง โครงสร้างหลักเทคโนโลยีสารสนเทศ (IT Infrastructure)ในปัจจุบัน ซึ่งตามคำจำกัดความของ K. Laudon and J. Laudon คือ ทรัพยากรเทคโนโลยีสารสนเทศที่ใช้ร่วมกันที่จะนำมาซึ่งโครงสร้างพื้นฐานสำหรับงานประยุกต์ระบบสารสนเทศเฉพาะตัวขององค์กรหนึ่งๆ โดยโครงสร้างหลักเทคโนโลยีสารสนเทศประกอบไปด้วย 7 ส่วนหลักที่จะต้องมีการประสานงานกันเพื่อประกอบการเป็นโครงสร้างหลักเทคโนโลยีสารสนเทศให้แก่องค์กรธุรกิจ ซึ่งประกอบไปด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต, และบริการที่ปรึกษาและการบูรณาการ โดยองค์กรในปัจจุบันสร้างโครงสร้างหลักเทคโนโลยีสารสนเทศด้วยการเลือกผสมผสานจากตัวแทนจำหน่าย คน และเทคโนโลยีจากหลายแหล่ง และทำให้ส่วนประกอบต่างๆสามารถทำงานร่วมกันได้เป็นระบบงานเดียวกันและเนื่องจากส่วนประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศถูกขับดันด้วยการสนับสนุนจากแหล่งที่มาต่างกันการทำให้ระบบสามารถทำงานร่วมกันเป็นหนึ่งเดียวจึงเป็นเรื่องที่ท้าทายความสามารถ องค์กรจำเป็นต้องบูรณาการข่าวสารที่ถูกจัดเก็บไว้ในโปรแกรมประยุกต์ต่างๆที่เก็บอยู่ในเครื่องต่างชนิดกัน เช่น โทรศัพท์, ระบบงานดั้งเดิม, อินทราเน็ต, อินเตอร์เน็ต, เว็บไซต์, PC, และอุปกรณ์มือถือต่างๆ ดังนั้นองค์กรธุรกิจต้องการโครงสร้างหลักเทคโนโลยีสารสนเทศที่มีความยืดหยุ่นที่สามารถทนทานปริมาณงานที่เพิ่มสูงอย่างมากและการโจมตีอย่างต่อเนื่องจากแฮกเกอร์และไวรัส เนื่องจากความต้องการของลูกค้าและพนักงานนั้นเพิ่มมากขึ้น และมีองค์ประกอบหลายอย่างที่จะมาขัดขวางการทำงานบนอินเตอร์เน็ตซึ่งถูกนำมาใช้ในการทำธุรกรรมมากมายโดยเฉพาะในธุรกิจการเงินและการธนาคาร โดยระบบเครือข่ายสาธารณะขนาดใหญ่อย่างอินเตอร์เน็ตนั้นความอ่อนไหวต่อการถูกโจมตีมาก จากการศึกษาของ Fheili (2011) ก็ยังช่วยยืนยันว่าธุรกิจการธนาคารนั้นมีการเปลี่ยนแปลงจากแบบดั้งเดิมที่ให้ลูกค้ามาเข้าคิวใช้บริการไปเป็นแบบสมัยใหม่ที่ลูกค้าสามารถเข้าถึงได้ทุกที่ทุกเวลาของการให้บริการ โดยอุตสาหกรรมการธนาคารถือเป็นหัวใจของการปฏิวัติทางด้าน IT โดยสารสนเทศจะเข้ามาช่วยในส่วนของการพัฒนาสินค้าและบริการ พัฒนาระบบโครงสร้างของธนาคารให้ดีขึ้น ซึ่งตรงนี้ส่งผลให้เกิดความเสี่ยงที่เกี่ยวข้องการใช้เทคโนโลยีสารสนเทศขึ้น

Aguilar (2011) มีความเห็นว่า บริษัทด้านการเงินจะต้องทำงานหนักขึ้นในเรื่องของ IT Risk ไม่ว่าจะเป็นการพัฒนากรอบความเสี่ยงที่ยอมรับได้ (Risk appetite framework) และสร้างโครงสร้างหลักเทคโนโลยีสารสนเทศ ในสภาวะที่มีวิกฤตทางการเงินเกิดขึ้น โดยเฉพาะในเรื่องความปลอดภัยของข้อมูลถือเป็นงานท้าทายสถาบันการเงินที่จะต้องทำ เช่นเดียวกันกับการศึกษาของ Reinhold, Doherty, Higgins (2011) ที่กล่าวไว้อย่างสอดคล้องว่า ในภาวะที่ต้องเผชิญกับวิกฤตทางการเงินสถาบันเงินต่างๆได้พัฒนากรอบของระดับความเสี่ยงที่องค์กรยอมรับได้และสร้างโครงสร้างพื้นฐานของระบบสารสนเทศ โดยเฉพาะความเสี่ยงทางด้านข้อมูล ดังนั้นสถาบันการเงินจะต้องกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้อย่างชัดเจนและต้องคอยติดตามความเสี่ยงนั้นอย่างมีประสิทธิภาพผ่านการเข้าถึงสารสนเทศที่ที่ถูกต้อง เชื่อถือได้ นอกจากนี้ทั้ง กรอบของระดับความเสี่ยงที่องค์กรยอมรับได้และโครงสร้างพื้นฐานของระบบสารสนเทศ ยังมีความสัมพันธ์กัน ซึ่งผู้บริหารระดับสูงจำเป็นต้องพิจารณาหรือประเมินการบริหารความเสี่ยงนี้อย่างดีและยังต้องมองอนาคตข้างหน้าของกลยุทธ์ทางธุรกิจด้วย ความเข้มแข็งและความมีพลังของผู้บริหารระดับสูงมีความสำคัญมากในการที่จะแสดงให้เห็นถึงความสำคัญของกรอบของระดับความเสี่ยงที่องค์กรยอมรับได้และความเสี่ยงทางด้านข้อมูลนั้นสามารถส่งผลกระทบต่อองค์กรได้

ในประเทศไทยเองนั้นบริษัทหลักทรัพย์ได้มีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการประกอบธุรกิจอย่างกว้างขวางซึ่งอาจก่อให้เกิดความเสี่ยงต่อบริษัทหลักทรัพย์ได้ เพื่อที่จะควบคุมความเสี่ยงที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศให้กับบริษัทหลักทรัพย์อ้างอิงจากประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และได้ออกข้อบังคับ และ แนวทางการปฏิบัติด้านเทคโนโลยีสารสนเทศขึ้นเพื่อควบคุมการปฏิบัติงาน และ รักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพและมาตรฐานในระดับเดียวกัน ซึ่งถ้าบริษัทหลักทรัพย์สามารถปฏิบัติตามได้จะสามารถควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพมากขึ้น โดยสาระสำคัญของแนวทางปฏิบัติมีเนื้อหาครอบคลุม 1) นโยบายรักษาความปลอดภัย 2) การแบ่งแยกอำนาจหน้าที่ 3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย 4) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย 5) การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ 6) การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน 7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ 8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

5. ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร

เท่าที่สำรวจดูจากเอกสารที่มีอยู่อาจพูดได้ว่ายังไม่มีการศึกษาใดในประเทศไทยที่พยายามสำรวจปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ ส่วนใหญ่จะเป็นการศึกษาของต่างประเทศและทำการศึกษาในองค์กรธุรกิจทั่วไปไม่ใช่ในบริษัทหลักทรัพย์ จากการค้นคว้าสามารถสรุปปัจจัยที่มีผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศใช้ในองค์กรได้ดังนี้

ปัจจัยที่1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ

จากการศึกษารายงานประจำปี IT Governance, Risk and Compliance - Improving Business Results and mitigating Financial risk ของ IT Policy Compliance Group (2008) พบว่าคณะกรรมการที่กำกับดูแลระบบเทคโนโลยีสารสนเทศควรประกอบไปด้วยผู้บริหารระดับสูงและสมาชิกจากฝ่ายทางธุรกิจ การเงิน กฎหมาย IT การกำกับดูแล และการตรวจสอบภายใน นอกจากนี้งานวิจัย นอกจากนี้งานวิจัยอีกชิ้นหนึ่ง เรื่อง What Color is Your Information Risk -Today? ของ IT Policy Compliance Group (2010) แสดงว่าผู้มีส่วนเกี่ยวข้องในการบริหารจัดการความเสี่ยงเพื่อให้ได้ผลลัพธ์ที่ดีควรประกอบไปด้วยบุคคลต่างๆจากหลายแผนก ดังนี้ ผู้จัดการฝ่าย IT ผู้ตรวจสอบภายใน, ผู้บริหารระดับสูง (CEO, COO), ผู้จัดการฝ่ายธุรกิจต่างๆ, ผู้จัดการฝ่ายกำกับดูแลความเสี่ยง, ผู้จัดการฝ่ายความปลอดภัยของระบบสารสนเทศ (CISO, CSO) และผู้จัดการฝ่ายกฎหมาย งานเรื่อง How the Master of IT Deliver More Value and Less Risk ของ IT Policy Compliance Group (2010) อีกชิ้นหนึ่งก็ได้ยืนยันในลักษณะเดียวกันว่าบุคคลที่เกี่ยวข้องในการบริหารจัดการคุณค่า ความเสี่ยงและกำกับดูแลสำหรับ ITเพื่อให้ได้ผลลัพธ์ในการดำเนินงานที่ดีหัวหน้าระดับสูงและผู้จัดการจากแผนกต่างๆก็ควรจะต้องมีบทบาทรับผิดชอบตรงนี้ด้วยซึ่งประกอบไปด้วย ผู้จัดการผ่าย IT ผู้จัดการฝ่ายกฎหมายและกำกับดูแลการทำงาน ผู้จัดการธุรกิจฝ่ายต่างๆ ผู้ตรวจสอบภายใน และผู้จัดการงานบริหารความเสี่ยง และจากศึกษาของ ISACA(2009) ก็แสดงผลสอดคล้องกันว่า ผู้บริหารระดับสูงจะต้องเข้ามามีส่วนร่วมและไม่มองว่า IT Risk เป็นงานของฝ่ายเทคโนโลยีสารสนเทศหรือเป็นเรื่องทางเทคนิคอย่างเดียว

ปัจจัยที่ 2 การควบคุมความปลอดภัยของงานสารสนเทศ

การควบคุมความปลอดภัยของระบบสารสนเทศคือการนำวิธีการหรือเทคนิคต่างๆมาใช้ในการป้องกันและรักษาความปลอดภัยหรือลดความเสี่ยง ความเสียหายที่จะเกิดกับทรัพย์สินในระบบสารสนเทศสามารถแบ่งได้เป็น

1. การควบคุมความปลอดภัยทางด้านกายภาพ ซึ่งมีวัตถุประสงค์เพื่อป้องกันจุดอ่อนของระบบสารสนเทศ ให้แน่ใจว่าทรัพย์สินในระบบจะปลอดภัยรอดพ้นจากอันตรายต่างๆ หรือ ภาวะฉุกเฉิน เช่น ไฟไหม้ น้ำท่วม และเป็นการจำกัดการเข้าถึงระบบสารสนเทศ โดยสามารถแบ่งการควบคุมได้ดังนี้
   1.1 การควบคุมเพื่อป้องกันความเสียหายที่เกิดจากอัคคีภัย ซึ่งมีวิธีการควบคุมดังนี้ การมีระบบแจ้งเตือนภัย, การมีอุปกรณ์ฉีดดับเพลิง เช่น น้ำ, สารคาร์บอนไดออกไซด์, หรือ แก๊ซฮาลอน, การมีแผนผังแสดงจุดที่ตั้งของระบบดับเพลิง, ตึกที่เป็นที่ตั้งอุปกรณ์และทรัพย์สินใช้อุปกรณ์กันไฟและโครงสร้างตึกกันไฟ, การมีสัญญาณเตือนภัยเชื่อมต่อยังสถานีดับเพลิง, อุปกรณ์เชื้อไฟเช่น กระดาษควรเก็บในห้องแยก, สายไฟมีฉนวนหุ้มป้องกัน และ การจัดให้มีการฝึกซ้อมระบบป้องกันอัคคีภัย
   1.2 การควบคุมเพื่อป้องกันความเสียหายที่เกิดจากน้ำ ซึ่งมีวิธีการควบคุมดังนี้ การมีหลังคา ผนัง พื้น ป้องกันการรั่วซึมมีทางระบายน้ำที่เหมาะสม, การมีการติดตั้งสัญญาณเตือนภัยเชื่อมต่อกับเครื่องตรวจจับ (water sensor), เก็บทรัพย์สินระบบสารสนเทศอยู่ในชั้นที่น้ำท่วมไม่ถึง และ การมีข้อห้ามพนักงานนำเครื่องดื่มเข้าใกล้คอมพิวเตอร์และอุปกรณ์
   1.3 การควบคุมเพื่อป้องกันความเสียหายที่เกิดจากระบบไฟฟ้าขัดข้อง ซึ่งมีวิธีการควบคุมดังนี้ มีการติดตั้งอุปกรณ์ตัดไฟ (circuit breaker) หรือ อุปกรณ์ควบคุมแรงดันกระแสไฟ (voltage regulator) และการมีอุปกรณ์สำรองไฟหรือ UPS
   1.4 การควบคุมเพื่อป้องกันความเสียหายที่เกิดจากฝุ่น ซึ่งมีวิธีการควบคุมดังนี้ มีการดูดฝุ่นอยู่เสมอและการมีพื้นห้องและพรมแบบกันฝุ่น
   1.5 การควบคุมเพื่อป้องกันความเสียหายที่เกิดจากผู้บุกรุกที่ไม่ได้รับอนุญาต ซึ่งมีวิธีการควบคุมดังนี้ การมีศูนย์คอมพิวเตอร์มีประตูแข็งแรงและมีสัญญาณเตือนภัย, การมีการจำกัดการเข้าออก และการเก็บดิสก์หรือเทปที่บันทึกข้อมูลเข้าตู้ล็อกกุญแจ
2. การควบคุมความปลอดภัยทางด้านตรรกะมีวัตถุประสงค์ เพื่อป้องกันไม่ให้ ซอฟต์แวร์ และข้อมูลถูกทำลายหรือแก้ไขเปลี่ยนแปลง เพื่อรักษาความลับของข้อมูล เพื่อให้ซอฟต์แวร์มีความปลอดภัยทำให้ธุรกิจดำเนินการได้อย่างต่อเนื่อง เพื่อสร้างความมั่นใจว่าผู้ที่เข้าสู่ระบบเป็นผู้ที่ได้รับอนุญาต แล้วเพื่อสร้างความน่าเชื่อถือของระบบให้กับองค์กร โดยสามารถแบ่งการควบคุมได้ดังนี้
   2.1 การควบคุมการเข้าถึงระบบสารสนเทศ ซึ่งมีวิธีการควบคุมดังนี้ การมีการระบุผู้ใช้และพิสูจน์ผู้ใช้ที่แท้จริง, การมีการกำหนดนโยบายการใช้ password เช่น ไม่อนุญาตให้ใช้รหัสผ่านที่มีลักษณะมีจุดอ่อน, การมีการกำหนดสิทธิอำนาจการใช้งานของผู้ใช้แต่ละคน, มีการบันทึกข้อมูลการใช้งาน เช่นเก็บข้อมูล Log File, การมีระเบียบกำหนดเกี่ยวกับการให้ เปลี่ยนแปลง และยกเลิกรหัสผู้ใช้
   2.2 การควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์ม ซึ่งมีวิธีการควบคุมดังนี้ มีการป้องกันไวรัส, มีการตรวจหาไวรัสอย่างสม่ำเสมอ, มีการแก้ไขเมื่อตรวจเจอ, มีการให้ความรู้แก่ผู้ใช้เกี่ยวกับอันตรายของไวรัสและการป้องกัน, แต่ละหน่วยงานร่วมกันกำหนดวิธีการควบคุมการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ในเครือข่าย เช่น การเข้ารหัสข้อมูลตั้งแต่จุดเริ่มต้นถึงปลายทาง (end-to-end encryption)

3. การควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ โดยสามารถแบ่งการควบคุมได้ดังนี้

a. มีแผนในการฟื้นสภาพระบบจากภัยพิบัติ (Disaster Recovery plan) ซึ่งประกอบได้ด้วย แผนฉุกเฉิน (Emergency plan), แผนสำรอง (Backup plan), แผนฟื้นสภาพ (Recovery plan) และแผนทดสอบ (Test plan)

b. มีการทำประกันภัย ซึ่งประกอบได้ด้วย การทำประกันอุปกรณ์ฮาร์ดแวร์, การทำประกันที่เก็บสื่อ, การทำประกันความหยุดชะงักทางธุรกิจ และการทำประกันเอกสารสำคัญ (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2545)

การศึกษาของ IT Policy Compliance Group (2010) เรื่อง What Color is Your Information Risk -Today? พบว่าการควบคุมความปลอดภัยของสารสนเทศ จะช่วยป้องกันการรั่วไหลของข้อมูลที่สำคัญได้ ด้วยการกำหนดและจัดกลุ่มข้อมูลที่สำคัญ, ระบุถึงเครื่องมืออุปกรณ์ที่เข้าถึงข้อมูลที่สำคัญ, มีการดูแลบำรุงรักษาข้อมูลที่สำคัญและอุปกรณ์เครื่องมือในการเข้าถึง, มีการตรวจจับและป้องกันการรั่วไหลของข้อมูล และการควบคุมความปลอดภัยในการใช้ข้อมูลที่สำคัญบนเครื่อง PC และบนเครื่องคอมพิวเตอร์พกพาต่างๆ ในทำนองเดียวกันจากงานศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) พบว่าการมีนโยบายหรือแผนควบคุมความปลอดภัยของงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ โดยการมีแผนการฟื้นสภาพของระบบจากภัยพิบัติ (DRP), การควบคุมความเสี่ยงจากภัยธรรมชาติ, จากผู้บุกรุกที่ไม่ได้รับอนุญาต, การควบคุมการเข้าถึงระบบสารสนเทศ, การควบคุมความปลอดภัยของข้อมูล, การควบคุมและการป้องกันไวรัสคอมพิวเตอร์จะช่วยลด IT Risk ได้

ปัจจัยที่ 3 งบประมาณ

จากงานศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) แสดงว่าถึงแม้จะมีการลงทุนทางด้านสารสนเทศเพิ่มขึ้นแต่ผลลัพธ์ที่ได้อาจต้องเผชิญกับความเสี่ยงจากความล้มเหลวของการใช้สารสนเทศ นอกจากนี้งานของ IT Policy Compliance Group เรื่อง How the Master of IT Deliver More Value and Less Risk พบว่าสภาพเศรษฐกิจส่งผลกระทบต่องบประมาณทางด้าน IT ในประเทศสหรัฐอเมริกา โดยมีแนวโน้มลดลงอันเป็นผลมาจากรายได้และผลกำไรที่ลดลง แต่อย่างไรก็ตาม การใช้งบประมาณทางด้าน IT ความปลอดภัยของข้อมูล และการตรวจสอบมีผลโดยตรงต่อผลลัพธ์การดำเนินงาน คือถ้าต้องการผลลัพธ์ที่ดีเยี่ยมการใช้งบประมาณก็ต้องสูงขึ้นด้วยถ้าใช้งบประมาณในส่วนของ IT ความปลอดภัยและการตรวจสอบน้อย ความเสี่ยงในเรื่องของการหยุดชะงักทางธุรกิจ การสูญหายของข้อมูลหรือโดนขโมยและปัญหาในตรวจสอบก็จะมากขึ้นด้วย และงานวิจัยอีกชิ้นหนึ่งของ IT Policy Compliance Group (2011) เรื่อง How High Performance Organization Manage IT พบว่าองค์กรที่มีการใช้งบประมาณสูงกว่าโดยเฉพาะการใช้งบประมาณทางด้าน IT , งบประมาณในการตรวจสอบและงบประมาณในการรักษาความปลอดภัยของข้อมูลจะมีผลลัพธ์ที่ดีกว่าในเรื่องของการลดความเสี่ยง โดยสามารถสรุปความสัมพันธ์ในการใช้งบประมาณกับขนาดขององค์กรและผลลัพธ์ได้ดังนี้ 1) การใช้งบประมาณทางด้าน IT และ ด้านการรักษาความปลอดภัย ควรเพิ่มขึ้นในทุกขนาดขององค์กร 2) การใช้งบประมาณในด้านการตรวจสอบควรเพิ่มขึ้นในองค์กรขนาดเล็กและขนาดกลาง โดยสามารถลดลงได้ในองค์กรขนาดใหญ่ 3) ถ้าต้องการผลลัพธ์ที่ดีการใช้งบประมาณด้าน IT ด้านการรักษาความปลอดภัยและการตรวจสอบควรเพิ่มขึ้น

ในส่วนของวัตถุประสงค์ของการใช้งบประมาณทางด้าน IT จากการศึกษาของ Fheili (2011) สามารถแบ่งในส่วนของการใช้งบประมาณไปกับ IT ได้เป็น 3 ประเภทคือใช้เพื่อให้ขับเคลื่อนองค์กร, ใช้เพื่อเปลี่ยนองค์กรและใช้เพื่อสร้างนวัตกรรมใหม่ๆให้กับองค์กร ซึ่งแต่ละประเภทก็จะเรื่องที่ต้องระมัดระวังเพื่อได้บรรลุตามเป้าหมายที่วางไว้

ปัจจัยที่ 4 เครื่องมือที่ใช้ในการบริหารจัดการความเสี่ยง

ดังที่การศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) กล่าวไว้ว่าการบริหารจัดการความเสี่ยงที่ดี ตามขั้นตอน Risk identification, Risk Analysis, Risk-reducing measures, และ Risk monitoring จะเป็นการป้องกันทรัพย์สินทางด้าน IT เป็นต้นว่าข้อมูล, ฮาร์ดแวร์, ซอฟต์แวร์, บุคลากร และ สิ่งอำนวยความสะดวกต่างๆจากการคุกคาม ภัยธรรมชาติ, ความผิดพลาดทางเทคนิค, การก่อวินาศกรรม, การเข้าถึงระบบโดยไม่ได้รับอนุญาต 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 ในขณะที่จากการสำรวจองค์กรที่อยู่ในอุตสาหกรรมทางการเงินทั่วโลก ของ Ernst & Young (2008) พบว่าเครื่องมือที่ใช้คือ COBIT, ITIL, ISO17799, SOX, COSO ตามลำดับ

มาตรฐาน ISO 27001 จะมุ่งเน้นการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรโดยจะกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมาคงปลอดภัยหรือ Information Security Management ให้กับองค์กร นอกจากนี้มาตรฐาน ISO 27001 ยังประกอบไปด้วยวงจรการจัดการความมั่นคงปลอดภัยคามขั้นตอน P-D-C-A (Plan-Do-Check-Act) และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีหรือมาตรการเพื่อป้องกัน ลดความเสี่ยงและรักษาทรัพย์สินที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

มาตรฐาน ISO 17799 เป็นมาตรฐานที่กล่าวถึงวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้นซึ่งจะต้องเป็นไปตามข้อกำหนดมาตรฐาน ISO 27001 โดยจะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบและให้แนวทางผู้จัดทำว่าควรปฏิบัติอย่างไรซึ่งประกอบไปด้วย 11 โดเมนดังนี้ 1) นโยบายการรักษาความปลอดภัย (Security Policy) 2) การจัดโครงสร้างระบบการรักษาความปลอดภัยขององค์กร (Organization Information Security) 3) การจัดการทรัพย์สิน (Asset Management) 4) การรักษาความปลอดภัยในระดับบุคลากร (Human Resource Security) 5) การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security) 6) การสื่อสารและการบริหารการปฏิบัติงาน (Communications and Operations Management) 7) การควบคุมการเข้าถึงระบบ (Access Control) 8) การดูแลและพัฒนาระบบ (Information System acquisition, development and maintenance) 9) การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย (Information security incident management) 10) การบริหารความต่อเนื่องทางธุรกิจ(Business Continuity Management) 11) การปฏิบัติตามข้อกำหนด(Compliance) (วชิราพร ปัญญาพินิจนุกุกุร. 2552 และ ThaiCERT, NECTEC. 2007)

COBIT เป็นหลักการที่ต้องการให้เกิดการบรรลุเป้าหมายระดับองค์กร (Enterprise Goals) ที่กำหนดไว้ โดยอาศัยปัจจัยบ่อเกิด(Enables) 7 ปัจจัยคือ 1) กระบวนการ (Process) 2) วัฒนธรรม จริยธรรมและความประพฤติ (Culture, ethics, behavior) 3) โครงสร้างบุคลากร(Organizational structure) 4) ข้อมูล(Information) 5) หลักการและนโยบายองค์กร (Principle and policies) 6) ทักษะ ความรู้ และความสามารถของบุคลากร (Skills and completeness) และ 7) โครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service capabilities) เพื่อทำให้เป้าหมายที่กำหนดไว้สามารถบรรลุได้ โดยปัจจัยบ่อเกิดเหล่านี้ต้องทำงานผสานกันหรือร่วมกัน (บรรจง หะรังสี, ภัทราวดี เหมทานนท์. 2555)

ITIL (IT Infrastructure Library) Framework เป็นมาตรฐานปฏิบัติการจัดการบริการด้านเทคโนโลยีสารสนเทศซึ่งการบริหารงานบริการด้านเทคโนโลยีสารสนเทศก็คือบริการด้านเทคโนโลยีสารสนเทศ (IT Service) เป็นกลุ่มของงานด้านเทคโนโลยีสารสนเทศที่ตอบสนองต่อธุรกิจ, โครงสร้าง IT พื้นฐาน (IT Infrastructure) และการจัดการบริการด้านเทคโนโลยี

สารสนเทศ (IT Service Management) เป็นการวิเคราะห์ วางแผน การนำระบบไปใช้ และการควบคุมงานด้านงานบริการสารสนเทศภายใต้โครงสร้างสารสนเทศ โดยจะช่วยเพิ่มประสิทธิภาพด้านคุณภาพในการดำเนินงานอย่างต่อเนื่องของบริการ IT ช่วยลดมูลค่าการลงทุนระยะยาว ช่วยลดความเสี่ยงของการดำเนินงาน ทำให้การสื่อสารระหว่าง IT และธุรกิจมีประสิทธิภาพ (ศูนย์ศึกษาและพัฒนาเทคโนโลยีทรัพยากรบุคคลมหาวิทยาลัยเกษตรศาสตร์. 2552) โดย ITIL จะเป็นองค์ความรู้ หลักการที่กล่าวถึงกระบวนการบริหารจัดการงานบริการเทคโนโลยีสารสนเทศโดยที่จะเน้นว่าควรทำอะไรบ้างเป็นการใช้แนวปฏิบัติจากมาตรฐาน ISO/IEC20000 มาประยุกต์ใช้ในกระบวนการเป็นต้นว่า Change management, Capacity management และ Incident management (ปริญญา หอมเอนก. 2551)

IT Portfolio Management แนวคิดที่จะเน้นการใช้ทรัพยากรที่มีอยู่เพื่อให้เกิดมูลค่าสูงสุดผ่านการประเมินการใช้อย่างเหมาะสมและการคัดเลือกโครงงาน โดยการตัดสิ่งที่ซ้ำซ้อนออกไป ประกอบด้วย 3 portfolio คือ Application portfolio, Project Portfolio และ Resource portfolio management(RPM) (Gawenda. 2008)

SOX (Sarbanes-Oxley Act) ถูกบัญญัติขึ้นเพื่อใช้จัดการกับทุจริตในบริษัททำให้มั่นใจในบูรณภาพของข้อมูลการเงินของบริษัทและการจัดการด้านธรรมาภิบาลองค์กร (บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูล) ซึ่งกฎหมาย Sarbanes-Oxley Act 2002 ฉบับนี้มุ่งเน้นที่การปรับปรุง ระบบการควบคุมภายในของบริษัทต่างๆอย่างแท้จริง โดยกำหนดให้ CEOs และ CFOs ของบริษัทแต่ละแห่งต้องประเมินและรายงานต่อสาธารณชนให้เห็นชัดเจนว่าการควบคุมภายในทางด้านรายงานการเงินของบริษัทนั้นมีประสิทธิภาพแค่ไหน ในประเทศไทยตลาดหลักทรัพย์แห่งประเทศไทยได้ออกกฎหมายให้บริษัทจดทะเบียนทุกแห่งต้องรายงานเกี่ยวกับความมีประสิทธิภาพและประสิทธิผลของการควบคุมภายในในรายงานประจำปีให้ประธานคณะกรรมการตรวจสอบเป็นผู้ลงนามรับรองรายงาน (ประชาติธุรกิจ. 2546)

COSO (Committee of Sponsoring Organization) คือกรอบควบคุมความเสี่ยงซึ่งการพัฒนาแบบจำลอง COSO นั้นต้องเข้าใจความหมายของการควบคุมภายใน (Internal Control) จึงเป็นวิธีการที่จะช่วยให้องค์กรบรรลุผลสำเร็จ เป็นกระบวนการที่เกิดขึ้นโดยคณะกรรมการบริหาร ผู้บริหาร และทุกคนในองค์กรออกแบบมาเพื่อเป็นการประกันการบรรลุวัตถุประสงค์ขององค์กรในด้านต่างๆดังนี้ 1) ประสิทธิผลและประสิทธิภาพของการดำเนินงาน 2) ความน่าเชื่อถือของรายงานการเงิน 3) การปฏิบัติตามกฎหมาย กฎระเบียบ โดย 5 องค์ประกอบของการควบคุมภายในคือ

1. สภาพแวดล้อมของการควบคุม (Control Environment) เนื่องจากสภาพแวดล้อมการทำงานเป็นสิ่งที่มีความสำคัญในการบริหารธุรกิจ จึงควรจัดสภาพแวดล้อมให้เหมาะสมกับการปฏิบัติงาน
2. การประเมินความเสี่ยง (Risk Assessment) เป็นการตระหนักถึงและจัดการกับความเสี่ยงที่องค์กรต้องเผชิญโดยต้องมีการกำหนดวัตถุประสงค์ที่บูรณาการขององค์กรเช่น การขาย การผลิต การตลาด การเงินเข้ากับกิจกรรมอื่นโดยองค์กรต้องวิเคราะห์ ประเมินผลและบริหารความเสี่ยงที่เผชิญทั้งปัจจุบันและอนาคตในทุกมุมมอง ทุกระดับ
3. กิจกรรมการควบคุม (Control Activities) เป็นการพิจารณากำหนดนโยบายและกระบวนการควบคุมให้รอบคอบว่าสิ่งที่กำหนดขึ้นมานั้นสามารถช่วยให้องค์กรบรรลุผลสำเร็จได้อย่างมีประสิทธิภาพ
4. ข้อมูลสารสนเทศและการสื่อสาร (Information and Communication) เป็นการเน้นการส่งข่าวและความเข้าใจร่วมในองค์กรสำหรับกิจกรรมและระเบียบต่างๆให้เข้าใจตรงกันตามความรับผิดชอบในแต่ละระดับชั้นในเวลาที่เหมาะสม
5. การติดตาม/การสอดส่องดูแล (Monitoring) ระบบการควบคุมต้องมีการติดตามและดัดแปลงรวมทั้งการตรวจสอบให้เหมาะสม โดยระบบการควบคุมภายในทุกระดับของฝ่ายในองค์กรต้องมีการสอดส่องดูแลอย่าง

ใกล้ชิดและมีการประเมินคุณภาพเป็นระยะทำได้โดยการสอดส่องและประเมินผลตลอดเวลาทุกขั้นตอนการทำงาน (ปริญญา หอมเอนก. 2556)

Balanced Scorecard เป็นกลยุทธ์ในการบริหารงานเพื่อที่ผู้บริหารขององค์กรจะได้รับทราบจุดอ่อนและความไม่ชัดเจนของการบริหารงาน โดยจะกำหนดวิสัยทัศน์ และแผนกลยุทธ์แล้วแปลผลลงไปสู่ทุกจุดขององค์กรเพื่อใช้เป็นแนวทางในการดำเนินงานของแต่ละฝ่าย โดยมีเป้าหมาย 4 ด้าน คือ มุมมองด้านการเงิน (Financial Perspective) มุมมองด้านลูกค้า (Customer Perspective) มุมมองด้านกระบวนการภายใน (Internal Process Perspective) และมุมมองด้านการเรียนรู้และการพัฒนา (Learning and Growth Perspective) (พสุ เตชะรินทร์. 2545)

CIS benchmarks (Center for internet security) มาตรฐานที่จัดทำโดยศูนย์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นแนวทางปฏิบัติที่ดีทางด้านการปรับแต่งค่า configuration ด้านการรักษาความปลอดภัย เป็นมาตรฐานที่ได้รับการพัฒนาและยอมรับร่วมกันจากทั้งองค์กรภาครัฐ ภาคธุรกิจ ภาคอุตสาหกรรม และภาคการศึกษา ซึ่งการวัดค่า benchmarks นี้ เป็นกฎ/หลักชี้นำ ที่ใช้ควบคุมทางเทคนิคเพื่อเสริมสร้างความแข็งแรงด้านความปลอดภัยให้กับระบบปฏิบัติการ, ซอฟต์แวร์สื่อกลางระหว่างผู้ใช้กับโปรแกรมต่างๆ, โปรแกรมประยุกต์ทางคอมพิวเตอร์ และ อุปกรณ์เครือข่าย สิ่งที่ CIS benchmarks มีดีเหนือคู่แข่งเป็นเพราะว่าได้มีการจัดทำท่ามกลางฉันทามติของผู้เชี่ยวชาญทางด้านความปลอดภัยทั่วโลก (Center for internet security)

ปัจจัยที่ 5 ขนาดขององค์กร

จากการศึกษาเรื่อง How the Master of IT Deliver More Value and Less Risk ของ IT Policy Compliance Group (2010) พบว่าบริษัทที่มีขนาดเล็ก (วัดจากผลประกอบการทั้งปี)ส่วนใหญ่ จะเผชิญกับปัญหาของการหยุดชะงักทางธุรกิจอันเกิดมาจาการใช้ระบบสารสนเทศ, ปัญหาในการตรวจสอบ และการสูญหายและถูกขโมยของข้อมูล ซึ่งบริษัทขนาดเล็กเหล่านี้เป็นบริษัทที่ลดค่าใช้จ่ายทางด้าน IT ในทางกลับกันบริษัทที่มีขนาดกลางและขนาดใหญ่จะพบกับปัญหาเหล่านี้น้อยกว่าโดยบริษัทขนาดใหญ่จะพบน้อยที่สุด

ปัจจัยที่ 6 การสื่อสารในเรื่องของความเสี่ยง

การสื่อสารถือเป็นส่วนหนึ่งของระบบสารสนเทศ บุคลากรต้องสามารถสื่อสารสารสนเทศที่เกี่ยวกับความเสี่ยงข้ามหน่วยงานได้ รวมทั้งไปตามสายบังคับบัญชา ซึ่งจำเป็นต้องมีการสื่อสารที่เหมาะสม แบบเปิดเผย ตรงไปตรงมา จากการเรียบเรียงของ นวพร เรืองสกุล (2553) พบว่าวิธีการสื่อสารอาจมาได้หลายรูปแบบเช่นในรูปของคู่มือนโยบาย บันทึกจดหมายอิเล็กทรอนิกส์ บอร์ดติประกาศ ประกาศเตือน การสื่อสารทางเว็บ การสื่อสารด้วยวาจา งานวิจัยของ IT Policy Compliance Group (2010) เรื่อง How the Master of IT Deliver More Value and Less Risk ยังพบว่า การสื่อสารและการแบ่งปันของมูลเกี่ยวกับคุณค่า ความเสี่ยงและการกำกับดูแลที่เกี่ยวกับการใช้ IT เพื่อให้ได้ผลลัพธ์ที่ดีควรจะใช้วิธีต่างๆ ดังนี้ Email, การพูดจา, dashboard และ scorecard, รายงานและข้อสรุปที่ได้จากฐานข้อมูล โดยการใช้เพียงการโทรศัพท์ Email และเอกสารอีเลกทรอนิกส์ แล้วเน้นการแจ้งเฉพาะเวลามีเหตุร้ายนั้นจะทำให้ผลลัพธ์ที่ออกมาไม่ดี

ปัจจัยที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศ

รูปแบบของการจัดโครงสร้างแผนก IT ภายในองค์กร สามารถแบ่งได้เป็น 3 โครงสร้างหลักคือ 1) Centralization คือการรวมศูนย์ทรัพยากรที่เกี่ยวข้องกับ IT ทั้งหมดมาที่ส่วนกลาง 2) Decentralization คือแบบกระจายศูนย์ โดยในแผนกต่างๆมี IT เป็นผู้ดูแลในหน่วยงานของตน และ 3) Federalism คือการผสมผสาน ระหว่าง Centralization และ

Decentralization เข้าด้วยกัน (Luftman and Bullen. 2004) โดยแบบรวมศูนย์ (Centralization) ทำให้การควบคุมจากฝ่ายบริหารระดับสูงในงานด้านเทคโนโลยีสารสนเทศเป็นไปโดยอัตโนมัติ การใช้งานด้านฮาร์ดแวร์ ซอฟต์แวร์ และบุคลากรเป็นอย่างประหยัด และแบบกระจายศูนย์(Decentralization) จะช่วยปรับปรุงความสามารถขององค์กรเนื่องจากมีกระจายโอกาสในการใช้งานด้านระบบสารสนเทศออกไป และช่วยลดค่าใช้จ่ายในการติดต่อสื่อสารเกี่ยวกับกิจกรรมด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามแบบกระจายศูนย์นั้นอาจเกิดปัญหาในการควบคุมมาตรฐานส่งผลให้ประสิทธิภาพและประสิทธิผลของการทำงานระบบสารสนเทศอาจต่ำกว่าที่คาดไว้ รวมถึงการรักษาทรัพย์สินและความปลอดภัยของข้อมูลอาจได้รับผลกระทบได้ (มหาวิทยาลัยสุโขทัยธรรมาธิราช. 2545) ซึ่งจากการศึกษาของ Co and Fink (2010) พบว่าโครงสร้างแบบ Decentralization จะมีความเสี่ยงสูงกว่าเนื่องจากการควบคุม IT เป็นไปได้ยาก ในขณะที่องค์กรที่ใช้แบบ Federalism ต้องการมีการบริหารจัดการ IT ที่ดี ต้องการได้รับประโยชน์และข้อดีของแบบ Centralization และ แบบ Decentralization

ปัจจัยที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ

โครงสร้างเทคโนโลยีสารสนเทศ(IT Infrastructure) ตามคำจำกัดความของ K. Laudon and J. Laudon คือทรัพยากรเทคโนโลยีสารสนเทศที่ใช้ร่วมกันที่จะนำมาซึ่งโครงสร้างพื้นฐานสำหรับงานประยุกต์ระบบสารสนเทศเฉพาะตัวขององค์กรหนึ่งๆ โดยโครงสร้างหลักเทคโนโลยีสารสนเทศประกอบไปด้วย 7 ส่วนหลักที่จะต้องมีการประสานงานกันเพื่อประกอบการเป็นโครงสร้างหลักเทคโนโลยีสารสนเทศให้แก่องค์กรธุรกิจ ซึ่งประกอบไปด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์ (computer hardware plateforms), โครงสร้างพื้นฐานระบบปฏิบัติการ (operating system platforms), โปรแกรมประยุกต์สำหรับวิสาหกิจ(enterprise software application), การบริหารจัดการระบบฐานข้อมูล (data management and storage), ระบบเครือข่ายและการสื่อสารระยะไกล (networking/telecommunications platforms), ระบบอินเตอร์เน็ต(internet platforms), และบริการที่ปรึกษาและการบูรณาการ(consulting and system integration service) จากการศึกษาของ Fheili (2011) พบว่าในปัจจุบัน IT เป็นสิ่งจำเป็นมากสำหรับองค์กรโดยเฉพาะธนาคารและเพื่อให้องค์กรมีระบบ IT ที่ทันสมัยจำเป็นต้องมีการ Outsource บริการทางด้าน IT เพิ่มขึ้น ซึ่งนำมาสู่ความเสี่ยงทางด้าน IT ได้ นอกจากการอยู่รอดของนี้ธุรกิจในปัจจุบันขึ้นกับ โครงสร้างหลักด้านเทคโนโลยีสารสนเทศ โดยจะต้องเป็นโครงสร้างที่ปลอดภัย รวดเร็ว และพร้อมใช้ เพราะถ้าเกิดความล้มเหลวจะส่งผลให้องค์กรมีความเสี่ยงเพิ่มขึ้น การศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) ยังช่วยยืนยันว่าโครงสร้างหลักเทคโนโลยีสารสนเทศมีผลต่อความเสี่ยงทางด้าน IT โดยเฉพาะถ้าองค์กรมี ระบบเครือข่ายและการสื่อสารระยะไกล และการใช้งานผ่านเว็บไซต์

ปัจจัยที่ 9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี

พนักงานทุกคนต้องได้รับรู้มีความเข้าใจในเรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องรู้ว่าใช้อย่างไรจึงจะปลอดภัย พนักงานต้องเล็งเห็นถึงความสำคัญของกฎเกณฑ์ นโยบาย ข้อบังคับที่องค์กรตั้งขึ้นเพื่อลดหรือหลีกเลี่ยงความเสี่ยงการฝึกอบรมและการสื่อสารให้พนักงานมีความรู้มีความเข้าใจเป็นปัจจัยช่วยลดความเสี่ยงในองค์กร (พลพฐ ปียวรรณ และ สุภาพร เชิงเอี่ยม. 2552) และจากการศึกษาของ IT Policy Compliance Group (2010) พบว่าพฤติกรรมของคน เช่นความผิดพลาด การละเลยไม่ปฏิบัติตามขั้นตอน การใช้งานอย่างไม่ถูกต้อง และการทุจริตการขโมยข้อมูล ก่อให้เกิดอันตรายต่อการใช้ระบบเทคโนโลยีสารสนเทศ ดังนั้นการให้การอบรม และเอกสารรายงานแก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ ที่สูงก็ได้ผลลัพธ์ที่ดี ลดปัญหาและอันตรายทีเกิดจากการใช้ IT ให้น้อยลง

กรอบแนวคิดในการวิจัย(Conceptual Framework)

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยเรื่อง ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย ในครั้งนี้ใช้ระเบียบวิธีวิจัยเชิงสำรวจ โดยจะนำเสนอรายละเอียดเกี่ยวกับวิธีดำเนินการวิจัยครอบคลุมวัตถุประสงค์ ขั้นตอนการวิจัย และรายละเอียดแต่ละขั้นตอนดังต่อไปนี้

วิธีดำเนินการวิจัย

ขั้นตอนที่ 1 การศึกษาองค์ความรู้เพื่อกำหนดกรอบแนวคิดงานวิจัย

ผู้วิจัยได้ศึกษาเอกสารทฤษฎีและหลักการที่เกี่ยวกับปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศจากเอกสาร บทความทางวิชาการ งานวิจัยที่เกี่ยวข้อง และฐานข้อมูลออนไลน์ หลังจากนั้นได้วิเคราะห์และสังเคราะห์ข้อมูลที่ได้มากำหนดเป็นกรอบแนวคิดในงานวิจัยถึงปัจจัยที่ส่งผลต่อปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ โดยผู้วิจัยกำหนดตัวแปรที่ส่งผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศได้ทั้งสิ้น 9 ตัว ดังนี้

ปัจจัยที่ 1. ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้

ปัจจัยที่ 2. นโยบายการควบคุมความปลอดภัยของงานสารสนเทศ

ปัจจัยที่ 3. งบประมาณ

ปัจจัยที่ 4. เครื่องมือที่ใช้ในการบริหารจัดการความเสี่ยง

ปัจจัยที่ 5. ขนาดขององค์กร

ปัจจัยที่ 6. การสื่อสารในเรื่องของความเสี่ยง

ปัจจัยที่ 7. รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศ

ปัจจัยที่ 8. องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ

ปัจจัยที่ 9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย แนวปฏิบัติที่ดี

ขั้นตอนที่ 2 การตรวจสอบการกำหนดองค์ประกอบของปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ

จากการวิเคราะห์และสังเคราะห์แนวคิดและผลงานวิจัยที่เกี่ยวข้อง ผู้วิจัยกำหนดตัวแปรที่ส่งผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ ได้ทั้งสิ้น 9 ตัว โดยผู้วิจัยได้กำหนดนิยามของตัวแปรต่างๆไว้ดังนี้

1. ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงหมายถึงบุคคลในบริษัทหลักทรัพย์ที่มีหน้าที่ในเรื่องของการกำหนดและบริหารจัดการความเสี่ยง, บริหารจัดการคุณค่า, และกำกับดูแลในเรื่องการบริหารความเสี่ยง อันประกอบไปด้วย
    - 1.1 Senior manager (CEO, COO)
    - 1.2 Senior IT manager (CIO)
    - 1.3 IT operations manager
    - 1.4 Information security manager
    - 1.5 Risk manager
    - 1.6 Internal auditors
    - 1.7 Legal and compliance manager

2. นโยบายการควบคุมความปลอดภัยของงานสารสนเทศ คือ การควบคุมทางกายภาพ (จาก ไฟไหม้, น้ำ, ไฟฟ้าขัดข้อง แผ่นดินไหว, ฝุ่น และผู้บุกรุกที่ไม่ได้รับอนุญาต) การควบคุมทางตรรกะ(การควบคุมการเข้าถึงระบบสารสนเทศและการควบคุมการป้องกันไวรัสคอมพิวเตอร์) และ การควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ (แผนการฟื้นสภาพระบบจากภัยพิบัติ ซึ่งประกอบไปด้วยการมีแผนฉุกเฉิน, แผนสำรอง, แผนฟื้นสภาพ, แผนทดสอบ และการทำประกันภัย)
3. งบประมาณคือจำนวนงบประมาณทางด้านเทคโนโลยีสารสนเทศ, จำนวนงบประมาณด้านการรักษาความปลอดภัยและจำนวนงบประมาณด้านการตรวจสอบ
4. เครื่องมือที่ใช้ในการบริหารความเสี่ยงคือรูปแบบของเครื่องที่ใช้ในการบริหารความเสี่ยงอันประกอบไปด้วยเครื่องมือดังต่อไปนี้ ISO 27001, CIS benchmarks, COBIT, IT portfolio management, Balanced Scorecard, ITIL, ISO 17799, SOX และ COSO
5. ขนาดขององค์กรแบ่งเป็น องค์กรขนาดเล็กคือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 44,684,048,523 ถึง 523,381,373,618 บาท, องค์กรขนาดกลางคือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 523,381,373,619 ถึง 1,002,078,698,712 บาท และ องค์กรขนาดใหญ่คือองค์กรที่ยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ตั้งแต่ 1,002,078,698,712 บาทขึ้นไป
6. การสื่อสารเรื่องของความเสี่ยงคือวิธีในการสื่อสารทั้งภายในและภายนอกอันประกอบไปด้วย รูปแบบรายงาน ซึ่งแบ่งเป็น Exception report, Priority report, Web-dashboard, Email, การพูดจา, โทรศัพท์,เอกสารอิเล็กทรอนิกส์, คู่มือนโยบาย และประกาศ
7. รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีคือ รูปแบบของการจัดโครงสร้างแผนก IT ภายในองค์กร ได้แก่ แบบรวมศูนย์ (Centralization), แบบกระจายศูนย์ (Decentralization) และ แบบผสม (Federalism)
8. องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศคือ โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต และ บริการที่ปรึกษาและการบูรณาการระบบงาน
9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำหรือไม่ ได้แก่ การสัมมนา, การอบรม, การแจกเอกสารคู่มือ

<u>ขั้นตอนที่ 3</u> การสร้างและพัฒนาเครื่องมือ

3.1 ผู้วิจัยใช้เครื่องมือเป็นแบบสอบถามการวัดระดับปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ
(ดูรายละเอียดในภาคผนวก ข)

3.2 ตรวจสอบความเที่ยงตรงของเนื้อหาของคำถาม เพื่อหาดรรชนีความสอดคล้อง (Index of Concurrence: IOC) ในการพิจารณาเนื้อหาของคำถามถึงปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศ วิเคราะห์ค่าดรรชนีความสอดคล้องของคำถามกับตัวแปรที่มีค่าตั้งแต่ 0.5 ขึ้นไป โดยมีรายละเอียดการวิเคราะห์ค่า IOC ดังตารางที่ 3.1 ดังนี้

ตารางที่ 3.1 ผลการพิจารณาของผู้ทรงคุณวุฒิต่อความสอดคล้องของข้อคำถามด้านปัจจัยความเสี่ยง

ปัจจัย	องค์ประกอบย่อย	ค่า IOC
1. ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้	1.1 Senior manager (CEO, COO) 1.2 Senior IT manager (CIO) 1.3 IT operations manager 1.4 Information security manager 1.5 Risk manager 1.6 Internal auditors 1.7 Legal and compliance manager	1
2. นโยบายการควบคุมความปลอดภัยของงานสารสนเทศ	2.1 การควบคุมทางกายภาพ (จาก ไฟไหม้, น้ำ, ไฟฟ้าขัดข้อง, แผ่นดินไหว, ฝุ่น และ ผู้บุกรุกที่ไม่ได้รับอนุญาต) 2.2 การควบคุมทางด้านตรรกะ (การควบคุมการเข้าถึงระบบสารสนเทศ และ การควบคุมการป้องกันไวรัสคอมพิวเตอร์) 2.3 การควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ (การมีแผนฟื้นสภาพจากภัยพิบัติซึ่งประกอบไปด้วยแผนฉุกเฉิน, แผนสำรอง, แผนฟื้นสภาพ, แผนทดสอบ และการทำประกันภัย)	1
3. งบประมาณ	3.1 งบประมาณทางด้าน IT 3.2 งบประมาณด้านการรักษาความปลอดภัย 3.3 งบประมาณด้านการตรวจสอบด้าน IT	1
4. เครื่องมือในการบริหารจัดการความเสี่ยงที่นำมาใช้	4.1 ISO 27001 4.2 CIS benchmarks 4.3 COBIT 4.4 IT portfolio management 4.5 Balanced scorecard 4.6 ITIL 4.7 ISO 17799 4.8 SOX 4.9 COSO	1

ตารางที่ 3.1 ผลการพิจารณาของผู้ทรงคุณวุฒิต่อความสอดคล้องของข้อคำถามด้านปัจจัยความเสี่ยง(ต่อ)

ปัจจัย	องค์ประกอบย่อย	ค่า IOC
5. ขนาดขององค์กร	5.1 ขนาดเล็ก 5.2 ขนาดกลาง 5.3 ขนาดใหญ่	1
6. วิธีการการติดต่อสื่อสารในเรื่องของความเสี่ยง	6.1 รายงานแบบต่างๆ เช่น exception report 6.2 อีเมล์ 6.3 การพูดจา 6.4 โทรศัพท์ 6.5 เอกสารอิเล็กทรอนิกส์ 6.6 คู่มือนโยบาย 6.7 ประกาศ	1
7. รูปแบบการจัดโครงสร้างแผนกเทคโนโลยี	7.1 แบบแบบรวมศูนย์ (Centralization) 7.2 แบบกระจายศูนย์ (Decentralization) 7.3 แบบผสม (Federalism)	1
8. องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ	8.1 โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์ (Computer H/W platforms) 8.2 โครงสร้างพื้นฐานระบบปฏิบัติการ (Operating system platforms) 8.3 โปรแกรมประยุกต์สำหรับวิสาหกิจ (Enterprise S/W applications) 8.4 การบริหารจัดการฐานข้อมูล (Data management and storage) 8.5 ระบบเครือข่ายและการสื่อสารทางไกล (Networking/Telecommunication platforms) 8.6 ระบบอินเตอร์เน็ต (Internet platforms) 8.7 บริการที่ปรึกษาและการบูรณาการระบบงาน (Consulting and system integration services)	1
9. การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ	9.1 การสัมมนา 9.2 การอบรม 9.3 การแจกเอกสารคู่มือ	0.67

ตารางที่ 3.2 ผลการพิจารณาของผู้ทรงคุณวุฒิต่อความสอดคล้องของข้อคำถามด้านความเสี่ยง

ความเสี่ยง	ค่า IOC
1. ข้อมูลที่สำคัญสูญหายหรือถูกขโมย	0.67
2. การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ต	1
3. การหยุดชะงักทางธุรกิจเนื่องมาจาก IT เช่นการเกิดช่วงเวลาที่ไม่สามารถใช้งานได้ (downtime)	1
4. การสูญเสียรายได้ ทรัพย์สิน	1
5. การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้	1
6. การขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT	1

โดยผู้วิจัยมีหลักเกณฑ์ในการคัดเลือกผู้ทรงคุณวุฒิ จำนวน 3 ท่าน ดังนี้

3.2.1 เป็นผู้ทรงคุณวุฒิทางการศึกษาระดับปริญญาเอกและมีตำแหน่งทางวิชาการ ในด้านวิทยาศาสตร์คอมพิวเตอร์

3.2.2 เป็นผู้เชี่ยวชาญในงานด้านการตรวจสอบ และได้ใบรับรองความสามารถทางด้านการตรวจสอบ (วุฒิบัตร CIA, CISA และ CISSP)

3.2.3 เป็นผู้ชำนาญในสายงานด้าน IT และ อยู่ในตำแหน่งผู้จัดการฝ่าย IT ในบริษัทหลักทรัพย์

(รายละเอียดในภาคผนวก ค)

3.3 นำผลวิเคราะห์จากผู้ทรงคุณวุฒิมาปรับปรุงแก้ไขข้อคำถามให้มีความสมบูรณ์ยิ่งขึ้น แล้วนำไปทดลองใช้กับบริษัทหลักทรัพย์จริง จำนวน 1 บริษัท เพื่อหาความเที่ยงตรงของแบบสอบถาม

3.4 นำผลที่ได้จากการทดลองใช้มาปรับปรุงแก้ไขแบบสอบถามเพื่อให้ได้เครื่องมือที่จะใช้ในการเก็บข้อมูลที่ถูกต้องและมีประสิทธิภาพ

3.5 นำเสนอโครงงานและแบบสอบถามต่อคณะกรรมการจริยธรรมงานวิจัย มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ และได้การพิจารณาเห็นชอบโดยสอดคล้องกับประกาศเฮลซิงกิ

3.6 ขอรับทุนสนับสนุนการทำวิจัยจากมหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

ขั้นตอนที่ 4 การเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล และการสรุปผล

ผู้วิจัยและผู้ช่วยนักวิจัยติดต่อนัดหมายเพื่อเข้าไปขอเก็บข้อมูลจากบริษัทหลักทรัพย์ทั้งหมดในประเทศไทย และมีการตรวจสอบความสมบูรณ์ของข้อมูลที่ได้คืน นำข้อมูลที่ได้มาวิเคราะห์ สรุปผล และอภิปรายผล (ดูรายละเอียดในภาคผนวก ง)

ประชากรที่ใช้ในการวิจัย

คือบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศไทยที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตจำนวนทั้งสิ้น 26 บริษัท

ผู้ให้ข้อมูล

ประกอบไปด้วย ผู้บริหารฝ่าย IT หรือเทียบเท่าของบริษัทหลักทรัพย์ เนื่องจากเป็นผู้ที่มีความรู้ความสามารถทางด้าน IT โดยตรง สามารถประเมินความต้องการขององค์กรที่เกี่ยวกับเทคโนโลยีที่จะนำมาใช้ให้เหมาะกับองค์กร เป็นผู้วางแผนในเรื่องของ Information Security ตลอดจนเป็นผู้ที่สามารถให้ข้อมูลที่มีความถูกต้องและน่าเชื่อถือสอดคล้องกับการทำการวิจัยในครั้งนี้

เครื่องมือที่ใช้ในการวิจัย

ในการวิจัยครั้งนี้ผู้วิจัยได้ใช้เครื่องมือในการเก็บรวบรวมข้อมูลดังนี้

1. แบบสอบถามกึ่งสัมภาษณ์ข้อมูลเกี่ยวกับข้อมูลทั่วไปของฝ่าย IT ของบริษัท ลักษณะของแบบสอบถามเป็นแบบเติมข้อมูลและตัวเลือกที่กำหนดไว้ให้
2. แบบสอบถามกึ่งสัมภาษณ์ข้อมูลเกี่ยวกับ ข้อมูลเรื่องการบริหารจัดการความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ลักษณะของแบบสอบถามเป็นแบบตัวเลือกที่กำหนดไว้ให้
3. แบบสอบถามกึ่งสัมภาษณ์ข้อมูลเพื่อวัดทัศนคติ/ความคิดเห็นของผู้บริหารด้าน IT ที่มีต่อปัจจัยความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ เป็นแบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ
4. แบบสอบถามกึ่งสัมภาษณ์ข้อมูลเกี่ยวกับระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ที่เกิดขึ้นในบริษัทเป็นแบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ

การเก็บรวบรวมข้อมูล

การเก็บข้อมูลในครั้งนี้ผู้วิจัยทำการรวบรวมข้อมูลจากประชากรทั้งหมด โดยทำหนังสือขอความร่วมมือจากบริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตจำนวนทั้งสิ้น 26 บริษัทเพื่อขออนุญาตและขอความร่วมมือในการเก็บข้อมูล รวมทั้งการนัดหมายวันเวลาที่สะดวกในการเข้าไปเก็บข้อมูล หลังจากนั้นจึงส่งผู้ช่วยนักวิจัยเข้าไปเพื่อเก็บข้อมูล ณ บริษัทนั้นๆ เพื่อให้การเก็บข้อมูลเป็นไปอย่างถูกต้องผู้ช่วยนักวิจัยได้รับการฝึกฝนในการถามคำถาม รวมทั้งมีความรู้ในหัวข้อที่ถาม ทำให้สามารถอธิบายและตอบข้อคำถามของผู้ตอบแบบสอบถามในกรณีที่ผู้ตอบมีข้อสงสัย ในส่วนของบริษัทที่ไม่ตอบกลับในระยะเวลาที่กำหนดได้มีการโทรศัพท์เพื่อติดต่อประสานงานเพื่อนัดหมายในการเข้าไปเก็บข้อมูลอีกครั้ง นอกจากนี้ในกรณีบริษัทที่ไม่สะดวกที่จะให้ผู้ช่วยนักวิจัยเข้าไปเก็บข้อมูล ทางผู้วิจัยจะส่งแบบสอบถามให้ทางไปรษณีย์และขอความอนุเคราะห์รับแบบสอบถามกลับทางไปรษณีย์

การวิเคราะห์ข้อมูล

การวิจัยในครั้งนี้ใช้บริษัทหลักทรัพย์ที่เป็นสมาชิกตลาดหลักทรัพย์แห่งประเทศไทย ที่เปิดให้บริการซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตจำนวนทั้งสิ้น 26 บริษัท โดยผู้วิจัยได้รับความร่วมมือในการให้ข้อมูลกลับจำนวน 21 บริษัท คิดเป็นร้อยละ 80.77 ซึ่งข้อมูลตอบกลับจากทั้ง 21 บริษัท นั้นสมบูรณ์ถูกต้องสามารถนำมาใช้วิเคราะห์ผลได้ทั้งหมด โดยใช้โปรแกรมสำเร็จรูป SPSS for Windows ในการวิเคราะห์ โดยสถิติที่ใช้ในการวิจัย ประกอบด้วย

1. การวิเคราะห์ค่าดรรชนีความสอดคล้องของผู้ทรงคุณวุฒิ (Index of concurrence)
2. วิเคราะห์ข้อมูลจากแบบสอบถามส่วนที่เป็นการเลือกตอบใช้วิธีการแจกแจงความถี่ (Frequency) และหาค่าเปอร์เซ็นต์ (Percents) ส่วนที่เป็นแบบมาตราส่วนประมาณค่าใช้วิธีการหาค่าเฉลี่ย(Mean) และค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)

3. วิเคราะห์ปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทยวิเคราะห์โดยใช้ วิธีการวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis), วิธีการวิเคราะห์ความถดถอยเชิงพหุคูณ (Multiple Regression Analysis), วิธีการใช้ค่าสถิติทดสอบทีแบบกลุ่มตัวอย่างไม่สัมพันธ์กัน (t-test Independent Group), วิธีการใช้ค่าสถิติวิเคราะห์ความแปรปรวนแบบทางเดียว (One – Way Anova)

บทที่ 4
ผลการวิเคราะห์ข้อมูล

การวิจัยนี้เป็นการเสนอผลการรายงานการวิจัย โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย รวมทั้งความเสี่ยงและผลกระทบผลกระทบที่เกิดจากความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ที่มีต่อผลการดำเนินงานของบริษัทหลักทรัพย์ โดยนำเสนอผลการวิเคราะห์ดังนี้

ตอนที่1. การวิเคราะห์สถานภาพของผู้ตอบแบบสอบถาม

การวิเคราะห์สถานภาพผู้ตอบแบบสอบถามเป็นผู้บริหารฝ่าย IT ของบริษัทหรือเทียบเท่า ในบริษัทหลักทรัพย์ในประเทศไทย รวมทั้งสิ้น 21 คน จำแนกตามเพศ อายุ วุฒิการศึกษา และ ตำแหน่งงาน ผลปรากฏดังตารางที่ 4.1 และ 4.2

ตารางที่ 4.1 จำนวน และ ร้อยละ ของผู้ตอบแบบสอบถามจำแนกตาม เพศ วุฒิการศึกษา และ ตำแหน่งงาน

สถานภาพ	จำนวน	ร้อยละ
1. เพศ		
หญิง	3	14.30
ชาย	18	85.70
2. วุฒิการศึกษา		
ปริญญาตรี	13	61.90
ปริญญาโท	8	38.10
3. ตำแหน่ง		
IT Manager	4	19.05
Vice President Information Technology	4	19.05
Senior Vice President Information Technology	2	9.52
Director	1	4.76
Senior Vice President Deputy Managing Director	1	4.76
IT Support	1	4.76
ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	2	9.52
ผู้อำนวยการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ	2	9.52
ผู้ช่วยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	1	4.76
ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ	1	4.76
ผู้จัดการอาวุโสและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	1	4.76
ฝ่าย IT	1	4.76

ตารางที่ 4.2 ค่าต่ำสุด ค่าสูงสุด ค่าเฉลี่ย และ ส่วนเบี่ยงเบนมาตรฐาน ของอายุผู้ตอบแบบสอบถาม

	ค่าต่ำสุด	ค่าสูงสุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน
อายุ	35	55	43.74	5.476

จากตารางที่ 4.1 และ ตารางที่ 4.2 พบว่า ผู้ตอบแบบสอบถามทั้งหมด 21 คนส่วนใหญ่เป็นเพศชายถึงร้อยละ 85.70 และเพศหญิงร้อยละ 14.30 ในส่วนของวุฒิการศึกษาส่วนใหญ่จบการศึกษาระดับปริญญาตรีร้อยละ 61.90 และระดับปริญญาโท ร้อยละ 38.10 ผู้ตอบแบบสอบถามส่วนใหญ่มีตำแหน่งเป็นระดับบริหารทางด้านเทคโนโลยีสารสนเทศ โดยมีตำแหน่ง IT Manager และ Vice President Information Technology ร้อยละ 19.05 ตำแหน่ง Senior Vice President Information Technology, ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และ ผู้อำนวยการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ ร้อยละ 9.52 โดยผู้ตอบแบบสอบถามมีอายุเฉลี่ยอยู่ที่ 43.74 ปี

ตอนที่2. การวิเคราะห์ข้อมูลฝ่าย IT ในบริษัทหลักทรัพย์

การวิเคราะห์ข้อมูลฝ่าย IT ของบริษัทหลักทรัพย์ในประเทศไทยจำนวนทั้งสิ้น 21 บริษัท สามารถสรุปผลได้ดังตารางต่อไปนี้

ตารางที่ 4.3 จำนวน และ ร้อยละ ของข้อมูลด้านต่างๆในฝ่าย IT ของบริษัทหลักทรัพย์

ข้อมูลฝ่าย IT	จำนวน	ร้อยละ
1. Data Center		
มี Data Center	21	100.00
- อยู่สูงกว่าชั้น 1	16	76.19
ไม่มี Data Center	0	0.00
2. Disaster Recovery Site		
มี Disaster Recovery Site	19	90.50
- มีอยู่ที่สาขาอื่น หรือ อาคารอื่น	17	89.47
- มีอยู่ที่บริษัท	1	5.26
- มีอยู่ที่ Cyber world	1	5.26
ไม่มี Disaster Recovery Site	2	9.50
3. จำนวนบุคลากรในฝ่าย IT		
น้อยกว่า 3 คน	1	4.80
3 - 5 คน	1	4.80
6 - 8 คน	2	9.50
12 - 15 คน	5	23.80
มากกว่า 15 คน	12	57.10

ตารางที่ 4.3 จำนวน และ ร้อยละ ของข้อมูลด้านต่าง ๆในฝ่าย IT ของบริษัทหลักทรัพย์ (ต่อ)

ข้อมูลฝ่าย IT	จำนวน	ร้อยละ
4. โครงสร้างแผนก/ฝ่าย IT		
แบบรวมศูนย์ (ฝ่าย IT เป็นหน่วยงานเดียวที่สรรหาและเก็บข้อมูลอยู่ที่ส่วนกลาง)	16	76.20
แบบกระจายศูนย์ (แผนกต่างๆมี IT เป็นผู้ดูแลงานของตนเอง)	1	4.80
แบบผสม (มีบางส่วนถูกกำหนดจากส่วนกลาง และ บางส่วนสามารถพัฒนาระบบสารสนเทศในหน่วยงานได้เอง)	4	19.00
5. การใช้ระบบสารสนเทศอื่นนอกจากระบบซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตมาช่วยในการทำงาน		
ไม่มีการใช้	4	19.00
มีการใช้ เช่น ระบบ Back office, efinance, ASPEN, Bloomberg, บัญชี, ความเสี่ยงลูกค้า, คิดคำนวณชำระราคา, ระบบของธุรกิจกองทุนรวมหลักทรัพย์, ระบบซื้อขายที่ไม่ใช้อินเตอร์เนตหรือการโทรขาย, การโอนเงิน, LotusNote	17	81.00

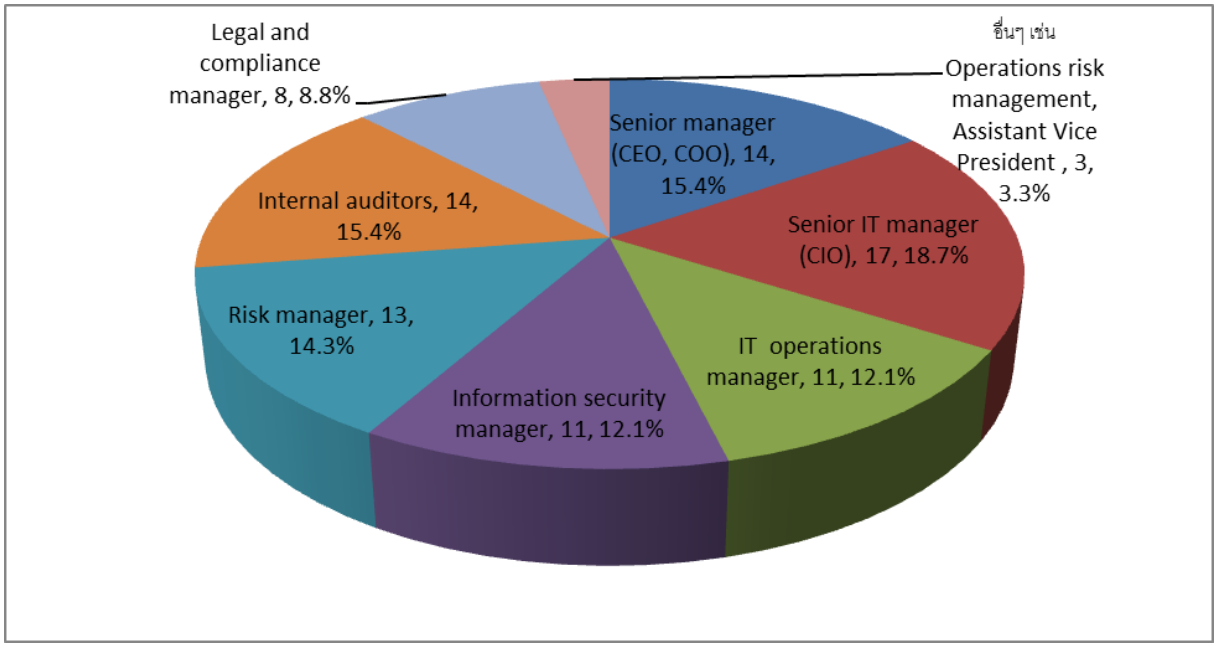
จากตารางที่ 4.3 พบว่า ทุกบริษัทหลักทรัพย์ในประเทศไทยมีศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลาง (Data Center) ที่บริษัทเอง โดยบริษัทที่ให้ข้อมูลรายละเอียดของศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางจำนวน 16 บริษัท คิดเป็นร้อยละ 76.19 มีศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางอยู่สูงกว่าชั้น 1 ทุกบริษัท ในส่วนของ ศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิดจากภัยพิบัติ (Disaster Recovery Site)พบว่าบริษัทหลักทรัพย์ร้อยละ 90.75 มีศูนย์นี้ โดยร้อยละ 89.47 ของบริษัทที่มีศูนย์นี้มีศูนย์อยู่ที่สาขาอื่นหรืออาคารอื่น รองลงมาร้อยละ 5.26 มีอยู่ที่บริษัทเอง และ Cyber World ในส่วนของบุคลากรพบว่าจำนวนบุคลากรในบริษัทหลักทรัพย์ที่เป็นบุคลากรในฝ่าย/แผนก IT มากกว่า 15 คน คิดเป็นร้อยละ 57.10 รองลงมา เป็นบุคลากรในฝ่าย/แผนก IT จำนวน 12 - 15 คน และ จำนวน 6 - 8 คน ร้อยละ 23.80 และ 9.50 ตามลำดับ

นอกจากนี้ยังพบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีการจัดรูปแบบโครงสร้างแผนก/ฝ่ายIT แบบรวมศูนย์ (Centralization) คิดเป็นร้อยละ 76.20 รองลงมาคือมีการจัดแบบผสม(Federalism)และแบบกระจายศูนย์ (Decentralization) คิดเป็นร้อยละ 19.00 และ 4.80 ตามลำดับ และยังพบอีกว่า ร้อยละ 81 ของบริษัทหลักทรัพย์มีการใช้ระบบสารสนเทศอื่นนอกจากระบบซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ต โดยมีการใช้ระบบ ระบบ Back office, e-finance, ASPEN, Bloomberg, บัญชี, ความเสี่ยงลูกค้า,คิดคำนวณชำระราคา,ระบบของธุรกิจกองทุนรวมหลักทรัพย์, ระบบซื้อขายที่ไม่ใช้อินเตอร์เนตหรือการโทรขาย, การโอนเงิน และ Lotus Note

ตอนที่3. การวิเคราะห์ข้อมูลเรื่องการบริหารจัดการความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัท

การวิเคราะห์ข้อมูลเรื่องการบริหารจัดการความเสี่ยงเกี่ยวข้องกับการใช้ระบบเทคโนโลยีในบริษัท ของบริษัทหลักทรัพย์ในประเทศไทยจำนวนทั้งสิ้น 21 บริษัท สามารถสรุปผลได้ดังตารางต่อไปนี้

ภาพที่ 4.1 สัดส่วนของผู้มีส่วนในเรื่องการบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์



จากภาพที่ 4.1 ในเรื่องผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์พบว่า พบว่า Senior IT manager (CIO) เป็นผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศมากที่สุดคิดเป็นร้อยละ18.7 รองลงมาคือ Senior manager (CEO, COO) และ Internal auditors เท่ากันคือร้อยละ 15.4 ตามด้วยตำแหน่ง Risk manager คิดเป็นร้อยละ 14.3 ส่วนตำแหน่ง IT operations manager และ Information security manager เท่ากันคือร้อยละ 12.1 ลำดับสุดท้ายคือ Legal and compliance manager คือร้อยละ 8.80 นอกจากนี้ยังมีตำแหน่งอื่นๆอีก คิดเป็นร้อยละ 3.3 โดยระบุว่าคือ ตำแหน่ง Operations risk management และ Assistant Vice President

ตารางที่ 4.4 ข้อมูลสรุปการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพ ของบริษัทหลักทรัพย์

ข้อมูลการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพ	จำนวน	ร้อยละ
1. **ด้านอัคคีภัย**		
- มีระบบแจ้งเตือนภัย	21	19.60
- มีอุปกรณ์ฉีดดับเพลิง เช่น น้ำ, สารคาร์บอนไดออกไซด์, หรือ แก๊ซฮาลอน	20	18.70

ตารางที่ 4.4 ข้อมูลสรุปการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพ ของบริษัทหลักทรัพย์ (ต่อ)

ข้อมูลการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพ	จำนวน	ร้อยละ
- มีการฝึกซ้อมระบบป้องกันอัคคีภัย	20	18.70
- มีแผนผังแสดงจุดที่ตั้งของระบบดับเพลิง	14	13.10
- สายไฟมีฉนวนหุ้มป้องกัน	14	13.10
- อุปกรณ์เชื้อไฟเช่น กระดาษ เก็บในห้องแยก	8	7.50
- ตึกที่เป็นที่ตั้งอุปกรณ์และทรัพย์สินใช้อุปกรณ์กันไฟและโครงสร้างตึกกันไฟ	5	4.70
- สัญญาณเตือนภัยเชื่อมต่อยังสถานีดับเพลิง	5	4.70
2. ด้านน้ำ		
- เก็บทรัพย์สินระบบสารสนเทศอยู่ในชั้นที่น้ำท่วมไม่ถึง	17	23.30
- มีการติดตั้งสัญญาณเตือนภัยเชื่อมต่อกับเครื่องตรวจจับ (water sensor)	16	21.90
- มีหลังคา ผนัง พื้น ป้องกันการรั่วซึม	15	20.50
- มีทางระบายน้ำที่เหมาะสม	14	19.20
- มีข้อห้ามพนักงานนำเครื่องดื่มเข้าใกล้คอมพิวเตอร์และอุปกรณ์	11	15.10
3. ด้านระบบไฟฟ้า		
- มีอุปกรณ์สำรองไฟหรือ UPS	21	52.50
- มีการติดตั้งอุปกรณ์ตัดไฟ (circuit breaker) หรือ อุปกรณ์ควบคุมแรงดันกระแสไฟ (voltage regulator)	19	47.50
4. ด้านฝุ่น		
- มีการดูดฝุ่นอยู่เสมอ	19	63.30
- มีพื้นห้องและพรมแบบกันฝุ่น	11	36.70
5. ด้านผู้บุกรุกที่ไม่ได้รับอนุญาต		
- มีการจำกัดการเข้าออก	21	36.20
- ศูนย์คอมพิวเตอร์มีประตูแข็งแรงและมีสัญญาณเตือนภัย	17	29.30
- เก็บดิสก์หรือเทปที่บันทึกข้อมูลเข้าตู้ล็อกกุญแจ	15	25.90
- อื่นๆ เช่น เก็บดิสก์หรือเทปไว้ข้างนอกบริษัท,เอาเข้าไปเก็บที่ ธนาคาร หรือ ติดตั้ง CCTV	5	8.60

จากตารางที่ 4.4 เรื่องการควบคุมความปลอดภัยทางกายภาพด้านกายภาพ ในด้านแรกอัคคีภัย พบว่าบริษัทหลักทรัพย์ทุกบริษัททั้ง 21 บริษัทมีระบบแจ้งเตือนภัย รองลงมาคือบริษัทมีอุปกรณ์ฉีดดับเพลิง เช่น น้ำ, สาร

คาร์บอนไดออกไซด์, หรือ แก๊ซฮาลอน และมี การฝึกซ้อมระบบป้องกันอัคคีภัย เท่ากัน คือจำนวน 20 บริษัทลำดับถัดมาคือ บริษัทมีแผนผังแสดงจุดที่ตั้งของระบบดับเพลิงและสายไฟมีฉนวนหุ้มป้องกันเท่ากัน คือ 14 บริษัท

ในส่วนของการควบคุมความปลอดภัยทางกายภาพด้านน้ำ โดยบริษัทหลักทรัพย์ส่วนใหญ่มีการเก็บทรัพย์สิน ระบบสารสนเทศอยู่ในชั้นที่น้ำท่วมจำนวน 17 บริษัท รองลงมาคือบริษัทมีการติดตั้งสัญญาณเตือนภัยเชื่อมต่อกับเครื่อง ตรวจจับ (water sensor) 16 บริษัทลำดับถัดมาคือบริษัทมีหลังคา ผนัง พื้น ป้องกันการรั่วซึมคิดจำนวน 15 บริษัท และมี ทางระบายน้ำที่เหมาะสมและมีข้อห้ามพนักงานนำเครื่องดื่มเข้าใกล้คอมพิวเตอร์และอุปกรณ์ จำนวน 14 และ 11 บริษัท ตามลำดับ ในเรื่องการควบคุมความปลอดภัยทางกายภาพด้านระบบไฟฟ้า โดยบริษัทหลักทรัพย์ทุกบริษัทมีการติดตั้ง อุปกรณ์สำรองไฟหรือ UPS รองลงมาคือบริษัทมีการติดตั้งอุปกรณ์ตัดไฟ (circuit breaker) หรือ อุปกรณ์ควบคุมแรงดัน กระแสไฟ (voltage regulator) ในเรื่องการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพด้านฝุ่น พบว่ามีบริษัท หลักทรัพย์ส่วนใหญ่มีการดูดฝุ่นอยู่เสมอจำนวน 19 บริษัท รองลงมาคือบริษัทมีพื้นห้องและพรมแบบกันฝุ่น จำนวน 11 บริษัท

ด้านสุดท้ายคือการควบคุมความปลอดภัยของงานด้าน IT ทางกายภาพจากผู้บุกรุกที่ไม่ได้รับอนุญาตพบว่า บริษัทหลักทรัพย์ทุกบริษัทมีการจำกัดการเข้าออก รองลงมาคือศูนย์คอมพิวเตอร์ของบริษัทมีประตูแข็งแรงและมีสัญญาณ เตือนภัย รองลงมาคือบริษัทเก็บดิสก์หรือเทปที่บันทึกข้อมูลเข้าตู้ล็อกกุญแจ นอกจากนี้ยังมีบริษัทที่มีการป้องกันผู้บุกรุกที่ ไม่ได้รับอนุญาตด้วยวิธีอื่นๆ เช่น เก็บดิสก์หรือเทปไว้ข้างนอกบริษัท,เอาเข้าไปเก็บที่ธนาคาร และติดตั้ง CCTV

ตารางที่ 4.5 ข้อมูลสรุปการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะ ของบริษัทหลักทรัพย์

ข้อมูลการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะ	จำนวน	ร้อยละ
1. การควบคุมการเข้าถึงระบบสารสนเทศ		
- มีการกำหนดนโยบายการใช้ password เช่น ไม่อนุญาตให้ใช้รหัสผ่านที่มีลักษณะมีจุดอ่อน	21	21.00
- มีการกำหนดสิทธิอำนาจการใช้งานของผู้ใช้แต่ละคน	20	20.00
- มีการบันทึกข้อมูลการใช้งาน เช่นเก็บข้อมูล Log File	20	20.00
- มีระเบียบกำหนดเกี่ยวกับการให้ เปลี่ยนแปลง และยกเลิกรหัสผู้ใช้	20	20.00
- มีการระบุผู้ใช้และพิสูจน์ผู้ใช้ที่แท้จริง	18	18.00
- อื่นๆ เช่น รีวิวสิทธิ์ประจำปี	1	1.00
2. การควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์ม		
- มีการป้องกันไวรัส	21	23.90
- มีการแก้ไขเมื่อตรวจเจอ	20	22.70
- มีการตรวจหาไวรัสอย่างสม่ำเสมอ	19	21.60
- มีการให้ความรู้แก่ผู้ใช้เกี่ยวกับอันตรายของไวรัสและการป้องกัน	19	21.60
- แต่ละหน่วยงานร่วมกันกำหนดวิธีการควบคุมการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ในเครือข่าย เช่น การเข้ารหัสข้อมูลตั้งแต่จุดเริ่มต้นถึงปลายทาง (end-to-end encryption)	18	18.00
- อื่นๆเช่นกำหนดห้ามเอาไฟล์หนัง เพลง มาลงในเครื่องคอมพิวเตอร์	1	1.00

จากตารางที่ 4.5 เรื่องการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะด้านการควบคุมการเข้าถึงระบบสารสนเทศพบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการกำหนดนโยบายการใช้ password เช่น ไม่อนุญาตให้ใช้รหัสผ่านที่มีลักษณะมีจุดอ่อน รองลงมาคือบริษัทมีการกำหนดสิทธิอำนาจการใช้งานของผู้ใช้แต่ละคน, มีการบันทึกข้อมูลการใช้งาน เช่นเก็บข้อมูล Log File, มีระเบียบกำหนดเกี่ยวกับการให้ เปลี่ยนแปลง และยกเลิกรหัส เท่ากันคือจำนวน 20 บริษัท รองลงมาคือบริษัทมีการระบุผู้ใช้และพิสูจน์ผู้ใช้ที่แท้จริง จำนวน 85.70 นอกจากนี้ยังมีบริษัทที่มีการป้องกันการควบคุมการเข้าถึงระบบสารสนเทศด้วยวิธีอื่น ๆ เช่น รีวิวสิทธิ์ประจำปี จำนวน 1 บริษัท

ส่วนในเรื่องการควบคุมความปลอดภัยของงานด้าน IT ทางตรรกะด้วยการควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์มพบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการมีการป้องกันไวรัส รองลงมาคือบริษัทมีการแก้ไขเมื่อตรวจเจอไวรัส จำนวน 20 บริษัท รองลงมาคือบริษัทมีมีการตรวจหาไวรัสอย่างสม่ำเสมอ และ มีการให้ความรู้แก่ผู้ใช้เกี่ยวกับอันตรายของไวรัสและการป้องกัน เท่ากันคือจำนวน 19 บริษัท ลำดับถัดมา คือบริษัทมีการให้แต่ละหน่วยงานร่วมกันกำหนดวิธีการควบคุมการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ในเครือข่าย เช่น การเข้ารหัสข้อมูล ตั้งแต่จุดเริ่มต้นถึงปลายทาง (end-to-end encryption) จำนวน 18 บรษัท นอกจากนี้ยังมีบริษัทที่มีการควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์มด้วยวิธีอื่นๆ เช่น กำหนดห้ามเอาไฟล์หนัง เพลง มาลงในเครื่องคอมพิวเตอร์ จำนวน 1 บริษัท

ตารางที่ 4.6 ข้อมูลสรุปการการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติของบริษัทหลักทรัพย์

ข้อมูลการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ	จำนวน	ร้อยละ
1. **มีแผนในการฟื้นสภาพระบบจากภัยพิบัติ** (Disaster Recovery plan)	21	15.9
- มีแผนฉุกเฉิน (Emergency plan)	19	14.40
- มีแผนสำรอง (Backup plan)	15	11.40
- มีแผนทดสอบ (Test plan)	13	9.80
- มีแผนฟื้นสภาพ (Recovery plan)	11	8.30
2. **มีการทำประกันภัย**	20	15.20
- ทำประกันอุปกรณ์ฮาร์ดแวร์	16	12.10
- ทำประกันที่เก็บสื่อ	5	3.80
- อื่นๆ เช่น ทำประกันทุกสิ่งทั้งหมดใน office	5	3.80
- ทำประกันเอกสารสำคัญ	4	3.00
- ทำประกันความหยุดชะงักทางธุรกิจ	3	2.30

จากตารางที่ 4.6 เรื่องการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีแผนในการฟื้นสภาพระบบจากภัยพิบัติ (Disaster Recovery plan) รองลงมาคือบริษัทมีการทำประกันภัยพบว่ามีเพียงบริษัทเดียวที่ไม่มีการทำประกันภัย โดยแผนที่บริษัทส่วนใหญ่มี คือ แผนฉุกเฉิน(Emergency plan) รองลงมาคือแผนสำรอง (Backup plan)และ แผนทดสอบ (Test plan) ส่วนแผนฟื้นสภาพ (Recovery plan) พบว่ามีบริษัทหลักทรัพย์ใช้น้อยที่สุด ในส่วนของการประกันภัย บริษัทส่วนใหญ่มีการทำประกันอุปกรณ์ฮาร์ดแวร์ รองลงมาคือทำประกันที่เก็บสื่อ และอื่นๆ เช่น ทำประกันทุกสิ่งทั้งหมดใน office เท่ากันคือจำนวน 5 บริษัท ลำดับถัดมาคือทำประกันเอกสารสำคัญและพบว่ามีบริษัทที่ทำประกันความหยุดชะงักทางธุรกิจน้อยที่สุด

ตารางที่ 4.7 ข้อมูลของงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012

ประเภทของงบประมาณ ปี 2012	ค่าต่ำสุด	ค่าสูงสุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน
1. งบประมาณด้าน IT (N=12)	2,000,000.00	400,000,000.00	56,000,000.00	109,967,763.87
(ทุกบริษัทมีการจัดสรรงบประมาณด้าน IT แต่มีบริษัทที่ยอมให้ข้อมูลจำนวน 12 บริษัท)				
2. งบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT (N=8)	100,000.00	50,000,000.00	7,218,750.00	17,310,606.52
(13 บริษัทมีการจัดสรรงบประมาณด้านการรักษาความปลอดภัย แต่มีบริษัทที่ยินยอมให้ข้อมูลจำนวน 8 บริษัท)				
3. งบประมาณทางด้านการตรวจสอบด้าน IT (N=2)	300,000.00	1,000,000.00	650,000.00	494,974.75
(12 บริษัทมีการจัดสรรงบประมาณด้านการรักษาความปลอดภัย แต่มีบริษัทที่ยินยอมให้ข้อมูลจำนวน 2 บริษัท)				

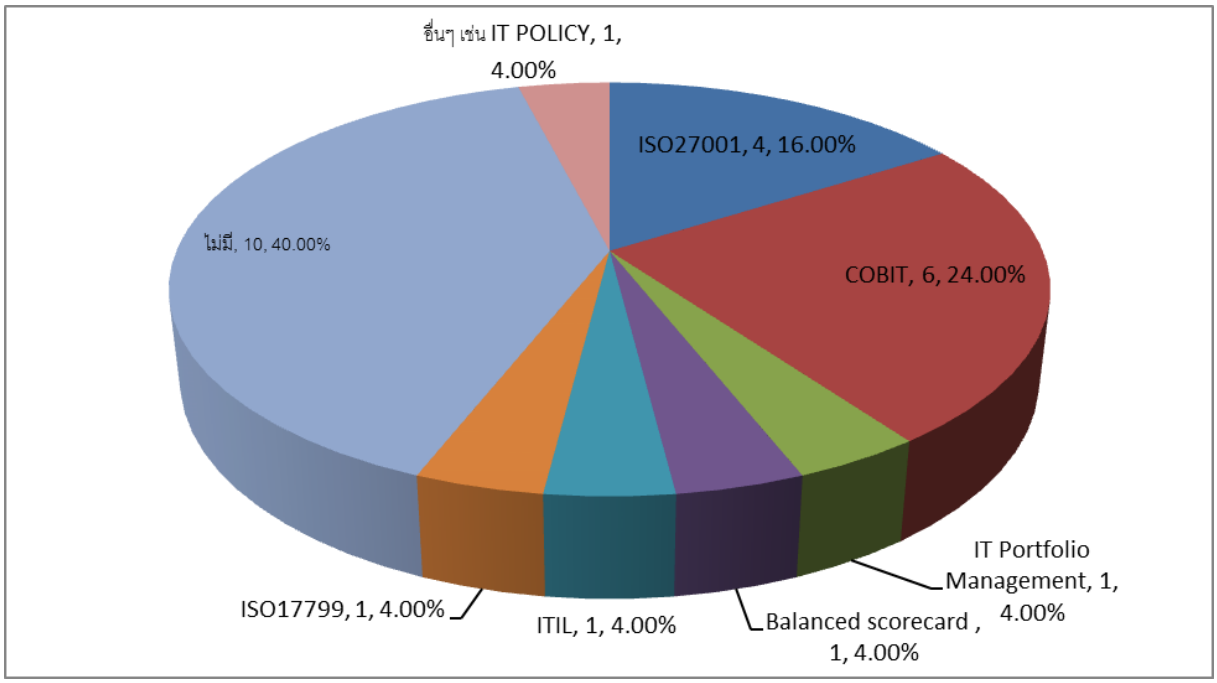
จากตารางที่ 4.7 เรื่องของงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 พบว่าบริษัทที่ยินยอมเปิดเผยข้อมูลทั้งสิ้น 12 บริษัท โดยมีค่างบประมาณทางด้าน IT ต่ำสุดอยู่ที่ 2,000,000.00 บาท สูงสุดอยู่ที่ 400,000,000.00 บาท และมีค่าเฉลี่ยอยู่ที่ 56,000,000.00 บาท ในเรื่องของงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ของบริษัทหลักทรัพย์ ในปี 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

ตารางที่ 4.8 การจัดสรรงบประมาณงบประมาณทางด้าน IT ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 ของบริษัทหลักทรัพย์

ประเภทของงบประมาณ	บริษัทที่มีการเปลี่ยนแปลง							
	เพิ่มขึ้น			ลดลง			ไม่เปลี่ยนแปลง	
	จำนวน	ร้อยละ	ค่าเฉลี่ย %(+)	จำนวน	ร้อยละ	ค่าเฉลี่ย %(-)	จำนวน	ร้อยละ
1.งบประมาณด้าน IT (N=17)	14	66.70	17.33	1	4.80	10.00	2	9.50
2.งบประมาณด้านการรักษาความปลอดภัยด้าน IT (N=11)	3	14.29	10.00	-	-	-	8	38.10
3.งบประมาณด้านการตรวจสอบด้าน IT (N=4)	2	9.52	-	-	-	-	2	9.52

จากตารางที่ 4.8 ในเรื่องของอัตราการจัดสรรงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 พบว่า มีบริษัทหลักทรัพย์ที่ยินยอมให้ข้อมูลจำนวน 17 บริษัท โดยส่วนใหญ่บริษัทมีอัตราการจัดสรรงบประมาณทางด้าน IT ในปี 2012 เพิ่มขึ้นจากปี 2011 คิดเป็นร้อยละ 66.70 โดยเมื่อเปรียบเทียบกับปี 2011 แล้วมีอัตราการเพิ่มขึ้นเฉลี่ยอยู่ที่ร้อยละ 17.33 ในทางกลับกันพบว่า มีบริษัทที่มีอัตราการจัดสรรงบประมาณทางด้าน IT ในปี 2012 ลดลงจากปี 2011 คิดเป็นร้อยละ 4.80 โดยเมื่อเปรียบเทียบกับปี 2011 แล้วมีอัตราการลดลงเฉลี่ยอยู่ที่ร้อยละ 10 นอกจากนี้มีบริษัทคิดเป็นร้อยละ 9.50 ที่มีอัตราการการจัดสรรงบประมาณทางด้าน IT ในปี 2012 ไม่เปลี่ยนแปลงเมื่อเทียบกับปี 2011 ในส่วนของข้อมูลอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 พบว่า มีบริษัทหลักทรัพย์ที่มีการจัดสรรงบประมาณด้านนี้ที่ยินยอมให้ข้อมูลจำนวน 11 บริษัท โดยส่วนใหญ่บริษัทมีอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ในปี 2012 ไม่เปลี่ยนแปลงจากปี 2011 คิดเป็นร้อยละ 38.10 โดยมีบริษัทคิดเป็นร้อยละ 14.29 ที่มีอัตราการจัดสรรงบประมาณทางด้านการรักษาความปลอดภัยทางด้าน IT ในปี 2012 เพิ่มขึ้นจากปี 2011 โดยเมื่อเปรียบเทียบกับปี 2011 แล้วมีอัตราการเพิ่มขึ้นเฉลี่ยอยู่ที่ร้อยละ 10.00 และข้อมูลของอัตราการจัดสรรงบประมาณทางด้านการตรวจสอบทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 เมื่อเปรียบเทียบกับปี 2011 พบว่า มีบริษัทหลักทรัพย์ที่มีการจัดสรรงบประมาณด้านนี้ที่ยินยอมให้ข้อมูลจำนวน 4 บริษัท โดยบริษัทมีอัตราการจัดสรรงบประมาณทางด้านการตรวจสอบทางด้าน IT ในปี 2012 ไม่เปลี่ยนแปลงจากปี 2011 คิดเป็นร้อยละ 9.52 โดยมีบริษัทคิดเป็นร้อยละ 9.52 ที่มีอัตราการจัดสรรงบประมาณทางด้านการตรวจสอบทางด้าน IT ในปี 2012 เพิ่มขึ้นจากปี 2011

ภาพที่ 4.2 สัดส่วนของการใช้เครื่องมือที่ช่วยบริหารจัดการความเสี่ยงทางด้าน IT แบบต่างๆของบริษัทหลักทรัพย์



จากภาพที่ 4.2 เรื่องเครื่องมือที่ช่วยบริหารจัดการความเสี่ยงทางด้าน IT พบว่ามี โดยบริษัทหลักทรัพย์มีการใช้เครื่องมือ Cobit มากที่สุด คิดเป็นร้อยละ 24.00 รองลงมาคือมีการใช้ ISO27001 คิดเป็นร้อยละ 16.00 ลำดับถัดไปคือ IT Portfolio Management, Balanced scoredcard, ITIL, ISO17799 และ เครื่องมืออื่นๆเช่น IT POLICY เท่ากันคิดเป็นร้อยละ 4.00

ตารางที่ 4.9 จำนวน และ ร้อยละ ของวิธีการแบบต่าง ๆในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงทางด้าน IT ที่บริษัทหลักทรัพย์ใช้

วิธีการแบบต่าง ๆในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงทางด้าน IT	ผลการตอบ	
	จำนวน	ร้อยละ
รายงาน	12	12.63
Exception report	5	5.26
Web-dashboard	1	1.05
Priority report	1	1.05
อื่นๆ เช่น paper	2	2.11
อีเมล์	17	17.89
การพูดจา	7	7.37
โทรศัพท์	10	10.53
เอกสารอีเล็กโทรนิกส์	8	8.42
คู่มือนโยบาย	17	17.89
ประกาศ	14	14.74
อื่นๆ เช่น Internet	1	1.05%
รวม	95	100.00

จากตารางที่ 4.9 เรื่องวิธีการแบบต่างๆในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงด้าน IT พบว่า โดยส่วนใหญ่บริษัทหลักทรัพย์ติดต่อสื่อสารด้วยวิธีแบบ อีเมล์ และ การใช้คู่มือนโยบาย เท่ากันคิดเป็นร้อยละ 17.89 รองลงมาคือมีการใช้การประกาศ คิดเป็นร้อยละ 14.74 ลำดับถัดไปคือ การใช้รายงาน คิดเป็นร้อยละ 12.63 โดยจำแนกเป็น Exception report ร้อยละ 5.26, Web-dashboard และ Priority report ร้อยละ 1.05 และ แบบอื่นๆ เช่น Paper ร้อยละ 2.11 รูปแบบการสื่อสารลำดับถัดไปคือ การใช้โทรศัพท์ คิดเป็นร้อยละ 10.53 ลำดับถัดมาคือใช้ เอกสารอีเล็กโทรนิกส์ และ การพูดจา คิดเป็นร้อยละ 8.42 และ 7.37 ตามลำดับ นอกจากนี้ยังมีการใช้วิธีอื่นๆในการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงด้าน IT เช่น การใช้ Internet คิดเป็นร้อยละ 1.05

ภาพที่ 4.10 ข้อมูลรูปแบบโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ (IT Infrastructure)ที่บริษัทหลักทรัพย์ใช้

ทางด้านฮาร์ดแวร์คอมพิวเตอร์						
เครื่อง PC	โน้ตบุ๊ค	เครื่อง Mini	Tablet	เครื่อง Mac	เครื่องเมนเฟรม	อื่นๆ เช่น Power PC
21 (30.00%)	17 (24.29%)	14 (20.00%)	8 (11.43%)	6 (8.57%)	2 (2.86%)	2 (2.86%)

ทางด้านระบบปฏิบัติการ					
Windows	Linux	Unix	Solaris	Mac OS	อื่นๆเช่น VMS, โอซีร่ี, Jbunto, OracleLinux, Aix ระบบปฏิบัติการบน risc 6000
21 (30.00%)	18 (25.71%)	16 (22.86%)	5 (7.14%)	3 (4.29%)	7 (10.00%)

ซอฟต์แวร์ประยุกต์วิสาหกิจ (ระบบ ERP)			
Oracle Application	SAP	J.D. Edwards	อื่นๆ เช่น SON, ซอฟต์แวร์ของไทย
2 (22.22%)	1 (11.11%)	1 (11.11%)	5 (55.56%)

ซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูล						
SQL Server	MS Access	MySQL	DB2	Oracle	Sybase	อื่นๆ เช่น Informix
13 (22.03%)	13 (22.03%)	12 (20.34%)	8 (13.56%)	4 (6.78%)	1 (1.69%)	8 (13.56%)

ระบบเครือข่ายและการสื่อสารระยะไกล	
มีระบบเครือข่ายและการสื่อสารระยะไกล	ไม่มีระบบเครือข่ายและการสื่อสารระยะไกล
19 (90.48%)	2 (9.52%)

การใช้บริการ Outsource ทางด้าน IT	
มีการใช้บริการ Outsource ทางด้าน IT (คือ การพัฒนาระบบสารสนเทศ, ระบบ network, การติดตั้ง เดินสายระบบ กล้องวงจรปิด, PC Support และ Hardware)	ไม่มีการใช้บริการ Outsource ทางด้าน IT
15 (71.43%)	6 (28.57%)

จากตารางที่ 4.10 เรื่องโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ (IT Infrastructure) ซึ่งประกอบไปด้วย 1) ด้านฮาร์ดแวร์คอมพิวเตอร์ ที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการใช้เครื่อง PC คือคิดเป็นร้อยละ 30.00 รองลงมาคือมีการใช้เครื่องโน้ตบุ๊คคิดเป็นร้อยละ 24.29 ลำดับถัดไปคือมีการใช้เครื่อง Mini computer, Tablet, เครื่อง Mac และ Mainframe computer คิดเป็นร้อยละ 20.00, 11.43, 8.57 และ 2.86 ตามลำดับ นอกจากนี้ยังมีบริษัทที่ใช้ฮาร์ดแวร์คอมพิวเตอร์แบบอื่นๆเช่น Power PC คิดเป็นร้อยละ 2.86 2) ด้านระบบปฏิบัติการ ที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์ทุกบริษัทมีการใช้ระบบปฏิบัติการ Windows คือคิดเป็นร้อยละ 30 รองลงมาคือมีการใช้ระบบปฏิบัติการ Linux และ Unix คิดเป็นร้อยละ 25.71 และ 22.86 ตามลำดับ โดยระบบปฏิบัติการที่บริษัท

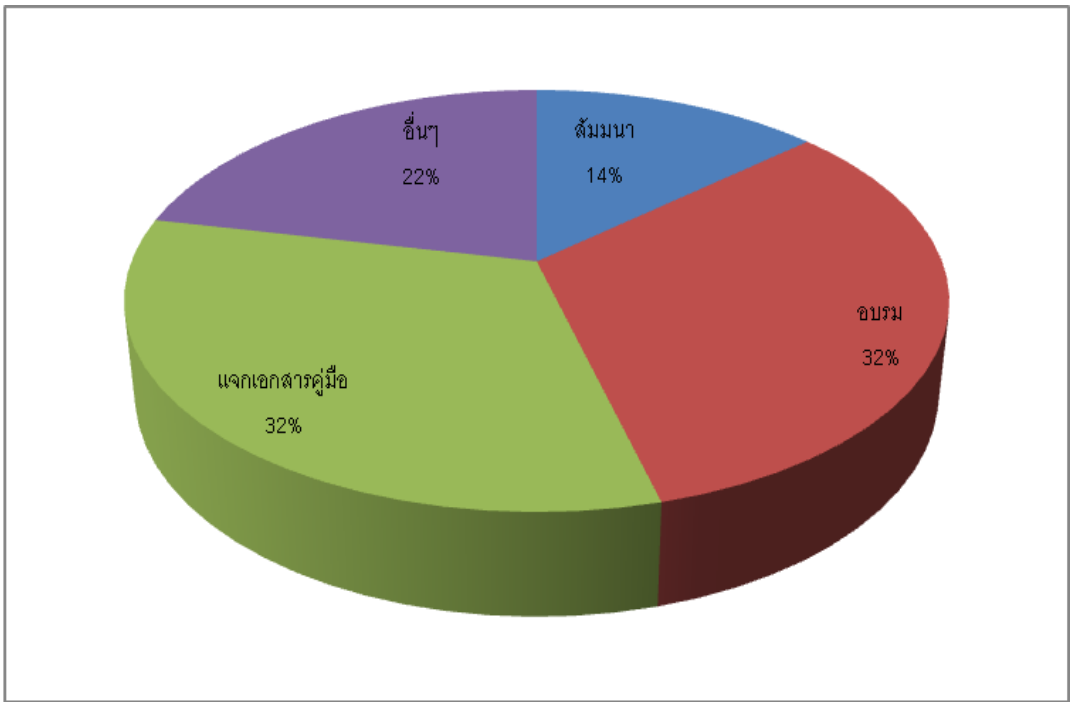
หลักทรัพย์ใช้น้อยที่สุดคือ Mac OS คิดเป็นร้อยละ 4.29 นอกจากนี้ยังมีบริษัทที่ระบบปฏิบัติการแบบอื่นๆเช่น VMS, โอซีรี่, Jbunto, OracleLinux, Aix ระบบปฏิบัติการบน risc 6000 คิดเป็นร้อยละ 10.00 3) ด้านซอฟต์แวร์ประยุกต์วิสาหกิจ (ระบบ ERP) ที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์มีการใช้ซอฟต์แวร์ประยุกต์วิสาหกิจ (ระบบ ERP) อื่น ๆ เช่น SON, ซอฟต์แวร์ของไทย คิดเป็นร้อยละ 55.56 รองลงมาคือมีการใช้ Oracle Application คิดเป็นร้อยละ 22.22 และ มีการใช้ SAP และ J.D. Edwards เท่ากันคือ ร้อยละ 11.11 4) ด้านซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูลที่บริษัทหลักทรัพย์ใช้ พบว่าบริษัทหลักทรัพย์มีการใช้ซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูล SQL Server และ MS Access มากที่สุดคือคิดเป็นร้อยละ 22.03 รองลงมาคือมีการใช้ MySQL คิดเป็นร้อยละ 20.34 โดย Sybase พบว่ามีการใช้น้อยที่สุดคือร้อยละ 1.69 นอกจากนี้ยังมีการใช้ซอฟต์แวร์อื่นๆ เช่น Informix คิดเป็นร้อยละ 13.56 5) ด้านระบบเครือข่ายและการสื่อสารระยะไกล พบว่า ร้อยละ 90.48 ของบริษัทหลักทรัพย์มีระบบเครือข่ายและการสื่อสารระยะไกล มีเพียงร้อยละ 9.52 ที่ไม่มีระบบเครือข่ายและการสื่อสารระยะไกล 6) ด้านการใช้บริการ Outsource ทางด้าน IT พบว่า ร้อยละ 71.43 ของบริษัทหลักทรัพย์มีการใช้บริการ Outsource ทางด้าน IT โดยพบบริษัทร้อยละ 28.57 ที่ไม่มีการใช้บริการ Outsource ทางด้าน IT โดยการใช้บริการ Outsource ที่บริษัทหลักทรัพย์ใช้บริการคือ การพัฒนาระบบสารสนเทศ, ระบบ network, การติดตั้ง เดินสายระบบ กล้องวงจรปิด, PC Support และ Hardware

ตารางที่ 4.11 จำนวน และ ร้อยละ ของบริษัทหลักทรัพย์ที่มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ

	จำนวน	**ร้อยละ**
ไม่มีการให้ความรู้แก่พนักงาน	1	4.80
มีการให้ความรู้แก่พนักงาน	20	95.20
รวม	**21**	**100.00**

จากตารางที่ 4.11 พบว่า ร้อยละ 95.20 ของบริษัทหลักทรัพย์มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ มีเพียงร้อยละ 4.80 ที่ไม่มีการให้ความรู้แก่พนักงาน

ภาพที่ 4.3 แสดงร้อยละของรูปแบบของการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ ของบริษัทหลักทรัพย์



จากภาพรูปที่ 4.3 พบว่ารูปแบบของการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี สิ่งใดที่อนุญาตให้ทำและไม่ ส่วนใหญ่จะเป็นการอบรมและการแจกเอกสารคู่มือคิดเป็นร้อยละ 32 รองลงมาจะเป็นรูปแบบอื่นๆเช่น ผ่านระบบ E-learning, Intranet, การประชุม และ การปฐมนิเทศพนักงานใหม่ คิดเป็นร้อยละ 22 และการจัดสัมมนา คิดเป็นร้อยละ 14

ตอนที่4. การวิเคราะห์ปัจจัยความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

การนำเสนอผลการวิเคราะห์ข้อมูลในเรื่องปัจจัยความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ผู้วิจัยขอกำหนดสัญลักษณ์และอักษรย่อในการวิเคราะห์ข้อมูลดังนี้

ตารางที่ 4.12 สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

$\overline{X}$	หมายถึง ค่าเฉลี่ยเลขคณิตของข้อมูลที่ได้จากกลุ่มตัวอย่าง
S.D.	หมายถึง ค่าส่วนเบี่ยงเบนมาตรฐานของกลุ่มตัวอย่าง
N	หมายถึง จำนวนบริษัทที่ใช้ในการวิเคราะห์
t	หมายถึง ค่าสถิติ t ที่ใช้ในการทดสอบสมมติฐาน
F	หมายถึง ค่าสถิติ F ที่ใช้ในการทดสอบสมมติฐาน
B	หมายถึง ค่าสัมประสิทธิ์การถดถอย
df	หมายถึง ค่าองศาอิสระ
Sum of Squares	หมายถึง ผลรวมของกำลังสองของค่าเบี่ยงเบน
Beta	หมายถึง ประมาณสัมประสิทธิ์การถดถอยมาตรฐาน
Mean Square	หมายถึง ค่าเฉลี่ยของค่าเบี่ยงเบนกำลังสอง
R	หมายถึง ค่าที่แสดงระดับของความสัมพันธ์ระหว่างกลุ่มตัวแปรอิสระทั้งหมดกับตัวแปรตาม ซึ่งเรียกว่า ค่าสัมประสิทธิ์ความสัมพันธ์พหุคูณ
R Square	หมายถึง ประสิทธิภาพการทำนาย
S.E.	หมายถึง ความคลาดเคลื่อนมาตรฐาน
Sig.	หมายถึง ค่าความน่าจะเป็นที่คำนวณได้จากค่าสถิติที่ใช้ในการทดสอบสมมติฐาน
*	หมายถึง มีระดับนัยสำคัญทางสถิติที่ระดับ 0.05

4.1 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยที่มีผลต่อความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในบริษัทหลักทรัพย์ ดังตารางที่ 4.13

ตารางที่ 4.13 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานและระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ความเสี่ยง	$\overline{X}$	S.D.	ระดับ	ลำดับ
1. ข้อมูลที่สำคัญสูญหายหรือถูกขโมย	1.65	0.933	ต่ำ	6
2. การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ตสารสนเทศ	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**	

จากตารางที่ 4.13 พบว่าระดับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้มี 2 ระดับ คือระดับต่ำ และปานกลาง โดยความเสี่ยงที่มีค่าเฉลี่ยสูงสุดคือการต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำให้ คือมีค่าเฉลี่ย 2.38 มีส่วนเบี่ยงเบนมาตรฐาน 1.071 โดยค่าเฉลี่ยความเสี่ยงมีค่าเท่ากับ 1.95 มีส่วนเบี่ยงเบนมาตรฐาน 0.480

4.2 การทดสอบสมมุติฐาน

สมมติฐานที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis)

H_0 : ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศไม่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตารางที่ 4.14 แสดงการวิเคราะห์ความถดถอยอย่างง่ายของปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตัวแปร	B	S.E.	Beta	t	Sig.
ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยง	-0.110	0.046	-0.483	-2.403	0.027*
ค่าคงที่	2.422	0.220		11.020	0.000
R	0.483				
R Square	0.233				
Adjust R Square	0.193				
F	5.773				

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.14 พบว่า ปัจจัยผู้มีส่วนเกี่ยวข้องอันประกอบด้วย Senior manager (CEO, COO), Senior IT manager (CIO), IT operations manager, Information security manager, Risk manager, Internal auditors และ Legal and compliance manager มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.483 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 23.30 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถเขียนสมการทำนายได้ดังนี้

ความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ = 2.422 - 0.110 (ผู้มีส่วนเกี่ยวข้อง)

โดยมีความสัมพันธ์ในทิศทางตรงกันข้ามนั่นคือถ้าผู้มีส่วนเกี่ยวข้องประกอบไปด้วยขึ้นค่าความเสี่ยงก็จะลดลง

สมมติฐานที่ 2 นโยบายการควบคุมความปลอดภัยงานสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์ความถดถอยเชิงพหุคูณ (Multiple Regression Analysis)

H_0 : นโยบายการควบคุมความปลอดภัยงานสารสนเทศไม่ส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : นโยบายการควบคุมความปลอดภัยงานสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตารางที่ 4.15 แสดงการวิเคราะห์ความถดถอยพหุคูณของปัจจัยนโยบายการควบคุมความปลอดภัยงานสารสนเทศที่มีผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตัวแปร	B	S.E.	Beta	t	Sig.
วิธีการควบคุมทางด้านกายภาพ	-0.235	0.098	-0.323	-2.407	0.028*
วิธีการควบคุมทางด้านตรรกะ	-0.170	0.067	-0.348	-2.558	0.020*
วิธีการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ	-0.330	0.092	-0.452	-3.582	0.002*
ค่าคงที่	3.417	0.209		16.321	0.000
R	0.887				
R Square	0.787				
Adjust R Square	0.749				
F	20.897				

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.15 พบว่า ปัจจัยนโยบายควบคุมความปลอดภัยมีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณเท่ากับ 0.887 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 78.70 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 มีตัวแปรในเรื่องการควบคุมความปลอดภัยที่สามารถทำนายความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์เรียงตามลำดับดังนี้ 1) การควบคุมทางกายภาพ 2) การควบคุมทางตรรกะ และ 3) การควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ โดยสามารถเขียนสมการทำนายได้ดังนี้

ความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ = -0.235 (วิธีการควบคุมทางด้านกายภาพ) - 0.170 (วิธีการควบคุมทางด้านตรรกะ) - 0.330 (วิธีการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ)

กล่าวคือเมื่อทดสอบความมีนัยสำคัญที่ระดับ 0.05 พบว่า การควบคุมทางกายภาพ การควบคุมทางตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ ส่งผลทางตรงข้ามต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์นั่นคือถ้ามีการความคุมความปลอดภัยงานสารสนเทศทางด้านกายภาพ, ทางด้านตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติอย่างครบถ้วนความเสี่ยงก็จะลดลง

สมมติฐานที่ 3 งบประมาณส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์ความถดถอยเชิงพหุคูณ (Multiple Regression Analysis)

H_0 : งบประมาณไม่ส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : งบประมาณส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

เนื่องจากว่ามีข้อจำกัดของการเปิดเผยข้อมูลในเรื่องงบประมาณทางด้าน IT งบประมาณทางด้านความปลอดภัย และงบประมาณทางด้านการตรวจสอบของบริษัทหลักทรัพย์ ทำให้ข้อมูลที่เก็บมาได้ไม่เพียงพอต่อการการประมวลผลกล่าวคือมีบริษัทที่ยอมเปิดเผยข้อมูลเรื่องงบประมาณน้อยกว่า 15 บริษัท

สมมติฐานที่ 4 เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่างส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ทดสอบสมมติฐานด้วยวิธีการใช้ค่าสถิติทดสอบทีแบบกลุ่มตัวอย่างไม่สัมพันธ์กัน (t-test Independent Group)

H_0 : เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่างกันส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน

H_1 : เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่างกันส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ตารางที่ 4.16 แสดงค่าความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ระหว่างบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยงและไม่ได้ใช้เครื่องมือ

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

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.16 พบว่าความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ในบริษัทที่ไม่ใช้เครื่องมือในการบริหารความเสี่ยงสูงกว่าบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยง อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 5 ขนาดของบริษัทที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ทดสอบสมมติฐานด้วยวิธีการใช้ค่าสถิติวิเคราะห์ความแปรปรวนแบบทางเดียว (One – Way Anova)

H_0 : ขนาดของบริษัทที่แตกต่างกันส่งผลต่อวามเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน

H_1 : ขนาดของบริษัทที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ตารางที่ 4.17 แสดงค่าเฉลี่ย จำนวน และส่วนเบี่ยงเบนมาตรฐานของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้จำแนกตามขนาดของบริษัท

ขนาดขององค์กร	$\overline{X}$	S.D.	N
เล็ก	1.95	0.459	14
กลาง	1.92	0.612	6
ใหญ่	2.00		1

จากตารางที่ 4.17 พบว่า บริษัทที่มีขนาดใหญ่จะมีค่าเฉลี่ยของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้สูงที่สุดคือมีค่าเฉลี่ย 2.00 โดยบริษัทขนาดกลางจะมีค่าเฉลี่ยของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ต่ำสุดคือมีค่าเฉลี่ย 1.92

ตารางที่ 4.18 แสดงค่าสถิติเปรียบเทียบความแตกต่างของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้จำแนกตามขนาดของบริษัท

แหล่งความแปรปรวน	Sum of Squares	df	Mean Square	F	Sig.
ระหว่างกลุ่ม	0.009	2	0.004	0.017	0.984
ภายในกลุ่ม	4.606	18	0.212		
รวม	4.614	20			

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.18 ผลการทดสอบสมมติฐานระหว่างขนาดของบริษัทกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้พบว่า บริษัทที่มีขนาดที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 6 การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis)

H_0 : การสื่อสารเรื่องความเสี่ยงไม่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตารางที่ 4.19 แสดงการวิเคราะห์ความถดถอยอย่างง่ายของปัจจัยการสื่อสารเรื่องความเสี่ยงที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตัวแปร	B	S.E.	Beta	t	Sig.
การสื่อสารเรื่องความเสี่ยง	- 0.156	0.049	0.589	-3.178	0.005*
ค่าคงที่	2.532	0.204		12.405	0.000
R	0.589				
R Square	0.347				
Adjust R Square	0.313				
F	10.098				

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.19 พบว่า การสื่อสารเรื่องความเสี่ยงอันประกอบด้วย รายงาน, อีเมล์, การพูดจา, โทรศัพท์, เอกสารอีเล็กโทรนิกส์, คู่มือนโยบาย, และ การประกาศ มีความสัมพันธ์กับความเสี่ยงที่เกี่ยงข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.589 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 34.70 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถเขียนสมการทำนายได้ดังนี้

ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ = 2.532 - 0.156 (วิธีการสื่อสารเรื่องความเสี่ยง) โดยมีความสัมพันธ์ในทิศทางตรงข้ามกันนั่นคือถ้าวิธีการสื่อสารเรื่องความเสี่ยงหลากหลายขึ้นค่าความเสี่ยงก็จะลดลง

สมมติฐานที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ทดสอบสมมติฐานด้วยวิธีการใช้ค่าสถิติวิเคราะห์ความแปรปรวนแบบทางเดียว (One – Way Anova)

H_0 : รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน

H_1 : รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ตารางที่ 4.20 แสดงค่าเฉลี่ย จำนวน และส่วนเบี่ยงเบนมาตรฐานของความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้จำแนกตามรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศของบริษัท

รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศ	$\overline{X}$	S.D.	N
Centralization	1.96	0.496	16
Decentralization	2.00		1
Federalism	1.86	0.549	4

จากตารางที่ 4.20 พบว่า บริษัทที่มีรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศแบบ แบบกระจายศูนย์ (Decentralization) จะมีค่าเฉลี่ยของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้สูงที่สุดคือมีค่าเฉลี่ย 2.00 โดยบริษัทที่มีรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศแบบผสม (Federalism แบบผสม) จะมีค่าเฉลี่ยของความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ต่ำสุดคือมีค่าเฉลี่ย 1.86

ตารางที่ 4.21 แสดงค่าสถิติเปรียบเทียบความแตกต่างของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้จำแนกตามรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศของบริษัท

แหล่งความแปรปรวน	Sum of Squares	df	Mean Square	F	Sig.
ระหว่างกลุ่ม	0.025	2	0.013	0.049	0.952
ภายในกลุ่ม	4.589	18	0.255		
รวม	4.614	20			

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.21 ผลการทดสอบสมมติฐานระหว่างรูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้พบว่า บริษัทที่มีรูปแบบที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis)

H_0 : องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศไม่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตารางที่ 4.22 แสดงการวิเคราะห์ความถดถอยอย่างง่ายของปัจจัยองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตัวแปร	B	S.E.	Beta	t	Sig.
องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ	0.388	0.143	0.529	-0.071	0.014*
ค่าคงที่	- 0.052	0.740		2.719	0.944
R	0.529				
R Square	0.280				
Adjust R Square	0.242				
F	7.394				

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.22 พบว่า ปัจจัยองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศอันประกอบด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต และ บริการที่ปรึกษาและการบูรณาการระบบงาน มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.529 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 28.00 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถเขียนสมการทำนายได้ดังนี้

ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ = - 0.052 + 0.388 (องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ) โดยมีความสัมพันธ์ในทิศทางเดียวกันนั่นคือถ้าองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศเพิ่มขึ้นค่าความเสี่ยงก็จะเพิ่มขึ้น

สมมติฐานที่ 9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ทดสอบสมมติฐานด้วยวิธีการวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis)

H_0 : การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติไม่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

H_1 : การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตารางที่ 4.23 แสดงการวิเคราะห์ความถดถอยอย่างง่ายของปัจจัยรูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ตัวแปร	B	S.E.	Beta	t	Sig.
การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ	-0.382	0.067	-0.796	-5.739	0.000*
ค่าคงที่	2.710	0.148		18.271	0.000
R	0.796				
R Square	0.634				
Adjust R Square	0.615				
F	32.937				

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.23 พบว่า ปัจจัยการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติอันประกอบด้วย การสัมมนา, การอบรม, การแจกเอกสารคู่มือ, E-learning, และ Email, มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.796 โดยสามารถ

อธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 63.40 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถเขียนสมการทำนายได้ดังนี้

ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ = 2.710 - 0.382 (รูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ) โดยมีความสัมพันธ์ในทิศทางตรงกันข้ามนั่นคือถ้ารูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติหลากหลายขึ้นค่าความเสี่ยงก็จะลดลง

ตารางที่ 4.24 การสรุปผลการทดสอบสมมติฐาน

สมมติฐาน	ผลการทดสอบ	สถิติที่ใช้
สมมติฐานที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Simple Regression Analysis
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	Simple Regression Analysis
สมมติฐานที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน	ไม่สอดคล้องกับสมมติฐาน	One – Way Anova
สมมติฐานที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Simple Regression Analysis
สมมติฐานที่ 9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์	สอดคล้องกับสมมติฐาน	Simple Regression Analysis

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง “ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย” มีวัตถุประสงค์เพื่อ

1. เพื่อศึกษาถึงความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย
2. เพื่อศึกษาปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย
3. เพื่อสำรวจข้อมูล รวมทั้งการบริหารจัดการของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

ในการดำเนินการวิจัย ผู้วิจัยใช้วิธีวิจัยเชิงปริมาณ (Quantitative Research) โดยผู้วิจัยใช้การสำรวจกึ่งสัมภาษณ์โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูลจากบริษัทหลักทรัพย์ทั้งหมดในประเทศไทยจำนวน 26 บริษัท โดยสามารถเข้าเก็บข้อมูลได้ทั้งสิ้น 21 บริษัท คิดเป็น ร้อยละ 80.77 ซึ่งการเก็บรวบรวมข้อมูลดำเนินการในช่วงระหว่างเดือน ธันวาคม 2555 – มิถุนายน 2556

สถิติที่ใช้ในการวิเคราะห์ข้อมูลคือวิเคราะห์ข้อมูลสถานภาพผู้ตอบ และ ข้อมูลฝ่ายรวมทั้งการบริหารจัดการ IT โดยใช้ความถี่ ร้อยละ(%) ค่าเฉลี่ย ($\overline{X}$) และ ส่วนเบี่ยงเบนมาตรฐาน (S.D.) วิเคราะห์ตัวแปรอิสระ ตัวแปรตาม โดยใช้ค่าเฉลี่ย ($\overline{X}$) และ ส่วนเบี่ยงเบนมาตรฐาน (S.D.) วิเคราะห์ความแตกต่างระหว่างกลุ่มใช้การทดสอบค่าที (t-test) และการทดสอบความแปรปรวนทางเดียว (One-way Anova) วิเคราะห์ตัวแปรอิสระที่ส่งผลต่อต่อตัวแปรตามโดยใช้วิธีการถดถอยอย่างง่าย (Simple Regression Analysis) และ วิธีการถดถอยพหุคูณ (Multiple Regression Analysis)

สรุปผลการวิจัย

1. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย

ผลการวิจัยพบว่าค่าความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับต่ำ (ค่าเฉลี่ย = 1.95, ส่วนเบี่ยงเบนมาตรฐาน = 0.48) โดยพบว่าความเสี่ยงที่มีค่าเฉลี่ยสูงสุด 3 อันดับแรก คือ การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ (ค่าเฉลี่ย = 2.38, ส่วนเบี่ยงเบนมาตรฐาน = 1.07) การขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT (ค่าเฉลี่ย = 2.24, ส่วนเบี่ยงเบนมาตรฐาน = 0.89) การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ต (ค่าเฉลี่ย = 1.90, ส่วนเบี่ยงเบนมาตรฐาน = 0.54) และพบว่าโดยส่วนใหญ่ความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้อยู่ในระดับต่ำ ไม่พบว่ามีความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้อยู่ในระดับสูง

2. ปัจจัยที่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ในประเทศไทย

สรุปผลการทดสอบสมมติฐาน

สมมติฐานที่ 1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อ ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยผู้มีส่วนเกี่ยวข้องอันประกอบด้วย Senior manager (CEO, COO), Senior IT manager (CIO), IT operations manager, Information security manager, Risk manager, Internal auditors และ Legal and compliance manager มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงข้ามกล่าวคือถ้าผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศประกอบไปด้วยหลายฝ่ายขึ้น ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ก็จะลดลง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.483 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 23.30 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 2 นโยบายการควบคุมความปลอดภัยงานสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิเคราะห์ ปัจจัยนโยบายควบคุมความปลอดภัย อันได้แก่ การควบคุมทางกายภาพ, การควบคุมทางตรรกะ และ การควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ พบว่า การควบคุมทางกายภาพ และ การควบคุมทางตรรกะ มีความสัมพันธ์ทางตรงข้ามกับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์กล่าวคือถ้ามีการความคุมความปลอดภัยงานสารสนเทศทางด้านกายภาพ, ทางด้านตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติอย่างครบถ้วนความเสี่ยงก็จะลดลง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.887 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 78.70 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 3 งบประมาณส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ข้อมูลที่เก็บได้ไม่พอเพียงต่อการประมวลผล

สมมติฐานที่ 4 เครื่องมือบริหารความเสี่ยงที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า เครื่องมือที่ใช้ในการบริหารความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ (t = -4.647, Sig = 0.000) โดยความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ในบริษัทที่ไม่ใช้เครื่องมือในการบริหารความเสี่ยงสูงกว่าบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยง อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 5 ขนาดของบริษัทที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า ปัจจัยขนาดของบริษัทไม่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ (F = 0.017, Sig = 0.984)

สมมติฐานที่ 6 การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยการสื่อสารเรื่องความเสี่ยงอันประกอบด้วย รายงาน, อีเมล์, การพูดจา, โทรศัพท์, เอกสารอีเล็กทรอนิกส์, คู่มือนโยบาย, และ การประกาศ มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงข้ามกล่าวคือถ้ามีการสื่อสารเรื่องความเสี่ยงทางด้านเทคโนโลยีสารสนเทศหลากหลายวิธี ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ก็จะลดลง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.589 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 34.70 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศไม่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ (F = 0.049, Sig = 0.952)

สมมติฐานที่ 8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศอันประกอบด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต และ บริการที่ปรึกษาและการบูรณาการระบบงาน มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางเดียวกัน

กล่าวคือถ้าบริษัทมีองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศหลายองค์ประกอบ ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ก็จะเพิ่มขึ้น โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.529 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 28.00 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

สมมติฐานที่ 9 รูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยปัจจัยรูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติอันประกอบด้วย การสัมมนา, การอบรม, การแจกเอกสารคู่มือ, E-learning, และ Email มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงกันข้ามกล่าวคือถ้าบริษัทมีรูปแบบการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยที่หลากหลายความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ก็จะลดลง โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.796 โดยสามารถอธิบายความแปรปรวนของความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ได้ร้อยละ 63.40 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

3. **ข้อมูลรวมทั้งการบริหารจัดการของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย**

ผลการวิเคราะห์

3.1 ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ

พบว่าผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ส่วนใหญ่เป็นเพศชายคิดเป็นร้อยละ 85.70 ส่วนใหญ่คิดเป็นร้อยละ 61.90 มีการศึกษาระดับปริญญาตรี และมีอายุเฉลี่ย 43.74 ปี

3.2 โครงสร้างฝ่ายเทคโนโลยีสารสนเทศ

พบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีการจัดโครงสร้างฝ่ายเทคโนโลยีสารสนเทศแบบรวมศูนย์(มีหน่วยงานเดียวที่สรรหาและเก็บข้อมูลอยู่ที่ส่วนกลาง) คิดเป็นร้อยละ 76.20 โดยจำนวนบุคลากรฝ่าย/แผนกเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ส่วนใหญ่ร้อยละ 57.10 มีจำนวนมากว่า 15 คน ทุกบริษัทมี Data Center(ศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางที่ทำหน้าที่ให้บริการสนับสนุนโครงสร้างทางเทคโนโลยีสารสนเทศประกอบไปด้วยเครื่อง server อุปกรณ์เครือข่าย ฮาร์ดแวร์และซอฟต์แวร์สนับสนุนต่างๆ)และตั้งอยู่ชั้น 2 ขึ้นไป บริษัทหลักทรัพย์ร้อยละ 90.50 มี Disaster Recovery Site (ศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิดจากภัยพิบัติ) โดยส่วนใหญ่ตั้งอยู่ที่สาขา/อาคารอื่น และร้อยละ 81.00 ของบริษัทหลักทรัพย์ที่มีการใช้ระบบสารสนเทศอื่นนอกจากระบบซื้อขายหลักทรัพย์ผ่านอินเตอร์เน็ตมาช่วยในการทำงาน

3.3 การบริหารจัดการของฝ่ายเทคโนโลยีสารสนเทศ

พบว่าผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศที่บริษัทหลักทรัพย์ตอบมากที่สุดคือ Senior IT manager (CIO) คิดเป็นร้อยละ 18.7 บริษัทส่วนใหญ่ร้อยละ 71.43 มีการจัดรูปแบบการกำหนดความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศทั้ง 2 แบบ คือ แบบ top-down (พัฒนาจากข้างบนลงสู่ข้างล่างโดยพิจารณาจากเป้าหมายทางธุรกิจทั้งหมดแล้วทำการวิเคราะห์ IT Risk ที่เกี่ยวข้องหรือมีผลกับความเสี่ยงทางธุรกิจ) และ แบบ bottom-up (กำหนดจากข้างล่างขึ้นสู่ข้างบนโดยระบุจากความเสี่ยงที่มีทั้งหมด) (รายละเอียดจากภาคผนวก ก ตารางที่ 1) บริษัทส่วนใหญ่ถึงร้อยละ 90.48 มีการจัดทำแผนงานระบบเทคโนโลยีสารสนเทศ (รายละเอียดจากภาคผนวก ก ตารางที่ 2) ทุกบริษัทมีการควบคุมความปลอดภัยของงานด้าน IT ทาง

กายภาพ, ทางตรรกะ และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ ในส่วนของงบประมาณทางด้าน IT ของบริษัทหลักทรัพย์ในปี 2012 มีค่าเฉลี่ยอยู่ที่ 56,000,000 บาท โดนส่วนใหญ่คิดเป็นร้อยละ 66.70 มีอัตราของการจัดสรรเพิ่มขึ้นเฉลี่ยจากปี 2011 ร้อยละ 17.33 และบริษัทหลักทรัพย์ส่วนใหญ่มีการจัดสรรในส่วนของงบประมาณด้านการรักษาความปลอดภัยและงบประมาณทางด้านการตรวจสอบด้าน IT คิดเป็นร้อยละ 61.90 และ 57.14 ตามลำดับ

บริษัทหลักทรัพย์ส่วนใหญ่ร้อยละ 52.38 มีการใช้เครื่องมือช่วยในการบริหารความเสี่ยงอันได้แก่ Cobit, ISO27001, IT Portfolio Management, Balanced scoredcard, ITIL, ISO17799 และ IT POLICY นอกจากนี้บริษัทหลักทรัพย์ทุกบริษัทมีการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงทางด้าน IT ในรูปแบบต่างๆ โดยแบบอีเมล์ และ การใช้คู่มือนโยบาย พบมากสุดคิดเป็นร้อยละ 17.89 ในส่วนของโครงสร้างหลักพื้นฐานเทคโนโลยีสารสนเทศ (IT Infrastructure) ที่ทุกบริษัทมีเหมือนกันหมดคือทางด้านฮาร์ดแวร์คอมพิวเตอร์, ระบบปฏิบัติการ, ซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูลและอุปกรณ์บันทึกข้อมูล และระบบอินเตอร์เน็ต แต่ที่บริษัทมีแตกต่างกันคือ การใช้โปรแกรมประยุกต์สำหรับวิสาหกิจ มีบริษัทเพียงร้อยละ 38.09 ที่มีการใช้งาน ส่วนการใช้ระบบเครือข่ายและการสื่อสารระยะไกลมีบริษัทร้อยละ 90.48 ที่มีการใช้งาน และการใช้บริการที่ปรึกษาและการบูรณาการระบบงาน มีบริษัทร้อยละ 71.43 ที่มีการใช้งาน และพบว่าร้อยละ 95.20 ของบริษัทหลักทรัพย์มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำ และไม่อนุญาตให้ทำ

การอภิปรายผล

1. ความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย

จากการวิเคราะห์ค่าความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทย พบว่าอยู่ในระดับต่ำ (ค่าเฉลี่ย = 1.95) โดยพบว่าค่าเฉลี่ยความเสี่ยงเรียงตามลำดับจากมากไปน้อยดังนี้ 1) การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ (ค่าเฉลี่ย = 2.38 ระดับปานกลาง) 2) การขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT (ค่าเฉลี่ย = 2.24 ระดับปานกลาง) 3) การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ต (ค่าเฉลี่ย = 1.90 ระดับปานต่ำ) 4)การหยุดชะงักทางธุรกิจเนื่องมาจาก IT เช่นการเกิดช่วงเวลาที่ไม่สามารถใช้งานได้(downtime) (ค่าเฉลี่ย = 1.81 ระดับปานต่ำ) 5) การสูญเสียรายได้ ทรัพย์สิน(ค่าเฉลี่ย = 1.71 ระดับปานต่ำ) และ 6) ข้อมูลที่สำคัญสูญหายหรือถูกขโมย (ค่าเฉลี่ย = 1.65 ระดับปานต่ำ) ซึ่งสอดคล้องกับที่ IT Policy Compliance Group (2010) ได้ทำการศึกษาถึงความเสี่ยงที่เกี่ยวข้องกับการใช้ IT ที่เกิดขึ้น แต่มีความแตกต่างในเรื่องลำดับ ดังนี้ 1) ความเสี่ยงในเรื่องของข้อมูลที่สำคัญสูญหายหรือถูกขโมย 2) การถูกคุกคามในเรื่องความปลอดภัยบนอินเตอร์เน็ต 3) การหยุดชะงักทางธุรกิจเนื่องมาจากเทคโนโลยีสารสนเทศ 4) สูญเสียรายได้ ทรัพย์สิน 5) การต้องจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้ และ 6) การขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน IT และยังพบว่ามีระดับความเสี่ยงที่สูงกว่า ทั้งนี้ความแตกต่างของลำดับและระดับความเสี่ยงอาจเป็นผลมาจากงานวิจัยของ IT Policy Compliance Group นั้นทำในต่างประเทศอีกทั้งยังทำกับบริษัทที่ไม่ได้อยู่ในอุตสาหกรรมการเงินและการธนาคารทั้งหมด และการที่ไม่พบว่ามีความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในประเทศไทยอยู่ในระดับสูงเลยก็เป็นเพราะบริษัทหลักทรัพย์ในประเทศไทยมีความตระหนักถึงความสำคัญของการรักษาความปลอดภัยรวมทั้งต้องปฏิบัติตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ/น. 32/2552 เรื่องการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ดังจะเห็นได้จากข้อมูลที่สำรวจได้พบว่าทุกบริษัทมี Data Center และ Data Center ส่วนใหญ่ ร้อยละ 76.19 อยู่ชั้น 2 ขึ้นไปเพื่อความปลอดภัยจากภัยพิบัติด้านน้ำท่วม นอกจากนี้บริษัทร้อยละ 90.50 มีศูนย์ที่ทำหน้าที่สำรองและกู้คืนข้อมูลเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิด

จากภัยพิบัติ (Disaster Recovery Site) และยังพบว่าบริษัทร้อยละ 90.48 มีการจัดทำแผนงานระบบ IT อีกทั้งทุกบริษัทยังมีการควบคุมความปลอดภัยทางกายภาพด้าน IT (เป็นต้นว่า ด้านน้ำ ระบบไฟฟ้า ฝุ่น และผู้บุกรุกที่ไม่ได้รับอนุญาต), การควบคุมความปลอดภัยทางตรรกะ(เป็นต้นว่า การควบคุมการเข้าถึงระบบสารสนเทศ, การควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์ม) และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ บริษัทร้อยละ 57.14 มีการจัดสรรงบประมาณด้านการรักษาความปลอดภัย และ บริษัทร้อยละ 61.90 มีการจัดสรรงบประมาณด้านการตรวจสอบด้าน IT บริษัทร้อยละ 52.38 มีการใช้เครื่องมือช่วยบริหารจัดการความเสี่ยง และทุกบริษัทมีการสื่อสารทั้งภายใน/ภายนอกในเรื่องความเสี่ยงด้าน IT นอกจากนี้ทุกบริษัทยังมีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี สิ่งใดอนุญาตให้ทำและไม่อนุญาตให้ทำ ซึ่งสอดคล้องกับการศึกษาของ Aguilar (2011) ที่กล่าวไว้ว่าบริษัทด้านการเงินต้องทำงานอย่างหนักและต้องตระหนักถึงในเรื่องความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ โดยเฉพาะในเรื่องความปลอดภัยของข้อมูล

2. ปัจจัยความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

2.1 ผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่าผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศมีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงข้าม ที่ระดับ 0.483 กล่าวคือผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศประกอบไปด้วยหลายฝ่าย(Senior manager (CEO, COO), Senior IT manager (CIO), IT operations manager, Information security manager, Risk manager, Internal auditors และ Legal and compliance manager) ความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศก็จะลดลง ซึ่งสอดคล้องการศึกษาของ IT Policy Compliance Group (2008) ที่กล่าวไว้ว่า คณะกรรมการที่กำกับดูแลระบบเทคโนโลยีสารสนเทศควรประกอบไปด้วยผู้บริหารระดับสูงและสมาชิกจากฝ่ายทางธุรกิจ การเงิน กฎหมาย IT การกำกับดูแล และการตรวจสอบภายใน และยังสอดคล้องกับผลงานวิจัยอีกชิ้นหนึ่งของ IT Policy Compliance Group (2010) ที่ยืนยันว่าบุคคลที่เกี่ยวข้องในการบริหารจัดการคุณค่า ความเสี่ยงและกำกับดูแลสำหรับ IT เพื่อให้ได้ผลลัพธ์ในการดำเนินงานที่ดี ประกอบไปด้วย ผู้จัดการฝ่าย IT ผู้จัดการฝ่ายกฎหมายและกำกับดูแลการทำงาน ผู้จัดการธุรกิจฝ่ายต่างๆ ผู้ตรวจสอบภายใน และผู้จัดการงานบริหารความเสี่ยง

นอกจากนี้จากการวิจัยยังพบว่าบริษัทหลักทรัพย์ในประเทศไทยส่วนใหญ่ ผู้บริหารระดับสูงเข้ามามีส่วนร่วมในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ โดยพบว่า Senior IT manager (CIO) เข้ามามีส่วนร่วมมากที่สุดถึงร้อยละ 18.7 รองลงมาคือ Senior manager (CEO, COO) และ Internal auditors เท่ากันคือร้อยละ 15.4 ซึ่งสอดคล้องกับการศึกษาของ ISACA(2009) ที่กล่าวไว้ว่า ผู้บริหารระดับสูงจะต้องเข้ามามีส่วนร่วมและไม่มองว่า IT Risk เป็นงานของฝ่ายเทคโนโลยีสารสนเทศหรือเป็นเรื่องทางเทคนิคอย่างเดียว และการศึกษาของ Reinhold, Doherty, Higgins (2011) ที่กล่าวไว้อย่างสอดคล้องว่า ผู้บริหารระดับสูงจำเป็นต้องพิจารณาหรือประเมินการบริหารความเสี่ยงอย่างดี ความเข้มแข็งและความมีพลังของผู้บริหารระดับสูงมีความสำคัญมากในการบริหารจัดการความเสี่ยง

2.2 นโยบายการควบคุมความปลอดภัยงานสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

จากนโยบายควบคุมความปลอดภัยงานสารสนเทศ อันได้แก่ การควบคุมทางกายภาพ, การควบคุมทางตรรกะและการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติ ผลการวิจัยพบว่า การควบคุมทางกายภาพ และ การควบคุมทางตรรกะ มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงข้ามที่ระดับ 0.887 กล่าวคือบริษัทที่มีการควบคุมทางกายภาพครบถ้วนทั้งด้านอัคคีภัย (มีระบบแจ้งเตือนภัย, มีอุปกรณ์ฉีดดับเพลิง, มีแผนผังแสดงจุดที่ตั้งของระบบดับเพลิง, ตึกที่เป็นที่ตั้งอุปกรณ์และทรัพย์สินใช้อุปกรณ์กันไฟและโครงสร้างตึกกันไฟ, สัญญาณเตือนภัยเชื่อมต่อยังสถานีดับเพลิง, อุปกรณ์เชื้อไฟเก็บในห้องแยก, สายไฟมีฉนวนหุ้มป้องกัน, มีการฝึกซ้อมระบบป้องกันอัคคีภัย), น้ำ (มีหลังคา ผนัง พื้น ป้องกันการรั่วซึม, มีทางระบายน้ำที่เหมาะสม, มีการติดตั้งสัญญาณเตือนภัยเชื่อมต่อกับเครื่องตรวจจับ, เก็บทรัพย์สินระบบสารสนเทศอยู่ในชั้นที่น้ำท่วมไม่ถึง, มีข้อห้ามพนักงานนำเครื่องดื่มเข้าใกล้คอมพิวเตอร์และอุปกรณ์), ระบบไฟฟ้า (มีการติดตั้งอุปกรณ์ตัดไฟ, มีอุปกรณ์สำรองไฟหรือ UPS), ฝุ่น (มีการดูดฝุ่นอยู่เสมอ, มีพื้นห้องและพรมแบบกันฝุ่น), และจากผู้บุกรุก (ศูนย์คอมพิวเตอร์มีประตูแข็งแรงและมีสัญญาณเตือนภัย, มีการจำกัดการเข้าออก, เก็บดิสก์หรือเทปที่บันทึกข้อมูลเข้าตู้ล็อกกุญแจ) มีการควบคุมทางตรรกะครบถ้วนทั้งด้านการควบคุมการเข้าถึงระบบสารสนเทศ (มีการระบุผู้ใช้และพิสูจน์ผู้ใช้ที่แท้จริง, มีการกำหนดนโยบายการใช้ password, มีการกำหนดสิทธิอำนาจการใช้งานของผู้ใช้แต่ละคน, มีการบันทึกข้อมูลการใช้งาน, มีระเบียบกำหนดเกี่ยวกับการให้เปลี่ยนแปลง และยกเลิกรหัสผู้ใช้), การควบคุมและป้องกันไวรัสคอมพิวเตอร์และเวิร์ม (มีการป้องกัน ตรวจหา แก้ไข, มีการให้ความรู้แก่ผู้ใช้เกี่ยวกับอันตรายของไวรัสและการป้องกัน, แต่ละหน่วยงานร่วมกันกำหนดวิธีการควบคุมการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ในเครือข่าย) มีการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติครบถ้วนทั้งด้านการมีแผนในการฟื้นสภาพระบบจากภัยพิบัติ (มีแผนฉุกเฉิน, มีแผนสำรอง, มีแผนฟื้นสภาพ, มีแผนทดสอบ), มีการทำประกันภัย (ทำประกันอุปกรณ์ฮาร์ดแวร์, ทำประกันที่เก็บสื่อ, ทำประกันความหยุดชะงักทางธุรกิจ, ทำประกันเอกสารสำคัญ) บริษัทจะมีความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ต่ำ ซึ่งสอดคล้องกับการศึกษาของ IT Policy Compliance Group(2010) ที่พบว่าการควบคุมความปลอดภัยของสารสนเทศ จะช่วยป้องกันการรั่วไหลของข้อมูลที่สำคัญได้ ด้วยการกำหนดและจัดกลุ่มข้อมูลที่สำคัญ, ระบุถึงเครื่องมืออุปกรณ์ที่เข้าถึงข้อมูลที่สำคัญ, มีการดูแลบำรุงรักษาข้อมูลที่สำคัญและอุปกรณ์เครื่องมือในการเข้าถึง, มีการตรวจจับและป้องกันการรั่วไหลของข้อมูล และการควบคุมความปลอดภัยในการใช้ข้อมูลที่สำคัญบนเครื่อง PC และบนเครื่องคอมพิวเตอร์พกพาต่างๆ ในทำนองเดียวกันจากงานศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) พบว่าการมีนโยบายหรือแผนควบคุมความปลอดภัยของงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ โดยการมีแผนการฟื้นสภาพของระบบจากภัยพิบัติ (DRP) , การควบคุมความเสี่ยงจากภัยธรรมชาติ, จากผู้บุกรุกที่ไม่ได้รับอนุญาต, การควบคุมการเข้าถึงระบบสารสนเทศ, การควบคุมความปลอดภัยของข้อมูล, การควบคุมและการป้องกันไวรัสคอมพิวเตอร์จะช่วยลด IT Risk ได้

2.3 งบประมาณส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

เนื่องจากข้อมูลในเรื่องงบประมาณด้าน IT ในปี 2012 ของบริษัทหลักทรัพย์ที่เก็บได้นั้นไม่พอเพียงต่อการประมวลผลทั้งนี้เนื่องจากบริษัทหลักทรัพย์ให้เหตุผลว่าข้อมูลเป็นความลับไม่สามารถเปิดเผยได้ ทั้งนี้พบว่าบริษัทส่วนใหญ่มีการจัดสรรงบประมาณ แต่มีบริษัทที่ยินยอมเปิดเผยข้อมูลงบประมาณด้าน IT จำนวน 12 บริษัท งบประมาณด้านการรักษาความปลอดภัยทางด้าน IT จำนวน 8 บริษัท และงบประมาณด้านการตรวจสอบด้าน IT จำนวน 2 บริษัท

2.4 เครื่องมือที่ใช้ในการบริหารความเสี่ยงที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า บริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยงอันประกอบด้วย ISO 27001, COBIT, IT Portfolio Management, Balanced scorecard, ITIL และ ISO 17799 ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ โดยความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทที่ไม่ใช้เครื่องมือในการบริหารความเสี่ยงมีค่าสูงกว่าบริษัทที่ใช้เครื่องมือในการบริหารความเสี่ยง ทั้งนี้การใช้เครื่องมือมาช่วยในการบริหารความเสี่ยงจะช่วยให้บริษัทมีหลักปฏิบัติที่ดีสำหรับการควบคุมข้อมูล, สารสนเทศและความเสี่ยงที่เกี่ยวข้องอื่นๆ ช่วยลดปัญหาอันเกิดจากภัยคุกคามต่างๆ และบริษัทยังสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับงานวิจัยของ Policy Compliance Group (2010) ที่กล่าวไว้ว่าการใช้เครื่องมือทางการบริหารเป็นต้นว่า ISO 27001, CIS benchmarks, COBIT, IT portfolio management, และ Balanced Scorecards ช่วยให้ความเสี่ยงนั้นลดลง ในขณะที่ผลการสำรวจองค์กรที่อยู่ในอุตสาหกรรมทางการเงินทั่วโลกของ Ernst & Young(2008) พบว่าเครื่องมือที่ใช้คือ COBIT, ITIL, ISO 17799, SOX, COSO ตามลำดับ

2.5 ขนาดของบริษัทที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า ปัจจัยขนาดของบริษัทไม่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ซึ่งขัดแย้งกับการศึกษา ของ IT Policy Compliance Group(2010) ที่พบว่าบริษัทที่มีขนาดเล็กซึ่งวัดจากผลประกอบการทั้งปีส่วนใหญ่ จะเผชิญกับความเสี่ยงสูงกว่าบริษัทขนาดกลางและขนาดใหญ่เนื่องจากบริษัทขนาดเล็กมักจะลดงบประมาณค่าใช้จ่ายทางด้าน IT ลง การที่ผลการวิจัยไม่สอดคล้องกันนั้นทั้งนี้อาจเป็นเพราะว่าผู้วิจัยไม่สามารถจำแนกขนาดของบริษัทหลักทรัพย์ตามผลประกอบการประจำปีได้เป็นเพราะบริษัทที่เปิดเผยข้อมูลผลประกอบการในเว็บไซต์ของตลาดหลักทรัพย์มีเพียง 11 บริษัทเท่านั้น ดังนั้นผู้วิจัยจึงแบ่งขนาดของบริษัทจากยอดสรุปการซื้อขายหลักทรัพย์ทั้งปีในปี 2011 ซึ่งอาจส่งผลให้การวิเคราะห์ผลถูกต้องไม่สมบูรณ์

2.6 การสื่อสารเรื่องความเสี่ยงส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยการสื่อสารเรื่องความเสี่ยงอันประกอบด้วย รายงาน, อีเมล์, การพูดจา, โทรศัพท์, เอกสารอีเล็กโทรนิกส์, คู่มือนโยบาย, และ การประกาศ มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงข้ามที่ระดับ 0.589 กล่าวคือถ้ามีการสื่อสารเรื่องความเสี่ยงทางด้านเทคโนโลยีสารสนเทศประกอบไปด้วยหลายวิธี ความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศก็จะลดลง ซึ่งสอดคล้องกับ นวพร เรืองสกุล (2553) ได้กล่าวไว้ว่าวิธีการสื่อสารอาจมาได้หลายรูปแบบเช่นในรูปของคู่มือนโยบาย บันทึก จดหมายอิเล็กทรอนิกส์ บอร์ดติประกาศ ประกาศเตือน การสื่อสารทางเว็บ การสื่อสารด้วยวาจา นอกจากนี้ยังสอดคล้องกับงานวิจัยของ IT Policy Compliance Group(2010) ที่พบว่าการสื่อสารและการแบ่งปันของมูลเกี่ยวกับคุณค่า ความเสี่ยงและการกำกับดูแลที่เกี่ยวกับการใช้ IT ที่ได้ผลลัพธ์ดีควรจะใช้วิธีต่างๆ ดังนี้ Email, การพูดจา, dashboard และ scorecard, รายงานและข้อสรุปที่ได้จากฐานข้อมูล การใช้เพียงการโทรศัพท์ Email และเอกสารอิเล็กทรอนิกส์ แล้วเน้นการแจ้งเฉพาะเวลามีเหตุร้ายนั้นจะทำให้ผลลัพธ์ที่ออกมาไม่ดี

2.7 รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศที่แตกต่างกันส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์แตกต่างกัน

ผลการวิจัยพบว่า รูปแบบการจัดโครงสร้างแผนกเทคโนโลยีสารสนเทศไม่มีผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ซึ่งจากการศึกษาของ Co and Fink (2010) พบว่าโครงสร้างแบบ Decentralization หรือแบบกระจายศูนย์ โดยในแผนกต่างๆมี IT เป็นผู้ดูแลในหน่วยงานของตน จะมีความเสี่ยงสูงกว่า เนื่องจากการควบคุม IT เป็นไปได้ยาก การที่ผลออกมาขัดแย้งกันนี้น่าจะมาจากบริษัทหลักทรัพย์เกือบทุกบริษัทคิดเป็นร้อยละ 95.20 มีการจัดโครงสร้างแบบ Centralization และ Federalism แสดงให้เห็นว่าบริษัทเหล่านี้ตระหนักถึงปัญหาของการจัดโครงสร้างแบบ Decentralization เป็นอย่างดี เพราะรูปแบบวิธีปฏิบัติงานและการบริหารจะแตกต่างกันบางแห่งอาจไม่ได้มาตรฐานพอ นอกจากนี้ยังอาจทำให้การควบคุมดูแลไม่ทั่วถึง ทำให้เกิดผลเสียหายได้ จากการสำรวจพบเพียง 1 บริษัทเท่านั้นที่มีการจัดโครงสร้างแบบ Decentralization

2.8 องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า ปัจจัยองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศอันประกอบด้วย โครงสร้างพื้นฐานฮาร์ดแวร์คอมพิวเตอร์, โครงสร้างพื้นฐานระบบปฏิบัติการ, โปรแกรมประยุกต์สำหรับวิสาหกิจ, การบริหารจัดการระบบฐานข้อมูล, ระบบเครือข่ายและการสื่อสารระยะไกล, ระบบอินเตอร์เน็ต และ บริการที่ปรึกษาและการบูรณาการระบบงาน มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางเดียวกันที่ระดับ 0.529 กล่าวคือถ้าบริษัทมีองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศหลายองค์ประกอบ ความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศก็จะเพิ่มขึ้น

จากการวิจัยยังพบว่าโครงสร้างหลักเทคโนโลยีสารสนเทศที่ทุกบริษัทมีเหมือนกันคือ มีการใช้ฮาร์ดแวร์คอมพิวเตอร์, ระบบปฏิบัติการ ซอฟต์แวร์สำหรับบริหารจัดการฐานข้อมูลและอุปกรณ์บันทึกข้อมูล และระบบอินเตอร์เน็ต แต่ที่บริษัทมีแตกต่างกันคือ การใช้โปรแกรมประยุกต์สำหรับวิสาหกิจ, การใช้ระบบเครือข่ายและการสื่อสารระยะไกล และการใช้บริการที่ปรึกษาและการบูรณาการระบบงาน ซึ่งสอดคล้องกับการศึกษาของ Fheili (2011) ที่พบว่าการ outsource บริการทางด้าน IT เพิ่มขึ้น นำมาสู่ความเสี่ยงทางด้าน IT ได้ ซึ่งการใช้โปรแกรมประยุกต์สำหรับวิสาหกิจเป็นต้นว่า SAP หรือ Oracle Application บริษัทจำเป็นต้อง outsource ใช้บริการบริษัทที่ปรึกษาในการติดตั้ง ซึ่งนำมาซึ่งความเสี่ยงได้ นอกจากนี้ ยังสอดคล้องกับการศึกษาของ Bandyopadhyay, Mykytyn P., Mykytyn K. (1999) ที่กล่าวว่าโครงสร้างหลักเทคโนโลยีสารสนเทศมีผลต่อความเสี่ยงทางด้าน IT โดยเฉพาะถ้าองค์กรมี ระบบเครือข่ายและการสื่อสารระยะไกล ดังนั้นบริษัทที่มีโครงสร้างหลักเทคโนโลยีที่เพิ่มขึ้นในส่วนของการใช้โปรแกรมประยุกต์สำหรับวิสาหกิจ, การใช้ระบบเครือข่ายและการสื่อสารระยะไกล และการใช้บริการที่ปรึกษาและการบูรณาการระบบงาน ก็จะมีความเสี่ยงเพิ่มขึ้นด้วย

2.9 การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์

ผลการวิจัยพบว่า การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติอันประกอบด้วย การสัมมนา, การอบรม, การแจกเอกสารคู่มือ, E-learning, และ Email มีความสัมพันธ์กับความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ในทิศทางตรงกันข้ามที่ระดับ 0.796 กล่าวคือถ้าบริษัทมีรูปแบบการให้

ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยที่หลากหลายความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ก็จะลดขึ้น ดังจะเห็นได้จากบริษัทหลักทรัพย์เกือบทุกบริษัทคิดเป็นร้อยละ 95.20 มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติในรูปแบบต่างๆกัน ทั้งนี้เนื่องจากการให้ความรู้แก่พนักงานจะช่วยให้พนักงานทราบถึงนโยบายและกฎเกณฑ์ข้อบังคับต่างๆในเรื่องความปลอดภัยของบริษัท ซึ่งจะช่วยลดความผิดพลาดอันเกิดจากความไม่รู้หรือการใช้งานอย่างไม่ถูกต้องของพนักงาน ซึ่งสอดคล้องกับการศึกษาของ IT Policy Compliance Group(2010) ที่พบว่าพฤติกรรมของคน เช่นความผิดพลาด การละเลยไม่ปฏิบัติตามขั้นตอน การใช้งานอย่างไม่ถูกต้อง และการทุจริตการขโมยข้อมูล ก่อให้เกิดอันตรายต่อการใช้ระบบเทคโนโลยีสารสนเทศ ดังนั้นการให้การอบรม และ เอกสารรายงานแก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ ที่จะช่วย ลดปัญหาและอันตรายที่เกิดจากการใช้ IT ลง

3. ข้อมูลรวมทั้งการบริหารจัดการของฝ่ายเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทย

ผลการสำรวจพบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีโครงสร้างและการบริหารจัดการ รวมทั้งการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ดีสอดคล้องกับประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โดยพบว่าบริษัทหลักทรัพย์ส่วนใหญ่มีการจัดโครงสร้างฝ่ายเทคโนโลยีสารสนเทศแบบรวมศูนย์ซึ่งจากการศึกษาของ Co and Fink (2010) พบว่ามีความเสี่ยงต่ำกว่าแบบกระจายศูนย์ นอกจากนี้ทุกบริษัทยังมี Data Center (ศูนย์ข้อมูลเทคโนโลยีสารสนเทศเป็นศูนย์กลางที่ทำหน้าที่ให้บริการสนับสนุนโครงสร้างทางเทคโนโลยีสารสนเทศประกอบไปด้วยเครื่อง server อุปกรณ์เครือข่าย ฮาร์ดแวร์และซอฟต์แวร์สนับสนุนต่างๆ)และตั้งอยู่ชั้น 2 ขึ้นไป ซึ่งอยู่ในชั้นที่น้ำท่วมไม่ถึง บริษัทหลักทรัพย์ร้อยละ 90.50 มี Disaster Recovery Site เพื่อสำรองข้อมูลและระบบคอมพิวเตอร์ของบริษัทหลักทรัพย์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันต่อเหตุการณ์ โดยส่วนใหญ่จะตั้งอยู่ที่สาขา/อาคารอื่น นอกจากนี้ยังพบว่าผู้บริหารระดับสูงเข้ามามีส่วนร่วมโดยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศที่บริษัทหลักทรัพย์ตอบมากที่สุดคือ Senior IT manager (CIO) และ Senior manager (CEO, COO) คิดเป็นร้อยละ 18.7 และ 15.4 ตามลำดับ ซึ่งสอดคล้องกับการศึกษาของ ISACA (2009) ที่กล่าวไว้ว่า ผู้บริหารระดับสูงจะต้องเข้ามามีส่วนร่วมและไม่มองว่า IT Risk เป็นงานของฝ่ายเทคโนโลยีสารสนเทศหรือเป็นเรื่องทางเทคนิคอย่างเดียว บริษัทหลักทรัพย์ส่วนใหญ่ถึงร้อยละ 90.48 มีการจัดทำแผนงานระบบเทคโนโลยีสารสนเทศ (รายละเอียด ตารางที่ 1 ภาคผนวก ก) ทุกบริษัทยังมีการควบคุมความปลอดภัยของงานสารสนเทศด้านกายภาพ, ตรรกะ และการควบคุมการฟื้นสภาพของระบบจากภัยพิบัติอย่างเพียงพอแก่การป้องกันไม่ให้บุคคลภายนอกที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ และยังจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆอีกด้วย บริษัทหลักทรัพย์ร้อยละ 52.38 มีการใช้เครื่องมือช่วยในการบริหารความเสี่ยงอันได้แก่ Cobit, ISO27001, IT Portfolio Management, Balanced scorecard, ITIL, ISO17799 และ IT POLICY ซึ่งจากการศึกษาของ IT Policy Compliance Group (2010) พบว่าจะช่วยลดความเสี่ยงลงได้นอกจากนี้บริษัทหลักทรัพย์ทุกบริษัทมีการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงทางด้าน IT ในรูปแบบต่างๆ โดยแบบ อีเมล์ และ การใช้คู่มือนโยบาย พบมากสุดคิดเป็นร้อยละ 17.89 และพบว่าร้อยละ95.20 ของบริษัทหลักทรัพย์มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย, แนวปฏิบัติที่ดี, สิ่งใดที่อนุญาตให้ทำและไม่อนุญาตให้ทำ ซึ่งจากการศึกษาของ IT Policy Compliance Group (2010) พบว่าจะช่วยลดปัญหาและอันตรายที่เกิดจากการใช้ IT ลงได้

ข้อเสนอแนะ

ข้อเสนอแนะจากการวิจัย

1. จากผลการวิจัยพบว่าผู้บริหารฝ่าย IT ของบริษัทหลักทรัพย์ทุกบริษัททราบถึงระดับความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศของบริษัทตัวเอง ไม่พบบริษัทใดที่ไม่ทราบ โดยพบว่าความเสี่ยงอันเกิดจากการต้องว่าจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้(outsource)อยู่ในระดับสูงสุด โดยร้อยละของบริษัทที่มีการใช้บริการ outsource มีถึงร้อยละ 71.43 ถึงแม้การจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้จะมีข้อดีหลายประการเป็นต้นว่าช่วยลดต้นทุน เพราะอาจไม่คุ้มค่าที่บริษัทจะลงทุนเองเพราะการดำเนินการโดยใช้เทคโนโลยีสารสนเทศเข้าช่วยในองค์กรเป็นการลงทุนที่สูง อีกทั้งบริษัท outsourcing มักจะมีความรู้ที่เกิดจากประสบการณ์ในการให้บริการกับลูกค้าหลายราย และมีบุคคลากรที่มีความรู้เฉพาะทางในด้าน IT ทำให้สามารถดำเนินงานได้อย่างมีมาตรฐานและมีคุณภาพสูงกว่าการที่บริษัทจะทำเองรวมทั้งยังช่วยแก้ปัญหาการขาดแคลนบุคลากรที่มีความเชี่ยวชาญทางด้าน ITของบริษัท อย่างไรก็ตามบริษัทอาจต้องเผชิญความเสี่ยงในเรื่องการเปิดเผยข้อมูลสำคัญบางอย่างให้แก่บริษัท outsourcing เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน นอกจากนี้ยังอาจมีความเสี่ยงที่ผลงานของบริษัท outsourcing จะไม่เป็นไปตามที่ต้องการ ทำให้ต้องเสียเวลาในการแก้ไข ซึ่งอาจส่งผลเสียหายต่องานโดยรวมของบริษัทได้ ดังนั้นบริษัทจะต้องคำนึงถึงคือผู้ให้บริการ(outsource) ควรเป็นบริษัทที่มีความชำนาญและมีประสบการณ์ในการให้บริการด้าน outsource ต้องเป็นบริษัทที่น่าเชื่อถือ และเคยมีผลงานปรากฏเด่นชัดและควรพิจารณาถึงขอบเขตและระดับการให้บริการอย่างรอบคอบ

2. จากผลการวิจัยพบว่า บริษัทหลักทรัพย์ในประเทศไทยส่วนใหญ่มีการบริหารจัดการของฝ่ายเทคโนโลยีสารสนเทศที่ดีไม่ว่าจะเป็นการจัดโครงสร้างฝ่ายเทคโนโลยีสารสนเทศ มีการติดต่อสื่อสารทั้งภายใน/ภายนอกในเรื่องของความเสี่ยงทางด้าน มีการให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัย รวมทั้งการที่ผู้บริหารระดับสูงเข้ามามีส่วนร่วมและเห็นความสำคัญ อย่างไรก็ตามยังพบบริษัทที่ไม่มี Disaster Recovery Site เพื่อสำรองข้อมูลและกู้คืนข้อมูลหลังภัยพิบัติ ซึ่งในประเทศไทยมีการกำหนดโดยธนาคารแห่งประเทศไทยให้สถาบันการเงินต้องมีศูนย์นี้แต่อาจเนื่องจากปัญหาทางเศรษฐกิจจึงมีการผ่อนผัน รวมทั้งอาจมองว่าประเทศไทยมีอัตราการเกิดภัยพิบัติต่ำ แต่ในปัจจุบันประเทศไทศไทยได้เผชิญกับภัยพิบัติเพิ่มขึ้นทั้ง แผ่นดินไหว คลื่นสึนามิ และน้ำท่วม เป็นต้น ดังนั้นบริษัทไม่ควรชะล่าใจและควรนำไปปฏิบัติอย่างจริงจังเพื่อจะได้ช่วยลดความเสี่ยง และทำให้บริษัทสามารถดำเนินงานได้อย่างต่อเนื่องแม้ในยามที่ประสบภัยพิบัติ

3. จากผลการวิจัยพบว่า ปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ, นโยบายการควบคุมความปลอดภัย, เครื่องมือที่ใช้ในการบริหารความเสี่ยง, การสื่อสารเรื่องความเสี่ยง, องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ และ การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ เป็นตัวแปรที่ส่งผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ ดังนั้นบริษัทหลักทรัพย์ควรตระหนักและให้ความสำคัญต่อปัจจัยเหล่านี้รวมทั้งมีการจัดการบริหารความเสี่ยง สร้างมาตรฐานทางด้านเทคโนโลยีสารสนเทศ เพื่อก้าวให้ทันต่อการเปลี่ยนแปลงที่อาจเกิดขึ้นได้ในการดำเนินธุรกิจ โดยต้องสร้างทัศนคติจากผู้บริหารระดับสูงจนถึงทุกฝ่ายที่เกี่ยวข้องให้มีจิตสำนึก ถึงความสำคัญต่อการรักษาความปลอดภัยและสร้างมาตรฐานทางด้านเทคโนโลยีสารสนเทศ จะได้เป็นเครื่องยืนยันถึงความน่าเชื่อถือและความมีประสิทธิภาพในการบริหารจัดการความเสี่ยงของบริษัทตลอดจนสร้างความเชื่อมั่นไว้ใจให้กับลูกค้าได้อย่างชัดเจน นอกจากนี้ยังพบว่าจากผลการสอบถามความคิดเห็นของผู้บริหารด้าน IT ของบริษัทหลักทรัพย์ที่มีต่อปัจจัยเหล่านี้ (รายละเอียด ตารางที่ 4 ภาคผนวก ก) พบว่าสอดคล้องกันกล่าวคือ ผู้บริหารด้าน IT เห็นว่าปัจจัยเหล่านี้ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัท

อย่างไรก็ตามในส่วนของปัจจัยเครื่องมือที่ใช้ในการบริหารความเสี่ยงถึงแม้จะพบว่าส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้แต่บริษัทยังมีการนำมาใช้ค่อนข้างจำกัด ดังนั้นบริษัทควรพิจาราณานำเครื่องมือหรือมาตรฐานเหล่านี้มาใช้เพราะเครื่องมือหรือมาตรฐานเหล่านี้ไม่ว่าจะเป็น ISO27001/ISO17799 , Cobit , IT Portfolio Management, Balanced scorecard, ITIL, ISO17799 และ IT POLICY นั้นมีประโยชน์มาก โดยสามารถนำมาเป็นแนวทางหรือวิธีการในการกำหนดนโยบาย กระบวนการทำงาน และควบคุมความเสี่ยง และนำไปสู่ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศในองค์กร รวมทั้งสามารถดำเนินงานตามมาตรฐานความปลอดภัยได้ในระดับสากล

4. จากผลการวิจัยพบว่าองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศส่งผลต่อความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์ และจากผลการวิเคราะห์ข้อมูลองค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์แสดงให้เห็นถึงความหลากหลายในการใช้งานของบริษัทในองค์ประกอบนี้ กล่าวคือบริษัทมีการใช้ฮาร์ดแวร์คอมพิวเตอร์(เครื่อง PC, โน้ตบุค, Tablet, เครื่อง Mac, Mini, Mainframe, Power PC)ที่หลากหลาย โดยพบบริษัทส่วนใหญ่มีการใช้ฮาร์ดแวร์ 3 แบบขึ้นไป ในส่วนของระบบปฏิบัติการ(Windows, Unix, Linux, Mac OS, Solaris, VMS, โอซีรี่, Jbunto, OracleLinux, Aix, ระบบปฏิบัติการบน risc 600)ก็พบความหลากหลายในการใช้งานเช่นเดียวกันและยังพบบริษัทที่มีการใช้งานระบบปฏิบัติการมากกว่า 5 แบบอีกด้วย ในทิศทางเดียวกันการใช้ซอฟแวร์สำหรับบริหารจัดการฐานข้อมูล (Oracle, DB2, SQL server, Sysbase, Mysql, MS Access, Informix) ก็พบว่าบริษัทส่วนใหญ่มีการใช้ตั้งแต่ 3 แบบขึ้นไป (รายละเอียดตารางที่ 5 ภาคผนวก ก) ซึ่งความหลากหลายที่มากเกินไปในการใช้งานของฮาร์ดแวร์คอมพิวเตอร์ ระบบปฏิบัติการ และ ซอฟแวร์สำหรับบริหารจัดการฐานข้อมูลนั้นทำให้บริษัทจำเป็นต้องจ้างบุคลากรเพิ่มขึ้นในการดูแลรักษาระบบ การดูแลรักษาทำได้ยากกว่า รวมทั้งปัญหาในการเชื่อมต่อ การอัพเกรดเวอร์ชั่นที่ไม่พร้อมกัน และอาจส่งผลทำให้มีค่าใช้จ่ายในการลงทุน บริหารจัดการ และดูแลรักษาที่เพิ่มขึ้น ดังนั้นถ้าเป็นไปได้บริษัทควรลดประเภทของการใช้งานลง

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. ควรมีการวิจัยเชิงคุณภาพถึงปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์บริษัทที่ความเสี่ยงในระดับต่ำเพื่อให้ได้ข้อมูลอีกรูปแบบหนึ่งประกอบการพิจารณา รวมทั้งจะได้ทราบแนวทางในการรับมือ แก้ไขและแนวทางปฏิบัติที่ดีของบริษัทในการบริหารและจัดการความเสี่ยงที่เกิดขึ้น

2. ควรมีการวิจัยทั้งเชิงปริมาณและเชิงคุณภาพถึงทัศนคติ/ความคิดเห็นของผู้บริหารฝ่าย IT ที่มีต่อปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์บริษัทว่าส่งผลกระทบต่อการดำเนินของบริษัทหลักทรัพย์อย่างไรซึ่งทางผู้วิจัยได้ทำการเก็บข้อมูลไปบางส่วนแล้ว

3. ควรมีการวิจัยถึงองค์ประกอบของแต่ปัจจัยที่ส่งผลต่อความเสี่ยงที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในบริษัทหลักทรัพย์อันประกอบด้วย ปัจจัยผู้มีส่วนเกี่ยวข้องในเรื่องการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ , นโยบายการควบคุมความปลอดภัย, เครื่องมือที่ใช้ในการบริหารความเสี่ยง, การสื่อสารเรื่องความเสี่ยง, องค์ประกอบของโครงสร้างหลักเทคโนโลยีสารสนเทศ และ การให้ความรู้แก่พนักงานในเรื่องนโยบายความปลอดภัยและแนวปฏิบัติ เพื่อให้ได้คำตอบที่ชัดเจนในรายละเอียดมากขึ้น

4. จากการค้นพบที่ว่าความเสี่ยงอันเกิดจากการต้องว่าจ้างบริษัทภายนอกที่เชี่ยวชาญมาทำงานให้(outsource) อยู่ในระดับสูงสุดดังนั้นควรมีการศึกษาถึง ปัจจัยที่มีผลต่อการตัดสินใจเลือกว่าจ้างบริษัทผู้ให้บริการ IT outsourcing สำหรับบริษัทหลักทรัพย์

บรรณานุกรม

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2552) **ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์ เรื่องแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์**. [ออนไลน์] แหล่งที่มา : http://capital.sec.or.th/webapp//nrs/data/4853s.pdf (1 สิงหาคม 2555)

ตลาดหลักทรัพย์แห่งประเทศไทย. (2555) **รายชื่อบริษัทสมาชิกตลาดหลักทรัพย์แห่งประเทศไทย**. [ออนไลน์] แหล่งที่มา : http://www.set.or.th/set/memberlist.do?language=th&country=TH (20 มิถุนายน 2555)

_____. (2555) **SETSMART(SET Market Analysis and Reporting Tool)**. [ออนไลน์] แหล่งที่มา : http://www.setsmart.com/ism/login.jsp (1 กรกฎาคม 2555)

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

นวพร เรืองสกุล. (2551) **กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ: บทสรุปสำหรับผู้บริหารกรอบโครงสร้าง**. พิมพ์ครั้งที่ 1. กรุงเทพฯ : อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง จำกัด.

บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูล. [ออนไลน์] แหล่งที่มา : http://www.th.recall.com/data-protection/~/media/files/Solutions/recall-data-protection-legislation-en.sdhx (12 ธันวาคม 2555)

บรรจง หะรังสี, ภัทราวดี เหมทานนท์. (2555) **COBIT 5 กับการนำไปใช้งาน**. [ออนไลน์] แหล่งที่มา : http://www.tnetsecurity.com/content_audit/cobit5_implementtation_step.php (12 ธันวาคม 2555)

ประชาชาติธุรกิจ. (2546) **การควบคุมภายใน...สิ่งที่เลี่ยงไม่ได้**. [ออนไลน์] แหล่งที่มา : http://www.nidambe11.net/ekonomiz/2003q2/article2003april24p2.htm (22 มกราคม 2555)

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

_____. (2553) **เจาะลึก IT Governance Implementation และบทวิเคราะห์ Cobit 5.0 “Enterprise Governance of IT Framework” และ IT Governance Implementation Guide ล่าสุดจาก ISACA**. [ออนไลน์] แหล่งที่มา : http://www.theiiat.or.th/media/km/thumbnail/18/111125151018/ITGovernanceImplementation.pdf (22 มกราคม 2555)

_____. (2556) **การประเมินตนเองเพื่อควบคุมความเสี่ยง-CSA/Controls self assessment ตอนที่ 8 COSO (Committee of Sponsoring Organization)**. [ออนไลน์] แหล่งที่มา : http://www.itgthailand.com/tag/องค์ประกอบของการควบคุม/ (22 สิงหาคม 2556)

พลพฐู 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 ปัญญาพินิจนุกุกุร. (2552) **มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC27001 และ ISO/IEC 17999 ฉบับประเทศไทย**. [ออนไลน์] แหล่งที่มา : http://www.oknation.net/blog/print1.php?id=404278 (22 ธันวาคม 2555)

ศูนย์ศึกษาและพัฒนาเทคโนโลยีทรัพยากรบุคคลมหาวิทยาลัยเกษตรศาสตร์. (2552) **เรียนรู้กับ ITL เวอร์ชั่น 3 IT Infrastructure Library**. [ออนไลน์] แหล่งที่มา : http://www.ict.doae.go.th/upload/iblock/595/595d4facdb522ba72035f1b2df45c2d1.pdf (20 สิงหาคม 2555)

Aguilar, M. (2011) **Financial firms have more work on Risk, IT**. [On-line] Available : http://www.complianceweek.com (November 22, 2011)

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

Center for Internet Security. **CIS benchmarks**. [On-line] Available : http://benchmarks.cisecurity.org/downloads/benchmarks/ (November 22, 2011)

Cisco. (2013) **Cisco Global IT Impact Survey**. [On-line] Available : http://www.cisco.com/en/US/solutions/collateral/ns1015/Cisco_IT_Impact_Survey_Results_2013.pdf (August 12, 2013)

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

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**. [On-line] Available : http://citebm.business.illinois.edu/TWC%20Class/Project_reports_Fall2008/Project%20and%20Risk%20Manag ement/Sebastian%20Gawenda/OT%20Portfolio%20Management%20Paperx.pdf (December 22, 2011)

ISACA. (2009) **The risk IT Framework**. [On-line] Available : http://www.isaca.org/riskitfw (July 20, 2012)

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

_____. (2010) **What Color is Your Information Risk—Today?**. [ออนไลน์] Available : http://www.itpolicycompliance.com/research-reports/what-color-is-your-information-risk-%e2%80%93-today (December 22, 2011)

_____. (2010) **How the Master of IT Deliver More Value and Less Risk**. [On-line] Available : http://www.itpolicycompliance.com/research-reports/how-the-master-of-it-deliver-more-value-and-less-risk (December 22, 2011)

_____. (2011) **How High Performance Organization Manage IT**. [On-line] Available : http://www.itpolicycompliance.com/research-reports/how-high-performance-organizations-manage-it (December 22, 2011)

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. (2008) **Management Information Systems**. Pearson Education Indochina Ltd.

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

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

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

ภาคผนวก

ภาคผนวก ก

ตารางแสดงผลการวิเคราะห์