แบบจำลองการเรียนรู้สำหรับการประเมินค่าอันดับโดยผู้เชี่ยวชาญ

นายชวิศ ทวีโรจน์กุลศรี

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ ที่ส่งผ่านทางบัณฑิตวิทยาลัย
The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository (CUIR)
are the thesis authors' files submitted through the University Graduate School.

LEARNING MODELS FOR RANKING ASSESSMENT BY EXPERTS

Mr. Chawis Taweerojkulsri

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2013

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	แบบจำลองการเรียนรู้สำหรับการประเมินค่าอันดับโดยผู้เชี่ยวชาญ
โดย	นายชวิศ ทวีโรจน์กุลศรี
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร. บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(ศาสตราจารย์ ดร. บุญเสริม กิจศิริกุล)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์)

.....กรรมการภายนอกมหาวิทยาลัย

(อาจารย์ ดร. ภาสกร อภิรักษ์วรพินิต)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ชวิศ ทวีโรจน์กุลศรี : แบบจำลองการเรียนรู้สำหรับการประเมินค่าอันดับโดยผู้เชี่ยวชาญ. (LEARNING MODELS FOR RANKING ASSESSMENT BY EXPERTS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร. ญาใจ ลิ่มปิยะกรณ์, 102 หน้า.

โดยทั่วไปการประมาณหรือประเมินค่ามักกระทำโดยผู้เชี่ยวชาญ การประเมินความเสี่ยงเป็นกิจกรรมหนึ่งที่มีวัตถุประสงค์เพื่อจัดลำดับความสำคัญความเสี่ยง โดยพิจารณาจากระดับความรุนแรงการสูญเสียที่อาจเกิดขึ้นได้ การวิเคราะห์สถานการณ์เป็นวิธีการที่นิยมใช้เพื่อประเมินผลกระทบในกรณีที่มีปัจจัยความเสี่ยงเกิดขึ้น อย่างไรก็ตาม การประเมินระดับความรุนแรงของผลกระทบในสถานการณ์ต่างๆ โดยผู้เชี่ยวชาญเป็นกิจกรรมที่สิ้นเปลืองทรัพยากร รวมถึงต้องมีการตรวจสอบและการประเมินใหม่ เพื่อใช้ในการเปรียบเทียบกับข้อมูลความเสียหายที่เกิดขึ้นจริงที่มีอยู่ตลอดเวลา นอกจากวิธีการประเมินค่าโดยผู้เชี่ยวชาญ การสร้างแบบจำลองเป็นเทคนิคหนึ่งที่สามารถใช้สำหรับการวิเคราะห์สถานการณ์ งานวิจัยนี้ได้ศึกษาวิธีการสร้างแบบจำลองสำหรับการประเมินค่าระดับความรุนแรงการสูญเสียด้วยโมเดลสมการโครงสร้างและแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กในบริบทของความเสี่ยงทางด้านปฏิบัติการ ซึ่งเป็นความเสี่ยงประเภทหนึ่งในกลุ่มธุรกิจที่ให้บริการทางด้านการธนาคารและการเงิน ผลลัพธ์ที่ได้พบว่าโมเดลสมการโครงสร้างมีความแม่นยำในการทำนายระดับความรุนแรงการสูญเสียน้อยกว่ามาก อันเป็นผลมาจากความสัมพันธ์ระหว่างตัวแปรที่ไม่เป็นเชิงเส้น ถึงแม้ว่าโมเดลสมการโครงสร้างจะไม่เหมาะสมกับการจำลองแบบความสัมพันธ์ที่ไม่เป็นเชิงเส้น แต่ก็มีข้อดีในการใช้เพื่อวิเคราะห์ความสัมพันธ์ทั้งทางตรงและทางอ้อมระหว่างตัวแปรที่ต้องการตรวจสอบได้

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2556

5570972321 : MAJOR SOFTWARE ENGINEERING

KEYWORDS: ASSESSMENT / OPERATIONAL RISK / STRUCTURAL EQUATION MODEL / BACKPROPAGATION NEURAL NETWORK

CHAWIS TAWEEROJKULSRI: LEARNING MODELS FOR RANKING ASSESSMENT BY EXPERTS. ADVISOR: ASSOC. PROF. YACHAI LIMPIYAKORN, 102 pp.

In general, estimation or assessment is performed by domain experts. Risk assessment is the activity aiming at prioritizing risks with regard to their potential loss severity. Scenario analysis is a method usually used for assessing the impact when risk factors really occur. However, the expert assessment of various risk scenarios that may result in a certain level of impact severity is considered as a resource consuming activity. In addition, it requires frequently validating and re-assessing to compare with the actual loss data available over time. Alternatively, model construction is one of the techniques that can be used for scenario analysis. This research has studied applying the modeling approach to assessing loss severity using the Structural Equation Model and Backpropagation neural network in the context of operational risk, which is one of the risk dimensions in banking and financial services community. The results reported that the Structural Equation Model provided much less accuracy when predicting the level of loss severity due to the finding that the relationship among variables is not linear. Although, the Structural Equation Model is not suitable for modeling nonlinear relationship, it is good at analyzing either direct or indirect relationship among variables under investigation.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Department: Computer Engineering Student's Signature .....

Field of Study: Software Engineering Advisor's Signature .....

Academic Year: 2013

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความอนุเคราะห์อย่างดียิ่งของรองศาสตราจารย์ ดร. ญาใจ ลิ่มปิยะกรณ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ ให้คำปรึกษา ตรวจสอบ ให้คำแนะนำแนวทางการวิจัย และสนับสนุน จนทำให้การวิจัยในครั้งนี้สำเร็จออกมาด้วยดี ข้าพเจ้าจึงขอกราบระลึกถึงพระคุณของรองศาสตราจารย์ ดร.ญาใจ ลิ่มปิยะกรณ์ไว้ ณ ที่นี้

ขอขอบพระคุณ ศาสตราจารย์ ดร.บุญเสริม กิจศิริกุล และอาจารย์ ดร.ภาสกร อภิรักษ์วรพินิต กรรมการสอบวิทยานิพนธ์ ที่กรุณาเสียสละเวลา ให้คำแนะนำ ตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ท้ายที่สุด ผู้เสนอวิทยานิพนธ์ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ และครอบครัว สำหรับกำลังใจที่มีค่ายิ่ง รวมถึงขอขอบพระคุณผู้บังคับบัญชาในสายงาน เพื่อนร่วมงาน และมิตรสหาย ที่คอยติดตามให้กำลังใจ ให้การสนับสนุนและความช่วยเหลือในด้านต่างๆ และท่านอื่นๆ ที่มิได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนช่วยให้วิทยานิพนธ์ของข้าพเจ้าสำเร็จไปได้ด้วยดี

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง ..... ญ

สารบัญภาพ ..... ฎ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์ของการวิจัย 2

1.3 ขอบเขตการวิจัย 2

1.4 ประโยชน์ที่คาดว่าจะได้รับ 2

1.5 วิธีการดำเนินการวิจัย 3

1.6 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์ 3

1.7 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์ 4

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5

2.1 ทฤษฎีที่เกี่ยวข้อง 5

2.1.1 การประเมินความเสี่ยง (Risk assessment) [1] 5

2.1.2 การวิเคราะห์สถานการณ์ (Scenario analysis) [2] 9

2.1.3 ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) [4] 12

2.1.4 แบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก (Back Propagation Neural Networks) [7, 8] . 15

2.1.5 โมเดลสมการโครงสร้าง (Structural Equation Model: SEM) [9, 10] 16

2.1.6 การวิเคราะห์เส้นทาง [9, 10] 18

2.2 งานวิจัยที่เกี่ยวข้อง 19

2.2.1 Quality of security metrics and measurement [11] 19

2.2.2 A Ranking of Software Engineering Measures Based on Expert Opinion [12] 21

บทที่ 3 วิธีการดำเนินการวิจัย 23

หน้า

3.1 แนวคิดในการพัฒนา 23
3.2 การกำหนดกรอบแนวคิดการวิจัย 23
3.2.1 กำหนดโดเมนปัญหา มาตรวัดการจัดอันดับ และปัจจัยที่เกี่ยวข้องกับงานวิจัย 23
3.2.2 รายละเอียดตัวแปรและการกำหนดค่าเกณฑ์ที่ใช้ในการวิจัย 23
3.2.3 เครื่องมือที่ใช้ในการวิจัย 31
3.3 การเก็บข้อมูล (Data collection) 35
3.4 การวิเคราะห์ข้อมูล 36
3.4.1 สถิติเบื้องต้น 36
3.4.2 สถิติที่ใช้ทดสอบสมมติฐานและโมเดล [9, 16-22] 36
3.5 การสร้างโมเดลสำหรับงานวิจัย 40
3.5.1 การสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก 40
3.5.2 การสร้างโมเดลสมการโครงสร้าง 41
บทที่ 4 ผลการวิจัยและอภิปรายผล 43
4.1 ผลการเก็บข้อมูล 43
4.2 การเตรียมข้อมูล (data preprocessing) 43
4.3 ผลการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก 44
4.4 ผลการสร้างโมเดลสมการโครงสร้าง 47
4.5 การเปรียบเทียบผลของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง 53
บทที่ 5 การสรุปผลและข้อเสนอแนะ 55
5.1 สรุปผลการวิจัย 55
5.2 ข้อจำกัดและข้อเสนอแนะ 55
5.3 แนวทางการวิจัยต่อ 55
รายการอ้างอิง 56
ภาคผนวก 58
ภาคผนวก ก ขั้นตอนการปรับโมเดลสมการโครงสร้าง 59
ภาคผนวก ข ผลการประมาณค่าระดับความรุนแรงการสูญเสียโดยโมเดลสมการโครงสร้าง 66
ประวัติผู้เขียนวิทยานิพนธ์ 102

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญตาราง

หน้า

ตารางที่ 1 Prioritization results of all respondents 20
ตารางที่ 2 W values for different clusters 21
ตารางที่ 3 ปัจจัยความเสี่ยงทางด้านการปฏิบัติงาน 24
ตารางที่ 4 ค่าสถิติที่เลือกใช้ในทดสอบสมมติฐานและการสร้างโมเดลการวิจัย 37
ตารางที่ 5 ระดับเกณฑ์การประเมินตัววัด RMSEA 38
ตารางที่ 6 ระดับเกณฑ์การประเมินตัววัด Kappa coefficient 40
ตารางที่ 7 สรุปเกณฑ์ที่ใช้ในการตรวจสอบความสอดคล้องของโมเดล 40
ตารางที่ 8 การกำหนดค่าข้อมูลนำเข้าและโครงสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก 44
ตารางที่ 9 การตั้งค่าพารามิเตอร์ของโครงข่ายประสาทเทียม 45
ตารางที่ 10 การประเมินผลการทำนายระดับการสูญเสียของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก 45
ตารางที่ 11 ผลการประเมินของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก 45
ตารางที่ 12 การกำหนดค่าข้อมูลนำเข้าและโครงสร้างโมเดลสมการโครงสร้าง 47
ตารางที่ 13 เกณฑ์การประเมินความแม่นยำของโมเดลสมการโครงสร้าง 52
ตารางที่ 14 การประเมินผลการทำนายระดับการสูญเสียของโมเดลสมการโครงสร้าง 52
ตารางที่ 15 ผลการเปรียบเทียบโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง 53
ตารางที่ 16 ผลการเปรียบเทียบโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง 66

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญภาพ

หน้า

ภาพที่ 1 บทบาทของการประเมินความเสี่ยงในกระบวนการบริหารความเสี่ยง 5
ภาพที่ 2 องค์ประกอบการวิเคราะห์สถานการณ์ 11
ภาพที่ 3 ปัจจัยความเสี่ยงทางด้านการปฏิบัติการได้จากมาตรฐาน..... 13
ภาพที่ 4 เพอร์เซปตรอน..... 16
ภาพที่ 5 ตัวอย่างเน็ตเวิร์กป้อนไปหน้าแบบหลายชั้น 16
ภาพที่ 6 ตัวอย่างโมเดลสมการโครงสร้าง 17
ภาพที่ 7 ตัวอย่างโมเดลการวิเคราะห์เส้นทาง..... 19
ภาพที่ 8 โมเดลเกณฑ์การวัดคุณภาพของตัวชี้วัดทางด้านความมั่นคงปลอดภัยที่ได้มาของชุดข้อมูล 21
ภาพที่ 9 ขั้นตอนการจัดลำดับวิธีการวัดทางด้านวิศวกรรมซอฟต์แวร์ 22
ภาพที่ 10 แบบฟอร์มการเก็บข้อมูลภูมิหลังผู้ทำแบบสอบถาม 32
ภาพที่ 11 แบบฟอร์มการเก็บข้อมูลการวิเคราะห์สถานการณ์ความเสี่ยง..... 33
ภาพที่ 12 ส่วนต่อประสานของโปรแกรม WEKA 34
ภาพที่ 13 ส่วนต่อประสานของโปรแกรมสถิติ SPSS..... 34
ภาพที่ 14 ส่วนต่อประสานของโปรแกรม SPSS AMOS 35
ภาพที่ 15 โครงสร้างของโครงข่ายหลายชั้นสำหรับโมเดลการเรียนรู้..... 46
ภาพที่ 16 โมเดลสมการโครงสร้างที่ได้จากงานวิจัยก่อนทำให้เป็นมาตรฐาน 49
ภาพที่ 17 โมเดลสมการโครงสร้างที่ได้จากงานวิจัยหลังทำให้เป็นมาตรฐาน 49
ภาพที่ 18 ผลการประเมินค่าความน่าเชื่อถือของโมเดล 50
ภาพที่ 19 ผลของค่าตัววัด SRC 50
ภาพที่ 20 ผลของค่า C.R. และค่า P-value..... 51
ภาพที่ 21 ผลของค่า SDE, SIE, STE และ TE..... 51
ภาพที่ 22 ผลของค่า SMC (Squared Multiple Correlations)..... 53
ภาพที่ 23 สมการโครงสร้างตามหลักทฤษฎี 59
ภาพที่ 24 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง 60
ภาพที่ 25 การพิจารณาปรับโมเดลจากค่า MI 60
ภาพที่ 26 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ2..... 61
ภาพที่ 27 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง2..... 61
ภาพที่ 28 การพิจารณาปรับโมเดลจากค่า MI2..... 62
ภาพที่ 29 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง3..... 62
ภาพที่ 30 การพิจารณาปรับโมเดลจากค่า MI3..... 63
ภาพที่ 31 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ3..... 63

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาพที่ 32 การตรวจสอบจากค่า C.R. และ P-value 64
ภาพที่ 33 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ4..... 64
ภาพที่ 34 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง4..... 65

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การจัดอันดับ (Ranking) เป็นวิธีการหนึ่งที่มีจุดประสงค์เพื่อช่วยการแก้ปัญหาการจัดเรียงลำดับความสำคัญ (Prioritization) ของสิ่งที่สนใจ การจัดอันดับถูกใช้ในวิเคราะห์และนำไปประยุกต์เพื่อแก้ปัญหาในหลายบริบท เช่น การจัดลำดับความสำคัญความต้องการ (Requirements Prioritization) การจัดลำดับความสำคัญกรณีทดสอบ (Test Case Prioritization) การจัดลำดับความเสี่ยง (Risk Prioritization) หรือการประเมินค่าอันดับของมาตรวัด (metric) จากน้ำหนักความสำคัญของปัจจัยต่างๆที่มีผลกระทบ อาทิ ความมั่นคงของระบบสารสนเทศ ความซับซ้อนโครงการ หรือ คุณภาพซอฟต์แวร์ เป็นต้น

โดยทั่วไป การบริหารโครงการมักมีเป้าหมายหลักในการบริหารจัดการทางด้าน ขอบเขตการทำงาน (scope) เวลาที่ต้องใช้ (time) และค่าใช้จ่าย (cost) ต่าง ๆ ซึ่งเป็นทรัพยากรที่มีอยู่อย่างจำกัดให้เกิดประโยชน์สูงสุด ดังนั้น จึงต้องมีการจัดลำดับความสำคัญของงานที่ต้องกระทำ เนื่องจากงานแต่ละด้านก็มีค่าใช้จ่ายและผลตอบแทนที่ไม่เท่ากัน ดังนั้น จึงต้องมีเกณฑ์ในการเลือกหรือจัดลำดับความสำคัญของปัจจัยดังกล่าว ซึ่งจะใช้วิธีการจัดอันดับนั่นเอง

การบริหารโครงการเป็นองค์ความรู้หนึ่งที่สำคัญของของศาสตร์วิศวกรรมซอฟต์แวร์ การบริหารความเสี่ยงเป็นกระบวนการหลักกระบวนการหนึ่งในการบริหารโครงการ และมีความสำคัญต่อความสำเร็จของโครงการ ความเสี่ยงอาจอยู่ในรูปของเหตุการณ์ต่างๆ ที่ไม่แน่นอน ซึ่งเมื่อเกิดขึ้นแล้วจะส่งผลกระทบต่อการดำเนินงานตั้งแต่ระดับปฏิบัติงาน ระดับฝ่ายงานไปจนถึงระดับความอยู่รอดของการดำเนินธุรกิจขององค์กร

โมเดลสมการโครงสร้าง (Structural Equation Model) เป็นเทคนิคทางสถิติสำหรับศึกษาความสัมพันธ์ระหว่างตัวแปรจากการตั้งสมมติฐานการทดลอง โดยการทดสอบความสัมพันธ์จะใช้หลักการวิเคราะห์การถดถอยแบบพหุ (Multiple Regression Analysis) เพื่อให้เข้าใจความเป็นเหตุและผลของตัวแปรที่สนใจ

โครงข่ายประสาทเทียม (Artificial Neural Network) เป็นเทคนิคการเรียนรู้ของศาสตร์การเรียนรู้ด้วยเครื่อง (Machine Learning) เพื่อสร้างโมเดลผลลัพธ์สำหรับการจำแนกประเภท (Classification) ซึ่งสามารถนำไปประยุกต์ใช้ในด้านต่างๆ เช่น การรู้จำ (Recognition) เสียงหรือตัวอักษร การทำนาย (Prediction) การดื้อยาของผู้ป่วยหรือราคาหุ้น เป็นต้น

การวิเคราะห์ความเสี่ยงเป็นการสร้างความเข้าใจความเสี่ยงที่อาจเกิดขึ้น โดยพิจารณาจากน้ำหนักของสาเหตุความเสี่ยงหลาย ๆ ปัจจัยที่มีผลกระทบ อย่างไรก็ตาม การวิเคราะห์ปัจจัยความเสี่ยงเป็นเรื่องยากต่อการเข้าใจ การประเมินความเสี่ยงจึงมักจะใช้วิธีประเมินโดยผู้เชี่ยวชาญ ซึ่งเป็นบุคคลที่มีความรู้และความเชี่ยวชาญเฉพาะทางด้านนั้น ๆ โดยทั่วไป องค์ความรู้ของผู้เชี่ยวชาญถือเป็นองค์ความรู้ที่ได้รับการยอมรับว่าเป็นมาตรฐานในการประเมินผล และวิธีประเมินด้วยกลุ่ม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ผู้เชี่ยวชาญเป็นวิธีที่ใช้กันอยู่อย่างแพร่หลาย ซึ่งวิธีการประเมินโดยกลุ่มผู้เชี่ยวชาญ เป็นกระบวนการที่สิ้นเปลืองทรัพยากร ทั้งเวลาและค่าใช้จ่าย งานวิจัยนี้จึงได้นำเสนอแนวทางการสร้างแบบจำลองเพื่อเรียนรู้การประเมินให้ค่าอันดับจากน้ำหนักหรือความสำคัญของปัจจัยต่างๆที่มีผลกระทบต่อการวิเคราะห์ความเสี่ยงทางด้านปฏิบัติการของธุรกิจทางด้านการธนาคารและการเงิน โดยใช้ความคิดเห็นของกลุ่มผู้เชี่ยวชาญ แนวทางการสร้างแบบจำลองการเรียนรู้ที่นำเสนอในงานวิจัยนี้ ประกอบด้วยการใช้วิธีการทางสถิติและวิธีการเรียนรู้ของเครื่อง (Machine Learning) ทั้งนี้ แบบจำลองผลลัพธ์การเรียนรู้ที่ได้สามารถนำไปใช้ประเมินค่าอันดับของมาตรวัด เสมือนเป็นการประเมินจากกลุ่มผู้เชี่ยวชาญ ทำให้ลดเวลาและค่าใช้จ่ายขององค์กรลงได้ พร้อมทั้งเปรียบเทียบผลลัพธ์จากการสร้างแบบจำลองทั้งสองอีกด้วย

1.2 **วัตถุประสงค์ของการวิจัย**

1. เพื่อนำเสนอวิธีการและพัฒนาแบบจำลองผลลัพธ์จากการเรียนรู้ความคิดเห็นของกลุ่มผู้เชี่ยวชาญในการวิเคราะห์ความเสี่ยงทางด้านปฏิบัติการของธุรกิจทางด้านการธนาคารและการเงิน จากการพิจารณาน้ำหนักความสำคัญของปัจจัยต่างๆที่มีผลกระทบต่อระดับความรุนแรงการสูญเสีย
2. เพื่อศึกษาความสัมพันธ์ของปัจจัยความเสี่ยงทางด้านปฏิบัติการที่มีต่อระดับความรุนแรงของผลกระทบในสถานการณ์ความเสี่ยงที่แตกต่างกัน
3. เพื่อประเมินเปรียบเทียบความถูกต้องของแบบจำลองผลลัพธ์ที่ได้จากวิธีการที่นำเสนอ 2 แนวทาง

1.3 **ขอบเขตการวิจัย**

1. งานวิจัยนี้ศึกษามาตรวัดที่เกี่ยวข้องกับการวิเคราะห์และประเมินความเสี่ยงทางด้านปฏิบัติการโดยมุ่งเน้นปัจจัยความเสี่ยงทางธุรกิจทางการธนาคารและสถาบันการเงิน
2. ปัจจัยที่ส่งผลกระทบต่อค่ามาตรวัดอันดับ มีจำนวนระหว่าง 5-10 ปัจจัย
3. การเปรียบเทียบแบบจำลองผลลัพธ์ที่ได้จาก 2 แนวทางที่นำเสนอ อย่างน้อยจะประเมินจากค่าความแม่นยำ (accuracy) และค่าความแม่นยำเฉลี่ย k-fold cross validation สำหรับโมเดลโครงข่ายประสาทเทียมในกรณีที่ขนาดตัวอย่างมีจำนวนจำกัด

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้วิธีการและแบบจำลองผลลัพธ์สำหรับการประเมินค่าอันดับมาตรวัดเพื่อใช้ในการวิเคราะห์ระดับความรุนแรงการสูญเสีย เพื่อจัดลำดับความสำคัญของเหตุการณ์ความเสี่ยง โดยเรียนรู้จากความคิดเห็นของกลุ่มผู้เชี่ยวชาญ
2. ผลของความสัมพันธ์ของปัจจัยที่ได้จากการวิเคราะห์ สามารถนำไปประยุกต์ใช้ในการกำหนดความสำคัญของปัจจัยในประบวนการวิเคราะห์ความเสี่ยงขององค์กร เพื่อใช้ในการประเมินระดับความรุนแรงการสูญเสียทางด้านความเสี่ยงด้านการปฏิบัติการได้

3. วิธีการสร้างแบบจำลองที่เรียนรู้จากความชำนาญของกลุ่มผู้เชี่ยวชาญ สามารถลดเวลาและค่าใช้จ่ายของกระบวนการประเมินค่ามาตรวัดอันดับโดยกลุ่มผู้เชี่ยวชาญได้

1.5 วิธีการดำเนินการวิจัย

ลำดับการเรียงงานวิจัยนี้มุ่งเน้นที่จะนำเสนอวิธีการและการพัฒนาแบบจำลองเพื่อช่วยในการประเมินค่าอันดับของมาตรวัดจากกลุ่มผู้เชี่ยวชาญ ซึ่งพิจารณาจากปัจจัยต่างๆ ที่กำหนดขึ้น ระเบียบวิธีวิจัยประกอบด้วยขั้นตอนหลักๆ ดังนี้

1. กำหนดมาตรวัดค่าอันดับของโดเมนปัญหาที่สนใจ และระบุปัจจัยต่างๆ ที่ใช้ในการประเมินค่าอันดับ โดยการวิจัยได้กำหนดปัจจัยทางด้านการวิเคราะห์ความเสี่ยงทางด้านการปฏิบัติการของธุรกิจธนาคารและสถาบันการเงิน
2. ค้นหาและกำหนดมาตรวัดจากมาตรฐานที่เกี่ยวข้อง บทความหรือวารสารทางวิชาการ
3. นำเสนอวิธีการในการประเมินอันดับผลลัพธ์ของโครงการ แบ่งออกเป็น 2 แนวทางคือ ใช้วิธีการทางสถิติโดยเลือกใช้โมเดลสมการโครงสร้าง และใช้วิธีทางการเรียนรู้ของเครื่องโดยเลือกใช้โมเดลการเรียนรู้โครงข่ายประสาทเทียมแบบแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก
4. วิเคราะห์และออกแบบการเก็บข้อมูล โดยออกแบบแบบสอบถามเพื่อเก็บข้อมูลจากกลุ่มผู้เชี่ยวชาญ
5. สร้างชุดข้อมูลจากการตอบแบบสอบถามของกลุ่มผู้เชี่ยวชาญ
6. พัฒนาโมเดลการเรียนรู้ทั้ง 2 แนวทางโดย
7. สร้างโมเดลผลลัพธ์จากการเรียนรู้แบบโครงข่ายประสาทเทียม โดยใช้เครื่องมือ WEKA
8. สร้างโมเดลสมการโครงสร้าง โดยใช้เครื่องมือสถิติ SPSS และ AMOS
9. ประเมินผลการสร้างแบบจำลองและเปรียบเทียบแบบจำลองผลลัพธ์ที่ได้จาก 2 แนวทางที่นำเสนอ
10. ตีพิมพ์ผลงานทางวิชาการ
11. สรุปผลการวิจัย และจัดทำเล่มวิทยานิพนธ์

1.6 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์ในรายงานสืบเนื่องจากการประชุมวิชาการระดับนานาชาติเรื่อง “Learning Model for Assessing Loss Severity of Operational Risk”, Chawis Taweerojkulsri and Yachai Limpiyakorn, in Proceedings of Information Science and Applications (ICISA), 2014 International Conference on , vol., no., pp.1,4, 6-9 May 2014 และตีพิมพ์ในวารสารวิชาการระดับชาติ เรื่อง “Study of Modeling Operational Risk Analysis with Structural Equation Model”, Chawis Taweerojkulsri and Yachai Limpiyakorn, Ramkhamhaeng Journal of Engineering, Vol.1 No. May 2014

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

1.7 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์นี้ได้แบ่งการจัดเรียงเนื้อหาออกเป็น 5 บทดังต่อไปนี้ บทที่ 1 บทนำกล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการวิจัย ขอบเขตของการวิจัย ประโยชน์ที่คาดว่าจะได้รับ และผลงานตีพิมพ์ บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องของงานวิจัย บทที่ 3 กล่าวถึงวิธีดาเนินการวิจัย บทที่ 4 กล่าวถึงผลการวิจัยและอภิปรายผล บทที่ 5 กล่าวถึงการสรุปผลการวิจัยและข้อเสนอแนะ และแนวทางสำหรับการวิจัยต่อในอนาคต

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

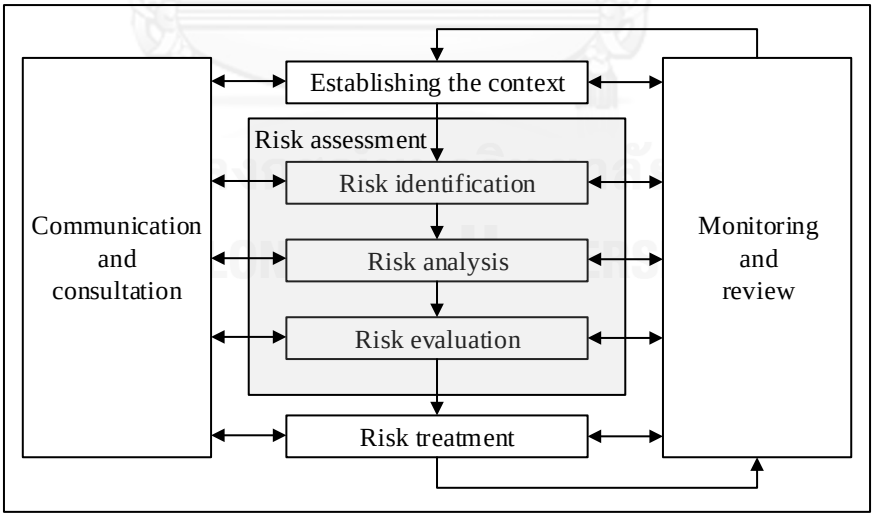
2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 การประเมินความเสี่ยง (Risk assessment) [1]

ในมาตรฐาน ISO 31000 ได้ให้ความหมายของความเสี่ยง (Risk) ไว้ว่า ความเสี่ยงคือผลกระทบจากความไม่แน่นอนของวัตถุประสงค์หรือเป้าหมาย ผลกระทบมีได้ทั้งทางบวกและทางลบ โดยมุมมองในแต่ละวัตถุประสงค์สามารถมองได้หลายด้านยกตัวอย่างเช่น ทางด้านการเงิน (Financial), ด้านความปลอดภัยและสุขภาพ (Health and safety), ด้านกระบวนการทำงาน (Operational) และอื่น ๆ ซึ่งในส่วนของวัดตุประสงค์สามารถประยุกต์ใช้ได้ในหลายระดับที่แตกต่างกันได้แก่ ระดับกลยุทธ์ (Strategic), ระดับองค์กร(Organization), ระดับโครงการ (Project), ระดับผลิตภัณฑ์ (Product) ไปจนถึงระดับกระบวนการทำงาน (Process)

ลักษณะของความเสี่ยงมักอ้างถึง เหตุการณ์ที่อาจเกิดขึ้นได้ (Potential event), ผลกระทบที่เกิดขึ้น (Consequence) และผลกระทบที่เกิดขึ้นในแต่ละเหตุการณ์ ซึ่งสามารถเปลี่ยนไปในสภาพแวดล้อมที่ต่างกัน รวมถึงโอกาสหรือความน่าจะเป็น (Likelihood) ที่อาจเกิดเหตุการณ์นั้น ๆ ด้วย

การบริหารความเสี่ยง (Risk management) เป็นกิจกรรมหนึ่งที่เกี่ยวข้องโดยงตรงกับการควบคุมความเสี่ยงในองค์กร ความสัมพันธ์ของแต่ละกระบวนการในการบริหารความเสี่ยงแสดงดังภาพที่ 1



ภาพที่ 1 บทบาทของการประเมินความเสี่ยงในกระบวนการบริหารความเสี่ยง

ภาพที่ 1 แสดงให้เห็นถึงบทบาทของกระบวนการประเมินความเสี่ยงที่มีในกระบวนการบริหารความเสี่ยง การบริหารความเสี่ยง การประเมินความเสี่ยงประกอบด้วยกระบวนการย่อย ๆ 3 กระบวนการคือการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและการประเมินค่าความเสี่ยง ซึ่ง

จุดประสงค์ของการประเมินความเสี่ยงคือเพื่อเข้าใจความเสี่ยงทั้งหลายที่เกิดขึ้นในองค์กร เข้าใจถึงสาเหตุ ผลกระทบที่เกิดขึ้นและความเป็นไปได้ของความเสี่ยงดังกล่าว ซึ่งจะส่งผลให้องค์กรต้องมีการเลือกแผนการที่จะบรรเทาหรือลดความเสี่ยงนั้นอย่างเหมาะสม การประเมินความเสี่ยงขององค์กรจะต้องมีการประเมินอย่างต่อเนื่อง เพื่อให้ทันต่อความเปลี่ยนแปลงและสามารถสร้างแผนตอบโต้ความเสี่ยงเกิดขึ้นได้อย่างทันท่วงที ซึ่งการจะดำเนินการกระบวนการบริหารความเสี่ยงให้เกิดผลอย่างมีประสิทธิภาพ กระบวนการบริหารความเสี่ยงควรรวมเป็นส่วนหนึ่งของกระบวนการบริหารจัดการ วัฒนธรรมองค์กร และแนวทางการปฏิบัติขององค์กร เพื่อให้การบริหารความเสี่ยงและการจัดการความเสี่ยงสอดคล้องกับกระบวนการทางในการดำเนินธุรกิจขององค์กรนั้น ๆ การบริหารความเสี่ยงแบ่งเป็นกระบวนการหลัก ๆ ดังต่อไปนี้

1. การสร้างบริบท (Establishing the context)

เป็นการสร้างบริบทขององค์กรที่เกี่ยวกับการบริหารความเสี่ยง การเรียบเรียงวัตถุประสงค์ขององค์กร การกำหนด ค่าพารามิเตอร์ต่าง ๆ ในการบริหารความเสี่ยงที่มาจากภายในและภายนอกองค์กร ทั้งในส่วนที่เป็นข้อมูลนำเข้า (Input) และผลลัพธ์ที่ออกมา (Output) ในแต่ละกระบวนการ เช่น ข้อมูลโครงสร้างองค์กรสำหรับเป็นข้อมูลนำเข้า ข้อมูลความเสี่ยงที่ได้มีการระบุแล้วในแต่ละส่วนงานสำหรับเป็นข้อมูลผลลัพธ์และอื่น ๆ รวมไปจนถึงการกำหนดขอบเขตการทำงาน และเกณฑ์การประเมินความเสี่ยง เพื่อใช้ในกระบวนการถัดไป ซึ่งค่าเหล่านี้จะต้องกำหนดไว้เป็นกรอบการทำงานในการบริหารความเสี่ยง (Risk management framework)

2. การระบุความเสี่ยง (Risk identification)

องค์กรควรมีการระบุต้นเหตุ (Risk source) ของความเสี่ยง, พื้นที่ ๆ ได้รับผลกระทบ (Areas of impacts), เหตุการณ์ที่อาจเกิดขึ้น, สาเหตุ (Cause) และผลกระทบที่อาจเกิดขึ้นได้ โดยเป้าหมายของขั้นตอนนี้คือ เพื่อสร้างรายการความเสี่ยงที่ครอบคลุมทั้งองค์กรบนพื้นฐานของ การจำลองเหตุการณ์ที่อาจเกิดขึ้นซึ่งส่งผลกระทบต่อการสร้าง การเพิ่ม การป้องกัน การลด การเร่ง การทำให้ล่าช้าซึ่งความสำเร็จตามวัตถุประสงค์ โดยสิ่งที่สำคัญของการระบุความเสี่ยงคือการระบุความเสี่ยงหรือเหตุการณ์ความเสี่ยงที่ไม่สัมพันธ์กับโอกาสที่จะเกิดขึ้น การระบุความเสี่ยงที่ครอบคลุมการทำงานทั้งหมดนั้นมีความสำคัญมากเนื่องจากความเสี่ยงที่ไม่สามารถระบุได้ จะไม่สามารถวิเคราะห์ความเสี่ยงนั้นในขั้นตอนถัดไปได้

การระบุความเสี่ยงควรระบุทั้งความเสี่ยงที่มีและไม่มีการควบคุม (Control) จากองค์กร แม้ว่าต้นเหตุของความเสี่ยง หรือสาเหตุของความเสี่ยงนั้นจะยังไม่ปรากฏชัดก็ตาม การระบุความเสี่ยงควรมีการตรวจสอบถึงผลกระทบที่ตามมารวมถึงผลกระทบที่อาจเกิดขึ้นจากผลกระทบก่อนหน้าต่อ ๆ กันด้วย ซึ่งการระบุผลกระทบดังกล่าวควรพิจารณาอย่างกว้างขวาง ควรมีการพิจารณาถึงสาเหตุและสถานการณ์ (Scenario) ที่เป็นไปได้ กับผลกระทบที่จะเกิดขึ้นจากเหตุการณ์ดังกล่าว

3. การวิเคราะห์ความเสี่ยง (Risk analysis)

การวิเคราะห์ความเสี่ยงเป็นการสร้างความเข้าใจในความเสี่ยงแต่ละตัว การวิเคราะห์ความเสี่ยงจะเป็นกระบวนการที่ทำให้เกิดข้อมูลตั้งต้นในการประเมินค่าความเสี่ยง และยังเป็นกระบวนการที่ช่วยในการเลือกวิธีการหรือกลยุทธ์ในการจัดการกับความเสี่ยงได้อย่างเหมาะสม

การวิเคราะห์ความเสี่ยงจะต้องพิจารณาถึงสาเหตุ ต้นเหตุของความเสี่ยง ผลกระทบที่เป็นไปได้ทั้งทางบวกและทางลบ รวมถึงโอกาสที่อาจเกิดขึ้นได้ ปัจจัยต่าง ๆ ที่ส่งผลต่อผลกระทบและความน่าจะเป็นดังกล่าวควรมีการระบุไว้ด้วย การวิเคราะห์ความเสี่ยงควรมีการกำหนดระดับของผลกระทบและโอกาสที่อาจเกิดขึ้น รวมถึงลักษณะของปัจจัยอื่น ๆ ด้วย เหตุการณ์เดียวอาจมีได้หลายผลกระทบและสามารถกระทบได้หลายวัตถุประสงค์ ประสิทธิภาพและประสิทธิผลของมาตรการควรคุมที่มีอยู่ควรมีการดูแลและประเมินใหม่อยู่เรื่อย ๆ

การกำหนดระดับความเสี่ยง เงื่อนไขที่จะทำให้เกิดเหตุการณ์ความเสี่ยงนั้น และสมมติฐานควรพิจารณาในการวิเคราะห์ และมีการสื่อสารอย่างมีประสิทธิภาพไปยังผู้ตัดสินใจ และผู้ที่เกี่ยวข้องอย่างเหมาะสม ปัจจัยต่าง ๆ เช่นความคิดเห็นที่มีหลายแนวทางของผู้เชี่ยวชาญ ความไม่แน่นอน ความพร้อมใช้งาน คุณภาพ ปริมาณ และข้อมูลที่เกี่ยวข้อง หรือข้อจำกัดของโมเดลควรให้ความสนใจมากยิ่งขึ้น

การวิเคราะห์ความเสี่ยงควรทำอย่างละเอียดถี่ถ้วน มีการลงรายละเอียดที่ชัดเจน ขึ้นอยู่กับวัตถุประสงค์ของการวิเคราะห์และข้อมูล หรือทรัพยากรที่มีอยู่ การวิเคราะห์สามารถทำได้ทั้งเชิงคุณภาพ กึ่งคุณภาพ หรือเชิงปริมาณได้ ขึ้นอยู่กับแต่ละสถานการณ์

ผลกระทบและโอกาสเกิดที่สามรถกำหนดได้โดยโมเดลของผลลัพธ์ของเหตุการณ์หรือเซตของเหตุการณ์ หรือการประมาณจากการศึกษาหรือจากข้อมูลที่มีอยู่ ผลกระทบสามารถอธิบายได้ทั้งที่เป็นนามธรรมและรูปอธรรม ในบางกรณีอาจกำหนดเป็นค่าตัวเลขมากกว่าหนึ่งค่า ก็เป็นสิ่งจำเป็นเพื่อใช้ในการบรรยายถึงผลกระทบ โอกานเกิดสำหรับความเสี่ยงที่อาจมีอัตราการเกิด สถานที่ กลุ่มหรือเหตุการณ์ที่แตกต่างกัน

4. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยงเป็นการประเมินที่เกี่ยวข้องกับการเปรียบเทียบระดับของความเสี่ยงที่มีการตรวจพบระหว่างกระบวนการวิเคราะห์ความเสี่ยงรวมถึงเกณฑ์ต่าง ๆ ที่ถูกกำหนดขึ้น ในขั้นตอนการสร้างบริบทของการประเมินความเสี่ยง โดยการเปรียบเทียบและเพื่อเลือกวิธีการจัดการที่จำเป็น โดยจุดประสงค์ของการประเมินค่าความเสี่ยงคือเพื่อช่วยในการตัดสินใจในการเลือกวิธีการจัดการความเสี่ยงและการนำวิธีการนั้นไปปฏิบัติให้เกิดผลจริง บนพื้นฐานผลลัพธ์ในการวิเคราะห์ความเสี่ยง ในบางกรณีการประเมินค่าความเสี่ยงสามารถนำไปสู่การตัดสินใจในการวิเคราะห์ต่อไป การประเมินค่าความเสี่ยงสามารถนำไปสู่การตัดสินใจที่ไม่ใช่การจัดการความเสี่ยงให้หมดไปแต่เป็นการบำรุงรักษามาตรการในการควบคุมความเสี่ยงที่มีให้คงอยู่และสามารถดำเนินการได้อย่างมีประสิทธิภาพ การตัดสินใจจะส่งผลต่อมุมมองความเสี่ยงขององค์กรและเกณฑ์ความเสี่ยงที่จะมีการสร้างขึ้น

5. การจัดการความเสี่ยง (Risk treatment)

การจัดการความเสี่ยงเป็นกระบวนการที่เกี่ยวข้องกับการเลือกทางเลือกสำหรับวิธีการในการเปลี่ยนแปลงความเสี่ยง ที่มีอยู่ การนำวิธีการดังกล่าวไปทำให้เกิดผล ซึ่งอาจส่งผลถึงการเปลี่ยนแปลงมาตรการควบคุมที่มีอยู่หรือเป็นการเพิ่มมาตรการควบคุมใหม่ การจัดการความเสี่ยงจะต้องมีการประเมินวิธีการจัดการความเสี่ยงที่สร้างขึ้น ซึ่งวิธีการดังกล่าวอาจไม่สามรถจัดการกับความเสี่ยงนั้นได้หมด ซึ่งเรียกความเสี่ยงนั้นว่าเป็นความเสี่ยงที่เหลืออยู่ (Residue risk) ถ้าหากมีการประเมินความเสี่ยงที่เหลืออยู่แล้วสามารถยอมรับได้สามารถใช้วิธีการดังกล่าวได้ แต่หากไม่สามรถยอมรับได้ก็ต้องทำการสร้างวิธีการในการจัดการความเสี่ยงนั้นใหม่ จากนั้นก็ต้องมีการประเมินประสิทธิผลของวิธีการจัดการนั้น ๆ

ทางเลือกของวิธีการในการจัดการความเสี่ยงมีหลายทางเลือกได้แก่ การหลีกเลี่ยงความเสี่ยงโดยการตัดสินใจยกเลิกกิจกรรมที่เป็นการเพิ่มความเสี่ยง การเพิ่มหรือทำให้เกิดความเสี่ยงนั้นให้มากขึ้นเพื่อหาโอกาสที่จะเกิด การยกเลิกหรือจัดการต้นเหตุหรือความเสี่ยง การเปลี่ยนแปลงความน่าจะเป็นที่จะเกิดความเสี่ยงนั้น ๆ การเปลี่ยนแปลงผลกระทบที่จะเกิดขึ้น การแบ่งปันความเสี่ยงเช่นการทำประกัน และการยอมรับความเสี่ยงให้คงอยู่ต่อไป

การเลือกทางเลือกที่เหมาะสมจะเป็นการสร้างสมดุลระหว่างค่าใช้จ่าย (Cost) และความพยายาม (Effort) ที่ต้องใช้ในการนำวิธีในการจัดการความเสี่ยงนั้นไปดำเนินการให้เกิดผลจริง กับประโยชน์ (Benefit) ที่ได้รับและสอดคล้องกับกฎหมาย ข้อบังครับและความต้องการอื่น ๆ เช่นความรับผิดชอบต่อสังคม การปกป้องสภาพแวดล้อมในธรรมชาติ และอื่น ๆ

เมื่อมีการเลือกทางเลือกใด ๆ ก็ตามในการจัดการความเสี่ยงองค์กรควรมีการพิจารณาถึงคุณค่าและความเข้าใจของผู้ที่เกี่ยวข้อง และหาทางในการสื่อสารที่เหมาะสมที่สุด ถ้าหากทางเลือกในการจัดการความเสี่ยงนั้น ส่งผลกระทบต่อองค์กรและบุคคลที่เกี่ยวข้อง ก็ควรให้บุคคลเหล่านั้นเข้ามามีส่วนร่วมในการตัดสินใจ เพื่อให้ทางเลือกนั้นเป็นที่ยอมรับจากบุคคลดังกล่าวและเกิดประสิทธิผลมากยิ่งขึ้น

นอกเหนือจากนั้นกระบวนการที่จำเป็นอีก 2 ส่วนที่ขาดเสียไม่ได้ในการบริหารความเสี่ยง ซึ่งต้องมีการดำเนินการตั้งแต่เริ่มต้นกระบวนการการสร้างบริบทของการบริหารความเสี่ยง การประเมินความเสี่ยงไปจนถึง การจัดการความเสี่ยงได้แก่

1. การสื่อสารและการให้คำปรึกษา (Communication and consultation)

การสื่อสารและการให้คำปรึกษากับผู้ที่เกี่ยวข้องทั้งจากภายในและภายนอกควรมีการทำในทุก ๆ ขั้นตอนในกระบวนการบริหารความเสี่ยง ดังนั้นควรมีการสร้างแผนการสื่อสารตั้งแต่แรก ๆ ควรมีการชี้ให้เห็นถึงประเด็นต่าง ๆ ที่สัมพันธ์กับความเสี่ยงนั้น ๆ ต้นเหตุของความเสี่ยงและผลกระทบที่ตามมาถ้าสามารถบอกได้ และวิธีการวัด

ในส่วนของการให้คำปรึกษามักจะให้คำปรึกษาในเรื่องของ การสร้างบริบทที่เหมาะสม ช่วยให้มั่นใจถึงความเข้าใจของผู้ที่เกี่ยวข้อง ช่วยในยืนยันว่ามีการระบุความเสี่ยงอย่างเพียงพอแล้ว ช่วยลดความต่างของความเชี่ยวชาญในการวิเคราะห์ความเสี่ยง ช่วยให้มั่นใจว่าการกำหนดและการประเมินค่าเกณฑ์ความเสี่ยงมีการพิจารณาอย่างเหมาะสม รับรองถึงความปลอดภัยในการช่วย

สนับสนุนในส่วนของการสร้างแผนการจัดการความเสี่ยง (Treatment plan) ช่วยในการจัดการกับการเปลี่ยนแปลงที่เกิดขึ้นในกระบวนการบริหารจัดการและช่วยในการพัฒนาการวางแผนในการสื่อสารและให้คำปรึกษาที่เหมาะสมทั้งจากภายในและภายนอก

การสื่อสารและการให้คำปรึกษาควรช่วยในการอำนวยความสะดวกในการสื่อสารข้อมูลที่ตรงกับความเป็นจริง มีความเกี่ยวข้องกับสิ่งที่ทำอยู่ มีความแม่นยำ และการสร้างเข้าใจในการแลกเปลี่ยนข้อมูลและรับผิดชอบในการสร้างความมั่นใจในมุมมองที่ถูกต้องในแต่ละบุคคล

2. การติดตามและการทบทวน (Monitoring and review)

ทั้งการติดตามและการทบทวนเกี่ยวข้องกับการตรวจสอบหรือตรวจตราผลการปฏิบัติงานในแต่ละกระบวนการ ควรมีการวางแผนไว้เป็นส่วนหนึ่งของกระบวนการบริหารซึ่งอาจมีการติดตามและทบทวนเป็นช่วง ๆ หรืออาจทำขึ้นอย่างเฉพาะกิจก็ได้ การติดตามผลและการทบทวนในการบริหารความเสี่ยงควรทำในหลายมุมมองสำหรับจุดประสงค์ที่แตกต่างกันคือ เพื่อให้มั่นใจว่ามาตรการควบคุมมีประสิทธิภาพและประสิทธิผลทั้งในด้านการออกแบบและการทำงานจริง ช่วยให้ได้รับข้อมูลสำหรับการปรับปรุงและการประเมินความเสี่ยง วิเคราะห์และเรียนรู้เหตุผลจากเหตุการณ์ต่าง ๆ การเปลี่ยนแปลง แนวโน้ม ความสำเร็จและความล้มเหลว การตรวจสอบความเปลี่ยนแปลงทั้งในบริบทภายนอกและภายใน รวมไปถึงการเปลี่ยนแปลงเกณฑ์การประเมินความเสี่ยงและตัวความเสี่ยงเองซึ่งจำเป็นที่จะต้องมีการจัดการในส่วนของเวอร์ชันในการสร้างนโยบายและวิธีการในการจัดการความเสี่ยง รวมถึงการระบุถึงความเสี่ยงที่จะเกิดขึ้นด้วย

ความก้าวหน้าในการทำงานตามแผนการจัดการความเสี่ยงจะต้องมีการวัดอย่างสิทธิภาพ ผลของการวัดสามารถรวมเป็นส่วนหนึ่งในการบ่งบอกถึงประสิทธิภาพในการบริหารงาน และการวัดและกิจกรรมที่เกี่ยวข้องกับการรายงานไปยังส่วนงานภายในและภายนอกขององค์กร

2.1.2 การวิเคราะห์สถานการณ์ (Scenario analysis) [2]

การวิเคราะห์สถานการณ์ เป็นวิธีการหนึ่งที่ใช้ในการประเมินความเสี่ยง การวิเคราะห์สถานการณ์เป็นชื่อที่ใช้อธิบายถึงการพัฒนาโมเดลที่ใช้ในการอธิบายถึงอนาคตที่อาจเกิดขึ้นได้ ซึ่งโมเดลดังกล่าวได้ใช้ในการระบุความเสี่ยงโดยพิจารณาจากการพัฒนาที่เป็นไปได้ในอนาคตประกอบกับผลกระทบที่จะเกิดขึ้นเมื่อมีเหตุการณ์นั้น ๆ เกิดขึ้น ซึ่งการวิเคราะห์สถานการณ์มีแนวทางการคิด 3 แบบคือ กรณีที่ดีที่สุด (Best case) กรณีที่แย่ที่สุด (Worst case) และกรณีที่คาดว่าจะเกิด (Expected case) ซึ่งความเป็นไปได้ของแต่ละสถานการณ์ขึ้นอยู่กับความรุนแรงหรือผลกระทบจะเกิดขึ้นจากการวิเคราะห์ความเสี่ยง

การวิเคราะห์สถานการณ์สามารถช่วยในการแสดงถึงแนวโน้มต่างที่อาจเกิดขึ้นจากการพิจารณาจากเทคโนโลยี ความต้องการ มุมมองของสังคม ค่านิยมของคนและปัจจัยอื่น ๆ ที่มีการเปลี่ยนแปลงตลอดระยะเวลา 50 ปีที่ผ่านมา กาวิเคราะห์สถานการณ์ไม่สามารถบ่งบอกถึงความเป็นไปได้ของการเปลี่ยนแปลงนั้นได้แต่สามารถใช้ในการพิจารณาผลกระทบและช่วยในการพัฒนาความแข็งแกร่งและความน่าเชื่อถือที่จำเป็นในการปรับปรุงเปลี่ยนแปลงสำหรับการเปลี่ยนแปลงที่ทำนายได้

การวิเคราะห์สถานการณ์สามารถประยุกต์ใช้ได้ในการสร้างนโยบายในการตัดสินใจ การวางแผนกลยุทธ์และพิจารณากิจกรรมต่าง ๆ ที่มีอยู่ ซึ่งเป็นหนึ่งในองค์ประกอบที่สำคัญในกระบวนการประเมินความเสี่ยง ที่ช่วยในการระบุและวิเคราะห์เซตของสถานการณ์ที่สะท้อนถึง 3 แนวทางในการวิเคราะห์สถานการณ์ซึ่งจะระบุว่าอะไรเป็นเหตุการณ์ที่อาจเกิดขึ้นได้ภายใต้เงื่อนไขหรือสภาพแวดล้อมหนึ่ง ๆ และวิเคราะห์ผลกระทบที่เป็นไปได้ และโอกาสที่จะเกิดเหตุการณ์ดังกล่าวของแต่ละสถานการณ์

การวิเคราะห์สถานการณ์อาจถูกคาดหวังว่าทั้งภัยคุกคาม (Threat) และโอกาสเกิดอาจพัฒนาและใช้สำหรับความเสี่ยงทุก ๆ ประเภทรวมถึงความเสี่ยงระยะสั้นและความเสี่ยงระยะยาว สำหรับความเสี่ยงระยะสั้นถ้าหากมีข้อมูลที่ดีสถานการณ์ที่ระบุจะมีความใกล้เคียงกับปัจจุบันมาก สำหรับความเสี่ยงระยะยาวหรือมีข้อมูลที่ไม่ชัดเจน การวิเคราะห์สถานการณ์จะต้องใช้จินตนาการมากและอาจใช้เป็นการวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นในอนาคตได้ การวิเคราะห์สถานการณ์จะเป็นประโยชน์อย่างมากเมื่อมีการแบ่งระหว่างผลลัพธ์ที่เกิดในทางบวกและทางลบในเรื่องของสถานที่ เวลา กลุ่มของธุรกิจ หรือลักษณะองค์กร

ในการวิเคราะห์สถานการณ์สิ่งที่จำเป็นคือทีมของกลุ่มคนที่มีความเข้าใจในธรรมชาติของการเปลี่ยนแปลงที่เกี่ยวข้องกันเช่น การเปลี่ยนแปลงของเทคโนโลยีที่เป็นไปได้ และจินตนาการถึงการเปลี่ยนที่จะอาจเกิดขึ้นโดยไม่จำเป็นต้องคาดคะเนจากอดีตที่ผ่านมา การสร้างภาพหรือข้อมูลเกี่ยวกับการเปลี่ยนแปลงที่เกิดขึ้นจะมีประโยชน์อย่างยิ่งเพื่อเป็นข้อมูลประกอบการวิเคราะห์

1. กระบวนการวิเคราะห์สถานการณ์ (Scenario analysis process)

กระบวนการวิเคราะห์สถานการณ์มีการสร้างทีมงานและช่องทางการสื่อสาร รวมถึงการกำหนดบริบทของปัญหาที่จะพิจารณา ประเด็นที่เกี่ยวข้อง และจะต้องมีการระบุถึงธรรมชาติของการเปลี่ยนแปลงที่อาจเกิดขึ้นของแนวโน้มที่เกิดขึ้นในปัจจุบัน ซึ่งต้องใช้จินตนาการคิดถึงสิ่งที่อาจเกิดขึ้นในอนาคต โดยการเปลี่ยนแปลงที่ต้องพิจารณามีดังนี้

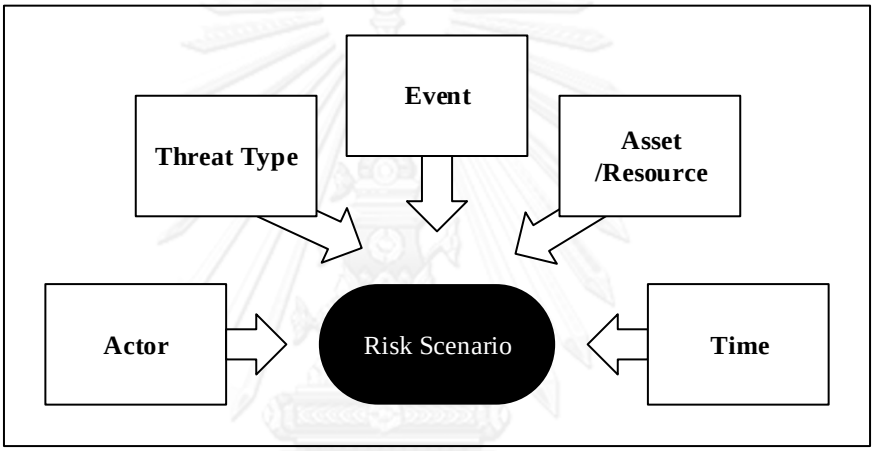
- การเปลี่ยนแปลงจากภายนอกเช่นการเปลี่ยนแปลงของเทคโนโลยีต่าง ๆ
- การตัดสินใจสิ่งที่จำเป็นต้องทำในอนาคตอันใกล้แต่อาจเกิดได้หลายผลลัพธ์
- ความต้องการของผู้ที่เกี่ยวข้องสิ่งที่จำเป็นต้องเปลี่ยนแปลงและกระทบต่อบุคคลเหล่านั้น
- การเปลี่ยนแปลงที่อาจเกิดขึ้นและส่งผลกระทบอย่างมากเช่นการเปลี่ยนแปลงกฎข้อบังคับ การเปลี่ยนแปลงของจำนวนบุคคลกร และอื่น ๆ ซึ่งบางส่วนอาจหลีกเลี่ยงไม่ได้ หรือยังไม่แน่นอน

บางเวลาการเปลี่ยนแปลงอาจเป็นผลมาจากความเสี่ยงอื่น ๆ การวิเคราะห์สถานการณ์เป็นการกำหนดส่วนหนึ่งหรือความเป็นไปได้หนึ่งของเหตุการณ์สิ่งที่สำคัญคือต้องมั่นใจได้ว่าสถานการณ์ที่กำหนดไว้มีการระบุถึงความเป็นไปได้ของผลลัพธ์ที่เกิดขึ้นเพื่อที่จะนำกรอบงานของความเสี่ยงนั้น ๆ ไปใช้ได้จริง

สิ่งที่ได้จากกระบวนการวิเคราะห์สถานการณ์อาจไม่ใช่สถานการณ์ที่เหมาะสมที่สุดแต่เป็นสถานการณ์ที่สามารถเข้าใจได้อย่างชัดเจน ทั้งขอบเขตของทางเลือกและวิธีการในการเปลี่ยนแปลง ผลที่จะเกิดขึ้นจากสาเหตุของการกระทำต่าง ๆ ที่จะเร่งให้เกิดการเปลี่ยนแปลง

2. องค์ประกอบของการวิเคราะห์สถานการณ์ความเสี่ยง (Risk scenario analysis component) [3]

ในการวิเคราะห์สถานการณ์ความเสี่ยง ISACA (Information Systems Audit and Control Association) ซึ่งเป็นองค์กรหนึ่งที่ทำหน้าที่ในการกำกับดูแลและพัฒนาองค์ความรู้และแนวทางการปฏิบัติสำหรับการบริหารระบบสารสนเทศ ได้จัดองค์ประกอบที่ใช้ในการวิเคราะห์สถานการณ์ความเสี่ยงดัง ภาพที่ 2



ภาพที่ 2 องค์ประกอบการวิเคราะห์สถานการณ์

การวิเคราะห์สถานการณ์โดยใช้องค์ประกอบดัง ภาพที่ 2 จะช่วยให้การสร้างหรือจำลองสถานการณ์มีความสมบูรณ์และมีความชัดเจนโดยต้องมีการระบุถึงรายละเอียดดังนี้

- Actor คือผู้ที่ทำให้เกิดภัยคุกคามหรือความเสี่ยง
- Threat Type คือลักษณะของเหตุการณ์หรือภัยคุกคามที่อาจเกิดขึ้นได้
- Event คือสถานการณ์ของเหตุการณ์หนึ่ง ๆ ซึ่งบรรยายถึงสิ่งที่เกิดขึ้น
- Asset/Resource คือทรัพย์สินหรือทรัพยากรที่ได้รับผลกระทบจากสถานการณ์นั้น
- Time คือลักษณะของเวลาที่เกี่ยวข้องกับสถานการณ์นั้นเช่น ระยะเวลาที่เกิดหรือระยะห่างของเวลาเมื่อเกิดสถานการณ์นั้นขึ้นกับผลกระทบที่ตามมา

3. ข้อดีและข้อเสียของการวิเคราะห์สถานการณ์

การวิเคราะห์สถานการณ์สามารถใช้ในการทำนายถึงสถานการณ์ต่าง ๆ ที่เป็นไปได้ในอนาคต โดยวิธีการทั่วไปจะขึ้นอยู่กับการตั้งสมมติฐานทั้งในระยะใกล้ กลางและไกลในการจำลองเหตุการณ์ โดยการใช้แนวโน้มของข้อมูลเหตุการณ์ในอดีตในการทำนายเหตุการณ์ที่จะเกิดขึ้น นี่เป็นวิธีที่

ความสำคัญถ้าหากเราจะทำนายเหตุการณ์ที่จะเกิดขึ้นแต่มีองค์ความรู้ไม่มากนักและเป็นพื้นฐานในการคาดการณ์หรือมีการพิจารณาเหตุการณ์ในอนาคตในระยะยาว

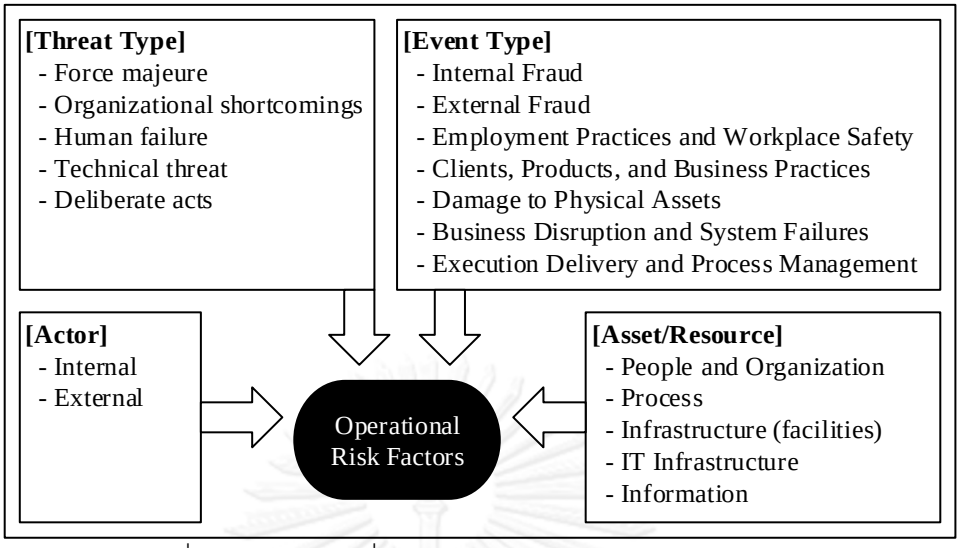
อย่างไรก็ตามการวิเคราะห์สถานการณ์ก็อาจมีจุดอ่อนเมื่อมีความไม่แน่นอนหรือเหตุการณ์ที่จำลองขึ้นไม่มีความใกล้เคียงกับความเป็นจริง ความยากของการวิเคราะห์สถานการณ์จะเกี่ยวข้องกับข้อมูลที่มี และความสามารถของการวิเคราะห์และผู้ตัดสินใจในการจำลองเหตุการณ์ที่เป็นไปได้จริงและสามารถบอกได้ว่าผลกระทบจะเป็นอย่างไร

สิ่งที่สำคัญถ้ามีการใช้การวิเคราะห์สถานการณ์เป็นเครื่องมือในการตัดสินในการจัดการกับความเสี่ยงในสถานการณ์ต่าง ๆ ถ้าหากมีองค์ความรู้ที่ไม่เพียงพอ ข้อมูลที่ได้อาจเป็นความคิดเห็นที่ไม่เป็นกลางและได้ผลที่ไม่สมจริงและไม่สามารถนำไปใช้งานได้จริง

2.1.3 ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) [4]

ความเสี่ยงด้านการปฏิบัติการได้ถูกให้คำนิยามไว้ว่าเป็นความเสี่ยงของความเสียหายที่เป็นผลมาจากความไม่เพียงพอหรือความล้มเหลวภายในของกระบวนการ คนหรือระบบ หรือเกิดจากเหตุการณ์ภายนอก ความเสี่ยงด้านการปฏิบัติการเป็นหนึ่งในประเภทของความเสี่ยงของธุรกิจทางด้านธนาคารและองค์กรที่ให้บริการทางด้านการเงินที่ทาง Basel II ได้กำหนดไว้ Basel II เป็นองค์กรอันดับที่สองของคณะกรรมการของ Basel ที่ให้คำปรึกษาและคำแนะนำสำหรับธนาคารหรือองค์กรทางด้านการเงินโดยเฉพาะ โดยมีวัตถุประสงค์ในการสร้างมาตรฐานและกฎข้อบังคับสำหรับการกำหนดค่าความต้องการขั้นต่ำของเงินทุนของสถาบันทางด้านการเงินเพื่อสร้างความมั่นใจและสร้างสภาพคล่องให้องค์กร

ความเสี่ยงทางด้านปฏิบัติการเป็นหนึ่งในประเภทของความเสี่ยงของธุรกิจทางด้านการธนาคารและองค์กรที่ให้บริการทางด้านการเงิน การประเมินความเสี่ยงทางด้านปฏิบัติการสำหรับสถาบันการเงินมักใช้เทคนิคการวิเคราะห์สถานการณ์ (Scenario Analysis) ซึ่งเป็นการพัฒนาโมเดลที่ใช้อธิบายเกี่ยวกับอนาคตที่อาจเกิดขึ้นได้ โมเดลดังกล่าวจะถูกใช้ในการระบุความเสี่ยงโดยพิจารณาจากการพัฒนาสถานการณ์ที่เป็นไปได้ในอนาคต ประกอบกับผลกระทบที่จะเกิดขึ้นเมื่อเหตุการณ์นั้นเกิดขึ้นจริง ซึ่งความเป็นไปได้ของแต่ละสถานการณ์ขึ้นอยู่กับความรุนแรงหรือผลกระทบที่จะเกิดขึ้นจากการวิเคราะห์ความเสี่ยงและปัจจัยของความเสี่ยงทางด้านการปฏิบัติการที่สำคัญแสดงดังภาพที่ 3



ภาพที่ 3 ปัจจัยความเสี่ยงทางด้านการปฏิบัติการได้จากมาตรฐาน

รายละเอียดของปัจจัยความเสี่ยงทางด้านการปฏิบัติการแสดงดังต่อไปนี้

1. Actor คือผู้ที่ก่อให้เกิดภัยคุกคาม ผู้กระทำสามารถมาได้จากภายในและภายนอก อาจเกิดจากมนุษย์หรือไม่ใช่มนุษย์ก็ได้ [3]
   - Internal actor เป็นผู้กระทำที่มาจากภายในองค์กรเช่นพนักงานบริษัท หรือผู้ที่จ้างมาทำงานในระยะเวลาหนึ่ง อื่น ๆ
   - External actor เป็นผู้กระทำที่มาจากภายนอกยกตัวอย่างเช่น คู่แข่งทางด้านการค้า กฎข้อบังคับ รวมถึงกลุ่มเป้าหมายทางด้านการค้าและอื่น ๆ
2. Threat Type หมายถึงลักษณะโดยธรรมชาติของเหตุการณ์เช่นความล้มเหลวของมนุษย์ภัยทางธรรมชาติและอื่น ๆ ไม่จำเป็นที่ประเภทของภัยคุกคามทุกประเภทต้องการผู้กระทำ โดยประเภทของภัยคุกคามได้ถูกแบ่งไว้ดังนี้ [5]
   - เหตุสุดวิสัย (Force majeure)
   - ข้อบกพร่องขององค์กร (Organizational shortcomings)
   - ความล้มเหลวของมนุษย์ (Human failure)
   - ภัยคุกคามทางเทคนิค (Technical threat)
   - การกระทำโดยเจตนา (Deliberate acts)
3. Event Type หมายถึงเหตุการณ์การปฏิบัติงานที่อาจก่อให้เกิดความเสียหาย สถานการณ์หนึ่ง ๆ ประกอบด้วย 1 เหตุการณ์ซึ่งอาจเกิดจากการใช้งานที่ไม่เหมาะสมทั้งจากภายในและภายนอก หรือเป็นเหตุการณ์ที่ขัดขวางการทำงานของระบบ โครงการและอื่น ๆ โดยมีการจำแนกไว้ดังนี้ [6]

- การทุจริตภายใน (Internal Fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายในองค์กร เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าวตกแก่พวกพ้องของตนเอง เช่น ปลอมแปลงเช็ค การปลอมแปลงแปลงเอกสาร การยักยอก หรือการรับสินบน เป็นต้น
- การทุจริตภายนอก (External Fraud) เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอกองค์กร แต่ก่อให้เกิดความเสียหายโดยตรงต่อสถาบันการเงิน เช่น การปลอมแปลงเช็ค การปลอมแปลงเอกสารทางการเงิน การฉ้อโกง เป็นต้น
- การจ้างงานและความปลอดภัยในสถานที่ปฏิบัติงาน (Employment Practices and Workplace Safety) เป็นความเสี่ยงที่เกิดขึ้นจากกระบวนการจ้างงานที่ไม่เหมาะสม การจ่ายค่าตอบแทน หรือการปฏิบัติต่อพนักงานอย่างไม่เป็นธรรม ซึ่งอาจก่อให้เกิดการฟ้องร้อง การลาออก หรือการหยุดงานประท้วงได้ นอกจากนี้ยังรวมถึงความเสี่ยงที่เกิดขึ้นเนื่องจากการกำหนดมาตรการรักษาความปลอดภัยในการปฏิบัติงาน และการควบคุมสภาพแวดล้อมในการปฏิบัติงานที่ไม่เพียงพอ จนส่งผลกระทบต่อสุขภาพของพนักงาน อันเนื่องมาจากโรคภัย หรือได้รับบาดเจ็บจากอุบัติเหตุอันเนื่องมาจากการปฏิบัติงานได้
- ลูกค้า ผลิตภัณฑ์ และวิธีปฏิบัติในการดำเนินธุรกิจ (Clients, Products, and Business Practices) เป็นความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจ กระบวนการออกผลิตภัณฑ์ และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสม ไม่เป็นไปตามกฎหมาย ระเบียบและข้อบังคับที่ทางการกำหนด เช่น การทำธุรกรรมที่ละเมิดกฎหมาย การดำเนินธุรกรรมที่ไม่ได้รับอนุญาต การทำธุรกรรมที่เกี่ยวข้องกับการฟอกเงิน และการที่สถาบันการเงินนำข้อมูลความลับของลูกค้าไปหาประโยชน์ เป็นต้น
- ความปลอดภัยของทรัพย์สิน (Damage to Physical Assets) เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของสถาบันการเงินอันเนื่องมาจากอุบัติเหตุต่างๆ เช่นอุบัติเหตุ อัคคีภัย ภัยธรรมชาติ การทำลายทรัพย์สิน การจลาจล การก่อความไม่สงบทางการเมือง การก่อวินาศภัย เป็นต้น
- การขัดข้องและหยุดชะงักของระบบงานและระบบคอมพิวเตอร์ (Business Disruption and System Failures) เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปรกติ หรือการหยุดทำงานด้านระบบงานด้านต่างๆ เช่น ความไม่สอดคล้องกันหรือความแตกต่างของระบบงานที่เกิดจากการควบรวมกิจการ ความบกพร่องของระบบงานคอมพิวเตอร์และระบบเครือข่าย รวมถึงการใช้เครื่องมือและเทคโนโลยีที่ไม่เหมาะสม ล้าสมัย และไม่มีประสิทธิภาพ เป็นต้น
- การจัดการกระบวนงาน (Execution Delivery and Process Management) เป็นความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน ความผิดพลาดของระบบ

ปฏิบัติงาน หรือ ความผิดพลาดจากการปฏิบัติงานของพนักงานภายในสถาบันการเงินและพนักงานจากการจ้างงานภายนอก เช่น การนำเข้าข้อมูลผิดพลาด การประเมินมูลค่าหลักประกันไม่ถูกต้อง การไม่ปฏิบัติตามสัญญาการจ้างงานตามสัญญางานจากภายนอก การขาดความรู้ความเข้าใจในการปฏิบัติงานและการใช้ระบบคอมพิวเตอร์ของพนักงาน การปรับปรุงกระบวนการทำงานที่ไม่เหมาะสม รวมถึงการจัดทำนิติกรรมสัญญาและเอกสารทางกฎหมายที่ไม่สมบูรณ์ ทำให้ไม่สามารถใช้บังคับได้ตามกฎหมาย เป็นต้น

4. Asset/Resource เป็นทรัพย์สินหรือทรัพยากรที่ถูกกระทบโดยการกระทำในสถานการณ์ดังกล่าว ทรัพย์สิน คือวัตถุใด ๆ ที่มีค่าต่อองค์กรซึ่งได้รับผลกระทบจากเหตุการณ์และทำให้เกิดผลกระทบทางธุรกิจ ทรัพยากรคือสิ่งใด ๆ ก็ตามที่ช่วยให้การทำงานสำเร็จตามเป้าหมาย ทรัพย์สินและทรัพยากรอาจเป็นสิ่งเดียวกันก็ได้ยกตัวอย่าง เช่น โครงสร้างพื้นฐานทางด้านสารสนเทศเป็นทรัพยากรที่มีความสำคัญและในขณะเดียวกันโครงสร้างพื้นฐานนั้นก็เป็นทรัพย์สินเนื่องจากมันก่อให้เกิดมูลค่าทางธุรกิจ ซึ่งมีแบ่งได้ดังนี้ [3]

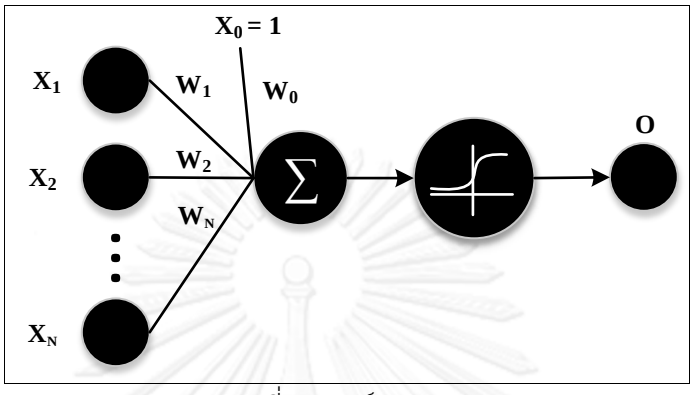
   - บุคลากรและองค์กร (People and Organization)
   - กระบวนการทำงาน (Process)
   - โครงสร้างพื้นฐานหรือสิ่งอำนวยความสะดวก (Infrastructure-facilities)
   - โครงสร้างพื้นฐานทางด้านสารสนเทศ (IT Infrastructure)
   - ข้อมูล (Information)

2.1.4 แบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก (Back Propagation Neural Networks) [7, 8]

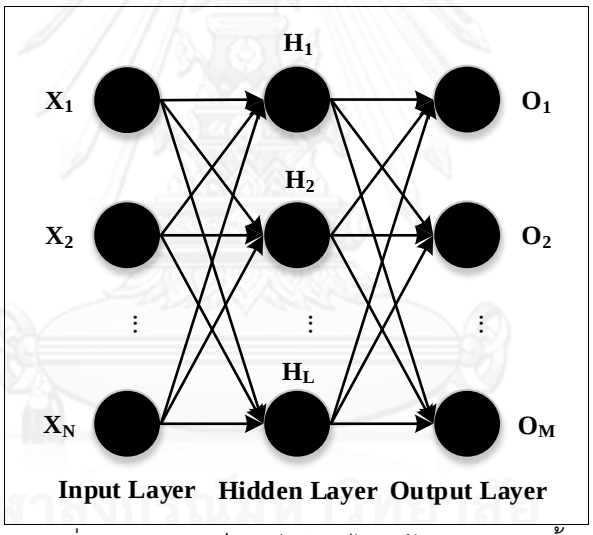
โครงข่ายประสาทเทียม (Artificial Neural Networks— ANN) เป็นการเรียนรู้ของเครื่องแบบมีการชี้นำ (Supervised learning) ที่มีแนวความคิดเลียนแบบการทำงานของระบบประสาทมนุษย์ หน่วยย่อยที่สุดของ ANN เรียกว่า เพอร์เซปตรอน (perceptron) เป็นโครงข่ายประสาทเทียมแบบง่ายที่มีหน่วยเดียว ซึ่งจำลองลักษณะของเซลประสาท (neuron) ของมนุษย์ เพอร์เซปตรอนทำหน้าที่รับอินพุตเป็นเวกเตอร์จำนวนจริงเข้ามาแล้วคำนวณหาผลรวมเชิงเส้น (linear combination) แบบถ่วงน้ำหนักของอินพุต (x1, x2, ..., xn) โดยที่ค่า w1, w2, ..., wn ใน ภาพที่ 4 เป็นค่าน้ำหนักของอินพุต และให้เอาท์พุต (o) เป็นค่าคงที่ที่แตกต่างกันตามค่าผลรวมที่ได้ว่ามีค่าเกินค่าขีดแบ่ง (θ) หรือไม่ ทั้งนี้ค่าเอาท์พุตจะต่างกันไปตามฟังก์ชันกระตุ้น (activation function) ที่ใช้เป็นฟังก์ชันเอาต์พุต เอาต์พุตที่ได้จะถูกนำไปคำนวณค่าผิดพลาด (error) เพื่อนำมาปรับน้ำหนักของอินพุตต่อไป ส่วน w0 ใน ภาพที่ 4 เป็นค่าลบของค่าขีดแบ่ง และ x0 เป็นอินพุตเทียมกำหนดให้มีค่าเป็น 1 เสมอ

เพอร์เซปตรอนเดี่ยวสามารถแสดงได้แค่ระนาบตัดสินใจเชิงเส้นเท่านั้น ในการใช้งานจริงที่มีความซับซ้อน เช่น การรู้จำ (recognition) จำเป็นต้องใช้โครงข่ายหลายชั้น (multilayer network)

และฟังก์ชันเอาต์พุตที่ไม่ใช่เชิงเส้น จึงจะสามารถแสดงระนาบตัดสินใจแบบไม่เชิงเส้น (nonlinear decision surface) ที่มีความซับซ้อนมากกว่าได้ ตัวอย่างเช่น เน็ตเวิร์กป้อนไปหน้าแบบหลายชั้น (Multilayer Feedforward network - MLFF) ตัวอย่างดังแสดงใน ภาพที่ 5 ซึ่งใช้ร่วมกับอัลกอริทึมแบ็คพรอพาเกชัน (Backpropagation) เพื่อเรียนรู้ค่าเวกเตอร์น้ำหนัก



ภาพที่ 4 เพอร์เซปตรอน



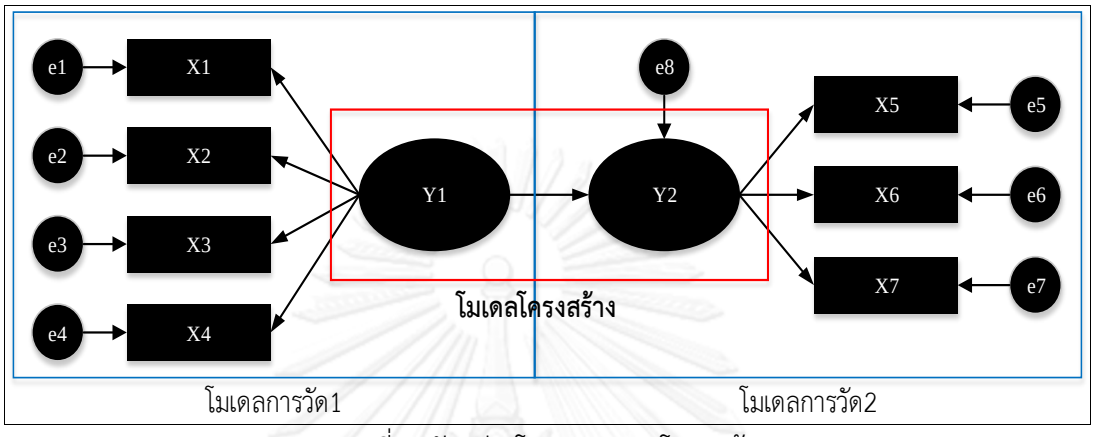
ภาพที่ 5 ตัวอย่างเน็ตเวิร์กป้อนไปหน้าแบบหลายชั้น

2.1.5 โมเดลสมการโครงสร้าง (Structural Equation Model: SEM) [9, 10]

โมเดลสมการโครงสร้างเป็นโมเดลหนึ่งที่รวบรวมแนวคิดที่เกี่ยวข้องกับการวิเคราะห์ตัวแปรหลายตัวแปรซึ่งช่วยในการหาสาเหตุหรือความสัมพันธ์โดยใช้หลักการของการวิเคราะห์การถดถอยแบบพหุ เพื่อวิเคราะห์และตรวจสอบโครงสร้างความสัมพันธ์ของข้อมูลแบบหลายตัวแปรทั้งตัวแปรอิสระ (Independent variable) และตัวแปรแฝง (Latent variable) ตั้งแต่สองตัวขึ้นไปและนำเสนอผลลัพธ์ด้วยค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation Coefficient) และแผนภาพโมเดลเส้นทาง (Path model) โดยความสัมพันธ์จะแสดงด้วยเส้นตรงที่มีหัวลูกศรแสดงทิศทางของความสัมพันธ์ และค่าความสัมพันธ์แสดงด้วยค่าสัมประสิทธิ์ที่กำกับอยู่บนเส้นความสัมพันธ์นั้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตัวแปรสังเกตได้เป็นตัวแปรที่ผู้วิจัยสามารถเก็บหรือวัดได้โดยตรงเช่นการสร้างคำถามคำตอบจากแบบสองถามโดยมีระดับความคิดเห็นให้เลือก ซึ่งตัวแปรสังเกตได้จะใช้สัญลักษณ์เป็นรูปสี่เหลี่ยม ส่วนตัวแปรแฝงเป็นตัวแปรที่ผู้วิจัยไม่สามารถเก็บได้โดยตรงเกิดจากการนำตัวแปรสังเกตได้มากำหนดเป็นตัวแปรใหม่ เพื่อใช้แทนตัวแปรสังเกตได้หลาย ๆ ตัวแปร โดยใช้สัญลักษณ์เป็นรูปวงรี



ภาพที่ 6 ตัวอย่างโมเดลสมการโครงสร้าง

โดยทั่วไป โมเดลสมการโครงสร้างจะประกอบด้วย 2 โมเดลคือ โมเดลการวัด (Measurement Model) และโมเดลโครงสร้าง (Structural Model) โดยรูปตัวอย่างของโมเดลสมการโครงสร้างแสดงดัง ภาพที่ 6

ภาพที่ 6 เป็นแผนภาพของโมเดลสมการที่มีสองโมเดลการวัดโดยมีตัวแปรสังเกตได้อยู่ 7 ตัว คือ X1-X7 และปัจจัยแฝง 2 ตัวคือ Y1 และ Y2 โดยค่า e1-e8 เป็นค่าความคลาดเคลื่อนที่เกิดจากการประมานค่าของตัวแปรนั้น ๆ โดยตัวอย่างโมเดลสมการโครงสร้างนี้ ต้องการหาอิทธิพลของปัจจัยแฝง Y1 ที่มีต่อปัจจัยแฝง Y2 จากตัวแปรที่มีอยู่ทั้งหมดโดยปัจจัย Y1 สามารถวัดได้จากตัวแปร X1-X4 และปัจจัย Y2 สามารถวัดได้จากตัวแปร X5-X7

โมเดลสมการโครงสร้างสามารถแบ่งออกเป็นประเภทหลัก ๆ ได้ 4 ประเภท ดังนี้

1. การวิเคราะห์เส้นทาง (Path Analysis: PA) เป็นการศึกษาค่าอิทธิพลของตัวแปรที่ต้องการศึกษาความสัมพันธ์ในทางตรงและทางอ้อมโดย ตัวแปรที่นำมาต้องเป็นตัวแปรสังเกตได้เท่านั้น ซึ่งมีรายละเอียดดังข้อ 2.1.6
2. การวิเคราะห์เชิงปัจจัยยืนยัน (Confirmatory Factor Analysis: CFA) เป็นการวิเคราะห์หรือการสร้างปัจจัยแฝงซึ่งการสร้างควรมีทฤษฎีรองรับ หรือมีงานวิจัยก่อนหน้ามายืนยันความสัมพันธ์
3. การวิเคราะห์สมการโครงสร้าง (Structural Regression Model: SR) เป็นการวิเคราะห์ความถดถอยของทั้งตัวแปรสังเกตได้และตัวแปรแฝง
4. โมเดลโค้งการพัฒนา (Latent Growth Model: LGM) เป็นการศึกษาถึงความเปลี่ยนแปลงของการวัดเมื่อเวลามีการเปลี่ยนไป โดยจะทำการเก็บข้อมูลจากองค์กรหรือหน่วยงานเดิมหลาย ๆ ครั้ง

2.1.6 การวิเคราะห์เส้นทาง [9, 10]

การวิเคราะห์เส้นทางคือ เทคนิคทางด้านสถิติที่ใช้ในการพิจารณาความสัมพันธ์ระหว่างตัวแปรทั้งทางตรง (Direct effect) และทางอ้อม (Indirect effect) ตัวแปรต่าง ๆ จะถูกประเมินโดยแก้ปัญหาสมการโครงสร้าง (Structural equation) เพื่อทดสอบความเหมาะสมของค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation) ระหว่างโมเดลเชิงสาเหตุ (Causal model) ตั้งแต่ 2 โมเดลขึ้นไป เพื่อให้ได้โมเดลที่มีความเหมาะสมกับข้อมูลนั้น ๆ โดยโมเดลดังกล่าวจะถูกตั้งขึ้นโดยผู้วิจัย

การวิเคราะห์เส้นทางเป็นหนึ่งในการวิเคราะห์ทางด้านสถิติซึ่งใช้หลักการของการวิเคราะห์สมการถดถอยแบบหลายตัวแปร (Multiple Regressive Analysis) เป็นวิธีการที่อยู่ในกลุ่มเดียวกับการวิเคราะห์สมการโครงสร้าง ซึ่งเป็นวิธีการในการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรเดียวกับตัวแปรอื่นๆ การวิเคราะห์เส้นทางเป็นวิธีการที่ใช้ในการอธิบายความสัมพันธ์ระหว่างตัวแปร [Kline, 2005] โดยการสร้างแผนภาพเส้นทางที่แสดงอิทธิพลของตัวแปรต้นและตัวแปรตาม เพื่อศึกษาถึงความเป็นเหตุเป็นผลของความสัมพันธ์ซึ่งข้อมูลดังกล่าวจะถูกใช้ในการอธิบายสาเหตุและผลกระทบที่อาจเกิดขึ้นของปรากฏการณ์ต่างๆ ทั้งในทางด้านการแพทย์ ทางสังคม ทางด้านวิศวกรรม และอื่นๆ

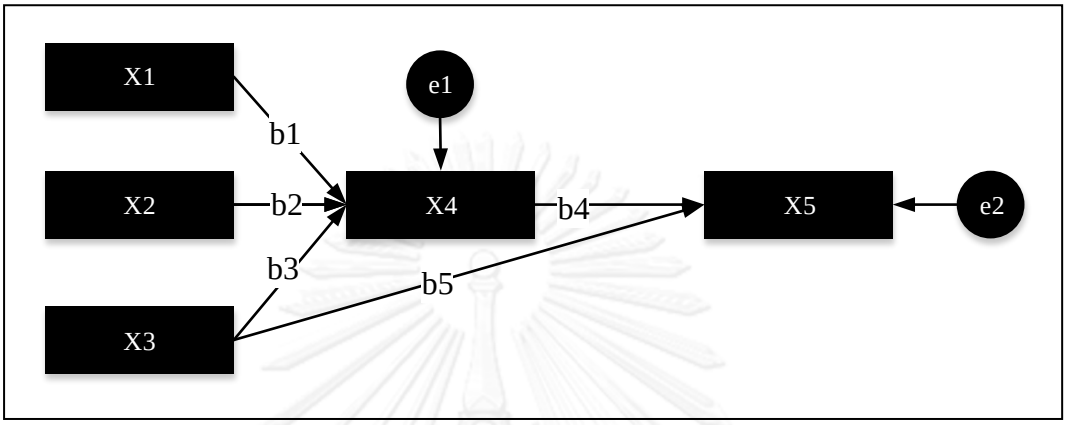
เป้าหมายหนึ่งของนักวิจัยทางด้านสังคมคือเพื่อเข้าใจระบบสังคมความเป็นไปของสังคมในปัจจุบันผ่านทางความสัมพันธ์เชิงเหตุและผล (Causal relationship) ที่เกิดขึ้น อย่างไรก็ตามการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรที่มีความซับซ้อนยังเป็นงานที่ยาก การวิเคราะห์เส้นทางจึงเป็นวิธีหนึ่งที่ช่วยนักวิจัยสามารถเข้าใจความสัมพันธ์ดังกล่าว โดยใช้ข้อมูลเชิงปริมาณ (Quantitative data) ในการค้นหาความสัมพันธ์ของตัวแปรเพื่อให้ได้ผลลัพธ์ที่มีความจำเพาะต่อข้อมูลที่ใช้วิจัย การวิเคราะห์เส้นทางเป็นส่วนขยายของการวิเคราะห์สมการถดถอยแบบหลายตัวแปร และใช้การประมาณขนาดและความรุนแรงของผลกระทบในระบบการตั้งสมติฐานที่เป็นเหตุเป็นผล

การวิเคราะห์เส้นทางเป็นการประเมินปริมาณของผลกระทบจากผลลัพธ์ที่แตกต่างกัน ความสัมพันธ์ระหว่างตัวแปรจะถูกอธิบายในรูปของค่าสัมประสิทธิ์สหสัมพันธ์และแสดงถึงสมติฐานที่กำหนด ดังนั้นความสัมพันธ์หรือเส้นทาง (Pathway) ไม่สามารถทดสอบทางสถิติในเรื่องของทิศทางและโมเดลต่าง ๆ เหล่านั้นไม่สามารถพิสูจน์หาสาเหตุด้วยตัวเองได้ อย่างไรก็ตามโมเดลการวิเคราะห์เส้นทางจะสะท้อนทฤษฎีที่เกี่ยวข้องกับสาเหตุและทำให้ผู้วิจัยทราบถึงสาเหตุในสมติฐานที่ตั้งไว้เมื่อโมเดลที่สร้างขึ้นนั้นมีความเหมาะสมโดยจะแสดงรูปแบบของความสัมพันธ์จากเซตของข้อมูลที่ใช้ในการวิจัย

ข้อดีอย่างหนึ่งในการใช้การวิเคราะห์เส้นทางคือวิธีนี้จะบังคับให้ผู้วิจัยระบุตัวแปรที่เกี่ยวข้องและส่งเสริมให้การพัฒนาโมเดลมีความชัดเจนและเป็นไปตามลอจิกของทฤษฎีที่ใช้อ้างอิงที่เกี่ยวข้องกับสิ่งที่มีอิทธิพลต่อผลลัพธ์ที่ออกมาโดยเฉพาะ นอกจากนั้นการวิเคราะห์เส้นทางยังอนุญาตให้นักวิจัยในการแตกองค์ประกอบปัจจัยหลายๆ อย่างที่ส่งผลถึงผลลัพธ์ที่ได้ออกมาเป็นส่วนย่อยๆ ทั้งองค์ประกอบที่ส่งผลทางตรงและทางอ้อม

จาก ภาพที่ 7 แสดงโมเดลการวิเคราะห์เส้นทางที่มีตัวแปรสังเกตได้ทั้งหมด 5 ตัวแปร โดยตัวแปรหนึ่งสามารถมีสถานะเป็นตัวแปรสาเหตุและตัวแปรผลได้ในเวลาเดียวกัน ซึ่งได้แก่ตัวแปร X4

การวิเคราะห์อิทธิพลของคู่ตัวแปรหนึ่ง ๆ ต้องสนใจทั้งอิทธิพลทางตรงและทางอ้อม ยกตัวอย่าง อิทธิพลของตัวแปร X3 ที่มีต่อตัวแปร X5 คือ b5 + (b3*b4) เรียกว่าอิทธิพลรวม โดย b5 เป็นค่าอิทธิพลทางตรงของตัวแปร X3 กับ X5 , b3 เป็นค่าอิทธิพลทางตรงของตัวแปร X3 กับ X4 และ b4 เป็นค่าอิทธิพลของตัวแปร X4 กับ X5 ซึ่ง b3*b4 เป็นอิทธิพลทางอ้อมของตัวแปร X3 กับ X5



ภาพที่ 7 ตัวอย่างโมเดลการวิเคราะห์เส้นทาง

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 Quality of security metrics and measurement [11]

งานวิจัยนี้นำเสนอผลของการสำรวจความคิดเห็นของผู้เชี่ยวชาญทางด้านมาตรวัดความมั่นคงปลอดภัยเชิงปริมาณจำนวน 141 คนและการสัมภาษณ์ ในการจัดลำดับความสำคัญของ 19 เกณฑ์ (Criteria) การวัดคุณภาพของมาตรวัดทางด้านความมั่นคงปลอดภัย โดยมีระเบียบวิธีการวิจัย คือ นำเกณฑ์ทั้ง 19 อย่าง ที่ได้มีการระบุในการทบทวนงานวิจัยไปให้ผู้เชี่ยวชาญที่เข้าร่วมจัดอันดับ โดยมีค่าตั้งแต่ 1-19 เมื่อได้ผลการจัดอันดับมาแล้วก็นำข้อมูลนั้นไปทำการปรับช่วงค่าในการจัดอันดับความคิดเห็น (Normalized Prioritization Opinion) ด้วยสมการ (1) เพื่อให้ค่าที่ได้อยู่ในช่วง $[e^{-6},1]$ และง่ายต่อการทำความเข้าใจ

$$\bar{\Omega}_{i,j} = \frac{e^{\Omega_{i,j}/3}}{e^{max(\Omega_{i,j})/3}} = \frac{e^{\Omega_{i,j}/3}}{e^{19/3}}, \quad \bar{\Omega}_{i,j} \epsilon [e^{-6}, 1] \tag{1}$$

ค่า j ∈ [2 19] เป็นค่าหมายเลขคุณภาพมิติที่ทำการวิจัย ค่า I ∈ G โดย G เป็นกลุ่มของผู้เชี่ยวชาญ ค่า Ω ∈ {1, 2, ..., 19} เป็นค่าการจัดอันดับมิติคุณภาพ

$$\mu_{j,G}(\Omega) = \frac{1}{n_G} \sum_{i=1}^{n_G} \Omega_{i,j} \tag{2}$$

$$\mu_{j,G}(\bar{\Omega}) = \frac{1}{n_G} \sum_{i=1}^{n_G} \bar{\Omega}_{i,j} \tag{3}$$

จากนั้นนำค่าที่ได้ไปผ่านการคำนวณทางด้านสถิติ คือ หาค่าเฉลี่ย (Mean) ของการจัดอันดับความคิดเห็นในแต่ละมิติคุณภาพด้วยสมการ (2) และ (3) โดย n_G คือจำนวนผู้เชี่ยวชาญในแต่ละกลุ่ม และหาค่าความแปรปรวน สำหรับใช้ในการวิเคราะห์การกระจายข้อมูลของการจัดอันดับมิติคุณภาพด้วยสมการ (4)

$$S_{j,R}^2(\Omega) = \frac{1}{M-1}\sum_{i=1}^{M}(\Omega_{i,j} - \mu_{j,R}(\Omega)^2) \quad (4)$$

หลังจากนั้น นำค่าที่ได้จากการสำรวจไปทำการจัดกลุ่มโดยใช้วิธี *k*-means ด้วยสมการที่ (5) กำหนดค่า *k* มีค่าเป็น 6 เพื่อแบ่งกลุ่มความคิดเห็นของผู้เชี่ยวชาญในการจัดอันดับของเกณฑ์ในการประเมินมาตรวัดด้านความมั่นคงปลอดภัยตามการวิเคราะห์รูปแบบของการจัดอันดับที่ชัดเจน โดยค่า O_p คือค่าการจัดอันดับของ 19 มิติคุณภาพ ซึ่งอยู่ในรูปแบบของเวกเตอร์ u_m คือค่าเฉลี่ยของการจัดอันดับในแต่ละกลุ่ม C_p และ p มีค่าอยู่ระหว่าง 1 ถึง k

$$WCSS_{\bar{\Omega}} = arg_R min \sum_{m=1}^{k} \sum_{O_p \epsilon C_i} ||O_p - \mu_m||^2 \quad (5)$$

เมื่อแบ่งข้อมูลได้ 6 กลุ่มแล้ว จึงนำข้อมูลที่มีการจัดลำดับความสำคัญของแต่ละกลุ่มมาคำนวณค่าความแปรปรวนอีกครั้งหนึ่ง เพื่อให้ทราบถึงการกระจายของข้อมูลในกลุ่มที่จัดไว้ โดยค่าที่ทำการคำนวณตามสมการที่กล่าวมาแสดงดัง ตารางที่ 1

ตารางที่ 1 Prioritization results of all respondents

j	Quality dimension	μ_{all}	C_1		C_2		C_3		C_4		C_5		C_6	
			p_1	s_1^2	p_2	s_2^2	p_3	s_3^2	p_4	s_4^2	p_5	s_5^2	p_6	s_6^2
1	Correctness	0.528	**1**	0.2	4	7.5	**2**	12.4	8	0.7	7	5.5	8	32.3
2	Measurability	0.378	**3**	19.6	**1**	1.2	**3**	22.5	15	18.2	10	12.6	**3**	8.3
3	Meaningfulness	0.373	4	14.1	**3**	21.9	**1**	0.1	12	19.5	5	33.5	10	30.3
4	Objectivity, unbiasedness	0.260	**2**	12.8	**2**	33.5	4	18.1	**1**	31.1	15	9.0	18	19.0
5	Reproducibility, repeatability, scale reliability	0.204	5	25.4	6	19.3	5	17.5	**3**	5.3	11	22.6	5	13.6
6	Effectiveness	0.168	10	23.2	10	18.4	12	12.1	7	8.6	**1**	0.5	17	4.0
7	Comparability	0.164	7	21.4	5	28.1	11	17.7	9	22.4	19	4.7	4	12.7
8	Attainability, availability, easiness	0.160	6	19.8	7	21.1	6	9.8	13	17.3	6	24.7	6	12.2
9	Clarity, succinctness	0.143	11	23.3	12	12.7	7	24.9	**2**	24.0	9	35.2	**1**	25.8
10	Cost effectiveness	0.140	15	19.7	9	26.4	8	29.2	5	34.9	**2**	18.2	14	31.0
11	Representativeness, contextual specificity	0.113	14	21.7	8	27.0	9	31.1	11	16.3	8	28.2	13	19.0
12	Controllability	0.107	8	19.4	15	19.8	13	24.8	6	6.2	12	26.0	12	25.2
13	Ability to show progression	0.089	17	29.3	16	20.4	10	32.9	4	25.7	17	26.2	11	44.3
14	Efficiency	0.084	16	18.0	11	18.9	14	16.0	17	8.9	4	24.6	9	12.7
15	Non-intrusiveness	0.081	12	34.3	18	23.2	17	25.8	19	0.9	**3**	41.8	16	52.0
16	Completeness	0.076	9	39.6	17	18.8	16	23.7	16	17.4	18	30.9	7	40.3
17	Scalability, portability	0.071	19	17.2	19	8.7	15	15.8	14	47.3	13	31.5	**2**	1.2
18	Granularity	0.062	18	21.6	14	25.7	18	27.9	10	49.8	14	36.8	15	30.0
19	Time dependability	0.055	13	28.7	13	23.5	19	17.3	18	8.9	16	25.5	19	0.3

The bold entries are used to emphasize the three most important quality criteria in each cluster (i.e. all rank numbers 1, 2 and 3).

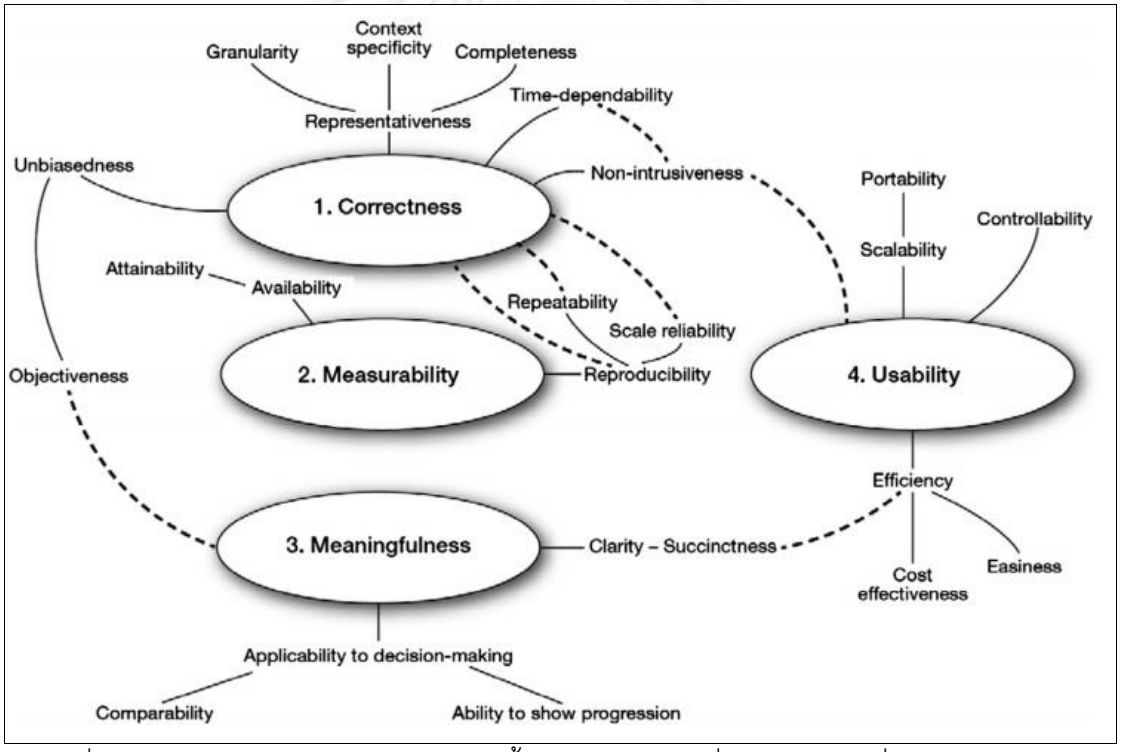
เมื่อทำการแบ่งกลุ่มข้อมูลเรียบร้อยแล้ว ขั้นตอนต่อไปคือการสัมภาษณ์ผู้เชี่ยวชาญ เพื่อวิเคราะห์หาค่าการจัดลำดับความสำคัญเพียง 3 ลำดับแรกของแต่ละกลุ่ม โดยใช้สมการ (6) ในการประเมินความเห็นของผู้ประเมินซึ่งมีค่าตั้งแต่ 0 (no agreement) ถึง 1 (complete agreement) ซึ่งผลที่ได้แสดงในตารางที่ 2

$$W = \frac{12S}{m^2(n^3-n)} \quad (6)$$

ตารางที่ 2 W values for different clusters

Result data	α					
	C_1	C_2	C_3	C_4	C_5	C_6
W	0.378	0.332	0.382	0.605	0.483	0.858
Number of total respondents in cluster	54	28	26	15	11	7
Number of respondents used in W calculation	37	11	16	3	4	2

หลังการวิเคราะห์ผลการวิจัย ได้มีการนำเสนอเป็นโมเดลเชิงแนวคิดสำหรับการใช้เป็นเกณฑ์ในการประเมินมาตรวัดทางด้านความมั่นคงปลอดภัยขึ้นมา เรียกว่า CMM+U (Correctness, Measurability, Meaningfulness + Usability) พร้อมทั้งแสดงความสัมพันธ์ของเกณฑ์ดังกล่าว ดังตารางที่ 8



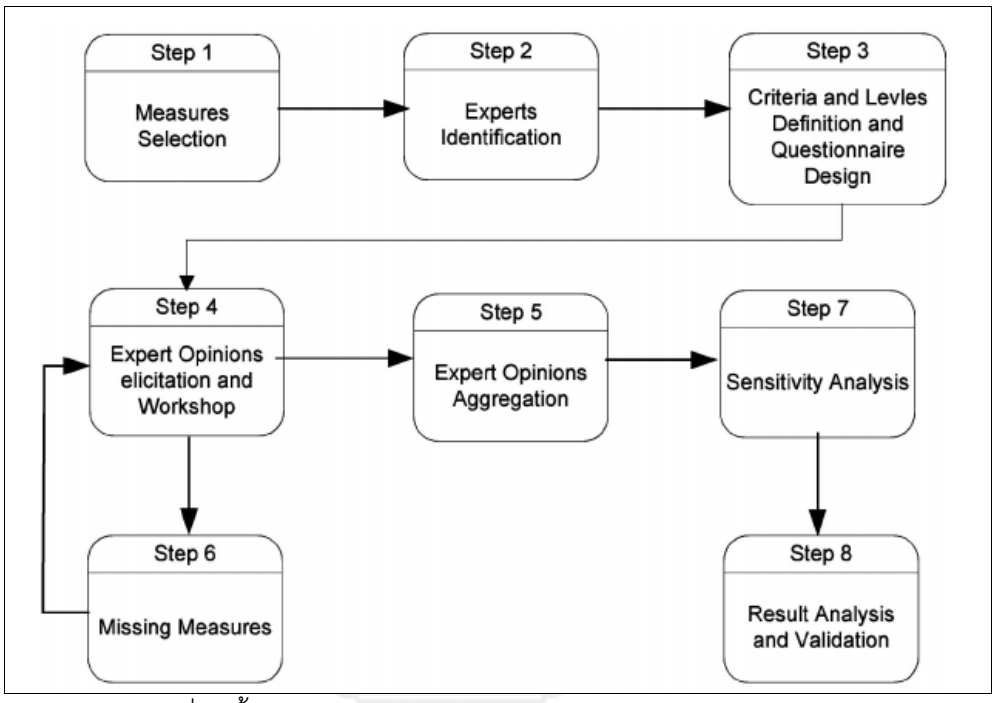
ภาพที่ 8 โมเดลเกณฑ์การวัดคุณภาพของตัวชี้วัดทางด้านความมั่นคงปลอดภัยที่ได้มาของชุดข้อมูล

2.2.2 A Ranking of Software Engineering Measures Based on Expert Opinion [12]

งานวิจัยนี้นำเสนอกรอบงาน (Framework) สำหรับเก็บข้อมูลความคิดเห็นของผู้เชี่ยวชาญ โดยถูกพัฒนาขึ้นเพื่อเลือกวิธีการวัดที่สามารถบ่งชี้ถึงความน่าเชื่อถือทางด้านซอฟต์แวร์ที่ดีที่สุด วิธีการวัดที่เลือกมาเป็น 30 อันดับแรกของวิธีการวัดที่มีการวิจัยโดย Lawrence Livermore National Laboratory มาทำการจัดลำดับโดยมีการให้คะแนนแต่ละวิธีการวัด โดยผู้เชี่ยวชาญจำนวน

10 คน วิธีการให้คะแนนใช้ทฤษฎีคุณลักษณะอรรถประโยชน์หลายทาง (Multi-attribute Utility Theory) เพื่อหาตัวบ่งชี้ที่ดีที่สุด 3 อันดับแรกในแต่ละเฟสของการพัฒนาซอฟต์แวร์

กรอบงานที่ใช้ในการเก็บข้อมูลความคิดเห็นจากผู้เชี่ยวชาญ แบ่งออกเป็น 8 ขั้นตอนหลักดังภาพที่ 9



ภาพที่ 9 ขั้นตอนการจัดลำดับวิธีการวัดทางด้านวิศวกรรมซอฟต์แวร์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 3
วิธีการดำเนินการวิจัย

3.1 แนวคิดในการพัฒนา

ชนิดของการแบ่งกลุ่มของสาเหตุสามารถใช้เป็นจุดเริ่มต้นสำหรับการบริหารความเสี่ยงในการปฏิบัติการได้ การวิจัยนี้นำเสนอวิธีการเชิงปริมาณที่มีประโยชน์ในการบริหารความเสี่ยงขององค์กรทางด้านธนาคารและองค์กรที่บริการทางด้านการเงิน โมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กใช้ในการสร้างและดึงเอาองค์ความรู้ของผู้เชี่ยวชาญในการประเมินผลของความรุนแรงของความเสียหายที่เกิดจากสถานการณ์ที่เกิดขึ้นของความเสี่ยงในการปฏิบัติงาน และโมเดลการวิเคราะห์เส้นทางใช้ในการหาความสัมพันธ์ของสาเหตุความเสี่ยง พร้อมทั้งเปรียบเทียบผลของโมเดลที่ได้ทั้งสองวิธี ซึ่งมีวิธีในการดำเนินการวิจัยดังนี้

3.2 การกำหนดกรอบแนวคิดการวิจัย

ในขั้นตอนนี้ผู้วิจัยได้ดำเนินการโดยการวิเคราะห์เอกสาร มาตรฐานต่าง ๆ รวมถึงงานวิจัยที่เกี่ยวข้อง และรวบรวมข้อมูลโดยใช้แบบสอบถามจากผู้เชี่ยวชาญทางด้านการบริหารความเสี่ยง แล้วนำผลการศึกษามากำหนดกรอบแนวคิดการวิจัย ซึ่งรายละเอียดมีดังนี้

3.2.1 กำหนดโดเมนปัญหา มาตรวัดการจัดอันดับ และปัจจัยที่เกี่ยวข้องกับงานวิจัย

1. ผู้วิจัยทำการเก็บรวบรวมข้อมูลข้อมูล เอกสารและมาตรฐานในการบริหารความเสี่ยงโดยเฉพาะส่วนที่เป็นการวิเคราะห์ความเสี่ยงในด้านการปฏิบัติการ
2. ผู้วิจัยได้วิเคราะห์ข้อมูลจากมาตรฐานและเอกสาร
   - ศึกษาเนื้อหาสาระจากแหล่งข้อมูลต่างๆ เพื่อกำหนดขอบเขตของการศึกษา
   - ทำการกำหนดวัตถุประสงค์เพื่อให้ทราบตัวแปรหรือปัจจัยต่างๆ ที่เกี่ยวข้อง
   - แยกแยะรายละเอียดในปัจจัยของตัวแปรที่ต้องการ เพื่อให้ทราบความสัมพันธ์ของปัจจัย
   - สรุปตัวแปรที่เกี่ยวข้องกับการวิเคราะห์ความเสี่ยงที่จะใช้ในงานวิจัย

3.2.2 รายละเอียดตัวแปรและการกำหนดค่าเกณฑ์ที่ใช้ในการวิจัย

ตัวแปรที่ใช้ในงานวิจัยแบ่งออกเป็น 6 กลุ่มหลัก ๆ คือ Organization Unit, Actor, Threat Type, Loss Event Type, Asset/Resource และ Severity Level ซึ่งแต่ละกลุ่มจะมีความหมายและสัญลักษณ์ที่ใช้แทนค่าในการเก็บข้อมูลดังตารางที่ 3 โดยตัวแปรดังกล่าวแบ่งออกเป็น 2 ประเภท คือตัวแปรสาเหตุและตัวแปรผล

1. ตัวแปรสาเหตุ เป็นตัวแปรที่กำหนดขึ้นโดยมีแนวคิดจากกรอบการทำงานในการวิเคราะห์สถานการณ์ความเสี่ยง [3] ซึ่งพัฒนาจาก ISACA ซึ่งเป็นผู้นำในด้านการเป็นผู้ให้บริการองค์ความรู้ การออกใบรับรอง (Certification) กลุ่มสนับสนุน (Community)

และศึกษาเกี่ยวกับระบบข้อมูล และการรักษาความปลอดภัยขององค์กรในการกำกับดูแลด้านไอทีซึ่งก่อตั้งในปี ค.ศ. 1969 โดยตัวแปรสาเหตุที่กำหนดได้แก่ Actor, Threat Type, Loss Event Type, Asset/Resource และนอกจากนั้นจากการสัมภาษณ์ผู้เชี่ยวชาญเกี่ยวกับการประเมินความเสี่ยงทางด้านการปฏิบัติการจึงทราบว่าความเสี่ยงแต่ละหน่วยงานจะมีความแตกต่างกันไปถึงแม้ว่าจะมีปัจจัยความเสี่ยงเดียวกันดังนั้นผู้วิจัยจึงได้กำหนดตัวแปรเพิ่มอีกหนึ่งตัวแปรคือ Organization Unit

2. ตัวแปรผล ได้แก่ระดับความรุนแรงเมื่อมีเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นซึ่งกำหนดไว้ 5 ระดับตามลักษณะความรุนแรงที่เกิดซึ่งมีรายละเอียดตามตารางที่ 3

ตารางที่ 3 ปัจจัยความเสี่ยงทางด้านการปฏิบัติงาน

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
1	ผู้กระทำ	ผู้ที่ก่อให้เกิดภัยคุกคาม โดยผู้กระทำเป็นได้ทั้งที่เป็นมนุษย์และไม่ใช่มนุษย์	ACTOR
	ค่าที่เป็นไปได้ของตัวแปร ACTOR		
1.1	ผู้กระทำจากภายใน	คนภายในองค์กร เช่น พนักงานบริษัท หรืออาจเป็นผู้ที่บริษัทจ้างมาช่วงระยะเวลาหนึ่ง	1
1.2	ผู้กระทำจากภายนอก	หมายถึงคู่แข่งทางการค้า กฎข้อบังคับ	2
2	ชนิดภัยคุกคาม	ลักษณะโดยธรรมชาติของภัยคุกคามที่อาจเกิดขึ้น โดยภัยคุกคามอาจมีหรือไม่มีผู้กระทำก็ได้	THREAT TYPE
	ค่าที่เป็นไปได้ของตัวแปร THREATTYPE		
2.1	เหตุสุดวิสัย	ลักษณะของภัยคุกคามที่เกิดขึ้นโดยฉับพลันโดยไม่คาดหมายและไม่สามารถป้องกันได้	1
2.2	ข้อบกพร่องขององค์กร	ลักษณะของภัยคุกคามที่เกิดจากความไม่เอาใจใส่ของคนในองค์กร ส่งผลกระทบให้เกิดความเสียหายต่อองค์กรในภาครวม	2
2.3	ความล้มเหลวของมนุษย์	ภัยคุกคามที่เกิดจากความผิดพลาดของมนุษย์ เช่น การกรอกข้อมูลเงินฝากไม่ถูกต้องตามความเป็นจริง	3
2.4	ภัยคุกคามทางเทคนิค	ภัยคุกคามที่เกิดจากการใช้เทคนิคทางด้านเทคโนโลยีสารสนเทศ เพื่อเข้าถึง	4
2.5	การกระทำโดยเจตนา	ภัยคุกคามที่เกิดจากเจตนาของมนุษย์ เช่น การยักยอกทรัพย์	5

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
3	ชนิดเหตุการณ์	ประเภทของเหตุการณ์ทางด้านการปฏิบัติการที่มีความเสี่ยงที่จะเกิดความเสียหายขึ้นในสถานการณ์หนึ่งๆ ซึ่งอาจประกอบด้วยหลายเหตุการณ์ และอาจเกิดจากทั้งบุคคลภายในหรือภายนอกองค์กร	EVENT TYPE
	ค่าที่เป็นไปได้ของตัวแปร EVENTTYPE		
3.1	การทุจริตภายใน	ความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายในองค์กรเพื่อให้ผลประโยชน์จากการทุจริตดังกล่าวตกแก่พวกพ้องของตนเอง	1
3.2	การทุจริตภายนอก	ความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอกองค์กรแต่ก่อให้เกิดความเสียหายโดยตรงต่อสถาบันการเงิน	2
3.3	การจ้างงานและความปลอดภัยในสถานที่ปฏิบัติงาน	ความเสี่ยงที่เกิดจากกระบวนการจ้างงานที่ไม่เหมาะสม การจ่ายค่าตอบแทน หรือการปฏิบัติต่อพนักงานอย่างไม่เป็นธรรม รวมถึงความเสี่ยงที่เกิดขึ้น เนื่องจากการกำหนดมาตรการรักษาความปลอดภัยในการปฏิบัติงาน	3
3.4	ลูกค้า ผลิตภัณฑ์ และวิธีปฏิบัติในการดำเนินธุรกิจ	ความเสี่ยงที่เกิดขึ้นจากวิธีปฏิบัติในการดำเนินธุรกิจ กระบวนการออกผลิตภัณฑ์ และการเข้าถึงข้อมูลลูกค้าที่ไม่เหมาะสม ไม่เป็นไปตามกฎหมาย ระเบียบและข้อบังคับที่ทางการกำหนด	4
3.5	ความปลอดภัยของทรัพย์สิน	ความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของสถาบันการเงินอันเนื่องมาจากอุบัติเหตุต่างๆ	5
3.6	การหยุดชะงักของระบบงานและระบบคอมพิวเตอร์	ความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติ หรือการหยุดทำงานของระบบงานด้านต่างๆ	6
3.7	การจัดการกระบวนงาน	ความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน ความผิดพลาดของระบบปฏิบัติงาน หรือ ความผิดพลาดจากการปฏิบัติงานของพนักงานภายในสถาบันการเงินและจากการจ้างงานภายนอก	7

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
4	ทรัพย์สินหรือทรัพยากร	เป็นทรัพย์สินหรือทรัพยากรที่ถูกกระทบจากการกระทำในสถานการณ์ดังกล่าว ทรัพย์สินคือวัตถุใด ๆ ที่มีค่าต่อองค์กร ทรัพยากรคือสิ่งใด ๆ ก็ตามที่ช่วยให้การทำงานสำเร็จตามเป้าหมาย ทรัพย์สินและทรัพยากรอาจเป็นสิ่งเดียวกันก็ได้	ASSET/ RESOURCE
	ค่าที่เป็นไปได้ของตัวแปร ASSET/RESOURCE		
4.1	บุคลากรและองค์กร	บุคคลที่ได้รับผลกระทบจากความเสี่ยงที่ระบุ	1
4.2	กระบวนการทำงาน	กระบวนการทำงานที่ได้รับผลกระทบจากความเสี่ยงเช่น กระบวนการฝาก ถอนเงินและโอนเงิน	2
4.3	โครงสร้างพื้นฐานหรือสิ่งอำนวยความสะดวก	โครงสร้างพื้นฐานหรือสิ่งอำนวยความสะดวกที่ได้รับผลกระทบจากความเสี่ยงที่ระบุ เช่น อาคาร ห้องเครื่องแม่ข่าย	3
4.4	โครงสร้างพื้นฐานทางด้านสารสนเทศ	โครงสร้างพื้นฐานทางด้านสารสนเทศที่ได้รับผลกระทบจากความเสี่ยงนั้น เช่นเครื่องแม่ข่าย อุปกรณ์จัดเส้นทาง อุปกรณ์รวมสายสัญญาณ	4
4.5	ข้อมูล	ทรัพย์สินที่เป็นข้อมูลที่ได้รับผลกระทบจากความเสี่ยงนั้น เช่น ข้อมูลส่วนตัวลูกค้า ข้อมูลองค์กร	5
5	ระดับความรุนแรง	ระดับของความรุนแรงของผลกระทบเมื่อเกิดสถานการณ์ความเสี่ยงนั้นขึ้น	LOSS SEVERITY
	ค่าที่เป็นไปได้ของตัวแปร LOSSSEVERITY		
5.1	ต่ำมาก	ความเสียหายน้อยมาก ไม่มีผลกระทบต่อเป้าหมายการทำงาน	1
5.2	ต่ำ	ความเสียหายส่งผลกระทบต่อการดำเนินงานภายในฝ่ายเป็นความเสี่ยงที่อยู่ในระดับยอมรับได้	2
5.3	ปานกลาง	ความเสียหายมีผลกระทบต่อการดำเนินงานภายในหน่วยงาน ต้องดำเนินการจำกัดหรือลดความรุนแรงของความเสี่ยงนั้น	3

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
5.4	สูง	ความเสียหายส่งผลกระทบต่อการดำเนิน งานภายในองค์กร ต้องใช้งบประมาณเฉพาะหรือเสียค่าใช้จ่ายเพื่อดำเนินการจำกัดหรือลดความรุนแรงของความเสี่ยง	4
5.5	สูงมาก	ความเสียหายมีผลกระทบต่อความอยู่รอดในการดำเนินธุรกิจขององค์กร จำเป็นต้องแจ้งผู้บริหารระดับสูงเพื่อระงับความเสี่ยงนั้นทันที	5
6	Organization Unit		ORGUNIT
	ค่าที่เป็นไปได้ของตัวแปร ORGUNIT		
6.1	ฝ่ายตรวจสอบ	ให้ความเชื่อมั่นและให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานขององค์กร ช่วยให้องค์กรบรรลุเป้าหมายด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบและเป็นระเบียบ	1
6.2	สำนักกรรมการผู้จัดการ	การตัดสินใจในแผนการระยะยาวที่เกี่ยวกับทิศทางโดยรวมขององค์การ กำหนดวัตถุประสงค์นโยบายและกลยุทธ์ การให้คำแนะด้านการจัดการกับสิ่งต่างๆทั้งหมด	2
6.3	ฝ่ายสื่อสารองค์กร	การสื่อสารองค์กรคือ กิจกรรมการสื่อสารโดยรวมทั้งหมด (The Total Communication Activity) ซึ่งจัดทำขึ้นโดยองค์กร เพื่อให้บรรลุวัตถุประสงค์ที่วางแผนไว้ (Planned Objectives)	3
6.4	ฝ่ายกิจการนโยบายภาครัฐและสังคม	เป็นหน่วยงานที่ดูแลเกี่ยวกับ การปฏิบัติตามกฎ ระเบียบข้อบังคับของหน่วยราชการ และการดูแลกิจการทางสังคมและสิ่งแวดล้อม	4
6.5	ฝ่ายบริหารความเสี่ยง	วิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อใช้ประกอบการปรับปรุงจัดทำหลักเกณฑ์การประเมินความเสี่ยงขององค์กร พัฒนากระบวนการบริหารความเสี่ยงและกรอบการ	5

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
		บริหารความเสี่ยงขององค์กรให้มีประสิทธิภาพสอดคล้องและเหมาะสมกับสภาพแวดล้อมปัจจุบัน	
6.6	ฝ่ายวิเคราะห์สินเชื่อรายย่อย	การประกันความเสี่ยงอันอาจเกิดขึ้นในอนาคต จากการปล่อยสินเชื่อรายย่อยให้อยู่ในระดับที่ยอมรับได้	6
6.7	ฝ่ายวิเคราะห์สินเชื่อโครงการ	การประกันความเสี่ยงอันอาจเกิดขึ้นในอนาคตจากการปล่อยสินเชื่อให้อยู่ในระดับที่ยอมรับได้	7
6.8	ฝ่ายพิธีการสินเชื่อ	จัดทำนิติกรรมสัญญาของสินเชื่อ จดทะเบียนสิทธิและนิติกรรม ตรวจสอบและควบคุมหลักประกันสัญญาไถ่ถอนหลักประกัน พัฒนา ปรับปรุง กำหนดหลักเกณฑ์และวิธีปฏิบัติด้านนิติกรรมสัญญาและพิธีการสินเชื่อ	8
6.9	กลุ่มงานกิจการสาขา	บริหารจัดการธุรกิจของธนาคารในหน่วยธุรกิจย่อยแทนธนาคาร	9
6.10	ฝ่ายบริหารสำนักงาน	ติดต่อสื่อสารบันทึกและจัดเก็บ ข้อมูล ความปลอดภัยของสินทรัพย์	10
6.11	ฝ่ายจัดหาและการพัสดุ	ควบคุมกำกับ ดูแล บริหารจัดการการจัดหาพัสดุ	11
6.12	ฝ่ายประเมินราคาหลักทรัพย์	สนับสนุนงานสินเชื่อเพื่อรองรับงานสินเชื่อของลูกค้าสำนักงานและสาขา	12
6.13	ฝ่ายพัฒนาการตลาดเงินฝาก	วางแผนการหาลูกค้าใหม่ นำเสนอแผนส่งเสริมการขายร่วมกับฝ่ายการตลาดและพัฒนาผลิตภัณฑ์	13
6.14	ฝ่ายบริหารการเงิน	พยากรณ์และวางแผนตัดสินใจลงทุนและจัดหาเงินทุน ประสานงานและควบคุม ติดต่อกับตลาดการเงินและบริหารความเสี่ยง	14
6.15	ฝ่ายการบัญชี	บันทึกบัญชีและทะเบียนคุมรายจ่าย รายงานผลการเบิก จ่ายเงิน ตรวจสอบทางระบบบัญชี ความถูกต้องของเอกสารขอเบิก จัดทำงบดุลและ	15

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
		งบแสดงฐานะทางการเงิน	
6.16	ฝ่ายกฎหมาย	ให้คำปรึกษาพิจารณาให้ความเห็น วินิจฉัย ตีความ ศึกษา ยกร่างรวมทั้งร่วมดำเนินการในการบังคับใช้กฎหมายที่เกี่ยวข้องกับอำนาจหน้าที่ของธนาคารโดยเฉพาะอย่างยิ่งกฎหมายด้านการเงินการธนาคาร	16
6.17	ฝ่ายบริหารหนี้ กทม.และปริมณฑล	บริหารจัดการเกี่ยวกับลูกหนี้ในกรุงเทพมหานครและปริมณฑล	17
6.18	ฝ่ายบังคับคดีและหนี้ส่วนขาด	บริหารจัดการการบังคับตามคำพิพากษาและคำสั่ง และการติดตามหนี้ส่วนที่นอกเหนือการบังคับจาหลักประกัน	18
6.19	ฝ่ายปฏิบัติการสารสนเทศ	บริหารจัดการเกี่ยวกับข้อมูลสาร สนเทศ เพื่อดำเนินธุรกิจของธนาคารและเพื่อการตัดสินใจของผู้บริหาร	19
6.20	ฝ่ายนโยบายและแผน	เป็นผู้กำหนดทิศทางให้เป็นไปตามวัตถุประสงค์และเป้าหมาย ตามวิสัยทัศน์และพันธะกิจขององค์กร	20
6.21	ฝ่ายวิชาการ	เป็นแหล่งข้อมูลที่สนับสนุนการดำเนินธุรกิจของธนาคารและผู้บริหาร	21
6.22	ฝ่ายการเงิน	ดูแลจัดเตรียม เช็คสั่งจ่าย การรับเงิน การจัดเก็บเงิน การนำเงินฝากธนาคาร รวมทั้งการตรวจสอบความถูกต้องเงินฝากธนาคาร	22
6.23	ฝ่ายกิจการสาขา กทม และปริมณฑล	กำกับดูแลและบริหารจัดการสาขาของธนาคารในกรุงเทพและปริมณฑล	23
6.24	ฝ่ายกิจการสาขาภูมิภาค 1	กำกับดูแลและบริหารจัดการเกี่ยวกับงานของสาขาธนาคาร	24
6.25	ฝ่ายกิจการสาขาภูมิภาค 2	กำกับดูแลและบริหารจัดการเกี่ยวกับงานของสาขาธนาคาร	25

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
6.26	ฝ่ายบริหารทรัพย์สิน	ควบคุมดูแลบริหารจัดการทรัพย์สิน รวมถึง อาคารสำนักงานของธนาคารทั้งสำนักงานใหญ่และสำนักงานสาขา	26
6.27	ธนาคารอาคารสงเคราะห์	ช่วยเหลือทางการเงินให้กับประชาชน ได้มีที่อยู่อาศัยตามสมควรแก่อัตภาพ	27
6.28	ฝ่ายตรวจสอบคอมพิวเตอร์	การตรวจสอบกิจกรรม หรือการดำเนินงานของหน่วยงานคอมพิวเตอร์ และการตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ประมวลผล	28
6.29	กลุ่มงานกลยุทธ์และปฏิบัติการ	เป็นหน่วยงานที่กำหนดทิศทางและผสานการดำเนินงานของธนาคาร ทำให้โดดเด่นแตกต่างจากคู่แข่ง และเป็นแนวทางให้ประสบความสำเร็จในการบริหารจัดการความเสี่ยงและสร้างผลตอบแทนการลงทุนที่ดี	29
6.30	กลุ่มงานบริหารหนี้	หน่วยงานที่ทำหน้าที่บริหารหนี้ที่มีปัญหา เช่น การขยายระยะเวลาในการชำระหนี้ การชำระหนี้ต่ำกว่างวดปกติ	30
31	กลุ่มงานเทคโนโลยีสารสนเทศ	กำกับดูแลงานด้านเทคโนโลยีสารสนเทศของธนาคาร	31
32	กลุ่มงานการตลาด	จัดการเกี่ยวกับสินค้าและบริการ คือ การดำเนินการเกี่ยวกับการเปลี่ยนแปลงในสินค้าและบริการ เพื่อให้เกิดความพอใจและตรงกับความต้องการของลูกค้ามากที่สุด	32
33	กลุ่มงานการเงินและบัญชี	งานการเงิน มีหน้าที่ ในการบันทึกและดูแลจัดเตรียมเช็คสั่งจ่าย การรับเงิน การจัดเก็บเงิน งานบัญชี มีหน้าที่รับผิดชอบในการตรวจสอบความถูกต้องครบถ้วนของการบันทึกรายการ การจัดทำรายงานทางการเงินและบัญชี และการจัดเก็บเอกสารทางบัญชี	33
34	สายงานตรวจสอบและกำกับ	กำกับสอบทาน และตรวจสอบการทำธุรกิจและการบริหารความเสี่ยงของธนาคารเพื่อให้มีความถูกต้องเหมาะสม มีประสิทธิภาพและประสิทธิผล ภายใต้นโยบายของธนาคารข้อกำหนดทางการที่กำกับดูแล รวมถึงจรรยาบรรณในการประกอบวิชาชีพ	34

ลำดับ	ชื่อตัวแปร	คำอธิบายตัวแปร	การแทนค่า
35	สายงาน กรรมการ ผู้จัดการ	ควบคุมการบริหารงานให้เป็นไปตามนโยบายที่ คณะกรรมการธนาคาร หรือคณะกรรมการบริหารกำหนดไว้และรายงานผลการดำเนินงานต่อคณะ กรรมการธนาคาร หรือคณะกรรมการบริหาร ตามลำดับ	35
36	กลุ่มงาน สินเชื่อ	วิเคราะห์และอำนวยสินเชื่ออย่างมีคุณภาพ โดยคำนึงถึงการบริหารความเสี่ยง มาตรฐาน และระเบียบที่ธนาคารกำหนด	36

3.2.3 เครื่องมือที่ใช้ในการวิจัย

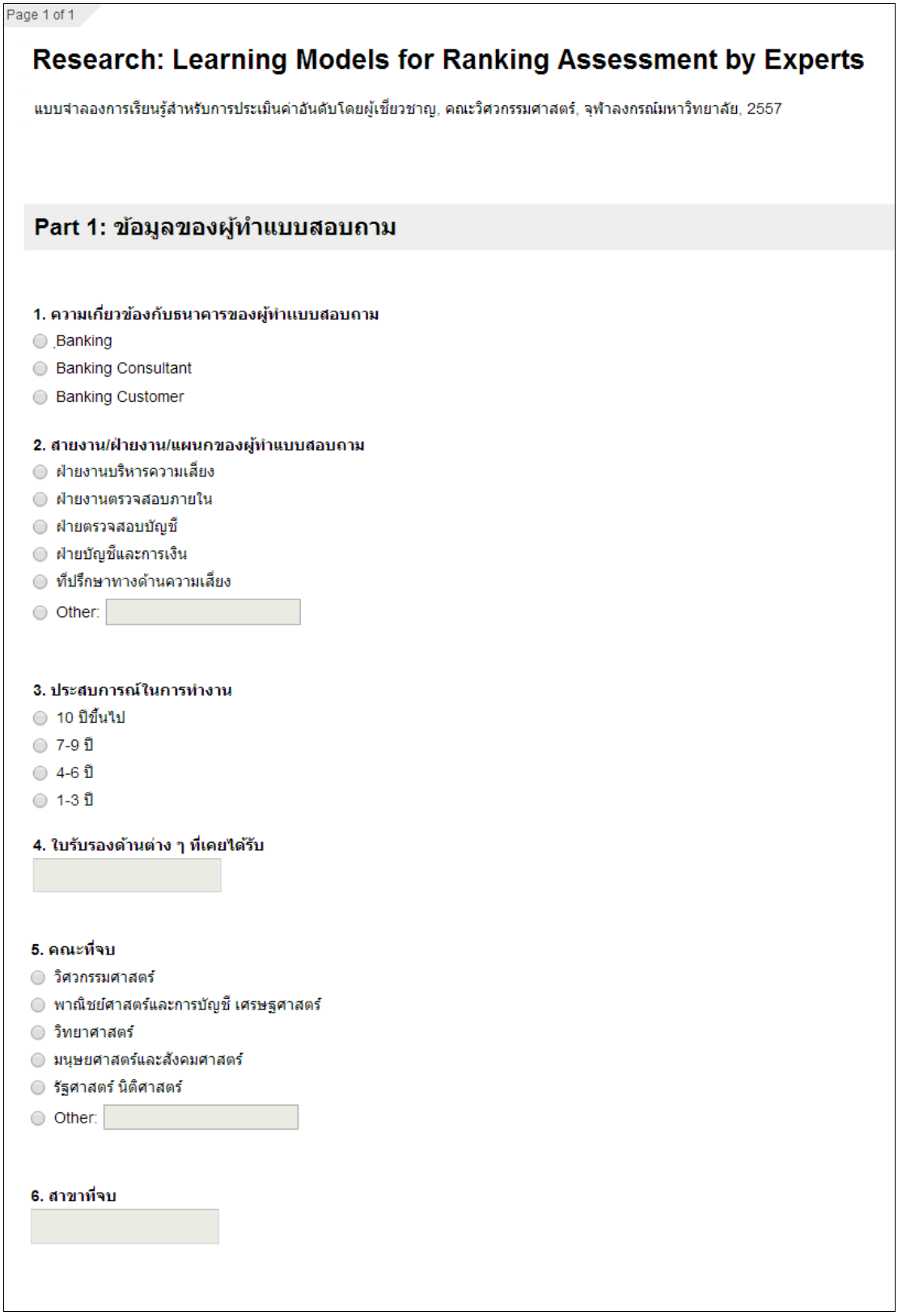
1. แบบสอบถามการประเมินความเสี่ยงทางด้านการปฏิบัติงาน

แบบสอบถามที่ใช้ในเก็บข้อมูลการประเมินความเสี่ยงจากผู้เชี่ยวชาญแบ่งออกเป็น 2 ส่วนซึ่งมีลักษณะดังนี้

ตอนที่ 1 แบบสอบถามเกี่ยวกับภูมิหลังและประสบการณ์การทำงาน เป็นแบบสอบถามความคิดเห็นทั่วไปของผู้เชี่ยวชาญที่เข้ามาทำการประเมินโดยข้อมูลที่ทำการเก็บประกอบด้วย อายุ ระดับการศึกษา ประสบการณ์ในการเป็นที่ปรึกษาหรือให้บริการในด้านความเสี่ยงและความมั่นคงปลอดภัยข้อมูลใบรับรองในการทำงาน โดยลักษณะแบบสอบถามเป็นแบบตรวจสอบ (Check list) และแบบเติมคำ โดยแบบฟอร์มตัวอย่างที่ใช้ในการเก็บข้อมูลแสดงดัง ภาพที่ 10

ตอนที่ 2 แบบสอบถามการวิเคราะห์สถานการณ์ความเสี่ยง ที่ประกอบด้วยข้อมูลตัวแปรที่กำหนดไว้ในงานวิจัย ประกอบกับคำบรรยายสถานการณ์ที่เกิดขึ้นในแต่ละหน่วยงานประกอบด้วยคำถามสถานการณ์ความเสี่ยงในแต่ละส่วนขององค์กรจำนวน 1308 ข้อ ซึ่งแต่ละสถานการณ์จะมีข้อมูลให้วิเคราะห์อยู่ 4 ส่วนที่เป็นตัวแปรสาเหตุและ 1 ส่วนที่เป็นตัวแปรผลลัพธ์ดัง ภาพที่ 11

Chulalongkorn University



Page 1 of 1

Research: Learning Models for Ranking Assessment by Experts

แบบจำลองการเรียนรู้สำหรับการประเมินค่าอันดับโดยผู้เชี่ยวชาญ, คณะวิศวกรรมศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2557

Part 1: ข้อมูลของผู้ทำแบบสอบถาม

1. ความเกี่ยวข้องกับธนาคารของผู้ทำแบบสอบถาม

- Banking
- Banking Consultant
- Banking Customer

2. สายงาน/ฝ่ายงาน/แผนกของผู้ทำแบบสอบถาม

- ฝ่ายงานบริหารความเสี่ยง
- ฝ่ายงานตรวจสอบภายใน
- ฝ่ายตรวจสอบบัญชี
- ฝ่ายบัญชีและการเงิน
- ที่ปรึกษาทางด้านความเสี่ยง
- Other:

3. ประสบการณ์ในการทำงาน

- 10 ปีขึ้นไป
- 7-9 ปี
- 4-6 ปี
- 1-3 ปี

4. ใบรับรองด้านต่าง ๆ ที่เคยได้รับ

5. คณะที่จบ

- วิศวกรรมศาสตร์
- พาณิชย์ศาสตร์และการบัญชี เศรษฐศาสตร์
- วิทยาศาสตร์
- มนุษยศาสตร์และสังคมศาสตร์
- รัฐศาสตร์ นิติศาสตร์
- Other:

6. สาขาที่จบ

ภาพที่ 10 แบบฟอร์มการเก็บข้อมูลภูมิหลังผู้ทำแบบสอบถาม

Part2: การจัดลำดับความเสี่ยงทางด้านการปฏิบัติงาน

No.	Risk Scenario	CAUSE					LOSS Severity
		Org Unit	Actor	Threat Type	Event Type	Asset/Resource	
1	risk scenario description	[1..36]	[1..2]	[1..5]	[1..7]	[1..5]	[1..5]
2	…						
3	…						
…	…						
…	…						
…	…						
…	…						
…	…						
1308	…						

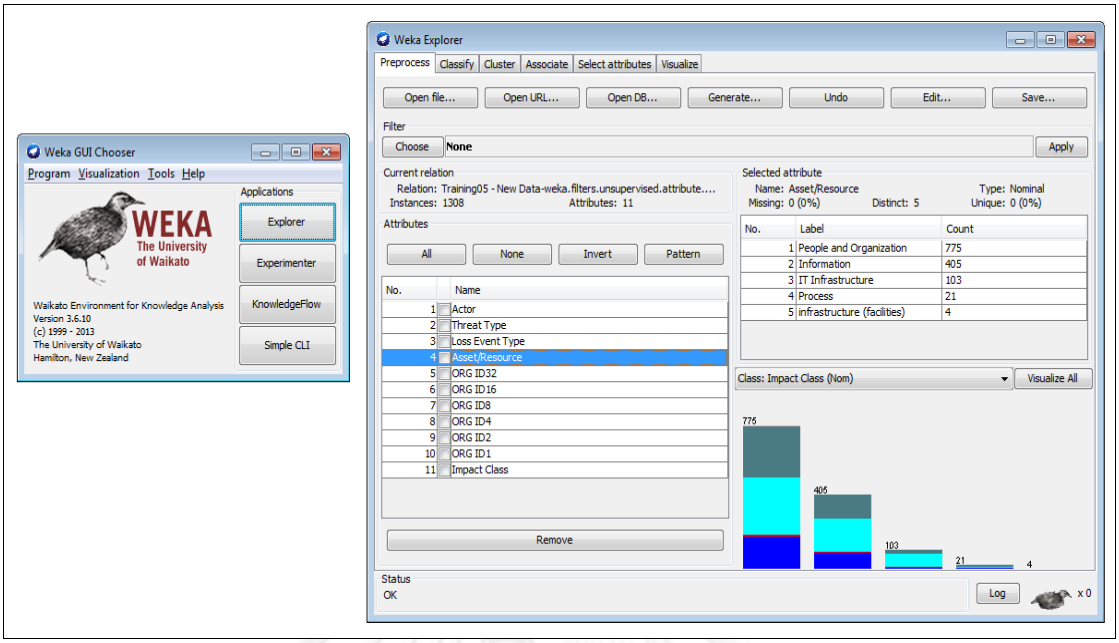
ภาพที่ 11 แบบฟอร์มการเก็บข้อมูลการวิเคราะห์สถานการณ์ความเสี่ยง

2. โปรแกรมในการสร้างโมเดล WEKA [13]

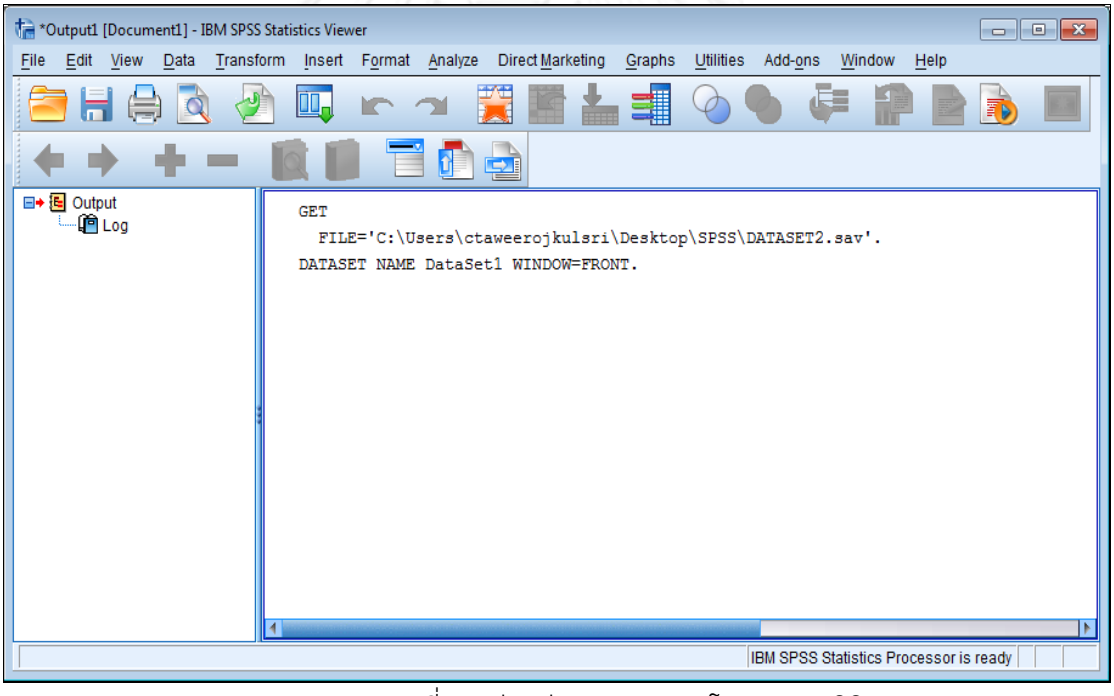
WEKA ย่อมาจาก Waikato Environment for Knowledge Analysis เป็นเครื่องมือที่เก็บรวบรวมอัลกอริทึมสำหรับการเรียนรู้ของเครื่อง (Machine Learning) ซึ่งใช้ในงานที่เกี่ยวข้องกันการทำเหมืองข้อมูล (Data Mining) เครื่องมือนี้ถูกพัฒนาโดยมหาวิทยาลัย Waikato จากประเทศนิวซีแลนด์ WEKA เป็นเครื่องมือที่พัฒนามาจากภาษาจาวา (Java) เป็นซอฟต์แวร์ที่สามารถใช้งานได้ฟรีสำหรับการศึกษาและมีการใช้งานอย่างแพร่หลายในฐานะที่เป็นเครื่องมือที่ใช้ในการสร้างโมเดลสำหรับงานวิจัยทางด้านการเรียนรู้ของเครื่อง โดยตัวอย่างหน้าตาของโปรแกรม WEKA ดัง ภาพที่ 12 งานวิจัยนี้จะใช้ WEKA ในการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กในการจำแนกค่าความรุนแรงของความเสียหายที่เกิดขึ้นบนพื้นฐานของรูปแบบที่เกิดขึ้นของความเสี่ยงทางด้านการปฏิบัติงาน

3. โปรแกรมทางสถิติ SPSS [14]

SPSS เป็นอุปกรณ์หนึ่งที่ใช้ในงานที่เกี่ยวข้องกับสถิติซึ่งผลิตโดยบริษัท IBM ในปี 2009 โปรแกรม SPSS ใช้ในงานที่เกี่ยวของกับการทำเหมืองข้อมูลรวมถึงใช้ในการเก็บรวบรวมข้อมูลและการสร้างไฟล์ฐานข้อมูลที่ใช้ในการวิจัยด้วย SPSS มีการใช้งานอย่างกว้างขวางในการวิเคราะห์ทางสถิติในด้านของสังคมศาสตร์ และอุตสาหกรรมที่เกี่ยวข้องกับวิทยาศาสตร์สุขภาพ การตลาด หรือการวิเคราะห์การสำรวจขององค์กร รัฐบาล โดยเฉพาะอย่างยิ่งในวงการการศึกษา ซึ่งตัวโปรแกรม SPSS จะมีเวอร์ชันสำหรับนักศึกษาให้สามารถใช้ได้ฟรี ตัวอย่างหน้าตาส่วนต่อประสานของโปรแกรม SPSS แสดงดัง ภาพที่ 13 ในงานวิจัยนี้จะใช้โปรแกรม SPSS ในการเตรียมข้อมูลและตรวจสอบสถิติเบื้องต้นของข้อมูลที่เก็บจากผู้เชี่ยวชาญได้แก่ การตรวจสอบการแจกแจงปกติของตัวแปร โดยพิจารณาจากความเบ้ (Skewness) ของข้อมูล และค่าความโด่ง (Kurtosis) ของข้อมูล



ภาพที่ 12 ส่วนต่อประสานของโปรแกรม WEKA

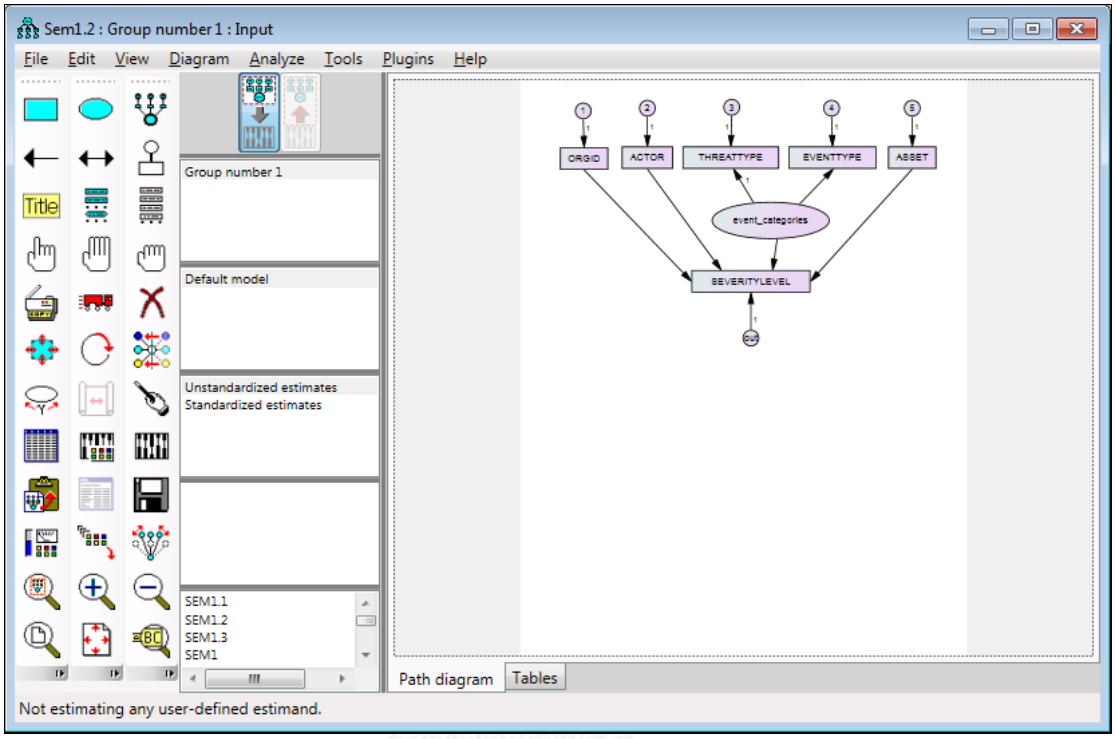


ภาพที่ 13 ส่วนต่อประสานของโปรแกรมสถิติ SPSS

4. โปรแกรมสำหรับสร้างโมเดล AMOS [15]

AMOS เป็นโปรแกรมที่ใช้ในการสร้างโมเดลสมการโครงสร้าง และช่วยในการวิเคราะห์งานวิจัยและการทดสอบทฤษฎี โดยช่วยในการวิเคราะห์ปัจจัยต่างๆ การวิเคราะห์สมการถดถอย และการหาความสัมพันธ์ระหว่างตัวแปรในการทดสอบสมติฐานต่างๆ โดยโปรแกรมนี้จะช่วยในการระบุ ประเมินและสร้างโมเดลโดยเริ่มต้นจากการสร้างแผนภาพเส้นทาง (Path diagram) ซึ่งแสดงความระหว่างตัวแปรที่ถูกตั้งสมติฐานไว้ โปรแกรม AMOS สามารถประมวลผลได้ทั้งข้อมูลที่เป็นตัวเลข

(Numeric) และไม่เป็นตัวเลขเช่น ข้อมูลที่เป็นลำดับ ข้อมูลที่เป็นชนิดหรือคุณลักษณะ (Categorical) โดยตัวอย่างหน้าตาโปรแกรมแสดงดัง ภาพที่ 14 โดยงานวิจัยนี้จะใช้โปรแกรม AMOS ในการสร้างโมเดลการวิเคราะห์เส้นทางเพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรจากข้อมูลที่ได้จากการทำแบบสอบถาม



ภาพที่ 14 ส่วนต่อประสานของโปรแกรม SPSS AMOS

3.3 การเก็บข้อมูล (Data collection)

การเก็บข้อมูลจะเก็บข้อมูลจากกลุ่มผู้เชี่ยวชาญที่ทำหน้าที่เป็นที่ปรึกษาของสถาบันทางการเงิน ธนาคาร ซึ่งเป็นผู้มีความเข้าใจในกระบวนการทำงานและความเสี่ยงที่อาจเกิดขึ้นในด้านการปฏิบัติงานโดยการรวบรวมข้อมูลจะทำการแบ่งข้อมูลคำถามออกเป็นส่วน ๆ เนื่องจาคำถามมีจำนวนมากและแบ่งให้กับผู้เชี่ยวชาญที่มาทำแบบประเมินเท่าๆ กัน โดยผู้เชี่ยวชาญที่เลือกจะทำหน้าที่ที่เกี่ยวข้องกับจัดการความมั่นคงปลอดภัยทางด้านสารสนเทศ เป็นปรึกษาหรือทำหน้าที่ในการตรวจสอบภายใน ซึ่งอาจให้บริการในการวัด จัดการและควบคุมความเสี่ยง และเพิ่มความน่าเชื่อถือของระบบและกระบวนการในระดับองค์กรของกลุ่มลูกค้าทางด้านการธนาคารและสถาบันทางด้านการเงิน โดยการประเมินจะส่งข้อมูลเป็นไฟล์ .xlsx ที่เป็นแบบสอบถามให้กับผู้ประเมินและคอยติดตามผลเป็นระยะ ๆ

แบบฟอร์มที่ใช้ในการเก็บข้อมูลแสดงใน ภาพที่ 11 การเก็บข้อมูลประกอบด้วย 1,308 ตัวอย่าง ซึ่งค่าที่เป็นไปได้ของปัจจัยความเสี่ยงในแต่คอลัมน์ได้อธิบายไว้แล้วในหัวข้อรายละเอียดตัวแปรและการกำหนดค่าเกณฑ์ที่ใช้ในการวิจัย (3.3.2) ยกตัวอย่างเช่นค่าที่เป็นไปได้ของ Actor เป็น 1 และ 2 ซึ่งค่าทั้งสองจะพิจารณาเป็นสัญลักษณ์ไม่ใช่การจัดอันดับตามค่าจำนวน

เนื่องจากค่าเวกเตอร์ที่เป็นข้อมูลนำเข้านั้นอาจมีบางส่วนที่มีค่า Actor, Threat Type, Event Type และ Asset/Resource เดียวกันแต่สามารถมีค่า Loss Severity ที่แตกต่างกันได้ในแต่ละหน่วยงานขององค์กร ดังนั้นจึงได้มีการเพิ่มส่วนของปัจจัย Organization Unit เพิ่มเข้าไปในเวกเตอร์นั้นด้วย

ค่าของ Loss severity ใน ภาพที่ 11 จะถูกประเมินบนพื้นฐานของความสัมพันธ์ของค่าปัจจัยความเสี่ยงทั้ง 5 ปัจจัยที่กล่าวถึงก่อนหน้านี้ โดยค่าของ Loss Severity จะถูกประเมินเป็นค่าของอันดับ 1-5 ซึ่งแสดงถึงอันดับความรุนแรงของของเหตุการณ์ที่มีรูปแบบของปัจจัยหนึ่ง ซึ่งมีความหมายเป็น น้อยมาก (Very Low), น้อย (Low), ปลานกลาง (Medium), สูง (High) และสูงมาก (Very High) ตามลำดับ

3.4 การวิเคราะห์ข้อมูล

3.4.1 สถิติเบื้องต้น

การวิเคราะห์ข้อมูลได้จากการทำแบบสำรวจโดยผู้เชี่ยวชาญ เพื่อให้ทราบถึงลักษณะของกลุ่มข้อมูลและสภาพของตัวแปร จึงใช้โปรแกรมสถิติ SPSS เข้ามาช่วยในการวิเคราะห์ซึ่งค่าทางสถิติที่ใช้ได้แก่ ค่าความถี่ ค่าสถิติร้อยละ ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐาน ค่าความเบ้และความโด่ง สำหรับการวิเคราะห์การแจกแจงของข้อมูล ค่าประสิทธิ์สหสัมพันธ์ของเพียร์สัน (Pearson's Product Moment Correlation Coefficient)

3.4.2 สถิติที่ใช้ทดสอบสมมติฐานและโมเดล [9, 16-22]

สำหรับงานวิจัยนี้จะต้องสร้างโมเดล 2 โมเดลคือโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กซึ่งเป็นโมเดลที่สร้างจากโปรแกรม WEKA และโมเดลการวิเคราะห์เส้นทางที่ได้จากโปรแกรม AMOS ทั้งสองจะต้องมีการวัดผลจากค่าตัววัดต่างๆ เพื่อบ่งบอกถึงความเหมาะสมและความน่าเชื่อถือของโมเดล โมเดลแต่ละโมเดลจะมีตัววัดที่เหมือนและแตกต่างกันซึ่งในการวิจัยนี้ได้ทำการเลือกค่าสถิติที่ใช้ ดังตารางที่ 4

การประเมินความน่าเชื่อถือของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง อาจมีการใช้ตัววัดในการตรวจสอบที่แตกต่างกัน โดยที่โมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กมีการตรวจสอบหลัก ๆ ในเรื่องของความแม่นยำของการทำนาย ค่าความคลาดเคลื่อนต่าง ๆ ที่เกิดขึ้นในการทำนายโดยใช้โปรแกรม WEKA ส่วนโมเดลสมการโครงสร้างต้องมีการตรวจสอบความสอดคล้องของรูปแบบความสัมพันธ์โครงสร้างสาเหตุตามทฤษฎีกับข้อมูลเชิงประจักษ์จากกลุ่มตัวอย่างที่ได้จากกลุ่มผู้เชี่ยวชาญ โดยใช้โปรแกรม AMOS โดยใช้การประมาณค่าพารามิเตอร์จากค่าความน่าจะเป็นสูงสุด (Maximum Likelihood Estimate) ตามโมเดลที่ใช้เป็นกรอบแนวคิดในการวิจัย โดยตัววัดที่สำคัญในการวิจัยมีดังนี้

ตารางที่ 4 ค่าสถิติที่เลือกใช้ในทดสอบสมมติฐานและการสร้างโมเดลการวิจัย

ลำดับ	ตัววัด	โมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก	โมเดลสมการโครงสร้าง
1	Chi-Square	-	✓
2	GFI	-	✓
3	AGFI	-	✓
4	RMR	-	✓
5	RMSEA	-	✓
6	RMSE	✓	✓
7	SRC	-	✓
8	C.R.	-	✓
9	HOELTER	-	✓
10	MI	-	✓
11	Accuracy	✓	✓
12	Kappa coefficient	✓	-

1. ค่าสถิติไค-สแควร์ (Chi-Square Statistics)

ในโปรแกรม เรียกว่าค่าตัวแปร CMIN ใช้ตรวจสอบความกลมกลืนของโมเดลในภาพรวม คำนวณจากผลคูณระหว่างองศาอิสระ (Degree of freedom: DF) กับฟังก์ชันความกลมกลืนดังสมการ 1 โดยที่ n เป็นขนาดตัวอย่าง, S คือ ค่าความแปรปรวนของข้อมูลเชิงประจักษ์ และ ∑ คือค่าแปรปรวนของโมเดลที่คาดไว้

$$\chi^2 = (n-1)(S-\sum) - m \quad (7)$$

ถ้าค่าไคสแควร์มีค่าเป็นศูนย์หรือใกล้ศูนย์ หรือค่า p-value > 0.05 จะบ่งบอกว่าโมเดลที่ผู้วิจัยสร้างไว้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยค่าไคแสควร์มีค่าตั้งแต่ 0 ขึ้นไป

การจะใช้ค่าไคสแควร์ข้อมูลควรมีขนาดใหญ่และตัวแปรจะต้องมีการแจกแจงแบบปกติเชิงพหุ ดังนั้นการใช้ค่านี้ในการทดสอบถ้าขนาดตัวอย่างใหญ่จะมีโอกาสที่ค่านี้จะมีค่ามากและบ่งบอกว่าโมเดลไม่สอดคล้องกันสูงทั้งที่ความจริงกลมกลืนก็มี ดังนั้นจึงต้องมีการวิเคราะห์ค่าตัววัดอื่น ๆ ด้วยประกอบกัน

ค่าองศาอิสระของการทดสอบโมเดลจะคำนวณจากสมการ

$$DF = \frac{1}{2}\big(P(P+1)\big) - m \quad (8)$$

โดย p คือจำนวนตัวแปรที่สังเกตได้ในโมเดลและ m คือจำนวนพารามิเตอร์ในโมเดลที่ต้องประมาณค่า

เพื่อลดอิทธิพลจากขนาดของตัวอย่างที่นำมาทดสอบอาจพิจารณาค่าไคสแควร์สัมพันธ์ (Relative Chi-square) แทนซึ่งคำนวณจาก CMIN/DF แทน โดยถ้าค่านี้มีค่าน้อยกว่า 2 (Carmines-McIver, 1981) หรือค่านี้น้อยกว่า 3 (Kline, 1988a) จะยอมรับว่าโมเดลมีความกลมกลืนกับข้อมูลเชิงประจักษ์

2. ตัววัดวัดระดับความสอดคล้อง (Goodness of Fit Index : GFI)

เป็นอัตราส่วนของผลต่างระหว่าง ค่าไคสแควร์ของโมเดลผู้วิจัย และ ค่าไคสแควร์ของโมเดลอิสระที่ตัวแปรทุกตัวเป็นอิสระต่อกัน โดยทั่วไปถ้าค่า GFI มีค่ามากกว่า 0.95 หรือ 0.90 จะถือว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์

3. ตัววัดวัดความสอดคล้องที่ปรับแล้ว (Adjusted Goodness of Fit Index : AGFI)

เป็นค่าสถิติที่ได้จากการนำ GFI มาปรับด้วยค่าองศาอิสระและจำนวนพารามิเตอร์ของโมเดลผู้วิจัย เช่นเดียวกับ GFI ถ้า AGFI มีค่ามากกว่า 0.90 (Schumacker-Lomax,2004) จะถือว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์

4. ตัววัด RMR (Root Mean Square Residual)

เป็นค่าเฉลี่ยของค่าความคลาดเคลื่อนที่ได้จากการเปรียบเทียบเมทริกซ์ค่าความแปรปรวน – ค่าความแปรปรวนร่วมของโมเดลผู้วิจัย (∑) กับเมทริกซ์ความแปรปรวน – ค่าความแปรปรวนรวมของข้อมูลเชิงประจักษ์ที่ได้จากกลุ่มตัวอย่าง (S) โดยทั่วไปถ้าค่า RMR มีค่าเข้าใกล้ 0 จะบ่งบอกว่าโมเดลมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

5. ตัววัด RMSEA (Root Mean Squared Error of Approximation)

เป็นค่าเฉลี่ยของความไม่กลมกลืนของโมเดลต่อค่าองศาอิสระ บอกถึงความไม่สอดคล้องกันของโมเดลกับข้อมูลเชิงประจักษ์ แสดงดังสมการ (9) โดย χ^2 คือค่าไคแสควร์ DF เป็นค่าองศาอิสระ และ n เป็นจำนวนของตัวอย่าง ซึ่งการทดสอบโมเดลจากค่า RMSEA จะแสดงดังตารางที่ 5

$$RMSEA = \sqrt{\frac{\chi^2}{(n-1)(DF)} - \frac{DF}{(n-1)(DF)}} \quad (9)$$

ตารางที่ 5 ระดับเกณฑ์การประเมินตัววัด RMSEA

ลำดับ	ค่า RMSEA	การสรุปผล
1	RMSEA <= 0.05	โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ดี
2	0.05 < RMSEA <= 0.08	โมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์
3	RMSEA > 0.08	โมเดลไม่มีความสอดคล้องกับข้อมูลเชิงประจักษ์

6. ตัววัด RMSE (Root Mean Squared Error)

เป็นตัววัดที่ใช้ในการวัดความแตกต่างระหว่างค่าที่โมเดลทำนายได้กับค่าที่ได้จากการสังเกตจริงจากสภาพแวดล้อมนั้น ๆ แสดงดังสมการ (10) โดยที่ X_{obs} เป็นค่าของตัวแปรที่ได้จากการสังเกต, X_{model} คือค่าของตัวแปรที่ได้จากการประมาณโดยโมเดลที่สร้างขึ้น และ N คือจำนวนของชุดข้อมูลตัวอย่างทั้งหมด

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(X_{obs,i}-X_{model,i})^2}{N}} \quad (10)$$

7. ตัววัด SRC (Standarded Residual Covariances)

เป็นค่าระหว่างเมตริกสหสัมพันธ์การวิเคราะห์กับเมตริกที่ประมาณได้ ถ้าค่า SRC มีค่าเข้าใกล้ 0 จะถือว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยค่า SRC ที่เหมาะสมจะต้องมีค่าอยู่ระหว่าง -2 ถึง +2 (Bollen, 1989)

8. ตัววัด C.R.

เป็นค่าสัดส่วนระหว่างค่าสัมประสิทธิ์ของความสัมพันธ์ที่ได้จากการประมาณและค่าสัมประสิทธิ์ที่อยู่ในรูปมาตรฐานระหว่างตัวแปรสองตัวโดยจะพิจารณาร่วมกับค่า P-value ของความสัมพันธ์นั้น ถ้าค่าทั้งสองอยู่ในช่วงค่าระดับการยอมรับ แสดงว่าตัวแปรทั้งสองมีอิทธิพลต่อกัน

9. ตัววัด HOELTER

เป็นค่าที่ใช้บอกถึงขนาดของข้อมูลต่ำสุดที่จะยอมรับว่าโมเดลที่สร้างมีความกลมกลืนกับข้อมูลเชิงประจักษ์ โดยทั่วไปค่านี้ควรมีค่ามากกว่า 200 ที่ความละเอียด 0.05

10. ตัววัด MI (Modification Index)

เป็นค่าที่แสดงให้เห็นว่าค่าไคสแควร์จะมีค่าดีขึ้นร้อยละเท่าไร เมื่อมีการลากเส้นระหว่างตัวแปร สามารถใช้ค่า MI เพื่อช่วยปรับโมเดลให้มีความเหมาะสม ซึ่งการปรับโมเดลควรปรับคู่ตัวแปรที่มีค่านี้สูงที่สุดก่อน

11. ความแม่นยำ (Accuracy)

เป็นค่าที่วัดความแม่นในการทำนายหรือแยกแยะข้อมูลแต่ละวัตถุไปยังกลุ่มที่ถูกต้อง ซึ่งบ่งบอกถึงระดับการเรียนรู้ที่ประสบความสำเร็จของโมเดลที่สร้างขึ้นมันแทนด้วยค่าเปอร์เซ็นต์ของสัดส่วนจำนวนของวัตถุที่ถูกจัดกลุ่มอย่างถูกต้องกับจำนวนวัตถุทั้งหมด

12. ตัววัด Kappa coefficient

มีอีกชื่อหนึ่งที่เป็นทางการคือ Cohen's kappa coefficient เป็นค่าสถิติที่ใช้ทดสอบความสอดคล้อง (Consistency) ของข้อมูล N ชุด ใช้เปรียบเทียบการประเมินค่าของข้อมูลชุดเดียวกันจากผู้ประเมินหลายแหล่ง ข้อมูลที่นำมาตรวจสอบไม่จำเป็นต้องมีการแจกแจงแบบปกติ โดยทั่วไปตัววัด Kappa coefficient มักใช้ประกอบการประเมินความแม่นยำของการจำแนกข้อมูล เป็นตัววัดความสอดคล้อง (Agreement) ระหว่างข้อมูลอ้างอิงและผลการจำแนกข้อมูลที่ได้จากการทดลองด้วยวิธีการจำแนกแบบต่างๆ โดยมีรายละเอียดดังตารางที่ 6

ตารางที่ 6 ระดับเกณฑ์การประเมินตัววัด Kappa coefficient

ลำดับ	ค่า Kappa coefficient	การสรุปผล
1	< 0.01	โมเดลที่ได้มีโอกาสมีความสอดคล้องของกลุ่มข้อมูลต่ำ
2	0.01 – 0.20	โมเดลที่ได้มีความสอดคล้องของกลุ่มข้อมูลเล็กน้อย
3	0.21 – 0.40	โมเดลที่ได้มีความสอดคล้องของกลุ่มข้อมูลน้อย
4	0.41 -0.60	โมเดลที่ได้มีความสอดคล้องของกลุ่มข้อมูลปลานกลาง
5	0.61 - 0.81	โมเดลที่ได้มีความสอดคล้องของกลุ่มข้อมูลมาก
6	0.81 – 0.99	โมเดลที่ได้มีความสอดคล้องกับค่าความแม่นยำเกือบสมบูรณ์

จากข้อมูลตัววัดที่กล่าวไปข้างต้นสามารถสรุปเป็นเกณฑ์ในการตรวจสอบความสอดคล้องระหว่างแบบจำลองที่ผู้วิจัยพัฒนาขึ้นกับข้อมูลเชิงประจักษ์ได้ดัง ตารางที่ 7

ตารางที่ 7 สรุปเกณฑ์ที่ใช้ในการตรวจสอบความสอดคล้องของโมเดล

ลำดับ	ตัววัด	ระดับการยอมรับ
1	Chi-Square	ค่าไคสแควร์มีค่าเข้าใกล้ศูนย์ หรือค่า CMIN/DF น้อยกว่า 2 และค่า p-value มากกว่า 0.05
2	GFI	มีค่ามากกว่า 0.90
3	AGFI	มีค่ามากกว่า 0.90
4	RMR	มีค่าเข้าใกล้ 0
5	RMSEA	มีค่าน้อยกว่า 0.08
6	SRC	มีค่าอยู่ระหว่าง +2 และ-2
7	C.R.	มีค่ามากกว่า 1.96 และ P-value น้อยกว่า 0.05
8	HOELTER	มีค่ามากกว่า 200
9	Kappa coefficient	มีค่ามากกว่า 0.81

3.5 การสร้างโมเดลสำหรับงานวิจัย

3.5.1 การสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

การสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะใช้โปรแกรม WEKA มีขั้นตอนดังต่อไปนี้

1. ศึกษาการทำงานของโปรแกรม WEKA รวมถึงทำการติดตั้งโปรแกรม WEKA ในเครื่องคอมพิวเตอร์

2. ข้อมูลที่เก็บมาจะถูกแปลงและบันทึกเป็นไฟล์ .CSV เพื่อให้โปรแกรม WEKA สามารถนำไปประมวลผลได้
3. ทำการกำหนดปัจจัยของข้อมูลนำเข้าเป็น Actor, Threat Type, Event Type, Asset/Resource และ Org. Unit ซึ่งเป็นข้อมูลชนิดนามบัญญัติ (Nominal scale) เพื่อใช้เป็นข้อมูลตั้งต้นในการเรียนรู้ของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก
4. เลือกปัจจัยของข้อมูลผลลัพธ์เป็น Loss Severity โดยข้อมูลที่ใส่เข้าไปในโปรแกรมเป็นชนิดนามบัญญัติ เพื่อใช้เป็นข้อมูลผลลัพธ์สำหรับโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก
5. การตั้งค่าพารามิเตอร์ต่างๆ ในการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะมี 4 ตัวค่าได้แก่ Learning Rate, Momentum, Num of Epochs และ K-Fold
6. ทดลองกำหนดค่าพารามิเตอร์ดังก่อนหน้าและปรับโครงสร้างข้อมูลนำเข้าในรูปแบบที่แตกต่างกันเพื่อสร้างโมเดลที่มีความเหมาะสมขึ้นมาซึ่ง โมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กเป็นโครงสร้างที่มนุษย์ไม่อาจเข้าใจถึงการทำงานของมันได้ คือเป็นดังกล่องดำที่ให้ข้อมูลผลลัพธ์ออกมาเมื่อใส่ข้อมูลนำเข้าเวกเตอร์เข้าไป

3.5.2 การสร้างโมเดลสมการโครงสร้าง

การจะสร้างโมเดลสมการโครงสร้างจะใช้โปรแกรมสถิติ SPSS และโปรแกรมการสร้างโมเดล AMOS ซึ่งมีขั้นตอนดังต่อไปนี้

1. ศึกษาการทำงานของโปรแกรมสถิติ SPSS และโปรแกรมการสร้างโมเดล AMOS พร้อมทั้งทำการติดตั้งโปรแกรมทั้งสองในเครื่องคอมพิวเตอร์
2. ทำการแปลงข้อมูลที่เก็บมาให้อยู่ในรูปแบบของไฟล์ .SAV และทำการศึกษาลักษณะของข้อมูลโดยใช้โปรแกรมสถิติ SPSS
3. จากนั้นนำไฟล์ .SAV ที่ได้เป็นข้อมูลนำเข้าสำหรับโปรแกรมการสร้างโมเดล AMOS โดยข้อมูลของแต่ละตัวแปรจะเป็นเลขฐานสิบ
4. ทำการทดลองสร้างโมเดลโดยการลากเส้นเชื่อมตามที่ทฤษฎีกำหนดเพื่อให้ได้แผนภาพเส้นทางสำหรับโมเดลการวิเคราะห์เส้นทาง พร้อมทั้งปรับค่าโมเดลเพื่อให้ได้โมเดลที่มีความเหมาะสมโดย
5. เนื่องจากโมเดลตั้งต้นส่วนใหญ่จะยังไม่เหมาะสมกับการนำไปใช้งาน การพิจารณาเทียบกับค่าของตัววัด MI และตัววัดอื่น ๆ ที่ได้กำหนดไว้ก่อนหน้านี้ โดยการปรับโมเดลจะต้องมีการปรับบนพื้นฐานของทฤษฎี และงานวิจัยเป็นหลัก โดยมีการดำเนินการจะต้องมีการตรวจสอบผลการประมาณค่าพารามิเตอร์ว่ามีความสมเหตุสมผลและมีค่าเกินความเป็นจริงหรือไม่ พิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ให้มีความเหมาะสม พิจารณาค่าความสอดคล้องโดยรวมของโมเดลที่สร้างว่าโดยภาพรวมแล้วโมเดลมีความสอดคล้องกับข้อมูล

เชิงประจักษ์ระดับไหน ซึ่งการปรับจะสิ้นสุดลงเมื่อโมเดลนั้นมีความเหมาะสมที่ยอมรับได้หรือไม่สามารถปรับโมเดลได้แล้ว

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

บทที่ 4
ผลการวิจัยและอภิปรายผล

4.1 ผลการเก็บข้อมูล

ข้อมูลที่ใช้ในการวิจัยได้จากการประเมินของผู้เชี่ยวชาญจำนวน 3 คนซึ่งทำหน้าที่เป็นผู้ช่วยผู้จัดการความมั่นคงปลอดภัยทางด้านสารสนเทศ (IT Security Assistant Manager) , ที่ปรึกษาอาวุโสทางด้านความมั่นคงปลอดภัย (Security Senior Consultant) และที่ปรึกษาทางด้านการตรวจสอบภายใน (Internal Audit Consultant) และให้บริการในการวัด จัดการและควบคุมความเสี่ยง และเพิ่มความน่าเชื่อถือของระบบและกระบวนการในระดับองค์กรของกลุ่มลูกค้าทางด้านการธนาคารและสถาบันทางด้านการเงิน

แบบฟอร์มที่แสดงใน ภาพที่ 11 ใช้ในการเก็บข้อมูลจากผู้เชี่ยวชาญ ซึ่งผลที่ได้จากการเก็บข้อมูลประกอบด้วย 1,308 ตัวอย่าง ซึ่งค่าที่เป็นไปได้ของปัจจัยความเสี่ยงในแต่คอลัมน์ได้อธิบายไว้แล้วในหัวข้อความเสี่ยงทางด้านการปฏิบัติงาน (2.1.3) ยกตัวอย่างเช่นค่าที่เป็นไปได้ของ Actor เป็น 1 และ 2 ซึ่งค่าทั้งสองจะพิจารณาเป็นสัญลักษณ์ไม่ใช่การจัดอันดับตามค่าจำนวน

เนื่องจากค่าเวกเตอร์ที่เป็นข้อมูลนำเข้านั้นอาจมีบางส่วนที่มีค่า Actor, Threat Type, Event Type และ Asset/Resource เดียวกันแต่สามารถมีค่า Loss Severity ที่แตกต่างกันได้ในแต่ละหน่วยงานขององค์กร ดังนั้นจึงได้มีการเพิ่มส่วนของปัจจัย Organization Unit เพิ่มเข้าไปในเวกเตอร์นั้นด้วย

ค่าของ Loss severity ใน ภาพที่ 11 จะถูกประเมินบนพื้นฐานของความสัมพันธ์ของค่าปัจจัยความเสี่ยงทั้ง 5 ปัจจัยที่กล่าวถึงก่อนหน้านี้ โดยค่าของ Loss Severity จะถูกประเมินเป็นค่าของอันดับ 1-5 ซึ่งแสดงถึงอันดับความรุนแรงของของเหตุการณ์ที่มีรูปแบบของปัจจัยหนึ่ง ซึ่งมีความหมายเป็น น้อยมาก (Very Low), น้อย (Low), ปลานกลาง (Medium), สูง (High) และสูงมาก (Very High) ตามลำดับ

4.2 การเตรียมข้อมูล (data preprocessing)

โดยทั่วไปแล้วการเตรียมข้อมูลประกอบด้วยงานที่เกี่ยวข้องกับการทำความสะอาดข้อมูล (Data Cleaning) การแปลงข้อมูล (Data Transformationและการลดข้อมูล (Data Reduction) เมื่อการเก็บข้อมูลเสร็จสิ้นชุดข้อมูลที่ได้จะผ่านการตรวจสอบจากผู้เชี่ยวชาญเพื่อจัดการกับข้อผิดพลาดที่อาจเกิดขึ้นและเพื่อลดความผิดพลาดของข้อมูลที่ใช้ในการวิจัย สำหรับการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะต้องมีการแปลงข้อมูล Organization Unit จากเลขฐานสิบไปเป็นเลขฐานสองที่แสดงด้วยค่า 0 และ 1 ที่เรียงต่อกันและปัจจัยที่เป็นข้อมูลนำเข้าส่วนอื่น ๆ จะถูกแปลงเช่นเดียวกันแต่จะมีการแปลงโดยอัตโนมัติโดยโปรแกรม Weka ส่วนการสร้างโมเดลการวิเคราะห์เส้นทางจะใช้ข้อมูลที่เป็นเลขฐานสิบเหมือนดังข้อมูลที่เก็บได้เลย

4.3 ผลการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

การกำหนดโครงสร้างของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กการกำหนดโครงสร้างของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะกำหนดโหลดข้อมูลนำเข้าจากปัจจัยสาเหตุของความเสี่ยงทางด้านการปฏิบัติการที่กำหนดไว้ ผลการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กที่สร้างขึ้นจากโปรแกรม WEKA แสดงดัง ภาพที่ 15 แสดงถึงโครงสร้างของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กสร้างขึ้นซึ่งประกอบด้วยโหนด (node) สีแดง เหลือง และเขียว ซึ่งจะแบ่งออกเป็น Input Layer, Hidden layer และ Output layer โดยมีจำนวนโหนดเป็น 55, 30 และ 5 ตามลำดับ โดยจำนวนของ Hidden layer เป็นผลลัพธ์จากผลบวกของจำนวนโหนดของ Input layer และ Output layer ที่เป็นคลาส แล้วหารด้วยสองซึ่งโครงสร้างของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กดังกล่าวได้จากการออกแบบข้อมูลนำเข้าและข้อมูลผลลัพธ์ดัง ตารางที่ 8 โดยโปรแกรม WEKA จะทำการแปลงข้อมูลที่เป็นชนิดนามบัญญัติเป็นข้อมูลนำเข้าแบบเลขฐานสองโดยอัตโนมัติ

ตารางที่ 8 การกำหนดค่าข้อมูลนำเข้าและโครงสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

ชื่อปัจจัย	สัญลักษณ์ที่ใช้	ค่าที่เป็นไปได้	ชนิดของข้อมูล	สถานะ	จำนวนโหนด
1. ผู้กระทำ	ACTOR	1-2	nominal	Input	2
2. ชนิดภัยคุกคาม	THREATTYPE	1-5	nominal	Input	5
3. ชนิดเหตุการณ์	EVENTTYPE	1-7	nominal	Input	7
4. ทรัพย์สินหรือทรัพยากร	ASSET/ RESOURCE	1-5	nominal	Input	5
5. หน่วยงาน	ORGUNIT	1-36	nominal	Input	36
6. ระดับความรุนแรง	LOSSSEVERITY	VL, L, M, VH, H	ordinal	Output	5

ผลการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กที่สร้างขึ้นจากโปรแกรม WEKA แสดงดังภาพที่ 15 โมเดลที่สร้างขึ้นจะใช้วิธีการตรวจสอบความแม่นยำโดยมีการแบ่งชุดข้อมูลแบบ K-fold ซึ่งได้กำหนดค่า K เท่ากับ 10

ตารางที่ 9 แสดงค่าพารามิเตอร์ต่าง ๆ ที่ใช้ในการสร้างโมเดลโครงข่ายประสาทเทียม เป็นค่าซึ่งได้มีการทดลองการปรับเปลี่ยนค่าอัตราการเรียนรู้ (Learning rate) โมเมนตัม (Momentum) และจำนวนรอบการเรียนรู้ (Number of Epochs) ประกอบกับการกำหนดรูปแบบของข้อมูลนำเข้าและข้อมูลผลลัพธ์ เพื่อให้ได้โมเดลที่เหมาะสมแล้ว

ตารางที่ 9 การตั้งค่าพารามิเตอร์ของโครงข่ายประสาทเทียม

พารามิเตอร์	K-Fold	อัตราการเรียนรู้	โมเมนตัม	จำนวนรอบการเรียนรู้
การตั้งค่า	10	0.01	0.2	50000

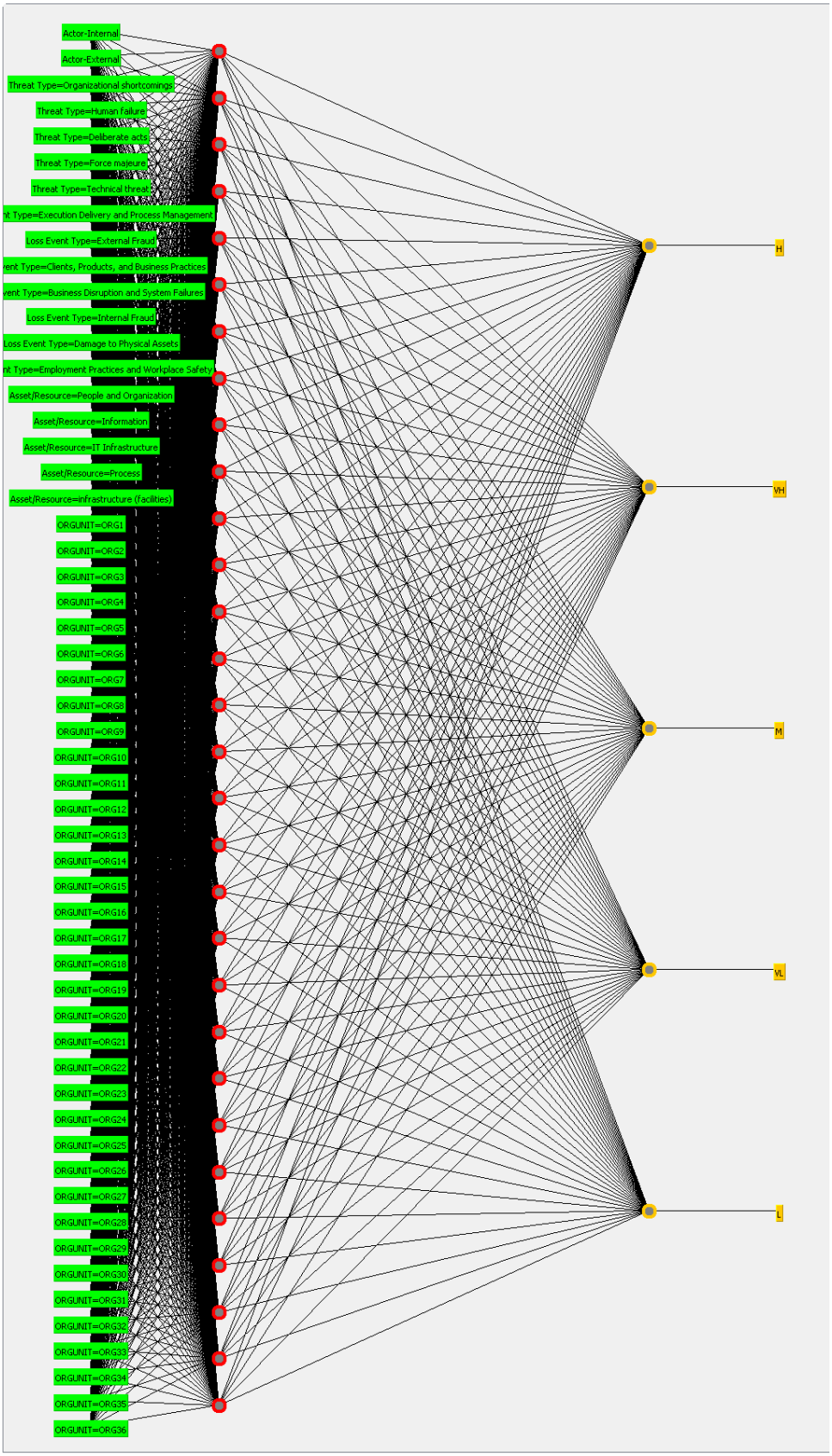
ตารางที่ 10 การประเมินผลการทำนายระดับการสูญเสียของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

การประเมินผลโมเดลการจัดอันดับสถานการณ์ความเสี่ยง	การสรุปผล	
	จำนวนวัตถุที่จำแนกกลุ่มผิด	จำนวนวัตถุที่จำแนกกลุ่มกลุ่มถูกต้อง
จำนวนวัตถุ	53	1,255
ร้อยละของวัตถุ	4.05%	95.95%

ตารางที่ 11 ผลการประเมินของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

ลำดับ	ตัววัด	การวัดผล
1	RMSEA	0.1131
2	ความแม่นยำ	95.95%
3	Kappa coefficient	0.9377

ประสิทธิภาพของการสร้างโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะถูกประเมินโดยใช้วิธีการวัดอัตราความแม่นยำของโมเดลซึ่งเป็นสัดส่วนของจำนวนข้อมูลที่ทำนายถูกต้องกับจำนวนข้อมูลทั้งหมด โดยทั่วไปเมื่อข้อมูลที่เก็บมีขนาดที่ไม่ใหญ่นักความถูกต้องของโมเดลจะถูกประเมินผลกับวิธีการตรวจสอบแบบ K-fold ซึ่งในงานวิจัยนี้ได้กำหนดค่า K ให้เท่ากับ 10 โดยการทำงานของวิธีการตรวจสอบความแม่นยำแบบ K-fold จะมีการแบ่งข้อมูลออกเป็นซึ่งการวัดค่าความแม่นยำโดยปกติจะต้องมีการแบ่งข้อมูลออกเป็น 2 ชุดคือ ข้อมูลชุดสอนและข้อมูลทดสอบ โดยจะแบ่งข้อมูลออกเป็น 10 กลุ่มและโดยชุดสอนจะมีขนาดเท่ากับ 9 กลุ่มและชุดข้อมูลทดสอบเท่ากับ 1 กลุ่ม การตรวจสอบจะต้องสั่งให้โปรแกรมทำการประเมินผลโมเดลทั้งหมด 10 รอบในแต่ละรอบกลุ่มที่ใช้ในการทดสอบจะสลับกันไปจนครบ และผลการทำนายความถูกต้องที่ได้ในแต่ละรอบจะนำมาเฉลี่ยออกมาเป็นค่าความแม่นยำรวมของโมเดลมีค่าเท่ากับ 95.95 เปอร์เซ็นต์ดังตารางที่ 10 นอกจากนั้นการประเมินค่าความถูกต้องของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก ควรพิจารณาตัววัดอื่น ๆ ประกอบด้วย ได้แก่ ตัววัด RMSEA และ Kappa coefficient เพื่อช่วยบอกถึงความน่าเชื่อถือและความสอดคล้องของโมเดล ซึ่งผลที่ได้มีค่าเท่ากับ 0.1131 และ 0.9377 ตามลำดับแสดงดังตารางที่ 11



ภาพที่ 15 โครงสร้างของโครงข่ายหลายชั้นสำหรับโมเดลการเรียนรู้

4.4 ผลการสร้างโมเดลสมการโครงสร้าง

การกำหนดตัวแปรนำเข้าของโมเดลสมการโครงสร้างผ่านโปรแกรมสถิติ SPSS จะกำหนดตัวแปรทั้งหมดเป็นชนิดตัวเลขมีค่าเป็นจำนวนเต็มบวก การกำหนดชื่อสัญลักษณ์ในโปรแกรมสถิติ SPSS จะต้องไม่มีสัญลักษณ์พิเศษหรือเป็นช่องว่าง แม้ว่าโมเดลสมการโครงสร้างจะใช้หลักการของหลักการวิเคราะห์การถดถอย แต่โมเดลสมการโครงสร้างจะมีข้อแตกต่างคือปัจจัยที่ใช้ในการกำหนดตัวแปรในโมเดลสามารถเป็นได้ทั้งปัจจัยสาเหตุและปัจจัยผลลัพธ์ในเวลาเดียวกัน ซึ่งรายละเอียดแสดงดังตารางที่ 12

ตารางที่ 12 การกำหนดค่าข้อมูลนำเข้าและโครงสร้างโมเดลสมการโครงสร้าง

ชื่อปัจจัย	สัญลักษณ์ที่ใช้	ค่าที่เป็นไปได้	ชนิดข้อมูล	สถานะ
1. ผู้กระทำ	ACTOR	1-2	numeric	ปัจจัยสาเหตุ
2. ชนิดภัยคุกคาม	THREATTYPE	1-5	numeric	ปัจจัยสาเหตุและผลลัพธ์
3. ชนิดเหตุการณ์	EVENTTYPE	1-7	numeric	ปัจจัยสาเหตุและผลลัพธ์
4. ทรัพย์สินหรือทรัพยากร	ASSET	1-5	numeric	ปัจจัยสาเหตุและผลลัพธ์
5. หน่วยงาน	ORGUNIT	1-36	numeric	ปัจจัยสาเหตุและผลลัพธ์
6. ระดับความรุนแรง	LOSSSEVERITY	1-5	numeric	ปัจจัยผลลัพธ์

เริ่มต้นจากการแปลงข้อมูลในแบบสอบถามให้อยู่ในรูปของไฟล์ .SAV โดยใช้โปรแกรมสถิติ SPSS แล้วนำเข้าไฟล์ .SAV สู่โปรแกรม AMOS เพื่อใช้ในการสร้างโมเดลสมการโครงสร้าง จากนั้นทำการสร้างโมเดลโดยวาดรูปตัวแปรต่างๆ ที่กำหนดไว้ในรูปสี่เหลี่ยม และทำการลากเส้นเชื่อมตามที่ทฤษฎีกำหนดเพื่อให้ได้แผนภาพโมเดลเส้นทาง ซึ่งจะใช้เป็นโมเดลตั้งต้นในการทดลองปรับโมเดลด้วยค่า MI ต่อไป การปรับโมเดลหรือการลากเส้นเชื่อมเพื่อหาความสัมพันธ์ในเชิงสาเหตุ ปกติเวลาปรับควรเลือกเส้นที่มีค่า MI มากที่สุดหรือค่าที่ใกล้เคียงกัน ณ ขณะที่เลือกและควรคำนึงถึงทฤษฎีด้วย ในการสร้างความสัมพันธ์ไม่จำเป็นต้องเลือกลากเส้นที่มีค่า MI สูงสุดเสมอไปอาจเลือกเป็นเส้นที่มี MI น้อยลงมาก็ได้ ขึ้นกับความสมเหตุสมผลเทียบกับทฤษฎี เนื่องจากโมเดลตั้งต้นส่วนใหญ่จะยังไม่เหมาะสมกับการนำไปใช้งาน พิจารณาได้จากค่าตัววัดทั้งหลายที่กล่าวไว้แล้วในข้อ 3.5 โดยรายละเอียดขั้นตอนการสร้างและการปรับโมเดลแสดงดังภาคผนวก ก

ภาพที่ 16 แสดงแผนภาพโมเดลเส้นทางของโมเดลสมการโครงสร้างที่สร้างขึ้น ก่อนที่จะมีการปรับค่าสัมประสิทธิ์สหสัมพันธ์ของโมเดลให้อยู่ในรูปมาตรฐาน ยังไม่สามารถนำมาเทียบกันได้ ใช้อธิบายค่าน้ำหนักที่ใช้ในการประมาณค่าของตัวแปรที่มีหน่วยต่างกัน ตัวเลขที่อยู่รอบ ๆ วงกลมบ่ง

บอกค่าความคลาดเคลื่อนของการประมาณ โดยค่าสัมประสิทธิ์ของเส้นเชื่อมระหว่างตัวแปรแต่ละตัวกับรูปวงกลมต้องมีค่าเป็น 1 เสมอ

ภาพที่ 17 แสดงแผนภาพโมเดลเส้นทางของโมเดลสมการโครงสร้างที่สร้างขึ้น ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรที่ปรับเป็นมาตรฐานแล้วกำกับอยู่บนเส้นเชื่อมบอกถึงอิทธิพลทางตรงของคู่ตัวแปร ซึ่งสามารถใช้เปรียบเทียบระหว่างตัวแปรได้ และค่าการเรียนรู้สำเร็จของแต่ละตัวแปรจะแสดงอยู่รอบๆ กรอบสี่เหลี่ยมของตัวแปร ตัวอย่างคำอธิบายแผนภาพ ได้แก่

1. ACTOR ทำหน้าที่เป็นตัวแปรสาเหตุเพียงอย่างเดียว
2. THREATTYPE เป็นตัวแปรที่มีอิทธิพลทางตรงกับตัวแปรอื่นๆ เกือบทั้งหมดยกเว้น ACTOR
3. THREATTYPE มีความสัมพันธ์ทางตรงในเชิงลบกับ EVENTTYPE มากที่สุด มีค่าเท่ากับ -0.64
4. ACTOR มีอิทธิพลทางตรงกับ EVENTTYPE มีค่า -0.10 และ ACTOR มีค่าอิทธิพลทางอ้อมกับ EVENTTYPE มีค่า -0.29 คำนวณจากผลคูณของค่าสัมประสิทธิ์สหสัมพันธ์ระหว่าง ACTOR กับ THREATTYPE และTHREATTYPE กับ EVENTTYPE คือ (0.46*(-0.64))

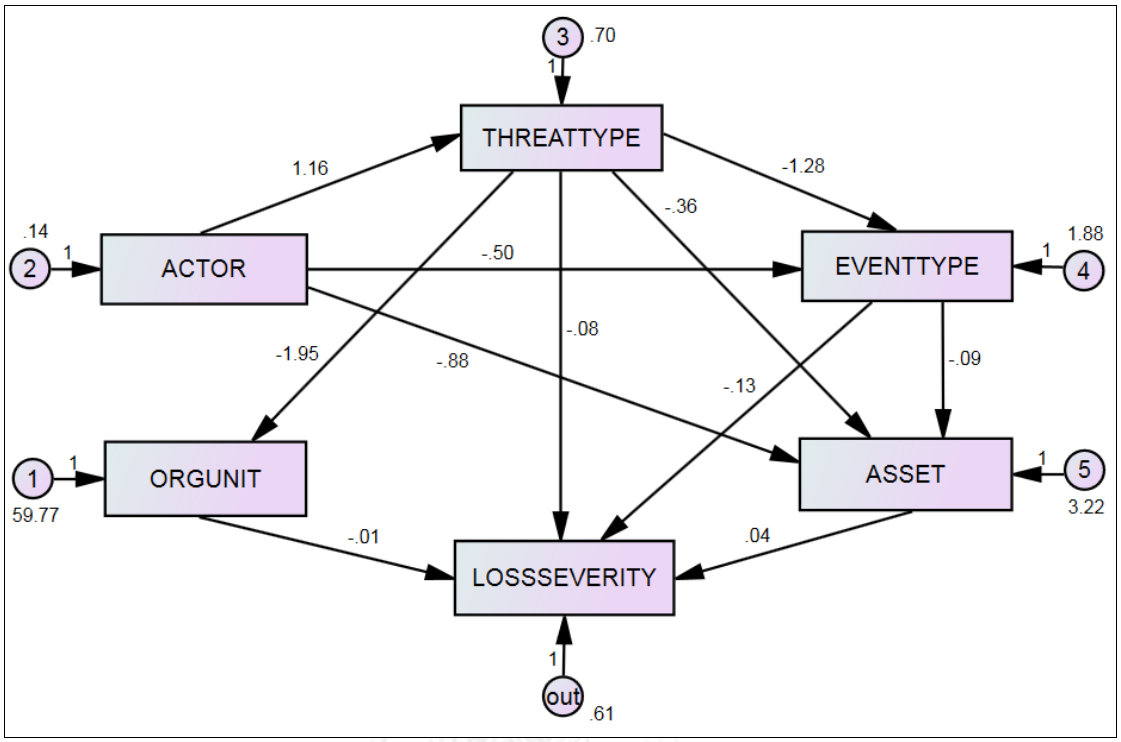
ภาพที่ 18,ภาพที่ 19ภาพที่ 20ภาพที่ 21 และภาพที่ 22 แสดงค่าตัววัดซึ่งบ่งบอกค่าความน่าเชื่อถือของโมเดล และค่าตัววัดที่ใช้ในการตรวจสอบค่าพารามิเตอร์ที่บ่งบอกความเหมาะสมของตัวแปรในโมเดลสมการโครงสร้างที่ได้จากงานวิจัย

ภาพที่ 18 แสดงค่าตัววัด CMIN/DF มีค่าเท่ากับ 0.722 และค่า P-value เท่ากับ 0.577 เป็นค่าที่ผ่านเกณฑ์ระดับการยอมรับ เนื่องจากค่า P-value มากกว่า 0.05 และค่าไคสแควร์มีนัยสำคัญ ส่วนค่าตัววัดอื่นๆ ได้แก่ GFI, AGFI และ RMSEA มีค่าเท่ากับ 0.999, 0.996 และ 0 ตามลำดับ ซึ่งผ่านเกณฑ์การยอมรับ หมายถึง โมเดลสมการโครงสร้างมีความสอดคล้องกับข้อมูลเชิงประจักษ์ สำหรับตัววัด HOELTER บ่งชี้ว่าขนาดข้อมูลที่ใช้สร้างโมเดลมีความเหมาะสม เนื่องจากมีค่าเท่ากับ 4,294 ซึ่งมากกว่าเกณฑ์ที่กำหนด

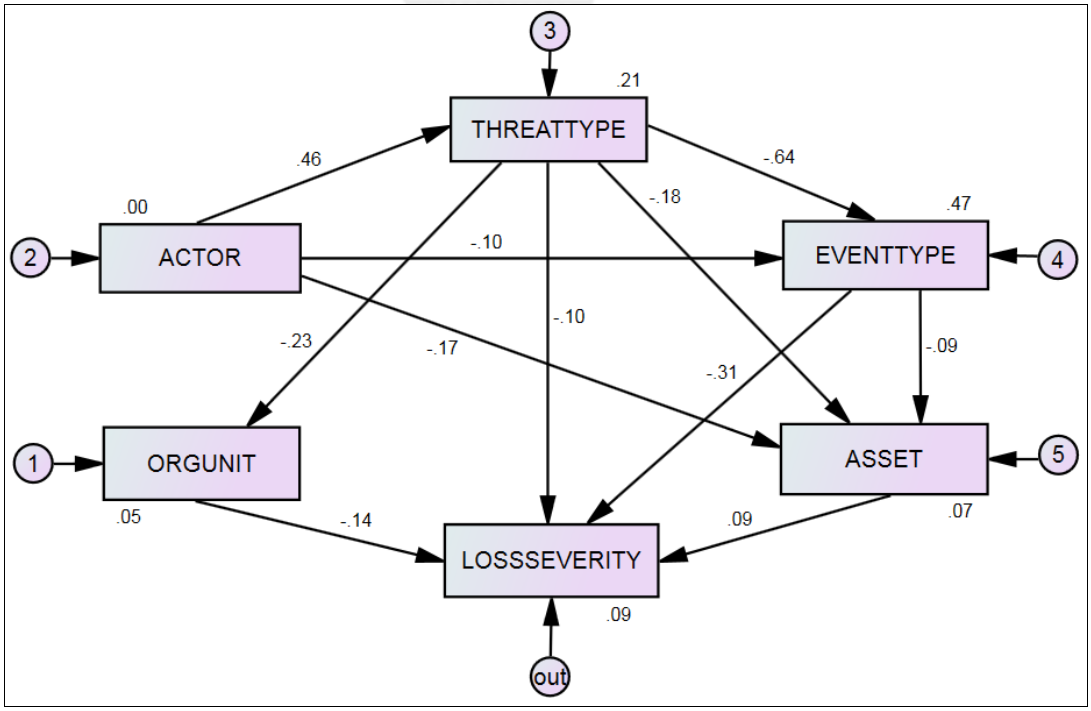
จากภาพที่ 19 พบว่า ค่าตัววัด SRC ของตัวแปรแต่ละคู่มีค่าอยู่ระหว่าง +2 และ -2 ประกอบกับผลใน ภาพที่ 20 ค่า C.R.ของทุกตัวแปรมากกว่า 1.96 และตัววัด P-value ของตัวแปรทุกตัวมีค่าน้อยกว่า 0.05 บ่งบอกว่าตัวแปรทุกตัวมีความเหมาะสมในโมเดล ไม่ต้องพิจารณาตัดตัวแปรตัวใดออก

ภาพที่ 21 แสดงผลของอิทธิพลทางตรง (SDE) อิทธิพลทางอ้อม (SIE) ผลรวมของอิทธิพลทางตรงและทางอ้อม (STE) ที่มีการทำให้เป็นมาตรฐานแล้ว และผลอิทธิพลรวม(ST) ของคู่ตัวแปรที่ยังไม่แปลงเป็นมาตรฐานของคู่ตัวแปรแต่ละตัว การเปรียบเทียบค่าอิทธิพลจะต้องเปรียบเทียบด้วยค่าที่ทำให้เป็นมาตรฐานแล้วเนื่องจากมีหน่วยเดียวกันแล้ว พบว่า ชนิดเหตุการณ์ความเสี่ยงมีอิทธิพลต่อระดับความรุนแรงการสูญเสียมากที่สุด สังเกตได้จากค่าความสัมพันธ์ของ EVENTTYPE ที่มีต่อ LOSSSEVERITY มีค่ามากที่สุดคือ -0.313 ตัวแปร ORGUNIT, THRETTYPE และ ASSET มีอิทธิพลต่อตัวแปร LOSSSEVERITY ในลำดับรองลงมาซึ่งมีค่าเป็น -0.137, 0.188 และ 0.086 ตามลำดับ และสุดท้าย

ACTOR มีอิทธิพลต่อระดับความรุนแรงการสูญเสียน้อยที่สุด มีค่าเป็น 0.069 เนื่องจาก ACTOR ไม่มีอิทธิพลทางตรงต่อ LOSSSEVERITY



ภาพที่ 16 โมเดลสมการโครงสร้างที่ได้จากงานวิจัยก่อนทำให้เป็นมาตรฐาน



ภาพที่ 17 โมเดลสมการโครงสร้างที่ได้จากงานวิจัยหลังทำให้เป็นมาตรฐาน

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	17	2.888	4	0.577	0.722
Saturated model	21	0	0		
Independence model	6	1430.011	15	0	95.334

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	0.071	0.999	0.996	0.19
Saturated model	0	1		
Independence model	0.803	0.724	0.614	0.517

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	0	0	0.036	0.994
Independence model	0.269	0.257	0.281	0

HOELTER

Model	HOELTER (0.05)	HOELTER (0.01)
Default model	4294	6009
Independence model	23	28

ภาพที่ 18 ผลการประเมินค่าความน่าเชื่อถือของโมเดล

Standardized Residual Covariances (Group number 1 - Default model)

	ACTOR	THREATTYPE	EVENTTYPE	ORGUNIT	ASSET	LOSSSEVERITY
ACTOR	.000					
THREATTYPE	.000	.000				
EVENTTYPE	.000	.000	.000			
ORGUNIT	-1.211	.000	.638	.000		
ASSET	.000	.000	.000	-.362	.000	
LOSSSEVERITY	-.022	.000	-.086	-.226	.050	.044

ภาพที่ 19 ผลของค่าตัววัด SRC

CHULALONGKORN UNIVERSITY

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
THREATTYPE	<---	ACTOR	1.162	.063	18.498	***	par_8
EVENTTYPE	<---	THREATTYPE	-1.276	.045	-28.165	***	par_10
EVENTTYPE	<---	ACTOR	-.502	.116	-4.350	***	par_11
ASSET	<---	ACTOR	-.880	.152	-5.785	***	par_2
ASSET	<---	THREATTYPE	-.359	.075	-4.785	***	par_3
ASSET	<---	EVENTTYPE	-.092	.036	-2.544	.011	par_5
ORGUNIT	<---	THREATTYPE	-1.954	.227	-8.606	***	par_9
LOSSSEVERITY	<---	EVENTTYPE	-.133	.016	-8.469	***	par_1
LOSSSEVERITY	<---	THREATTYPE	-.085	.032	-2.635	.008	par_4
LOSSSEVERITY	<---	ASSET	.038	.012	3.192	.001	par_6
LOSSSEVERITY	<---	ORGUNIT	-.014	.003	-5.068	***	par_7

ภาพที่ 20 ผลของค่า C.R. และค่า P-value

Standardized Direct Effects (Group number 1 - Default model)

	ACTOR	THREATTYPE	ASSET	EVENTTYPE	ORGUNIT
THREATTYPE	.455	.000	.000	.000	.000
ASSET	-.166	-.123	.000	.000	.000
EVENTTYPE	-.107	-.643	-.053	.000	.000
ORGUNIT	.000	-.232	.000	.000	.000
LOSSSEVERITY	.000	-.098	.086	-.305	-.137

Standardized Indirect Effects (Group number 1 - Default model)

	ACTOR	THREATTYPE	ASSET	EVENTTYPE	ORGUNIT
THREATTYPE	.000	.000	.000	.000	.000
ASSET	-.056	.000	.000	.000	.000
EVENTTYPE	-.281	.006	.000	.000	.000
ORGUNIT	-.105	.000	.000	.000	.000
LOSSSEVERITY	.069	.215	.016	.000	.000

Standardized Total Effects (Group number 1 - Default model)

	ACTOR	THREATTYPE	ASSET	EVENTTYPE	ORGUNIT
THREATTYPE	.455	.000	.000	.000	.000
ASSET	-.222	-.123	.000	.000	.000
EVENTTYPE	-.388	-.636	-.053	.000	.000
ORGUNIT	-.105	-.232	.000	.000	.000
LOSSSEVERITY	.069	.118	.102	-.305	-.137

Total Effects (Group number 1 - Default model)

	ACTOR	THREATTYPE	EVENTTYPE	ORGUNIT	ASSET
THREATTYPE	1.162	.000	.000	.000	.000
EVENTTYPE	-1.984	-1.276	.000	.000	.000
ORGUNIT	-2.270	-1.954	.000	.000	.000
ASSET	-1.115	-.242	-.092	.000	.000
LOSSSEVERITY	.154	.103	-.136	-.014	.038

ภาพที่ 21 ผลของค่า SDE, SIE, STE และ TE

การประเมินค่าความแม่นยำของโมเดลสมการโครงสร้างจะอยู่บนพื้นฐานของหลักการวิเคราะห์การถดถอยแบบพหุ ซึ่งจะประเมินค่าระดับความรุนแรงของการสูญเสียโดยใช้สมการ (10) และมีเกณฑ์การประมาณค่าความแม่นยำตามตาราง 13 พบว่าการประเมินค่าของโมเดลสมการโครงสร้างที่ได้มีจำนวนชุดข้อมูลที่สามารถทำนายได้ถูกต้องจำนวน 583 ชุดจากข้อมูล 1,308 ชุดคิดเป็นค่าความแม่นยำเท่ากับ 44.57 เปอร์เซ็นต์แสดงดังตาราง 14 โดยรายละเอียดของผลของการทำนายค่าความเสียหายของการสูญเสียโดยใช้โมเดลสมการโครงสร้างแสดงในภาคผนวก ข

$$Loss\ Severity_{est} = ACTOR(0.069) + THREATTYPE(0.118) + ASSET(0.102) + EVENTTYPE(-0.305) + ORGUNIT(-0.137) + C \quad (10)$$

ตารางที่ 13 เกณฑ์การประเมินความแม่นยำของโมเดลสมการโครงสร้าง

ลำดับ	ช่วงการประมาณค่า	การประเมินผล	LOSSEVERITY
1.	0.51-1.50	1	VL
2.	1.51-2.50	2	L
3.	2.51-3.50	3	M
4.	3.51-4.50	4	H
5.	4.51-5.50	5	VH

ตารางที่ 14 การประเมินผลการทำนายระดับการสูญเสียของโมเดลสมการโครงสร้าง

การประเมินผลโมเดลการจัดอันดับสถานการณ์ความเสี่ยง	การสรุปผล	
	จำนวนวัตถุที่ประมาณผิด	จำนวนวัตถุที่ประมาณถูกต้อง
จำนวนวัตถุ	725	583
ร้อยละของวัตถุ	55.43%	44.57%
RMSE	-	0.2066

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Squared Multiple Correlations: (Group number 1 - Default model)

	Estimate
ACTOR	.000
THREATTYPE	.207
EVENTTYPE	.471
ORGUNIT	.054
ASSET	.066
LOSSSEVERITY	.092

ภาพที่ 22 ผลของค่า SMC (Squared Multiple Correlations)

จากผลการวิเคราะห์ข้างต้น และผลดังภาพที่ 22 พบว่าค่าตัววัด SMC ของ LOSSSEVERITY ที่ถูกอธิบายโดยตัวแปรสาเหตุอื่นๆ มีค่าเป็นมีค่าเป็น 0.092 ซึ่งแปลผลได้ว่าความผันแปรของระดับความรุนแรงของการสูญเสียขึ้นกับค่าตัวแปรสาเหตุ ได้แก่ ผู้กระทำ ชนิดภัยคุกคาม ชนิดเหตุการณ์ความเสี่ยง และหน่วยงาน ร้อยละ 9.20 หมายความว่าโมเดลสามารถวัดผลความสำเร็จได้ในระดับน้อย

4.5 การเปรียบเทียบผลของโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง

จากตารางที่ 15 แสดงให้เห็นถึงค่าการเปรียบเทียบโดยใช้ตัววัดที่มีความเหมือนและต่างกัน ซึ่งจะเห็นได้ว่าค่าตัววัดโมเดลสมการโครงสร้าง CMIN/DF, GFI, RMSEA และ GFI ผ่านเกณฑ์การยอมรับ รวมถึงโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กค่า Kappa coefficient ก็อยู่ในระดับที่ดีเกณฑ์ที่ยอมรับได้ ซึ่งหมายความว่าทั้งสองโมเดลมีความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ ส่วนค่า RMSE ที่บ่งบอกถึงความคลาดเคลื่อนของการทำนายของโมเดลซึ่งจะเห็นได้ว่าโมเดลสมการโครงสร้างมีค่ามากกว่า ซึ่งหมายความว่าโมเดลสมการโครงสร้างมีความคลาดเคลื่อนในการทำนายมากกว่าโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก

ตารางที่ 15 ผลการเปรียบเทียบโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง

ลำดับ	ตัววัด	โมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์ก	โมเดลสมการโครงสร้าง
1	CMIN/DF	-	0.722
2	GFI	-	0.999
3	RMSEA	-	0
4	RMSE	0.1131	0.2066
5	Accuracy	95.95%	44.57%
6	Kappa coefficient	0.9377	-
7	GFI	-	0.999

อย่างไรก็ตาม เมื่อมาเปรียบเทียบโมเดลทั้งสองด้วยค่าความแม่นยำ พบว่าโมเดลสมการโครงสร้างอธิบายความสัมพันธ์เชิงเส้นของค่าตัวแปรสาเหตุ ได้แก่ ผู้กระทำ ชนิดภัยคุกคาม ชนิดเหตุการณ์ความเสี่ยง และหน่วยงาน ซึ่งมีผลต่อความถูกต้องของการทำนายระดับความรุนแรงการสูญเสียได้เพียงร้อยละ 44.57. เปรียบเทียบกับค่าความแม่นยำของโมเดลโครงข่ายประสาทเทียมมีค่าเท่ากับร้อยละ 95.95 ดังตารางที่ 15 เห็นได้ว่าโมเดลสมการโครงสร้างมีความสามารถในการทำนายค่าระดับความรุนแรงการสูญเสียได้น้อยกว่ามาก เนื่องจากโมเดลสมการโครงสร้างใช้หลักการการประเมินค่าบนพื้นฐานของความสัมพันธ์เชิงเส้น แต่โมเดลโครงข่ายประสาทเทียมมีความสามารถเรียนรู้ความสัมพันธ์ที่ไม่ใช่เชิงเส้น จากผลการวิจัยทำให้ทราบว่าความสัมพันธ์ระหว่างปัจจัยสาเหตุที่กำหนดขึ้น ได้แก่ ผู้กระทำ ชนิดภัยคุกคาม ชนิดเหตุการณ์ความเสี่ยง ทรัพย์สินหรือทรัพยากรที่ได้รับผลกระทบ และหน่วยงาน ที่มีต่อปัจจัยผล คือ ระดับความรุนแรงการสูญเสีย ไม่ใช่ความสัมพันธ์เชิงเส้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 5
การสรุปผลและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

งานวิจัยนี้ใช้เทคนิคการสร้างโมเดลสมการโครงสร้างซึ่งเป็นโมเดลทางสถิติ และโมเดลทางการเรียนรู้ของเครื่อง เพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรสาเหตุที่มีผลต่อตัวแปรผลลัพธ์ของความเสี่ยงทางด้านปฏิบัติการของธุรกิจทางด้านธนาคารและสถาบันการเงิน และใช้ตัวแปรสาเหตุดังกล่าวในการทำนายค่าระดับความรุนแรงการสูญเสีย จากโมเดลสมการโครงสร้างพบว่า ตัวแปรสาเหตุที่มีอิทธิพลต่อตัวแปรผลซึ่งได้แก่ LOSSSEVERITY โดยเรียงจากมากที่สุด คือ EVENTTYPE, ORGUNIT, THREATTYPE, ASSET และ ACTOR ซึ่งมีค่าความสัมพันธ์เท่ากับ -0.313, -0.137, -0.118, 0.086 และ 0.069 ตามลำดับ และการทำนายมีค่าความแม่นยำร้อยละ 44.05 ซึ่งมีค่าน้อยเมื่อเปรียบเทียบกับโมเดลโครงข่ายประสาทเทียมที่ให้ค่าความแม่นยำร้อยละ 95.95 จึงสรุปได้ว่าความสัมพันธ์ระหว่างตัวแปรสาเหตุกับตัวแปรระดับความรุนแรงมีความสัมพันธ์ที่ไม่เป็นเชิงเส้นทำให้โมเดลสมการโครงสร้างไม่สามารถอธิบายความสัมพันธ์ดังกล่าวได้ทั้งหมด อย่างไรก็ตาม ผลที่ได้จากการเปรียบเทียบค่าความแม่นยำของทั้งสองโมเดลไม่ได้หมายความว่าโมเดลโครงข่ายประสาทเทียมจะดีกว่าโมเดลสมการโครงสร้างในทุกด้าน ข้อดีของโมเดลสมการโครงสร้าง คือ สามารถใช้ทดสอบความสัมพันธ์ระหว่างตัวแปรด้วยการวิเคราะห์เส้นทาง ซึ่งช่วยให้สามารถวิเคราะห์อิทธิพลของตัวแปรหนึ่งที่ส่งผลถึงอีกตัวแปรหนึ่งได้ทั้งทางตรงและทางอ้อม

5.2 ข้อจำกัดและข้อเสนอแนะ

1. จำนวนปัจจัยสาเหตุที่นำมาใช้ในการวิจัย การประเมินความเสี่ยงทางด้านการปฏิบัติการโดยใช้การวิเคราะห์สถานการณ์ยังไม่เพียงพอที่จะอธิบายลักษณะของความเสี่ยงที่เกิดขึ้นได้ทั้งหมดยกตัวอย่าง ลักษณะของระยะเวลาที่เกิดขึ้น
2. การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสาเหตุโดยใช้สมการโครงสร้าง โดยใช้โปรแกรม AMOS เป็นการศึกษาความสัมพันธ์โดยแนวคิดของสมการเชิงเส้น จึงไม่สามารถอธิบายความสัมพันธ์ของเหตุที่ต้องการศึกษาที่มีต่อตัวแปรผลได้
3. ความสัมพันธ์ระหว่างตัวแปรที่เกิดขึ้นโดยโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กจะอยู่ในรูปของค่าน้ำหนักของเส้นเชื่อมระหว่างโหนดซึ่งมีจำนวนมาก ความสัมพันธ์ที่ได้จึงยากที่มนุษย์จะเข้าใจได้โดยง่าย

5.3 แนวทางการวิจัยต่อ

1. เพิ่มขอบเขตของการศึกษาการวิเคราะห์ตัวแปรสาเหตุที่เกี่ยวข้องกับการบริหารความเสี่ยงให้มากขึ้น อาจรวมไปจนถึงระยะเวลาที่เกิดขึ้น หรือปัจจัยที่เกี่ยวข้องกับการบริหารโครงการ
2. ทำการเพิ่มจำนวนและกลุ่มของผู้เชี่ยวชาญที่ทำการประเมินแบบสอบถามให้มีความหลากหลายเพิ่มขึ้นเพื่อศึกษามุมมองของการบริหารความเสี่ยงที่แตกต่างออกไปได้

รายการอ้างอิง

1. ISO/IEC31000, *Risk management - Principles and guidelines*. 2009.
2. IEC/FDIS31010, *Risk management - Risk assessment techniques*. 2009.
3. ISACA, *The Risk IT Framework.* 2009.
4. IT Governance Institute (ITGI), *The Importance of Governance and Risk Management for Compliance - IT Control Objectives for BASEL II*. 2007.
5. Thomas Peltier, *Information Security Risk Analysis*. 3 ed. 2010, Boca Raton: CRC Press.
6. Basel Committee on Banking Supervision, *Operational Risk Data Collection Exercise – 2002.* 2002.
7. รศ.ดร.ญาใจ ลิ่มปิยะกรณ์, เอกสารคำสอนการทำเหมืองข้อมูล. 2012.
8. Thom Mitchell, *Machine Learning*. 1997: The McGraw-Hill Companies, Inc.
9. กัลยา วานิชย์บัญชา, การวิเคราะห์สมการโครงสร้างด้วย *AMOS*. 1 ed. 2556, กรุงเทพมหานคร: ห้างหุ้นส่วนจำกัดสามลดา.
10. สมถวิล วิจิตรวรรณา สุภมาส อังศุโชติ, รัชนีกูล ภิญโญภานุวัฒน์, สถิติวิเคราะห์สำหรับการวิจัยทางสังคมศาสตร์และพฤติกรรม: เทคนิคการใช้โปรแกรม *LISREL*. 2554, บริษัทเจริญดีมั่นคงการพิมพ์: กรุงเทพมหานคร.
11. Reijo Savola, *Quality of security metrics and measurements.* Computers & Security, 2013. **37**: p. 78-90.
12. Carol Smidts Ming Li, *A ranking of software engineering measures based on expert opinion.* IEEE Transactions on Software Engineering, 2003. **29**(9): p. 811-824
13. *Weka tool*. Available from: http://www.cs.waikato.ac.nz/ml/weka/.
14. IBM Software Business Analytics *IBM SPSS Statistics - Solve research problems easily and efficiently*. 2012.
15. IBM Software Business Analytics *Structural Equation Modeling with IBM SPSS Amos - A methodology for predicting behavioral intentions in the services sector*. 2010.
16. Kenneth Bollen, *Structural Equations with Latent Variable*. 1989, New York: Wliey.
17. John Mclver Edward Carmines, *Analyzing Models with Unobserved Variable: Analysis of covariance structures.* 1981(Social measurement: current issues (66-115)).
18. Jon Hoelter, *The analysis of covariance structures: Goodness-of-fit indices.* Sociological Methods and Research, 1983(11): p. 325-344.

19. Rick Hoyle, *Structural Equation Modeling: Concept, Issues and Application*. 1995, Sage Publecatios, Inc: California.
20. Micheline Kamber Jiawei Han, *Data Mining: Concepts and Techniques*. 2 ed. 2006: Morgan Kaufmann.
21. Dag Sörbom Karl Gustav Jöreskog, *LISREL-VI user's guide*. 3 ed. 1984, Mooresville, IN: Scientific Software.
22. Joanne Garrett Anthony Viera, *Understanding Interobserver Agreement: The Kappa Statistic.* Family Medicine, 2005. **37**(5): p. 360-363.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

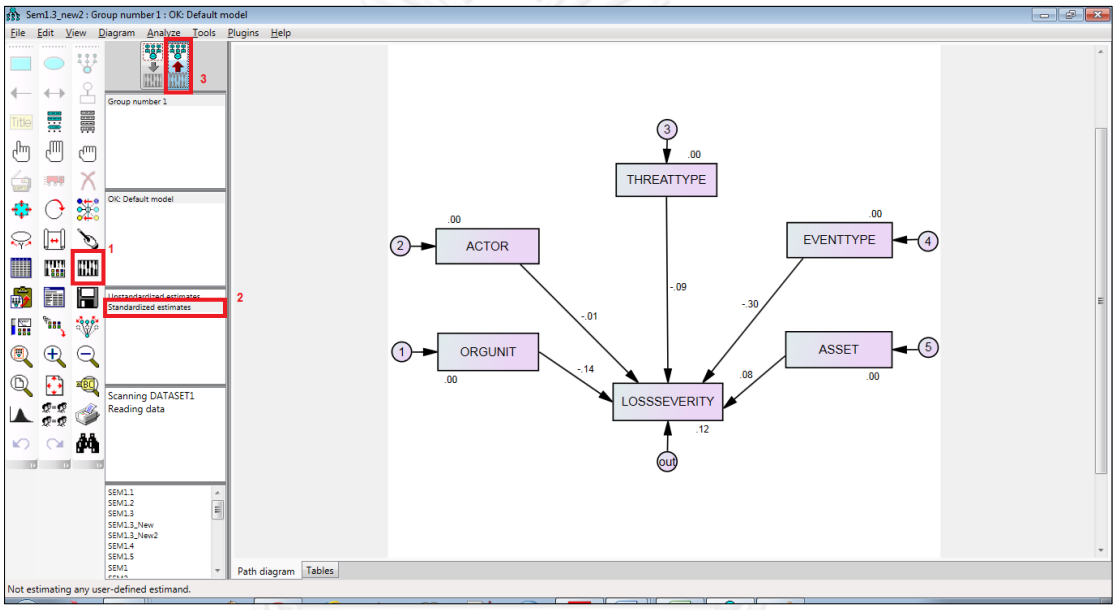
ภาคผนวก

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาคผนวก ก

ขั้นตอนการปรับโมเดลสมการโครงสร้าง

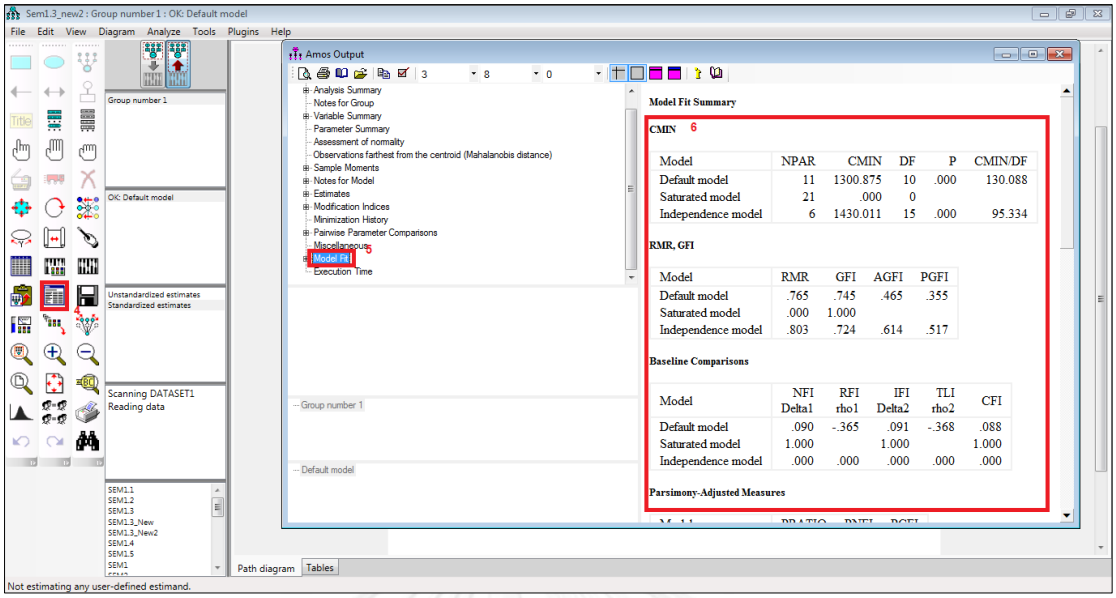
1. วาดแผนภาพเส้นทางของตัวแปรสาเหตุกับตัวแปรผลตามทฤษฎีที่กำหนดใส่ในโปรแกรม AMOS
2. ทำการสั่งประมวลผลโดยกดไปที่หมายเลข 1
3. จากนั้นเลือกโหมดการแสดงผลเป็น Standardized estimate
4. กดแสดงผลการสร้างโมเดลโดยกดที่ปุ่มหมายเลข 3



ภาพที่ 23 สมการโครงสร้างตามหลักทฤษฎี

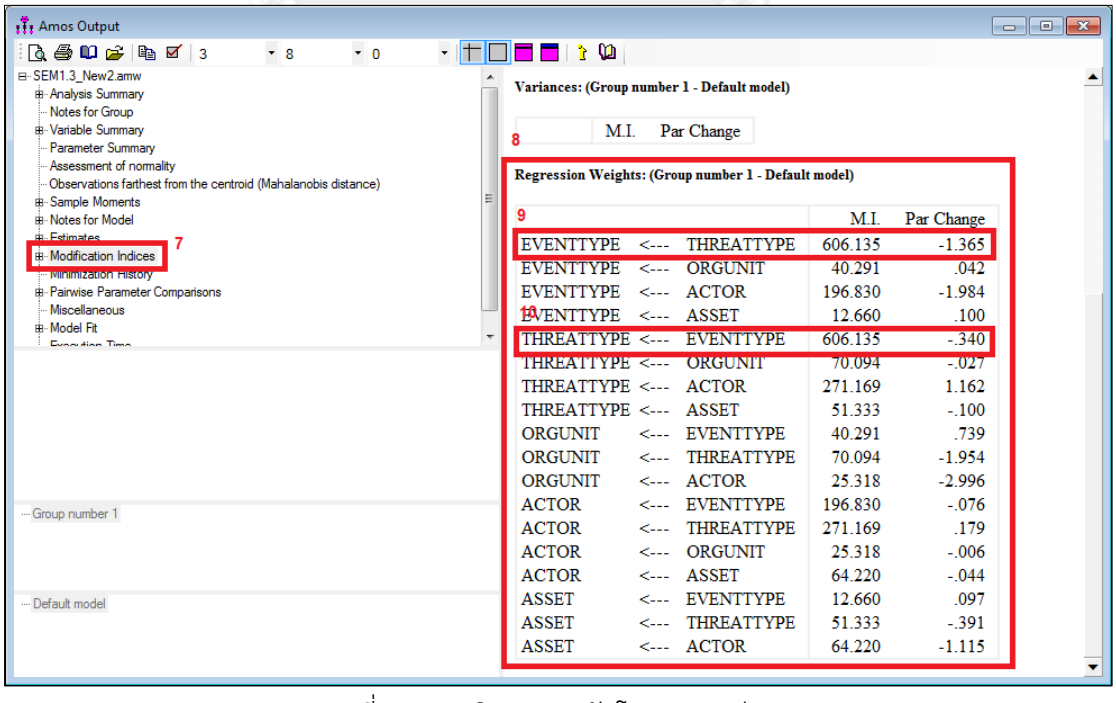
5. กดไปที่หมายเลข 4 เพื่อทำการเปิดรายละเอียดการประมวลผลเลือกไปที่ Model fit ตามหมายเลข 5 และทำการพิจารณาค่าเกณฑ์ที่หมายเลข 6 ตามที่ได้กล่าวไปในหัวข้อ 3.4 ซึ่งผลที่ได้ในที่นี้ยังไม่ดี ต้องทำการปรับโมเดล

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY



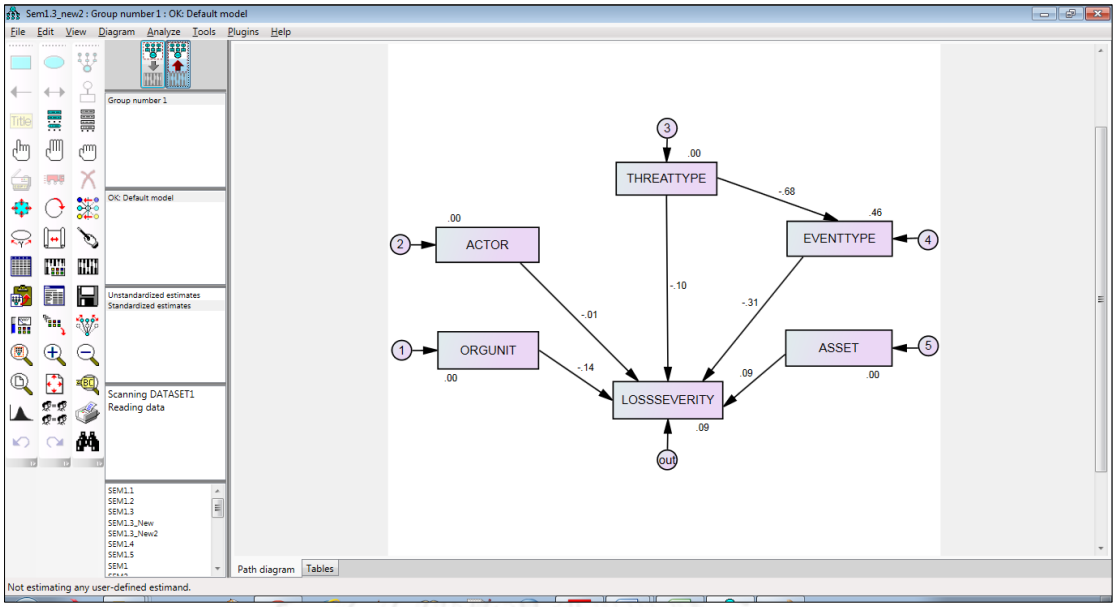
ภาพที่ 24 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง

6. ทำการวิเคราะห์การปรับโมเดลโดยกดไปที่ Modification Indice ตามหมายเลข 7
7. จากนั้นพิจารณาการลากเส้นเพื่อสร้างความสัมพันธ์จากตาราง Regression Weight ดังหมายเลข 8
8. จากนั้นทำการเลือก คู่ตัวแปรและทิศทางที่จะทำการปรับโมเดลในที่นี้จะเป็นว่าคู่ตัวแปรหมายเลข 9 และ 10 มีค่ามากที่สุด ในที่นี้เลือกหมายเลข 9 เนื่องจากชนิดของภัยคุกคามจะก่อให้เกิดลักษณะของเหตุการณ์ความสูญเสียที่แตกต่างกันได้ตามทฤษฎี



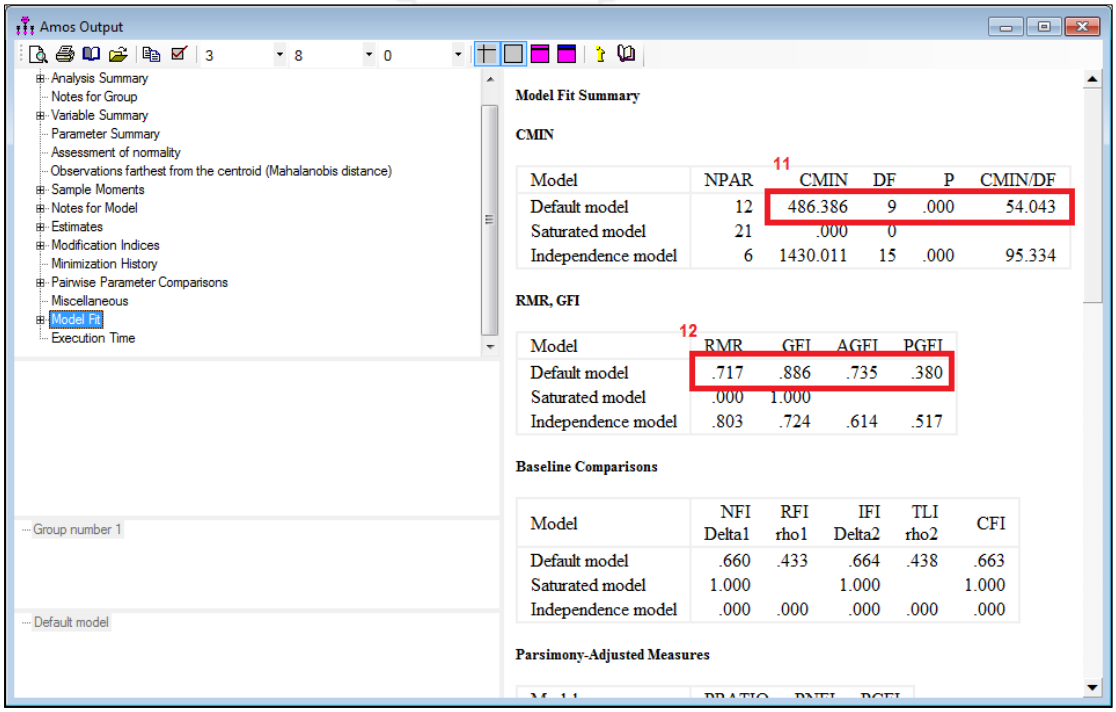
ภาพที่ 25 การพิจารณาปรับโมเดลจากค่า MI

9. จากนั้นทำการปรับโมเดลตามที่เลือกในข้อ 9 และทำการสั่งประมวลผลและแสดงผลใหม่ ซึ่งจะสังเกตได้ถึงเส้นความสัมพันธ์ที่เพิ่มขึ้น

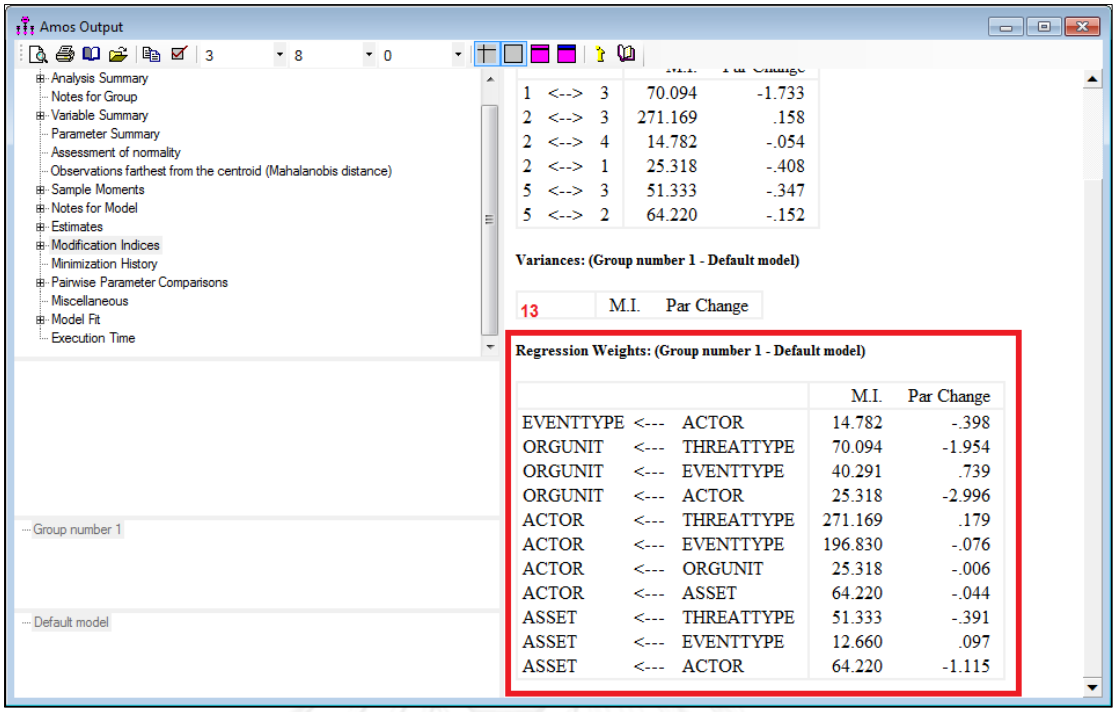


ภาพที่ 26 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ2

10. จากนั้นจะเห็นได้ถึงค่าความน่าเชื่อถือของโมเดลที่ดีขึ้น และรายการตัวแปรที่ต้องทำการปรับที่เปลี่ยนไปดังหมายเลข 11, 12 จากภาพที่ 27 และหมายเลข 13 จากภาพที่ 28

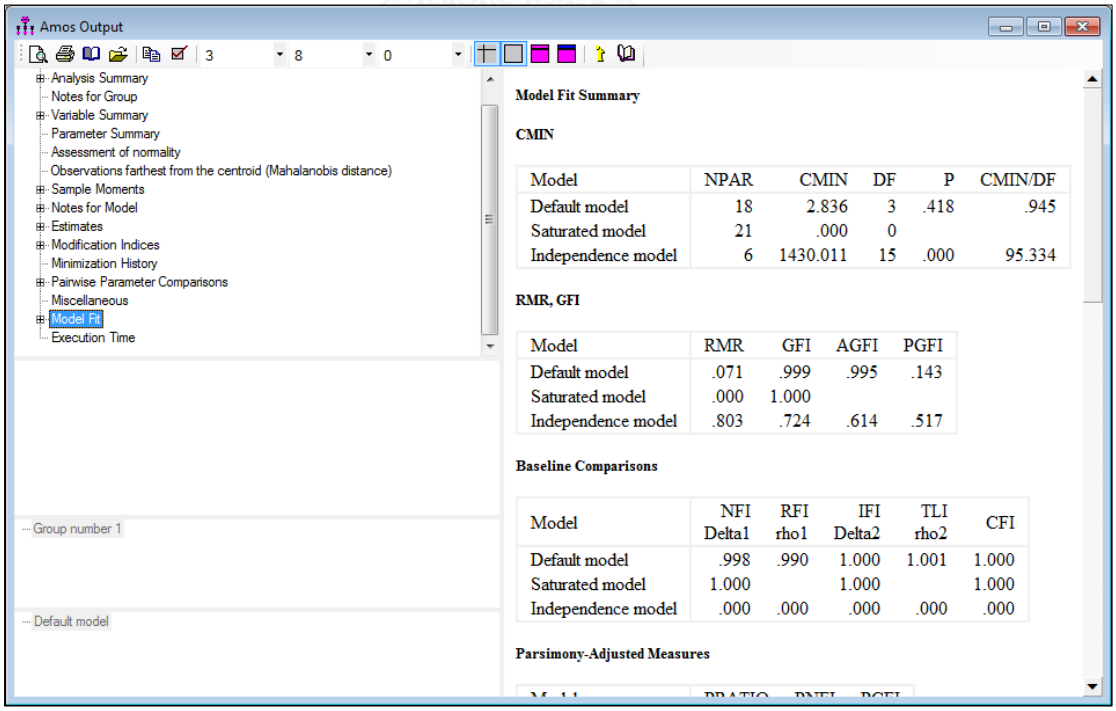


ภาพที่ 27 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง2

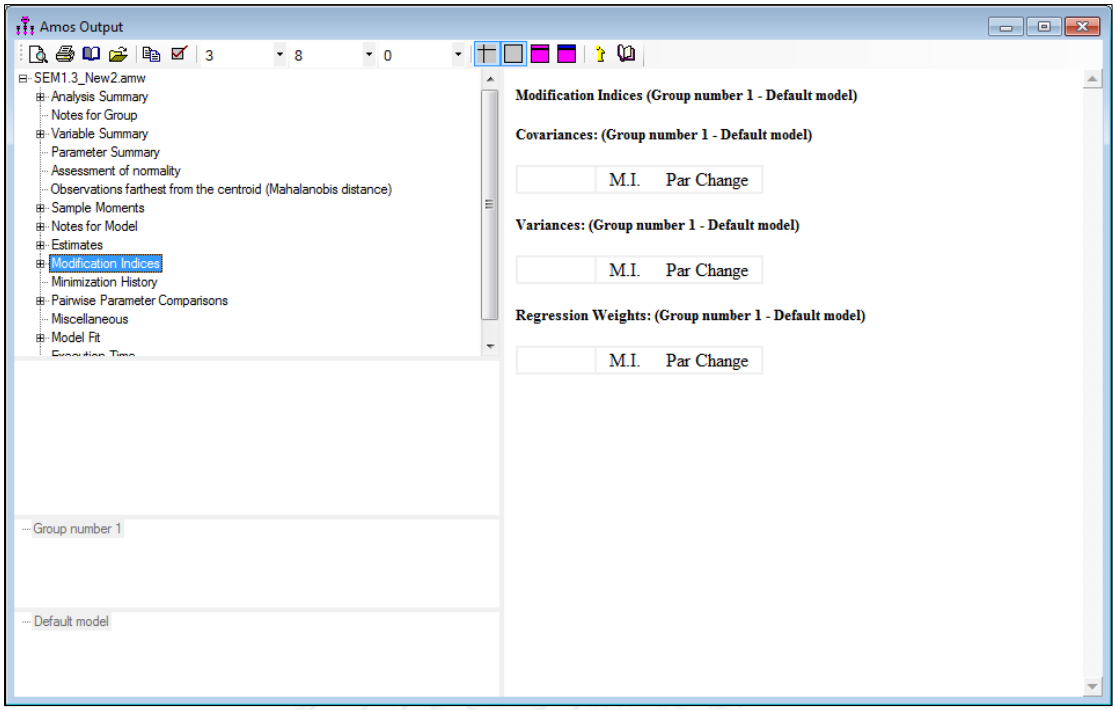


ภาพที่ 28 การพิจารณาปรับโมเดลจากค่า MI2

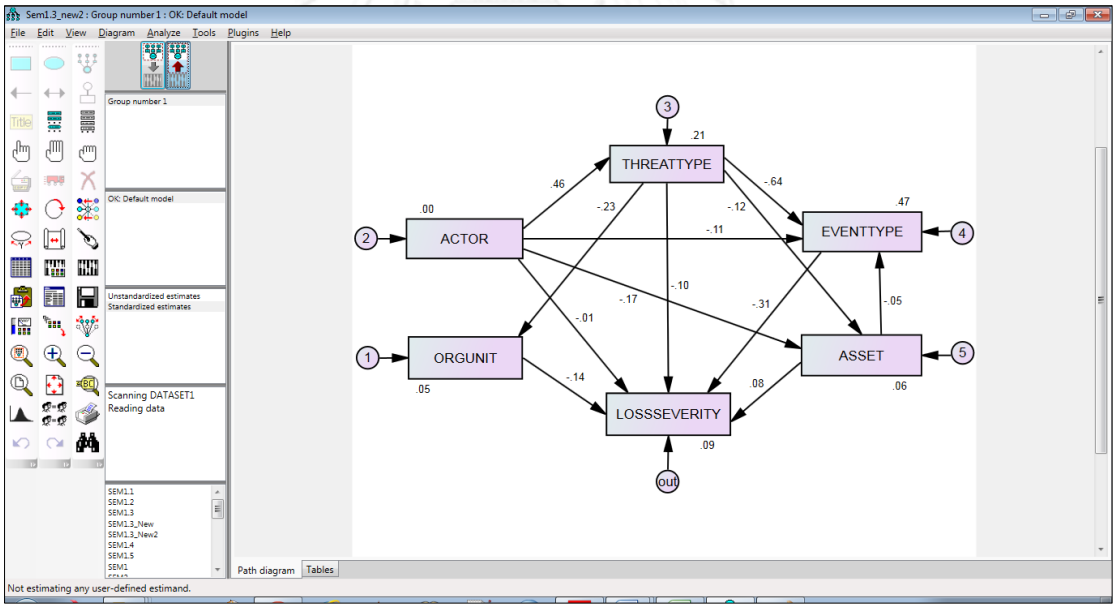
11. จากนั้นทำการปรับโมเดลไปเรื่อย ๆ จนกว่าค่าความน่าเชื่อถือของโมเดลจะอยู่ในเกณฑ์ที่ยอมรับและไม่สามารถปรับได้อีกดัง ภาพที่ 29,ภาพที่ 30 และได้แผนภาพโมเดลตามภาพที่ 31



ภาพที่ 29 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง3

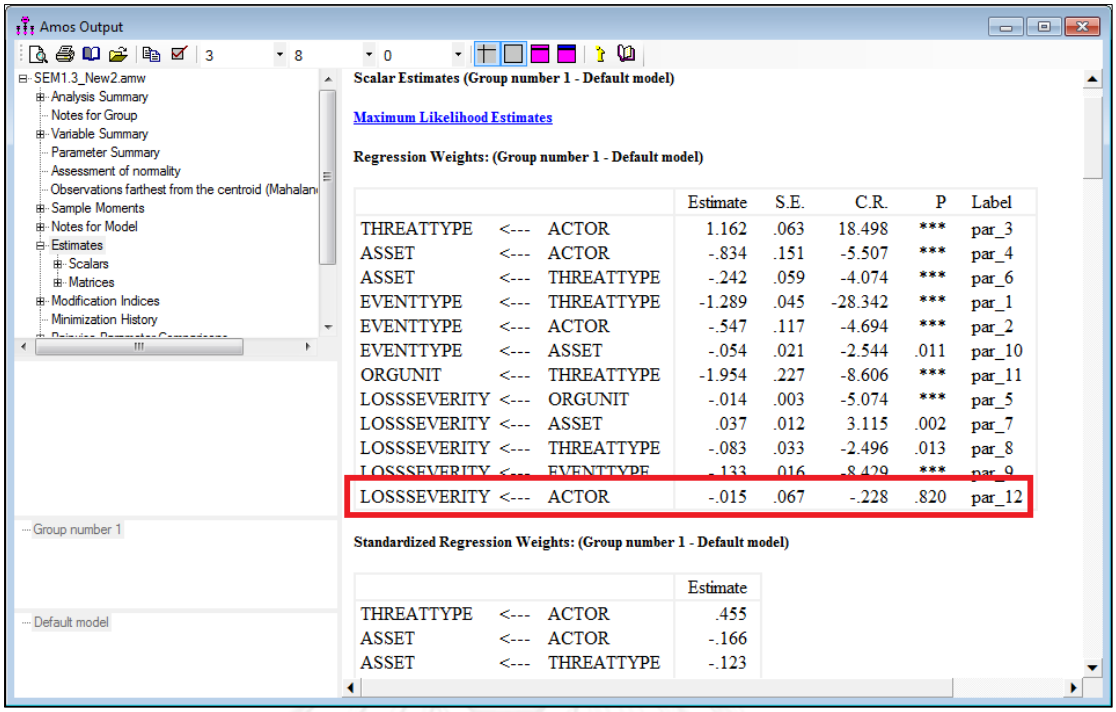


ภาพที่ 30 การพิจารณาปรับโมเดลจากค่า MI3



ภาพที่ 31 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ3

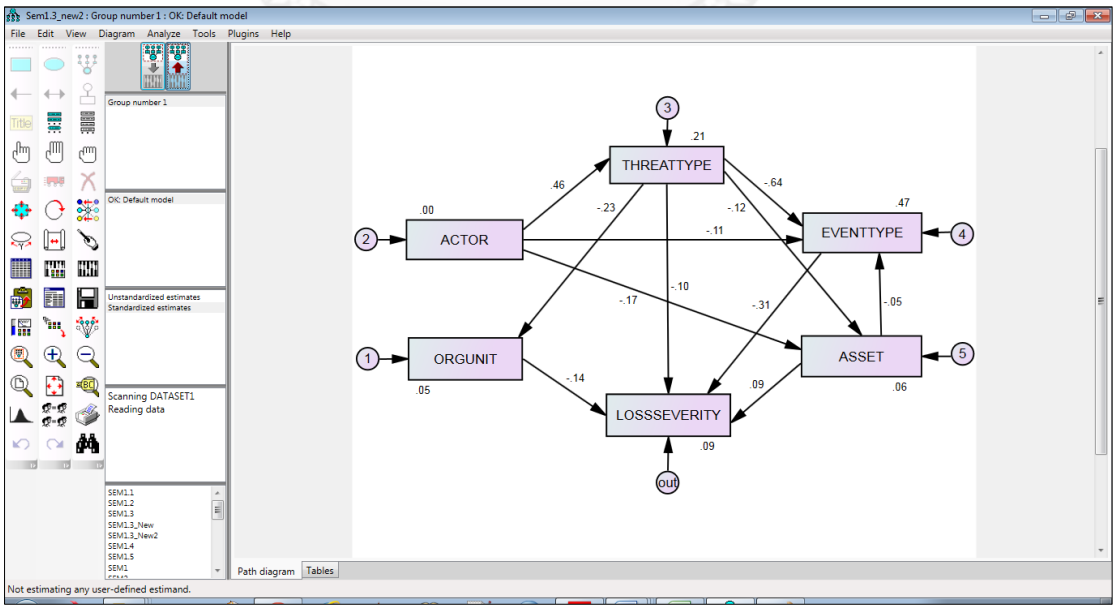
12. จากนั้นทำการตรวจสอบค่าความสัมพันธ์ตัวแปรแต่ละเส้นอีกครั้งโดยกดไปที่ Estimates และพิจารณาค่า C.R. และ P-value จากตาราง Maximum Likelihood Estimates ในส่วนของ Regression Weight ซึ่งจะพบว่าความสัมพันธ์ระหว่าง ACTOR->LOSSSEVERITY มีค่า |C.R.| น้อยกว่า 1.96 และ P-value มากกว่า 0.05 แสดงว่าตัวแปรนี้ไม่มีอิทธิพลต่อกัน ควรตัดทิ้ง



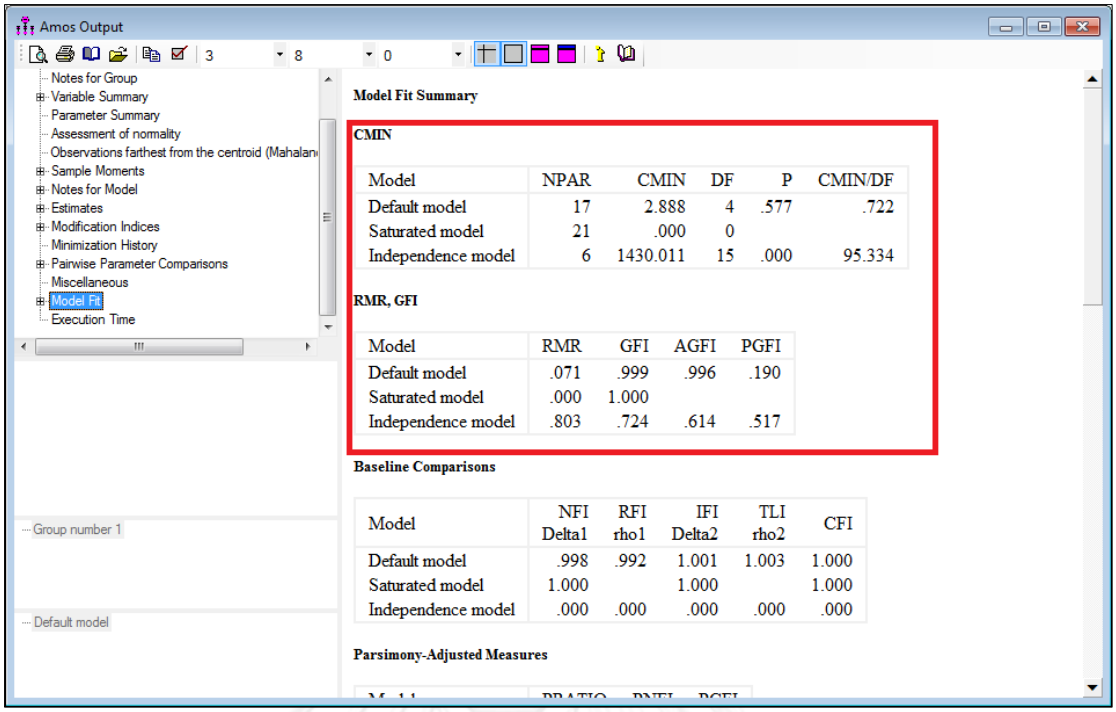
ภาพที่ 32 การตรวจสอบจากค่า C.R. และ P-value

13. ทำการตัดเส้นเชื่อมระหว่าง ACTOR และ LOSSSEVERITY ออกและจะได้โมเดลดังภาพที่ 33 และจะพบว่าค่าความน่าเชื่อถือของโมเดลจะดีขึ้นดังภาพที่ 34

14. กลับไปตรวจสอบค่า C.R. และ P-value อีกครับพบว่าไม่มีความสัมพันธ์ของตัวแปรคู่ใดมีค่า |C.R.| น้อยกว่า 1.96 และ P-value มากกว่า 0.05 บ่งบอกว่าไม่ต้องตัดตัวความสัมพันธ์ใดออกแล้วก็เสร็จสิ้นการปรับโมเดล



ภาพที่ 33 สมการโครงสร้างตามหลักทฤษฎีที่มีการปรับ4



ภาพที่ 34 ค่าความน่าเชื่อถือของโมเดลสมการโครงสร้าง4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาคผนวก ข

ผลการประมาณค่าระดับความรุนแรงการสูญเสียโดยโมเดลสมการโครงสร้าง

ตารางที่ 16 ผลการเปรียบเทียบโมเดลแบ็คพรอพาเกชันนิวรอลเน็ตเวิร์กและโมเดลสมการโครงสร้าง

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1	27	1	2	7	1	2.923513761	3	2
2	27	1	2	7	1	2.923513761	3	2
3	14	1	3	7	5	3.360513761	3	5
4	14	1	3	7	5	3.360513761	3	5
5	23	1	3	7	5	3.234513761	3	4
6	23	2	5	2	1	4.122513761	4	4
7	23	1	2	6	4	3.229513761	3	4
8	23	1	3	7	5	3.234513761	3	4
9	23	2	3	7	1	3.236513761	3	4
10	23	1	3	7	1	3.082513761	3	4
11	23	1	3	7	5	3.234513761	3	4
12	23	1	3	7	1	3.082513761	3	4
13	23	1	3	7	5	3.234513761	3	4
14	23	2	5	2	1	4.122513761	4	4
15	24	1	3	7	1	3.068513761	3	4
16	24	1	3	7	5	3.220513761	3	4
17	24	2	5	2	1	4.108513761	4	4
18	24	2	3	7	1	3.222513761	3	4
19	24	1	3	7	1	3.068513761	3	4
20	24	1	2	7	1	2.965513761	3	3
21	24	1	3	7	1	3.068513761	3	4
22	24	1	3	7	1	3.068513761	3	4
23	24	1	5	1	1	4.090513761	4	4
24	24	1	3	7	1	3.068513761	3	4
25	24	1	2	4	5	3.525513761	4	4
26	24	2	5	2	1	4.108513761	4	4
27	24	1	3	7	5	3.220513761	3	4
28	24	1	5	1	5	4.242513761	4	4
29	24	1	3	7	5	3.220513761	3	4
30	24	1	3	7	1	3.068513761	3	4
31	24	1	5	1	5	4.242513761	4	4
32	24	1	2	7	1	2.965513761	3	3
33	24	1	2	7	1	2.965513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
34	24	1	2	7	1	2.965513761	3	3
35	24	1	2	4	5	3.525513761	4	4
36	24	1	3	7	5	3.220513761	3	4
37	24	1	2	7	1	2.965513761	3	3
38	24	1	3	7	5	3.220513761	3	4
39	24	1	3	7	5	3.220513761	3	4
40	24	1	2	6	4	3.215513761	3	4
41	24	2	3	7	1	3.222513761	3	4
42	24	2	5	2	1	4.108513761	4	4
43	24	1	3	7	5	3.220513761	3	4
44	24	1	3	7	1	3.068513761	3	4
45	23	1	3	7	5	3.234513761	3	4
46	23	1	3	7	5	3.234513761	3	4
47	23	1	2	4	5	3.539513761	4	2
48	23	1	3	7	1	3.082513761	3	4
49	23	1	3	7	5	3.234513761	3	4
50	23	1	3	7	1	3.082513761	3	4
51	23	2	5	2	1	4.122513761	4	4
52	23	1	2	7	5	3.131513761	3	4
53	23	1	3	7	5	3.234513761	3	4
54	23	1	2	7	1	2.979513761	3	2
55	23	1	2	6	4	3.229513761	3	4
56	23	1	2	4	5	3.539513761	4	2
57	23	1	2	6	2	3.153513761	3	2
58	23	1	3	7	5	3.234513761	3	4
59	23	1	3	7	1	3.082513761	3	4
60	23	1	2	7	2	3.017513761	3	3
61	23	1	3	7	5	3.234513761	3	4
62	23	1	2	6	4	3.229513761	3	4
63	23	2	5	2	1	4.122513761	4	4
64	23	1	2	6	4	3.229513761	3	4
65	23	1	3	7	1	3.082513761	3	4
66	23	2	5	2	1	4.122513761	4	4
67	23	1	3	7	5	3.234513761	3	4
68	23	1	3	7	1	3.082513761	3	4
69	23	1	3	7	5	3.234513761	3	4
70	23	2	5	2	1	4.122513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
71	23	1	3	7	1	3.082513761	3	4
72	23	1	3	7	1	3.082513761	3	4
73	23	2	5	2	1	4.122513761	4	4
74	23	1	3	7	5	3.234513761	3	4
75	23	1	2	7	1	2.979513761	3	2
76	25	2	3	7	5	3.360513761	3	2
77	25	2	5	2	1	4.094513761	4	4
78	25	1	2	7	1	2.951513761	3	4
79	25	1	2	4	5	3.511513761	4	4
80	25	2	5	2	1	4.094513761	4	4
81	25	2	3	7	1	3.208513761	3	2
82	25	1	3	7	1	3.054513761	3	2
83	25	1	3	7	1	3.054513761	3	2
84	25	1	5	1	1	4.076513761	4	4
85	25	1	3	7	1	3.054513761	3	2
86	25	1	2	4	5	3.511513761	4	4
87	25	1	3	7	5	3.206513761	3	4
88	25	1	2	7	1	2.951513761	3	4
89	25	2	5	2	1	4.094513761	4	4
90	25	2	3	7	1	3.208513761	3	2
91	25	1	3	7	1	3.054513761	3	2
92	25	1	3	7	1	3.054513761	3	2
93	25	1	3	7	1	3.054513761	3	2
94	25	2	5	2	1	4.094513761	4	4
95	25	1	3	7	5	3.206513761	3	4
96	25	1	3	7	5	3.206513761	3	4
97	25	1	2	7	1	2.951513761	3	4
98	25	1	2	4	5	3.511513761	4	4
99	25	2	5	2	1	4.094513761	4	4
100	25	2	3	7	1	3.208513761	3	2
101	25	1	3	7	1	3.054513761	3	2
102	25	1	2	7	1	2.951513761	3	4
103	25	1	3	7	1	3.054513761	3	2
104	25	1	3	7	1	3.054513761	3	2
105	25	1	5	1	1	4.076513761	4	4
106	25	1	3	7	1	3.054513761	3	2
107	25	1	2	4	5	3.511513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
108	25	2	5	2	1	4.094513761	4	4
109	25	1	3	7	5	3.206513761	3	4
110	25	1	5	1	5	4.228513761	4	2
111	25	1	3	7	5	3.206513761	3	4
112	25	1	3	7	1	3.054513761	3	2
113	25	1	2	7	1	2.951513761	3	4
114	25	1	2	7	1	2.951513761	3	4
115	25	1	2	7	1	2.951513761	3	4
116	25	1	2	4	5	3.511513761	4	4
117	25	1	2	7	1	2.951513761	3	4
118	25	1	3	7	1	3.054513761	3	2
119	25	1	3	7	1	3.054513761	3	2
120	25	1	2	7	5	3.103513761	3	4
121	25	2	5	2	1	4.094513761	4	4
122	25	1	3	7	5	3.206513761	3	4
123	25	1	5	1	5	4.228513761	4	2
124	25	1	3	7	5	3.206513761	3	4
125	25	1	3	7	1	3.054513761	3	2
126	25	1	2	7	1	2.951513761	3	4
127	25	1	2	7	1	2.951513761	3	4
128	25	1	2	7	1	2.951513761	3	4
129	25	1	2	4	5	3.511513761	4	4
130	25	1	2	7	1	2.951513761	3	4
131	25	2	3	7	1	3.208513761	3	2
132	25	1	3	7	1	3.054513761	3	2
133	25	1	5	1	1	4.076513761	4	4
134	25	2	5	2	1	4.094513761	4	4
135	25	1	3	7	5	3.206513761	3	4
136	25	1	3	7	5	3.206513761	3	4
137	25	1	2	4	5	3.511513761	4	4
138	25	1	3	7	1	3.054513761	3	2
139	25	1	3	7	1	3.054513761	3	2
140	25	1	3	7	1	3.054513761	3	2
141	25	1	3	7	5	3.206513761	3	4
142	25	1	2	7	1	2.951513761	3	4
143	25	1	2	4	5	3.511513761	4	4
144	25	2	5	2	1	4.094513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
145	25	2	3	7	1	3.208513761	3	2
146	25	1	3	7	1	3.054513761	3	2
147	25	1	2	7	1	2.951513761	3	4
148	25	1	3	7	1	3.054513761	3	2
149	25	1	3	7	1	3.054513761	3	2
150	25	1	3	7	1	3.054513761	3	2
151	25	1	2	4	5	3.511513761	4	4
152	25	2	5	2	1	4.094513761	4	4
153	25	1	3	7	5	3.206513761	3	4
154	25	1	5	1	5	4.228513761	4	2
155	25	1	3	7	5	3.206513761	3	4
156	25	1	3	7	1	3.054513761	3	2
157	25	1	2	7	1	2.951513761	3	4
158	25	1	2	7	1	2.951513761	3	4
159	25	1	2	7	1	2.951513761	3	4
160	25	1	2	4	5	3.511513761	4	4
161	25	1	3	7	5	3.206513761	3	4
162	25	1	2	7	1	2.951513761	3	4
163	25	1	2	7	1	2.951513761	3	4
164	25	1	2	6	4	3.201513761	3	4
165	25	2	3	7	5	3.360513761	3	2
166	25	2	3	6	5	3.496513761	3	2
167	25	1	2	7	1	2.951513761	3	4
168	24	1	3	7	1	3.068513761	3	4
169	24	1	3	7	1	3.068513761	3	4
170	24	2	3	7	1	3.222513761	3	4
171	24	1	3	7	1	3.068513761	3	4
172	24	2	5	2	1	4.108513761	4	4
173	24	1	3	7	5	3.220513761	3	4
174	25	2	5	2	1	4.094513761	4	4
175	25	1	3	7	1	3.054513761	3	2
176	25	1	2	4	5	3.511513761	4	4
177	25	1	3	7	5	3.206513761	3	4
178	25	1	3	7	5	3.206513761	3	4
179	25	1	2	4	5	3.511513761	4	4
180	25	2	5	2	1	4.094513761	4	4
181	25	1	3	7	1	3.054513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
182	25	1	3	7	5	3.206513761	3	4
183	25	1	3	7	5	3.206513761	3	4
184	25	1	2	7	1	2.951513761	3	4
185	25	1	2	4	5	3.511513761	4	4
186	25	2	3	7	1	3.208513761	3	2
187	25	1	3	7	1	3.054513761	3	2
188	25	1	3	7	1	3.054513761	3	2
189	25	1	3	7	1	3.054513761	3	2
190	25	1	3	7	5	3.206513761	3	4
191	25	1	3	7	5	3.206513761	3	4
192	25	1	2	7	1	2.951513761	3	4
193	25	1	2	4	5	3.511513761	4	4
194	25	1	3	7	5	3.206513761	3	4
195	25	1	3	7	5	3.206513761	3	4
196	25	1	2	4	5	3.511513761	4	4
197	25	1	3	7	5	3.206513761	3	4
198	25	2	3	7	1	3.208513761	3	2
199	25	1	3	7	1	3.054513761	3	2
200	25	1	3	7	1	3.054513761	3	2
201	25	1	3	7	1	3.054513761	3	2
202	24	2	5	2	1	4.108513761	4	4
203	24	2	3	7	1	3.222513761	3	4
204	24	1	3	7	1	3.068513761	3	4
205	24	1	2	7	1	2.965513761	3	3
206	24	1	3	7	1	3.068513761	3	4
207	24	1	5	1	1	4.090513761	4	4
208	24	1	3	7	1	3.068513761	3	4
209	24	1	2	4	5	3.525513761	4	4
210	24	1	3	7	1	3.068513761	3	4
211	24	2	5	2	1	4.108513761	4	4
212	24	1	3	7	1	3.068513761	3	4
213	24	1	3	7	5	3.220513761	3	4
214	24	1	3	7	5	3.220513761	3	4
215	24	1	2	7	1	2.965513761	3	3
216	9	2	5	2	1	4.318513761	4	3
217	9	1	2	6	4	3.425513761	3	4
218	9	2	3	7	1	3.432513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
219	9	1	3	7	1	3.278513761	3	2
220	9	1	5	1	1	4.300513761	4	4
221	9	1	3	7	1	3.278513761	3	2
222	9	1	5	1	1	4.300513761	4	4
223	9	2	5	2	1	4.318513761	4	3
224	9	1	3	7	5	3.430513761	3	2
225	9	1	3	7	5	3.430513761	3	2
226	24	1	3	7	1	3.068513761	3	4
227	24	1	3	7	5	3.220513761	3	4
228	24	2	5	2	1	4.108513761	4	4
229	24	2	3	7	5	3.374513761	3	2
230	24	2	5	2	1	4.108513761	4	4
231	24	1	3	7	1	3.068513761	3	4
232	24	2	3	7	5	3.374513761	3	2
233	24	2	5	2	1	4.108513761	4	4
234	24	2	3	7	1	3.222513761	3	4
235	24	1	3	7	1	3.068513761	3	4
236	24	1	2	7	1	2.965513761	3	3
237	24	1	3	7	1	3.068513761	3	4
238	24	1	3	7	1	3.068513761	3	4
239	24	1	5	1	1	4.090513761	4	5
240	24	1	3	7	1	3.068513761	3	4
241	24	1	2	4	5	3.525513761	4	4
242	24	2	5	2	1	4.108513761	4	4
243	24	1	3	7	5	3.220513761	3	4
244	24	1	5	1	5	4.242513761	4	4
245	24	1	3	7	5	3.220513761	3	4
246	24	1	3	7	1	3.068513761	3	4
247	24	1	5	1	5	4.242513761	4	4
248	24	1	2	7	1	2.965513761	3	3
249	24	1	2	7	1	2.965513761	3	3
250	24	1	2	7	1	2.965513761	3	3
251	24	1	2	4	5	3.525513761	4	4
252	24	1	3	7	5	3.220513761	3	4
253	24	1	2	7	1	2.965513761	3	3
254	24	2	5	2	1	4.108513761	4	4
255	24	1	3	7	5	3.220513761	3	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
256	24	1	5	1	5	4.242513761	4	4
257	24	1	3	7	5	3.220513761	3	4
258	24	1	3	7	1	3.068513761	3	4
259	24	1	5	1	5	4.242513761	4	4
260	24	1	2	7	1	2.965513761	3	3
261	24	1	2	7	1	2.965513761	3	3
262	24	1	2	4	5	3.525513761	4	4
263	24	1	2	7	1	2.965513761	3	3
264	23	1	2	4	5	3.539513761	4	2
265	23	1	2	6	4	3.229513761	3	4
266	5	2	5	2	1	4.374513761	4	4
267	5	2	5	2	1	4.374513761	4	4
268	9	2	5	2	1	4.318513761	4	3
269	9	1	3	7	1	3.278513761	3	2
270	9	1	5	1	1	4.300513761	4	4
271	9	1	3	7	1	3.278513761	3	2
272	5	2	5	2	1	4.374513761	4	4
273	5	2	5	2	1	4.374513761	4	4
274	5	2	5	2	1	4.374513761	4	4
275	5	1	3	7	1	3.334513761	3	4
276	5	1	3	7	5	3.486513761	3	3
277	5	2	5	2	1	4.374513761	4	4
278	5	1	3	7	1	3.334513761	3	4
279	5	1	3	7	5	3.486513761	3	3
280	33	1	2	7	5	2.991513761	3	2
281	33	1	3	7	1	2.942513761	3	3
282	33	1	3	7	5	3.094513761	3	3
283	33	1	3	7	1	2.942513761	3	3
284	33	1	3	7	1	2.942513761	3	3
285	33	1	2	7	5	2.991513761	3	2
286	33	1	2	7	5	2.991513761	3	2
287	33	1	3	7	1	2.942513761	3	3
288	33	1	3	7	5	3.094513761	3	3
289	33	1	3	7	1	2.942513761	3	3
290	33	1	3	7	1	2.942513761	3	3
291	31	1	2	7	1	2.867513761	3	4
292	31	1	3	7	1	2.970513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
293	31	1	2	7	5	3.019513761	3	3
294	31	1	2	7	3	2.943513761	3	3
295	31	1	2	6	4	3.117513761	3	4
296	31	1	3	7	1	2.970513761	3	3
297	31	1	2	7	1	2.867513761	3	4
298	31	1	3	7	1	2.970513761	3	3
299	31	1	2	7	5	3.019513761	3	3
300	31	1	3	7	4	3.084513761	3	4
301	31	1	3	7	4	3.084513761	3	4
302	31	1	3	7	1	2.970513761	3	3
303	31	1	2	4	1	3.275513761	3	3
304	31	1	2	6	4	3.117513761	3	4
305	33	1	3	7	1	2.942513761	3	3
306	33	1	3	7	5	3.094513761	3	3
307	33	1	3	7	5	3.094513761	3	3
308	33	1	3	7	1	2.942513761	3	3
309	33	1	2	7	5	2.991513761	3	2
310	33	1	2	7	5	2.991513761	3	2
311	33	1	3	7	5	3.094513761	3	3
312	33	1	2	7	5	2.991513761	3	2
313	34	2	5	2	1	3.968513761	4	3
314	34	1	2	7	1	2.825513761	3	3
315	34	1	2	7	1	2.825513761	3	3
316	34	1	3	7	1	2.928513761	3	3
317	34	1	3	7	1	2.928513761	3	3
318	34	1	2	7	5	2.977513761	3	3
319	34	1	2	7	5	2.977513761	3	3
320	32	1	3	7	1	2.956513761	3	2
321	32	1	3	7	4	3.070513761	3	3
322	32	2	3	7	4	3.224513761	3	3
323	32	2	1	6	4	3.154513761	3	3
324	32	2	3	7	1	3.110513761	3	3
325	32	1	2	7	5	3.005513761	3	3
326	32	1	2	7	5	3.005513761	3	3
327	32	1	2	7	5	3.005513761	3	3
328	32	1	2	6	4	3.103513761	3	4
329	32	1	3	7	5	3.108513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
330	32	2	3	7	1	3.110513761	3	3
331	32	1	2	7	1	2.853513761	3	3
332	32	1	3	7	5	3.108513761	3	3
333	32	1	3	7	5	3.108513761	3	3
334	32	2	3	7	5	3.262513761	3	3
335	32	1	2	7	1	2.853513761	3	3
336	32	1	2	7	4	2.967513761	3	3
337	32	1	2	7	1	2.853513761	3	3
338	32	1	2	7	1	2.853513761	3	3
339	32	1	2	7	1	2.853513761	3	3
340	32	2	3	7	1	3.110513761	3	3
341	32	1	3	7	1	2.956513761	3	2
342	34	1	2	7	1	2.825513761	3	3
343	34	1	3	7	1	2.928513761	3	3
344	34	1	3	7	4	3.042513761	3	3
345	34	1	3	7	1	2.928513761	3	3
346	34	1	2	7	5	2.977513761	3	3
347	34	1	2	7	1	2.825513761	3	3
348	34	1	3	7	1	2.928513761	3	3
349	34	1	3	7	5	3.080513761	3	3
350	34	1	3	1	5	3.896513761	4	3
351	34	1	3	7	1	2.928513761	3	3
352	34	1	3	1	5	3.896513761	4	3
353	34	1	2	7	5	2.977513761	3	3
354	34	1	3	4	1	3.336513761	3	3
355	34	1	3	7	1	2.928513761	3	3
356	34	1	3	7	1	2.928513761	3	3
357	34	1	3	7	1	2.928513761	3	3
358	34	1	3	7	1	2.928513761	3	3
359	32	1	3	7	2	2.994513761	3	4
360	32	1	3	7	5	3.108513761	3	3
361	32	1	3	7	5	3.108513761	3	3
362	32	1	2	6	4	3.103513761	3	4
363	32	1	3	7	5	3.108513761	3	3
364	32	1	3	7	5	3.108513761	3	3
365	32	1	3	7	5	3.108513761	3	3
366	32	1	3	7	1	2.956513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
367	32	1	3	7	5	3.108513761	3	3
368	34	1	3	7	1	2.928513761	3	3
369	34	1	2	7	1	2.825513761	3	3
370	34	1	2	7	1	2.825513761	3	3
371	34	1	3	7	5	3.080513761	3	3
372	34	1	2	7	1	2.825513761	3	3
373	34	1	3	7	5	3.080513761	3	3
374	34	1	3	7	5	3.080513761	3	3
375	34	1	3	7	5	3.080513761	3	3
376	34	1	3	7	1	2.928513761	3	3
377	34	1	2	7	5	2.977513761	3	3
378	34	1	2	7	5	2.977513761	3	3
379	34	1	3	4	1	3.336513761	3	3
380	34	1	2	6	4	3.075513761	3	2
381	31	1	2	7	1	2.867513761	3	4
382	31	1	3	7	4	3.084513761	3	4
383	31	1	3	7	4	3.084513761	3	4
384	31	1	3	7	1	2.970513761	3	3
385	31	1	2	7	5	3.019513761	3	3
386	31	1	2	7	4	2.981513761	3	3
387	31	1	3	7	1	2.970513761	3	3
388	31	1	3	7	1	2.970513761	3	3
389	31	1	3	7	1	2.970513761	3	3
390	31	1	3	7	4	3.084513761	3	4
391	31	1	3	7	4	3.084513761	3	4
392	32	1	3	7	1	2.956513761	3	2
393	32	1	2	7	1	2.853513761	3	3
394	32	1	2	4	1	3.261513761	3	2
395	32	1	2	6	4	3.103513761	3	4
396	33	2	5	2	1	3.982513761	4	5
397	33	1	5	1	1	3.964513761	4	5
398	33	1	3	7	1	2.942513761	3	3
399	33	1	3	7	5	3.094513761	3	3
400	33	1	3	7	5	3.094513761	3	3
401	33	1	3	7	5	3.094513761	3	3
402	33	1	3	4	1	3.350513761	3	4
403	33	1	2	7	5	2.991513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
404	33	1	2	7	1	2.839513761	3	4
405	33	1	2	7	5	2.991513761	3	2
406	33	2	3	7	5	3.248513761	3	3
407	33	1	3	7	1	2.942513761	3	3
408	33	1	3	7	1	2.942513761	3	3
409	33	1	3	7	1	2.942513761	3	3
410	33	1	2	4	1	3.247513761	3	4
411	33	1	3	4	1	3.350513761	3	4
412	33	1	2	4	5	3.399513761	3	4
413	33	1	2	4	5	3.399513761	3	4
414	33	1	2	7	5	2.991513761	3	2
415	33	1	3	7	5	3.094513761	3	3
416	24	2	5	2	1	4.108513761	4	4
417	24	1	2	7	1	2.965513761	3	3
418	24	1	3	7	1	3.068513761	3	4
419	24	1	2	7	4	3.079513761	3	4
420	24	1	5	1	1	4.090513761	4	2
421	24	1	3	7	1	3.068513761	3	4
422	24	1	2	7	5	3.117513761	3	2
423	24	1	5	1	1	4.090513761	4	1
424	24	1	3	7	1	3.068513761	3	4
425	24	1	3	7	1	3.068513761	3	4
426	24	2	5	2	1	4.108513761	4	4
427	24	2	5	2	1	4.108513761	4	4
428	24	1	2	7	1	2.965513761	3	3
429	24	1	3	7	1	3.068513761	3	4
430	24	2	5	2	1	4.108513761	4	4
431	24	1	2	7	2	3.003513761	3	2
432	24	1	3	7	1	3.068513761	3	4
433	24	1	2	4	1	3.373513761	3	4
434	24	1	2	7	1	2.965513761	3	3
435	24	1	3	7	1	3.068513761	3	4
436	24	1	5	1	1	4.090513761	4	2
437	26	1	2	7	5	3.089513761	3	2
438	26	1	3	7	1	3.040513761	3	2
439	26	1	3	7	1	3.040513761	3	2
440	26	2	3	5	1	3.466513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
441	26	2	2	4	1	3.499513761	3	2
442	26	1	3	7	5	3.192513761	3	2
443	26	1	3	7	5	3.192513761	3	2
444	26	1	3	7	1	3.040513761	3	2
445	26	1	3	7	1	3.040513761	3	2
446	26	1	2	7	5	3.089513761	3	2
447	26	2	3	5	1	3.466513761	3	2
448	18	1	3	7	1	3.152513761	3	2
449	18	2	3	7	1	3.306513761	3	2
450	18	2	3	7	1	3.306513761	3	2
451	18	1	3	7	1	3.152513761	3	2
452	18	1	3	7	1	3.152513761	3	2
453	18	1	3	7	1	3.152513761	3	2
454	18	1	3	7	5	3.304513761	3	1
455	18	1	3	7	1	3.152513761	3	2
456	18	1	3	7	1	3.152513761	3	2
457	12	1	3	7	5	3.388513761	3	4
458	4	2	5	2	1	4.388513761	4	5
459	23	1	3	6	1	3.218513761	3	4
460	23	1	2	7	1	2.979513761	3	2
461	23	1	5	2	1	3.968513761	4	4
462	23	1	2	7	1	2.979513761	3	2
463	24	1	2	7	1	2.965513761	3	3
464	24	1	2	6	4	3.215513761	3	4
465	2	1	2	7	1	3.273513761	3	4
466	2	1	3	7	1	3.376513761	3	4
467	18	1	2	4	1	3.457513761	3	4
468	11	1	2	7	5	3.299513761	3	3
469	12	1	2	7	1	3.133513761	3	2
470	21	1	2	6	4	3.257513761	3	2
471	21	1	2	7	5	3.159513761	3	2
472	17	1	2	3	3	3.683513761	4	1
473	13	2	2	4	1	3.681513761	4	4
474	22	1	2	7	1	2.993513761	3	4
475	8	1	2	6	5	3.477513761	3	4
476	25	1	2	6	4	3.201513761	3	4
477	15	1	5	1	1	4.216513761	4	1

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
478	16	2	3	5	1	3.606513761	4	2
479	7	2	5	6	4	3.916513761	4	4
480	7	1	5	6	4	3.762513761	4	4
481	9	1	2	6	4	3.425513761	3	4
482	14	1	2	4	1	3.513513761	4	5
483	26	2	3	5	1	3.466513761	3	2
484	10	1	2	6	4	3.411513761	3	4
485	19	1	2	6	4	3.285513761	3	5
486	19	1	2	6	4	3.285513761	3	5
487	3	1	2	7	5	3.411513761	3	4
488	3	1	2	7	5	3.411513761	3	4
489	1	1	2	7	1	3.287513761	3	4
490	1	1	2	7	5	3.439513761	3	4
491	1	1	2	7	5	3.439513761	3	4
492	1	1	2	7	1	3.287513761	3	4
493	28	1	3	6	4	3.262513761	3	4
494	6	1	3	6	4	3.570513761	4	1
495	20	1	2	4	5	3.581513761	4	4
496	5	1	3	7	1	3.334513761	3	4
497	5	1	3	7	1	3.334513761	3	4
498	5	1	2	7	1	3.231513761	3	4
499	5	1	2	7	5	3.383513761	3	5
500	5	1	3	7	1	3.334513761	3	4
501	5	1	3	4	1	3.742513761	4	1
502	5	1	2	6	4	3.481513761	3	5
503	5	1	3	7	1	3.334513761	3	4
504	5	1	2	6	1	3.367513761	3	4
505	5	1	2	7	5	3.383513761	3	5
506	3	1	2	7	5	3.411513761	3	4
507	3	2	2	7	5	3.565513761	4	4
508	3	1	2	7	5	3.411513761	3	4
509	3	2	2	7	5	3.565513761	4	4
510	23	1	2	7	2	3.017513761	3	3
511	5	1	3	7	1	3.334513761	3	4
512	27	2	5	2	1	4.066513761	4	5
513	27	1	2	7	1	2.923513761	3	2
514	24	1	2	7	1	2.965513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
515	24	1	3	7	1	3.068513761	3	4
516	24	1	2	7	1	2.965513761	3	3
517	24	1	2	7	1	2.965513761	3	3
518	24	1	2	6	4	3.215513761	3	4
519	24	1	3	7	1	3.068513761	3	4
520	24	1	3	7	1	3.068513761	3	4
521	25	1	2	7	1	2.951513761	3	4
522	25	1	5	1	5	4.228513761	4	2
523	25	1	3	7	5	3.206513761	3	4
524	25	1	2	6	4	3.201513761	3	4
525	25	1	2	6	4	3.201513761	3	4
526	25	1	2	6	4	3.201513761	3	4
527	25	1	2	6	4	3.201513761	3	4
528	25	1	3	7	1	3.054513761	3	2
529	25	1	3	7	1	3.054513761	3	2
530	25	1	3	4	1	3.462513761	3	2
531	23	1	3	6	4	3.332513761	3	4
532	23	1	2	6	4	3.229513761	3	4
533	23	1	3	6	4	3.332513761	3	4
534	23	1	3	7	1	3.082513761	3	4
535	23	1	3	7	1	3.082513761	3	4
536	23	2	5	2	1	4.122513761	4	4
537	23	1	2	6	4	3.229513761	3	4
538	23	1	3	7	1	3.082513761	3	4
539	23	1	3	7	5	3.234513761	3	4
540	23	2	5	2	1	4.122513761	4	4
541	23	1	3	7	5	3.234513761	3	4
542	23	2	5	2	1	4.122513761	4	4
543	23	1	2	6	4	3.229513761	3	4
544	23	1	3	7	4	3.196513761	3	4
545	23	1	3	6	4	3.332513761	3	2
546	23	1	3	7	1	3.082513761	3	4
547	23	1	2	5	3	3.327513761	3	4
548	5	1	2	7	5	3.383513761	3	5
549	14	1	3	7	5	3.360513761	3	5
550	14	1	3	7	5	3.360513761	3	5
551	5	2	5	2	1	4.374513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
552	5	1	2	6	4	3.481513761	3	5
553	5	2	3	7	1	3.488513761	3	4
554	5	1	3	7	1	3.334513761	3	4
555	23	1	3	7	5	3.234513761	3	4
556	23	2	5	2	1	4.122513761	4	4
557	23	1	2	6	4	3.229513761	3	4
558	23	1	3	7	5	3.234513761	3	4
559	23	2	3	7	1	3.236513761	3	4
560	23	1	3	7	1	3.082513761	3	4
561	23	1	3	7	5	3.234513761	3	4
562	23	1	3	7	1	3.082513761	3	4
563	23	1	3	7	5	3.234513761	3	4
564	23	2	5	2	1	4.122513761	4	4
565	24	1	3	7	1	3.068513761	3	4
566	24	1	3	7	5	3.220513761	3	4
567	24	2	5	2	1	4.108513761	4	4
568	24	2	3	7	1	3.222513761	3	4
569	24	1	3	7	1	3.068513761	3	4
570	24	1	2	7	1	2.965513761	3	3
571	24	1	3	7	1	3.068513761	3	4
572	24	1	3	7	1	3.068513761	3	4
573	24	1	5	1	1	4.090513761	4	4
574	24	1	3	7	1	3.068513761	3	4
575	24	1	2	4	5	3.525513761	4	4
576	24	2	5	2	1	4.108513761	4	4
577	24	1	3	7	5	3.220513761	3	4
578	24	1	5	1	5	4.242513761	4	4
579	24	1	3	7	5	3.220513761	3	4
580	24	1	3	7	1	3.068513761	3	4
581	24	1	5	1	5	4.242513761	4	4
582	24	1	2	7	1	2.965513761	3	3
583	24	1	2	7	1	2.965513761	3	3
584	24	1	2	7	1	2.965513761	3	3
585	24	1	2	4	5	3.525513761	4	4
586	24	1	3	7	5	3.220513761	3	4
587	24	1	2	7	1	2.965513761	3	3
588	24	1	3	7	5	3.220513761	3	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
589	24	1	3	7	5	3.220513761	3	4
590	24	1	2	6	4	3.215513761	3	4
591	24	2	3	7	1	3.222513761	3	4
592	24	2	5	2	1	4.108513761	4	4
593	24	1	3	7	5	3.220513761	3	4
594	24	1	3	7	1	3.068513761	3	4
595	23	1	3	7	5	3.234513761	3	4
596	23	1	3	7	5	3.234513761	3	4
597	23	1	2	4	5	3.539513761	4	2
598	23	1	3	7	1	3.082513761	3	4
599	23	1	3	7	5	3.234513761	3	4
600	23	1	3	7	1	3.082513761	3	4
601	23	2	5	2	1	4.122513761	4	4
602	23	1	2	7	5	3.131513761	3	4
603	23	1	3	7	5	3.234513761	3	4
604	23	1	2	7	1	2.979513761	3	2
605	23	1	2	6	4	3.229513761	3	4
606	23	1	2	4	5	3.539513761	4	2
607	23	1	2	6	2	3.153513761	3	2
608	23	1	3	7	5	3.234513761	3	4
609	23	1	3	7	1	3.082513761	3	4
610	23	1	2	7	2	3.017513761	3	3
611	23	1	3	7	5	3.234513761	3	4
612	23	1	2	6	4	3.229513761	3	4
613	23	2	5	2	1	4.122513761	4	4
614	23	1	2	6	4	3.229513761	3	4
615	23	1	3	7	1	3.082513761	3	4
616	23	2	5	2	1	4.122513761	4	4
617	23	1	3	7	5	3.234513761	3	4
618	23	1	3	7	1	3.082513761	3	4
619	23	1	3	7	5	3.234513761	3	4
620	23	2	5	2	1	4.122513761	4	4
621	23	1	3	7	1	3.082513761	3	4
622	23	1	3	7	1	3.082513761	3	4
623	23	2	5	2	1	4.122513761	4	4
624	23	1	3	7	5	3.234513761	3	4
625	23	1	2	7	1	2.979513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
626	25	2	3	7	5	3.360513761	3	2
627	25	2	5	2	1	4.094513761	4	4
628	25	1	2	7	1	2.951513761	3	4
629	25	1	2	4	5	3.511513761	4	4
630	25	2	5	2	1	4.094513761	4	4
631	25	2	3	7	1	3.208513761	3	2
632	25	1	3	7	1	3.054513761	3	2
633	25	1	3	7	1	3.054513761	3	2
634	25	1	5	1	1	4.076513761	4	4
635	25	1	3	7	1	3.054513761	3	2
636	25	1	2	4	5	3.511513761	4	4
637	25	1	3	7	5	3.206513761	3	4
638	25	1	2	7	1	2.951513761	3	4
639	25	2	5	2	1	4.094513761	4	4
640	25	2	3	7	1	3.208513761	3	2
641	25	1	3	7	1	3.054513761	3	2
642	25	1	3	7	1	3.054513761	3	2
643	25	1	3	7	1	3.054513761	3	2
644	25	2	5	2	1	4.094513761	4	4
645	25	1	3	7	5	3.206513761	3	4
646	25	1	3	7	5	3.206513761	3	4
647	25	1	2	7	1	2.951513761	3	4
648	25	1	2	4	5	3.511513761	4	4
649	25	2	5	2	1	4.094513761	4	4
650	25	2	3	7	1	3.208513761	3	2
651	25	1	3	7	1	3.054513761	3	2
652	25	1	2	7	1	2.951513761	3	4
653	25	1	3	7	1	3.054513761	3	2
654	25	1	3	7	1	3.054513761	3	2
655	25	1	5	1	1	4.076513761	4	4
656	25	1	3	7	1	3.054513761	3	2
657	25	1	2	4	5	3.511513761	4	4
658	25	2	5	2	1	4.094513761	4	4
659	25	1	3	7	5	3.206513761	3	4
660	25	1	5	1	5	4.228513761	4	2
661	25	1	3	7	5	3.206513761	3	4
662	25	1	3	7	1	3.054513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
663	25	1	2	7	1	2.951513761	3	4
664	25	1	2	7	1	2.951513761	3	4
665	25	1	2	7	1	2.951513761	3	4
666	25	1	2	4	5	3.511513761	4	4
667	25	1	2	7	1	2.951513761	3	4
668	25	1	3	7	1	3.054513761	3	2
669	25	1	3	7	1	3.054513761	3	2
670	25	1	2	7	5	3.103513761	3	4
671	25	2	5	2	1	4.094513761	4	4
672	25	1	3	7	5	3.206513761	3	4
673	25	1	5	1	5	4.228513761	4	2
674	25	1	3	7	5	3.206513761	3	4
675	25	1	3	7	1	3.054513761	3	2
676	25	1	2	7	1	2.951513761	3	4
677	25	1	2	7	1	2.951513761	3	4
678	25	1	2	7	1	2.951513761	3	4
679	25	1	2	4	5	3.511513761	4	4
680	25	1	2	7	1	2.951513761	3	4
681	25	2	3	7	1	3.208513761	3	2
682	25	1	3	7	1	3.054513761	3	2
683	25	1	5	1	1	4.076513761	4	4
684	25	2	5	2	1	4.094513761	4	4
685	25	1	3	7	5	3.206513761	3	4
686	25	1	3	7	5	3.206513761	3	4
687	25	1	2	4	5	3.511513761	4	4
688	25	1	3	7	1	3.054513761	3	2
689	25	1	3	7	1	3.054513761	3	2
690	25	1	3	7	1	3.054513761	3	2
691	25	1	3	7	5	3.206513761	3	4
692	25	1	2	7	1	2.951513761	3	4
693	25	1	2	4	5	3.511513761	4	4
694	25	2	5	2	1	4.094513761	4	4
695	25	2	3	7	1	3.208513761	3	2
696	25	1	3	7	1	3.054513761	3	2
697	25	1	2	7	1	2.951513761	3	4
698	25	1	3	7	1	3.054513761	3	2
699	25	1	3	7	1	3.054513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
700	25	1	3	7	1	3.054513761	3	2
701	25	1	2	4	5	3.511513761	4	4
702	25	2	5	2	1	4.094513761	4	4
703	25	1	3	7	5	3.206513761	3	4
704	25	1	5	1	5	4.228513761	4	2
705	25	1	3	7	5	3.206513761	3	4
706	25	1	3	7	1	3.054513761	3	2
707	25	1	2	7	1	2.951513761	3	4
708	25	1	2	7	1	2.951513761	3	4
709	25	1	2	7	1	2.951513761	3	4
710	25	1	2	4	5	3.511513761	4	4
711	25	1	3	7	5	3.206513761	3	4
712	25	1	2	7	1	2.951513761	3	4
713	25	1	2	7	1	2.951513761	3	4
714	25	1	2	6	4	3.201513761	3	4
715	25	2	3	7	5	3.360513761	3	2
716	25	2	3	6	5	3.496513761	3	2
717	25	1	2	7	1	2.951513761	3	4
718	24	1	3	7	1	3.068513761	3	4
719	24	1	3	7	1	3.068513761	3	4
720	24	2	3	7	1	3.222513761	3	4
721	24	1	3	7	1	3.068513761	3	4
722	24	2	5	2	1	4.108513761	4	4
723	24	1	3	7	5	3.220513761	3	4
724	25	2	5	2	1	4.094513761	4	4
725	25	1	3	7	1	3.054513761	3	2
726	25	1	2	4	5	3.511513761	4	4
727	25	1	3	7	5	3.206513761	3	4
728	25	1	3	7	5	3.206513761	3	4
729	25	1	2	4	5	3.511513761	4	4
730	25	2	5	2	1	4.094513761	4	4
731	25	1	3	7	1	3.054513761	3	2
732	25	1	3	7	5	3.206513761	3	4
733	25	1	3	7	5	3.206513761	3	4
734	25	1	2	7	1	2.951513761	3	4
735	25	1	2	4	5	3.511513761	4	4
736	25	2	3	7	1	3.208513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
737	25	1	3	7	1	3.054513761	3	2
738	25	1	3	7	1	3.054513761	3	2
739	25	1	3	7	1	3.054513761	3	2
740	25	1	3	7	5	3.206513761	3	4
741	25	1	3	7	5	3.206513761	3	4
742	25	1	2	7	1	2.951513761	3	4
743	25	1	2	4	5	3.511513761	4	4
744	25	1	3	7	5	3.206513761	3	4
745	25	1	3	7	5	3.206513761	3	4
746	25	1	2	4	5	3.511513761	4	4
747	25	1	3	7	5	3.206513761	3	4
748	25	2	3	7	1	3.208513761	3	2
749	25	1	3	7	1	3.054513761	3	2
750	25	1	3	7	1	3.054513761	3	2
751	25	1	3	7	1	3.054513761	3	2
752	24	2	5	2	1	4.108513761	4	4
753	24	2	3	7	1	3.222513761	3	4
754	24	1	3	7	1	3.068513761	3	4
755	24	1	2	7	1	2.965513761	3	3
756	24	1	3	7	1	3.068513761	3	4
757	24	1	5	1	1	4.090513761	4	4
758	24	1	3	7	1	3.068513761	3	4
759	24	1	2	4	5	3.525513761	4	4
760	24	1	3	7	1	3.068513761	3	4
761	24	2	5	2	1	4.108513761	4	4
762	24	1	3	7	1	3.068513761	3	4
763	24	1	3	7	5	3.220513761	3	4
764	24	1	3	7	5	3.220513761	3	4
765	24	1	2	7	1	2.965513761	3	3
766	9	2	5	2	1	4.318513761	4	3
767	9	1	2	6	4	3.425513761	3	4
768	9	2	3	7	1	3.432513761	3	2
769	9	1	3	7	1	3.278513761	3	2
770	9	1	5	1	1	4.300513761	4	4
771	9	1	3	7	1	3.278513761	3	2
772	9	1	5	1	1	4.300513761	4	4
773	9	2	5	2	1	4.318513761	4	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
774	9	1	3	7	5	3.430513761	3	2
775	9	1	3	7	5	3.430513761	3	2
776	24	1	3	7	1	3.068513761	3	4
777	24	1	3	7	5	3.220513761	3	4
778	24	2	5	2	1	4.108513761	4	4
779	24	2	3	7	5	3.374513761	3	2
780	24	2	5	2	1	4.108513761	4	4
781	24	1	3	7	1	3.068513761	3	4
782	24	2	3	7	5	3.374513761	3	2
783	24	2	5	2	1	4.108513761	4	4
784	24	2	3	7	1	3.222513761	3	4
785	24	1	3	7	1	3.068513761	3	4
786	24	1	2	7	1	2.965513761	3	3
787	24	1	3	7	1	3.068513761	3	4
788	24	1	3	7	1	3.068513761	3	4
789	24	1	5	1	1	4.090513761	4	5
790	24	1	3	7	1	3.068513761	3	4
791	24	1	2	4	5	3.525513761	4	4
792	24	2	5	2	1	4.108513761	4	4
793	24	1	3	7	5	3.220513761	3	4
794	24	1	5	1	5	4.242513761	4	4
795	24	1	3	7	5	3.220513761	3	4
796	24	1	3	7	1	3.068513761	3	4
797	24	1	5	1	5	4.242513761	4	4
798	24	1	2	7	1	2.965513761	3	3
799	24	1	2	7	1	2.965513761	3	3
800	24	1	2	7	1	2.965513761	3	3
801	24	1	2	4	5	3.525513761	4	4
802	24	1	3	7	5	3.220513761	3	4
803	24	1	2	7	1	2.965513761	3	3
804	24	2	5	2	1	4.108513761	4	4
805	24	1	3	7	5	3.220513761	3	4
806	24	1	5	1	5	4.242513761	4	4
807	24	1	3	7	5	3.220513761	3	4
808	24	1	3	7	1	3.068513761	3	4
809	24	1	5	1	5	4.242513761	4	4
810	24	1	2	7	1	2.965513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
811	24	1	2	7	1	2.965513761	3	3
812	24	1	2	4	5	3.525513761	4	4
813	24	1	2	7	1	2.965513761	3	3
814	23	1	2	4	5	3.539513761	4	2
815	23	1	2	6	4	3.229513761	3	4
816	5	2	5	2	1	4.374513761	4	4
817	5	2	5	2	1	4.374513761	4	4
818	5	2	5	2	1	4.374513761	4	4
819	5	1	3	7	1	3.334513761	3	4
820	5	1	5	1	1	4.356513761	4	1
821	5	1	3	7	1	3.334513761	3	4
822	5	2	5	2	1	4.374513761	4	4
823	5	2	5	2	1	4.374513761	4	4
824	9	2	5	2	1	4.318513761	4	3
825	9	1	3	7	1	3.278513761	3	2
826	9	1	5	1	1	4.300513761	4	4
827	9	1	3	7	1	3.278513761	3	2
828	5	2	5	2	1	4.374513761	4	4
829	5	2	5	2	1	4.374513761	4	4
830	5	2	5	2	1	4.374513761	4	4
831	5	2	5	2	1	4.374513761	4	4
832	5	1	3	7	1	3.334513761	3	4
833	5	1	3	7	5	3.486513761	3	3
834	5	2	5	2	1	4.374513761	4	4
835	5	1	3	7	1	3.334513761	3	4
836	5	1	3	7	5	3.486513761	3	3
837	5	1	3	7	1	3.334513761	3	4
838	5	2	5	2	1	4.374513761	4	4
839	5	1	3	7	1	3.334513761	3	4
840	5	1	3	7	5	3.486513761	3	3
841	5	2	5	2	1	4.374513761	4	4
842	5	1	3	7	1	3.334513761	3	4
843	5	1	3	7	5	3.486513761	3	3
844	29	1	3	7	1	2.998513761	3	3
845	29	1	3	7	1	2.998513761	3	3
846	29	1	2	7	5	3.047513761	3	3
847	29	1	3	7	1	2.998513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
848	29	1	2	3	1	3.439513761	3	4
849	29	1	2	7	5	3.047513761	3	3
850	29	1	2	7	5	3.047513761	3	3
851	29	2	1	7	1	2.946513761	3	4
852	29	1	5	1	1	4.020513761	4	3
853	29	1	3	7	1	2.998513761	3	3
854	29	1	3	7	5	3.150513761	3	2
855	29	1	2	7	5	3.047513761	3	3
856	29	1	3	7	1	2.998513761	3	3
857	29	1	3	7	5	3.150513761	3	2
858	29	1	3	7	1	2.998513761	3	3
859	29	1	5	1	1	4.020513761	4	3
860	29	1	3	7	1	2.998513761	3	3
861	29	1	3	7	1	2.998513761	3	3
862	29	1	3	7	1	2.998513761	3	3
863	29	1	2	7	5	3.047513761	3	3
864	32	1	2	7	5	3.005513761	3	3
865	32	1	2	6	4	3.103513761	3	4
866	32	1	3	7	1	2.956513761	3	2
867	32	1	3	7	5	3.108513761	3	3
868	32	1	3	7	5	3.108513761	3	3
869	33	1	2	7	5	2.991513761	3	2
870	33	1	3	7	1	2.942513761	3	3
871	33	1	3	7	5	3.094513761	3	3
872	33	1	3	7	1	2.942513761	3	3
873	33	1	3	7	1	2.942513761	3	3
874	33	1	2	7	5	2.991513761	3	2
875	33	1	2	7	5	2.991513761	3	2
876	33	1	3	7	1	2.942513761	3	3
877	33	1	3	7	5	3.094513761	3	3
878	33	1	3	7	1	2.942513761	3	3
879	33	1	3	7	1	2.942513761	3	3
880	36	1	5	1	1	3.922513761	4	4
881	36	1	2	7	1	2.797513761	3	3
882	36	1	2	7	1	2.797513761	3	3
883	36	1	2	6	5	3.085513761	3	2
884	36	1	5	1	1	3.922513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
885	36	1	2	7	1	2.797513761	3	3
886	36	1	2	7	1	2.797513761	3	3
887	36	1	2	6	4	3.047513761	3	3
888	36	1	2	7	1	2.797513761	3	3
889	36	1	3	7	5	3.052513761	3	3
890	36	1	2	7	2	2.835513761	3	4
891	36	1	2	7	5	2.949513761	3	3
892	36	1	2	6	4	3.047513761	3	3
893	36	1	2	6	4	3.047513761	3	3
894	36	1	3	7	1	2.900513761	3	3
895	36	1	2	7	5	2.949513761	3	3
896	36	1	2	6	4	3.047513761	3	3
897	36	1	2	6	4	3.047513761	3	3
898	36	1	2	6	5	3.085513761	3	2
899	36	1	3	7	1	2.900513761	3	3
900	36	1	3	7	1	2.900513761	3	3
901	36	1	3	7	1	2.900513761	3	3
902	36	1	3	7	2	2.938513761	3	3
903	36	1	2	7	1	2.797513761	3	3
904	36	1	2	6	4	3.047513761	3	3
905	36	1	2	6	4	3.047513761	3	3
906	36	1	3	7	1	2.900513761	3	3
907	36	1	3	7	1	2.900513761	3	3
908	36	1	2	4	1	3.205513761	3	4
909	36	1	2	4	1	3.205513761	3	4
910	36	1	2	6	5	3.085513761	3	2
911	36	1	2	6	4	3.047513761	3	3
912	36	1	3	7	1	2.900513761	3	3
913	36	1	2	4	1	3.205513761	3	4
914	36	1	2	4	1	3.205513761	3	4
915	36	1	2	7	1	2.797513761	3	3
916	36	1	5	1	1	3.922513761	4	4
917	36	1	2	7	2	2.835513761	3	4
918	36	1	3	7	5	3.052513761	3	3
919	36	1	2	7	5	2.949513761	3	3
920	36	1	2	7	2	2.835513761	3	4
921	36	1	3	7	5	3.052513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
922	36	1	3	7	5	3.052513761	3	3
923	36	1	3	7	5	3.052513761	3	3
924	36	1	3	7	5	3.052513761	3	3
925	36	1	3	7	1	2.900513761	3	3
926	36	1	2	7	2	2.835513761	3	4
927	36	1	2	4	1	3.205513761	3	4
928	36	1	2	4	5	3.357513761	3	4
929	36	1	3	7	1	2.900513761	3	3
930	36	2	3	7	1	3.054513761	3	3
931	36	2	3	7	1	3.054513761	3	3
932	36	2	3	7	1	3.054513761	3	3
933	36	1	2	7	5	2.949513761	3	3
934	36	2	3	7	1	3.054513761	3	3
935	36	1	3	7	1	2.900513761	3	3
936	30	1	2	6	5	3.169513761	3	3
937	30	1	3	7	1	2.984513761	3	2
938	30	1	2	7	1	2.881513761	3	3
939	30	1	3	7	1	2.984513761	3	2
940	30	1	3	7	5	3.136513761	3	2
941	30	1	3	7	1	2.984513761	3	2
942	30	1	3	7	1	2.984513761	3	2
943	30	1	2	7	2	2.919513761	3	3
944	30	2	3	7	1	3.138513761	3	3
945	30	1	3	7	1	2.984513761	3	2
946	30	1	3	7	1	2.984513761	3	2
947	30	1	2	7	5	3.033513761	3	2
948	30	2	3	7	1	3.138513761	3	3
949	30	1	2	7	1	2.881513761	3	3
950	30	2	3	7	1	3.138513761	3	3
951	30	1	2	6	4	3.131513761	3	4
952	30	1	3	7	1	2.984513761	3	2
953	30	1	2	6	4	3.131513761	3	4
954	30	2	5	2	1	4.024513761	4	2
955	30	1	3	7	1	2.984513761	3	2
956	30	1	2	7	1	2.881513761	3	3
957	30	1	3	7	5	3.136513761	3	2
958	30	1	2	7	1	2.881513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
959	30	1	2	7	5	3.033513761	3	2
960	30	1	3	7	1	2.984513761	3	2
961	30	1	2	7	2	2.919513761	3	3
962	31	1	2	7	1	2.867513761	3	4
963	31	1	3	7	1	2.970513761	3	3
964	31	1	2	7	5	3.019513761	3	3
965	31	1	2	7	3	2.943513761	3	3
966	31	1	2	6	4	3.117513761	3	4
967	31	1	3	7	1	2.970513761	3	3
968	31	1	2	7	1	2.867513761	3	4
969	31	1	3	7	1	2.970513761	3	3
970	31	1	2	7	5	3.019513761	3	3
971	31	1	3	7	4	3.084513761	3	4
972	31	1	3	7	4	3.084513761	3	4
973	31	1	3	7	1	2.970513761	3	3
974	31	1	2	4	1	3.275513761	3	3
975	31	1	2	6	4	3.117513761	3	4
976	33	2	5	2	1	3.982513761	4	5
977	33	1	3	7	1	2.942513761	3	3
978	33	1	3	7	5	3.094513761	3	3
979	33	1	3	7	5	3.094513761	3	3
980	33	1	3	7	1	2.942513761	3	3
981	33	1	2	7	5	2.991513761	3	2
982	33	1	2	7	5	2.991513761	3	2
983	33	1	3	7	5	3.094513761	3	3
984	33	1	2	7	5	2.991513761	3	2
985	9	1	2	7	1	3.175513761	3	4
986	9	1	2	7	1	3.175513761	3	4
987	9	1	2	6	4	3.425513761	3	4
988	9	1	2	6	4	3.425513761	3	4
989	9	1	2	7	1	3.175513761	3	4
990	9	1	2	7	1	3.175513761	3	4
991	9	1	2	7	1	3.175513761	3	4
992	9	1	2	6	4	3.425513761	3	4
993	9	1	2	6	4	3.425513761	3	4
994	9	1	2	7	1	3.175513761	3	4
995	9	1	5	1	1	4.300513761	4	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
996	9	2	5	2	1	4.318513761	4	3
997	9	1	3	7	1	3.278513761	3	2
998	9	1	3	7	1	3.278513761	3	2
999	9	1	3	7	5	3.430513761	3	2
1000	9	2	5	2	1	4.318513761	4	3
1001	9	1	3	7	1	3.278513761	3	2
1002	9	1	3	7	5	3.430513761	3	2
1003	34	1	3	7	4	3.042513761	3	3
1004	34	1	3	7	1	2.928513761	3	3
1005	34	1	2	7	1	2.825513761	3	3
1006	34	2	5	2	1	3.968513761	4	3
1007	34	1	2	7	1	2.825513761	3	3
1008	34	1	2	7	1	2.825513761	3	3
1009	34	1	3	7	1	2.928513761	3	3
1010	34	1	3	7	1	2.928513761	3	3
1011	34	1	2	7	5	2.977513761	3	3
1012	34	1	2	7	5	2.977513761	3	3
1013	34	1	3	7	1	2.928513761	3	3
1014	34	1	3	7	1	2.928513761	3	3
1015	34	1	2	7	1	2.825513761	3	3
1016	35	2	1	7	1	2.862513761	3	4
1017	35	2	1	7	1	2.862513761	3	4
1018	30	2	5	2	1	4.024513761	4	2
1019	30	1	3	7	1	2.984513761	3	2
1020	30	1	3	7	5	3.136513761	3	2
1021	30	1	2	7	2	2.919513761	3	3
1022	30	2	5	2	5	4.176513761	4	2
1023	30	1	3	7	5	3.136513761	3	2
1024	30	1	3	7	1	2.984513761	3	2
1025	30	2	3	7	1	3.138513761	3	3
1026	32	1	3	7	1	2.956513761	3	2
1027	32	1	3	7	4	3.070513761	3	3
1028	32	2	3	7	4	3.224513761	3	3
1029	32	2	1	6	4	3.154513761	3	3
1030	32	2	3	7	1	3.110513761	3	3
1031	32	1	2	7	5	3.005513761	3	3
1032	32	1	2	7	5	3.005513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1033	32	1	2	7	5	3.005513761	3	3
1034	32	1	2	6	4	3.103513761	3	4
1035	32	1	3	7	5	3.108513761	3	3
1036	30	1	3	7	1	2.984513761	3	2
1037	30	1	3	7	5	3.136513761	3	2
1038	30	1	3	7	1	2.984513761	3	2
1039	30	2	3	7	1	3.138513761	3	3
1040	32	2	3	7	1	3.110513761	3	3
1041	32	1	2	7	1	2.853513761	3	3
1042	32	1	3	7	5	3.108513761	3	3
1043	32	1	3	7	5	3.108513761	3	3
1044	32	2	3	7	5	3.262513761	3	3
1045	32	1	2	7	1	2.853513761	3	3
1046	32	1	2	7	4	2.967513761	3	3
1047	32	1	2	7	1	2.853513761	3	3
1048	32	1	2	7	1	2.853513761	3	3
1049	32	1	2	7	1	2.853513761	3	3
1050	32	2	3	7	1	3.110513761	3	3
1051	32	1	3	7	1	2.956513761	3	2
1052	34	1	2	7	1	2.825513761	3	3
1053	34	1	3	7	1	2.928513761	3	3
1054	34	1	3	7	4	3.042513761	3	3
1055	34	1	3	7	1	2.928513761	3	3
1056	34	1	2	7	5	2.977513761	3	3
1057	34	1	2	7	1	2.825513761	3	3
1058	30	1	2	7	1	2.881513761	3	3
1059	30	2	3	7	1	3.138513761	3	3
1060	34	1	3	7	1	2.928513761	3	3
1061	34	1	2	7	1	2.825513761	3	3
1062	34	1	3	7	5	3.080513761	3	3
1063	34	1	3	7	5	3.080513761	3	3
1064	34	1	3	7	5	3.080513761	3	3
1065	34	1	3	7	1	2.928513761	3	3
1066	34	1	3	7	5	3.080513761	3	3
1067	34	1	3	1	5	3.896513761	4	3
1068	34	1	3	7	1	2.928513761	3	3
1069	34	1	3	1	5	3.896513761	4	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1070	34	1	2	7	5	2.977513761	3	3
1071	34	1	3	4	1	3.336513761	3	3
1072	34	1	3	7	1	2.928513761	3	3
1073	34	1	3	7	1	2.928513761	3	3
1074	34	1	3	7	1	2.928513761	3	3
1075	34	1	3	7	1	2.928513761	3	3
1076	32	1	3	7	2	2.994513761	3	4
1077	32	1	3	7	5	3.108513761	3	3
1078	32	1	3	7	5	3.108513761	3	3
1079	32	1	2	6	4	3.103513761	3	4
1080	32	1	3	7	5	3.108513761	3	3
1081	32	1	3	7	5	3.108513761	3	3
1082	32	1	3	7	5	3.108513761	3	3
1083	32	1	3	7	1	2.956513761	3	2
1084	32	1	3	7	5	3.108513761	3	3
1085	34	1	3	7	1	2.928513761	3	3
1086	34	1	2	7	1	2.825513761	3	3
1087	34	1	2	7	1	2.825513761	3	3
1088	34	1	3	7	5	3.080513761	3	3
1089	34	1	2	7	1	2.825513761	3	3
1090	34	1	3	7	5	3.080513761	3	3
1091	34	1	3	7	5	3.080513761	3	3
1092	34	1	3	7	5	3.080513761	3	3
1093	34	1	3	7	1	2.928513761	3	3
1094	34	1	2	7	5	2.977513761	3	3
1095	34	1	2	7	5	2.977513761	3	3
1096	34	1	3	4	1	3.336513761	3	3
1097	34	1	2	6	4	3.075513761	3	2
1098	35	1	3	7	1	2.914513761	3	3
1099	35	1	3	7	1	2.914513761	3	3
1100	35	1	3	7	1	2.914513761	3	3
1101	35	1	2	6	4	3.061513761	3	1
1102	35	1	3	7	5	3.066513761	3	3
1103	35	1	3	7	5	3.066513761	3	3
1104	35	1	3	7	5	3.066513761	3	3
1105	31	1	2	7	1	2.867513761	3	4
1106	31	1	3	7	4	3.084513761	3	4

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1107	31	1	3	7	4	3.084513761	3	4
1108	31	1	3	7	1	2.970513761	3	3
1109	31	1	2	7	5	3.019513761	3	3
1110	31	1	2	7	4	2.981513761	3	3
1111	31	1	3	7	1	2.970513761	3	3
1112	31	1	3	7	1	2.970513761	3	3
1113	31	1	3	7	1	2.970513761	3	3
1114	31	1	3	7	4	3.084513761	3	4
1115	31	1	3	7	4	3.084513761	3	4
1116	32	1	3	7	1	2.956513761	3	2
1117	32	1	2	7	1	2.853513761	3	3
1118	32	1	2	4	1	3.261513761	3	2
1119	32	1	2	6	4	3.103513761	3	4
1120	35	1	2	7	5	2.963513761	3	3
1121	35	1	3	7	1	2.914513761	3	3
1122	35	1	2	7	5	2.963513761	3	3
1123	35	1	3	7	1	2.914513761	3	3
1124	35	1	2	7	5	2.963513761	3	3
1125	35	2	3	7	5	3.220513761	3	4
1126	35	1	3	7	5	3.066513761	3	3
1127	35	1	3	7	5	3.066513761	3	3
1128	35	1	2	7	5	2.963513761	3	3
1129	35	1	2	7	1	2.811513761	3	3
1130	35	2	1	7	1	2.862513761	3	4
1131	35	1	3	7	1	2.914513761	3	3
1132	35	1	3	7	1	2.914513761	3	3
1133	35	1	3	7	1	2.914513761	3	3
1134	35	1	3	7	1	2.914513761	3	3
1135	35	1	3	7	1	2.914513761	3	3
1136	35	1	2	7	2	2.849513761	3	3
1137	35	1	2	7	5	2.963513761	3	3
1138	35	1	2	7	1	2.811513761	3	3
1139	35	1	2	7	1	2.811513761	3	3
1140	35	1	2	7	1	2.811513761	3	3
1141	35	1	2	7	1	2.811513761	3	3
1142	35	1	3	7	1	2.914513761	3	3
1143	35	1	3	7	1	2.914513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1144	35	1	2	7	1	2.811513761	3	3
1145	35	2	2	4	1	3.373513761	3	3
1146	35	2	2	4	1	3.373513761	3	3
1147	35	2	2	4	1	3.373513761	3	3
1148	35	1	2	4	1	3.219513761	3	3
1149	35	1	2	4	1	3.219513761	3	3
1150	35	1	2	4	1	3.219513761	3	3
1151	35	1	3	7	1	2.914513761	3	3
1152	35	1	2	7	1	2.811513761	3	3
1153	35	1	2	7	1	2.811513761	3	3
1154	35	1	2	7	1	2.811513761	3	3
1155	35	1	2	7	1	2.811513761	3	3
1156	35	1	3	7	1	2.914513761	3	3
1157	35	1	3	7	5	3.066513761	3	3
1158	29	1	3	7	5	3.150513761	3	2
1159	29	1	3	7	5	3.150513761	3	2
1160	29	2	3	7	1	3.152513761	3	3
1161	29	2	3	7	1	3.152513761	3	3
1162	29	2	3	7	5	3.304513761	3	2
1163	29	2	3	7	5	3.304513761	3	2
1164	29	1	3	7	5	3.150513761	3	2
1165	29	1	3	7	1	2.998513761	3	3
1166	29	1	3	6	4	3.248513761	3	2
1167	29	1	3	7	5	3.150513761	3	2
1168	29	1	3	7	5	3.150513761	3	2
1169	29	2	3	7	2	3.190513761	3	3
1170	29	1	5	1	1	4.020513761	4	3
1171	29	1	2	6	4	3.145513761	3	4
1172	29	2	3	7	2	3.190513761	3	3
1173	29	2	3	7	1	3.152513761	3	3
1174	29	2	2	7	1	3.049513761	3	3
1175	29	2	3	7	5	3.304513761	3	2
1176	29	1	3	7	1	2.998513761	3	3
1177	29	1	3	7	5	3.150513761	3	2
1178	29	2	3	7	1	3.152513761	3	3
1179	29	2	3	7	5	3.304513761	3	2
1180	29	1	2	7	1	2.895513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1181	29	1	2	6	2	3.069513761	3	3
1182	29	1	2	7	5	3.047513761	3	3
1183	29	1	2	7	5	3.047513761	3	3
1184	29	1	2	7	5	3.047513761	3	3
1185	29	1	2	7	5	3.047513761	3	3
1186	29	1	3	7	1	2.998513761	3	3
1187	29	1	3	7	1	2.998513761	3	3
1188	29	1	2	7	5	3.047513761	3	3
1189	29	1	2	7	5	3.047513761	3	3
1190	29	1	2	7	1	2.895513761	3	2
1191	29	2	1	7	1	2.946513761	3	4
1192	29	2	1	7	1	2.946513761	3	4
1193	29	1	5	1	1	4.020513761	4	3
1194	29	1	3	7	5	3.150513761	3	2
1195	29	1	5	1	1	4.020513761	4	3
1196	29	1	5	1	1	4.020513761	4	3
1197	29	1	5	1	1	4.020513761	4	3
1198	29	1	5	1	1	4.020513761	4	3
1199	29	1	3	7	5	3.150513761	3	2
1200	9	2	5	2	1	4.318513761	4	3
1201	9	1	3	7	5	3.430513761	3	2
1202	9	1	3	7	5	3.430513761	3	2
1203	9	1	3	7	5	3.430513761	3	2
1204	9	1	3	7	5	3.430513761	3	2
1205	9	1	3	7	1	3.278513761	3	2
1206	9	1	2	6	4	3.425513761	3	4
1207	9	1	5	1	1	4.300513761	4	2
1208	9	1	3	7	1	3.278513761	3	2
1209	29	1	3	7	1	2.998513761	3	3
1210	29	1	3	7	5	3.150513761	3	2
1211	29	1	3	7	1	2.998513761	3	3
1212	29	1	3	7	1	2.998513761	3	3
1213	29	1	3	7	1	2.998513761	3	3
1214	29	1	3	7	1	2.998513761	3	3
1215	29	1	3	7	1	2.998513761	3	3
1216	29	1	2	7	1	2.895513761	3	2
1217	29	1	2	7	1	2.895513761	3	2

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1218	29	1	3	7	1	2.998513761	3	3
1219	29	1	5	7	1	3.204513761	3	4
1220	29	1	2	7	1	2.895513761	3	2
1221	29	1	2	7	1	2.895513761	3	2
1222	29	1	2	7	1	2.895513761	3	2
1223	29	1	2	7	1	2.895513761	3	2
1224	29	1	3	7	1	2.998513761	3	3
1225	29	1	2	7	5	3.047513761	3	3
1226	29	1	2	7	1	2.895513761	3	2
1227	29	1	2	7	1	2.895513761	3	2
1228	29	1	2	7	1	2.895513761	3	2
1229	29	1	2	7	1	2.895513761	3	2
1230	29	1	2	7	1	2.895513761	3	2
1231	29	1	2	7	1	2.895513761	3	2
1232	29	1	2	7	1	2.895513761	3	2
1233	9	2	5	2	5	4.470513761	4	4
1234	9	1	2	6	4	3.425513761	3	4
1235	9	1	3	7	5	3.430513761	3	2
1236	9	1	3	7	1	3.278513761	3	2
1237	9	2	3	7	1	3.432513761	3	2
1238	9	1	2	7	2	3.213513761	3	2
1239	9	1	3	7	1	3.278513761	3	2
1240	29	2	4	6	4	3.505513761	4	4
1241	29	1	2	6	4	3.145513761	3	4
1242	29	1	3	7	1	2.998513761	3	3
1243	29	1	3	7	1	2.998513761	3	3
1244	29	2	2	7	5	3.201513761	3	3
1245	29	2	2	7	1	3.049513761	3	3
1246	29	2	2	7	5	3.201513761	3	3
1247	29	2	3	7	1	3.152513761	3	3
1248	29	2	3	7	1	3.152513761	3	3
1249	29	2	3	7	1	3.152513761	3	3
1250	29	2	3	7	1	3.152513761	3	3
1251	33	2	5	2	1	3.982513761	4	5
1252	33	1	5	1	1	3.964513761	4	5
1253	33	1	3	7	1	2.942513761	3	3
1254	33	1	3	7	5	3.094513761	3	3

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1255	33	1	3	7	5	3.094513761	3	3
1256	33	1	3	7	5	3.094513761	3	3
1257	33	1	3	4	1	3.350513761	3	4
1258	33	1	2	7	5	2.991513761	3	2
1259	33	1	2	7	1	2.839513761	3	4
1260	35	2	2	4	1	3.373513761	3	3
1261	35	2	2	4	1	3.373513761	3	3
1262	35	2	2	4	1	3.373513761	3	3
1263	35	1	2	4	1	3.219513761	3	3
1264	35	1	2	4	1	3.219513761	3	3
1265	35	1	2	4	1	3.219513761	3	3
1266	35	1	3	7	1	2.914513761	3	3
1267	35	1	2	7	1	2.811513761	3	3
1268	35	1	2	7	1	2.811513761	3	3
1269	35	1	2	7	1	2.811513761	3	3
1270	35	1	2	7	1	2.811513761	3	3
1271	35	1	3	7	1	2.914513761	3	3
1272	35	1	3	7	5	3.066513761	3	3
1273	9	1	3	7	5	3.430513761	3	2
1274	9	1	3	7	1	3.278513761	3	2
1275	9	1	2	6	4	3.425513761	3	4
1276	9	1	5	1	1	4.300513761	4	2
1277	9	1	3	7	1	3.278513761	3	2
1278	33	1	2	7	5	2.991513761	3	2
1279	33	2	3	7	5	3.248513761	3	3
1280	33	1	3	7	1	2.942513761	3	3
1281	33	1	3	7	1	2.942513761	3	3
1282	33	1	3	7	1	2.942513761	3	3
1283	33	1	2	4	1	3.247513761	3	4
1284	33	1	3	4	1	3.350513761	3	4
1285	33	1	2	4	5	3.399513761	3	4
1286	33	1	2	4	5	3.399513761	3	4
1287	33	1	2	7	5	2.991513761	3	2
1288	33	1	3	7	5	3.094513761	3	3
1289	33	1	3	7	5	3.094513761	3	3
1290	33	1	5	1	1	3.964513761	4	5
1291	33	1	5	1	1	3.964513761	4	5

No	Org Unit	Actor	Threat Type	Event Type	Asset	Estimated Loss severity	Loss severity (Model)	Loss severity (Observe)
1292	33	1	2	4	1	3.247513761	3	4
1293	33	1	2	4	1	3.247513761	3	4
1294	33	1	2	4	1	3.247513761	3	4
1295	33	1	2	7	1	2.839513761	3	4
1296	33	1	2	4	1	3.247513761	3	4
1297	33	1	2	7	1	2.839513761	3	4
1298	33	1	2	7	1	2.839513761	3	4
1299	33	1	2	7	1	2.839513761	3	4
1300	33	1	2	7	1	2.839513761	3	4
1301	9	1	3	7	1	3.278513761	3	2
1302	9	1	3	7	1	3.278513761	3	2
1303	9	1	3	7	5	3.430513761	3	2
1304	9	1	2	6	4	3.425513761	3	4
1305	9	1	3	7	1	3.278513761	3	2
1306	29	1	3	7	1	2.998513761	3	3
1307	29	1	3	7	5	3.150513761	3	2
1308	29	1	3	7	1	2.998513761	3	3

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ประวัติผู้เขียนวิทยานิพนธ์

นายชวิศ ทวีโรจน์กุลศรี เกิดเมื่อวันที่ 18 พฤศจิกายน พ.ศ. 2532 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีหลักสูตรวิศวกรรมศาสตรบัณฑิต (วศ.บ.) สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2554 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมซอฟต์แวร์ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2555

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University