แบบจำลองการบริหารความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษาระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์

THE MODEL OF RISK AND INTERNAL CONTROL MANAGEMENT FOR INFORMATION TECHNOLOGY: A CASE STUDY OF ELETRONIC BANKING

จิราวนี สิริประภาวัสดิ์
JIRAVANEE SIRIPRAPASAWAD

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2556

แบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์

THE MODEL OF RISK AND INTERNAL CONTROL MANAGEMENT FOR INFORMATION TECHNOLOGY: A CASE STUDY OF ELETRONIC BANKING

โดย

จิรวณี สิริประภาสวัสดิ์

JIRAVANEE SIRIPRAPASAWAD

อาจารย์ที่ปรึกษา

ดร. สิงหะ ฉวีสุข

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2556

THE MODEL OF RISK AND INTERNAL CONTROL MANAGEMENT FOR INFORMATION TECHNOLOGY: A CASE STUDY OF ELETRONIC BANKING

JIRAVANEE SIRIPRAPASAWAD

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2 / 2013

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

แบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์

THE MODEL OF RISK AND INTERNAL CONTROL MANAGEMENT FOR INFORMATION TECHNOLOGY: A CASE STUDY OF ELETRONIC BANKING

นางสาวจิรวณี สิริประภาสวัสดิ์

รหัสประจำตัว 55660908

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2556

.....อาจารย์ที่ปรึกษา

(ดร. สิงหะ ฉวีสุข)

.....กรรมการสอบ

(รศ.ดร. อาริต ธรรมโน)

.....กรรมการสอบ

(ดร. กนกวรรณ อัจฉริยะชาญวณิช)

หัวข้อ	แบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์
นักศึกษา	นางสาวจิรวณี สิริประภาสวัสดิ์
รหัสนักศึกษา	55660908
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีสารสนเทศและการจัดการ
ปีการศึกษา	2556
อาจารย์ที่ปรึกษา	ดร. สิงหะ ฉวีสุข

บทคัดย่อ

การทำธุรกรรมทางการเงินของลูกค้าธนาคารพาณิชย์ในปัจจุบันสามารถใช้ช่องทางในการติดต่อกับธนาคารและเลือกทำธุรกรรมที่หลากหลายมากขึ้นตามความต้องการของลูกค้า รวมทั้งธนาคารพาณิชย์ก็มีการเพิ่ม หรือปรับปรุงผลิตภัณฑ์ทางการเงินให้เข้ากับลูกค้าได้มากมายเพิ่มขึ้น ซึ่งส่วนที่มีความสำคัญที่ช่วยขับเคลื่อนการทำธุรกิจธนาคารพาณิชย์ให้ประสบความสำเร็จได้ คือ การนำเทคโนโลยีสารสนเทศเข้ามาประยุกต์ใช้ให้เข้ากับการทำธุรกรรมทางการเงิน ให้มีความคล่องตัวและสะดวกสบายมากขึ้น สามารถตอบสนองความต้องการของลูกค้าได้อย่างต่อเนื่อง แต่การทำธุรกรรมอิเล็กทรอนิกส์ต่าง ๆ ของสถาบันการเงินก็มีความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ซึ่งทำให้หน่วยงานกำกับธนาคารพาณิชย์ มีการสั่งการและออกกฎเกณฑ์ระเบียบ เพื่อให้ธนาคารพาณิชย์มีการป้องกัน ปรับปรุงความปลอดภัยให้เหมาะสม เพื่อป้องกันข้อมูลของลูกค้าซึ่งเป็นสิทธิส่วนบุคคลในการทำธุรกรรมการเงินให้มีความปลอดภัย และไม่ก่อให้เกิดความเสียหาย ธนาคารพาณิชย์จึงความมีมาตรฐานการบริหารจัดการความเสี่ยงและการควบคุมภายในเทคโนโลยีสารสนเทศขององค์กรโดยมีการนำมาตรฐาน Information Security Management System (ISMS) หรือที่เรียกว่า มาตรฐาน ISO/IEC 27001 มาช่วยสนับสนุนการบริหารจัดการความเสี่ยง และการควบคุมภายในขององค์กรที่ดีด้านเทคโนโลยีสารสนเทศขององค์กร

Title	The Model of Risk and Internal Control Management for Information Technology: A Case Study of Electronic Banking
Student	Ms. Jiravanee Siriprapasawad
Student ID.	55660908
Degree	Master of Science
Program	Information Technology
Major	Information Technology and Management
Academic Year	2013
Advisor	Dr. Singha Chaveesuk

ABSTRACT

Customer can currently operate their financial transaction with banks via variety of channels and products upon the customer's requirements. Recently, with the rapid changes in customer needs, banks have to improve or create their products to serve the needs. Thus, Information Technology (IT) is used as the key business driver to drive the bank successfully. Information technology can make the business more agility, comfortably and can also support the requirement continuously. However, the more uses of information technology the more risk in securing the Information technology system can be identified. Therefore, the regulators have asked the banks to comply rules and regulations. The objective is to help the banks to set the appropriate security controls and secure the confidential information such as customer information. Nowadays, Information Security Management System (ISMS) or ISO/IEC 27001 standard had also been brought to many banks as a framework for insisting them in managing the risk and having the better internal control for Information system.

กิตติกรรมประกาศ

โครงการศึกษาค้นคว้าอิสระนี้ประสบความสำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา ดร. สิงหะ ฉวีสุข ที่คอยให้ความรู้ คำสั่งสอนและคำแนะนำตลอดการพัฒนาโครงการ ทำให้โครงการสามารถสำเร็จลุล่วงได้ด้วยดี นอกจากนี้ข้าพเจ้าขอขอบคุณบุคคลทุกท่านซึ่งคอยให้การสนับสนุนด้านต่าง ๆ ที่เป็นประโยชน์ในการพัฒนาระบบ

ขอขอบคุณคณาจารย์คณะเทคโนโลยีสารสนเทศที่ได้ประสิทธิประสาทวิชาความรู้อันเป็นประโยชน์ให้แก่ข้าพเจ้า

ขอขอบคุณหัวหน้างานและเพื่อนร่วมงาน ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ และสายเทคโนโลยีสารสนเทศ ธนาคารพาณิชย์แห่งหนึ่ง ที่คอยให้ความรู้ทางเทคนิคและข้อมูล

ขอขอบคุณบิดา มารดา รวมถึงญาติพี่น้องที่คอยสนับสนุนและเป็นกำลังใจ ทำให้มีความมุ่งมั่นในการพัฒนาโครงการศึกษา

สุดท้ายนี้ขอขอบคุณรุ่นพี่และเพื่อนร่วมรุ่นทุกท่านที่คอยแนะนำและช่วยเหลือทุกด้าน ไม่ว่าจะเป็นด้านวิชาการหรือด้านอื่น ๆ

จิรวณี สิริประภาสวัสดิ์

สารบัญ

หน้า

บทคัดย่อ I

ABSTRACT II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญตาราง VII

สารบัญภาพ IX

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์ของโครงการศึกษา 2

1.3 ขอบเขตของโครงการศึกษา 2

1.4 ประโยชน์ที่คาดว่าจะได้รับ 3

1.5 กำหนดการดำเนินโครงการ 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5

2.1 กฎหมาย ระเบียบ ข้อบังคับ 5

2.1.1 พระราชกฤษฎีกา 5

2.1.2 ประกาศธนาคารแห่งประเทศไทย 6

2.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 7

2.2.1 ความเสี่ยง (Risk) 7

2.2.2 การระบุความเสี่ยง 8

2.2.3 การประเมินความเสี่ยง 9

2.2.4 ตอบสนองต่อความเสี่ยง 10

2.3 ทฤษฎีมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ 11

บทที่ 3 วิธีการศึกษาโครงการ 24

3.1 วิธีการนำเสนอ (Methodology) 24

3.2 เครื่องมือที่ใช้ในการศึกษาโครงการ 33

บทที่ 4 กรณีศึกษาองค์กรปัจจุบัน 37

4.1 ข้อมูลเบื้องต้นของกรณีศึกษา 37

4.2 โครงสร้างองค์กร และโครงสร้างสายเทคโนโลยีสารสนเทศ 38

สารบัญ (ต่อ)

หน้า

4.3 ความสอดคล้องของการกำหนดเป้าหมายองค์กรและเทคโนโลยีสารสนเทศ 43
4.4 นโยบาย ระเบียบ หลักเกณฑ์ คู่มือ ที่เกี่ยวข้องกับองค์กรศึกษา 44
4.4.1 นโยบายด้านเทคโนโลยีสารสนเทศ (IT Policy) 45
4.4.2 ระเบียบด้านเทคโนโลยีสารสนเทศ (IT Procedure) 56
4.4.3 หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศ (IT Principle Operation) 60
4.4.4 บันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off) ... 64
4.4.5 คู่มือการปฏิบัติงาน 67
4.5 ความเสี่ยงขององค์กร 68
4.6 การควบคุมภายในองค์กรศึกษา 74
บทที่ 5 การพัฒนาแบบจำลอง 76
5.1 การพัฒนาการสร้างแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ 76
5.1.1 การสำรวจตัวชี้วัดการดำเนินการที่เหมาะสมกับธนาคาร 76
5.1.2 การสร้างแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ 79
5.2 การพัฒนาการสร้างแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ 89
บทที่ 6 การทดสอบแบบจำลอง (ก่อนทำโครงการ) 96
6.1 การประเมินผลการจัดทำโครงการ (ก่อนทำโครงการ) 96
6.1.1 การจัดทำ Checklist เพื่อสอบทานผลการดำเนินการ (ก่อนทำโครงการ) 96
6.1.2 การประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) ... 130
6.2 การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) 140
6.3 ข้อเสนอแนะการเพิ่มเติม ปรับปรุงการดำเนินการ 159
6.3.1 การจัดลำดับความเสี่ยงความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศ 159
6.3.2 การตอบสนองต่อความเสี่ยงตามลำดับความสำคัญ 163
บทที่ 7 การทดสอบแบบจำลอง (หลังทำโครงการ) 169
7.1 การประเมินผลการจัดทำโครงการ (หลังทำโครงการ) 169
7.1.1 ผู้ปฏิบัติงานนำแนวทางข้อเสนอแนะไปบริหารการจัดการความมั่นคงปลอดภัย ... 169
7.1.2 การประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) ... 184
7.2 การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) 195
บทที่ 8 สรุปผลการดำเนินโครงการ 217

สารบัญ (ต่อ)

หน้า

8.1 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนและหลังทำโครงการ)..... 217
8.2 สรุปผลประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนและหลังทำโครงการ)..... 219
8.3 สรุปขั้นตอนดำเนินการแบบจำลองความเสี่ยงและการควบคุมภายใน IT..... 224
บรรณานุกรม..... 225
ภาคผนวก..... 227
ภาคผนวก ก..... 228
ภาคผนวก ข..... 232
ภาคผนวก ค..... 241
ภาคผนวก ง..... 245
ประวัติผู้เขียน..... 253

สารบัญตาราง

ตารางที่ หน้า

1.5 กำหนดการดำเนินโครงการ 3

3.1.3 ขอบเขตการจัดการความมั่นคงปลอดภัย Access Control 26

3.2.1.1 เทคนิคการประเมินความน่าจะเป็นตาม Risk Value 33

3.2.1.2 ระดับการประเมินความเสี่ยง (Risk Rating) 34

3.2.2 การจำแนกความเสี่ยงตามเกณฑ์ธนาคารแห่งประเทศไทย 35

4.4.1 ความแตกต่างของนโยบายด้านเทคโนโลยีสารสนเทศ ปี 2552 และ 2555 46

4.4.2.1 สรุประเบียบการใช้งานทรัพย์สินสารสนเทศ 56

4.4.2.2 สรุประเบียบการกำหนดบัญชีผู้ใช้งานและรหัสผ่าน 57

4.4.2.3 สรุประเบียบการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาวะแวดล้อม 58

4.4.3.1 ระดับผลกระทบและความเสี่ยงการเปลี่ยนแปลงเทคโนโลยีสารสนเทศ 61

4.4.4.1 หน้าที่ความรับผิดชอบของสายงานการใช้งาน Mobile Device and Network 65

4.4.4.2 หน้าที่ความรับผิดชอบการบริหารจัดการสิทธิผู้ใช้งาน และรหัสผ่าน 66

4.4.5 คู่มือการปฏิบัติงานด้านเทคโนโลยีสารสนเทศขององค์กรศึกษา 68

4.5.1 การกำหนดประเภทความเสี่ยงขององค์กรศึกษา 69

4.5.2.1 เกณฑ์การประเมินความเสี่ยงจากความถี่ของเหตุการณ์ที่เกิดขึ้น 72

4.5.2.2 เกณฑ์การประเมินความเสี่ยงจากผลกระทบ/ความเสียหายที่เกิดขึ้น 73

5.1.1.1 สรุปผลแบบสำรวจตัวชี้วัดที่เหมาะสมกับธนาคาร 77

5.1.1.2 การแบ่งระดับแบบสำรวจตัวชี้วัดที่เหมาะสมกับธนาคาร 79

5.1.2.1 แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ 81

5.1.2.2 ผลสรุปแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ 88

5.2.1 การกำหนดประเภทความเสี่ยงในแบบจำลอง 89

5.2.2 การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ 90

5.2.3 การประเมินผลกระทบหรือความเสียหายของการเกิดเหตุการณ์ 92

5.2.4.1 วิธีการคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้นได้ในแบบจำลองความเสี่ยง 93

5.2.4.2 ระดับการประเมินความเสี่ยงในแบบจำลองความเสี่ยง 94

6.1.1 แบบสอบถามกระบวนการปฏิบัติงาน การควบคุมภายใน (ก่อนทำโครงการ) 97

6.1.2.1 แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) 131

6.1.2.2 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) 138

สารบัญตาราง (ต่อ)

ตารางที่		หน้า
6.2.1	การกำหนดประเภทความเสี่ยงในแบบจำลอง (ก่อนทำโครงการ)	141
6.2.2	การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ (ก่อนทำโครงการ)	144
6.2.3	การประเมินผลกระทบหรือความเสียหายการเกิดเหตุการณ์ (ก่อนทำโครงการ)	149
6.2.4	การคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้น (ก่อนทำโครงการ)	154
6.3.1	การจัดลำดับความเสี่ยงการจัดการความมั่นคงปลอดภัยเพื่อการแก้ไข	160
6.3.2.1	ข้อเสนอแนะสำหรับผลลัพธ์ความเสี่ยงสูง	163
6.3.2.2	ข้อเสนอแนะด้านเทคนิคสำหรับผลลัพธ์ความเสี่ยงระดับปานกลาง	166
6.3.2.3	ข้อเสนอแนะด้านกระบวนการสำหรับผลลัพธ์ความเสี่ยงระดับปานกลาง	167
7.1.1	แบบสอบถามกระบวนการปฏิบัติงาน การควบคุมภายใน (หลังทำโครงการ)	170
7.1.2.1	แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)	185
7.1.2.2	สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)	192
7.2.1	การกำหนดประเภทความเสี่ยงในแบบจำลอง (หลังทำโครงการ)	195
7.2.2	การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ (หลังทำโครงการ)	200
7.2.3	การประเมินผลกระทบหรือความเสียหายการเกิดเหตุการณ์ (หลังทำโครงการ)	205
7.2.4	การคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้น (หลังทำโครงการ)	211
8.1.1	สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากแบบจำลอง	218
8.2.1	ผลลัพธ์จากการประเมินความเสี่ยงและทิศทาง	219
8.2.2	สรุปผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ก่อนหลังทำโครงการ	222
8.2.3	สรุปผลความเสี่ยงและทิศทางของความเสี่ยง (Risk Heat Map)	223

สารบัญภาพ

รูปที่		หน้า
2.1	วงจรความมั่นคงปลดดภัย CIA	6
2.3	วงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Chcek-Act	12
3.1	มาตรฐาน ISO/IEC 27001 ในขอบเขตเรื่อง Access Control	25
3.2	วิธีการนำเสนอโครงการ (Methodology)	32
4.2.1	โครงสร้างองค์กรกรณีศึกษา (Organization Chart)	40
4.2.2	โครงสร้างส่วนงานเทคโนโลยีสารสนเทศ	42
4.2.3	โครงสร้างองค์กรส่วนตรวจสอบเทคโนโลยีสารสนเทศ	43
4.3	ความสอดคล้องของธรรมาภิบาลองค์กรและธรรมาภิบาลเทคโนโลยีสารสนเทศ	44
4.4	เอกสารต่าง ๆ ที่เกี่ยวข้องกับองค์กรศึกษา	44
4.6	แนวป้องกันสามชั้น (Three Lines of Defence)	75
5.1.2	แผนภูมิแสดงผลสรุปแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ	88
5.2.1	การระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง	90
5.2.2	การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง	91
5.2.3	การประเมินผลกระทบหรือความเสียหายของเหตุการณ์ในแบบจำลองที่จัดสร้าง	93
5.2.4	วิธีการคำนวณมูลค่าความเสียหาย (RiskValue)	94
5.2.4	ผลลัพธ์ที่ได้จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศที่จัดสร้าง	95
6.1.2	แผนภูมิแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)	140
6.2.1	แสดงการระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)	143
6.2.2	การประเมินโอกาสของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)	147
6.2.3	การประเมินผลกระทบเหตุการณ์ที่เกิดในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)	153
6.2.4.1	การคำนวณมูลค่าความเสียหาย (Risk Value) ก่อนทำโครงการ	157
6.2.4.2	ผลลัพธ์จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)	158
7.1.2	แผนภูมิแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)	194
7.2.1	แสดงการระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)	198
7.2.2	การประเมินโอกาสของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)	203
7.2.3	การประเมินผลกระทบเหตุการณ์ที่เกิดในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)	210
7.2.4.1	การคำนวณมูลค่าความเสียหาย (Risk Value) หลังทำโครงการ	215
7.2.4.2	ผลลัพธ์จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)	216

สารบัญภาพ (ต่อ)

รูปที่		หน้า
8.1.1	แผนภูมิการควบคุมภายในด้านเทคโนโลยีสารสนเทศก่อนและหลังทำโครงการ	218
8.3	สรุปขั้นตอนการดำเนินการแบบจำลองความเสี่ยงและการควบคุมภายในด้าน IT	224
1.2.1	เอกสารแนบหน้าจอ IT Request การร้องขอสิทธิเข้าถึงระบบงาน	242
1.3.2	เอกสารแนบหน้าจอการกำหนดค่า Configuration การเข้าถึงระบบงานระดับ Server	243
1.4.3	หน้าจอการกำหนดค่า IP Address ให้เข้าถึงระบบเครือข่ายได้เฉพาะผู้ดูแลระบบ	244
1.4.4.1	เอกสารแนบหน้าจอการเปิดพอร์ตการเข้าถึงระบบเครือข่าย	244
1.2.2	เอกสารแนบตัวอย่างแบบฟอร์มขอใช้สิทธิเฉพาะ(Privilege User) การทบทวน Log	246
1.3.1	เอกสารแนบหน้าจอการกำหนดค่า Configuration การเลือกใช้งานรหัสผ่าน	247
1.4.1.1	เอกสารแนบตัวอย่างประกาศใช้งานนโยบายใช้บริการเครือข่าย(Network Policy)	248
1.4.4.2	เอกสารแนบการกำหนดค่าป้องกันพอร์ตความมั่นคงปลอดภัยระบบเครือข่าย	248
1.4.7	เอกสารแนบการควบคุมการกำหนดเส้นทางบนเครือข่ายที่สำคัญ	249
1.5.4	เอกสารแนบการกำหนดสิทธิไม่ให้ผู้ใช้งานติดตั้งโปรแกรมยูทิลิตี้	250
1.7.1	เอกสารแนบทบทวนบัญชีผู้ใช้งานที่ได้รับสิทธิ Mobile computing and Teleworking	251
1.7.2	เอกสารแนบรายละเอียดทบทวนบัญชีผู้ใช้งาน Mobile computing and Teleworking	252

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทในการขับเคลื่อนการดำเนินการธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ต่าง ๆ เพื่อให้องค์กรเกิดความสะดวกรวดเร็ว มีประสิทธิภาพและเพิ่มโอกาสการแข่งขันทางธุรกิจได้ ตลอดจนสร้างความพึงพอใจให้กับลูกค้าในการทำธุรกรรมทางการเงินกับธนาคารต่าง ๆ โดยในหลายธนาคารนั้นมีการพัฒนา จัดซื้อจัดจ้างระบบสารสนเทศต่าง ๆ เข้ามาสนับสนุนการดำเนินธุรกิจขององค์กร อย่างไรก็ตาม การใช้งานเทคโนโลยีสารสนเทศย่อมมีความเสี่ยงหลายประการที่ธนาคารพาณิชย์ หรือองค์กรต่าง ๆ ควรคำนึงถึง โดยหากองค์กรใดก็ตามไม่มีกระบวนการ วิธีการบริหารจัดการรักษาความมั่นคงปลอดภัย หรือการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่เพียงพอ อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อองค์กร และลูกค้าได้

ประกอบกับธนาคารแห่งประเทศไทย มีการกำหนดให้ธนาคารพาณิชย์ต่าง ๆ ซึ่งมีการทำธุรกรรมด้านอิเล็กทรอนิกส์ จำเป็นต้องมีการกำหนดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคารอย่างเหมาะสม อาทิ การกำหนดให้มีการป้องกันระบบสารสนเทศ ตลอดจนการบำรุงรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสารสนเทศต่าง ๆ ตามแต่ประกาศของหน่วยงานรัฐบาลหรือ หน่วยงานกำกับดูแลของรัฐต่าง ๆ กำหนดขึ้น

ดังนั้นการประเมินความเสี่ยง (Risk Assessment) การจัดการความเสี่ยง (Risk Management) และการควบคุมภายในความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงเป็นเรื่องที่องค์กรหรือธนาคารพาณิชย์ต่าง ๆ ควรให้ความสำคัญ โดยในแต่ละองค์กรนั้น ย่อมมีการกำหนดกลยุทธ์การดำเนินธุรกิจที่มีความหลากหลายและแตกต่างกัน ซึ่งในการจำแนกความเสี่ยง และควบคุมความเสี่ยงที่ดีนั้น องค์กรย่อมต้องมีการกำหนดนโยบายการกำกับดูแล และตรวจสอบเกี่ยวกับการบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อให้การนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการประกอบธุรกิจธนาคารพาณิชย์สามารถเกิดประโยชน์สูงสุด สอดคล้องกับเป้าหมายการดำเนินธุรกิจของธนาคารพาณิชย์ที่กำหนดไว้ได้

ผู้ศึกษาจึงได้พิจารณาทำโครงการศึกษาแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ โดยการนำมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001 Information Security Management System) ซึ่งระบุถึงแนวทางการปฏิบัติงานที่ดีในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ มาประยุกต์ใช้ในการประเมินความเสี่ยง และการบริหาร

จัดการให้มีความเหมาะสม เพื่อเป็นแนวทางการปฏิบัติความมั่นคงปลอดภัยการใช้งานระบบสารสนเทศที่ดีของกับธนาคารพาณิชย์ซึ่งเป็นกรณีศึกษาได้

1.2 วัตถุประสงค์ของโครงการศึกษา

1. เพื่อศึกษาและสร้างแบบจำลองที่ช่วยประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรที่มีในปัจจุบันได้อย่างถูกต้อง
2. เพื่อให้สามารถระบุความเสี่ยงที่เป็นจุดอ่อนด้านเทคโนโลยีสารสนเทศขององค์กรได้
3. เพื่อให้สามารถใช้สร้างเกณฑ์พื้นฐานในการบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัยมากขึ้น

1.3 ขอบเขตของโครงการศึกษา

ขอบเขตของโครงการศึกษาแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ เพื่อช่วยประเมินความเพียงพอของการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศการดำเนินธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ในประเทศไทย เฉพาะในขอบเขตเรื่องการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) ซึ่งมีขอบเขตการศึกษาโครงการ ดังนี้

1. โครงการศึกษาดังกล่าวเป็นการศึกษาเฉพาะการสร้างแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์แห่งหนึ่ง ซึ่งสายบริหารความเสี่ยงมีการกำหนดระดับความเสี่ยงขององค์กร มาประยุกต์ใช้งานกับการประเมินความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศธนาคารได้อย่างถูกต้องและสอดคล้องกัน
2. โครงการศึกษาดังกล่าวมีการศึกษาการดูแลความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศขององค์กรกรณีศึกษา เพื่อประเมินความเสี่ยง และความเพียงพอต่อการควบคุมภายในด้านเทคโนโลยีสารสนเทศ
3. โครงการศึกษาดังกล่าวมีการศึกษาและวิเคราะห์ประยุกต์ใช้การบริหารจัดการสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ เนื่องจากเป็นนโยบายด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์เป็นผู้กำหนดไว้ (Policy Maker) ว่าด้วยการกำหนดแนวนโยบายการบริหารจัดการให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ที่แปลความมาจากมาตรฐานดังกล่าว เพื่อสามารถ

จัดทำแบบจำลองการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศในขอบเขตเรื่องการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control)

4. โครงการศึกษามีการประเมินผลการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์แห่งหนึ่ง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้องค์กรได้มาซึ่งแบบจำลองที่สามารถใช้ประโยชน์ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรที่มีอยู่ได้อย่างมีประสิทธิภาพมากขึ้น
2. ช่วยให้องค์กรทราบถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ และสามารถจำแนกความเสี่ยง รวมถึงนำไปใช้วิเคราะห์ความเสี่ยงที่ควรพิจารณาจัดการในจุดที่เหมาะสม และคุ้มค่าต่อการจัดการด้านเทคโนโลยีสารสนเทศได้อย่างถูกต้องยิ่งขึ้น
3. สามารถใช้เป็นแนวทางปฏิบัติการบริหารจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัยมากขึ้น

1.5 กำหนดการดำเนินโครงการ

ตารางที่ 1.5 กำหนดการดำเนินโครงการ

การดำเนินโครงการ	ปี 2556							ปี 2557	
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.
1. ศึกษาความเป็นไปได้ของโครงการศึกษา	←	→							
2. ศึกษาค้นคว้างานวิจัย และทฤษฎีที่เกี่ยวข้อง		←	→						
3. ศึกษามาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ		←	→	→					

ตารางที่ 1.5 (ต่อ)

การดำเนินโครงการ	ปี 2556							ปี 2557	
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.
4. ศึกษาการการบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กรศึกษาและความเสี่ยงองค์กรเพื่อกำหนดขอบเขตศึกษา				←	→				
5. สร้างแบบจำลองการควบคุมภายใน ตามมาตรฐานการบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศตามความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) ที่ดีในขอบเขตการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control)					←	→			
6. ทดสอบการประเมินความเสี่ยงและการควบคุมภายในความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศก่อนและหลังทำโครงการ (ตามขอบเขตการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control)						←	→	←	→
7. สรุปผลการดำเนินโครงการการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ								←	→

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีที่ศึกษาและนำมาประยุกต์ใช้เพื่อสร้างแบบจำลองการประเมินความเสี่ยง และการควบคุมภายในเทคโนโลยีสารสนเทศ ขององค์กรศึกษา ซึ่งเป็นธนาคารพาณิชย์แห่งหนึ่งของประเทศไทย ซึ่งธนาคารในปัจจุบันย่อมต้องมีเทคโนโลยีสารสนเทศต่าง ๆ ในการนำมาใช้เพื่อการขับเคลื่อนการดำเนินการธุรกรรมด้านอิเล็กทรอนิกส์ของธนาคาร และจำเป็นต้องมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้มีความเพียงพอและเหมาะสม โดยมีรายละเอียดดังนี้

2.1 กฎหมาย ระเบียบ ข้อบังคับ

2.1.1 พระราชกฤษฎีกา

พระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ที่ประกาศให้ องค์กรควรกำหนดวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ สื่อให้เห็นถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information security) อันได้แก่

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

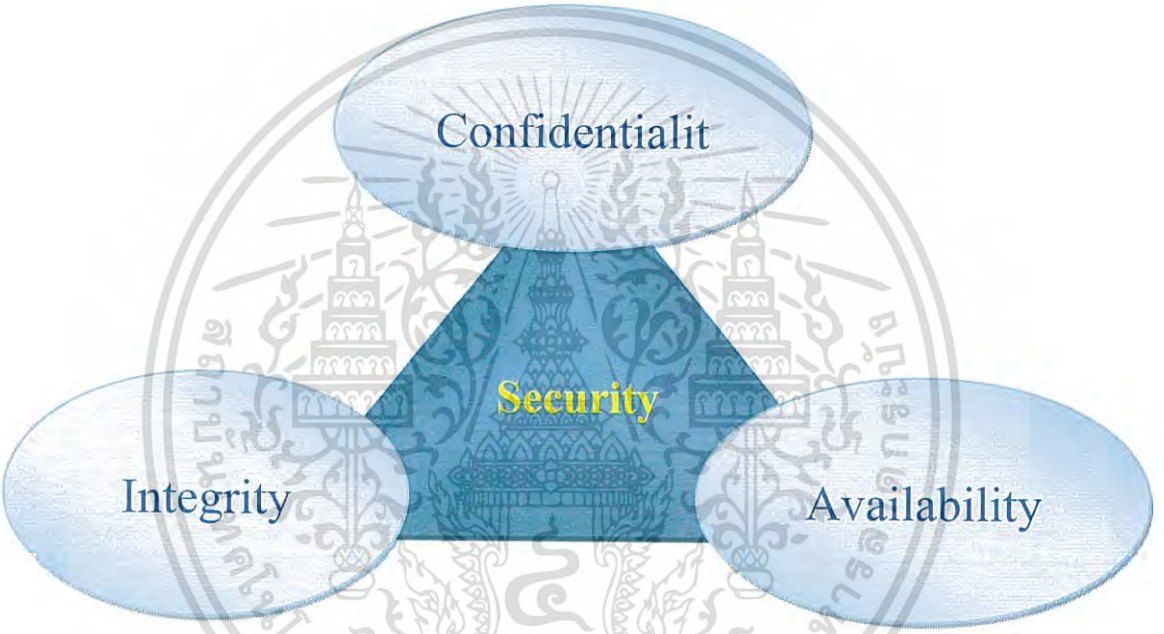
โดยให้มีการจัดการเพื่อทำการป้องกันจากการเข้าถึง การใช้งาน การเปิดเผย ตลอดจนขัดขวาง การเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ ซึ่งตามประกาศฯ ดังกล่าว คำนึงถึงหลักการพื้นฐานของวิธีการบริหารจัดการการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ มุ่งเน้นให้มีการจัดการให้มีการควบคุมภายในอย่างเหมาะสม อาทิ

- การรักษาความลับ (Confidentiality) เป็นการรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

- การรักษาความครบถ้วน (Integrity) เป็นการดำเนินการเพื่อให้ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

- การรักษาสภาพพร้อมใช้งาน (Availability) เป็นการจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

ซึ่งโดยทั่วไปการรักษาความมั่นคงปลอดภัย บุคคลมักทราบและเรียกกันว่า CIA Security Triangle หรือ C+I+A Triad ซึ่งมีความสัมพันธ์ดังภาพ



รูปที่ 2.1 วงจรความมั่นคงปลดภัย CIA

2.1.2 ประกาศธนาคารแห่งประเทศไทย

ตามประกาศธนาคารแห่งประเทศไทย ที่ สรข. 3/2552 เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ที่กำหนดว่า ผู้ให้บริการจะต้องจัดทำนโยบายการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเป็นลายลักษณ์อักษร โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการบริหารหรือผู้บริหารระดับสูงของผู้ให้บริการ ทั้งนี้ผู้ให้บริการจะต้องเผยแพร่นโยบายดังกล่าว และอบรมให้แก่บุคลากรที่เกี่ยวข้องเพื่อถือปฏิบัติ รวมทั้งจัดให้มีการทบทวนหรือปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์อย่างสม่ำเสมอ

โดยเนื้อหาของนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการ อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

(1) การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

(2) การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

(3) การรักษาสภาพความพร้อมใช้งานของการให้บริการ

(4) การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการจะต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้สอดคล้องกับนโยบายที่ได้กำหนดขึ้น และมาตรการดังกล่าวจะต้องเหมาะสมกับลักษณะของธุรกิจ โดยครอบคลุมถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ การรักษาสภาพความพร้อมใช้งานของการให้บริการ การแก้ไขปัญหาและการรายงาน รวมถึงจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง ทั้งนี้ ผู้ให้บริการจะต้องดำเนินการทบทวนหรือปรับปรุงมาตรการตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับนโยบายและมาตรการที่ได้กำหนดไว้ ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้องทั้งหมดขององค์กร

2.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2.2.1 ความเสี่ยง (Risk)

ความเสี่ยง คือ โอกาสหรือบางสิ่งที่อาจเกิดขึ้น ซึ่งเป็นผลลัพธ์ของสิ่งที่เป็นอันตรายหรือภัยคุกคาม การขัดขวางที่อาจส่งผลกระทบต่อกิจกรรมทางธุรกิจหรือแผนงานที่กำหนดไว้ทำให้ไม่สามารถดำเนินการได้อย่างราบรื่น หรือมีโอกาสที่เป็นปัจจัยก่อให้เกิดความล้มเหลว

ซึ่งหากเป็นความเสี่ยงด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศแล้ว นั้นอาจสื่อถึงการที่เหตุการณ์ (Event) ภัยคุกคาม (Threat) ใด ๆ โดยใช้ช่องโหว่ (Vulnerability) ของเทคโนโลยีสารสนเทศส่งผลต่อความเสียหายด้านเทคโนโลยีสารสนเทศขององค์กร ทำให้ระบบเทคโนโลยีสารสนเทศไม่สามารถสนับสนุนการดำเนินการธุรกิจขององค์กร ทำให้องค์กรหยุดชะงัก หรือดำเนินธุรกิจได้อย่างล่าช้า ก่อให้เกิดผลเสียหายทั้งด้านที่เป็นตัวเงิน เช่น ทรัพย์สินหรือหลักทรัพย์ต่าง ๆ และด้านที่ไม่เป็นตัวเงิน เช่น ชื่อเสียง กระบวนการ กลยุทธ์ทางธุรกิจได้

2.2.2 การระบุความเสี่ยง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ล้วนสามารถเกิดขึ้นได้กับทุกองค์กรที่มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยสนับสนุนการดำเนินธุรกิจขององค์กร ซึ่งองค์กรต่าง ๆ ควรจะสามารถระบุความเสี่ยงจึงเป็นการระบุถึงเหตุการณ์ที่เคยเกิดขึ้นกับองค์กรหรือมีแนวโน้มที่อาจเกิดขึ้นได้ให้ใกล้เคียง หรือมีโอกาสความน่าจะเป็นของการเกิดเหตุการณ์มากที่สุด โดยการกำหนดปัจจัยที่อาจส่งผลกระทบ อาทิ

1) ปัจจัยภายนอก

- **ปัจจัยด้านเศรษฐกิจ** เป็นเหตุการณ์ที่เกี่ยวข้องกับการเงินและการลงทุนของประเทศ การกีดกันทางการค้า การรักษาฐานะทางการเงินของประเทศ อันสามารถส่งผลให้เกิดความเสี่ยงด้านความผันผันทางเศรษฐกิจ เช่น การลดภาษีในบางประเทศเพื่อลดโอกาสทางการกีดกันทางการค้า (เปิดการค้าเสรี) ก่อให้เกิดคู่แข่งขันรายใหม่

- **ปัจจัยด้านการเมือง** เป็นเหตุการณ์ที่เกี่ยวข้องความมั่นคงปลอดภัยของประชนชนภายในประเทศ กฎหมาย ข้อบังคับ นโยบายการบริหารประเทศ การเลือกตั้ง อันสามารถส่งให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยทางการเมือง เช่น การปฏิวัติรัฐประหารทางการเมืองในบางประเทศ ก่อให้เกิดข้อจำกัดในการเข้าสู่ตลาดการค้า

- **ปัจจัยด้านสภาพแวดล้อมทางธรรมชาติ** เป็นเหตุการณ์ที่เกิดขึ้นตามธรรมชาติ อันส่งผลให้เกิดความเสี่ยงการเข้าถึงแหล่งวัตถุดิบ การผลิต และการสูญเสียบุคลากร เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหว เป็นต้น

- **ปัจจัยด้านสังคม** เป็นเหตุการณ์ที่เกิดขึ้นจากปัจจัยการเปลี่ยนแปลงวิถีทางสังคม โครงสร้างประชากร หรือจารีตทางสังคม อันส่งผลให้เกิดความเสี่ยงกับกลุ่มบุคคลหรือประชากรได้ เช่น ปัญหาการก่ออาชญากรรมของสังคม มีผลต่อความล่าช้า หรือการหยุดชะงักของการดำเนินธุรกิจกับบางองค์กรในประเทศได้

2) ปัจจัยภายใน

- **ปัจจัยด้านบุคลากร** เป็นเหตุการณ์ที่เกิดขึ้นกับบุคลากรในองค์กร อันก่อให้เกิดความเสี่ยงในการปฏิบัติงาน ชื่อเสียง หรือสถานะทางการเงินขององค์กรได้ เช่น การกระทำทุจริตของบุคคลในองค์กร อันเนื่องมาจากความตั้งใจ หรือความไม่เจตนา ส่งผลให้เกิดความเสียหายทั้งด้านการเงินและชื่อเสียงขององค์กรในด้านความน่าเชื่อถือของการบริหารจัดการที่ขาดธรรมาภิบาล และความโปร่งใส

- **ปัจจัยด้านกระบวนการ** เป็นเหตุการณ์หรือปัจจัยที่เกิดขึ้นกับวิธีการ ขั้นตอน หรือแนวปฏิบัติอันส่งผลต่อการปฏิบัติงานของบุคลากรภายในองค์กร ทั้งในด้านการปรับเปลี่ยนกระบวนการโดยขาดแบบแผนหรือการวางแผนที่เหมาะสม ก่อให้เกิดความผิดพลาดในการปฏิบัติงาน เช่น การจัดจ้างบริษัทภายนอก (Outsourcing) เพื่อการจัดส่ง

สินค้าโดยขาดการดูแลอย่างเพียงพอ รวมทั้งไม่มีการประเมินการบริการจากบริษัทและความพึงพอใจงานบริหารที่ได้รับจากลูกค้า

- **ปัจจัยด้านเทคโนโลยี และระบบงาน** เป็นเหตุการณ์หรือปัจจัยที่อาจเกิดขึ้นกับการทำงานของระบบงาน หรือเทคโนโลยีต่าง ๆ ขององค์กร อันส่งผลทำให้ระบบงานขององค์กรไม่สามารถสนับสนุนการดำเนินธุรกิจ จนส่งผลต่อความล่าช้า หรือหยุดชะงักในการดำเนินธุรกิจขององค์กรได้

2.2.3 การประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นการช่วยให้องค์กรสามารถพิจารณากับเหตุการณ์ที่เกิดขึ้นได้ว่ามีผลกระทบต่อวัตถุประสงค์หรือเป้าหมายที่องค์กรกำหนดไว้หรือไม่ และมีความเสียหายต่อองค์กรมากน้อยเพียงใด โดยประเมินจากเหตุการณ์จาก 2 มุมมอง ซึ่งได้แก่ โอกาสที่เหตุการณ์จะเกิดขึ้น (Likelihood) และผลกระทบของเหตุการณ์ดังกล่าว (Impact) เพื่อให้สามารถวัดระดับความรุนแรงของความเสี่ยงดังกล่าว โดยทั่วไปแล้วการประเมินสามารถใช้ได้ทั้งการประเมินด้วยวิธีการเชิงคุณภาพและเชิงปริมาณร่วมกัน โดยองค์กรจะพิจารณาผลกระทบทั้งในเชิงบวกและเชิงลบจากเหตุการณ์ที่อาจเกิดขึ้น ซึ่งในการประเมินความเสี่ยงต้องอยู่บนพื้นฐานของความเสี่ยงที่มีด้วยกันอยู่ 2 ลักษณะได้แก่

1) ความเสี่ยงที่มีอยู่ตามธรรมชาติ (Inherent Risk) เป็นความเสี่ยงที่เกิดขึ้นกับองค์กร โดยผู้ปฏิบัติงานหรือผู้บริหารยังไม่มีการดำเนินการใด ๆ ในการเปลี่ยนแปลงโอกาสที่จะเกิดความเสี่ยงดังกล่าวหรือลดผลกระทบที่จะเกิดขึ้น

2) ความเสี่ยงที่องค์กรยังคงเหลืออยู่ (Residual Risk) เป็นความเสี่ยงที่ยังคงเหลืออยู่ในองค์กรภายหลังจากที่ผู้ปฏิบัติงานหรือผู้บริหารได้ดำเนินการตอบสนองความเสี่ยงแล้ว

โดยความเสี่ยงที่องค์กรประเมินแล้วนั้น พบว่ามีความเสี่ยงที่มีอยู่ตามธรรมชาติ ซึ่งองค์กรยังไม่ได้มีการควบคุม หรือลดความเสี่ยงนั้นจะสะท้อนให้เห็นว่า องค์กรมีโอกาส หรืออาจได้รับผลกระทบที่เกิดขึ้นจากการเกิดเหตุการณ์ใด ๆ ได้โดยที่องค์กรยังไม่มีการวางแผนการรับมือ หรือป้องกันอย่างเพียงพอ และในส่วนความเสี่ยงที่องค์กรประเมินแล้วพบว่า มีความเสี่ยงคงเหลืออยู่จะสะท้อนให้เห็นถึงความเสี่ยงที่องค์กรยังคงต้องเผชิญอยู่ในปัจจุบัน หลังจากที่ฝ่ายบริหารได้กำหนดมาตรการต่าง ๆ ในการบรรเทาความเสี่ยง และได้ดำเนินการอย่างมีประสิทธิผลแล้ว ซึ่งในบางองค์กรอาจเพิ่มกระบวนการ หรือวิธีการในการตอบสนองความเสี่ยงในอนาคตตามกลยุทธ์ธุรกิจให้อยู่ในมาตรฐานที่องค์กรสามารถยอมรับความเสี่ยงได้

2.2.4 ตอบสนองต่อความเสี่ยง

การที่องค์กรเลือกวิธีการตอบสนองต่อความเสี่ยงที่เกิดขึ้นกับองค์กรได้นั้น องค์กรต้องพิจารณาความเสี่ยงที่เกิดขึ้นจากการประเมินความเสี่ยงที่ได้กล่าวมา ให้อยู่ในเกณฑ์ที่องค์กรสามารถยอมรับได้ (Acceptable Level) ซึ่งการตอบสนองความเสี่ยงสามารถจำแนกเป็นประเภทได้ดังนี้

1) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การยกเลิกกิจกรรมที่ก่อให้เกิดความเสี่ยงกับองค์กรดังกล่าวให้สิ้น ซึ่งการหลีกเลี่ยงดังกล่าวอาจเป็นการสั่งยกเลิก ระงับ หรือแจ้งสิ้นสุดการดำเนินการ เช่น การยกเลิกสัญญาการพัฒนาระบบงานเนื่องจากการที่ผู้ให้บริการไม่สามารถพัฒนาระบบงานตรงตามกลยุทธ์การดำเนินธุรกิจได้

2) การลดความเสี่ยง (Risk Reduction) คือ การกระทำการใด ๆ เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถดำเนินกิจกรรมต่าง ๆ ต่อไปได้

3) การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การลดโอกาสที่จะเกิดความเสี่ยง หรือลดผลกระทบของความเสี่ยงด้วยวิธีการโอนความเสี่ยงบางส่วน หรือทั้งหมดไปให้ผู้รับผิดชอบอื่น เช่น เทคนิคการซื้อประกันภัย (Maintenance Agreement) ศูนย์คอมพิวเตอร์กับผู้ให้บริการในการรับผิดชอบความเสี่ยงหากเกิดความเสียหายกับศูนย์คอมพิวเตอร์ขององค์กร

4) การยอมรับความเสี่ยง (Risk Acceptance) คือ การที่องค์กรไม่กระทำการใด ๆ ที่จะมีผลต่อโอกาสที่เกิดขึ้นความเสี่ยง หรือผลกระทบของความเสี่ยงที่เกิดขึ้น เช่น ค่าใช้จ่ายในการดำเนินการแก้ไขการตั้งค่าความปลอดภัยของระบบงานบางระบบขององค์กร (Configuration) มีมูลค่าสูงกว่ามูลค่าของข้อมูล หรือความสำคัญของระบบงาน ผู้บริหารอาจพิจารณาตามความเหมาะสมในการยอมรับความเสี่ยงดังกล่าว

2.2.5 การควบคุมภายใน

การที่องค์การเลือกวิธีการตอบสนองต่อความเสี่ยงที่เกิดขึ้นให้เหมาะสมกับองค์กรแล้วนั้น จำเป็นต้องมีการควบคุมภายในกิจกรรมต่าง ๆ ขององค์กรให้มีกระบวนการปฏิบัติงานที่มีประสิทธิภาพสอดคล้องกับการดำเนินธุรกิจ สามารถช่วยบริหารจัดการความเสี่ยงที่องค์กรเผชิญอยู่ให้สามารถดำเนินกิจกรรมต่าง ๆ ได้อย่างราบรื่นตามมาตรฐานการบริหารจัดการเพื่อการควบคุมภายในองค์กรที่ดี โดยส่วนงานด้านเทคโนโลยีสารสนเทศสามารถวางแนวทางการปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามแนวทางการควบคุมภายในตามมาตรฐานของสมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditors : IIA) ที่มีการกำหนดประเภทของการควบคุมภายในไว้ 3 ประเภท ได้แก่

1) การควบคุมภายในแบบป้องกัน (Preventive Control) เป็นการควบคุมเพื่อป้องกันหรือลดความเสี่ยงจากความผิดพลาด ความเสียหายจากเหตุการณ์ที่เกิดขึ้น หรือการรักษาความปลอดภัย เช่น กำหนดนโยบาย ระเบียบ หลักเกณฑ์ให้ชัดเจนเป็นลายลักษณ์อักษร การแบ่งแยกหน้าที่การงาน การควบคุมการเข้าถึงทรัพย์สิน เป็นต้น

2) การควบคุมภายในแบบตรวจหา (Detective Control) เป็นการควบคุมโดยทำการตรวจสอบ ตรวจเช็ค ค้นหาข้อผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การติดตาม (Monitor) การสอบทานงาน การสอบยันยอด การตรวจนับพัสดุ การใช้เครื่องมือเทคโนโลยีสารสนเทศทำการตรวจสอบการทำงานของระบบงาน เป็นต้น

3) การควบคุมภายในแบบแก้ไข (Corrective Control) เป็นการควบคุมเพื่อแก้ไขข้อผิดพลาดหรือเหตุการณ์ที่เกิดขึ้นให้ถูกต้อง เพื่อหาแนวทางการแก้ไขปัญหาไม่ให้เกิดข้อผิดพลาดซ้ำอีกภายในองค์กร

2.3 ทฤษฎีมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ

2.3.1 มาตรฐานความมั่นคงปลอดภัย (ISO/IEC 27001)

มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Management System : ISMS) หรือที่เรียกว่ามาตรฐาน ISO/IEC 27001 เป็นการจัดทำมาตรฐานขึ้นเพื่อการรักษาความมั่นคงปลอดภัยให้เทคโนโลยีสารสนเทศ โดยความร่วมมือขององค์การระหว่างประเทศว่าด้วยการมาตรฐาน (the International Organization for Standardization : ISO) และคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอเทคนิกส์ (The International Electrotechnical Commission : IEC) ซึ่งประกอบไปด้วยมาตรฐานต่าง ๆ ซึ่งในปัจจุบันคณะอนุกรรมการด้านความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

โดยกระบวนการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ มีวิธีการปฏิบัติงานในรูปแบบของกิจกรรม ได้แก่ การวางแผน – การปฏิบัติ– การตรวจสอบ – การปรับปรุงแก้ไข (Plan – Do – Check – Act : PDCA) ดังนี้

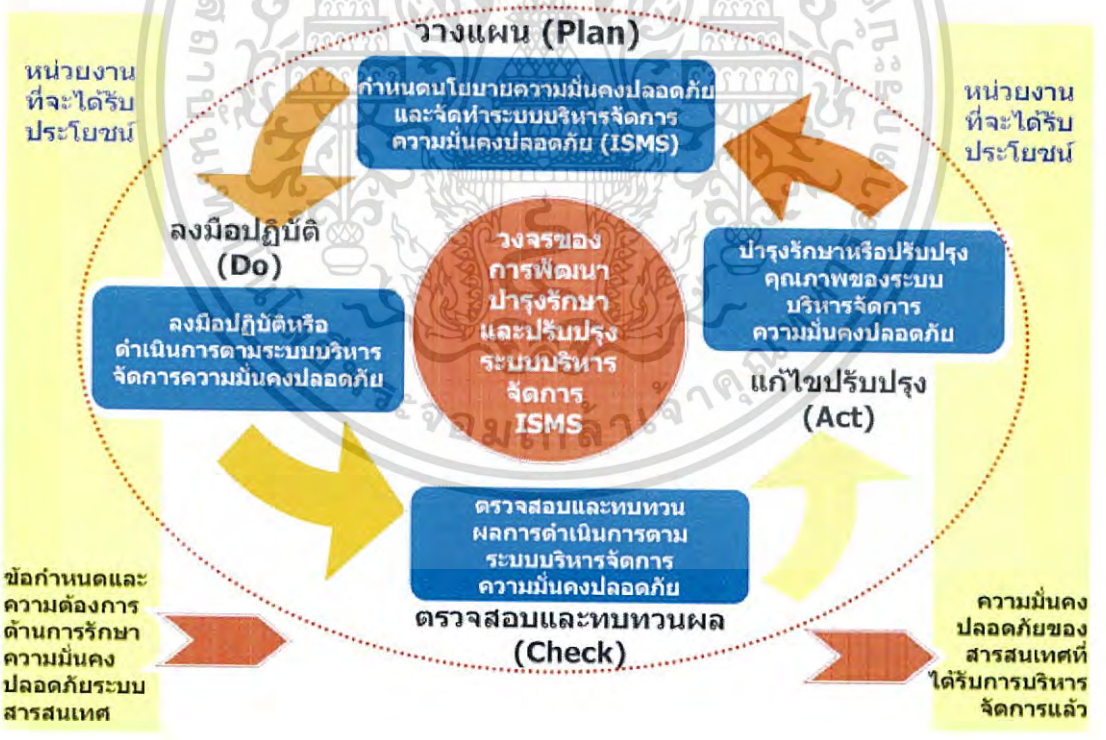
1) การวางแผน (Plan) เป็นกิจกรรมการวางแผนเพื่อดำเนินการตามกระบวนการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ (ISMS) ซึ่งในขั้นตอนแรกองค์กรควรระบุขอบเขต และนโยบายของการสร้างความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กรให้มีความเหมาะสม และทำการประเมินความเสี่ยงตามขอบเขต และนโยบายที่ได้ระบุไว้ เพื่อให้องค์กรนั้นสามารถระบุความเสี่ยงที่องค์กรมีอยู่ในปัจจุบัน และมีแนวโน้มอาจเกิดขึ้นกับองค์กรได้ โดยพิจารณาแนวทางในการจัดการความเสี่ยงดังกล่าว รวมทั้งระบุความเสี่ยงที่หลงเหลือ ให้อยู่ในระดับที่องค์กรยอมรับได้

2) การปฏิบัติ (Do) เป็นการดำเนินการเพื่อจัดการกับความเสี่ยงตามแนวทางจัดการความเสี่ยงที่ได้จากขั้นตอนการวางแผน โดยระบุวิธีการพิจารณาประสิทธิภาพหรือประสิทธิผลของแนวทางจัดการความเสี่ยง และสร้างความตระหนักในการปฏิบัติตามแนวทางจัดการความเสี่ยงเพื่อให้แนวทางจัดการความเสี่ยงดำเนินไปอย่างมีประสิทธิภาพ

3) การตรวจสอบ (Check) เป็นกิจกรรมการเฝ้าระวังแนวทางจัดการความเสี่ยงที่ได้ดำเนินการไปและทำการทบทวนประสิทธิภาพของแนวทางจัดการความเสี่ยงตามที่ได้มีการกำหนดไว้ รวมถึงดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นได้ซ้ำ โดยทำการตรวจสอบกระบวนการตามระยะเวลาที่เหมาะสมและให้สอดคล้องกับการเปลี่ยนแปลงที่สำคัญของเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกิจกรรมใด ๆ ขององค์กร

4) การปรับปรุงแก้ไข (Act) เป็นกิจกรรมของการพัฒนากระบวนการกระบวนการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ (ISMS) ตามผลประเมิน ความเสี่ยง และการตรวจสอบที่ได้รับให้มีการควบคุมที่มีความเหมาะสมด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กร

ซึ่งมีความสัมพันธ์ดังรูป



รูปที่ 2.3 วงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Chcek-Act

ซึ่งจากแผนภาพวงจรการบริหารจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 มีวิธีการในการบริหารจัดการ โดยแบ่งเป็น 11 หัวข้อหลัก (Domain) ดังนี้

1. นโยบายความมั่นคงขององค์กร (Security Policy)

เป็นการกำหนดนโยบายความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศขององค์กร โดยมีวัตถุประสงค์เพื่อกำหนดทิศทางและสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขององค์กร เพื่อให้สอดคล้องและเป็นไปตามข้อกำหนดทางธุรกิจ ระเบียบและวิธีการปฏิบัติที่เกี่ยวข้อง โดยควรจะมีการกำหนดรายละเอียดดังนี้

1.1 การจัดทำเอกสารนโยบายเทคโนโลยีขององค์กรอย่างเป็นลายลักษณ์อักษร (Information security policy document) ซึ่งเอกสารนโยบายฉบับดังกล่าวต้องได้รับการอนุมัติจากผู้บริหาร หรือผู้มีอำนาจลงนามอนุมัติขององค์กรก่อนนำไปใช้งาน และต้องมีการเผยแพร่ ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.2 เอกสารนโยบายเทคโนโลยีสารสนเทศขององค์กรควรมีการกำหนดให้มีทบทวนนโยบายดังกล่าว (Review of the information security policy) โดยผู้บริหารองค์กรต้องดำเนินการทบทวนนโยบายเทคโนโลยีสารสนเทศตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

2. โครงสร้างความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

เป็นการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กร รวมถึงอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่สามารถเข้าถึง ประมวลผล หรือใช้งานในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก โดยมีรายละเอียดดังนี้

2.1 โครงสร้างความมั่นคงปลอดภัยในองค์กร (Internal organization) ผู้บริหารองค์กรต้องให้ความสำคัญและสนับสนุนการบริหารจัดการความมั่นคงปลอดภัย โดยการกำหนดทิศทางการมอบหมายงานที่เหมาะสมกับบุคลากรให้เหมาะสมกับบทบาทหน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กร ทั้งผู้ประสานงานในหน่วยงานต่าง ๆ ผู้ดูแลความมั่นคงปลอดภัยสารสนเทศองค์กร รวมถึงกำหนดกระบวนการอนุมัติการใช้งานประมวลผลสารสนเทศ ข้อตกลงการเปิดเผยความลับขององค์กร ข้อมูลการติดต่อกับหน่วยงานภายนอก และการกำหนดให้มีการตรวจสอบโดยผู้ตรวจสอบอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กรอย่างเหมาะสม

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties) เป็นการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศจากบุคคลหรือหน่วยงานภายนอก ผู้ซึ่งเป็นลูกค้าหรือผู้ให้บริการ เช่น Vendor, Suppler, Outsource เป็นต้น โดยต้องมีการประเมินความเสี่ยงของการเข้าถึงสารสนเทศขององค์กร การกำหนดหรือระบุข้อตกลง

การเข้าถึงก่อนที่องค์กรจะทำการอนุญาตให้สามารถเข้าถึงสารสนเทศขององค์กรให้มีความถูกต้องเหมาะสม

3. การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

เป็นการกำหนดการบริหารจัดการทรัพย์สินขององค์กรให้สามารถจัดจำแนกทรัพย์สิน และความรับผิดชอบตัวตนทรัพย์สิน โดยมีรายละเอียดดังนี้

3.1 การกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) โดยมีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้ โดยควรจัดทำบัญชีทรัพย์สิน และระบุผู้รับผิดชอบทรัพย์สินขององค์กรให้มีความถูกต้องอย่างสม่ำเสมอ

3.2 การจัดหมวดหมู่สารสนเทศ (Information classification) โดยมีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์อย่างเหมาะสม ซึ่งองค์กรควรมีกระบวนการจัดจำแนกหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย หรือระดับความสำคัญที่มีต่อองค์กร รวมถึงการจัดการทรัพย์สินสารสนเทศให้มีความเหมาะสม

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resource security)

เป็นการกำหนดการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กรจากบุคลากรที่สามารถเข้าถึง ใช้งานระบบสารสนเทศขององค์กรได้ โดยมีรายละเอียดดังนี้

4.1 กระบวนการก่อนการว่าจ้างงาน (Prior to employment) มีจุดประสงค์ให้ผู้ที่องค์กรทำสัญญาว่าจ้างไม่ว่าเป็นพนักงาน หรือหน่วยงานภายนอก เข้าใจบทบาทหน้าที่ความรับผิดชอบเพื่อลดความเสี่ยงจากการขโมย ฉ้อโกง และการใช้อุปกรณ์ที่ผิดวัตถุประสงค์ โดยให้กำหนดหน้าที่ความรับผิดชอบให้ชัดเจนเป็นลายลักษณ์อักษร ตรวจสอบคุณสมบัติผู้สมัคร และกำหนดเงื่อนไขการจ้างงานให้เหมาะสม

4.2 กระบวนการระหว่างการจ้างงาน (During employment) มีจุดประสงค์ให้ผู้ที่องค์กรว่าจ้างได้ตระหนักถึงภัยคุกคามและปัญหาความมั่นคงปลอดภัยที่เกี่ยวข้องกับสารสนเทศขององค์กร โดยให้ผู้ที่องค์กรว่าจ้างได้เข้าใจหน้าที่ความรับผิดชอบ และมีความรู้ด้านความมั่นคงปลอดภัย และวินัยลงโทษหากละเมิดนโยบายขององค์กร

4.3 กระบวนการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination or change of employment) มีจุดประสงค์เพื่อให้ผู้ที่องค์กรว่าจ้าง หรือหน่วยงานภายนอกรับทราบหน้าที่ความรับผิดชอบและบทบาทของบุคลกรเมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนแปลง โดยควรมีการคืนทรัพย์สินขององค์กร และการถอดถอนสิทธิการเข้าถึง หรือใช้งานสารสนเทศขององค์กรโดยทันที

5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environmental security)

เป็นการป้องกันการเข้าถึงจากบุคคลภายนอกที่ไม่ได้รับอนุญาต รวมไปถึงป้องกันความเสียหายและการแทรกแซงข้อมูลต่าง ๆ โดยมีรายละเอียดดังนี้

5.1 การกำหนดบริเวณพื้นที่การรักษาความมั่นคงปลอดภัยที่ชัดเจน (Secure Area) เพื่อป้องกันการถึงทางกายภาพโดยไม่ได้รับอนุญาต ก่อให้เกิดความเสียหาย และก่อกวนหรือแทรกแซงต่อทรัพย์สินขององค์กร โดยให้ทำการจัดบริเวณโดยรอบควบคุม ติดตั้งประตูการเข้าออก การป้องกันภัยคุกคามภายนอกและสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น รวมถึงกำหนดกระบวนการปฏิบัติงานในพื้นที่ซึ่งต้องรักษาความมั่นคงปลอดภัย และบริเวณสำหรับการเข้าถึง หรือส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

5.2 การกำหนดความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security) เพื่อป้องกันการสูญหาย ความเสียหาย การขโมย หรือการเปิดเผยโดยไม่ได้รับอนุญาตในทรัพย์สินขององค์กร อันก่อให้เกิดกิจกรรมการดำเนินการต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงักได้ จึงควรให้องค์กรมีการจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงในการเข้าถึงที่ไม่ได้รับอนุญาต การทำให้ระบบและอุปกรณ์สนับสนุนการทำงานมีกลไกการป้องกันการล้มเหลว เช่น กระแสไฟฟ้า ประปา ระบบระบายอากาศ ไฟฟ้าสำรอง เป็นต้น รวมถึงการเดินสายไฟ สายสื่อสาร สายเคเบิ้ลให้มีความปลอดภัยลดอุปสรรคการต่อสายสัญญาณ และมีการบำรุงรักษาอุปกรณ์ ป้องกันอุปกรณ์ที่ใช้งานอยู่ภายนอกสำนักงานให้มีสภาพสมบูรณ์พร้อมใช้งาน และการจัดการกับอุปกรณ์ที่ต้องนำกลับมาใช้อีกครั้ง หรือนำทรัพย์สินออกนอกสำนักงานให้มีการอนุญาตเพื่อการจัดการที่ถูกต้องและสมควร

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and operations management)

เป็นการกำหนดแนวทางในการปฏิบัติงานและการสื่อสารเพื่อเพิ่มความปลอดภัยของอุปกรณ์สารสนเทศขององค์กร การบริหารจัดการและการสื่อสารกับผู้ปฏิบัติงานขององค์กร โดยมีรายละเอียดดังนี้

6.1 การกำหนดบทบาทหน้าที่และความรับผิดชอบในการปฏิบัติงาน (Operational procedures and responsibilities) โดยมีจุดประสงค์เพื่อให้สามารถดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย ตั้งแต่การกำหนดขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร วิธีการควบคุมการเปลี่ยนแปลง ระบบหรืออุปกรณ์ประมวลผลสารสนเทศ รวมถึงการแบ่งหน้าที่ความรับผิดชอบ และแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน เพื่อลดความเสี่ยงจากการเข้าถึง เปลี่ยนแปลง และการดำเนินการที่ต้องได้รับอนุญาตอย่างเหมาะสม

6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management) โดยมีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่ของหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก ตั้งแต่การกำหนดมารฐานการรักษาความปลอดภัย การตรวจสอบติดตามการให้บริการของหน่วยงานภายนอกอย่างสม่ำเสมอ รวมถึงการปรับปรุงการบริหารจัดการของหน่วยงานภายนอกให้เป็นไปตามเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับสารสนเทศขององค์กร

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance) โดยมีจุดประสงค์เพื่อลดความเสี่ยงที่เกิดจากความล้มเหลวของระบบให้น้อยที่สุด โดยองค์กรควรมีการวางแผนความต้องการทรัพยากรสารสนเทศของอนาคตให้เหมาะสม (Capacity Management) และทำการเตรียมการที่ดีในการตรวจรับระบบงาน (System Acceptance) ซึ่งจะเป็นส่วนช่วยสร้างความมั่นใจเกี่ยวกับความเพียงพอของของทรัพยากรขององค์กรได้

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code) โดยมีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายจากโปรแกรมที่ไม่ประสงค์ดี ซึ่งองค์กรจำเป็นต้องมีมาตรการตรวจจับ ป้องกัน และกู้คืนเพื่อป้องกันทรัพย์สินสารสนเทศ รวมถึงสร้างควรตระหนักให้กับผู้ใช้งานทราบเกี่ยวกับภัยคุกคามจากโปรแกรมที่ไม่ได้ประสงค์ดี และทำการป้องกันโปรแกรมชนิดเคลื่อนที่ (mobile code) เพื่อควบคุมการทำงานของโปรแกรมชนิดเคลื่อนที่ดังกล่าวไม่ให้สมารถทำงานหรือใช้งานเคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งไปอีกในเครื่องอื่นในองค์กร จนเกิดความเสียหาย

6.5 การสำรองข้อมูล (Back up) มีจุดประสงค์เพื่อรักษาความถูกต้อง สมบูรณ์ และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลขององค์กร ซึ่งองค์กรต้องมีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และเป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6.6 การบริหารจัดการความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management) มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานสารสนเทศขององค์กร ซึ่งองค์กรต้องมีการบริหารและจัดการเครือข่ายเพื่อป้องกันภัยคุกคาม และดูแลรักษาความมั่นคงปลอดภัยระบบงานที่มีการใช้งานผ่านระบบเครือข่าย ซึ่งต้องกำหนดคุณสมบัติด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับการบริการเครือข่ายทั้งหมดที่องค์กรมีการใช้บริการ

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling) มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และการชะงักหรือหยุดให้บริการทางธุรกิจ ซึ่งองค์กรควรมีกำหนดขั้นตอนการปฏิบัติงานเพื่อการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ และกำจัดสื่อบันทึกข้อมูล

ที่ไม่จำเป็นใช้งานหรือมีความจำเป็นต้องทำลายให้มีความมั่นคงปลอดภัย และการกำหนดมาตรฐานการป้องกันการเข้าถึงเอกสารต่าง ๆ โดยไม่ได้รับอนุญาต เช่น อุปกรณ์จัดเก็บข้อมูล (เทป, ดิสก์)

6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information) มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันทั้งภายในองค์กร และภายนอกองค์กร โดยองค์กรควรมีการกำหนดนโยบาย ขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนสารสนเทศภายใน และระหว่างองค์กร โดยทำข้อตกลงอย่างเป็นลายลักษณ์อักษร รวมถึงการกำหนดวิธีการป้องกันการส่งสื่อบันทึกข้อมูลออกไปนอกหน่วยงานโดยไม่ได้รับอนุญาต หรือใช้งานผิดวัตถุประสงค์ทำให้เกิดความเสียหายระหว่างการส่งข้อมูลออกภายนอก ตลอดต้องมีการกำหนดมาตรการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์ หรือระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกันให้มีความปลอดภัยในการแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างองค์กรที่ดี

6.9 การสร้างความมั่นคงปลอดภัยสำหรับการบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services) มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ และความปลอดภัยของการใช้งาน โดยองค์กรต้องมีการกำหนดมาตรการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ใด ๆ ที่องค์กรมีการทำธุรกิจ หรือมีการส่งผ่านข้อมูลทางเครือข่ายสาธารณะให้มีความปลอดภัยมากที่สุดจากการถูกฉ้อโกง ปฏิเสธ เปิดเผย เปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมถึงการทำธุรกรรมออนไลน์ต้องมีการป้องกันการส่งข้อมูลบนเครือข่ายที่ผิดพลาด หรือเปิดเผยออกสู่สาธารณะให้มีการควบคุมความปลอดภัย ความถูกต้องสมบูรณ์ของการทำธุรกรรมพาณิชย์อย่างเหมาะสม

6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring) มีจุดประสงค์เพื่อควบคุมติดตามกิจกรรมการประมวลสารสนเทศที่ไม่เหมาะสม ซึ่งองค์กรต้องมีการบันทึกเหตุการณ์การใช้งานสารสนเทศ (Audit logging) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ และมีการกำหนดขั้นตอนการปฏิบัติเพื่อการตรวจสอบการใช้งานระบบ หรือการใช้งานทรัพย์สินสารสนเทศ เช่น การตรวจสอบสิ่งผิดปกติของการใช้งาน รวมถึงมีการป้องกันข้อมูลบันทึกเหตุการณ์เพื่อเป็นการป้องกันการเปลี่ยนแปลงแก้ไขที่ไม่ได้รับอนุญาต บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้อง เช่น ผู้ดูแลระบบงาน เป็นต้น และมีการบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศไว้อย่างครบถ้วน เพื่อสามารถนำไปใช้วิเคราะห์ข้อผิดพลาด และแก้ไขการดำเนินการได้ตามความเหมาะสม ตลอดจนองค์กรต้องมีการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกันโดยต้องอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบ ติดตามหากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยกับสารสนเทศขององค์กรได้

7. การควบคุมการเข้าถึง (Access Control)

เป็นกิจกรรมเพื่อให้มั่นใจว่าผู้ใช้งานมีการควบคุมการเข้าถึงและระบบสารสนเทศต้องมีการป้องกันการเข้าถึงอย่างเหมาะสม โดยมีรายละเอียดดังนี้

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) โดยองค์กรควรมีการกำหนดนโยบายการควบคุมการเข้าถึงสารสนเทศขององค์กรตามความต้องการทางธุรกิจและความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่สมควร

7.2 การบริหารจัดการการเข้าถึงสารสนเทศของผู้ใช้งาน (User access management) มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยองค์กรควรมีการกำหนดขั้นตอนอย่างเป็นทางการเพื่อลงทะเบียนพนักงานให้มีสิทธิการใช้งานสารสนเทศขององค์กรตามความจำเป็น และมีการควบคุม จำกัดสิทธิการใช้งานระบบของผู้ใช้งานที่ได้รับสิทธิเฉพาะ (Privilege) รวมถึงมีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความเหมาะสม เพื่อควบคุมจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมั่นคงปลอดภัย ตลอดจนองค์กรควรมีกระบวนการในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างเป็นทางการตามระยะเวลาที่องค์กรกำหนด

7.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศขององค์กร โดยไม่ได้รับอนุญาต หรือเปิดเผย ขโมย ดักรับ แก้ไขสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศอย่างไม่ถูกต้อง โดยองค์กรต้องมีการกำหนดการใช้งานรหัสผ่าน (Password use) ในการเลือกและใช้งานรหัสผ่านความปลอดภัย มีการกำหนดวิธีการป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์หรือสารสนเทศใด ๆ ที่ไม่มีพนักงานดูแล รวมถึงควรมีนโยบายเพื่อควบคุมป้องกันมิให้มีการปล่อยทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ไม่ปลอดภัย เช่น ในบริเวณสาธารณะ โดยไม่มีการควบคุมใด ๆ เป็นต้น

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control) มีจุดประสงค์เพื่อป้องกันการถึงการให้บริการของระบบเครือข่ายโดยไม่ได้รับอนุญาต โดยองค์กรต้องมีการกำหนดนโยบายการใช้งานระบบเครือข่ายขององค์กรให้ผู้ใช้งานที่ได้รับอนุญาตสามารถใช้งานได้ และมีกลไกการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กรที่มีความประสงค์เชื่อมต่อระบบเครือข่ายขององค์กร รวมถึงมีการป้องกันช่องทางของระบบเครือข่าย เช่น พอร์ต (Port) ต่าง ๆ ของระบบสารสนเทศขององค์กรให้มีความปลอดภัยและมีการตรวจสอบ ปรับแต่งระบบเครือข่ายให้มีความเหมาะสมมีการป้องกันภัยคุกคามและผู้ไม่ได้รับอนุญาต ตลอดจนมีการแบ่งแยกเครือข่ายตามกลุ่มของการบริการสารสนเทศที่ใช้งาน หรือกลุ่มของผู้ใช้งานให้มีความเหมาะสมจากผู้ใช้งานภายในและหน่วยงานภายนอก และต้องมีการควบคุมการเชื่อมต่อทางเครือข่ายโดยต้องมีการจำกัดผู้ใช้งาน

ในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรให้เป็นไปตามนโยบายและข้อกำหนดที่แอปพลิเคชันระบุไว้ ตลอดจนควบคุมการกำหนดเส้นทางบนเครือข่ายสารสนเทศให้เป็นไปตามนโยบายการควบคุมการเข้าถึงขององค์กร

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยองค์กรควรมีการกำหนดขั้นตอนการปฏิบัติงานในการเข้าถึงระบบปฏิบัติการให้มั่นคงปลอดภัย (Secure log-on procedures) และมีการระบุพิสูจน์ตัวตนของผู้ใช้งานก่อนเข้าถึงระบบงาน มีการบริหารจัดการรหัสผ่านให้มีคุณภาพและปลอดภัย รวมถึงมีการจำกัดการใช้งานและควบคุมโปรแกรมประเภทอรรถประโยชน์ (System Utilities) ของผู้ใช้งานให้ทำการติดตั้งโปรแกรมด้วยตนเอง เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงการปฏิบัตินโยบายข้อกำหนดที่องค์กรกำหนดไว้ รวมทั้งองค์กรต้องมีการกำหนดการหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out) เพื่อตัดการเชื่อมต่อหรือใช้งานของผู้ใช้งานที่ไม่มีการใช้งานระบบมาระยะเวลาหนึ่งให้มีความเหมาะสม และควรมีการจำกัดระยะเวลาการในการเชื่อมต่อกับระบบงานที่มีความสำคัญสูงขององค์กร

7.6 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and information access control) มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอปพลิเคชันโดยไม่ได้รับอนุญาต ซึ่งองค์กรควรมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันงานต่าง ๆ ของแอปพลิเคชั่นโดยแยกตามประเภทของผู้ใช้งาน รวมถึงมีการแบ่งแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่มีการกำหนดไว้อย่างเหมาะสม

7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking) มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและสามารถปฏิบัติงานจากภายนอกได้ โดยองค์กรต้องทำการกำหนดนโยบายควบคุมหรือป้องกันอุปกรณ์พกพา เช่น Notebook, Palm และ smartphone เป็นต้น ต้องกำหนดมาตรฐานในการป้องกันความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ รวมถึงการกำหนดนโยบายขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่ต้องปฏิบัติงานจากภายนอกสำนักงาน

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

เป็นกิจกรรมเพื่อให้มั่นใจว่าองค์กรมีการจัดหา พัฒนาและบำรุงรักษาระบบสารสนเทศขององค์กรอย่างต่อเนื่องและเหมาะสม โดยมีรายละเอียดดังนี้

8.1 การกำหนดความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information system) มีจุดประสงค์เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศขององค์กรโดยต้องมีการพิจารณาความมั่นคงปลอดภัยเป็นข้อกำหนดพื้นฐานเบื้องต้นในการจัดหาและพัฒนา ซึ่งจำเป็นต้องมีการวิเคราะห์ และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบ

สารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบงานที่องค์มีอยู่แล้วให้มีหลักเกณฑ์ที่ชัดเจน และเหมาะสม

8.2 การประมวลสารสนเทศในแอปพลิเคชั่น (Correct processing in application) มีจุดประสงค์เพื่อป้องกันความผิดพลาดของระบบสารสนเทศ ทำให้ข้อมูลสูญหาย หรือมีการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือใช้งานผิดวัตถุประสงค์ โดยองค์กรต้องมีการตรวจสอบข้อมูลนำเข้า ให้มีความถูกต้องการนำไปประมวลผล และมีการตรวจสอบข้อมูลที่อยู่ระหว่างประมวลผลให้มีความถูกต้อง ไม่ให้เกิดข้อผิดพลาดระหว่างการดำเนินการประมวลผลสารสนเทศ รวมถึงมีการกำหนดกลไกตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชั่น เพื่อให้สามารถยืนยันได้ว่าเป็นข้อความที่ถูกต้อง มีการป้องกันการเปลี่ยนแปลงอย่างเหมาะสม และมีการตรวจสอบข้อมูลที่ส่งออกเพื่อทบทวนการประมวลผลของสารสนเทศให้เป็นไปอย่างถูกต้องทั้งแอปพลิเคชั่น

8.3 การควบคุมการเข้ารหัสข้อมูล (Cryptographic controls) มีจุดประสงค์เพื่อรักษาความลับของข้อมูล และมีการยืนยันตัวตนของผู้ส่งข้อมูล หรือมีความถูกต้องสมบูรณ์โดยใช้วิธีการเข้ารหัสข้อมูล ซึ่งองค์กรควรมีการกำหนดนโยบายการเข้ารหัสข้อมูลเพื่อควบคุมการใช้งานไฟล์เอกสารในองค์กร และมีการบริหารจัดการกุญแจการเข้ารหัส และการถอดรหัส (Key management) โดยมีกลไกที่เป็นเทคนิคการเข้ารหัสข้อมูลตามมาตรฐานขององค์กรให้มีความมั่นคงปลอดภัยให้มากที่สุด

8.4 การจัดการความมั่นคงปลอดภัยของไฟล์เอกสารระบบสารสนเทศ (Security of system files) มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยของไฟล์เอกสารต่าง ๆ บนระบบสารสนเทศ โดยองค์กรต้องมีขั้นตอนการปฏิบัติงานเพื่อการควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศขององค์กร ซึ่งจะช่วยลดความเสี่ยงที่ทำให้ระบบเสียหาย หรือเกิดข้อผิดพลาดจากซอฟต์แวร์ดังกล่าว รวมถึงมีการป้องกันข้อมูลที่ใช้สำหรับการทดสอบโดยให้หลีกเลี่ยงการนำข้อมูลที่ใช้งานจริงมาทดสอบ หากมีความจำเป็นต้องมีการควบคุมป้องกันข้อมูลที่เป็นความลับข้อมูลส่วนตัว หรือข้อมูลที่สำคัญขององค์กรอย่างเหมาะสม และมีการควบคุมการเข้าถึงซอร์สโค้ดของระบบงานเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตจนส่งผลต่อการทำงานของระบบสารสนเทศ

8.5 การจัดการความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes) มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และระบบสารสนเทศขององค์กร โดยองค์กรควรมีการกำหนดขั้นตอนการปฏิบัติงานสำหรับความคุมการเปลี่ยนแปลงหรือแก้ไขระบบงาน และควรมีการกำหนดการตรวจสอบการทำงานของแอปพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ และควรหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต รวมถึงควรมีการกำหนดมาตรการ

เพื่อป้องกันการรั่วไหลของสารสนเทศองค์กร อีกทั้งต้องมีการกำหนดวิธีการควบคุม ติดตามการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management) มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ โดยองค์กรต้องมีมาตรการควบคุมช่องโหว่ทางเทคนิคในระบบงานสารสนเทศต่าง ๆ ที่องค์กรมีการใช้งาน ด้วยวิธการติดตามข้อมูลข่าวสาร หรือประเมินความเสี่ยงของช่องโหว่อย่างสม่ำเสมอ

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

เป็นกิจกรรมเพื่อให้มั่นใจว่าเหตุการณ์ความมั่นคงปลอดภัยที่มีส่วนเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศมีการสื่อสารและการจัดการอย่างทันเหตุการณ์อย่างถูกต้อง และเหมาะสม โดยมีรายละเอียดดังนี้

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses) มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม โดยองค์กรต้องมีการกำหนดให้พนักงาน หรือผู้องค์กรว่าจ้างทั้งภายในและภายนอก ต้องมีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่องค์กรกำหนดไว้ให้มีการดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ และต้องมีการบันทึก รายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบเทคโนโลยีสารสนเทศหรือการให้บริการที่องค์กรดำเนินการอยู่อย่างทันที

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements) มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร โดยองค์กรต้องทำการกำหนดหน้าที่ความรับผิดชอบในการรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรอย่างรวดเร็ว และได้ผล มีระเบียบที่ดี รวมถึงต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยควรมีการพิจารณาประเภทของเหตุการณ์ ปริมาณ ค่าใช้จ่ายที่เกิดขึ้น เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เคยเกิดขึ้นกับองค์กร และเตรียมป้องกันไว้ล่วงหน้าได้ ตลอดจนองค์กรต้องมีการเก็บรวบรวมหลักฐานสำหรับการอ้างอิงในกระบวนการทางกฎหมายในอนาคตได้

10. การบริหารความต่อเนื่องในการดำเนินธุรกิจขององค์กร (Business continuity management)

เป็นการดำเนินการกิจกรรมเพื่อป้องกันการหยุดชะงักการดำเนินธุรกิจ และการป้องกันกิจกรรมที่สำคัญขององค์กรจากผลกระทบที่อาจส่งผลต่อระบบสารสนเทศขององค์กร โดยสามารถให้นำกลับมาใช้งานได้ในเวลาที่เหมาะสม ซึ่งมีรายละเอียดดังนี้

10.1 การรักษาความปลอดภัยข้อมูลเพื่อการจัดการความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) มีจุดประสงค์เพื่อป้องกันการติดขัดหรือหยุดชะงักกิจกรรมต่าง ๆ ของการดำเนินธุรกิจที่สำคัญ อันเป็นผลมาจากความล้มเหลวหรือสร้างความเสียหายต่อระบบสารสนเทศ ให้สามารถทำการกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม โดยองค์กรควรกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ มีการบริหารจัดการและการปรับปรุงกระบวนการอย่างสม่ำเสมอ มีการประเมินความเสี่ยงโดยต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจหยุดชะงัก หรือมีโอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ และจัดทำแผนในการสร้างความต่อเนื่องให้กับธุรกิจ ซึ่งควรมีการกำหนดกรอบการวางแผนเพื่อการสร้างความต่อเนื่องให้กับความมั่นคงปลอดภัยของธุรกิจ และจัดลำดับความสำคัญของงานต่าง ๆ ที่ต้องดำเนินการ รวมถึงควรมีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้มีแผนงานมีความทันสมัยและได้ผลเป็นอย่างดี

11. การปฏิบัติตามข้อกำหนด (Compliance)

เป็นกิจกรรมขององค์กรเพื่อให้มั่นใจว่าองค์กรได้ปฏิบัติตามกฎหมาย หรือหน่วยงานกำกับต่าง ๆ อย่างเคร่งครัด ซึ่งมีรายละเอียดดังนี้

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirement) มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบ ข้อกำหนดทางด้านความมั่นคงปลอดภัย โดยองค์กรต้องทำการระบุข้อกำหนดกฎหมาย ระเบียบต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจขององค์กรเป็นลายลักษณ์อักษร และมีการปรับปรุงข้อกำหนดให้ทันสมัยอยู่เสมอ และต้องมีการกำหนดขั้นตอนการปฏิบัติเพื่อป้องกันการละเมิดสิทธิและทรัพย์สินทางปัญญา รวมถึงป้องกันข้อมูลที่เกี่ยวข้องกับทางกฎหมาย ข้อมูลความเป็นส่วนตัว และการใช้งานอุปกรณ์ประมวลผลสารสนเทศที่ผิดวัตถุประสงค์ ตลอดจนข้อกำหนดในการใช้มาตรการการเข้ารหัสข้อมูลโดยยึดถือ ปฏิบัติให้สอดคล้องกับข้อกฎหมายให้มีความถูกต้องเหมาะสม

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance) มีจุดประสงค์เพื่อให้ระบบงานสารสนเทศเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร โดยองค์กรควรมีการกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน

ผู้ใต้บังคับบัญชาให้ปฏิบัติตามขั้นตอนทางด้านการรักษาความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบ และมีการตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กรอย่างสม่ำเสมอ

11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations) มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้การหยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด โดยองค์กรควรมีการระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการดำเนินธุรกิจ และควรมีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศเพื่อป้องกันการใช้งานที่ผิดวัตถุประสงค์ หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

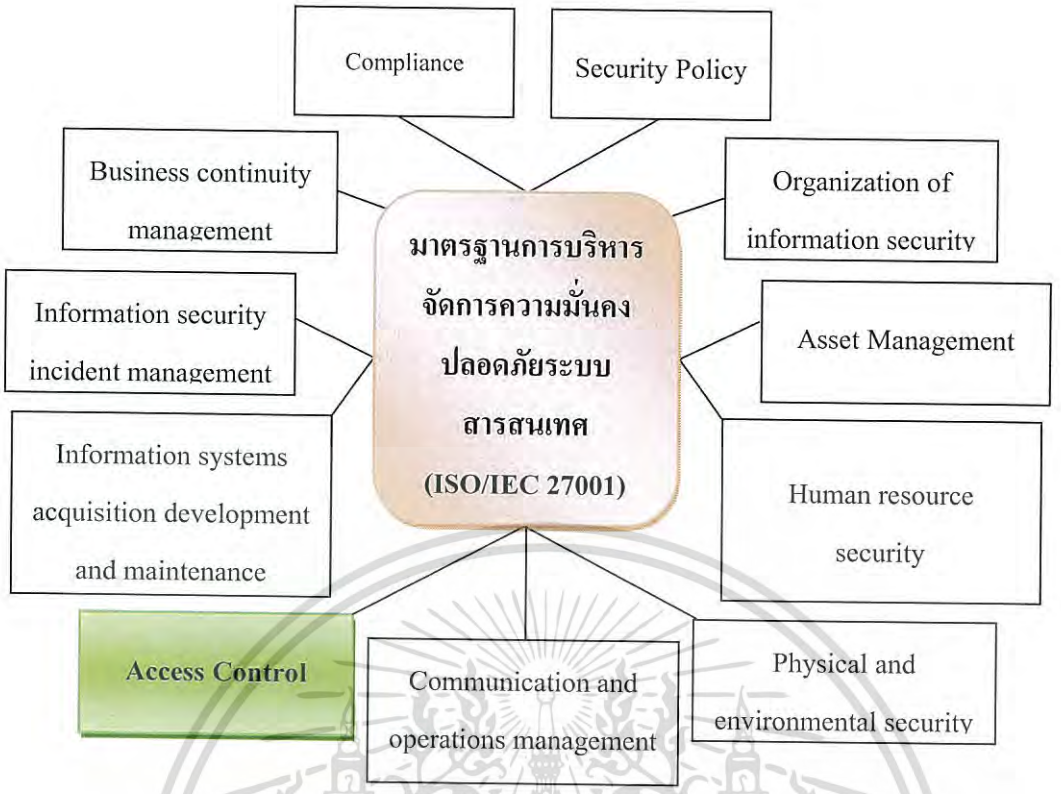
บทที่ 3
วิธีการศึกษาโครงการ

3.1 วิธีการนำเสนอ (Methodology)

วิธีการนำเสนอ ผู้ศึกษาโครงการพิจารณานำมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) ซึ่งมีการระบุข้อควรปฏิบัติในการดำเนินการเพื่อให้ได้มาซึ่งความมั่นคงปลอดภัยของการใช้งานเทคโนโลยีสารสนเทศ และสอดคล้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ที่มีมาตรฐานการรักษาความมั่นคงปลอดภัยขององค์กร โดยมีขั้นตอนการดำเนินการศึกษาโครงการ ดังนี้

3.1.1 ศึกษาค้นคว้าทฤษฎี งานวิจัย มาตรฐานที่เกี่ยวข้อง

ผู้ศึกษาโครงการทำการค้นคว้าทฤษฎี งานวิจัย มาตรฐานที่เกี่ยวข้องข้องกับความเสี่ยงและการควบคุมภายใน ซึ่งเป็นมาตรฐานของการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่ดี (Good Or Best Practices) ให้กับองค์กรศึกษา เช่น กฎหมาย ระเบียบ ข้อบังคับของหน่วยงานกำกับองค์กรศึกษา อาทิ พระราชกฤษฎีกา ประกาศธนาคารแห่งประเทศไทย และมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เนื่องจากเป็นนโยบายด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์เป็นผู้กำหนดไว้ (Policy Maker) ว่าด้วยการกำหนดแนวนโยบายการบริหารจัดการให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยในการ ประกอบธุรกรรมทางอิเล็กทรอนิกส์ โดยทำการศึกษาค้นคว้าเพื่อสร้างแบบจำลองการควบคุมภายในเฉพาะขอบเขตเรื่องการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) เพื่อประยุกต์ใช้ในการควบคุมภายในการบริหารจัดการองค์กรศึกษาให้ทำงานได้อย่างมีประสิทธิภาพ และมีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอยู่ในมาตรฐานที่องค์กรยอมรับความเสี่ยงได้



รูปที่ 3.1 มาตรฐาน ISO/IEC 27001 ในขอบเขตเรื่อง Access Control

3.1.2 ศึกษากระบวนการปฏิบัติงานและระบบสารสนเทศขององค์กรศึกษา

ผู้ศึกษาโครงการทำการเก็บรวมรวมข้อมูลขององค์กร ซึ่งเป็นสถาบันการเงิน (ธนาคารพาณิชย์) แห่งหนึ่งของประเทศไทยจากเอกสาร การสัมภาษณ์ สอบทาน สังเกตการณ์ กระบวนการปฏิบัติงานและวิธีการบริหารจัดการระบบสารสนเทศขององค์กรศึกษา เช่น การกำหนดนโยบาย หลักเกณฑ์ แนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศขององค์กร การระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงวิธีการกำหนดความมั่นคงปลอดภัยของการเข้าถึง ใช้งานเทคโนโลยีสารสนเทศและอุปกรณ์สารสนเทศต่าง ๆ ขององค์กร ในส่วนของระบบงานที่เป็นธุรกรรมอิเล็กทรอนิกส์ของกลุ่มตัวอย่าง (Sampling System) ได้แก่ ระบบงานเงินฝาก

3.1.3 กำหนดขอบเขตการจัดการความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

ผู้ศึกษาโครงการทำการกำหนดขอบเขตการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) และเกณฑ์ที่ใช้ในการบริหารความเสี่ยงซึ่งต้องเป็นไปตามกลยุทธ์การดำเนินธุรกิจขององค์กรซึ่งเป็นสถาบันการเงิน (ธนาคารพาณิชย์) ในประเทศไทย โดยทำการศึกษาขอบเขตในด้านการเข้าถึงระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ดังนี้

ตารางที่ 3.1.3 ขอบเขตการจัดการความมั่นคงปลอดภัย Access Control

หัวข้อ	ขอบเขตการศึกษาด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศซึ่งเป็นธุรกรรมอิเล็กทรอนิกส์ของธนาคาร	รายละเอียดการจัดทำแบบจำลองตามมาตรฐาน ISO/IEC 27001
1	**ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) เพื่อควบคุมการเข้าถึงสารสนเทศ**	
	1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	ธนาคารควรกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ
2.	**การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)**	
	2.1 การลงทะเบียนพนักงาน (User registration)	ธนาคารควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น
	2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	ธนาคารควรจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน
	2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	ธนาคารควรจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย
	2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	ธนาคารควรจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

ตารางที่ 3.1.3 (ต่อ)

หัวข้อ	ขอบเขตการศึกษาด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศซึ่งเป็นธุรกรรมอิเล็กทรอนิกส์ของธนาคาร	รายละเอียดการจัดทำแบบจำลองตามมาตรฐาน ISO/IEC 27001
3.	**หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต**	
	3.1 การใช้งานรหัสผ่าน (Password use)	ธนาคารควรกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน
	3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)	ธนาคารควรมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล
4.	**การควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต**	
	4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	ธนาคารควรจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้
	4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	ธนาคารควรกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้
	4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	ธนาคารควรกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ซึ่งได้รับอนุญาตแล้ว
	4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	ธนาคารควรมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

ตารางที่ 3.1.3 (ต่อ)

หัวข้อ	ขอบเขตการศึกษาด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศซึ่งเป็นธุรกรรมอิเล็กทรอนิกส์ของธนาคาร	รายละเอียดการจัดทำแบบจำลองตามมาตรฐาน ISO/IEC 27001
	4.5 การแบ่งแยกเครือข่าย (Segregation in networks)	ธนาคารควรทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ
	4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	ธนาคารควรจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจ
	4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	ธนาคารควรกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง
5.	**การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต**	
	5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	ธนาคารควรจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ
	5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	ธนาคารควรจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ
	5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)	ธนาคารควรจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ
	5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	ธนาคารควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

ตารางที่ 3.1.3 (ต่อ)

	5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	ธนาคารควรกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้
	5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	ธนาคารควรจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง
6	**การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control) เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต**	
	6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	ธนาคารควรจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน
	6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	ธนาคารควรแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ
7.	**การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking) เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**	
	7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	ธนาคารควรกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้
	7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	ธนาคารควรกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

3.1.4 สำรวจเกณฑ์การยอมรับความเสี่ยงการบริหารจัดการความมั่นคงปลอดภัยขององค์กรศึกษา

ผู้ศึกษาโครงการทำการสอบถามเกณฑ์การยอมรับความเสี่ยงด้านการบริหารจัดการข้อมูลสารสนเทศ ด้วยวิธีการเก็บข้อมูลจากแบบสอบถามผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญการควบคุมภายในสารสนเทศ เพื่อให้ทราบกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรที่อยู่ในมาตรฐานที่องค์กรยอมรับได้ โดยการผสมผสานระหว่างวิธีการเชิงคุณภาพและเชิงปริมาณ โดยทำการสำรวจเกณฑ์การยอมรับความเสี่ยงจำแนกเป็นเกณฑ์เพื่อสร้างแบบจำลองมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศเพื่อให้ทราบระดับความเสี่ยงที่องค์กรยอมรับได้ด้วยเทคนิคเชิงปริมาณ หรือมีการประเมินความเสี่ยงด้วยเกณฑ์เชิงคุณภาพเพื่อกำหนดให้สอดคล้องกับความเสี่ยงตามกลยุทธ์ขององค์กรศึกษา

3.1.5 จัดทำแบบจำลองมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

ผู้ศึกษาโครงการทำการสร้างแบบจำลองการประเมินความเสี่ยง และการควบคุมภายในการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศจากโมเดลจากมาตรฐาน ISO/IEC 27001 ประกอบด้วยการใช้เทคนิคการประเมินผลเชิงปริมาณ เพื่อวัดค่าผลการบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กรศึกษา มาตรฐานจากแบบจำลองดังกล่าวว่า องค์กรกรณีศึกษาโครงการมีการบริหารจัดการความมั่นคงปลอดภัยอยู่ในระดับที่องค์กรยอมรับความเสี่ยงได้

3.1.6 สำรวจการบริหารจัดการด้านเทคโนโลยีสารสนเทศในปัจจุบัน (ก่อนทำโครงการ)

ผู้ศึกษาโครงการทำการสอบถามด้วยวิธีการเก็บข้อมูลจากแบบสอบถามการบริหารจัดการด้านเทคโนโลยีสารสนเทศในปัจจุบัน (ก่อนทำโครงการ) ซึ่งเป็นไปตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001)

3.1.7 ประเมินการควบคุมภายในและความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

ผู้ศึกษาโครงการทำการประเมินการควบคุมภายในจากแบบสอบถาม เอกสารแนบคำชี้แจงที่ได้รับการตอบกลับ การรวบรวมข้อมูล โดยประยุกต์ใช้กับแบบจำลองที่ได้พัฒนาตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีในปัจจุบันจากเทคนิคความน่าจะเป็น (Probabilistic) ซึ่งเป็นการประเมินความเสี่ยงจากโอกาสและผลกระทบ ประกอบด้วยการผสมผสานระหว่างเทคนิคการประเมินผลความเสี่ยงและการควบคุมภายในเชิงคุณภาพเพื่อจำแนกประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กร หรือใช้ในกรณีที่ไม่สามารถวัดเป็น

ปริมาณได้ หรือไม่สามารถหาข้อมูลที่น่าเชื่อถือได้เพียงพอสำหรับการประเมินความเสี่ยงเชิงปริมาณ

3.1.8 กำหนดแนวทางจัดการความเสี่ยง ตามผลการการประเมินความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

ผู้ศึกษาโครงการกำหนดแนวทางการจัดการความเสี่ยง โดยพิจารณาตามหลักการควบคุมภายใน และวิธีการตอบสนองความเสี่ยง เช่น การหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การถ่ายโอนความเสี่ยง และการยอมรับความเสี่ยง เป็นต้น โดยสามารถจำแนก ระบุความเสี่ยงที่เป็นจุดอ่อนที่สำคัญ เพื่อการตอบสนองความเสี่ยงที่สำคัญให้อยู่ในเกณฑ์ที่องค์กรยอมรับความเสี่ยงได้

3.1.9 ประเมินการควบคุมภายในและความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

ผู้ศึกษาโครงการทำการประเมินการควบคุมภายในจากแบบสอบถามที่ได้รับการตอบกลับหลังทำโครงการ เปรียบเทียบกับการควบคุมภายใน (ก่อนทำโครงการ) และมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่หลงเหลือในองค์กรศึกษา จากเทคนิคความน่าจะเป็น (Probabilistic) ซึ่งเป็นการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศจากโอกาสและผลกระทบ ซึ่งต้องมีค่าความเสี่ยงรวมน้อยกว่าการประเมินความเสี่ยงก่อนทำโครงการ รวมถึงความเสี่ยงต้องอยู่ในเกณฑ์ที่องค์กรยอมรับความเสี่ยงได้

3.1.10 สรุปผลการศึกษาโครงการ

ผู้ศึกษาโครงการทำการสรุปผลแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ ให้มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีวิธีประเมินความเสี่ยงจากแบบจำลอง ตามแนวทางที่องค์กรควรดำเนินการปฏิบัติให้สอดคล้องกับการบวนการปฏิบัติงาน หรือการบริหารจัดการจากผู้ที่เกี่ยวข้อง (Stakeholder) อย่างเหมาะสม รวมถึงเป็นไปตามกฎหมาย ระเบียบ หรือข้อบังคับจากหน่วยงานภายนอก และนโยบาย หลักเกณฑ์ ระเบียบปฏิบัติของภายในองค์กรอย่างเหมาะสมและมีความเพียงพอ

รูปที่ 3.2 วิธีการนำเสนอโครงการ (Methodology)

3.2 เครื่องมือที่ใช้ในการศึกษาโครงการ

3.2.1 เครื่องมือที่ใช้ในการศึกษาโครงการด้วยเทคนิคเชิงปริมาณ

เป็นการใช้เครื่องมือในการประเมินความเสี่ยงเชิงปริมาณนั้น ผู้ศึกษาใช้เป็นเครื่องมือช่วยในการประเมินความเสี่ยง และการควบคุมภายในขององค์กรศึกษาเพื่อใช้เป็นแนวทางให้องค์กรสามารถชี้วัด และเห็นถึงโอกาส หรือปัจจัยอันจะทำให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศตลอดจนอาจส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร ซึ่งทำให้การดำเนินธุรกิจขององค์กรเกิดความล่าช้า ขัดข้อง หรืออาจหยุดชะงักได้ โดยเทคนิคการใช้งานเครื่องมือเชิงปริมาณ ได้แก่

- **การใช้เทคนิคการประเมินความน่าจะเป็น (Probabilistic)** ของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้วยการใช้เทคนิคของการคำนวณมูลค่าของความเสียหาย จากโอกาสของการเกิดเหตุการณ์ความเสี่ยง และผลกระทบที่คาดว่าจะได้รับ มาคำนวณเพื่อหาความน่าจะเป็นของการเกิดเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ดังนี้

$$\text{Risk Value} = \text{Likelihood} \times \text{Impact} \tag{3.2}$$

เมื่อ Likelihood คือ โอกาสที่จะเกิดเหตุการณ์

และ Impact คือ ผลกระทบของเหตุการณ์

ตารางที่ 3.2.1.1 เทคนิคการประเมินความน่าจะเป็นตาม Risk Value

Risk Value = Likelihood x Impact			โอกาสการเกิดความเสี่ยง (Likelihood)				
			น้อยที่สุด / ต่ำที่สุด	น้อย / ต่ำ	ปานกลาง	สูง / บ่อย	สูงมาก / บ่อยมาก
			1	*2*	*3*	*4*	*5*
ผลกระทบ (Impact)	มากที่สุด	*5*	5	10	15	20	25
	มาก	*4*	4	8	12	16	20
	ปานกลาง	*3*	3	6	9	12	15
	น้อย	*2*	2	4	6	8	10
	น้อยที่สุด	*1*	1	2	3	4	5

เกณฑ์ที่ใช้ในการประเมินโอกาสการเกิดความเสี่ยง (Likelihood) แบ่งเป็นระดับคะแนนได้ดังนี้

โอกาสเกิดน้อยที่สุด = 1
โอกาสเกิดน้อย = 2
โอกาสเกิดปานกลาง = 3
โอกาสเกิดสูง = 4
โอกาสเกิดสูงมาก = 5

และเกณฑ์ที่ใช้ในการประเมินผลกระทบหรือความเสียหายที่ได้รับ (Impact) แบ่งเป็นระดับคะแนนได้ดังนี้

ผลกระทบน้อยที่สุด = 1
ผลกระทบน้อย = 2
ผลกระทบปานกลาง = 3
ผลกระทบสูง = 4
ผลกระทบสูงมาก = 5

ตารางที่ 3.2.1.2 ระดับการประเมินความเสี่ยง (Risk Rating)

ระดับการประเมินความเสี่ยง (Risk Rating)		
ระดับคะแนนความเสี่ยงจากการประเมินผล	เกณฑ์ความเสี่ยง	การตอบสนองความเสี่ยง
1-8	ต่ำ	เป็นระดับความเสี่ยงที่องค์กรสามารถยอมรับได้
9-16	ปานกลาง	เป็นระดับความเสี่ยงที่องค์กรควรมีมาตรการควบคุมหรือลดความเสี่ยงให้ไปอยู่ในระดับที่องค์กรยอมรับได้
17-25	สูง	เป็นระดับความเสี่ยงที่องค์กรควรมีมาตรการจัดการอย่างเร่งด่วน เพื่อลดความเสี่ยง หรือยกเลิกการดำเนินกิจกรรมที่ทำ เพื่อให้องค์กรมีการบริหารจัดการที่ดีมากยิ่งขึ้น

3.2.2 เครื่องมือที่ใช้ในการศึกษาโครงการด้วยเทคนิคเชิงคุณภาพ

เป็นการใช้เครื่องมือในการประเมินโดยใช้ดุลพินิจ และบางอย่างมีการประเมินภายใต้พื้นฐานของความเป็นจริงก็ตาม แต่คุณภาพของการประเมินนั้นขึ้นอยู่กับความรู้และการตัดสินใจของบุคคลเป็นอย่างมาก รวมถึงความเข้าใจต่อเหตุการณ์ที่เกิดขึ้น ตลอดจนสภาพแวดล้อมและการเปลี่ยนแปลงที่เกิดขึ้นตลอดเวลา ได้แก่

- **การจำแนกความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรให้สอดคล้องกับความเสี่ยงขององค์กรหรือตามที่หน่วยงานกำกับกำหนด** เช่น แนวทางการกำกับตรวจสอบความเสี่ยง (Risk-base supervision) ของธนาคารแห่งประเทศไทยเพื่อเป็นแนวทางให้ธนาคารพาณิชย์ใช้ในการปฏิบัติงานและเพื่อเกิดความเข้าใจที่ตรงกันระหว่างสถาบันการเงินและธนาคารแห่งประเทศไทยในการประเมินความเสี่ยงของสถาบันการเงิน โดยผู้ใช้งานจำเป็นต้องพิจารณาด้วยการใช้เทคนิคคุณภาพ เพื่อพิจารณาความเสี่ยงโดยใช้ดุลพินิจหรือวิจารณญาณความเสี่ยงที่ตรวจพบ ได้แก่

ตารางที่ 3.2.2 การจำแนกความเสี่ยงตามเกณฑ์ธนาคารแห่งประเทศไทย

ความเสี่ยง	
ความเสี่ยงด้านกลยุทธ์	ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งแผลกระทบต่อรายได้ เงินกองทุน หรือความดำรงอยู่ของกิจการ
ความเสี่ยงด้านเครดิต	โอกาสหรือความน่าจะเป็นที่คู่สัญญาไม่สามารถปฏิบัติตามภาระที่ตกลงไว้ รวมถึงโอกาสที่คู่ค้าจะถูกปรับลดอันดับ ความเสี่ยงด้านเครดิต ซึ่งอาจส่งผลกระทบต่อรายได้และเงินกองทุนของสถาบัน
ความเสี่ยงด้านตลาด	ความเสี่ยงที่เกิดจากการเคลื่อนไหวของอัตราดอกเบี้ย อัตราแลกเปลี่ยนเงินตราต่างประเทศ และราคาตราสารในตลาดเงินตลาดทุน ที่มีผลกระทบในทางลบต่อรายได้และเงินกองทุนของสถาบันการเงิน

ตารางที่ 3.2.2 (ต่อ)

ความเสี่ยง	
ความเสี่ยงด้านสภาพคล่อง	ความเสี่ยงที่เกิดจากการที่สถาบันการเงินไม่สามารถชำระหนี้สินและภาระผูกพันเมื่อถึงกำหนด เนื่องจากไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดได้ หรือไม่สามารถจัดหาเงินทุนได้เพียงพอ หรือสามารถหาเงินมาชำระได้แต่ต้นทุนที่สูงเกินกว่าระดับที่ยอมรับได้ ซึ่งอาจส่งผลกระทบต่อรายได้และเงินกองทุนของสถาบันการเงิน
ความเสี่ยงด้านปฏิบัติการ	ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กร และการขาดการควบคุมที่ดี โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายในคน ระบบงาน หรือเหตุการณ์ภายนอกและส่งผลกระทบต่อรายได้และเงินกองทุนของสถาบันการเงิน

บทที่ 4
กรณีศึกษาองค์กรปัจจุบัน

4.1 ข้อมูลเบื้องต้นของกรณีศึกษา

องค์กรที่ทำการศึกษาเป็นสถาบันการเงิน (ธนาคารพาณิชย์) แห่งหนึ่งของประเทศไทย มีสำนักงานให้บริการเทคโนโลยีสารสนเทศ (Data center) อยู่ใจกลางถนนสุขุมวิท โดยได้เปิดบริการเป็นธนาคารพาณิชย์เมื่อ พ.ศ. 2548 ซึ่งการดำเนินการธุรกิจธนาคารพาณิชย์ของกรณีศึกษาแห่งนี้ดำเนินกิจกรรมทางธุรกิจด้านเงินฝาก เช่น ออมทรัพย์ ประจำ ตั๋วแลกเงิน (BE) เป็นต้น และกิจกรรมด้านการให้สินเชื่อที่มีการดำเนินธุรกิจ (Core Business) ในการให้สินเชื่อเฉพาะด้านมุ่งเน้นตลาดที่สามารถเข้าถึงลูกค้าได้สะดวกตามความเชี่ยวชาญการดำเนินการธุรกิจของแต่ละธนาคาร ซึ่งเป็นกลยุทธ์การดำเนินธุรกิจขององค์กรศึกษานี้มุ่งเน้นกลุ่มลูกค้าสินเชื่อ ได้แก่ สินเชื่อเช่าซื้อ (Hire Purchase) สินเชื่อธุรกิจอสังหาริมทรัพย์ (Real Estate) สินเชื่อฟลอแพลน (Floor Plan) เป็นต้น โดยทุกส่วนงานขององค์กรศึกษามีการใช้งานเทคโนโลยีสารสนเทศมาเป็นส่วนช่วยสนับสนุนกิจกรรมการดำเนินธุรกิจ ซึ่งทางธนาคารให้การสนับสนุนการลงทุนด้านเทคโนโลยี การพัฒนาระบบงานเพื่อใช้งานให้ตอบโจทย์การดำเนินธุรกิจการกลยุทธ์ของธนาคารให้มากที่สุด ไม่ว่าจะเป็นการจัดซื้อจัดหาเทคโนโลยี การจัดจ้างพัฒนาระบบงาน โดยองค์กรมีการกำหนดส่วนงานสายเทคโนโลยีสารสนเทศเพื่อทำหน้าที่บริหารจัดการอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายขององค์กรให้มีการทำงานที่ถูกต้อง เหมาะสมอยู่เสมอ โดยองค์กรให้ความสำคัญการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นอย่างยิ่ง เนื่องจากเป็นระบบเทคโนโลยีสารสนเทศที่สามารถรองรับการทำธุรกรรมอิเล็กทรอนิกส์ให้กับลูกค้าของธนาคาร ซึ่งหากเกิดเหตุการณ์เสียหายอาจส่งผลกระทบต่อภาพลักษณ์ด้านชื่อเสียงของธนาคารได้ รวมทั้งหากเกิดเหตุการณ์ระบบสารสนเทศล่าช้า หรือหยุดชะงัก อันจะทำให้พนักงานไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพส่งผลต่อการบริการอันทำให้ลูกค้าไม่พึงพอใจได้เช่นกัน ซึ่งการที่มีสายเทคโนโลยีสารสนเทศช่วยสนับสนุนการทำงานของผู้ปฏิบัติงานต่าง ๆ ตั้งแต่ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และเจ้าหน้าที่ปฏิบัติที่มีความต้องการแตกต่างกันในการใช้งาน และความต้องการเพื่อการตอบสนองการทำงานตามกลยุทธ์ของธนาคารในแต่ละระดับชั้น ทำให้สายเทคโนโลยีสารสนสนเทศเป็นส่วนงานหนึ่งที่มีความสำคัญกับการดำเนินธุรกิจธนาคารพาณิชย์เพื่อให้มีการปฏิบัติงานที่ถูกต้อง น่าเชื่อถือ และอำนวยความสะดวกให้ลูกค้าได้อย่างรวดเร็วอีกด้วย ส่งผลให้หน่วยงานกำกับธนาคารพาณิชย์ อาทิ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เริ่มเล็งเห็นและให้ความสำคัญกับการกำกับการดำเนินงานของสายเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย มีความโปร่งใส มีความถูกต้องของข้อมูล

สามารถตรวจสอบกระบวนการต่าง ๆ ด้านเทคโนโลยีสารสนเทศได้ทุกขั้นตอนส่งผลต่อและความน่าเชื่อถือของธนาคารได้

4.2 โครงสร้างองค์กร และโครงสร้างสายเทคโนโลยีสารสนเทศ

4.2.1 โครงสร้างองค์กรกรณีศึกษา (Organization chart)

โครงสร้างขององค์กรศึกษานั้นมีการจัดแบ่งโครงสร้างเป็นสายงานต่าง ๆ ให้มีการทำงานร่วมกันเพื่อขับเคลื่อนการดำเนินการธุรกิจธนาคารพาณิชย์ให้มีประสิทธิภาพ ได้แก่

1. กลุ่มการบริหารและปฏิบัติงานธนาคาร (First Line) เป็นส่วนงานที่ทำหน้าที่ตั้งแต่การวางกลยุทธ์การดำเนินการธุรกิจ ขับเคลื่อนยุทธวิธีนำกลยุทธ์ไปใช้งาน และการปฏิบัติงานให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งประกอบด้วยส่วนงานต่าง ๆ ดังนี้

- คณะกรรมการธนาคาร อันประกอบด้วยคณะกรรมการบริหาร ซึ่งทำหน้าที่ในการกำหนดกลยุทธ์ขององค์กรให้มีการบริหารจัดการที่ดี มีความยุติธรรม ถูกต้อง โปร่งใส และให้มีความมั่นคงมีผลตอบแทนที่ดีกับผู้ถือหุ้น ซึ่งในกลุ่มดังกล่าวนี้จะประกอบด้วยผู้บริหารระดับสูงในการทำหน้าที่บริหารจัดการธนาคาร

- ส่วนงาน Front office ที่ทำหน้าติดต่อกับลูกค้า ทั้งลูกค้าที่เป็นบุคคลและลูกค้าที่เป็นภาคธุรกิจในด้านการทำธุรกรรมด้านการเงิน เช่น การฝาก ถอน โอนเงินเป็นต้น และด้านการทำธุรกรรมสินเชื่อ เช่น ขอกู้ Refinance เร่งรัด ฟ้องดำเนินคดี เป็นต้น

- กลุ่มของส่วนงาน Back Office ที่ทำหน้าที่สนับสนุนการปฏิบัติงานขององค์กรให้มีประสิทธิภาพ ซึ่งประกอบด้วยส่วนงาน อาทิ สายทรัพยากรบุคคล สายปฏิบัติการ สายการเงินและงบประมาณ สายสำนักกฎหมาย และสายเทคโนโลยีสารสนเทศ ซึ่งทำหน้าที่การบริหารจัดการการดำเนินธุรกิจกิจการของธนาคารให้เป็นไปอย่างสะดวก รวดเร็ว ถูกต้อง

2. กลุ่มการกำกับดูแล ติดตามการบริหารและปฏิบัติงานธนาคาร (Second Line) เป็นส่วนที่ทำหน้าที่ในการประเมินผล ควบคุม ติดตามความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบกับองค์กรให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ และให้สอดคล้องหรือเป็นไปตามกฎเกณฑ์ กฎระเบียบของหน่วยงานกำกับ อันประกอบด้วย

- คณะกรรมการบริหารความเสี่ยง/กำกับการปฏิบัติตามกฎเกณฑ์ กำหนดนโยบายต่อคณะกรรมการธนาคารเพื่อพิจารณาในเรื่องของการบริหารความเสี่ยงโดยรวมของธนาคารและบริษัทในกลุ่มธุรกิจทางการเงิน ซึ่งต้องครอบคลุมถึงความเสี่ยงประเภทต่าง ๆ ที่สำคัญ เช่น ความเสี่ยงด้านเครดิต ความเสี่ยงด้านตลาด ความเสี่ยงด้านสภาพคล่อง ความเสี่ยงด้านปฏิบัติการ เป็นต้น รวมถึงกำกับดูแลให้ธนาคารมีการปฏิบัติตามกฎหมาย กฎเกณฑ์ ข้อบังคับมาตรฐานแนวทางปฏิบัติที่บังคับใช้กับธุรกรรมต่าง ๆ ของธนาคาร เช่น ธนาคารแห่งประเทศไทย เป็นต้น

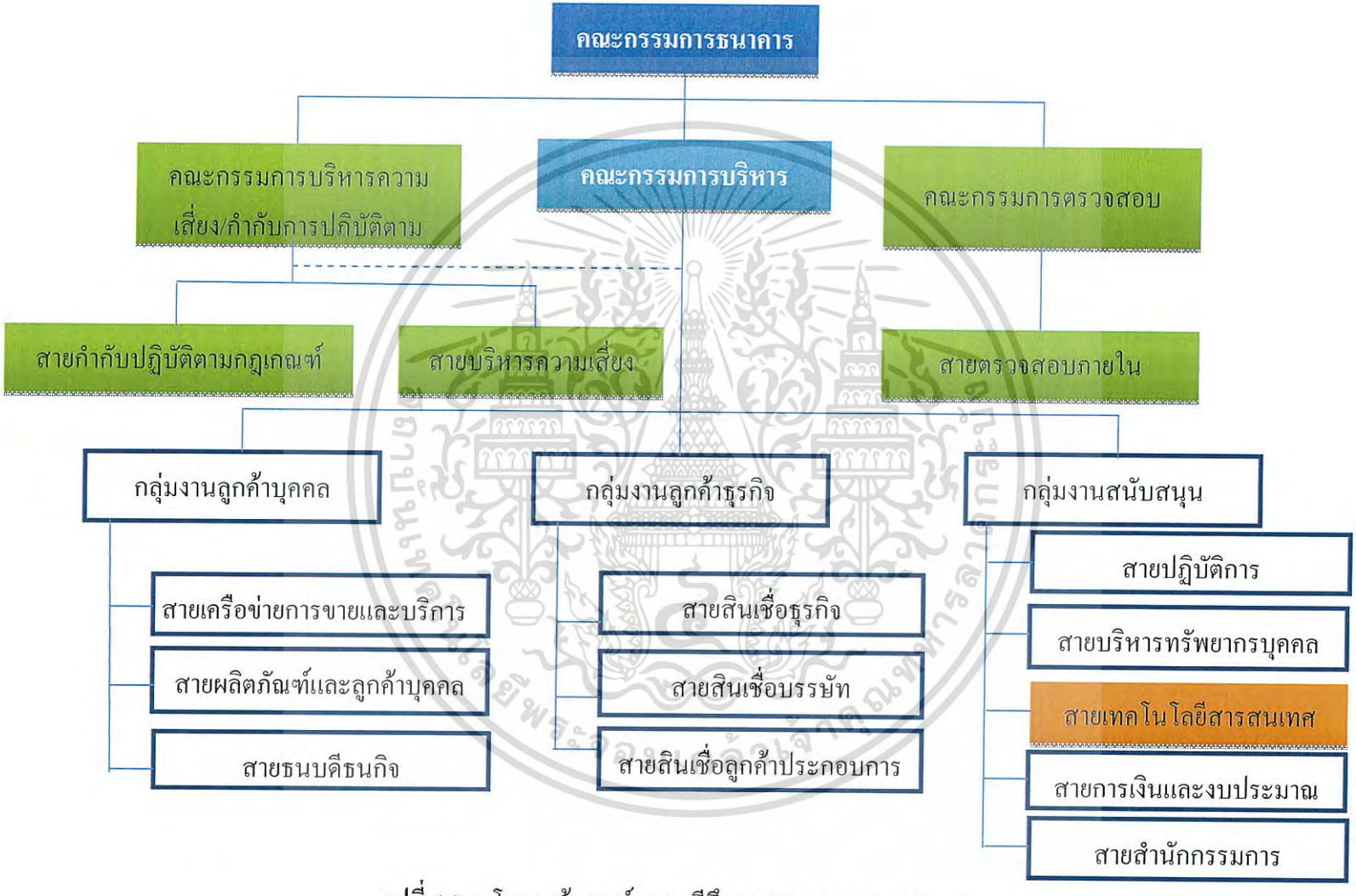
- กลุ่มงานการบริหารความเสี่ยง (Risk) ทำหน้าที่บริหารความเสี่ยงของธนาคาร โดยการประเมินติดตามผล และกับดูแลปริมาณความเสี่ยงของธนาคารให้อยู่ในระดับที่เหมาะสม และรายงานผลการปฏิบัติงานให้คณะกรรมการบริหารความเสี่ยงทราบอย่างสม่ำเสมอ

- กลุ่มงานการกำกับปฏิบัติตามกฎเกณฑ์ (Compliance) ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎเกณฑ์ และกำกับดูแลกิจการ (Good Governance) ให้มีประสิทธิภาพ และมีความเป็นอิสระสอดคล้องกับข้อปฏิบัติตามกฎหมาย กฎเกณฑ์ ข้อบังคับมาตรฐานแนวทางปฏิบัติของหน่วยงานกำกับที่บังคับใช้กับธุรกรรมต่าง ๆ ของธนาคาร

3. กลุ่มการตรวจสอบการควบคุมภายในการบริหารจัดการงานธนาคาร (Third Line) เป็นส่วนที่มีหน้าที่สอบทานให้ธนาคารมีรายงานทางการเงินอย่างถูกต้องและเพียงพอ มีระบบการควบคุมภายใน (Internal Control) ที่ดีส่งผลต่อภาพรวมของธนาคารที่ต้องมีข้อมูลที่ถูกต้อง โปร่งใส สามารถตรวจสอบได้ทุกขั้นตอน ซึ่งประกอบด้วย

- คณะกรรมการตรวจสอบ มีหน้าที่กำหนดการตรวจสอบ สอบทานให้รายงานทางการเงินของธนาคารมีความถูกต้องและเพียงพอ รวมถึงการกำหนดระบบการควบคุมภายใน และระบบการตรวจสอบภายในให้มีความเหมาะสมเพื่อลดโอกาส ความเสี่ยงของการทุจริต หรือการปฏิบัติงานที่ไม่เหมาะสม ตลอดจนความถูกต้องของข้อมูลภายในธนาคารเป็นสำคัญ

- กลุ่มงานตรวจสอบภายใน มีหน้าที่ตรวจสอบ สอบทาน ตรวจเช็คกระบวนการสำหรับการบริหารจัดการภายในธนาคารตั้งแต่การปฏิบัติงาน หน้าที่ความรับผิดชอบ ตลอดจนระบบงานเทคโนโลยีสารสนเทศของธนาคารซึ่งเป็นสิ่งสำคัญที่เป็นเครื่องมือที่สนับสนุนการทำธุรกรรมทางการเงิน รายงานข้อมูลต่าง ๆ ของธนาคารให้มีความถูกต้อง แม่นยำและมีความเหมาะสมสอดคล้องกับการตอบสนองความต้องการในการดำเนินการกิจกรรมของสถาบันการเงิน ซึ่งอาจประกอบด้วยผู้ตรวจสอบภายในหลากหลายประเภท เช่น ส่วนงานตรวจสอบกระบวนการปฏิบัติงานทั่วไป ส่วนงานตรวจสอบสาขาธนาคาร ส่วนสอบทานสินเชื่อตามเกณฑ์ธนาคารแห่งประเทศไทย และส่วนงานตรวจสอบเทคโนโลยีสารสนเทศ เป็นต้น



รูปที่ 4.2.1 โครงสร้างองค์กรกรณีศึกษา (Organization Chart)

4.2.2 โครงสร้างส่วนงานเทคโนโลยีสารสนเทศ

สายเทคโนโลยีสารสนเทศ เป็นส่วนงานที่ทำหน้าที่สนับสนุนการดำเนินธุรกิจของธนาคารพาณิชย์ให้สามารถขับเคลื่อนไปด้วยระบบเทคโนโลยีสารสนเทศให้มีความรวดเร็ว สะดวกสบาย ซึ่งสายเทคโนโลยีสารสนเทศประกอบด้วยฝ่ายงานต่าง ๆ ดังนี้

1) ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศ ทำหน้าที่จัดทำนโยบาย ระเบียบ หลักเกณฑ์การบริหารจัดการด้านเทคโนโลยีสารสนเทศของธนาคารให้มีความถูกต้องเหมาะสม รวมถึงกำกับควบคุม ติดตามการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องให้สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศขององค์กรและเป็นไปตามมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ดี

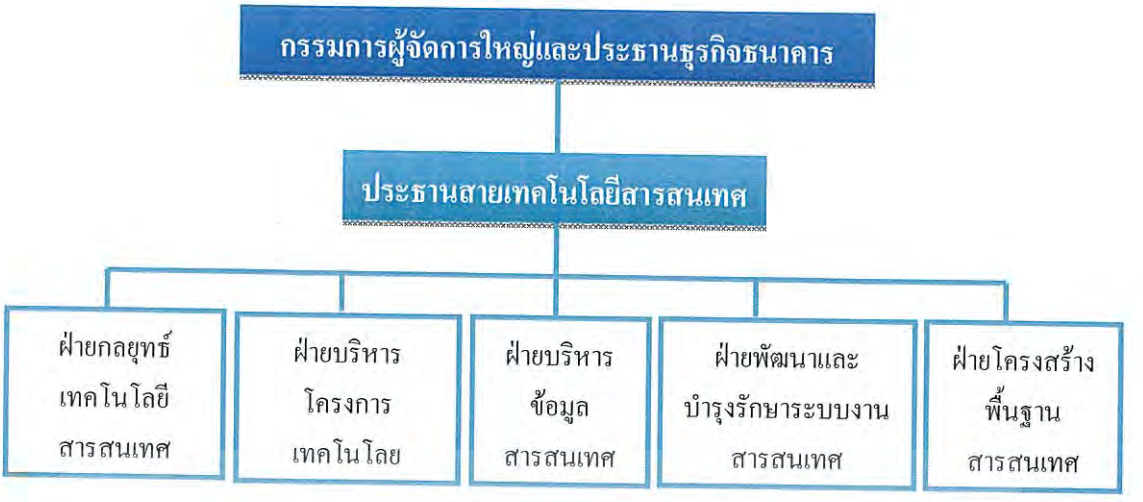
2) ฝ่ายบริหารโครงการเทคโนโลยีสารสนเทศ ทำหน้าที่บริหารโครงการเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนงานหนึ่งที่ต้องทำงานร่วมกับส่วนงานพัฒนาระบบงานและผลิตภัณฑ์ (Project Management) ในการร่วมให้ความคิดเห็น เป็นคณะทำงานเพื่อให้ความคิดเห็นด้านเทคโนโลยีสารสนเทศขององค์กร

3) ฝ่ายบริหารข้อมูลสารสนเทศ ทำหน้าที่บริหารข้อมูลต่าง ๆ เพื่อสนับสนุนผู้บริหารขององค์กรในการใช้งานข้อมูลสนับสนุนการตัดสินใจ เช่น รายงานระบบสารสนเทศเพื่อการบริหาร (Management Information System : MIS Report) , รายงานระบบงาน Business Intelligent เป็นต้น ตลอดจนการบริหารจัดการข้อมูลเพื่อแจ้งให้กับหน่วยงานกำกับภายนอกทราบตามที่กฎหมายกำหนด เช่น รายงานธุรกรรมการฟอกเงินจากการโอนเงินหรือชำระเงินทางอิเล็กทรอนิกส์ให้สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) เป็นต้น

4) ฝ่ายพัฒนาและบำรุงรักษาระบบงานสารสนเทศ ทำหน้าที่ในการบำรุงรักษาระบบงานสารสนเทศต่าง ๆ ของธนาคารให้สามารถสนับสนุนการทำงานได้อย่างต่อเนื่อง ไม่ส่งผลกระทบต่อการดำเนินธุรกิจของธนาคาร เช่น ระบบงานด้านเงินฝาก ระบบงานด้านสินเชื่อ ระบบงาน Internet Banking เป็นต้น

5) ฝ่ายโครงสร้างพื้นฐานสารสนเทศ ทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เช่น ระบบเครือข่าย ศูนย์คอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และฐานข้อมูลของธนาคาร เป็นต้น ให้สามารถทำงานได้อย่างต่อเนื่อง และมีการป้องกันความมั่นคงปลอดภัยในการเข้าถึงอย่างเหมาะสม

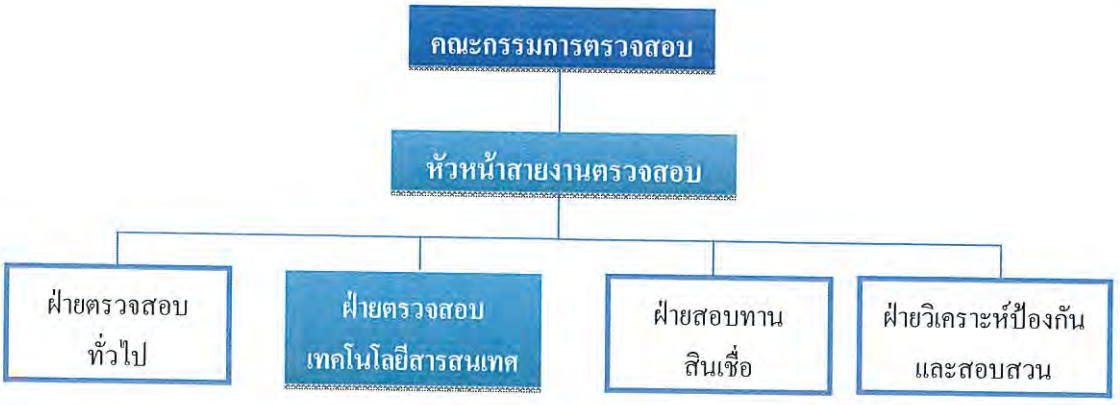
ซึ่งจากโครงสร้างสายงานเทคโนโลยีสารสนเทศที่มีการกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการในแต่ละส่วนงานให้สามารถรองรับ สนับสนุนการดำเนินธุรกิจของธนาคารให้มีความถูกต้องเหมาะสม สนับสนุนการปฏิบัติงานได้อย่างรวดเร็ว สามารถอธิบายได้จากแผนภาพโครงสร้างสายงานเทคโนโลยีสารสนเทศ ดังนี้



รูปที่ 4.2.2 โครงสร้างส่วนงานเทคโนโลยีสารสนเทศ

4.2.3 โครงสร้างส่วนงานตรวจสอบเทคโนโลยีสารสนเทศ

การตรวจสอบภายในเป็นกิจกรรมที่ให้ความเชื่อมั่นแก่ธนาคาร อย่างมีอิสระและเที่ยงธรรม รวมทั้งการให้คำปรึกษาหารือเพื่อเพิ่มคุณค่าปรับปรุงการปฏิบัติงานของธนาคาร ให้ดียิ่งขึ้น และจะช่วยให้ธนาคารบรรลุวัตถุประสงค์ได้ โดยการนำวิธีการที่เป็นระบบและใช้หลักวิชาการในการประเมินและปรับปรุงประสิทธิภาพ วิธีการในเรื่องการบริหารความเสี่ยง การควบคุม และการกำกับดูแล ซึ่งการตรวจสอบเทคโนโลยีสารสนเทศนั้นเป็นสิ่งสำคัญอย่างมากในการให้การช่วยเหลือผู้ปฏิบัติงานทุกระดับของธนาคารให้สามารถปฏิบัติงานหน้าที่ได้อย่างมีประสิทธิภาพจากการใช้งานระบบงานเทคโนโลยีสารสนเทศขององค์กรที่มีการทำงานที่ถูกต้อง ตลอดจนหน่วยงานเทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลรับผิดชอบระบบงานเทคโนโลยีสารสนเทศของธนาคาร สามารถทราบการประเมินความเพียงพอของการปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามมาตรฐานสากล หรือการดำเนินการสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับของหน่วยงานกำกับที่กำหนด เช่น ระเบียบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ เป็นต้น รวมถึงสามารถสร้างความมั่นใจและความน่าเชื่อถือการดำเนินธุรกิจของธนาคารให้กับลูกค้า (Customer) หรือผู้มีส่วนได้ส่วนเสีย (Stakeholder) ว่าธนาคารมีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อประมวลผลข้อมูลที่มีความถูกต้อง โปร่งใส สามารถตรวจสอบได้ ซึ่งเป็นพื้นฐานของระบบเทคโนโลยีสารสนเทศที่ดีมาใช้ในการสนับสนุนการขับเคลื่อนธุรกิจของธนาคาร



รูปที่ 4.2.3 โครงสร้างองค์กรส่วนตรวจสอบเทคโนโลยีสารสนเทศ

4.3 ความสอดคล้องของการกำหนดเป้าหมายองค์กรและเทคโนโลยีสารสนเทศ

องค์กรศึกษาเป็นธนาคารพาณิชย์ ขนาดกลางมีหน่วยงานฝ่ายวางแผนกลยุทธ์และธุรกิจ ซึ่งเป็นหน่วยงานสำคัญที่ทำหน้าที่ในการกำหนดแผนกลยุทธ์การดำเนินธุรกิจของธนาคารให้สามารถขับเคลื่อน และสร้างความได้เปรียบทางการแข่งขันเหนือธนาคารพาณิชย์อื่น ๆ ในอันดับของสถาบันการเงินที่อยู่ในระดับเดียวกัน และสามารถก้าวไปสู่ตลาดการแข่งขันของสถาบันการเงินขนาดใหญ่ได้ โดยการกำหนดแผนการดำเนินกลยุทธ์ของธนาคารกรณีศึกษามีการจัดทำแผนระยะยาวทุก 5 ปี ซึ่งในปัจจุบันมีการจัดทำการวางแผนกลยุทธ์ทางธุรกิจฉบับปี 2555-2559 ตั้งแต่การกำหนดวิสัยทัศน์ (Vision) พันธกิจ (Mission) โดยมีใจความสำคัญที่เกี่ยวกับการบริหารจัดการองค์กรให้มีธรรมาภิบาลที่ดี (Corporate Governance) โดยองค์กรกรณีศึกษามุ่งเน้นการบริการให้กับลูกค้าให้มีความถูกต้อง ส่งเสริมความสำเร็จให้กับลูกค้าที่มาใช้บริการกับธนาคาร รวมถึงผู้มีส่วนได้ส่วนเสียขององค์กรศึกษา (Stakeholder) ต้องมีการปฏิบัติงานที่ดี โปร่งใส สะท้อนภาพลักษณ์ และประโยชน์ต่อสังคม

ซึ่งนอกจากมีการกำหนดกลยุทธ์ขององค์กรศึกษาให้ดำเนินการตามหลักของธรรมาภิบาลองค์กรที่ดีแล้วนั้น การกำหนดแผนกลยุทธ์ของหน่วยงานเทคโนโลยีสารสนเทศ ก็มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดี (Information Technology Governance) สอดคล้องกับการดำเนินการขององค์กรศึกษาด้วย โดยควรมีการกำหนดแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ได้แก่ การบริหารจัดการกระบวนการทำงานด้านเทคโนโลยีสารสนเทศตั้งแต่เริ่มต้นจนสิ้นสุดให้มีความสะดวกและเป็นไปอย่างอัตโนมัติ รวมถึงในการพัฒนาระบบเทคโนโลยีสารสนเทศให้เป็นไปตามแผนงานที่กำหนดไว้ ตลอดจนระบบงานต้องสามารถตอบสนอง รองรับการเปลี่ยนแปลงทางธุรกิจที่สำคัญซึ่งต้องมีการดำเนินการที่สอดคล้องกับแผนกลยุทธ์ขององค์กรที่มีการปรับเปลี่ยนได้

รูปที่ 4.3 ความสอดคล้องของธรรมาภิบาลองค์กรและธรรมาภิบาลเทคโนโลยีสารสนเทศ

4.4 นโยบาย ระเบียบ หลักเกณฑ์ คู่มือ ที่เกี่ยวข้องกับองค์กรศึกษา

องค์กรกรณีศึกษามีการกำหนดวิธีการในการบริหารงานด้านเทคโนโลยีสารสนเทศขององค์กรให้มีแนวทางปฏิบัติในทิศทางเดียวกัน และอยู่ภายใต้กรอบข้อตกลงร่วมกันสามารถตอบสนองการดำเนินธุรกิจธนาคารพาณิชย์เพื่อให้สามารถใช้งานได้ทั้งกลุ่มธุรกิจทางการเงิน อันประกอบด้วยธนาคารพาณิชย์ และกลุ่มธุรกิจตลาดทุน อันประกอบด้วยธุรกิจในเครือของธนาคารพาณิชย์ที่เป็นองค์กรศึกษา เช่น บริษัทหลักทรัพย์ บริษัทจัดการกองทุน เป็นต้น ซึ่งแนวทางในการจัดทำแบ่งออกได้เป็นระดับ ดังภาพ

รูปที่ 4.4 เอกสารต่าง ๆ ที่เกี่ยวข้องกับองค์กรศึกษา

4.4.1 นโยบายด้านเทคโนโลยีสารสนเทศ (IT Policy)

นโยบายด้านเทคโนโลยีสารสนเทศขององค์กรศึกษามีลักษณะของการระบุสิ่งที่องค์กรต้องปฏิบัติในด้านเทคโนโลยีสารสนเทศในมุมกว้าง และเป็นเหตุผล หรือเป็นเป้าหมายที่ต้องการเพื่อการบริหารจัดการในทิศทางเดียวกันทั้งองค์กร ซึ่งนโยบายเทคโนโลยีสารสนเทศขององค์กรศึกษาได้รับการอนุมัติลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุดทางด้านเทคโนโลยีสารสนเทศ (Chief Information Technology: CIO) และผู้บริหารที่เกี่ยวข้อง โดยองค์กรศึกษาดังกล่าวเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ ซึ่งต้องมีการนำเสนอการขออนุมัติการประกาศใช้งานภายในองค์กรจากคณะกรรมการธนาคาร พร้อมทั้งประกาศสื่อสารมีผลบังคับใช้งานแก่พนักงานในองค์กรและบริษัทในกลุ่มธุรกิจ

องค์กรศึกษาได้มีการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศของธนาคาร เพื่อจุดประสงค์ให้องค์กรมีนโยบายในการดำเนินการหรือการจัดการทางด้านเทคโนโลยีสารสนเทศ และให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร พนักงาน และบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศของธนาคาร และบริษัทในกลุ่มธุรกิจทางการเงิน ได้มีแผนงานและกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ ความปลอดภัยในการให้บริการสูงสุด และมีมาตรฐานยิ่งขึ้น โดยนโยบายฉบับแรกขององค์ศึกษาเป็นนโยบายการบริหารจัดการด้านสารสนเทศ ฉบับปี 2552 ซึ่งมีการใช้งานภายในธนาคารพาณิชย์ที่เป็นองค์กรศึกษาเท่านั้นและมีเพียงฉบับเดียวที่มีการระบุรายละเอียดระเบียบวิธีปฏิบัติเป็นภาคผนวกในส่วนท้ายของนโยบาย ซึ่งจากนโยบายฉบับดังกล่าวสายเทคโนโลยีสารสนเทศได้มีการทบทวนนโยบายฉบับต่อมาในปี 2555 โดยองค์กรศึกษาได้มีการขออนุญาตการขอคัดลอกและปรับปรุงเนื้อหาให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย Version 2.5 ปี พ.ศ. 2550 ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) (ดังที่กล่าวมาแล้วในบทที่ 2) โดยมีใจความสำคัญสรุปส่วนที่เปลี่ยนแปลง ดังนี้

ตารางที่ 4.4.1 ความแตกต่างของนโยบายด้านเทคโนโลยีสารสนเทศ ปี 2552 และ 2555

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
1. การแยกระเบียบวิธีปฏิบัติออกจากนโยบาย	มีการจัดทำหมวดระเบียบวิธีปฏิบัติ ในภาคผนวกของนโยบาย ได้แก่ ก. มาตรการในการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม ข. มาตรการการจัดการทรัพย์สินสารสนเทศ ค. มาตรการการปฏิบัติงานในพื้นที่ซึ่งต้องรักษาความมั่นคงปลอดภัย ง. มาตรการการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน จ. ระเบียบการปฏิบัติการจัดทำบัญชีผู้ใช้สำหรับผู้ดูแลระบบ ฉ. ระเบียบปฏิบัติการจัดการรหัสผ่านสำหรับพนักงาน ช. มาตรการจัดการรหัสผ่าน ซ. มาตรการเชื่อมต่อกับระบบสารสนเทศเพื่อปฏิบัติงานจากภายนอกสำนักงาน	เรียบเรียงเนื้อหาใหม่ โดยแยกในส่วนของภาคผนวกมาตรการการปฏิบัติ หมวด ข-ช (เดิม) ออกจากนโยบาย และทำการจัดกลุ่มเพื่อจัดทำเป็นระเบียบปฏิบัติของสายเทคโนโลยีสารสนเทศจำนวน 3 ฉบับ

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
	ฌ. มาตรการตรวจสอบข้อมูลนำเข้า ข้อมูลขณะประมวลผล และข้อมูลส่งออก ญ. มาตรการตรวจสอบข้อมูลนำเข้า ข้อมูลขณะประมวลผล และข้อมูลส่งออก ฎ. มาตรการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ ฏ. มาตรการควบคุมช่องโหว่ทางเทคนิค ฐ. คู่มือปฏิบัติด้านเหตุการณ์ทางด้านความมั่นคงปลอดภัย ฑ. มาตรการป้องกันการละเมิดสิทธิ และทรัพย์สินทางปัญญา ฒ. มาตรการการตรวจประเมินระบบสารสนเทศแบบฟอร์มขอผ่อนผันการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ (IT Policy Waiver)	
2. เพิ่มรายละเอียดการร้องขอเปลี่ยนแปลงให้เป็นลายลักษณ์อักษรในนโยบายฉบับปัจจุบัน	นโยบายกำหนดการร้องขอให้มีการเปลี่ยนแปลง หรือแก้ไขระบบงานคอมพิวเตอร์ ตามความต้องการของแต่ละสายงานต้องมีการร้องขออย่างเหมาะสม	ทำการเพิ่มเติมรายละเอียดในนโยบายเรื่องการร้องขอให้มีการเปลี่ยนแปลง หรือแก้ไขระบบงานคอมพิวเตอร์ ตามความต้องการของแต่ละสายงาน ต้องมีการบันทึกเป็นลายลักษณ์

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
3. เพิ่มเติมเรื่องการควบคุมและแยกการเชื่อมต่อทางเครือข่ายระหว่างระบบงานที่ใช้พัฒนา (Development Area) ระบบงานที่ใช้ทดสอบ (User Acceptance Area) และระบบงานที่ใช้ให้บริการจริง (Production Area) ออกจากกัน	นโยบายกำหนดให้มีการควบคุมและแบ่งแยกการเชื่อมต่อทางเครือข่ายระหว่างเครือข่ายที่มีการใช้งานในปัจจุบันและเครือข่ายที่ใช้ทดสอบระบบงานอย่างเหมาะสม	- ทำการเพิ่มเติมการแยกส่วนระบบพัฒนา (Development area) และ ส่วนระบบทดสอบ (User Acceptance Area) ออกจากส่วนระบบให้บริการจริง (Production area) อย่างเด็ดขาด - จัดให้มีการควบคุมการพัฒนาระบบงานและการย้ายระบบงานที่ผ่านการตรวจรับจากกรรมการตรวจรับระบบงานไปยังระบบให้บริการจริง (Production Area) โดยผู้ที่ได้รับการแต่งตั้งเพื่อทำหน้าที่ควบคุมอย่างรัดกุม และตรวจสอบได้
4. เพิ่มเติมเรื่องการบันทึกเหตุการณ์และแนวทางแก้ไข (Incident: Problem Log) เมื่อเกิดปัญหาระหว่างการปิดระบบงานระบบสารสนเทศ	นโยบายกำหนดให้เมื่อเกิดเหตุการณ์ควรมีการบริหารจัดการ Incident อย่างเหมาะสม	ในกรณีที่พบปัญหาขณะทำการปิดระบบงาน ต้องมีการบันทึกปัญหา และวิธีการแก้ไข (Incident Problem Log) รวมถึงรายงานต่อผู้บังคับบัญชาหรือผู้ควบคุมดูแลให้ทราบทันที เพื่อให้สามารถแก้ไขปัญหาได้อย่างทันท่วงที

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
5. เพิ่มเติมการจัดการระบบสารสนเทศสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRC, DRP)	**นโยบายกำหนดให้ระบบสารสนเทศสามารถสำรองข้อมูลและมีแผนรองรับเหตุฉุกเฉินของธนาคารและบริษัทในกลุ่มธุรกิจทางการเงินให้สามารถทำธุรกรรมได้อย่างต่อเนื่อง**	**เพิ่มเติมรายละเอียดในนโยบายเรื่องการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)**
6. เพิ่มเติมเรื่องการควบคุมและกำกับ และการคิดค่าธรรมเนียมด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น(IT Insourcing)	นโยบายกำหนดเป็นกรอบการปฏิบัติงานในการให้บริการงานเทคโนโลยีสารสนเทศให้เกิดประโยชน์สูดสุดต่อธนาคารและบริษัทในกลุ่มธุรกิจทางการเงิน	ทำการกำหนดนโยบายเกี่ยวกับการคิดค่าบริการ และค่าธรรมเนียม ธนาคารคิดค่าบริการ และค่าธรรมเนียม โดยเป็นที่ตกลงร่วมกันระหว่างผู้ให้บริการและผู้ใช้บริการ สามารถอธิบายที่มาของค่าธรรมเนียม ค่าบริการได้ชัดเจน โปร่งใส
7. เพิ่มเติมเรื่องการประเมินนโยบายการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)	นโยบายกำหนดเป็นกรอบการปฏิบัติงานในการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายต่าง ๆ ของธนาคาร	ทำการเพิ่มเติมรายละเอียดการประเมินนโยบายการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น โดยสายเทคโนโลยีสารสนเทศร่วมกับหน่วยงานที่ใช้บริการ เพื่อรายงานคณะกรรมการที่ได้รับมอบหมายทราบ เป็นประจำทุกปี อย่างน้อยปีละครั้ง

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
8. เพิ่มเติมเรื่องการกำหนดความต้องการ ในการใช้บริการด้านงานเทคโนโลยีสารสนเทศ	**นโยบายกำหนดให้ความต้องการใช้บริการด้านเทคโนโลยีสารสนเทศต้องมีการทำการขออนุมัติจากคณะกรรมการธนาคารเพื่อพิจารณาอย่างเหมาะสม**	**การกำหนดความต้องการ เพื่อให้มีการระบุชัดเจนถึงความคาดหวังต่าง ๆ เกี่ยวกับโครงการ และใช้ในการติดตามผลการดำเนินงาน**
9. เพิ่มเติมการคัดเลือกผู้ให้บริการโดยประธานสายงาน (หรือเทียบเท่า)	นโยบายกำหนดให้มีคณะทำงานเพื่อดำเนินการ ตามอำนาจอนุมัติที่มี	ทำการเพิ่มเติมรายละเอียดของการคัดเลือกผู้ให้บริการโดยประธานสายงาน (หรือเทียบเท่า)
10.เพิ่มเติมหัวข้อการติดตามข้อมูลเกี่ยวกับสถานะ และปัญหาของผู้ให้บริการ	นโยบายกำหนดให้ทำการติดตาม ประเมินผล และตรวจสอบการให้บริการ	ทำการเพิ่มเติมเกี่ยวกับนโยบายการบริหารจัดการติดตามข้อมูลเกี่ยวกับสถานะ และปัญหาของผู้ให้บริการ เช่น ในกรณีปัญหาทางด้านการเงิน เพื่อให้สามารถคาดการณ์ และทราบถึงคุณภาพการให้บริการที่อาจเปลี่ยนแปลงในอนาคต
11.เพิ่มเติมเรื่องการแลกบัตรที่มีรูปภาพในหัวข้อการควบคุมการเข้าออก (Physical entry controls)	นโยบายกำหนดให้มีการควบคุมการเข้าออกต้องมีการควบคุมอย่างเหมาะสมโดยผู้ที่ได้รับอนุญาต	นโยบายทำการกำหนดเพิ่มเติมให้ผู้ที่มีความจำเป็นในการเข้าถึงบริเวณที่ต้องมีการรักษาความปลอดภัย ต้องผ่านการอนุมัติจากผู้บริหารสายงาน และผู้บริหารสารสนเทศแล้วเท่านั้น และต้องมีเจ้าหน้าที่ของกลุ่มธุรกิจทางการเงินเฝ้าติดตามอย่างใกล้ชิด

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
12.พิ่มเติมเรื่องการทำลาย สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)	นโยบายกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เช่น ทำลายสื่อจัดการข้อมูลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ เป็นต้น	นโยบายกำหนดรายละเอียดเพิ่มเติมให้สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable media) เช่น Tapes, disks, flash disks, removable hard drives, CDs, DVD ให้ตระหนักถึงข้อมูลว่าถูกทำลายจริง และไม่สามารถนำกลับมากู้ข้อมูลได้อีก เพื่อลดความเสี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
13.เพิ่มเติมเรื่องการระบุกลุ่มผู้ใช้งาน และสิทธิในการเข้าถึงข้อมูลของหน่วยงานภายนอกให้ชัดเจน ในระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)	นโยบายกำหนดว่าเป็นการใช้งานข้อมูล หรือระบบสารสนเทศร่วมกันระหว่างธนาคารและบริษัทในกลุ่มธุรกิจทางการเงิน และหน่วยงานภายนอก ผ่านสื่อต่าง ๆ ขององค์กรควรมีการจัดการอย่างเหมาะสม	นโยบายกำหนดเพิ่มเติมโดยให้ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน ต้องมีการระบุกลุ่มผู้ใช้งาน และสิทธิในการเข้าถึงข้อมูลของหน่วยงานภายนอกให้ชัดเจน และกำหนดวิธีการป้องกันการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศอื่น ๆ ของธนาคารที่ไม่ต้องการให้หน่วยงานภายนอกเข้าถึงได้
14.เพิ่มเติมเรื่องการตรวจสอบช่องโหว่ในระบบสารสนเทศ (Vulnerability Assessment)	นโยบายกำหนดให้มีการบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ทางด้านเทคนิคให้มีความเหมาะสม	ทำการเพิ่มเติมนโยบายโดยให้ระบบธุรกรรมออนไลน์ที่มีการเริ่มใช้งานใหม่ต้องมีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบการเจาะระบบ (Penetration

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
(Penetration Testing) ในระบบที่มีการทำธุรกรรมออนไลน์		และทดสอบการเจาะระบบ
15. เพิ่มเติมเรื่องการล้างข้อมูลในระบบสารสนเทศที่เกี่ยวกับบัญชีผู้ใช้ที่พ้นสภาพจากการเป็นพนักงาน โอนย้ายตำแหน่งงาน	นโยบายกำหนดให้บัญชีผู้ใช้งานเมื่อสิ้นสุดการใช้งานต้องมีการร้องเพื่อทำการยกเลิกสิทธิอย่างเหมาะสม และควรมีการทบทวนความถูกต้องของสิทธิการเข้าถึงอย่างเหมาะสม	ทำการเพิ่มเติมในนโยบายให้การทบทวนความถูกต้องของสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง
16. เพิ่มจำนวนการจำกัดจำนวนครั้งในการพยายามเข้าถึง (Log on Attempts จาก 4 ครั้งเป็น 7 ครั้ง	นโยบายกำหนดให้มีการบันทึกความพยายามเข้าถึงที่สำเร็จและไม่สำเร็จ และแจ้งเตือนเมื่อมีการพยายามเข้าระบบหลาย ๆ ครั้ง ซึ่งเมื่อมีการใส่รหัสผ่านผิดเกิน 3 ครั้งระบบต้องล็อกหน้าจอไม่ได้ทำงานต่อไปจนกว่าจะมีการตรวจสอบและแก้ไขจากผู้ดูแลระบบงาน	การจำกัดจำนวนครั้งในการพยายามเข้าถึง (Log on Attempts) เมื่อมีการพยายามเข้าถึง หรือใส่รหัสผ่านผิดไม่เกิน 3 ครั้ง และการใส่รหัสผิดครั้งที่ 4
17. เพิ่มเติมเรื่องระบบบริหารจัดการรหัสผ่าน (Password management system)	นโยบายกำหนดในภาคผนวกของการบริหารจัดการรหัสผ่าน เช่น มาตรการจัดการรหัสผ่านของพนักงาน ผู้ดูแลระบบงาน ให้มีความเหมาะสม อาทิ การกำหนดการเก็บรหัสผ่านโดยพนักงานต้องเก็บเป็นความลับไม่เปิดเผยโดยไม่ได้รับอนุญาต	ระบบสารสนเทศที่มีระบบการพิสูจน์ตัวตน ในรูปแบบบัญชีผู้ใช้ และรหัสผ่าน ต้องมีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมต่าง ๆ ดังนี้

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
	การกำหนดรหัสผ่านให้มีประสิทธิภาพ มาตรการจัดการรหัสผ่าน เช่น ความถี่การเปลี่ยนรหัสผ่าน การจัดเก็บ Log จำนวนครั้งของการเข้าถึง เป็นต้น	➢ การจัดเก็บรหัสผ่าน และการจัดส่ง ต้องกระทำโดยมีมาตรการป้องกันเช่น การเข้ารหัสลับ และกำหนดให้ไม่มีการแสดงรหัสผ่านขณะมีการป้อนเข้าระบบ ➢ รหัสผ่านที่มาพร้อมกับระบบสารสนเทศ (Default Password) หรืออุปกรณ์สารสนเทศใด ๆ ต้องเปลี่ยนทันทีเมื่อมีการนำมาใช้งานภายในกลุ่มธุรกิจทางการเงิน ➢ กำหนดให้ความยาวขั้นต่ำของรหัสผ่าน 7 ตัวอักษร ➢ กำหนดให้มีการบังคับการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด 90 วัน ➢ กำหนดจำนวนครั้งของการเปลี่ยนรหัสผ่านให้ไม่สามารถใช้รหัสผ่านซ้ำเดิมได้ 3 ครั้ง (Password History) ➢ กำหนดระยะเวลาทำการ Disable บัญชีผู้ใช้งานเมื่อไม่มีการเข้าใช้งานตามระยะเวลาเกิน 90 วัน ➢ กรณีเป็นบัญชีผู้ใช้ที่ติดมากับระบบประเภท System Account และไม่สามารถดำเนินการเปลี่ยน Password ได้

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
		ตามนโยบายด้านเทคโนโลยีสารสนเทศให้ทำการบริหารจัดการสิทธิการใช้งานระบบ (Password Custodian) และต้องมีการแจ้งและบันทึกการขอใช้ทุกครั้งอย่างเคร่งครัด
18.เพิ่มเติมขั้นตอนปฏิบัติงานที่มีความมั่นคงปลอดภัยการปฏิบัติงานภายนอกสำนักงาน (Tele working)	นโยบายกำหนดให้ควบคุมอุปกรณ์สื่อสารพกพาและการปฏิบัติงานจากภายนอก เพื่อลดความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล	โดยให้พิจารณาเพิ่มขั้นตอนปฏิบัติงานที่มีความมั่นคงปลอดภัยมากกว่าการปฏิบัติงานจากภายในสำนักงาน ➢ การจัดเตรียมอุปกรณ์เครือข่าย และวิธีการในการเชื่อมต่อจากภายนอก ให้มีความปลอดภัย เช่น การป้องกันข้อมูลที่มีความสำคัญที่ส่งผ่านเครือข่าย ผ่านการใช้ช่องทางที่มีการเข้ารหัสลับ เช่น (Virtual Private Network :VPN) ➢ การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness) เกี่ยวกับความเสี่ยงที่เกิด ➢ การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness) เกี่ยวกับความเสี่ยงที่เกิดจากการใช้งาน ปฏิบัติงานจากภายนอกสำนักงานและการเข้าถึงจากครอบครัว เพื่อน หรือบุคคลภายนอกที่สามารถเข้าถึง

ตารางที่ 4.4.1 (ต่อ)

เรื่อง/รายละเอียด	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2552	นโยบายเทคโนโลยีสารสนเทศ ฉบับปี 2555
		สถานที่และอุปกรณ์ที่ใช้ในการเชื่อมต่อได้ ➢ มีความเคร่งครัดในการถอดถอนสิทธิการเข้าถึง เมื่อสิ้นสุดความจำเป็นในการใช้บริการ
19.เพิ่มเติมเรื่องมาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)	นโยบายกำหนดให้มีการติดตามข้อมูลข่าวสารช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน เพื่อประเมินความเสี่ยงของช่องโหว่ ลดความเสี่ยงตามมาตรฐานการควบคุมช่องโหว่ให้เหมาะสม	กำหนดความรับผิดชอบในการปฏิบัติงานการบริหารจัดการช่องโหว่ รวมไปถึง การเฝ้าสังเกตการณ์ ช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ การ Patch และการประสานงานกับหน่วยงานที่จำเป็น
20.การปรับปรุงเนื้อหาการขอผ่อนผันการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ (IT Policy Waiver)	นโยบายกำหนดให้กรณีที่หน่วยงานไม่สามารถปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศได้ต้องทำการขออนุมัติเป็นลายลักษณ์อักษรจากคณะกรรมการที่ได้รับมอบหมาย โดยหน่วยงานมีเวลา 90 วันนำเสนอการขอผ่อนผัน และต้องรายงานความคืบหน้า โดยต้องไม่ขัดต่อข้อกฎหมายใด ๆ	เพื่อให้การขอผ่อนผันการปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศ มีการจัดทำเอกสารเป็นลายลักษณ์อักษร และผ่านการอนุมัติจากผู้มีอำนาจเพื่อป้องกันการยกเว้นการปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศไม่ได้รับอนุญาต 90 วัน
21.เพิ่มเติมคำจำกัดความ “ระบบงานที่สำคัญ (High Priority Application System)”	นโยบายกล่าวเพียงภาพรวมของระบบงานที่สำคัญของธนาคารต้องมีการบริหารจัดการให้เหมาะสม	หมายถึง ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบบงานที่นำส่งข้อมูลรายงานแก่ทางการ (เช่น ธปท, ก.ล.ต.)

4.4.2 ระเบียบด้านเทคโนโลยีสารสนเทศ (IT Procedure)

ระเบียบเป็นข้อปฏิบัติที่องค์กรทำการกำหนดขึ้นเพื่อให้สอดคล้องกับพระราชบัญญัติที่เกี่ยวข้อง หรือนโยบายขององค์กร โดยเป็นกฎเกณฑ์ที่ทุกคนต้องปฏิบัติตาม โดยในบางองค์กรอาจมีการระบุบทลงโทษหากไม่ปฏิบัติตามระเบียบ หรือกระทำการฝ่าฝืนทางวินัยตามข้อบังคับขององค์กรไว้ด้วย

ซึ่งองค์กรศึกษาได้ทำการกำหนดระเบียบของการปฏิบัติด้านเทคโนโลยีสารสนเทศของธนาคารให้มีความมั่นคงปลอดภัยสอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร โดยทำการแยกระเบียบการปฏิบัติงานออกจากภาคผนวกของนโยบายเทคโนโลยีสารสนเทศขององค์กร ฉบับปี 2552 รวมทั้งได้มีการอนุมัติการประกาศใช้ระเบียบภายในธนาคารเพื่อให้พนักงานและผู้บริหารทุกคนปฏิบัติตามอย่างเป็นลายลักษณ์อักษรโดยผ่านคณะกรรมการบริหารของธนาคาร ซึ่งหากกระทำการฝ่าฝืนหรือไม่ปฏิบัติตามมีการกำหนด มีการกำหนดบทลงโทษโดยให้เป็นไปตามข้อบังคับเกี่ยวกับการทำงานของธนาคาร โดยปัจจุบันองค์กรศึกษาได้ทำการกำหนดระเบียบด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ 3 ฉบับ ได้แก่

1) **ระเบียบเรื่อง การใช้งานทรัพย์สินสารสนเทศ โดยสายเทคโนโลยีสารสนเทศ**
มีจุดประสงค์เพื่อให้การใช้งานทรัพย์สินสารสนเทศของธนาคารเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมถึงเพื่อเป็นการกำหนดข้อปฏิบัติให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน โดยสรุปมีดังนี้

ตารางที่ 4.4.2.1 สรุประเบียบการใช้งานทรัพย์สินสารสนเทศ

การใช้งานทรัพย์สินสารสนเทศ โดยสายเทคโนโลยีสารสนเทศ
1. การใช้งานเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศขององค์กร ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร จากผู้บังคับบัญชาต้นสังกัด และสายเทคโนโลยีสารสนเทศ ตลอดจนการใช้งานต้องอยู่บนพื้นฐานของความจำเป็น และความมั่นคงปลอดภัย อาทิ ต้องมีการยืนยันตัวตนบุคคล (Authentication) ก่อนการใช้งาน รวมถึงห้ามทำการเปลี่ยนแปลงแก้ไข สำเนาซอฟต์แวร์ลิขสิทธิ์ของธนาคาร หรือละเมิดทรัพย์สินทางปัญญา หรือเชื่อมต่อกับระบบเครือข่ายอื่นนอกจากที่ธนาคารและบริษัทในกลุ่มธุรกิจทางการเงินจัดให้ รวมทั้งต้องมีความตระหนักในการใช้งานจากภายนอก หรือใช้งานผ่านระบบเครือข่ายไร้สาย (Wireless Network) จดหมายอิเล็กทรอนิกส์ (E-mail) และเครือข่ายสังคมออนไลน์ (Social Network) ให้มีความมั่นคงปลอดภัยไม่เกิดความเสียหายกับธนาคาร หากเกิดปัญหาการใช้งานต้องรายงานผู้บังคับบัญชาต้นสังกัด และสาย

ตารางที่ 4.4.2.1 (ต่อ)

เทคโนโลยีสารสนเทศอย่างเหมาะสม รวมถึงต้องมีการป้องกันไวรัสและควบคุมช่องโหว่ทางเทคนิคกับทรัพย์สินสารสนเทศของธนาคาร **2. การใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์สื่อสารเคลื่อนที่** ต้องใช้งานเครื่องคอมพิวเตอร์ขององค์กรเท่านั้น ไม่อนุญาตทำการติดตั้งโปรแกรมโดยพลการ ต้องป้องกันการสูญหายของทรัพย์สินสารสนเทศธนาคารให้มีความปลอดภัย กรณีอุปกรณ์สูญหายต้องแจ้งผู้บังคับบัญชาและสายเทคโนโลยีสารสนเทศอย่างทันที **การใช้งานข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์** ต้องห้ามเผยแพร่เอกสารสำคัญ ความลับธนาคาร ห้ามจัดเก็บข้อมูลสำคัญไว้บนเครื่องที่ใช้งานอยู่ รวมถึงมีการควบคุมการจัดเก็บข้อมูลสำคัญ และทำลายข้อมูลให้มีความเหมาะสม

2) **ระเบียบเรื่อง การกำหนดบัญชีผู้ใช้งาน และรหัสผ่าน โดยสายเทคโนโลยีสารสนเทศ** มีจุดประสงค์เพื่อควบคุมการกำหนดบัญชีและสิทธิผู้ใช้งาน และป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต รวมถึงกำหนดข้อปฏิบัติให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน โดยสรุปมีดังนี้

ตารางที่ 4.4.2.2 สรุประเบียบการกำหนดบัญชีผู้ใช้งานและรหัสผ่าน

การกำหนดบัญชีผู้ใช้งาน และรหัสผ่าน โดยสายเทคโนโลยีสารสนเทศ
1. การกำหนดบัญชีผู้ใช้งาน และสิทธิผู้ใช้งาน ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร จากผู้บังคับบัญชาต้นสังกัด และสายเทคโนโลยีสารสนเทศ ตลอดจนการใช้งานต้องอยู่บนพื้นฐานของความจำเป็น กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องขออนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาสายเทคโนโลยีสารสนเทศ โดยกำหนดระยะเวลาในการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา สามารถจำแนกบัญชีผู้ใช้ และกลุ่มผู้ใช้งาน เพื่อกำหนดสิทธิแยกตามหน้าที่ความรับผิดชอบ และต้องมีการถอดถอนสิทธิหรือยกเลิกการใช้งานเมื่อสิ้นสุดความจำเป็นในการใช้งาน โดยการแจ้งของพนักงานผู้ขอใช้งาน และผู้บังคับบัญชาต้นสังกัด ตลอดจนจัดให้มีการทบทวนสิทธิ และบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสิทธิต่างๆ ยังคงมีความเหมาะสม

ตารางที่ 4.4.2.2 (ต่อ)

2. การจัดการรหัสผ่าน (User password management) ต้องมีการส่งมอบรหัสผ่านตั้งต้นให้กับผู้ใช้ ด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกัน และผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และกำหนดรหัสผ่านที่มีความยากต่อการเดา รวมถึงต้องเก็บรักษารหัสผ่านไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น กรณีที่ต้องการออกรหัสผ่านใหม่หรือปลดล็อกรหัสผ่าน ต้องขออนุมัติจากผู้บังคับบัญชาต้นสังกัดและสายเทคโนโลยีสารสนเทศ กำหนดให้มีการบริหารจัดการรหัสผ่านดังนี้ - ความยาวขั้นต่ำของรหัสผ่าน 7 ตัวอักษร (Minimum Password Length) - บังคับการเปลี่ยนรหัสผ่านทุก 90 วัน (Force Password Duration Change) - จำกัดการตั้งค่ารหัสผ่านซ้ำเดิม 3 ครั้ง (Enforce Password History) - จำกัดจำนวนครั้งในการพยายามเข้าถึง (Log on Attempts) เมื่อมีการพยายามเข้าถึง หรือใส่รหัสผ่านผิด 4 ครั้ง ระบบต้องล็อกบัญชีไม่ให้ทำงานจนกว่าจะมีการแก้ไขจากผู้ดูแลระบบ

3) **ระเบียบเรื่อง การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาวะแวดล้อม โดยสายเทคโนโลยีสารสนเทศ**

มีจุดประสงค์เพื่อรักษาความปลอดภัยด้านกายภาพ สถานที่ สภาวะแวดล้อมของทรัพย์สินสารสนเทศ และโครงสร้างพื้นฐาน ให้อยู่ในสภาพพร้อมใช้ ป้องกันการเสียหาย หรือการถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงกำหนดข้อปฏิบัติให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน โดยสรุปมีดังนี้

ตารางที่ 4.4.2.3 สรุประเบียบการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาวะแวดล้อม

การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาวะแวดล้อม โดยสายเทคโนโลยีสารสนเทศ
1. พื้นที่ซึ่งต้องมีการรักษาความมั่นคงปลอดภัย (Secured Area) สามารถแบ่งออกเป็น 3 ส่วน คือ - พื้นที่ห้อง Patching Room เป็นพื้นที่ใช้ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ และโทรศัพท์

ตารางที่ 4.4.2.3 (ต่อ)

- พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ (Operation Room) เป็นพื้นที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศ
- พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) เป็นพื้นที่ใช้เก็บอุปกรณ์ประมวลผลสารสนเทศและเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน

2. การควบคุมการเข้าออกในพื้นที่ซึ่งต้องมีการรักษาความมั่นคงปลอดภัย ต้องมีการจัดให้มีระบบการควบคุมการเข้าออก ให้สามารถเข้าถึงได้เฉพาะพนักงานที่มีความจำเป็นที่ต้องปฏิบัติงานเท่านั้น และได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาต้นสังกัด และสายเทคโนโลยีสารสนเทศ โดยบุคคลที่มีความจำเป็นต้องเข้าในพื้นที่ปฏิบัติงานเป็นรายครั้ง ต้องขออนุมัติต่อสายเทคโนโลยีสารสนเทศ พร้อมทั้งระบุเหตุผล, ความจำเป็น และช่วงเวลาในการเข้าออก โดยระหว่างนั้นต้องมีพนักงานผู้รับผิดชอบกำกับดูแลอย่างน้อย 1 คน

3. การปฏิบัติงานภายในพื้นที่ซึ่งต้องมีการรักษาความมั่นคงปลอดภัย ต้องปฏิบัติงานตามคู่มือปฏิบัติงาน หรือคู่มือการจัดการอุปกรณ์ต่าง ๆ อย่างเคร่งครัด และห้ามนำสิ่งของต่อไปนี้เข้าพื้นที่ซึ่งต้องมีการรักษาความมั่นคงปลอดภัยโดยเด็ดขาด อาทิ อาหารเครื่องดื่ม วัตถุไวไฟ กล้องบันทึกภาพ เสียง ตลอดจนการปฏิบัติงานนอกเหนือจากเวลางานปกติ และการขนย้ายอุปกรณ์ใด ๆ เข้า–ออกห้องต้องผ่านการอนุมัติจากผู้บังคับบัญชาต้นสังกัด และสายเทคโนโลยีสารสนเทศ

4. การป้องกันภัยคุกคามจากสิ่งแวดล้อมในพื้นที่ซึ่งต้องมีการรักษาความมั่นคงปลอดภัย โดยห้องศูนย์ข้อมูลคอมพิวเตอร์ต้องปฏิบัติตามทุกข้อเนื่องจากเป็นบริเวณที่ต้องมีการรักษาความปลอดภัยในระดับความสำคัญสูงสุด สำหรับพื้นที่อื่น ๆ ให้พิจารณาตามความจำเป็น โดยต้องจัดให้มีสิ่งอำนวยความสะดวก (Facility) ให้เกิดความมั่นคงปลอดภัยอย่างเพียงพอ เช่น การป้องกันอัคคีภัย การควบคุมน้ำรั่ว ระบบควบคุมอุณหภูมิ เป็นต้น ตลอดจนจัดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

ระบบและอุปกรณ์สนับสนุนการทำงาน ต้องจัดให้มีสิ่งอำนวยความสะดวก (Facility) ให้เกิดความมั่นคงปลอดภัยอย่างเพียงพอ เช่น แหล่งไฟฟ้าสำรอง (Generator) เครื่องสำรองไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply: UPS) ระบบควบคุมอุณหภูมิ เป็นต้น ตลอดจนจัดให้มีระบบเฝ้าดูและรายงานเมื่อพบข้อผิดพลาด และการตรวจสอบหรือทดสอบ ระบบและอุปกรณ์สนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานได้ตามปกติ

4.4.3 หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศ (IT Principle Operation)

หลักเกณฑ์เป็นมาตรฐาน วิธีการปฏิบัติเพื่อให้ผู้ปฏิบัติงานสามารถนำไปใช้งานได้ในทิศทางเดียวกัน และและอยู่ภายใต้กรอบข้อตกลง ตลอดจนสามารถเป็นเครื่องมือที่รวดเร็วในการตอบสนองนโยบายด้านเทคโนโลยีสารสนเทศ มาตรฐานหรือบรรทัดฐานที่ดี (Good Governance) ภายในสายเทคโนโลยีสารสนเทศส่วนงานต่าง ๆ ซึ่งหลักเกณฑ์ของสายเทคโนโลยีสารสนเทศมีการจัดทำโดยฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศ ในการกำกับมาตรการ วิธีการปฏิบัติให้เป็นไปตามระเบียบ หรือนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งปัจจุบันมีการจัดทำหลักเกณฑ์ 7 ฉบับ สามารถสรุปได้ดังนี้

1) หลักเกณฑ์ในการปฏิบัติเรื่องการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ Principle of Operation: IT Change Management

มีจุดประสงค์เพื่อควบคุมความเสี่ยง และลดผลกระทบในเชิงลบต่อการให้บริการด้านเทคโนโลยีสารสนเทศจากการเปลี่ยนแปลงของการแก้ไขเหตุการณ์ผิดปกติ (Incident) และการปรับปรุงแก้ไขระบบเทคโนโลยีสารสนเทศ ตลอดจนควบคุมปัจจัยที่ส่งผลกระทบต่อความสำเร็จของการเปลี่ยนแปลง เช่น ระยะเวลา บุคลากร องค์ความรู้ ความพร้อมด้านเทคโนโลยีสารสนเทศ งบประมาณ ขอบเขตการดำเนินงาน เป็นต้น รวมถึงการสร้างความเชื่อมั่นในคุณภาพ และระยะเวลาการส่งมอบผลงานที่ได้จากการเปลี่ยนแปลง รวมถึงสร้างความพึงพอใจแก่ผู้ขอรับบริการ โดยสามารถสรุปประเภทการร้องขอเปลี่ยนแปลง (Type of Change request) แบ่งเป็น 3 ประเภท ได้แก่

- Standard Change Request คือ การร้องขอเปลี่ยนแปลงระหว่างสายเทคโนโลยีสารสนเทศด้วยกัน ซึ่งอาจมีผลกระทบต่อพนักงานภายในและภายนอกสายเทคโนโลยีสารสนเทศ
- Normal Change Request คือ การร้องขอเปลี่ยนแปลงแก้ไขโดยพนักงานภายในและภายนอกสายเทคโนโลยีสารสนเทศ ทำการร้องขอผ่านช่องทางที่กำหนด (IT Request)
- Emergency Change Request คือ การร้องขอเปลี่ยนแปลงกรณีเร่งด่วน ผ่านหัวหน้าสายเทคโนโลยีสนเทศ (Chief Information Office: CIO) เพื่อทำการเปลี่ยนแปลง แก้ไขอย่างเร่งด่วน และดำเนินการตามกระบวนการในภายหลัง ผ่านช่องทาง IT Request

ซึ่งผู้ทำการร้องขอ (Change Requester) ต้องทำการประเมินระดับผลกระทบและความเสี่ยงให้มีความถูกต้องเพื่อการร้องขอตามประเภทการเปลี่ยนแปลงที่ถูกต้องเหมาะสม

ตารางที่ 4.4.3.1 ระดับผลกระทบและความเสี่ยงการเปลี่ยนแปลงเทคโนโลยีสารสนเทศ

ระดับความเสี่ยง	ระดับผลกระทบ	ระดับความเสี่ยง
สูง	การเปลี่ยนแปลงที่ดำเนินการแล้วมีผลกระทบต่อลูกค้า	การเปลี่ยนแปลงที่ไม่เคยมีการดำเนินการมาก่อน
ปานกลาง	การเปลี่ยนแปลงที่ดำเนินการแล้ว มีผลกระทบต่อผู้ใช้งาน/พนักงานทั่วไปของธนาคาร	การเปลี่ยนแปลงที่เคยมีผู้ดำเนินการมาก่อน แต่ยังไม่มีเอกสารกำหนดรูปแบบการดำเนินการและมีแผนถอยกลับ กรณีที่ดำเนินการไม่สำเร็จอย่างชัดเจน
ต่ำ	การเปลี่ยนแปลงที่ดำเนินการแล้ว มีผลกระทบต่อผู้ดูแลระบบงาน/พนักงานเทคโนโลยีสารสนเทศ	การเปลี่ยนแปลงที่เคยมีผู้ดำเนินการมาก่อน ซึ่งมีเอกสารกำหนดรูปแบบ ขั้นตอนการดำเนินการ และมีแผนถอยกลับ กรณีที่ดำเนินการไม่สำเร็จได้อย่างชัดเจน

2) หลักเกณฑ์ในการปฏิบัติเรื่องการบริหารจัดการเหตุผิดปกติและการจัดการปัญหาที่ต้นเหตุ IT Principle: Incident and Problem Management

มีจุดประสงค์เพื่อให้มีกระบวนการและขั้นตอนในการบริหารจัดการเหตุผิดปกติ (Incident Management) ด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ ซึ่งมุ่งเน้นการกู้หรือบรรเทาความเสียหายของการให้บริการระบบสารสนเทศให้กลับคืนสภาวะปกติโดยเร็วที่สุด ตลอดจนเพื่อให้มีกระบวนการในการบริหารจัดการปัญหาที่ต้นเหตุ มุ่งเน้นการวิเคราะห์สาเหตุของปัญหาที่มีความซับซ้อน หรือมีผลกระทบต่อการให้บริการระบบงานที่สำคัญ (High Priority) ซึ่งประเภทของเหตุผิดปกติ (Incident) แบ่งได้เป็น 3 ประเภท ได้แก่

- Minor Incident คือ จำนวนรายการการแจ้งปัญหาจากผู้ใช้งานที่มีความถี่ของการเกิดซ้ำจำนวนมากเกินกว่าที่กำหนดไว้
- Normal Incident คือ เหตุผิดปกติที่เกิดขึ้นกับระบบงานประเภท Medium Priority ที่องค์กรกำหนดซึ่งเป็นระบบงานที่ให้บริการภายในองค์กร
- Major Incident คือ เหตุผิดปกติที่เกิดขึ้นกับระบบงานประเภท High Priority ที่องค์กรกำหนดซึ่งเป็นระบบงานที่กระทบการให้บริการลูกค้า

โดยมีการกำหนดให้สายเทคโนโลยีสารสนเทศเป็นผู้ที่มีหน้าที่ช่วยประสานงาน หรือดำเนินการกอบกู้ให้บริการด้านเทคโนโลยีสารสนเทศกลับมาใช้งานได้ตามปกติให้ได้อย่างโดยเร็วที่สุดตามความเหมาะสม

3) หลักเกณฑ์ในการปฏิบัติเรื่องกระบวนการรายงานเหตุผิดปกติ IT Principle: Incident Report and Escalation Process

มีจุดประสงค์เพื่อให้มีการสื่อสารที่ทั่วถึง ตั้งแต่ผู้ปฏิบัติงาน จนถึงผู้บริหารสายงาน และผู้ใช้งานหรือบริการที่เกี่ยวข้อง ให้รับทราบสถานะของเหตุผิดปกติ (Incident) อย่างเป็นปัจจุบัน ตลอดจนให้พนักงานสายเทคโนโลยีสารสนเทศเข้าใจขั้นตอนการปฏิบัติในการรายงานเมื่อเกิดเหตุผิดปกติ ที่จำเป็นต้องควบคู่ไปกับการบริหารจัดการเหตุผิดปกติ และบริหารจัดการปัญหาที่ต้นเหตุ

ซึ่งในกรณีที่เกิดเหตุผิดปกติขึ้นระบบงานหรือบริการใช้บริการเทคโนโลยีสารสนเทศ นอกจากการเข้าไปแก้ไขเหตุผิดปกติแล้ว ผู้ดูแลระบบงาน หัวหน้าทีม และหัวหน้าฝ่าย ต่างต้องมีหน้าที่รายงานเหตุผิดปกติให้ผู้ที่เกี่ยวข้องรับทราบและรายงานให้ผู้บริหารทราบโดยเร็วที่สุด ผ่านช่องทางที่สายเทคโนโลยีสารสนเทศกำหนด เช่น รายงานผู้ใช้บริการระบบสารสนเทศ ผ่านระบบ Sevice Level Agreement & Problem Log และ Email รวมถึงรายงานผู้บริหารสาย IT และทีมงานผ่าน Email รายงาน SMS หรือทางวาจาให้ทราบโดยทันที

4) หลักเกณฑ์ในการปฏิบัติเรื่องการบริหารจัดการแฟ้มข้อมูลกลางของสายงาน IT Principle: IT Shared Folder Management

มีจุดประสงค์เพื่อให้มีการบริหารจัดการแฟ้มข้อมูล ข้อมูล และขนาดของข้อมูลที่อยู่ในแฟ้มข้อมูลกลางของรายงานอย่างเป็นระบบ รวมทั้งสามารถดึงและส่งผ่านข้อมูลไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ตลอดจนเป็นองค์ความรู้ของสายงาน ทั้งข้อมูลทั่วไปที่เจ้าหน้าที่ทุกท่านต้องรับทราบ และข้อมูลที่สำคัญด้านเทคโนโลยีสารสนเทศ โดยสายเทคโนโลยีสารสนเทศต้องมีกระบวนการ ขั้นตอนตั้งแต่การขอสร้างแฟ้มข้อมูลใหม่ การขอลบแฟ้มข้อมูลหรือ Folder การขอลบข้อมูลในแฟ้มข้อมูลชื่อ Temp File และการสอบทานและรายงานความจุที่เพิ่มขึ้นของแฟ้มข้อมูล รวมถึงการขอเพิ่มความจุของแฟ้มข้อมูลให้มีการบริหารจัดการที่เหมาะสม และมีความถูกต้องในการดำเนินการ

5) หลักเกณฑ์ในการปฏิบัติเรื่องมาตรฐานการทดสอบระบบงาน IT Principle: Standard Testing

มีจุดประสงค์เพื่อใช้เป็นแนวทางในการอ้างอิงการทำงานของธนาคาร ให้ผู้ปฏิบัติงานมีความเข้าใจที่ตรงกันสามารถปฏิบัติให้เป็นไปในทิศทางเดียวกันในกระบวนการพัฒนาระบบงาน และสอดคล้องกับนโยบายเทคโนโลยีสารสนเทศ โดยสายเทคโนโลยีสารสนเทศทำการแบ่งระดับของการทดสอบ (Level of Testing) เป็น 4 ระดับ ได้แก่

- Unit Integration System Testing (UIS) คือ การทำการทดสอบโดย Vendor หรือทีมพัฒนาระบบงาน เพื่อการทดสอบระบบงานบน Development Environment ตลอดจนมีการใช้ข้อมูลในการทดสอบสร้างเป็นข้อมูลจำลองเพื่อป้องกันข้อมูลสำคัญของธนาคาร
- System Integration Test (SIT) คือ การทำการทดสอบโดย Vendor และทีมทดสอบของธนาคาร เช่น System Analyst เพื่อทำการทอสอบบน UAT Environment
- Pre User Acceptance Test (Pre_UAT) คือ การทดสอบโดยทีมทดสอบของธนาคาร เช่น Business Analyst หรือ Quality Assurance เป็นต้น
- User Acceptance Test (UAT) คือ การทดสอบโดยทีมทดสอบของธนาคาร เช่น ผู้ใช้ระบบงาน (User) หรือ IT Infrastructure

ซึ่งจากหลักเกณฑ์ดังกล่าวสามารถนำไปใช้เป็นชุดมาตรฐานการทดสอบระบบงาน (Standard Test Case) ของธนาคารได้ในช่วงต่าง ๆ ของโครงการตั้งแต่ เนื้อหาของเอกสารของโครงการ TOR หรือหนังสือร่างขอบเขตของงาน ขั้นตอนการวางแผนทดสอบระบบงาน ทดสอบระบบงาน และขั้นตอนการสอบทานเอกสาร เป็นต้น

6) หลักเกณฑ์ในการปฏิบัติเรื่องการบริหารจัดการการใช้พื้นที่ทดสอบระบบงาน IT Principle: Test Environment Management

มีจุดประสงค์เพื่อปรับช่วงเวลาการใช้พื้นที่ทดสอบระบบงานให้เหมาะสมกับการปฏิบัติงานจริงในปัจจุบันของธนาคาร โดยสายเทคโนโลยีสารสนเทศทำการกำหนดให้สามารถทำการจองพื้นที่เพื่อทดสอบระบบงานได้ในวันทำงานปกติ ระหว่างเวลา 09.00 – 22.00 น. ซึ่งหากมีความจำเป็นต้องใช้งานพื้นที่ดังกล่าวนอกเวลาที่กำหนดต้องมีการขออนุมัติอย่างเหมาะสมจากผู้มีอำนาจ

7) หลักเกณฑ์ในการปฏิบัติเรื่องการบริหารจัดการซอร์สโค้ด IT Principle: Source code Management

มีจุดประสงค์เพื่อให้มีกระบวนการจัดการซอร์สโค้ด และชุดติดตั้ง (Deployment package) อย่างเป็นระบบ เพื่อป้องกันความเสียหายและลดผลกระทบจากการใช้งาน ตลอดจนควบคุมการเข้าถึง และป้องกันการเปลี่ยนแปลงซอร์สโค้ด และชุดติดตั้งโดยไม่ได้รับอนุญาต รวมถึงใช้เป็นแนวทางอ้างอิงในการทำงานให้ผู้ปฏิบัติงานในทิศทางเดียวกันได้ผลลัพธ์ที่มีคุณภาพและสอดคล้องกับนโยบายเทคโนโลยีสารสนเทศขององค์กร

โดยสายเทคโนโลยีสารสนเทศทำการกำหนดแนวทางการบริหารจัดการโดยกำหนดว่าให้ซอร์สโค้ดถือเป็นข้อมูลสารสนเทศของธนาคาร ห้ามทำการแก้ไขเปลี่ยนแปลง หรือทำสำเนาโดยไม่ได้รับอนุญาต รวมถึงการส่งซอร์สโค้ดไปยังผู้ให้บริการภายนอกต้องอยู่บนพื้นฐานของความ

จำเป็นที่ต้องใช้งานเท่านั้นโดยพิจารณาถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อธนาคารได้ ตลอดจนกำหนดให้มีการจัดเก็บและสิทธิในการเข้าถึงที่เครื่องแม่ข่าย (Server) ของธนาคารและกระบวนการควบคุมเปลี่ยนแปลงซอร์สโค้ดอย่างเหมาะสม

4.4.4 บันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off)

เป็นข้อตกลงในการปฏิบัติงานระหว่างสายเทคโนโลยีสารสนเทศ และหน่วยงานทางธุรกิจ (Business Unit) เพื่อให้ปฏิบัติงานในฐานะผู้ใช้งาน หรือผู้ดูแลระบบงานที่เกี่ยวข้องสามารถใช้เป็นแนวทาง หลักเกณฑ์ในการปฏิบัติงานในทิศทางเดียวกันทั้งองค์กร และปฏิบัติงานให้เป็นไปตามนโยบายเทคโนโลยีสารสนเทศของธนาคารอย่างเหมาะสม ซึ่งทางสายเทคโนโลยีสารสนเทศได้มีการจัดทำบันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off) โดยมีการลงนามเป็นลายลักษณ์อักษรร่วมกันกับหัวหน้าสายงานทางธุรกิจต่าง ๆ และผ่านการตรวจทานจากสายกำกับปฏิบัติตามกฎเกณฑ์เพื่อให้เป็นไปตามหลักเกณฑ์ที่ธนาคารแห่งประเทศไทย หรือหน่วยงานกำกับอื่น ๆ กำหนด รวมถึงผ่านการลงนามรับทราบการบริหารจัดการจากสายบริหารความเสี่ยงซึ่งทำหน้าที่ควบคุม ติดตาม กำกับความเสี่ยงในทุกด้านของธนาคาร

โดยปัจจุบันสายเทคโนโลยีสารสนเทศขององค์กรศึกษา ได้จัดทำบันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off) ระหว่างสายเทคโนโลยีสารสนเทศและหน่วยงานธุรกิจส่วนงานต่าง ๆ จำนวน 2 ฉบับ โดยมีการจัดทำเอกสารเป็นลายลักษณ์อักษรผ่านการลงนามรับทราบแนวทางในการปฏิบัติงานร่วมกันทั้งธนาคารจากผู้บริหารส่วนงานต่าง ๆ และผ่านการลงนามกำกับจากสายบริหารความเสี่ยงและสายกำกับการปฏิบัติตามกฎเกณฑ์ รวมถึงมีการประกาศใช้งานเพื่อทราบให้กับพนักงานทั่วไป ดังนี้

1) บันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off) เรื่อง การใช้งานอุปกรณ์สื่อสารเคลื่อนที่ และเครือข่ายคอมพิวเตอร์ (Mobile Device and Network)

โดยมีวัตถุประสงค์เพื่อให้พนักงานธนาคารและหน่วยงานที่เกี่ยวข้อง รับทราบถึงหน้าที่ความรับผิดชอบ และขั้นตอนการใช้อุปกรณ์สื่อสารเคลื่อนที่ เพื่อเชื่อมต่อเครือข่ายและระบบงานของธนาคาร ครอบคลุม การลงทะเบียนขอใช้ การอนุมัติ การปฏิบัติเมื่อเปลี่ยนแปลงอุปกรณ์เทคโนโลยีสารสนเทศของธนาคาร หรืออุปกรณ์เทคโนโลยีสารสนเทศสูญหาย การโอนย้าย/ลาออก และการทบทวนสิทธิ เพื่อให้สามารถปฏิบัติได้ถูกต้องตามกฎระเบียบของธนาคาร (อ้างอิงระเบียบเรื่อง การใช้งานทรัพย์สินสารสนเทศ) และเป็นมาตรฐานในการทำงานร่วมกัน

การใช้งานอุปกรณ์สื่อสารเคลื่อนที่เป็นสิทธิที่กำหนดเฉพาะบุคคลที่ต้องใช้อุปกรณ์เทคโนโลยีสารสนเทศของธนาคารในการปฏิบัติงาน เพื่อสนับสนุนการดำเนินงานได้ทันต่อความต้องการทางธุรกิจ และเพื่อให้ธนาคารรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้ จึงกำหนดให้มีการควบคุม ดูแล และการอนุญาตจากธนาคาร ตลอดการใช้งานอุปกรณ์ต่าง ๆ เพื่อ

เชื่อมต่อเครือข่ายและระบบงานของธนาคาร หรือเมื่อมีการเปลี่ยนแปลง เช่น โอนย้าย/ลาออก อุปกรณ์ใด ๆ สูญหาย เป็นต้น โดยมีการกำหนดหน้าที่ความรับผิดชอบ ดังนี้

ตารางที่ 4.4.4.1 หน้าที่ความรับผิดชอบของสายงานการใช้งาน Mobile Device and Network

หน้าที่ของสายงาน	รายละเอียดความรับผิดชอบ
สายเทคโนโลยีสารสนเทศ	➢ จัดทำทะเบียนคุมการให้สิทธิใช้งานอุปกรณ์สื่อสารเคลื่อนที่เพื่อเชื่อมต่อเครือข่ายหรือระบบงานของธนาคาร ➢ ติดตั้ง และถอดถอนโปรแกรมต่าง ๆ ในอุปกรณ์สื่อสารเคลื่อนที่เมื่อมีการลงทะเบียน และถอดถอนสิทธิการใช้งาน ➢ จัดทำรายงานการทบทวนสิทธิ และปรับสิทธิในระบบงานตามผลการทบทวน
ทุกสายงานในฐานะผู้ใช้งาน	➢ ลงทะเบียนเพื่อขอใช้งานอุปกรณ์สื่อสารเคลื่อนที่ สำหรับผู้ที่ต้องใช้อุปกรณ์เทคโนโลยีสารสนเทศ ในการปฏิบัติงานของธนาคาร รวมทั้งแจ้งการเปลี่ยนแปลงที่ส่งผลกระทบต่อสิทธิการใช้งาน และความปลอดภัยของข้อมูลสารสนเทศที่ใช้งานผ่านอุปกรณ์เทคโนโลยีสารสนเทศของธนาคาร เช่น เมื่อมีการเปลี่ยนอุปกรณ์ หรืออุปกรณ์ใด ๆ สูญหาย ➢ เก็บรักษา และไม่เปลี่ยนแปลง ค่าพารามิเตอร์ของอุปกรณ์สื่อสารเคลื่อนที่ซึ่งสายเทคโนโลยีสารสนเทศเป็นผู้กำหนดให้เพื่อเชื่อมต่อเครือข่ายหรือระบบของธนาคาร ตลอดอายุการใช้อุปกรณ์เทคโนโลยีสารสนเทศ ➢ ดูแลรักษาอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งเป็นทรัพย์สินของธนาคาร รวมทั้งข้อมูลสารสนเทศของธนาคารที่ใช้งานผ่านอุปกรณ์เทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย จากการสูญหาย เสียหาย ถูกขโมย การเข้าถึง/เปิดเผยโดยไม่ได้รับอนุญาต และรับผิดชอบหากเกิดความเสียหายต่อธนาคารและบริษัทในกลุ่มธุรกิจทางการเงิน

ตารางที่ 4.4.4.1 (ต่อ)

หน้าที่ของสายงาน	รายละเอียดความรับผิดชอบ
ทุกสายงานในฐานะผู้อนุมัติ (ผู้บริหารฝ่ายงาน)	➢ พิจารณาความจำเป็น และพิจารณารับทราบความเสี่ยงผลกระทบต่อการดำเนินงาน และความมั่นคงปลอดภัยของธนาคาร ทุกครั้งที่อนุมัติสิทธิ ให้กับพนักงานภายในสายงาน ➢ ตรวจสอบรายงานการทบทวนสิทธิเพื่อทบทวนความถูกต้องและความเป็นปัจจุบันของสิทธิการเข้าถึงระบบสารสนเทศ

2) บันทึกความเข้าใจกระบวนการทำงานในการปฏิบัติระหว่างหน่วยงาน (Sign off) เรื่องการบริหารจัดการสิทธิผู้ใช้งาน และรหัสผ่าน โดยมีวัตถุประสงค์เพื่อให้พนักงานธนาคารและหน่วยงานที่เกี่ยวข้อง รับทราบถึงหน้าที่ ความรับผิดชอบ ที่มีต่อการบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่าน เพื่อให้สามารถปฏิบัติได้ถูกต้องตามกฎระเบียบของธนาคาร (อ้างอิงระเบียบเรื่องการกำหนดบัญชีผู้ใช้งาน และรหัสผ่าน) และมีมาตรฐานในการทำงานร่วมกัน รวมถึงสามารถบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่านได้อย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย โดยมีการกำหนดหน้าที่ความรับผิดชอบ ดังนี้

ตารางที่ 4.4.4.2 หน้าที่ความรับผิดชอบการบริหารจัดการสิทธิผู้ใช้งาน และรหัสผ่าน

หน้าที่ของสายงาน	รายละเอียดความรับผิดชอบ
สายเทคโนโลยีสารสนเทศ	❖ จัดการสิทธิในระบบสารสนเทศตามที่เจ้าของข้อมูล/ระบบงานอนุมัติ ❖ นำข้อมูลประเภทผู้ใช้งานมาตรฐานไปปรับใช้ในการออกแบบและพัฒนาระบบงาน ❖ บริหารจัดการสิทธิในระบบจัดการสิทธิ (IDM) ให้มีความสอดคล้องกับสิทธิในระบบสารสนเทศ ❖ จัดทำรายงานการทบทวนสิทธิของผู้ใช้งาน และปรับสิทธิในระบบสารสนเทศตามผลการทบทวน ❖ จัดการปลดรหัสผ่านในระบบสารสนเทศตามที่ได้รับแจ้งผ่าน IT Request

ตารางที่ 4.4.4.2 (ต่อ)

หน้าที่ของสายงาน	รายละเอียดความรับผิดชอบ
สายงานเจ้าของข้อมูล/ระบบงาน	❖ **ควบคุมการเข้าถึงข้อมูล และให้สิทธิการเข้าถึงระบบสารสนเทศ** ❖ **กำหนดประเภทผู้ใช้งานมาตรฐานและนำไปใช้ในการกำหนดกลุ่มผู้ใช้งานในระบบสารสนเทศ** ❖ **พิจารณาความจำเป็น ความเสี่ยง ผลกระทบต่อการดำเนินงานและความมั่นคงปลอดภัยของธนาคาร ในการอนุมัติสิทธินอกเหนือมาตรฐาน (Exception)** ❖ **ตรวจสอบสิทธิในรายงานการทบทวนสิทธิ และอนุมัติผลการทบทวนสิทธิ**
พนักงานทุกสายงาน	❖ รับทราบเรื่องการกำหนดประเภทผู้ใช้งานมาตรฐานและสิทธิในระบบสารสนเทศ และนำมาปรับใช้ในการดำเนินงาน ❖ ยื่นเรื่องร้องขอ กรณีต้องการใช้สิทธินอกเหนือมาตรฐาน (Exception) ❖ ยื่นเรื่องร้องขอ กรณีต้องการปลดรหัสผ่าน (Password) ❖ ตรวจสอบสิทธิในรายงานการทบทวนสิทธิ

4.4.5 คู่มือการปฏิบัติงาน

คู่มือการปฏิบัติงานเป็นแนวทาง วิธีการปฏิบัติงานซึ่งผู้ดูแลระบบงานสายเทคโนโลยีสารสนเทศจัดทำขึ้นเองในแต่ละส่วนงานที่รับผิดชอบหรือสามารถใช้คู่มือการปฏิบัติงานมาตรฐาน (Standard) ของซอฟต์แวร์ที่สายเทคโนโลยีสารสนเทศมีการจัดซื้อมาเป็นซอฟต์แวร์สำเร็จรูป (Software Package) รวมถึงคู่มือการปฏิบัติงานที่หน่วยงานธุรกิจ (Business Unit) จัดทำขึ้นเพื่อเป็นการถ่ายทอดการปฏิบัติงานภายในสายงานสามารถนำมาประยุกต์ใช้งานในการดำเนินการด้านเทคโนโลยีสารสนเทศได้ ซึ่งองค์กรกรณีศึกษาได้มีการจัดทำเอกสารคู่มือการปฏิบัติงานจำนวนมาก ซึ่งธนาคารขององค์กรศึกษาไม่มีการบริหารจัดการเอกสารอย่างรวมศูนย์ (Centralized Document Management) ทำให้การค้นหาอ้างอิงเอกสารที่เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จึงต้องอ้างอิงจากส่วนงานผู้ดูแลระบบงานด้าน Application, Database, Infrastructure และหน่วยงานธุรกิจตามโครงสร้างองค์กร อาทิ

ตารางที่ 4.4.5 คู่มือการปฏิบัติงานด้านเทคโนโลยีสารสนเทศขององค์กรศึกษา

คู่มือการปฏิบัติงานขององค์กรศึกษา	ตัวอย่างเอกสารคู่มือการปฏิบัติงาน
คู่มือการปฏิบัติงานของผู้ใช้งาน (User) ระบบงาน	➢ คู่มือการปฏิบัติงานกระบวนการจัดการเรื่องร้องเรียนด้านเงินฝากของลูกค้า ประจำหน่วยงาน ฝ่ายธนบดีธนกิจและพัฒนาธุรกิจสายธุรกิจเงินฝากและการตลาด ➢ คู่มือการปฏิบัติงานประจำหน่วยงานเรื่องการจัดการภายในระบบงาน ATM และ Internet Banking ของฝ่ายปฏิบัติการการเงิน
คู่มือการ Configuration / Setting ระบบงาน	➢ คู่มือการ Configuration System ของผู้ดูแลระบบ (Administrator) ➢ คู่มือการ Configuration Database ➢ คู่มือ Server Configuration
คู่มือ IT Operation	➢ คู่มือการ Monitor Backup Tape ➢ คู่มือการปฏิบัติงานสิ้นวัน (End of Day : EOD)

4.5 ความเสี่ยงขององค์กร

องค์กรกรณีศึกษาได้มีการจัดตั้งสายบริหารความเสี่ยง เพื่อทำการบริหารจัดการความเสี่ยงในด้านต่าง ๆ ของธนาคารให้เป็นไปตามหลักเกณฑ์ ข้อปฏิบัติของหน่วยงานกำกับ เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต) เป็นต้น ซึ่งสายบริหารความเสี่ยงขององค์กรศึกษาได้ทำการบริหารจัดการ ควบคุม ติดตาม และรายงานผลของความเสี่ยงที่เกิดขึ้นภายในองค์กรให้คณะกรรมการบริหารความเสี่ยง (Risk Management Committee : RMC)

4.5.1 การกำหนดประเภทความเสี่ยงของธนาคาร

สายบริหารความเสี่ยงขององค์กรศึกษา ได้มีการกำหนดประเภทความเสี่ยงของธนาคารให้มีความสอดคล้องกับหน่วยงานกำกับ และความเสี่ยงที่เกิดขึ้นภายในองค์กร เพื่อให้บริหารจัดการความเสี่ยงที่มีอยู่ภายในองค์กรได้ตรงตามความเสี่ยงที่เกิดขึ้นจริง จึงมีการกำหนดประเภทของความเสี่ยงไว้ 8 ด้าน ซึ่งประเภทของความเสี่ยงที่องค์กรกำหนดไว้ดังกล่าวนี้ มีส่วนเกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศขององค์กรด้วย ตั้งแต่การกำหนดกลยุทธ์ การบริหารจัดการความมั่นคง

ปลอดภัยของระบบงานเทคโนโลยีสารสนเทศขององค์กร ซึ่งหากเกิดความเสี่ยงหรือผลกระทบกับเทคโนโลยีสารสนเทศขององค์กร ก็อาจส่งผลต่อความเสี่ยงในประเภทต่าง ๆ ที่องค์กรกำหนดไว้ได้

ตารางที่ 4.5.1 การกำหนดประเภทความเสี่ยงขององค์กรศึกษา

ประเภทความเสี่ยง	ความหมาย
ความเสี่ยงด้านกลยุทธ์	ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และ การปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึง ความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร ภาวะการแข่งขัน ฯลฯ อันส่งผลกระทบต่อรายได้และเงินกองทุน
ความเสี่ยงด้านชื่อเสียง	ความเสี่ยงจากการที่สาธารณะชน ได้แก่ ลูกค้า คู่ค้า นักลงทุน และผู้กำกับดูแล รับรู้ถึงภาพลักษณ์ในเชิงลบ หรือขาดความเชื่อมั่น ซึ่งอาจส่งผลกระทบต่อรายได้ และ/หรือ เงินกองทุน ทั้งในปัจจุบันและอนาคต ความเสี่ยงด้านชื่อเสียงอาจเกิดจากการปฏิบัติที่ไม่สอดคล้องกับความคาดหวังของสังคม หรือมาตรฐานการบริการของธุรกิจ หรือ ไม่เป็นไปตามข้อตกลงหรือการบริการที่ไม่เป็นมิตรกับลูกค้า
ความเสี่ยงด้านเครดิต	ความเสี่ยงที่เกิดจากคู่สัญญาไม่สามารถปฏิบัติตามภาระที่ตกลงไว้ ซึ่งอาจก่อให้เกิดผลเสียหายต่อรายได้ และเงินกองทุน
ความเสี่ยงจากการกระจุกตัวด้านเครดิต	การให้สินเชื่อ ลงทุน ก่อภาระผูกพัน หรือทำธุรกรรมที่มีลักษณะคล้ายการให้สินเชื่อแก่กลุ่มลูกหนี้หรือภาคธุรกิจใดเป็นจำนวนสูงมาก ซึ่งหากเกิดความเสียหายขึ้นจะส่งผลต่อฐานะและความสามารถในการดำเนินงานอย่างมีนัยสำคัญ
ความเสี่ยงด้านตลาด	ความเสี่ยงที่อาจได้รับความเสียหายจากการเปลี่ยนแปลงมูลค่าของฐานะในงบดุลและนอกงบดุล อันเนื่องมาจากการเคลื่อนไหวของอัตราดอกเบี้ย อัตราแลกเปลี่ยนเงินตราต่างประเทศ รวมถึงราคาตราสารในตลาดเงินและตลาดทุน
ความเสี่ยงด้านอัตราดอกเบี้ยในบัญชีเพื่อการธนาคาร	ความเสียหายต่อรายได้ และ/หรือ มูลค่าทางเศรษฐกิจ จากการเปลี่ยนแปลงของอัตราดอกเบี้ย ซึ่งเกิดจากฐานะทั้งในงบดุลและนอกงบดุล ที่อยู่ในบัญชีเพื่อการธนาคาร

ตารางที่ 4.5.1 (ต่อ)

ประเภทความเสี่ยง	ความหมาย
ความเสี่ยงด้านสภาพคล่อง	**ความเสี่ยงที่ไม่สามารถชำระหนี้สิน และ ภาระผูกพันเมื่อถึงกำหนด เนื่องจากไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดหรือไม่สามารถจัดหาเงินทุนได้เพียงพอ หรือ สามารถจัดหาเงินทุนได้แต่ด้วยต้นทุนที่สูงเกินกว่าระดับที่ยอมรับได้ ซึ่งอาจเกิดผลกระทบต่อรายได้และเงินกองทุน ทั้งในปัจจุบันและในอนาคต**
ความเสี่ยงด้านปฏิบัติการ	ความเสี่ยงจากการขาดการกำกับดูแลกิจการที่ดี มีระบบการควบคุมภายในไม่เพียงพอ ละเมิดการปฏิบัติตามระบบการควบคุมภายใน หรือเนื่องจากภัยพิบัติต่าง ๆ ซึ่งอาจก่อให้เกิดปัญหาในการปฏิบัติงาน และส่งผลกระทบต่อรายได้ และเงินกองทุน

4.5.2 การกำหนดเกณฑ์การประเมินความเสี่ยงขององค์กรศึกษา

สายบริหารความเสี่ยงได้มีการกำหนดการระบุและประเมินความเสี่ยงในแต่ละสายงานขององค์กรด้วยวิธีการประเมินตนเอง (Risk and Control Self Assessment : RCSA) ในงานที่แต่ละสายงานดำเนินการปฏิบัติอยู่ ซึ่งสายงานเทคโนโลยีสารสนเทศเป็นส่วนงานหนึ่งขององค์กรที่จำเป็นต้องมีการประเมินความเสี่ยงด้วยวิธีการด้านเทคนิคเชิงคุณภาพ ที่ต้องใช้ดุลพินิจในการตัดสินใจโอกาสเหตุการณ์ที่จะเกิดขึ้น หรือผลกระทบความเสี่ยง ความเสียหายตามเกณฑ์ที่สายบริหารความเสี่ยงได้มีการกำหนดและมีการขออนุมัติจากคณะกรรมการบริหารความเสี่ยง (Risk Management Committee : RMC) ดังต่อไปนี้

4.5.2.1 ความถี่ของเหตุการณ์ (Frequency) ซึ่งเป็นโอกาสหรือความถี่ของการเกิดเหตุการณ์ (Likelihood) เพื่อประเมินสถานการณ์ของโอกาสเกิดขึ้นบ่อยเพียงใด (โดยการใช้การประมาณการของโอกาสที่เกิดขึ้น) แบ่งได้เป็น 5 ช่วง ดังนี้

1) ความถี่ของเหตุการณ์เกิดขึ้นต่ำ : เกิดขึ้นน้อยกว่า 0.33 ครั้งต่อปี
2) ความถี่ของเหตุการณ์เกิดขึ้นค่อนข้างต่ำ : เกิดขึ้น 0.33 – 5 ครั้งต่อปี
3) ความถี่ของเหตุการณ์เกิดขึ้นกลาง : เกิดขึ้น 6 – 11 ครั้งต่อปี
4) ความถี่ของเหตุการณ์เกิดขึ้นค่อนข้างสูง : เกิดขึ้น 12 – 120 ครั้งต่อปี
5) ความถี่ของเหตุการณ์เกิดขึ้นสูง : เกิดขึ้นมากกว่า 120 ครั้งต่อปี

4.5.2.2 ความเสียหาย (Impact) ซึ่งเป็นผลกระทบของความเสียหายที่เกิดขึ้นจากเหตุการณ์ เพื่อประเมินผลกระทบว่ามีความเป็นไปได้ หรือความน่าจะเป็นจำนวนเงิน หรือไม่เป็นจำนวนเงินอย่างไร ซึ่งแบ่งได้เป็นประเภทต่าง ๆ ดังนี้

- **ด้านการเงิน (Financial Impact)** เป็นจำนวนความเสียหายที่สามารถประเมินมูลค่าเป็นจำนวนเงินได้ ว่าเหตุการณ์ที่เกิดขึ้นมีจำนวนความเสียหายในแต่ละครั้งประมาณเท่าใด (ใช้การประมาณการจำนวนความเสียหายต่อครั้ง) แบ่งได้เป็น 5 ช่วง ดังนี้

1) ความเสียหายมีมูลค่าต่ำ : 0 – 50,000 บาท
2) ความเสียหายมีมูลค่าค่อนข้างต่ำ : 50,001 – 500,000 บาท
3) ความเสียหายมีมูลค่าปานกลาง : 500,001 -1,000,000 บาท
4) ความเสียหายมีมูลค่าค่อนข้างสูง : 1,000,001 – 10,000,000 บาท
5) ความเสียหายมีมูลค่าสูง : มากกว่า 10,000,000 บาท

- **ด้านกฎหมาย/กฎระเบียบ (Legal/Compliance)** เป็นผลกระทบของเหตุการณ์ที่สามารถประเมินผลกระทบขนาดความรุนแรงได้ (ใช้การประมาณผลกระทบของเหตุการณ์ต่อครั้ง) แบ่งได้เป็น 5 ช่วง ดังนี้

1) ผลกระทบต่อกฎหมาย/กฎระเบียบต่ำ : ไม่มีผลกระทบ
2) ผลกระทบต่อกฎหมาย/กฎระเบียบค่อนข้างต่ำ : เสียค่าปรับหรือถูกตักเตือน แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจธนาคาร
3) ผลกระทบต่อกฎหมาย/กฎระเบียบปานกลาง : เสียค่าปรับหรือถูกตักเตือน และมีผลกระทบต่อการดำเนินธุรกิจธนาคาร แต่ยังไม่มีผลต่อการปรับลดระดับความน่าเชื่อถือ
4) ผลกระทบต่อกฎหมาย/กฎระเบียบค่อนข้างสูง : เสียค่าปรับ มีผลกระทบต่อการดำเนินธุรกิจธนาคาร ถูกลงโทษจากทางการ อาจส่งผลต่อการปรับลดระดับความน่าเชื่อถือ เช่น โดนเพิกถอนใบอนุญาตชั่วคราว
5) ผลกระทบต่อกฎหมาย/กฎระเบียบสูง : ถูกลงโทษจากทางการในระดับรุนแรง เช่น เพิกถอนใบอนุญาตถาวร ทำธุรกรรมฟอกเงิน ไม่สำรองเงินทุน หรือถูกสั่งห้ามดำเนินธุรกิจอีกต่อไป

- **ด้านลูกค้า (Customer Impact)** เป็นผลกระทบของเหตุการณ์หรือความเสียหายที่ประเมินได้ว่ามีผลกระทบรุนแรงกับลูกค้าของธนาคาร (ใช้การประมาณการผลกระทบของเหตุการณ์ที่เกิดกับลูกค้าต่อครั้ง) แบ่งได้เป็น 5 ช่วง ดังนี้

1) ผลกระทบต่อกลุ่มลูกค้าต่ำ : น้อยกว่า 1 %
2) ผลกระทบต่อกลุ่มค่อนข้างต่ำ : 1 – 5 %
3) ผลกระทบต่อกลุ่มปานกลาง : 6 – 25 %

4) ผลกระทบต่อกลุ่มค่อนข้างสูง : 26 – 50 %

5) ผลกระทบต่อกลุ่มสูง : มากกว่า 50 %

- **ด้านชื่อเสียง (Reputational impact)** เป็นผลกระทบของเหตุการณ์ที่ประเมินว่ามีผลกระทบรุนแรงกับชื่อเสียงขององค์กร (ใช้การประมาณผลกระทบของเหตุการณ์ที่มีผลกับชื่อเสียงต่อครั้ง) แบ่งได้เป็น 5 ช่วง ดังนี้

1) ความเสียหายที่เกิดกับชื่อเสียงต่ำ : ความเสียหายที่เกิดขึ้นจำกัดวงเฉพาะภายในธนาคารเท่านั้น

2) ความเสียหายที่เกิดกับชื่อเสียงค่อนข้างต่ำ : ความเสียหายที่เกิดขึ้นรับรู้เฉพาะที่เป็นลูกค้าของธนาคาร

3) ความเสียหายที่เกิดกับชื่อเสียงปานกลาง : ความเสียหายที่เกิดขึ้นรับรู้ในหมู่ประชาชนบางส่วน อาจมีการรายงานข่าวของสื่อมวลชนในบางแขนง

4) ความเสียหายที่เกิดกับชื่อเสียงค่อนข้างสูง: ความเสียหายที่เกิดขึ้นมีรายงานข่าวความเสียหาย และวิพากษ์วิจารณ์อย่างแพร่หลายโดยสื่อมวลชนในประเทศและประชาชนทั่วไป

5) ความเสียหายที่เกิดกับชื่อเสียงสูง : ความเสียหายที่เกิดขึ้นมีรายงานข่าวอย่างแพร่หลายของสื่อมวลชนในและต่างประเทศ และมีผลกระทบต่อความน่าเชื่อถือของธนาคารในระยะยาว หรือเกิดการแห่ถอนเงินฝาก และธนาคารแห่งประเทศไทยเข้ามาตรวจเป็นกรณีพิเศษ

ซึ่งสามารถสรุปเป็นตารางเพื่อการอธิบายเกณฑ์การกำหนดความถี่และผลกระทบของความเสียหายที่สายบริหารความเสี่ยงกำหนด

ตารางที่ 4.5.2.1 เกณฑ์การประเมินความเสี่ยงจากความถี่ของเหตุการณ์ที่เกิดขึ้น

ความถี่ของเหตุการณ์ (Frequency)	
ต่ำ	เกิดขึ้นน้อยกว่า 0.33 ครั้งต่อปี
ค่อนข้างต่ำ	เกิดขึ้น 0.33 – 5 ครั้งต่อปี
ปานกลาง	เกิดขึ้น 6 – 11 ครั้งต่อปี
ค่อนข้างสูง	เกิดขึ้น 12 – 120 ครั้งต่อปี
สูง	เกิดขึ้นมากกว่า 120 ครั้งต่อปี

ตารางที่ 4.5.2.2 เกณฑ์การประเมินความเสี่ยงจากผลกระทบ/ความเสียหายที่เกิดขึ้น

ผลกระทบ/ความเสียหายที่เกิดขึ้น				
ระดับ	**ด้านการเงิน**	**ด้านกฎระเบียบ/กฎหมาย**	**ด้านลูกค้า**	**ด้านชื่อเสียง**
ต่ำ	0 – 50,000 บาท	ไม่มีผลกระทบ	< 1 %	ความเสียหายที่เกิดขึ้นจำกัดวงเฉพาะภายในธนาคารเท่านั้น
ค่อนข้างต่ำ	50,001 – 500,000 บาท	เสียค่าปรับหรือถูกตักเตือน แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจธนาคาร	1 – 5 %	ความเสียหายที่เกิดขึ้นรับรู้เฉพาะที่เป็นลูกค้าของธนาคาร
ปานกลาง	500,001 - 1,000,000 บาท	เสียค่าปรับหรือถูกตักเตือน และมีผลกระทบต่อการดำเนินธุรกิจธนาคาร แต่ยังไม่มีผลต่อการปรับลดระดับความน่าเชื่อถือ	6 – 25 %	ความเสียหายที่เกิดขึ้นรับรู้ในหมู่ประชาชนบางส่วน อาจมีการรายงานข่าวของสื่อมวลชนในบางแขนง
ค่อนข้างสูง	1,000,001 – 10,000,000 บาท	เสียค่าปรับ มีผลกระทบต่อการดำเนินธุรกิจธนาคาร ถูกลงโทษจากทางการ อาจส่งผลต่อการปรับลดระดับความน่าเชื่อถือ เช่น โดนเพิกถอนใบอนุญาตชั่วคราว	26 – 50 %	ความเสียหายที่เกิดขึ้นมีรายงานข่าวความเสียหาย และวิพากษ์วิจารณ์อย่างแพร่หลายโดยสื่อมวลชนในประเทศและประชาชนทั่วไป
สูง	>10,000,000 บาท	ถูกลงโทษจากทางการในระดับรุนแรง เช่น เพิกถอนใบอนุญาตถาวร ทำธุรกรรมฟอกเงิน ไม่สำรองเงินทุน หรือถูกสั่งห้ามดำเนินธุรกิจอีกต่อไป	> 50 %	ความเสียหายที่เกิดขึ้นมีรายงานข่าวอย่างแพร่หลายของสื่อมวลชนในและต่างประเทศ และมีผลกระทบต่อความน่าเชื่อถือของธนาคารในระยะยาว เกิดการแห่ถอนเงินฝาก ธนาคารแห่งประเทศไทยเข้ามาตรวจเป็นกรณีพิเศษ

4.6 การควบคุมภายในองค์กรศึกษา

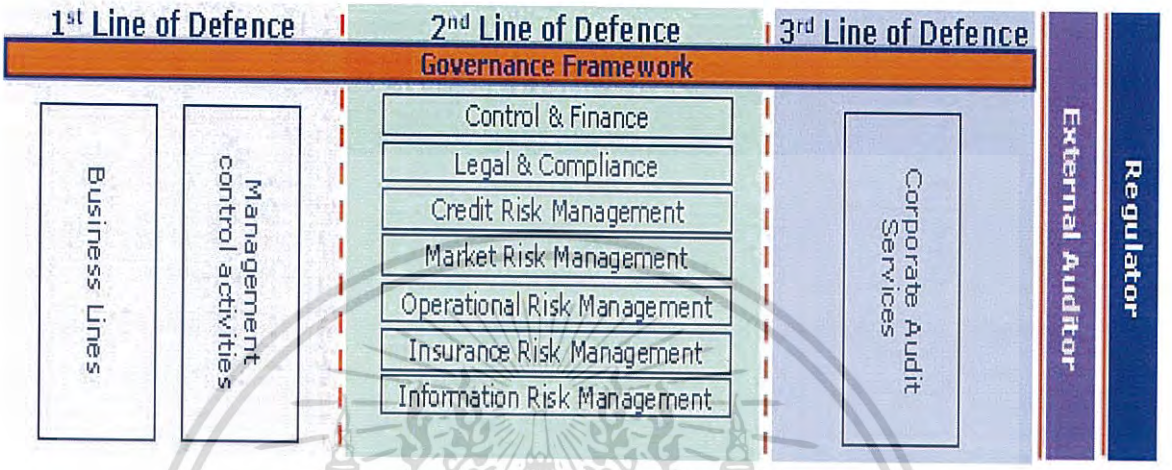
การควบคุมภายในเป็นกระบวนการที่กำหนดขึ้นและนำมาใช้โดยผู้บริหารทุกระดับ รวมถึงบุคลากรต่าง ๆ ขององค์กรเพื่อให้เกิดความมั่นใจว่าองค์กรมีการควบคุม สามารถตรวจสอบ สอบทานความถูกต้องระหว่างกันได้ในทุกกระบวนการอย่างสมเหตุสมผล เพื่อบรรลุเป้าหมายขององค์กร ซึ่งเทคโนโลยีสารสนเทศขององค์กรศึกษา ก็เป็นปัจจัยหนึ่งที่ต้องมีการควบคุมภายในให้ระบบงานเทคโนโลยีสารสนเทศสามารถทำงานได้อย่างถูกต้องเหมาะสม ครบถ้วนตามขั้นตอนหรือกระบวนการประมวลผลตามมาตรฐานที่ควรมีการดำเนินการ โดยในการตรวจสอบการควบคุมภายในเป็นการให้ข้อแนะนำ หรือข้อเสนอแนะบนพื้นฐานของมาตรฐานที่ควรปฏิบัติงานโดยผู้ตรวจสอบมีการใช้ดุลพินิจ ประสบการณ์ หรือความเชี่ยวชาญของผู้ตรวจสอบ ผู้บริหารการตรวจสอบ ซึ่งเป็นการให้ข้อเสนอแนะเพื่อให้สายเทคโนโลยีสารสนเทศดำเนินการปรับปรุงให้มีคุณภาพในการสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของธนาคาร โดยสายเทคโนโลยีสารสนเทศควรมีการนำมาตรฐานการบริหารจัดการสารสนเทศมาใช้ในการควบคุมภายในตั้งแต่ระดับนโยบาย ระเบียบ หลักเกณฑ์ คู่มือการปฏิบัติงานตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Management System : ISMS) ซึ่งในการตรวจสอบการควบคุมภายในของผู้ตรวจสอบเทคโนโลยีสารสนเทศขององค์กรศึกษาจำเป็นต้องศึกษามาตรฐานดังกล่าวจากวิธีการกำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ในส่วนของการกำกับ การควบคุม ติดตาม สื่อสารการปฏิบัติงานภายในสายเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้องในการปฏิบัติงานให้เป็นไปตามนโยบายด้านเทคโนโลยีสารสนเทศ (IT Policy) ให้กับผู้ที่เกี่ยวข้องทราบ เพื่อเป็นไปตามแนวทางการปฏิบัติงานภายในธนาคารทิศทางเดียวกันทั้งองค์กร

ธนาคารพาณิชย์ดังกล่าวที่เป็นองค์กรศึกษาได้มีการกำหนดแนวป้องกันสามชั้น (Three Lines of Defence) ซึ่งตามหลักการของแนวป้องกันสามชั้นของสมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditor : IIA) ประกอบด้วยหน่วยงานต่าง ๆ ดังนี้

1. หน่วยงานในแนวป้องกันชั้นที่หนึ่ง (First Line of Defence) ได้แก่ สายธุรกิจ และสายปฏิบัติการต่าง ๆ มีหน้าที่จัดให้มีคู่มือการปฏิบัติงานประจำวันและระบบควบคุมภายในให้รัดกุมเป็นไปตามกรอบการบริหารความเสี่ยงแต่ละด้านที่กำหนดโดยสายบริหารความเสี่ยง และหน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ เป็นต้น

2. หน่วยงานในแนวป้องกันชั้นที่สอง (Second Line of Defence) ได้แก่ สายบริหารความเสี่ยง หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ ควบคุมบัญชีการเงิน เป็นต้น มีหน้าที่กำหนดกรอบนโยบายการควบคุมความเสี่ยง เสนอให้คณะกรรมการชุดต่าง ๆ ที่เกี่ยวข้องเป็นผู้อนุมัติและมีการควบคุมติดตาม (Monitor) เป็นครั้งคราว

3. หน่วยงานในแนวป้องกันที่สาม (Third Line of Defence) โดยมีสายตรวจสอบภายในเป็นหน่วยงานอิสระทำหน้าที่ตรวจสอบประสิทธิภาพและประสิทธิผลของกลไกและการปฏิบัติงานของหน่วยงานในแนวป้องกันชั้นที่หนึ่งและสองดังกล่าว และรายงานผลการตรวจสอบให้คณะกรรมการธนาคาร คณะกรรมการตรวจสอบ และผู้บริหารระดับสูงทราบ



รูปที่ 4.6 แนวป้องกันสามชั้น (Three Lines of Defence)

บทที่ 5
การพัฒนาแบบจำลอง

การพัฒนาแบบจำลองโครงการศึกษามาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) ในขอบเขตของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) ต้องมีการพัฒนาแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ เพื่อประเมินการดำเนินการของผู้ปฏิบัติงานที่มีอยู่ในปัจจุบัน ซึ่งเมื่อรับรู้และทราบว่าการควบคุมที่มีอยู่ ณ ปัจจุบันจุดใดมีความเสี่ยงสูง หรือมีการควบคุมที่ยังไม่เหมาะสม จึงควรมีการพัฒนาต่อไป โดยการทำให้ผู้ปฏิบัติงานเห็นภาพนั้น จึงนำมาสู่การพัฒนาแบบจำลองแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อทำให้ผู้ปฏิบัติงานเข้าใจถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจมีโอกาสและผลกระทบจากการเกิดการควบคุมภายในที่ไม่เหมาะสมนำไปสู่ความเสี่ยงขององค์กรได้

5.1 การพัฒนาการสร้างแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

การพัฒนาแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ จากมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) โดยมีการดำเนินการดังนี้

5.1.1 การสำรวจตัวชี้วัดการดำเนินการที่เหมาะสมกับธนาคาร

เป็นการดำเนินการสำรวจตัวชี้วัดเพื่อการวัดผลการดำเนินการจากแบบจำลอง ตั้งแต่การกำหนดนโยบายด้านการจัดการเข้าถึงระบบสารสนเทศ รวมทั้งวิธีการ เทคนิคในการจัดการความมั่นคงปลอดภัย จากผู้บริหารด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นผู้เชี่ยวชาญด้านเทคนิคการกำหนดความมั่นคงปลอดภัยของธนาคาร และผู้เชี่ยวชาญด้านการควบคุมภายใน จำนวนทั้งสิ้น 11 ท่าน ร่วมประเมินแบบสอบถามเกี่ยวกับเกณฑ์ การบริหารจัดการความมั่นคงปลอดภัยขององค์กร ตามมาตรฐาน ISO 27001 ในขอบเขตการเข้าถึงระบบสารสนเทศของธนาคาร (Acess Control) **(ภาคผนวก ก)**

โดยในส่วนที่ 1 ของแบบสอบถาม เป็นส่วนที่เกี่ยวข้องกับประชากรและกลุ่มตัวอย่างที่มีผลต่อแบบประเมินความเป็นผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (Expert Information Technology) และผู้เชี่ยวชาญด้านการควบคุมภายใน (Expert Internal Audit) โดยจำเป็นต้องมีประสบการณ์อย่างครบถ้วน ดังนี้

- ผู้ตอบแบบสำรวจต้องมีประสบการณ์ทำงานในสายงานธุรกิจที่เกี่ยวข้องกับธนาคารพาณิชย์

- ผู้ตอบแบบสอบถามต้องมีประสบการณ์ทำงานในส่วนงานสายเทคโนโลยีสารสนเทศหรือสายงานที่เกี่ยวข้องกับการควบคุมภายใน

- ผู้ตอบแบบสอบถามต้องมีประสบการณ์ในการทำงานธนาคารพาณิชย์ไม่ต่ำกว่า 3 ปี เป็นต้นไป

ในส่วนที่ 2 ประเภทของแบบสอบถามที่จัดทำ เป็นแบบเลือกตอบคำตอบเดียว ในการประเมินความเห็นตามทัศนคติเพื่อการบริหารจัดการความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศของธนาคาร (Access Control) ที่ดีและมีความเหมาะสมกับธนาคาร โดยแบบสอบถามนี้จะเป็นการถามคำถามที่มีหลายคำตอบให้เลือก แต่เลือกได้เพียงคำตอบเดียว ซึ่งเป็นส่วนของข้อมูลที่ให้ผู้เชี่ยวชาญเป็นผู้ตอบแบบสอบถาม มีจำนวน 7 ข้อ

ดังนั้น สามารถสรุปผลแบบสำรวจตัวชี้วัดเพื่อการบริหารจัดการความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศของธนาคาร(Access Control) ได้ดังนี้

ตารางที่ 5.1.1.1 สรุปผลแบบสำรวจตัวชี้วัดที่เหมาะสมกับธนาคาร

รายละเอียด	ข้อ7.1	ข้อ 7.2	ข้อ 7.3	ข้อ 7.4	ข้อ 7.5	ข้อ 7.6	ข้อ 7.7	
ผู้เชี่ยวชาญท่านที่ 1	100	100	75	75	100	50	75	
ผู้เชี่ยวชาญท่านที่ 2	100	75	100	100	100	100	100	
ผู้เชี่ยวชาญท่านที่ 3	75	50	100	100	50	75	100	
ผู้เชี่ยวชาญท่านที่ 4	50	75	100	75	100	100	100	
ผู้เชี่ยวชาญท่านที่ 5	75	75	100	75	100	100	75	
ผู้เชี่ยวชาญท่านที่ 6	100	75	100	75	100	100	75	
ผู้เชี่ยวชาญท่านที่ 7	100	100	100	75	50	75	75	
ผู้เชี่ยวชาญท่านที่ 8	75	75	50	100	75	75	100	
ผู้เชี่ยวชาญท่านที่ 9	100	75	100	100	100	75	100	
ผู้เชี่ยวชาญท่านที่ 10	75	100	75	75	75	50	100	
ผู้เชี่ยวชาญท่านที่ 11	100	100	100	100	75	75	75	
ค่าเฉลี่ยแต่ละข้อ	**86.36**	**81.82**	**90.91**	**86.36**	**84.09**	**79.55**	**88.64**	**85.39**

โดยจากแบบสอบถามเกณฑ์การบริหารจัดการความมั่นคงปลอดภัยขององค์กร ตามมาตรฐาน ISO/IEC 27001 ในขอบเขตการเข้าถึงระบบสารสนเทศของธนาคาร (Acess Control) นำมาสู่การดำเนินการจัดทำตารางเพื่อชี้วัดในแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ ได้ดังต่อไปนี้

1) การแบ่งระดับการสำรวจได้เป็น 5 ระดับที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายใน ได้แก่

- **ระดับ Excellent** เป็นระดับที่มีการบริหารจัดการความมั่นคงปลอดภัยที่ดีมาก ซึ่งจากการสำรวจที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในพึงพอใจและคาดหวังให้ระบบเทคโนโลยีสารสนเทศของธนาคารมีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยสูงที่สุด
- **ระดับ Good** เป็นระดับที่มีการบริหารจัดการความมั่นคงปลอดภัยที่ดี ซึ่งจากการสำรวจที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในพึงพอใจและคาดหวังให้ระบบเทคโนโลยีสารสนเทศของธนาคารมีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยที่ดี
- **ระดับ Marginal** เป็นระดับที่มีการบริหารจัดการความมั่นคงปลอดภัยที่พอใช้ ซึ่งจากการสำรวจที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในยังพอใจต่อความเพียงพอในการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศของธนาคารมีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัยในระดับที่ยอมรับได้ แต่หากให้มีการบริหารจัดการที่ดีมากยิ่งขึ้นควร เพิ่มเติม ปรับปรุง การจัดการให้อยู่ในระดับที่ดี หรือดีมาก
- **ระดับ Poor** เป็นระดับที่มีการบริหารจัดการความมั่นคงปลอดภัยที่ต้องปรับปรุง ซึ่งจากการสำรวจที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในยังไม่พึงพอใจต่อความเพียงพอในการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศของธนาคารให้มีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัย ซึ่งควรปรับปรุง แก้ไข เพิ่มเติมการบริหารจัดการให้อยู่ในระดับที่เหมาะสมมากยิ่งขึ้น
- **ระดับ At Risk** เป็นระดับที่มีการบริหารจัดการความมั่นคงปลอดภัยที่มีความเสี่ยงมาก ซึ่งจากการสำรวจที่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในไม่พึงพอใจต่อการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศของธนาคาร ที่ไม่มีการควบคุมการเข้าถึงที่มีความมั่นคงปลอดภัย ซึ่งควรปรับปรุง แก้ไข เพิ่มเติมการบริหารจัดการให้อยู่ในระดับที่เหมาะสมอย่างเร่งด่วน

2) ค่าตัวชี้วัด (Indicatior) เพื่อการประเมินการควบคุมภายในที่สำรวจจากผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายใน

3) ค่าต่ำสุด (Minimum) และค่าสูงสุด (Maximum) จากแบบสำรวจที่สามารถยอมรับได้ในแต่ละเกณฑ์ของผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายใน

ตารางที่ 5.1.1.2 การแบ่งระดับแบบสำรวจตัวชี้วัดที่เหมาะสมกับธนาคาร

Rating	Indicator	Minimum	Maximum
Excellent	100.00	92.71	100.00
Good	92.70	85.40	92.70
Marginal	85.39	67.70	85.39
Poor	67.69	50.01	67.69
At Risk	50.00	0.00	50.00

5.1.2 การสร้างแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

จากแบบสำรวจตัวชี้วัดการดำเนินการที่เหมาะสมกับการสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร นำมาสู่การสร้างแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศในขอบเขตของการศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) เพื่อให้ผู้ศึกษาโครงการสามารถนำแบบจำลองโครงการดังกล่าวมาสร้างเป็นข้อกำหนด / ข้อควรปฏิบัติ (Best or Good Practice) ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีกลไกการควบคุมการเข้าถึง หรือใช้งานให้มีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐาน (ISO/IEC 27001) ซึ่งสามารถดำเนินการได้โดยดังต่อไปนี้

1) การนำแนวทางปฏิบัติงานจากมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) ใน 7 หัวข้อเรื่องการการบริหารจัดการเพื่อการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) มาจัดสร้างเป็นตารางแบบจำลอง

2) กำหนดแนวคำถามเพื่ออธิบายข้อกำหนดที่ธนาคารควรมีการปฏิบัติตามเพื่อให้เกิดการจัดการระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัยที่ดี และเหมาะสมกับธนาคาร

3) กำหนดเกณฑ์การประเมินผลว่าธนาคารมีการดำเนินการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศในลักษณะใดบ้าง ได้แก่

- Preventive Control เป็นแนวทางปฏิบัติของธนาคารเพื่อประเมินว่ามีการควบคุมภายในแบบป้องกัน หรือลดความเสี่ยงจากความผิดพลาด ความเสียหายจากเหตุการณ์ที่เกิดขึ้น หรือการรักษาความปลอดภัย เช่น กำหนดนโยบาย ระเบียบหลักเกณฑ์ให้ชัดเจนเป็นลายลักษณ์อักษร การแบ่งแยกหน้าที่การงาน การควบคุมการเข้าถึงทรัพย์สินธนาคารไว้อย่างเหมาะสมหรือไม่
- Detective Control เป็นแนวทางปฏิบัติของธนาคารเพื่อประเมินว่ามีการควบคุมภายในแบบตรวจหา หรือทำการตรวจสอบ ตรวจเช็ค ค้นหาข้อผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การติดตาม (Monitor) ด้วยคนหรือเครื่องมือ (Tools) ใดๆ ในการ การสอบทานงาน ยืนยันสิทธ์การเข้าถึงอย่างสม่ำเสมอ ตลอดจดการใช้เครื่องมือเทคโนโลยีสารสนเทศทำการตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ผิดปกติ หรือไม่เหมาะสมหรือไม่
- Corrective Control เป็นแนวทางปฏิบัติของธนาคารเพื่อประเมินว่ามีการควบคุมภายในเพื่อแก้ไขข้อผิดพลาดหรือเหตุการณ์ที่เกิดขึ้นให้ถูกต้อง จากการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร เพื่อหาแนวทางการแก้ไขปัญหาไม่ให้เกิดข้อผิดพลาดซ้ำอีกภายในองค์กรไว้หรือไม่

4) ผลการประเมินการดำเนินการเพื่อการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) ตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) จากเกณฑ์ที่กล่าวมาข้างต้นซึ่งหากมีการดำเนินการที่เป็น Yes หรือ No จะแสดงออกมาเป็นเปอร์เซ็นต์ของการดำเนินการที่มีอยู่ในปัจจุบันด้วยวิธีการคำนวณแบบอัตโนมัติ ในช่องแสดงผล Percentage ดังนี้

ตารางที่ 5.1.2.1 แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)		**เพื่อควบคุมการเข้าถึงสารสนเทศ**				-
1.1.1	นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ				
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)		**เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต**				-
1.2.1	การลงทะเบียนพนักงาน (User registration)	ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น				

ตารางที่ 5.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
1.2.2	การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน				
1.2.3	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย				
1.2.4	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้				
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		**เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ**				-
1.3.1	การใช้งานรหัสผ่าน (Password use)	ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน				
1.3.2	การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)	ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล				

ตารางที่ 5.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)		**เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต**				-
1.4.1	นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้				
1.4.2	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้				
1.4.3	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ซึ่งได้รับอนุญาตแล้ว				
1.4.4	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ	ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทาง				

ตารางที่ 5.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
	(Remote diagnostic and configuration port protection)	กายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย				
1.4.5	การแบ่งแยกเครือข่าย (Segregation in networks)	ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ				
1.4.6	การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้				
1.4.7	การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง				
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)		**เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต**				-

ตารางที่ 5.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.5.1	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ				
1.5.2	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ				
1.5.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ				
1.5.4	การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว				
1.5.5	การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้				

ตารางที่ 5.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance Preventive Control	 Detective Control	 Corrective Control	Percentage
1.5.6	การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง				
1.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)		**เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต**				-
1.6.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงต้องแยกตามประเภทผู้ใช้งาน				
1.6.2	การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ				

ตารางที่ 5.1.2.1 (ต่อ)

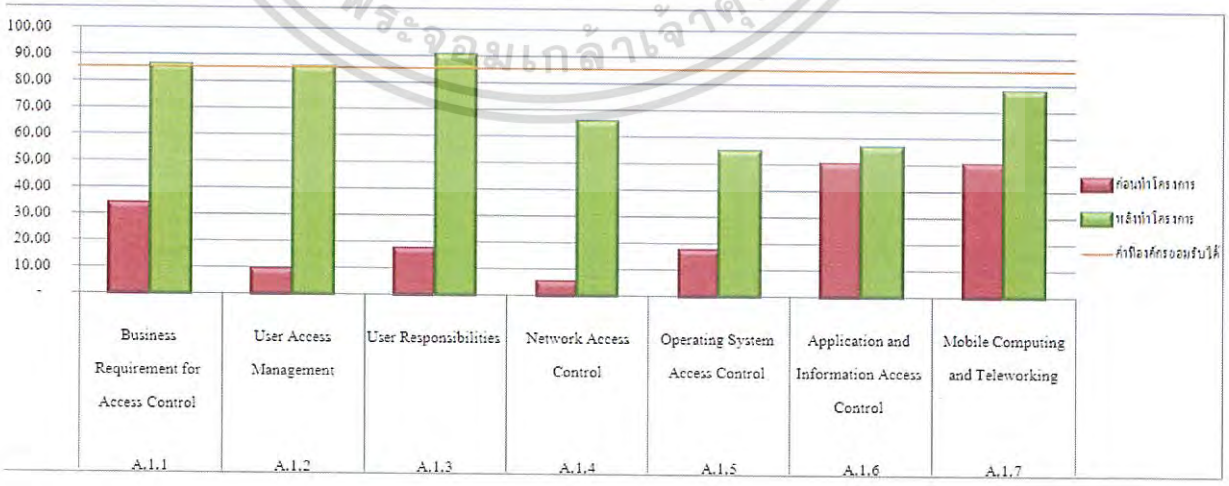
หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)		**เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**				-
1.7.1	การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้				
1.7.2	การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน				

ซึ่งจากการนำแบบจำลองมาประเมินจะสามารถทำให้ทราบว่า ระบบงานเทคโนโลยีสารสนเทศของธนาคารมีการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพียงใด และอยู่ในระดับที่เพียงพอที่องค์กรสามารถยอมรับได้ ดังตาราง

ตารางที่ 5.1.2.2 ผลสรุปแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

A.1	Access Control	Overall Rating	Overall Risk
		-	At Risk
A.1.1	Business Requirement for Access Control	-	At Risk
A.1.2	User Access Management	-	At Risk
A.1.3	User Responsibilities	-	At Risk
A.1.4	Network Access Control	-	At Risk
A.1.5	Operating System Access Control	-	At Risk
A.1.6	Application and Information Access Control	-	At Risk
A.1.7	Mobile Computing and Teleworking	-	At Risk

โดยหากผู้ศึกษาโครงการทำการสรุปผลแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศแล้วนั้น ก็สามารถนำมาจัดทำเป็นแผนภูมิภาพให้เห็นถึงข้อมูลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน (ISO/IEC 27001) และระดับที่องค์กรยอมรับได้ ดังนี้



รูปที่ 5.1.2 แผนภูมิแสดงผลสรุปแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

5.2 การพัฒนาการสร้างแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ผู้ศึกษาโครงการต้องทำการสร้างแบบจำลอง และประเมินโครงการแล้วพบว่า มีหัวข้อการที่อยู่ต่ำกว่าเกณฑ์ที่ผู้บริหารธนาคารก อันประกอบด้วยผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในของธนาคารยอมรับได้ เช่น อยู่ในเกณฑ์ที่มีความเสี่ยงสูง (At Risk) หรือต้องปรับปรุง (Poor) นั้นควรทำการประเมินให้ผู้รับการตรวจสอบเห็นภาพการดำเนินการที่มีอยู่ซึ่งมีความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงขององค์กรได้

ซึ่งการสร้างแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะทำให้ผู้ปฏิบัติงานทราบและแสดงเห็นถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีผลต่อความเสี่ยงขององค์กร (ธนาคาร) ได้ จึงนำมาสู่การสร้างแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

1) นำหัวข้อเรื่องจากการประเมินการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศที่พบว่าอยู่ในระดับความเสี่ยงสูง (At Risk) หรือ ระดับที่ควรปรับปรุง (Poor) มาเพื่อประเมินว่ามีความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งสอดคล้องกับความเสี่ยงขององค์กรประเภทใด และมีรายละเอียดของความเสี่ยงอย่างไร

ตารางที่ 5.2.1 การกำหนดประเภทความเสี่ยงในแบบจำลอง

Risks		
#	Risk Category	Risk Description
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ

RRAM - RISK OVERVIEW

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control

วันที่ประเมิน : วว-ดด-ปปปป

Risks

#	Risk Category	Risk Description
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ

รูปที่ 5.2.1 การระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง

2) กำหนดการประเมิน Likelihood ซึ่งเป็นโอกาสหรือความถี่ของการเกิดเหตุการณ์ เพื่อประเมินสถานการณ์ของโอกาสเกิดขึ้นบ่อยเพียงใด โดยการใช้การประมาณการของโอกาสที่เกิดขึ้นได้มากที่สุด (จำนวนเท่าไรต่อปีที่สามารถมีโอกาสเกิดเหตุการณ์ได้)

ตารางที่ 5.2.2 การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์

LIKELIHOOD						
#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	Participant 3
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes			
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes			

ตารางที่ 5.2.2 (ต่อ)

LIKELIHOOD						
#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	Participant 3
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes			
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes			
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes			

RRAM - RISK ASSESSMENT (LIKELIHOOD)

ชื่อการตรวจสอบ : *ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control*

วันที่ประเมิน : *วว-ดด-ปปปป*

LIKELIHOOD (score 1-5)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes		
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes		
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes		
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes		
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes		

รูปที่ 5.2.2 การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง

3) กำหนดการประเมิน Impact ซึ่งเป็นผลกระทบหรือความเสียหายของการเกิดเหตุการณ์เพื่อประเมินสถานการณ์ความเสียหายที่มากที่สุดที่อาจเกิดขึ้นได้ ทั้งในด้านความเสียหายที่เป็นตัวเงิน ผลกระทบที่ไม่เป็นตัวเงิน เช่น ด้านกฎหมาย/กฎระเบียบ ด้านชื่อเสียง หรือลูกค้า โดยการใช้การประมาณการของความเสียหายที่มากที่สุด (จำนวนเท่าไรต่อการเกิดเหตุการณ์ขึ้น)

ตารางที่ 5.2.3 การประเมินผลกระทบหรือความเสียหายของการเกิดเหตุการณ์

IMPACT				Participant1			
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes				
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes				
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes				
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes				
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes				

RRAM - RISK ASSESSMENT (IMPACT)

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control

วันที่ประเมิน : วว-ดด-ปปปป

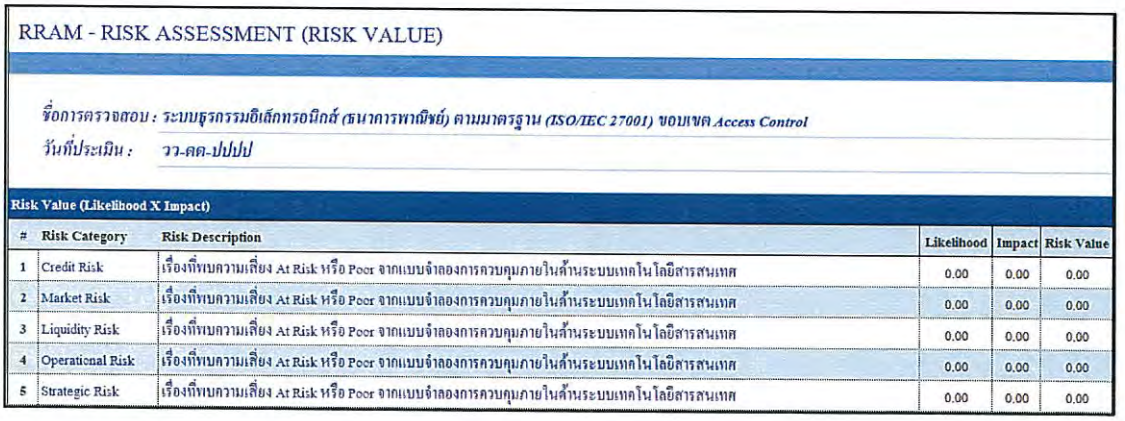
IMPACT (score 1-11)				Participant1				Participant2			
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านปฏิบัติการ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านปฏิบัติการ	ด้านชื่อเสียง	ด้านลูกค้า
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes								
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes								
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes								
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes								
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	Yes								

รูปที่ 5.2.3 การประเมินผลกระทบหรือความเสียหายของเหตุการณ์ในแบบจำลองที่จัดสร้าง

4) ผลลัพธ์ของการแสดงแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ มาจากการมูลค่าความเสียหายที่อาจจะเกิดขึ้นได้ (Risk Value) ซึ่งเกิดขึ้นได้จากการที่โอกาสหรือความถี่ของการเกิดเหตุการณ์ขึ้น คูณผลกระทบหรือความเสียหายที่เกิดขึ้น ซึ่งสามารถคิดคำนวณได้ดังนี้

ตารางที่ 5.2.4.1 วิธีการคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้นได้ในแบบจำลองความเสี่ยง

เรื่องที่เกิดความเสี่ยง	Likelihood Level	Impact Level	Risk Value	Risk Rating
เรื่องที่พบความเสี่ยงระดับ At Risk หรือ Poor	1	1	1	ต่ำ
เรื่องที่พบความเสี่ยงระดับ At Risk หรือ Poor	4	3	12	ปานกลาง
เรื่องที่พบความเสี่ยงระดับ At Risk หรือ Poor	5	5	25	สูง



RRAM - RISK ASSESSMENT (RISK VALUE)

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control

วันที่ประเมิน : วว-ดด-ปปปป

Risk Value (Likelihood X Impact)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
1	Credit Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	0.00	0.00	0.00
2	Market Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	0.00	0.00	0.00
3	Liquidity Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	0.00	0.00	0.00
4	Operational Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	0.00	0.00	0.00
5	Strategic Risk	เรื่องที่พบความเสี่ยง At Risk หรือ Poor จากแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ	0.00	0.00	0.00

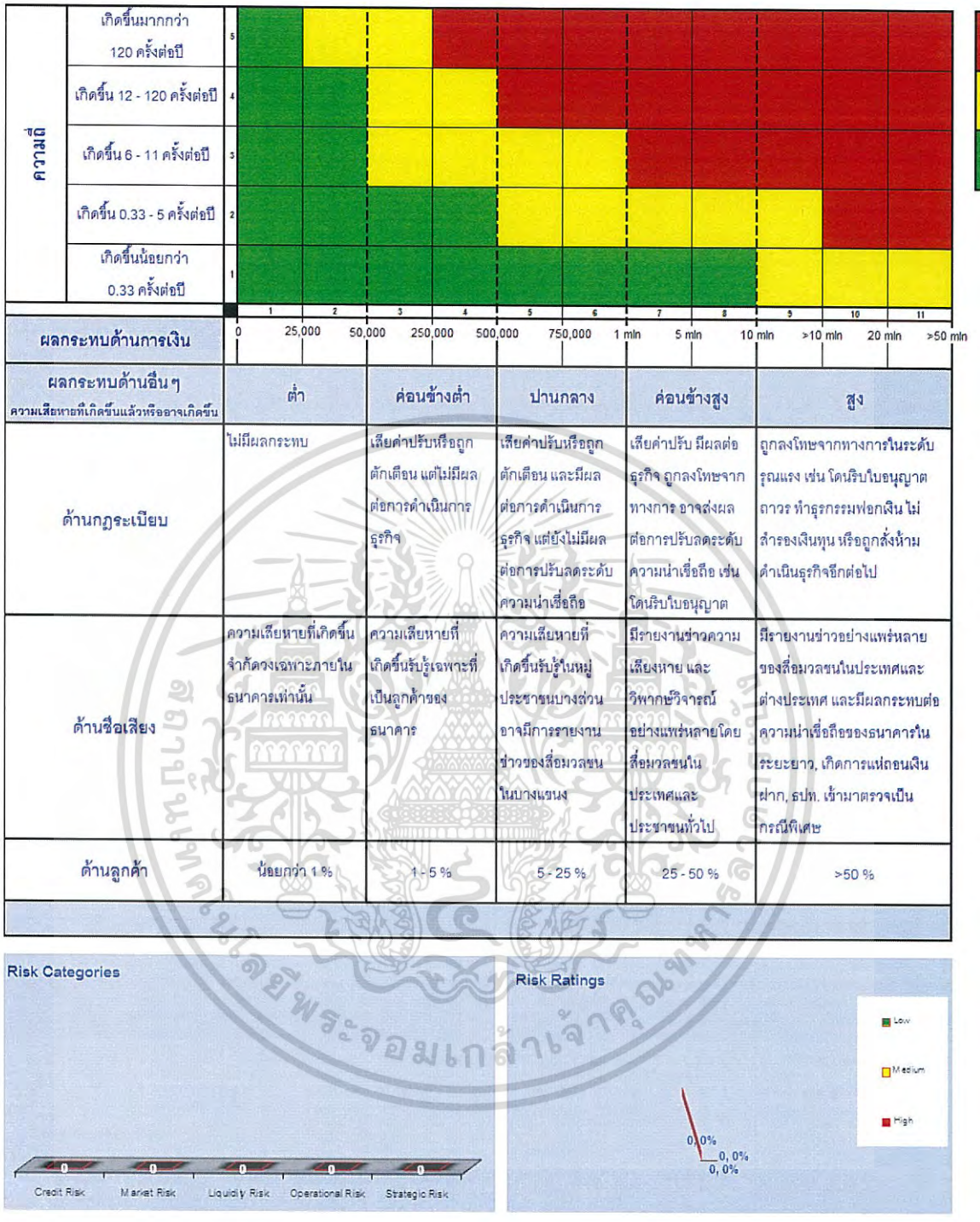
รูปที่ 5.2.4 วิธีการคำนวณมูลค่าความเสียหาย (RiskValue)

โดยจากการสำรวจตัวชี้วัดการดำเนินการที่เหมาะสมกับธนาคาร สามารถนำมาคำนวณและสร้างเป็นเกณฑ์ระดับการประเมินความเสี่ยงให้สอดคล้องกับเกณฑ์การยอมรับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งผู้เชี่ยวชาญจากด้านเทคโนโลยีสารสนเทศ และผู้เชี่ยวชาญด้านการควบคุมภายในสามารถยอมรับความเสี่ยงขององค์กรได้ ดังตาราง

ตารางที่ 5.2.4.2 ระดับการประเมินความเสี่ยงในแบบจำลองความเสี่ยง

ระดับการประเมินความเสี่ยง (Risk Rating)		
ระดับคะแนนความเสี่ยงจากการประเมินผล	เกณฑ์ความเสี่ยง	การตอบสนองความเสี่ยง
1-8	ต่ำ	เป็นระดับความเสี่ยงที่องค์กรสามารถยอมรับได้
9-18	ปานกลาง	เป็นระดับความเสี่ยงที่องค์กรควรมีมาตรการควบคุมหรือลดความเสี่ยงให้ไปอยู่ในระดับที่องค์กรยอมรับได้
19-55	สูง	เป็นระดับความเสี่ยงที่องค์กรควรมีมาตรการจัดการอย่างเร่งด่วน เพื่อลดความเสี่ยง หรือยกเลิกการดำเนินกิจกรรมที่ทำ เพื่อให้องค์กรมีการบริหารจัดการที่ดีมากยิ่งขึ้น

ซึ่งจากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโครงการแล้วนั้น ผู้ศึกษาโครงการสามารถแสดงเป็นแผนภาพแบบจำลองความเสี่ยงที่แสดงให้เห็นระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงขององค์กรได้ดังแผนภาพ Risk Rating Matrix ดังต่อไปนี้



รูปที่ 5.2.4 ผลลัพธ์ที่ได้จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศที่จัดสร้าง

บทที่ 6
การทดสอบแบบจำลอง (ก่อนทำโครงการ)

การทดสอบแบบจำลองโครงการ (ก่อนทำโครงการ) เป็นการนำแบบจำลองที่มีการพัฒนาเพื่อมาใช้ในการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนทเทศ ที่มีการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารในปัจจุบัน จากผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศของธนาคาร และเมื่อทราบการควบคุมภายในว่าจุดใดมีความเสี่ยง หรือมีการควบคุมภายในไม่เหมาะสม แล้วจึงนำจุดที่มีการควบคุมภายในที่ยังไม่เหมาะสม หรืออยู่ต่ำกว่าระดับเกณฑ์ที่องค์กรยอมรับได้ มาประเมินให้เห็นภาพรวมของความเสี่ยงบนแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ทราบถึงความเสี่ยงที่สอดคล้องกับองค์กรกำหนดไว้ ซึ่งเมื่อเกิดเหตุการณ์ดังกล่าวขึ้นอาจส่งผลเสียหายต่อธนาคาร โดยทำการประเมินความเสี่ยงจากแบบจำลองที่พัฒนา พร้อมทั้งเสนอแนะแนวทางการบริหารจัดการเพื่อให้ธนาคารมีการเพิ่มเติมปรับปรุงการบริหารจัดการให้มีความเหมาะสมอยู่ในระดับที่องค์กรยอมรับได้

6.1 การประเมินผลการจัดทำโครงการ (ก่อนทำโครงการ)

จากขอบเขตการพัฒนาแบบจำลองการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศนำมาสู่การประเมินผลการโครงการ โดยทำการประเมินผลโครงการที่มีการปฏิบัติงานในปัจจุบันของธนาคารพาณิชย์แห่งหนึ่ง เพื่อแสดงให้เห็นการบริหารจัดการความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศตามมาตรฐาน (ISO/IEC 27001) ซึ่งได้ทำการประเมินผลการบริหารจัดการส่วนที่เกี่ยวข้องกับระบบงานด้านเงินฝาก อันเป็นธุรกิจหลัก (Core Business) ของธนาคารพาณิชย์ เพื่อประเมินให้เห็นถึงศักยภาพการบริหารจัดการความมั่นคงปลอดภัยระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคาร ดังนี้

6.1.1 การจัดทำ Checklist เพื่อสอบทานผลการดำเนินการ (ก่อนทำโครงการ)

ในขั้นตอนการตรวจสอบการบริหารจัดการตามมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) นั้นผู้ศึกษาโครงการต้องจัดทำ Checklist เพื่อให้หน่วยงานผู้รับการตรวจสอบทำการประเมินผลกระบวนการปฏิบัติงานและการควบคุมภายในโดยการประเมินตนเอง (Control Self Assessment: CSA) ให้ทราบถึงการดำเนินการที่ผู้ปฏิบัติของธนาคารมีการจัดการให้สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศ และเป็นไปตามมาตรฐานอย่างเหมาะสม (ภาคผนวก ข) ซึ่งมีรายละเอียดดังนี้

ตารางที่ 6.1.1 แบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายในโดยการประเมินตนเอง (ก่อนทำโครงการ)

แบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายใน โดยการประเมินตนเอง (Control Self Assessment: CSA) **มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ โดยสายงาน IT**
<u>เกณฑ์การประเมิน Control Self Assessment</u> **กรุณาทำเครื่องหมาย ✓ ในช่อง ☐ เพื่อทำการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ที่ปัจจุบันธนาคารมีการกำหนด พร้อมทั้งอธิบาย อ้างอิงเอกสารที่มีการดำเนินการ ดังนี้** ☐ **Preventive Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในแบบป้องกัน หรือลดความเสี่ยงจากความผิดพลาด ความเสียหายจากเหตุการณ์ที่เกิดขึ้น หรือการรักษาความปลอดภัย เช่น กำหนดนโยบาย ระเบียบ หลักเกณฑ์ให้ชัดเจนเป็นลายลักษณ์อักษร การแบ่งแยกหน้าที่การงาน การควบคุมการเข้าถึงทรัพย์สินธนาคารไว้อย่างเหมาะสม ☐ **Detective Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในแบบตรวจหาหรือทำการตรวจสอบ ตรวจเช็คค้นหาข้อผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การติดตาม (Monitor) ด้วยคนหรือเครื่องมือ (Tools) ใด ๆ ในการ การสอบทานงาน ยืนยันสิทธ์การเข้าถึงอย่างสม่ำเสมอ ตลอดจดการใช้เครื่องมือเทคโนโลยีสารสนเทศทำการตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ผิดปกติ หรือไม่เหมาะสม ☐ **Corrective Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในเพื่อแก้ไขข้อผิดพลาดหรือเหตุการณ์ที่เกิดขึ้นให้ถูกต้องจากการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารสำหรับการหาแนวทางการแก้ไขปัญหาไม่ให้เกิดข้อผิดพลาดซ้ำอีกภายในองค์กร
<u>ขอบเขตการตรวจสอบ</u> การจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) โดยระบบงานที่เป็นธุรกรรมอิเล็กทรอนิกส์ของกลุ่มตัวอย่าง (Sampling System) ได้แก่ ระบบงานเงินฝาก Flexcute (FCR) เนื่องมาจากเป็นธุรกรรมหลักด้านเงินฝากสำหรับสนับสนุนธุรกิจหลัก (Core Business Financial Bank) ที่มีฐานข้อมูลการทำธุรกรรมทางการเงินของซึ่งเป็นลูกค้า เพื่อควบคุมการเข้าถึงให้เป็นไปตามมาตรฐาน (ISO/IEC 27001)

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)			
1.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy) ธนาคารกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)	ธนาคารมีนโยบายฯ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ ครอบคลุมถึงการควบคุมการเข้าถึงระบบเครือข่ายภายในกลุ่มธุรกิจทางการเงิน ระบบปฏิบัติการ และ Application ของระบบสารสนเทศ โดยมีการกำหนดในเรื่องของการพิสูจน์ตัวตน และพิสูจน์สิทธิ ป้องกันการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต และเป็นลายลักษณ์อักษร
	☑ Detective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.1 การสร้างนโยบายความมั่นคงปลอดภัยทางสารสนเทศ(Information security policy)	ธนาคารมีการทบทวนนโยบายความมั่นคงปลอดภัยทางสารสนเทศ (Review of the information security policy) ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยหน่วยงานเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ
	☑ Corrective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.1 การสร้างนโยบายความมั่นคงปลอดภัยทางสารสนเทศ(Information security policy)	ธนาคารมีการทบทวนนโยบายความมั่นคงปลอดภัยทางสารสนเทศ (Review of the information security policy) ต้องมีการทบทวนเมื่อมีการเปลี่ยนแปลงที่สำคัญเพื่อให้สอดคล้องกับเทคโนโลยีที่พัฒนาหรือเปลี่ยนแปลงไป โดย IT เป็นผู้ดำเนินการ

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
1.2.1 การลงทะเบียนพนักงาน (User registration) ธนาคารกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร ***<u>ใช่หรือไม่อย่างไร</u>***	☑ Preventive Control	1) นโยบายเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้(Use access management) 2) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่าน ข้อ 5.1.2 (2.1) สำหรับการกำหนดสิทธิสำหรับบุคคล กรณีเป็นการให้สิทธิมาตรฐานตามตำแหน่งงาน	1) ธนาคารมีนโยบายฯ การลงทะเบียนพนักงาน (User registration) การกำหนดแนวทางปฏิบัติงานเรื่องการลงทะเบียนพนักงาน หรือการให้สิทธิในการเข้าถึงระบบสารสนเทศ 2) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย และได้รับสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม โดยกรณีเป็นการให้สิทธิมาตรฐานตามตำแหน่งงาน เป็นไปตามการปฏิบัติงานปัจจุบันของฝ่ายพัฒนาระบบบริหารทรัพยากรบุคคล (สายทรัพยากรบุคคล) ซึ่งผู้ดูแลระบบจะทำการลงทะเบียน ปรับปรุงสิทธิในระบบสารสนเทศตามที่ได้รับแจ้งรายชื่อพนักงานเข้าใหม่ โอนย้าย ปรับเปลี่ยนตำแหน่งงาน พ้นสภาพ และสิทธิดังกล่าวจะเริ่มมีผลตามที่กำหนดไว้ใน “วันที่มีผล (Effective Date)” กรณีที่สายเทคโนโลยี

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
			สารสนเทศได้รับแจ้งหลังจาก “วันที่มีผล (Effective Date)” ให้ผู้ดูแลระบบปรับปรุงสิทธิตามวันที่ได้รับแจ้งในระบบ HR แทน
	☑ Detective Control	Flow ในการควบคุมติดตามการปฏิบัติงาน กรณีพนักงานเข้าใหม่ โอนย้าย พ้นสภาพ	ธนาคารมีวิธีการกำหนดให้ผู้ใช้งานร้องขอผ่านระบบงานแบบฟอร์มร้องขอ (IT Request) โดยมีการอนุมัติการดำเนินการควบคุม ติดตาม (Monitor) จากผู้ที่ได้รับมอบหมายให้ลงทะเบียน User ให้กับผู้ร้องขอ และปิดงานจากผู้ร้องผ่านระบบงาน
	☑ Corrective Control	เอกสารหน้าจอระบบงาน IT Request การร้องขอสิทธิเข้าถึงระบบงานธนาคาร ภาคผนวก ค 1.2.1(1)	ธนาคารมีวิธีการกำหนดให้ผู้ใช้งานสามารถร้องขอ การลงทะเบียนของขอสิทธิผ่านทาง IT Request ในกรณีที่ไม่ได้รับสิทธิ หรือได้รับไม่ถูกต้องเพื่อทำการเพิ่มเติม แก้ไขการลงทะเบียนผู้ใช้งาน โดยต้องมีการอนุมัติผ่านระบบงาน IT Request หัวหน้างาน เจ้าของข้อมูลในระบบงานอย่างเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (Use access management 2) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่าน ข้อ 5.1.2 (2.1) สำหรับการกำหนดสิทธิสำหรับบุคคล กรณีขอใช้สิทธินอกเหนือมาตรฐาน (Exception) 3) เอกสาร Authorization matrix ขั้นตอนการร้องขอผู้ใช้สิทธิพิเศษ	1) ธนาคารมีนโยบายฯ การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) การจัดการสิทธิเฉพาะในการใช้งานระบบตามความจำเป็นในการใช้งานของผู้ใช้ในแต่ละบัญชีผู้ใช้ (UserID) 2) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย และได้รับสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม โดยกรณีขอใช้สิทธินอกเหนือมาตรฐาน (Exception) โดยทั่วไประบบสารสนเทศต่าง ๆ ไม่อนุญาตให้มีการกำหนดสิทธินอกเหนือมาตรฐานเว้นแต่มีความจำเป็น โดยจะต้องทำเรื่องขออนุมัติเป็นกรณีไป 3) ในระบบงานที่เป็น Core Business ธนาคารมีการกำหนด Role and Matrix เพื่อให้ทราบถึงอำนาจอนุมัติในระบบงานในแต่ละสิทธิที่ได้รับอย่างเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
	☐ Detective Control		
	☑ Corrective Control	เอกสารการขอเบิกใช้ Privilege User ของระบบงานเงินฝาก	ธนาคารมีการกำหนดเอกสารแบบฟอร์มเอกสารการขอเบิกใช้สิทธิเฉพาะ (Privilege User) เพื่อให้ผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศนำไปใช้ในการแก้ไขปัญหาระบบงานที่เกิดขึ้น กรณีที่สิทธิของพนักงานปฏิบัติงานไม่สามารถดำเนินการได้
1.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ธนาคารกำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานเพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (Use access management) 2) ระเบียบเรื่อง การกำหนดบัญชีผู้ใช้งาน และรหัสผ่านโดย สายเทคโนโลยีสารสนเทศ ข้อ 3 การจัดการรหัสผ่าน (User password management)	1) ธนาคารมีนโยบายฯการบริหารจัดการรหัสผ่าน (User password management) การจัดสรรรหัสผ่านสำหรับผู้ใช้งานและการดูแลรักษารหัสผ่านให้มีความมั่นคงปลอดภัย 2) ธนาคารมีการกำหนดระเบียบ ซึ่งเป็นรายละเอียดของการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร โดยมีการกำหนดกระบวนการจัดการรหัสผ่าน ดังนี้

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			2.1 การส่งมอบรหัสผ่านตั้งต้นให้กับผู้ใช้ ด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกัน 2.2 ต้องเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และกำหนดรหัสผ่านที่มีความยากต่อการเดา 2.3 ต้องเก็บรักษารหัสผ่านไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น 2.4 หากสงสัยว่าผู้อื่นล่วงรู้รหัสผ่านของตน ให้ทำการเปลี่ยนรหัสผ่านทันที 2.5 กรณีที่ต้องการออกรหัสผ่านใหม่หรือปลดล็อกรหัสผ่านต้องขออนุมัติจากผู้บังคับบัญชาต้นสังกัดและสายเทคโนโลยีสารสนเทศ 2.6 กำหนดให้มีการบริหารจัดการรหัสผ่าน ดังนี้ - ความยาวขั้นต่ำของรหัสผ่าน 7 ตัวอักษร (Minimum Password Length)

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			- บังคับการเปลี่ยนรหัสผ่านทุก 90 วัน (Force Password Duration Change) - จำกัดการตั้งค่ารหัสผ่านซ้ำเดิม 3 ครั้ง (Enforce Password History) - จำกัดจำนวนครั้งในการพยายามเข้าถึง (Log on Attempts) เมื่อมีการพยายามเข้าถึง หรือใส่รหัสผ่านผิด 4 ครั้ง โดยระบบต้องล็อกบัญชีไม่ให้ทำงานจนกว่าจะมีการแก้ไขจากผู้ดูแล
	☑ Detective Control	ตัวอย่างซองส่งรหัสผ่านคาร์บอน เพื่อการป้องกันการล่วงรู้รหัสผ่าน	ธนาคารมีวิธีการอย่างมั่นคงปลอดภัยในการกำหนดการส่งมอบรหัสผ่านให้ผู้ใช้งานผ่านซองรหัสผ่านโดยบรรจุปิดผนึกในซองเอกสารคาร์บอน และมีการลงทะเบียนผ่านการจัดส่ง ควบคุมการส่งมอบรหัสผ่านให้ถึงมือผู้ใช้งานอย่างเหมาะสม
	☑ Corrective Control	อ้างอิงเอกสารตาม IT Request	ธนาคารมีวิธีการกำหนดให้ผู้ใช้งานสามารถร้องขอ การขอปลดล็อกรหัสผ่าน โดยผ่านทาง IT Request ในกรณีที่ไม่ได้ สามารถใช้งานรหัสผ่านที่ธนาคารส่งมอบให้ โดยต้องมีการอนุมัติผ่าน

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			ระบบงาน IT Request ของหัวหน้างาน และเจ้าของข้อมูลในระบบงานอย่างเหมาะสม ซึ่งทางผู้ปฏิบัติงานจะดำเนินการ Generate รหัสผ่านและส่งมอบให้ตามกระบวนการในลำดับต่อไป
1.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)ธนาคารกำหนดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (Use access management 2) ระเบียบเรื่อง การกำหนดบัญชีผู้ใช้งาน และรหัสผ่านโดย สายเทคโนโลยีสารสนเทศ ข้อ 2 การกำหนดบัญชีผู้ใช้งาน และสิทธิผู้ใช้งาน มีข้อปฏิบัติ	1) ธนาคารมีนโยบายฯ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) มีกระบวนการทบทวนสิทธิการเข้าถึงของระบบสารสนเทศระบบงานที่สำคัญอย่างเป็นทางการ เพื่อป้องกันการให้สิทธิพนักงานเกินกว่าที่จำเป็น และการเปลี่ยนแปลงสิทธิโดยไม่ได้รับอนุญาต 2) ธนาคารจัดให้มีการทบทวนสิทธิ และบัญชีผู้ใช้งานอย่างน้อยปีละ1 ครั้ง เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ยังคงมีความเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
		3) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่าน ข้อ 5.4 การทบทวนสิทธิ	3) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย และได้รับสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม โดยทบทวนสิทธิการเข้าถึงของผู้ใช้งานในระบบสารสนเทศ (Review of user access rights) และทบทวนปรับปรุงให้เหมาะสมอยู่เสมอ
	☑ Detective Control	เอกกสารทบทวนบัญชีผู้ใช้งานประจำปี	ธนาคารมีการกำหนดให้มีการทบทวนบัญชีผู้ใช้งานประจำปี ในทุกระดับที่มีผู้ใช้งานสามารถเข้าถึงระบบงานของธนาคารได้ อาทิ ระดับ Server (OS) ระดับ Database และระดับ Application อย่างครบถ้วนทุกระบบงาน
	☑ Corrective Control	เอกสารการยืนยันการทบทวนสิทธิระบบงานธนาคาร	ธนาคารมีการกำหนดให้ผู้ดูแลระบบงานสังกัดสายเทคโนโลยีสารสนเทศ ทำการรวบรวม และส่งรายงานการสอบทานสิทธิที่ต้องมีการแก้ไขให้หน่วยงานผู้ปฏิบัติงานรับทราบ เช่น ผ่านทาง IT Request หรือ Mail ในการร้องขอแก้ไขสิทธิ ทบทวนอย่างเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			
1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารมีการกำหนดวิธีปฏิบัติที่มั่นคงปลอดภัยสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	ธนาคารมีนโยบายฯ การใช้งานรหัสผ่าน สำหรับผู้ใช้งาน (Password use) พนักงานที่มีสิทธิในระบบสารสนเทศใด ๆ ของกลุ่มธุรกิจทางการเงิน ต้องเก็บรักษารหัสผ่านเป็นความลับ และกำหนดรหัสผ่านให้ยากต่อการคาดเดา
	☐ Detective Control		
	☑ Corrective Control	อ้างอิงเอกสาร IT Request การขอปลดล็อกรหัสผ่าน ภาคผนวก ค 1.2.1(1)	ธนาคารมีวิธีการกำหนดให้ผู้ใช้งานสามารถร้องขอผ่านทาง IT Request ในกรณีไม่สามารถใช้งานรหัสผ่านที่ตนเองเปลี่ยน หรือเกิดปัญหาการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนด โดยต้องมีการอนุมัติผ่านระบบงาน IT Request ของหัวหน้างาน และเจ้าของข้อมูลในระบบงานอย่างเหมาะสม ซึ่งทางผู้ปฏิบัติงานจะดำเนินการ Generate รหัสผ่านและส่งมอบให้ตามกระบวนการในลำดับต่อไป

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
1.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment) ธนาคารมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	ธนาคารมีนโยบายฯ การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment) การป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานส่วนกลางที่ไม่มีพนักงานดูแล นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ซึ่งไม่ปลอดภัย (Clear desk and clear screen policy) ผู้ใช้งานมีหน้าที่ควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ อยู่ในสถานที่ซึ่งไม่ปลอดภัย เช่น การป้องกันไม่ให้เอกสาร หรือสื่อบันทึกข้อมูล อยู่ในพื้นที่ซึ่งสามารถเข้าถึงได้โดยบุคคลภายนอก
	☑ Detective Control	ผู้ศึกษาโครงการใช้เทคนิคในการเข้าถึง Server ศึกษาการตั้งค่า configuration ความมั่นคงปลอดภัย ภาคผนวก ค 1.3.2(1)	ธนาคารมีการกำหนดให้ระบบที่มีความสำคัญ มีการควบคุมให้ล็อกหน้าจอถ้าไม่ใช้งานเกินกว่าเวลาที่กำหนด ตลอดจนผู้ใช้ยังได้รับการสื่อสารกับวิธีการปฏิบัติเมื่อไม่อยู่ที่หน้าเครื่อง
	☑ Corrective Control	เอกสาร IT Request การร้องขอเข้า CAB	การแก้ไขป้องกันการเข้าถึงอุปกรณ์ ธนาคารมีการกำหนดให้ Admin สามารถทำการเปลี่ยนแปลงค่า Configuration ใดที่ได้ ที่เป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล แต่การกระทำใด ๆ ในการเปลี่ยนแปลงต้องมี

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			การขออนุมัติอย่างเหมาะสม โดยผ่านกระบวนการ Change Management ซึ่งต้องผ่านการอนุมัติจากคณะทำงาน CAB / ECAB ให้มีความเหมาะสม (จากที่ผ่านมาธนาคารมีการทบทวน พบว่า ระยะเวลา 30 นาทีเป็นเวลาที่เหมาะสม
1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)			
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารมีการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ การควบคุมการใช้งานบริการเครือข่าย (Policy on use of network services) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ รวมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ หรือบริการใดไม่สามารถใช้งานได้
	☐ Detective Control		
	☑ Corrective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) เกี่ยวกับนโยบายการรักษาความมปลอดภัยทางสารสนเทศ	ธนาคารมีการกำหนดให้มีการทบทวนปรับปรุงนโยบายด้านเทคโนโลยีสารสนเทศ ครอบคลุมถึง การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ เนื่องจากระบบเครือข่ายสื่อสารมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจในปัจจุบัน หากไม่มีการบริหารจัดการที่ดี จะส่งผลกระทบต่อการ

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			ดำเนินธุรกิจ จึงมีการแบ่งหน้าที่ความรับผิดชอบ การเฝ้าระวังทั้งที่เป็นการทำงานของอุปกรณ์ การเฝ้าระวังการบุกรุก และการกำหนดขั้นตอนการปฏิบัติงานสร้างกระบวนการให้บริการของผู้ให้บริการภายนอก ซึ่งต้องสอดคล้องนโยบายฉบับใหม่
1.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ธนาคารกำหนดให้มีการพิสูจน์ตัวตนก่อนอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้ ***<u>ใช่หรือไม่อย่างไร</u>***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้
	☑ Detective Control	1) เอกสารหน้าจอการแสดงผลVPN with Citrix ของธนาคาร	1) ธนาคารมีการกำหนดให้ผู้ใช้งานที่อยู่ภายนอกองค์กร เข้าถึงระบบงานของธนาคารได้ผ่านช่องทาง VPN with Citrix ซึ่งเป็นการใช้งานที่ปลอดภัยช่องทางเดียวที่ธนาคารกำหนด โดยใช้รหัสผ่านของ Windows ที่ธนาคารกำหนดและส่งมอบให้เท่านั้น

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
		2) เอกสาร IBM Quarterly Employment Verification (QEV) ,Continue Business Need (CBN) and Privilege Access Revalidation for Q1-2013	2) ธนาคารมีการกำหนดการควบคุม ติดตามผู้ใช้งานที่อยู่ภายนอกธนาคารในการเข้าถึงระบบงานของธนาคาร โดยการทบทวนผู้ใช้งานที่เข้าถึงด้วยวิธี VPN With Citrix จากภายนอกและผู้ใช้งาน (Outsource IBM) ที่สามารถเข้าถึงในการสนับสนุน Core Bank ของธนาคารตามสัญญาจ้างบริการ โดยการทบทวนสิทธิเป็นประจำไตรมาส และนำสรุปผลเป็นลายลักษณ์อักษร
		3) เอกสารการทบทวน Log Active Directory ของระบบงาน Citrix	3) ธนาคารมีการกำหนดให้ทำการทบทวน Log การเข้าถึงระบบงานของ Citrix ซึ่งมีการใช้งาน Server ของ Active Directory ซึ่งเป็น Server เดียวกันกับการใช้ User Password เดียวกับระบบงาน Citrix จึงต้องทำการทบทวน Log การเข้าถึงระบบงานอย่างเหมาะสม
	☑ Corrective Control	อ้างอิงเอกสารหน้าจอการแสดงผลVPN with Citrix ของธนาคาร	มีการกำหนดให้ผู้ใช้งานที่อยู่ภายนอกองค์กร ในกรณีพิสูจน์ตัวตนผู้ใช้งาน Authenticate ผ่าน VPN With Citrix ไม่ได้หรือเกิดปัญหา ให้ติดต่อผ่านช่องทางการโทรศัพท์เข้ามายังศูนย์บริการพนักงานเพื่อแก้ไขปัญหาการเข้าถึงอย่างเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
1.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) ธนาคารมีการกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุ พิสูจน์ตัวตนเพื่อบ่งบอกการเชื่อมต่อนั้นมาจากอุปกรณ์ สถานที่ได้รับอนุญาตแล้ว***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ กำหนดให้มีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) การบ่งบอกการเชื่อมต่อของอุปกรณ์บนเครือข่าย เพื่อให้ทราบว่าการเชื่อมต่อมาจากอุปกรณ์ หรือสถานที่ซึ่งได้รับอนุญาตแล้วจริง (Automatic Equipment identification)
	☑ Detective Control	ผู้ศึกษาโครงการใช้เทคนิคในการเข้าถึงระบบเครือข่ายที่มีการตั้งความมั่นคงปลอดภัยไว้ ภาคผนวก ค 1.4.3(1)	ธนาคารมีการกำหนดให้ผู้ใช้งานเครื่องคอมพิวเตอร์อุปกรณ์ใด ๆ ในทุกเครื่องต้องมีการกำหนด Mac Address, IP Address แยกสำหรับแต่ละอุปกรณ์เพื่อการเข้าถึง จึงต้องพิสูจน์ตัวตนอุปกรณ์บนระบบเครือข่ายอย่างเหมาะสม
	☑ Corrective Control	เอกสารหน้าจอ Firewall กำหนด Admin เข้าถึงอุปกรณ์ได้เท่านั้นตาม IP Address	ธนาคารมีการกำหนดผู้ปฏิบัติงาน ซึ่งเป็นผู้ดูแลระบบเครือข่าย (Administrator) เข้าถึงอุปกรณ์บนระบบเครือข่ายได้ โดยการกำหนดการ Manage Permitted IP Address เฉพาะผู้ดูแลระบบเท่านั้นที่อุปกรณ์ Firewall
1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่ง	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การ	ธนาคารมีนโยบายฯ กำหนดให้มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
ระบบ (Remote diagnostic and configuration port protection) ธนาคารมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ***ใช่หรือไม่อย่างไร***		ควบคุมการเข้าถึงเครือข่าย (Network access control)	configuration port protection) มาตรการการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
	☐ Detective Control	ผู้ศึกษาโครงการทดสอบเข้าถึงระบบเครือข่ายผ่านพอร์ตการเชื่อมต่อที่มีเปิดอย่างไม่เหมาะสม ภาคผนวก ค 1.4.4(1)	
	☑ Corrective Control	เอกสาร Request For Change (RFC) Network	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสม ก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงที่อุปกรณ์เครือข่ายเพื่อป้องกันความมั่นคงปลอดภัย
1.4.5 การแบ่งแยกเครือข่าย (Segregation in networks) ธนาคารมีการจัดทำการแบ่งแยก	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network	1) ธนาคารมีนโยบายฯ กำหนดให้ทำการแบ่งแยกเครือข่าย (Segregation in networks) การแบ่งแยกเครือข่ายตามกลุ่มของข้อมูลสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ตามการดำเนินงานทาง

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
เครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ ***ใช่หรือไม่อย่างไร***		access control) 2) คู่มือการปฏิบัติงานประจำหน่วยงาน Vendor Network Access Control ฝ่ายโครงสร้างพื้นฐานสารสนเทศ	ธุรกิจ และกลุ่มของระบบสารสนเทศ เช่น การแบ่งแยกเครือข่ายภายใน กับเครือข่ายภายนอก การแบ่งเครือข่ายตามกลุ่มระดับความสำคัญของข้อมูล หรือเครือข่ายไร้สาย เพื่อกำหนดระดับการรักษาความปลอดภัยให้เหมาะสมกับความเสี่ยงที่เกิดในแต่ละกลุ่ม 2) ธนาคารมีการกำหนดคู่มือปฏิบัติงานประจำหน่วยงาน ซึ่งเป็นขั้นตอนการปฏิบัติงานของผู้ดูแลระบบงานส่วนระบบเครือข่ายของธนาคาร ทำการกำหนดให้ Vendorใหม่ ผู้ตรวจสอบภายนอกหรือเจ้าหน้าที่ของธนาคารแห่งประเทศไทย ใช้เพื่อบอกถึงขั้นตอนในการขอใช้งาน Network โดยสามารถให้ Vendor จะสามารถใช้งานระบบสารสนเทศเท่าที่จำเป็นเท่านั้น หรือการเพิ่มสิทธิในการเข้าถึง Serverให้มีความเหมาะสม
	☑ Detective Control	เอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการกำหนดการกั้นเพื่อแบ่งแยกเครือข่ายที่อุปกรณ์ Firewall เพื่อจำกัดและควบคุมการเข้าถึงระหว่างกลุ่มผู้ใช้งานภายในและผู้ใช้งานภายนอก โดยมีกระบวนการร้องขอและติดตามการให้สิทธิอย่างเหมาะสม

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	☑ Corrective Control	เอกสาร Request For Change (RFC) Network เพื่อการกำหนดการเข้าถึงของ Vendor/Outsource	ธนาคารมีการกำหนดการแก้ไข ความมั่นคงปลอดภัยของการแบ่งแยกระบบเครือข่าย โดยกำหนด Firewall Rule และกระบวนการร้องขอเปลี่ยนแปลงค่า Configuration ในเอกสาร Request For Change (RFC)
1.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ธนาคารมีการจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบายเทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ กำหนดให้ควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นตาม การควบคุมการเข้าถึง
	☑ Detective Control	เอกสารการกำหนด Wireless Network Property Setting ในการเข้าถึงต้องใช้ Windows to configure wireless Network ของธนาคาร	ธนาคารยังไม่ได้ Block การใช้อุปกรณ์เชื่อมต่อเช่น แอร์การ์ด หรือ hotspot ที่เครื่องอุปกรณ์ แต่ใช้วิธีการกำหนดอุปกรณ์เครือข่ายใด ๆ ของธนาคารให้เข้าถึงโดยผ่านการ Authentication User Password ของ Windows ที่ธนาคารกำหนดให้เท่านั้นในการใช้ Single sign on ตลอดจนมีการจัดเก็บ Log ตามพรบ.ว่าด้วยการกระทำความผิดการจราจรทางคอมพิวเตอร์

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	☑ Corrective Control	เอกสารการร้องขอสิทธิ VPN with Citrix ผ่านระบบ IT Request	ธนาคารมีการจำกัดการเชื่อมต่อหรือเข้าถึง โดยกำหนดให้ผู้ใช้งานต้องการเข้าถึงระบบเครือข่ายอื่น ต้องมีการร้องขอผ่าน IT Request เพื่อให้ผู้ดูและระบบงานทำการกำหนดสิทธิ และ IP Address ที่อุปกรณ์เครือข่าย (manage permitted IP Address)
1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารมีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☑ Detective Control	อ้างอิงเอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการกำหนด Mac Address, IP Address แยกสำหรับแต่ละอุปกรณ์ ตลอดจนเส้นทางที่จำเป็นต้องมีการเชื่อมต่อบนเครือข่ายเพื่อให้ข้อมูลสารสนเทศสามารถติดต่อสื่อสารกับหน่วยงานกำกับ เช่น Site VOIP conference กับธนาคารแห่งประเทศไทย
	☑ Corrective Control	อ้างอิงเอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการกำหนดเส้นทางการติดตั้งระบบเครือข่ายสำหรับกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถรองรับการดำเนินการของธุรกรรมอิเล็กทรอนิกส์ (Core Bank) ได้อย่างต่อเนื่อง โดยอุปกรณ์ Switch สามารถ Manage เส้นทางการไหลข้อมูลเปลี่ยนอัตโนมัติ เป็น สาขา > ISP > ศูนย์ DC สำรอง ตลอดจนผู้ดูแล

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			ระบบเครือข่ายจะดำเนินการปรับ configuration firewall ของศูนย์ DC สำรองให้ธนาคารสามารถรับส่งข้อมูลได้อย่างต่อเนื่อง เพื่อให้สามารถรองรับการดำเนินการของธุรกรรมอิเล็กทรอนิกส์ (Core Bank) ได้อย่างต่อเนื่อง
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
1.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures) ธนาคารมีการจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) 2) ระเบียบเรื่อง การกำหนดบัญชีผู้ใช้งาน และรหัสผ่านโดย สายเทคโนโลยีสารสนเทศ	1) ธนาคารมีนโยบายฯ ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures) สำหรับการเข้าถึงหรือการใช้งานระบบปฏิบัติการ 2) ธนาคารมีการกำหนดระเบียบ ซึ่งเป็นรายละเอียดของการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคารสอดคล้องกับจัดการรหัสผ่าน (User password management) ของผู้ใช้งานในทุกระดับชั้น เช่น Application หรือ Server (อ้างอิงตามเนื้อหาข้อ 2.3)

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	☑ Detective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.1 การสร้างนโยบายความมั่นคงปลอดภัยทางสารสนเทศ(Information security policy)	ธนาคารมีการกำหนดให้มีการทบทวนนโยบายด้านเทคโนโลยีสารสนเทศ และเอกสารที่เกี่ยวข้องอื่น ๆ อาทิ ระเบียบ บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ
	☑ Corrective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.1 การสร้างนโยบายความมั่นคงปลอดภัยทางสารสนเทศ(Information security policy)	ธนาคารมีการทบทวนนโยบายความมั่นคงปลอดภัยทางสารสนเทศ (Review of the information security policy) ต้องมีการทบทวนเมื่อมีการเปลี่ยนแปลงที่สำคัญเพื่อให้สอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป โดยหน่วยงานเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ
1.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication) ธนาคารมีการจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และ	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	ธนาคารมีนโยบายฯ การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and authentication) เพื่อการระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ
	☑ Detective Control	เอกสารหน้าจอการกำหนดผู้ใช้งานเข้าถึงระบบงาน ระดับ OS	ที่ระดับระบบปฏิบัติการ (Operating system access control) ธนาคารมีการกำหนดการตั้งค่าให้ที่ระบบงานให้ผู้ใช้งานต้องพิสูจน์ตัวตนด้วย Username และ Password ก่อนการเข้าใช้

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
ต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ ***ใช่หรือไม่อย่างไร***			ระบบงานทุกครั้ง ตามนโยบาย และระเบียบของธนาคารที่กำหนดให้เกิดความมั่นคงปลอดภัย
	☑ Corrective Control	เอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสม ก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันความมั่นคงปลอดภัย
1.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system) ธนาคารมีการจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุม หรือกำหนดรหัสผ่านที่มีคุณภาพ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	ธนาคารมีนโยบายฯ ระบบบริหารจัดการรหัสผ่าน (Password management system) ระบบสารสนเทศที่มีระบบการพิสูจน์ตัวตน ในรูปแบบบัญชีผู้ใช้ และรหัสผ่าน ต้องมีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมต่าง ๆ
	☑ Detective Control	เอกสารหน้าจอการกำหนดสิทธิให้ผู้ใช้งานสามารถเข้าถึงระบบงานได้ในระดับ Server	ที่ระดับระบบปฏิบัติการ ธนาคารมีการกำหนดให้ผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงระบบงานในระดับ Server ได้ ตลอดจนการเข้าใช้งานต้องเป็นไปตามการตั้งค่าเพื่อให้ผู้ใช้งานต้องพิสูจน์ตัวตนด้วย Password ตามที่กำหนดไว้ว่าจำนวนรหัสผ่านไม่ต่ำ

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			กว่า 7 ตัวอักษรก่อนการเข้าใช้ระบบงานทุกครั้ง ตามนโยบายฯ และระเบียบของธนาคารที่กำหนดให้เกิดความมั่นคงปลอดภัย
	☑ Corrective Control	อ้างอิงเอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS ภาคผนวก ค 1.5.2(2)	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสม ก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันความมั่นคงปลอดภัย
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารมีการจำกัดควบคุมการใช้โปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	ธนาคารมีนโยบายฯ การใช้งานโปรแกรมประเภท Utility (Use of system utilities) การจำกัดและควบคุมการใช้งานโปรแกรมประเภท Utility เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้
	☐ Detective Control		
	☑ Corrective Control	เอกสารการร้องขอสิทธิ ผ่านระบบ IT Request	ธนาคารมีการจำกัดการติดตั้งโปรแกรมประเภทยูทิลิตี้ โดยกำหนดให้ผู้ใช้งานต้องการใช้งาน ต้องมีการร้องขอผ่าน IT

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			Request เพื่อให้ผู้ดูและระบบงานทำการติดตั้งระบบงานให้อย่างเหมาะสมเพื่อป้องกันความปลอดภัยในการติดตั้ง Software ใด ๆ
1.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out) ธนาคารมีการกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)	ธนาคารมีนโยบายฯ การหมดเวลาการใช้งานระบบสารสนเทศ (Session time out) การจำกัดเวลาในการใช้งานระบบสารสนเทศเมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น ระบบตัดการใช้งานอัตโนมัติ โดยควรใช้กับระบบสารสนเทศที่มีข้อมูลตั้งแต่ระดับข้อมูลลับขึ้นไป
	☑ Detective Control	อ้างอิงตามเอกสารแนบของผู้ศึกษา โครงการใช้เทคนิคในการเข้าถึง Server ดูค่า configuration การตั้งความมั่นคงปลอดภัย	ธนาคารมีการกำหนดให้ระบบที่มีความสำคัญ (Core Bank) มีการควบคุมให้ระบบงานมีการหมดเวลาการใช้งานระบบงาน (Session Time out) โดยกำหนดเป็นระยะเวลา หรือถ้ามีการใส่รหัสผ่านผิดระบบงานจะล็อก ดังนี้ - Account Lockout Duration คือ เวลาที่จะล็อก Account ที่ใส่ password ผิดครบจำนวนที่กำหนดไว้ (ธนาคารมีการกำหนด = 0 ต้องให้ผู้ดูแลระบบงานที่มีสิทธิมาปลดล็อคเท่านั้น) - Account Lockout Threshold คือ จำนวนครั้งที่คีย์ผิด ธนาคารมีการกำหนด = 4 ครั้ง)

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			- Reset account Lockout counter after คือ ระยะเวลาที่คีย์ผิดตั้งแต่ผิดครั้งแรก แล้วนับไปอีกกี่นาทีถึง reset จำนวนที่นับ ถ้าคีย์ผิดครบตามจำนวนครั้งที่กำหนดแล้วอยู่ในเวลาก็จะล็อก แต่ถ้าคีย์ผิดแต่ยังไม่ครบ แล้วเวลานับถึงที่ตั้งแล้ว ก็จะเริ่มนับที่ 0 ใหม่ (ธนาคารกำหนดไว้ = 30 นาที)
	☑ Corrective Control	อ้างอิงเอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสม ก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันความมั่นคงปลอดภัย
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารมีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่	☐ Preventive Control		

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
มีความสำคัญสูง ***ใช่หรือไม่อย่างไร***	☑ Detective Control	อ้างอิงตามเอกสารแนบของผู้ศึกษา โครงการใช้เทคนิคเข้าถึง Server ดูค่า configuration ความมั่นคงปลอดภัย	ธนาคารมีการกำหนดให้ระบบที่มีความสำคัญ (Core Bank) มีการควบคุมให้ระบบงานมีจำกัดระยะเวลาเชื่อมต่อ โดยกำหนดเป็นระยะเวลา หรือถ้ามีการใส่รหัสผ่านผิดระบบงานจะล็อก ดังนี้ - Reset account Lockout counter after คือ ระยะเวลาที่คีย์ผิดตั้งแต่ผิดครั้งแรก แล้วนับไปอีกกี่นาทีถึง reset จำนวนที่นับ ถ้าคีย์ผิดครบตามจำนวนครั้งที่กำหนดแล้วอยู่ในเวลาก็จะโดนล็อก แต่ถ้าคีย์ผิดแต่ยังไม่ครบ แล้วเวลานับถึงที่ตั้งแล้ว ก็จะเริ่มนับที่ 0 ใหม่ (ธนาคารกำหนดไว้ = 30 นาที) จากการดำเนินการกำหนดค่า ดังกล่าว จะทำให้การใช้งานโปรแกรมจำพวกสุ่มรหัสผ่าน เช่น Flickr หรือ Brute force ในการเข้าถึงระบบงานธนาคารระดับ OS ได้ยาก เมื่อเปิด Log ของเครื่อง OS จะพบว่าแหล่งต้นทางมาจากที่ใด และสามารถทำการ log account ต้นทางดังกล่าวไม่ให้มีการใช้งานเพื่อความปลอดภัย
	☑ Corrective Control	อ้างอิงเอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างาน

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			อย่างเหมาะสม ก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันความมั่นคงปลอดภัย
1.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)			
1.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ธนาคารมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)	ธนาคารมีนโยบายฯ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) การจำกัดการเข้าถึงข้อมูลสารสนเทศ ของระบบงานต่าง ๆ โดยการเข้าถึงจะต้องแยกตามความจำเป็นตามหน้าที่ของผู้ใช้งาน
	☑ Detective Control	ผู้ศึกษาโครงการใช้เทคนิคในการเข้าถึงข้อมูล User Matrix ในระบบงานเงินฝากระดับ Application และ Export ข้อมูลออกมา	ระบบงาน (Core Bank) ของธนาคารมีการกำหนดสิทธิในระดับ Application ซึ่งให้ผู้ใช้งานเข้าถึงระบบงานในฟังก์ชันที่แตกต่างกันตามหน้าที่ความรับผิดชอบ ซึ่งเป็นการจำกัด ควบคุมการเข้าถึงเพื่อความมั่นคงปลอดภัย ตามนโยบายเทคโนโลยีสารสนเทศธนาคาร
	☑ Corrective Control	เอกสารการร้องขอสิทธิ ผ่านระบบ IT Request	ธนาคารมีการจำกัดการติดตั้งโปรแกรมประเภทยูทิลิตี้ โดยกำหนดให้ผู้ใช้งานต้องการใช้งาน ต้องมีการร้องขอผ่าน IT

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			Request เพื่อให้ผู้ดูและระบบงานทำการติดตั้งระบบงานให้อย่างเหมาะสมเพื่อป้องกันความปลอดภัยในการติดตั้ง Software ใด ๆ
1.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) ธนาคารมีการแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.6. การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)	ธนาคารมีนโยบายฯ - การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) การแยกระบบสารสนเทศที่มีระดับความสำคัญเพื่อกำหนดระดับการควบคุมและการรักษาความมั่นคงปลอดภัยตามระดับความสำคัญของข้อมูล
	☑ Detective Control	เอกสาร SLA and Problem ระบุ Priority และอ้างอิงเอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการแบ่งแยกระบบงานสารสนเทศตามความสำคัญของข้อมูลระบบงาน โดยการกำหนดเป็น Priority ของระบบงาน ซึ่งระบบงาน Core Bank เป็นระบบงานธุรกรรมหลักของธนาคารจึงมีการกำหนดลำดับความสำคัญ (Service Level Agreement) เพื่อการรองรับสนับสนุนระบบงานระดับ Application ได้ 7X24 ชั่วโมง ตลอดจนมีการแบ่งแยกระบบเครือข่ายออกมาโดยเฉพาะตาม Network Diagram
	☑ Corrective Control	อ้างอิงเอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลง หรือแบ่งแยกระบบสารสนเทศใด ๆ ที่สำคัญเพื่อการจัดการความมั่นคง

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			ปลอดภัย ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลง โดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสมก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบงานสารสนเทศระดับ Application ให้สามารถดำเนินการได้อย่างต่อเนื่อง
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing & communications) ธนาคารมีการต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา เช่น notebook, palm, และ laptop เป็นต้น และต้องกำหนดมาตรการป้องกันโดยพิจารณาความเสี่ยงที่มีต่ออุปกรณ์ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน (2012) ข้อ 2.7.7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile computing and teleworking)	1) ธนาคารมีนโยบายฯ การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communication) อุปกรณ์สื่อสารประเภทพกพา คือ อุปกรณ์สื่อสารที่สามารถประมวลผล บันทึกข้อมูล และเชื่อมต่อเครือข่ายได้ เช่น Notebooks, Tablet, Smart-Phones และอุปกรณ์อื่น ๆ ที่สามารถทำงานลักษณะคล้ายคลึงอุปกรณ์เหล่านี้ ให้พิจารณาเพิ่มขั้นตอนปฏิบัติงานที่มีความมั่นคงปลอดภัยมากกว่าอุปกรณ์สารสนเทศทั่วไป โดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์ที่ใช้เชื่อมต่อ

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
		2) ระเบียบการใช้งานทรัพย์สินสารสนเทศธนาคาร ข้อ 3.2 การใช้งานอุปกรณ์สื่อสารเคลื่อนที่	2) ธนาคารมีการกำหนดระเบียบในการใช้งานทรัพย์สินสารสนเทศเพื่อให้ผู้ใช้งานและผู้ปฏิบัติงานตระหนักในหน้าที่ความรับผิดชอบของตนเอง เช่น ผู้ใช้งานต้องขอลงทะเบียนอุปกรณ์สื่อสารเคลื่อนที่กับผู้ดูแลระบบงานผ่าน IT Request และขออนุมัติเป็นลายลักษณ์อักษร ตามความจำเป็นของการใช้งาน และส่งคืนอุปกรณ์หรือแจ้งการถอดถอนสิทธิเมื่อสิ้นสุดความจำเป็นในการใช้งาน
		3) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การใช้งานอุปกรณ์สื่อสารเคลื่อนที่ และเครือข่ายคอมพิวเตอร์ (Mobile Device and Network) ข้อ 5 เนื้อหา ขั้นตอนการปฏิบัติงาน ตั้งแต่การขอใช้งาน ลงทะเบียน และอนุมัติ	3) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย ผ่านการใช้งานด้วยอุปกรณ์เคลื่อนที่พกพา และสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม ดังนี้ - การขอใช้งาน ลงทะเบียน และอนุมัติกลุ่มผู้ใช้งานที่ได้รับสิทธิโดยมาตรฐาน กรณีพนักงานมีความประสงค์จะใช้งาน ให้ส่ง “IT Request” ต่อสายเทคโนโลยีสารสนเทศ และต้องผ่านการอนุมัติจากหัวหน้าผู้ขอใช้งาน ซึ่งจะพิจารณาคำขอเป็นราย ตามหน้าที่ความจำเป็น และพิจารณารับทราบความเสี่ยงต่อธนาคาร

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
			- การปฏิบัติเมื่อเปลี่ยนอุปกรณ์สื่อสารเคลื่อนที่ หรือสูญหาย ให้ผู้ใช้งานแจ้งสาย IT ผ่านทาง "IT Request" ทุกครั้ง เพื่อลบโปรแกรมและข้อมูลสารสนเทศจากอุปกรณ์ ติดตั้งโปรแกรมใหม่ ปรับปรุงทะเบียนอุปกรณ์ให้ถูกต้องและเป็นปัจจุบัน -การปฏิบัติเมื่อโอนย้าย ลาออกสายเทคโนโลยีสารสนเทศจะได้รับแจ้งจากสายบริหารทรัพยากรบุคคล เพื่อปฏิบัติงานถอดถอนสิทธิของผู้ใช้งานที่มีการใช้อุปกรณ์ฯ เพื่อเชื่อมต่อหรือใช้งานระบบของธนาคาร ทั้งนี้สายเทคโนโลยีสารสนเทศจะนำข้อมูลที่ได้รับมาตรวจสอบกับทะเบียนอุปกรณ์ฯ
	☐ Detective Control		
	☑ Corrective Control	เอกสารหน้าจอ Firewall Setup อุปกรณ์มือถือของผู้บริหาร Nokia ผ่าน Firewall	ธนาคารมีการกำหนด Firewall ในการตรวจสอบอุปกรณ์เคลื่อนที่พกพา (Mobile) ที่ได้รับอนุญาตเท่านั้นถึงสามารถเข้าถึงระบบงานธนาคารได้ ตลอดจนหากต้องมีการเปลี่ยนแปลงใด ๆ กับค่าอุปกรณ์ต้องมีการกำหนดการเปลี่ยนแปลง เช่น IMEI ของมือถือผ่านทางการร้องขอ IT Request

ตารางที่ 6.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012)ข้อ 2.7.7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile computing and teleworking)	ธนาคารมีนโยบายฯ การปฏิบัติงานภายนอกสำนักงาน (Teleworking) คือ การปฏิบัติงานโดยเชื่อมต่อระบบเครือข่ายจากสถานที่ภายนอกกลุ่มธุรกิจทางการเงิน เข้าสู่ระบบเครือข่ายภายในกลุ่มธุรกิจทางการเงินโดยทั่วไปแล้วจะทำผ่านอินเทอร์เน็ต โดยมีการใช้งานการเชื่อมต่อที่มีความมั่นคงปลอดภัย เช่น เครือข่ายเสมือนส่วนตัว (Virtual Private Network ,VPN)
	☐ Detective Control		
	☑ Corrective Control	อ้างอิงเอกสารหน้าจอระบบงาน IT Request การร้องขอสิทธิเพื่อการขอปฏิบัติงานจากภานอกสำนักงาน	ธนาคารมีการกำหนดการขอร้องขอการขอปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยการขอผ่านระบบงาน IT Request เพื่อให้หัวหน้างานทำการอนุมัติ ก่อนการใช้งาน Lotus note บน Mobile เพื่อควบคุมสิทธิร้องขอเปลี่ยนแปลงแก้ไขที่ไม่เหมาะสม

ความเห็นเพิ่มเติม .....

.....

ขอรับรองว่าข้อมูลที่ได้ให้ไว้ในแบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายใน โดยการประเมินตนเอง (Control Self Assessment: CSA) ถูกต้องตรงกับการปฏิบัติงานจริงทุกประการ

6.1.2 การประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

จาก Checklist การประเมินผลกระบวนการปฏิบัติงานและการควบคุมภายในโดยการประเมินตนเอง (Control Self Assessment : CSA) ของผู้รับการตรวจสอบที่ประเมินการทำงานของตนเองในการจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ในขอบเขตด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) แล้ว ผู้ศึกษาโครงการต้องนำข้อมูลที่ได้รับจาก Checklist ตลอดจนอาจมีการใช้เทคนิคการสอบถาม สัมภาษณ์การปฏิบัติงานเพิ่มเติม เพื่อนำข้อมูลที่ได้รับมานั้นบันทึกในแบบจำลองการประเมินการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศที่ได้จัดสร้างไว้แล้วนั้น เพื่อประเมินความเพียงพอของการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบัน ว่าองค์กร (ธนาคารพาณิชย์) มีการบริหารจัดการเรื่องมาตรฐานความมั่นคงปลอดภัยด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศมากน้อยเพียงใด และอยู่ในระดับที่องค์กรสามารถยอมรับได้หรือไม่อย่างไร โดยทำการ Plot คำชี้แจงและหลักฐานการจัดการตามคำชี้แจงจากประเมินตนเอง (Control Self Assessment : CSA)

โดยในการชี้วัดจากแบบสอบถามเชิงคุณภาพที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สายเทคโนโลยีสารสนเทศของธนาคารมีการดำเนินการในการป้องการควบคุมติดตาม และแก้ไขอย่างเหมาะสมนั้น ให้แปลงเป็นข้อมูลเชิงปริมาณในการแสดงผลผลลัพธ์ของแนวทางการจัดการที่มีอยู่กับระดับการยอมรับได้ขององค์กรในรูปแบบของตัวเลขนั้น ในส่วนนี้ผู้ศึกษาโครงการต้องใช้เทคนิคในการใช้ดุลพินิจประกอบเพื่อพิจารณา อาทิ

1) ผู้ศึกษาโครงการจำเป็นต้องพิจารณาจากหลักฐาน (Evidence) ที่ผู้ตอบแบบสอบถามการประเมินตนเองมีการอ้างอิง และแนบเอกสาร

2) ผู้ศึกษาโครงการพิจารณาคำชี้แจง ซึ่งเป็นลักษณะของการสอบทาน ความถูกต้องของการบริหารจัดการว่ามีแนวทางการปฏิบัติเป็นไปตามมาตรฐานความมั่นคงปลอดภัยอย่างเพียงพอเหมาะสมหรือไม่

3) ผู้ศึกษาโครงการจำเป็นต้องใช้เทคนิคด้านเทคโนโลยีสารสนเทศในการเข้าถึงระบบงานสารสนเทศขององค์กรเพื่อพิสูจน์กระบวนการ หรือวิธีการตั้งค่าการดำเนินการด้วยตนเองเพื่อสังเกตการณ์หรือรวบรวมหลักฐาน

ซึ่งจากรายละเอียดดังที่กล่าวมาแล้วนั้น ผู้ศึกษาโครงการสามารถจำมาใช้ในการเป็นข้อมูลนำเข้า (Input) เพื่อประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้ดังต่อไปนี้

ตารางที่ 6.1.2.1 แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)		**เพื่อควบคุมการเข้าถึงสารสนเทศ**				**100.00**
1.1.1	นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ	Yes	Yes	Yes	
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)		**เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต**				**91.67**
1.2.1	การลงทะเบียนพนักงาน (User registration)	ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น	Yes	Yes	Yes	

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.2.2	การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน	Yes	No	Yes	
1.2.3	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย	Yes	Yes	Yes	
1.2.4	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้	Yes	Yes	Yes	
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		**เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ**				**83.33**
1.3.1	การใช้งานรหัสผ่าน (Password use)	ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน	Yes	No	Yes	

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.3.2	การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)	ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล	Yes	Yes	Yes	
1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)		**เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต**				**85.71**
1.4.1	นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้	Yes	No	Yes	
1.4.2	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	Yes	Yes	Yes	
1.4.3	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ซึ่งได้รับอนุญาตแล้ว	Yes	Yes	Yes	

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.4.4	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย	Yes	No	Yes	
1.4.5	การแบ่งแยกเครือข่าย (Segregation in networks)	ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ	Yes	Yes	Yes	
1.4.6	การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้	Yes	Yes	Yes	
1.4.7	การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง	No	Yes	Yes	
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)		**เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต**				**88.89**

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
1.5.1	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ	Yes	Yes	Yes	
1.5.2	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ	Yes	Yes	Yes	
1.5.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ	Yes	Yes	Yes	
1.5.4	การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว	Yes	No	Yes	
1.5.5	การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้	Yes	Yes	Yes	

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.5.6	การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง	No	Yes	Yes	
1.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)		**เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต**				**100.00**
1.6.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน	Yes	Yes	Yes	
1.6.2	การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ	Yes	Yes	Yes	

ตารางที่ 6.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)		**เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**				**66.67**
1.7.1	การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้	Yes	No	Yes	
1.7.2	การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติบุคลากรที่จำเป็นต้องปฏิบัติงานจากภายนอกสำนักงาน	Yes	No	Yes	

ซึ่งจากการประเมินผลการควบคุมภายในด้านเทคโนโลยีสาสนเทศ (ก่อนทำโครงการ) ทำให้ทราบว่า ระบบงานเทคโนโลยีสารสนเทศของธนาคารที่มีการจัดการอยู่ในปัจจุบัน มีการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศอยู่ในระดับต่าง ๆ ที่เพียงพอที่องค์กรสามารถยอมรับได้ และมีบางส่วนที่จำเป็นต้องปรับปรุงให้มีความเพียงพออย่างเหมาะสม สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) สามารถสรุปได้ดังตาราง

ตารางที่ 6.1.2.2 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

A.1	Access Control (ก่อนดำเนินโครงการ)	Indicator Organize	Overall Score	Overall Rating
			88.04	Marginal
A.1.1	Business Requirement for Access Control	85.39	100.00	Excellent
A.1.2	User Access Management	85.39	91.67	Marginal
A.1.3	User Responsibilities	85.39	83.33	Poor
A.1.4	Network Access Control	85.39	85.71	Marginal
A.1.5	Operating System Access Control	85.39	88.89	Marginal
A.1.6	Application and Information Access Control	85.39	100.00	Excellent
A.1.7	Mobile Computing and Teleworking	85.39	66.67	At Risk

โดยผู้ศึกษาโครงการได้ทำการสรุปผลแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) และนำมาจัดทำเป็นแผนภูมิภาพให้เห็นถึงข้อมูลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน (ISO/IEC 27001) และระดับที่องค์กรยอมรับได้ (ก่อนทำโครงการ) พบว่า จากแผนภูมิภาพแสดงให้เห็นถึงตามแนวปฏิบัติที่องค์การมีการปฏิบัติงานอยู่ในปัจจุบันนั้น แบ่งเป็น 3 รูปแบบที่เป็นการดำเนินการที่ดีเป็นไปตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ในเฉพาะขอบเขตเรื่องการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) ดังนี้

1) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับดีมาก (Excellent) ประกอบด้วย

- ✓ การจัดการด้านข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)
- ✓ การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)

ซึ่งมีลักษณะการดำเนินการที่เป็นเชิงป้องกันตั้งแต่การวางนโยบาย ระเบียบ หลักเกณฑ์ต่าง ๆ ครอบคลุมการดำเนินการเข้าถึงระบบสารสนเทศของธนาคารอย่างเหมาะสม และสามารถประยุกต์ใช้ในการควบคุมการเข้าถึงระดับ Application ได้อย่างถูกต้อง ครบถ้วน

2) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับพอใช้ (Marginal) ประกอบด้วย

- ➢ การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)
- ➢ การควบคุมการเข้าถึงเครือข่าย (Network access control)
- ➢ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ซึ่งมีลักษณะการดำเนินการอยู่ในระดับที่องค์กรสามารถยอมรับได้ แต่ยังคงไม่ถึงระดับที่ดีมาก โดยหากดูในรายละเอียดยังพบว่า การดำเนินการบางประการยังคงมีความเสี่ยงด้านเทคโนโลยีสารสนเทศนำไปสู่ความเสี่ยงให้กับธนาคารได้ เช่น การยังไม่มีการดำเนินการในการควบคุม ติดตาม ประเมินความเสี่ยงการเข้าถึงระบบเครือข่ายอย่างต่อเนื่อง เป็นต้น

3) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับต้องปรับปรุง (Poor) ประกอบด้วย

- ● การจัดการที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

ซึ่งมีลักษณะการดำเนินการอยู่ในระดับที่ต่ำกว่าองค์กรยอมรับได้ โดยอาจนำมาซึ่งความเสี่ยงในการเข้าถึงระบบสารสนเทศของธนาคารที่ไม่เหมาะสมได้ เช่น การกำหนดให้พนักงานจำเป็นต้องมีวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่านอย่างเหมาะสม ซึ่งอาจเป็นการดำเนินการให้ระบบ Detect หรือ บังคับให้พนักงานมีการเปลี่ยนแปลงรหัสผ่านหลังจากที่ได้รับ Username และ Password จากผู้ดูแลระบบงานแล้วเพื่อป้องการเข้าถึงโดยไม่ได้รับอนุญาตได้

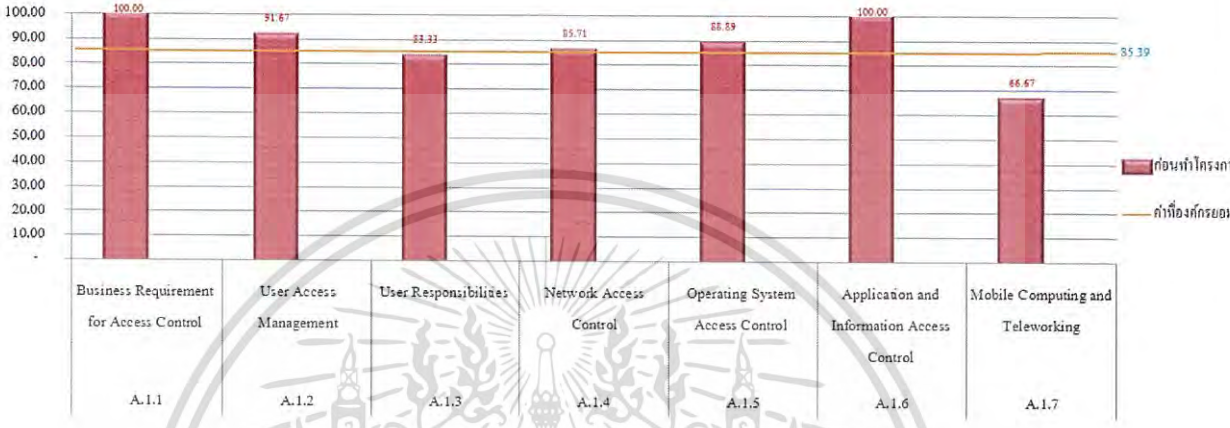
4) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับที่มีความเสี่ยงมาก (At Risk) ประกอบด้วย

- ○ การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

ซึ่งมีลักษณะการดำเนินการที่มีอยู่ในปัจจุบันมีระดับความเสี่ยงสูงในการเข้าถึงระบบสารสนเทศของธนาคารได้ เช่น การที่ธนาคารอนุญาตให้พนักงานหรือผู้ดูแลระบบงาน ใช้อุปกรณ์

พกพาส่วนตัว (Bring Your Own Device : BYOD) มาเชื่อมต่อกับระบบสารสนเทศของธนาคารโดยไม่มีการควบคุม ติดตาม อย่างต่อเนื่อง และเหมาะสม

จากประเด็นดังที่กล่าวมาข้างต้น ผู้ศึกษาโครงการสามารถแสดงให้เห็นถึงแผนภูมิภาพรายละเอียดการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่มีการควบคุมภายในอยู่ในปัจจุบัน ดังต่อไปนี้



รูปที่ 6.1.2 แผนภูมิแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

6.2 การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

จากการปรเมินผลแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) ตามมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) แล้วนั้น พบว่า มีบางประเด็นสายเทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลระบบงานมีการบริหารจัดการอยู่ในระดับที่ต่ำกว่าองค์กรยอมรับได้ ซึ่งสามารถนำมาประเมินความเสี่ยงการขาดการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ดี นำไปสู่ความเสี่ยงของธนาคารที่กำหนดไว้ได้จึงนำมาสู่การสร้างแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

1) ผู้ศึกษาโครงการ นำหัวข้อเรื่องจากการประเมินการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศที่พบว่า ยังไม่มีการควบคุมภายในอย่างเหมาะสม ทั้งที่อยู่ในระดับความเสี่ยงสูง (At Risk) หรือ ระดับที่ควรปรับปรุง (Poor) หรือ ระดับพอใช้ (Margianal) มาเพื่อประเมินว่ามีความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งสอดคล้องกับความเสี่ยงขององค์กรประเภทใด และมีรายละเอียดของความเสี่ยง ดังต่อไปนี้

ตารางที่ 6.2.1 การกำหนดประเภทความเสี่ยงในแบบจำลอง (ก่อนทำโครงการ)

Risks		
#	**Risk Category**	**Risk Description**
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ Detective Control เพื่อควบคุม ติดตาม อย่างต่อเนื่อง และเหมาะสม
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ Detective Control เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ Detective Control เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ Detective Control เพื่อการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ Preventive Control เพื่อการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรให้เป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ไม่ว่าเป็นการหยุดชะงักหรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม

ตาราง 6.2.1 (ต่อ)

Risks		
#	**Risk Category**	**Risk Description**
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ Detective control เพื่อการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่าง ๆ ที่ไม่เหมาะสมกับธนาคาร
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ Preventive Control
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม

RRAM - RISK OVERVIEW

ชื่อการตรวจสอบ : *ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control (ก่อนทำโครงการ)*

วันที่ประเมิน : *07-12-2013*

Risks

#	Risk Category	Risk Description
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม ทบทวนสิทธิ์ หรือ Log อย่างต่อเนื่องและเหมาะสม
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่างๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุมติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่างๆ ที่ไม่เหมาะสมกับธนาคาร
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานของตนจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม

รูปที่ 6.2.1 แสดงการระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)

2) ผู้ศึกษาโครงการทำการประเมิน Likelihood ซึ่งเป็นโอกาสหรือความถี่ของการเกิดเหตุการณ์ เพื่อประเมินสถานการณ์ของโอกาสเกิดขึ้น โดยการใช้การประมาณการของโอกาสที่เกิดขึ้นได้มากที่สุด ซึ่งจากการประเมินการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หากผู้ศึกษาโครงการร่วมประเมินความเสี่ยงกับผู้เชี่ยวชาญด้านการควบคุมภายในท่านอื่น และมีความคิดเห็นในการประเมินความเสี่ยงในส่วนโอกาสหรือความถี่ของการเกิดเหตุการณ์ที่แตกต่างกัน สามารถทำการประเมินความเสี่ยงได้โดยระบุในช่องความเห็นในแต่ละ Paticipant โดยแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศจะทำการเฉลี่ยความเสี่ยงตามความคิดเห็นของผู้ร่วมศึกษาโครงการ ดังนี้

ตารางที่ 6.2.2 (ต่อ)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของการ Preventive Control เพื่อการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรให้เป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	Yes	5		**5.0**
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ Detective control เพื่อการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่าง ๆ ที่ไม่เหมาะสมกับธนาคาร	Yes	5		**5.0**
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนการ Preventive Control	Yes	5		**5.0**

ตารางที่ 6.2.2 การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ (ก่อนทำโครงการ)

LIKELIHOOD						
#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ Detective Control ควบคุม ติดตาม อย่างต่อเนื่องและเหมาะสม	Yes	5		**5.0**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนการDetective Control เพื่อผู้ใช้งานเปลี่ยนรหัสผ่านให้เหมาะสม	Yes	4		**4.0**
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ Detective Control เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	Yes	5		**5.0**
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ Detective Control เพื่อการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงระบบเครือข่ายธนาคาร	Yes	5		**5.0**

ตารางที่ 6.2.2 (ต่อ)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	Yes	5	4	**4.5**
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	Yes	5		**5.0**

RRAM - RISK ASSESSMENT (LIKELIHOOD)

ชื่อการตรวจสอบ : *ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control (ก่อนทำโครงการ)*

วันที่ประเมิน : *07-12-2013*

LIKELIHOOD (score 1-5)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	AVRG
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม ทบทวนสิทธิ์ หรือ Log อย่างต่อเนื่องและเหมาะสม	Yes	5		5.0
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	Yes	4		4.0
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	Yes	5		5.0
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	Yes	5		5.0
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่างๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	Yes	5		5.0
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่างๆ ที่ไม่เหมาะสมกับธนาคาร	Yes	5		5.0
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	Yes	5		5.0
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	Yes	5	4	4.5
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	Yes	5		5.0

รูปที่ 6.2.2 การประเมินโอกาสของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)

3) ผู้ศึกษาโครงการทำการประเมิน Impact ซึ่งเป็นผลกระทบหรือความเสียหายของการเกิดเหตุการณ์เพื่อประเมินสถานการณ์ความเสียหายที่มากที่สุดที่อาจเกิดขึ้นได้ ทั้งในด้านความเสียหายที่เป็นตัวเงิน ผลกระทบที่ไม่เป็นตัวเงิน เช่น ด้านกฎหมาย กฎระเบียบ ด้านชื่อเสียง หรือลูกค้า โดยการใช้การประมาณการของความเสียหายที่มากที่สุด (จำนวนเท่าไรต่อการเกิดเหตุการณ์ขึ้น) ซึ่งการประเมินการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หากมีผู้เชี่ยวชาญด้านการควบคุมภายในท่านอื่น และมีความคิดเห็นในการประเมินความเสี่ยงของผลกระทบหรือความเสียหายการเกิดเหตุการณ์ที่แตกต่างกัน สามารถทำการประเมินความเสี่ยงได้โดยระบุในช่องความเห็นในแต่ละ Paticipant โดยแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศจะทำการเฉลี่ยความเสี่ยงตามความคิดเห็นของผู้ร่วมศึกษาโครงการ ดังนี้

ตารางที่ 6.2.3 การประเมินผลกระทบหรือความเสียหายของการเกิดเหตุการณ์ (ก่อนทำโครงการ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกระบวนการ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกระบวนการ	ด้านชื่อเสียง	ด้านลูกค้า	
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งานในส่วนของการ Detective Control เพื่อควบคุม ติดตาม อย่างต่อเนื่อง และเหมาะสม	Yes	6	4	6	8					**6.0**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ Detective Control เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	Yes	6	3	2	5					**4.0**
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ Detective Control เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	Yes	1	3	1	2					**1.8**

ตาราง 6.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ Detective Control เพื่อการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	Yes	11	4	6	8					**7.3**
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของการ Preventive Control เพื่อการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรให้เป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	Yes	1	3	2	5					**2.8**

ตาราง 6.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ Detective control เพื่อการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่าง ๆ ที่ไม่เหมาะสมกับธนาคาร	Yes	6	3	1	3					**3.3**
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ Preventive Control	Yes	1	3	1	3					**2.0**
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกัน โดยพิจารณาความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ log ของผู้ใช้งานและผู้ดูแลระบบของธนาคารผ่านอุปกรณ์สื่อสารพกพา	Yes	6	4	6	8	6	6	6	8	**6.3**

ตาราง 6.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ Detective Control เพื่อการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	Yes	6	4	6	5					**5.3**

RRAM - RISK ASSESSMENT (IMPACT)

ชื่อการตรวจสอบ : *ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control (ก่อนทำโครงการ)*

วันที่ประเมิน : *07-12-2013*

IMPACT (score 1-11)				Participant1				Participant2				
#	Risk Category	Risk Description	Plot	ผู้จัดการเงิน	ผู้จัดการระบบ	ผู้ใช้ (ลูกค้า)	ผู้ใช้ (ลูกค้า)	ผู้จัดการเงิน	ผู้จัดการระบบ	ผู้ใช้ (ลูกค้า)	ผู้ใช้ (ลูกค้า)	AVRG
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม ทบทวนสิทธิ์ หรือ Log อย่างต่อเนื่องและเหมาะสม	Yes	6	4	6	8					6.0
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	Yes	6	3	2	5					4.0
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	Yes	1	3	1	2					1.8
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	Yes	11	4	6	8					7.3
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดตอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่างๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	Yes	1	3	2	5					2.8
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่างๆ ที่ไม่เหมาะสมกับธนาคาร	Yes	6	3	1	3					3.3
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	Yes	1	3	1	3					2.0
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ log ของผู้ใช้งานและผู้ดูแลระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	Yes	6	4	6	8	6	6	6	8	6.3
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานของท่านจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	Yes	6	4	6	5					5.3

รูปที่ 6.2.3 การประเมินผลกระทบของเหตุการณ์ที่เกิดในแบบจำลองที่จัดสร้าง (ก่อนทำโครงการ)

4) ผู้ศึกษาโครงการได้นำผลลัพธ์ของการแสดงแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ มาจากการมูลค่าความเสียหายที่อาจจะเกิดขึ้นได้ (Risk Value) ซึ่งเกิดขึ้นได้จากการที่โอกาสหรือความถี่ของการเกิดเหตุการณ์ขึ้น คูณผลกระทบหรือความเสียหายที่เกิดขึ้น ซึ่งสามารถคิดคำนวณได้ดังนี้

ตารางที่ 6.2.4 การคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้น (ก่อนทำโครงการ)

Risk Value (Likelihood X Impact)					
#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม ทบทวนสิทธิ หรือ Log อย่างต่อเนื่องและเหมาะสม	5.00	6.00	**30.00**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	4.00	4.00	**16.00**
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	5.00	1.75	**8.75**

ตารางที่ 6.2.4 (ต่อ)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	5.00	7.25	**36.25**
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	5.00	2.75	**13.75**
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ใน	5.00	3.25	**16.25**

ตารางที่ 6.2.4 (ต่อ)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
		ส่วนของการ (Detective control) ในการควบคุม ติดตาม ป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ ที่ไม่เหมาะสมกับธนาคาร			
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	5.00	2.00	**10.00**
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา เช่น notebook, palm, และ laptop เป็นต้น และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ log ของผู้ใช้งานและผู้ดูแลระบบของธนาคารผ่านอุปกรณ์สื่อสารพกพา	4.50	6.25	**28.13**
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	5.00	5.25	**26.25**

RRAM - RISK ASSESSMENT (RISK VALUE)

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control (ก่อนทำโครงการ)

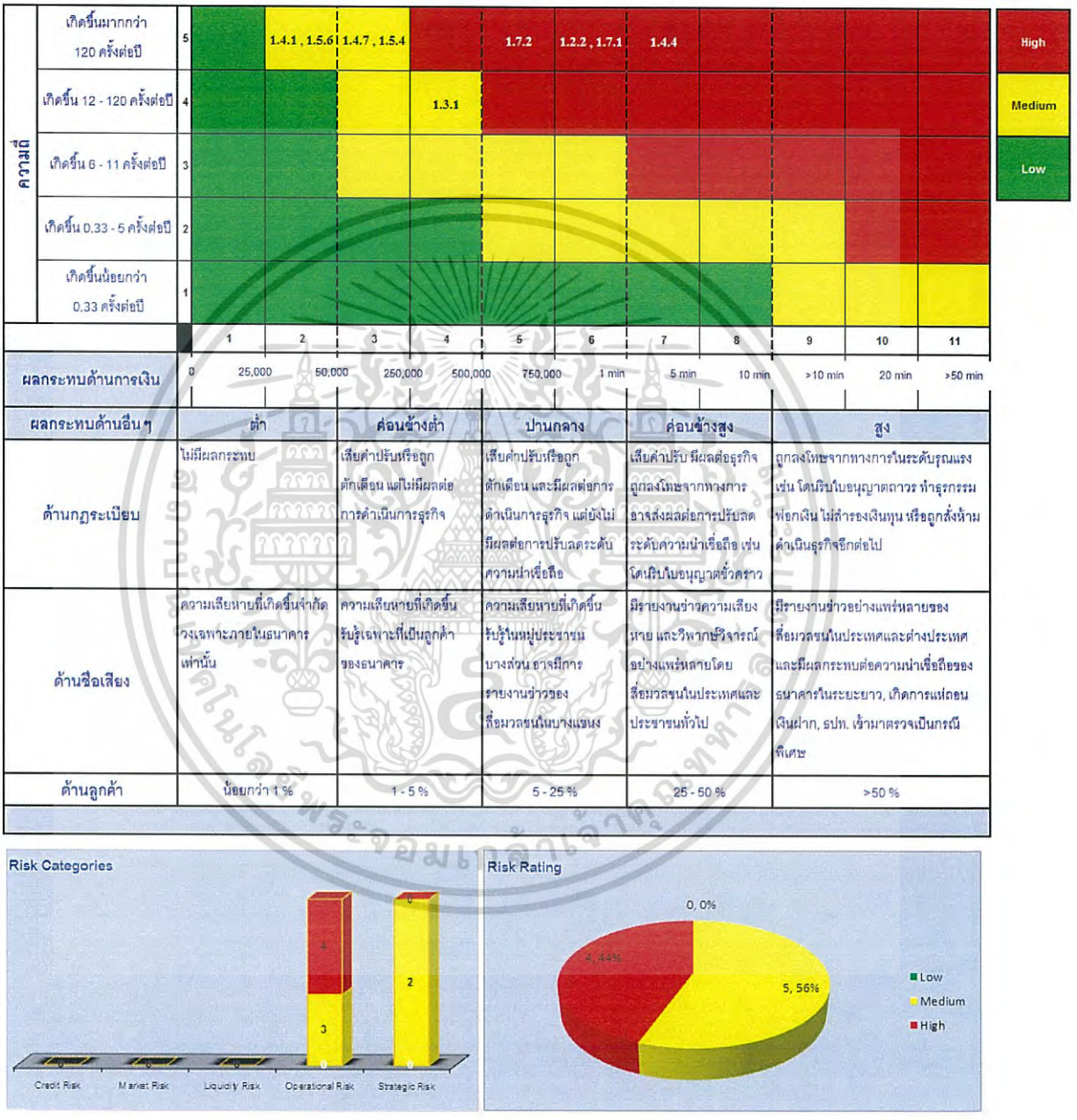
วันที่ประเมิน : 07-12-2013

Risk Value (Likelihood X Impact)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม ทบทวนสิทธิ์ หรือ Log อย่างต่อเนื่องและเหมาะสม	5.00	6.00	30.00
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	4.00	4.00	16.00
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	5.00	1.75	8.75
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	5.00	7.25	36.25
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่างๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	5.00	2.75	13.75
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุม ติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่างๆ ที่ไม่เหมาะสมกับธนาคาร	5.00	3.25	16.25
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	5.00	2.00	10.00
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ log ของผู้ใช้งานและผู้ดูแลระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	4.50	6.25	28.13
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานของหน่วยงานจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ์ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	5.00	5.25	26.25

รูปที่ 6.2.4.1 การคำนวณมูลค่าความเสียหาย (Risk Value) ก่อนทำโครงการ

ซึ่งจากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโครงการแล้วนั้น ผู้ศึกษาโครงการสามารถแสดงเป็นแผนภาพแบบจำลองความเสี่ยงที่แสดงให้เห็นระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงขององค์กรได้ดังแผนภาพ Risk Rating Matrix ดังต่อไปนี้



รูปที่ 6.2.4.2 ผลลัพธ์จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ)

6.3 ข้อเสนอแนะการเพิ่มเติม ปรับปรุงการดำเนินการ

จากการประเมินความสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) แล้วนั้น ทำให้ผู้ปฏิบัติงานหน่วยงานสายเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ได้เห็นถึงภาพรวม (Over all) ผลการปฏิบัติงานว่าอยู่ในเกณฑ์ที่องค์กรสามารถยอมรับความเสี่ยงได้หรือไม่ และมีการบริหารจัดการเป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) มากน้อยเพียงใด

ซึ่งผู้ศึกษาโครงการมีข้อเสนอแนะเพื่อให้ผู้ปฏิบัติงาน เพิ่มเติม ปรับปรุงการดำเนินการดังนี้

6.3.1 การจัดลำดับความเสี่ยงความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศ

ผู้ศึกษาโครงการ แนะนำให้ผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศทำการจัดเรียงลำดับความเสี่ยงการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ยังคงขาดการควบคุมภายในด้านเทคโนโลยีสารสนเทศตาม (Risk base Approach) ซึ่งได้เห็นจากผลลัพธ์ของแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังตารางต่อไปนี้

ตารางที่ 6.3.1 การจัดลำดับความเสี่ยงการจัดการความมั่นคงปลอดภัยเพื่อการแก้ไข

ลำดับแก้ไข	รายละเอียดความเสี่ยงจากการขาดการความคุมภายใน	ผลประเมิน Likelihood	ผลประเมิน Impact	ผลลัพธ Risk Value	ระดับความเสี่ยง
1	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	5.0	7.3	**36.5**	High
2	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม อย่างต่อเนื่อง และเหมาะสม	5.0	6.0	**30.0**	High
3	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกัน โดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	4.5	6.3	**28.35**	High

ตารางที่ 6.3.1 (ต่อ)

ลำดับแก้ไข	รายละเอียดความเสี่ยงจากการขาดการความคุมภายใน	ผลประเมิน Likelihood	ผลประเมิน Impact	ผลลัพธ Risk Value	ระดับความเสี่ยง
4	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	5.0	5.3	**26.5**	**High**
5	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุมติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่าง ๆ ที่ไม่เหมาะสมกับธนาคาร	5.0	3.3	**16.5**	**Medium**
6	1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่านให้มีความเหมาะสม	4.0	4.0	**16.0**	**Medium**

ตารางที่ 6.3.1 (ต่อ)

ลำดับแก้ไข	รายละเอียดความเสี่ยงจากการขาดการควบคุมภายใน	ผลประเมิน Likelihood	ผลประเมิน Impact	ผลลัพธ Risk Value	ระดับความเสี่ยง
7	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุหรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ให้สามารถใช้งานได้อย่างเหมาะสม	5.0	2.8	**14.0**	**Medium**
8	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	5.0	2.0	**10.0**	**Medium**
9	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	5.0	1.8	**9.0**	**Medium**

6.3.2 การตอบสนองต่อความเสี่ยงตามลำดับความสำคัญ

จากตารางการจัดลำดับความเสี่ยงการบริหารจัดการความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศของธนาคารนั้น ทำให้ผู้ศึกษาโครงการ หรือผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศทราบถึงภาพรวมของการบริหารจัดการว่าจุดใดอยู่ในระดับที่มีความเสี่ยงสูง ปานกลาง หรือต่ำ ซึ่งควรมีแนวทางการบริหารจัดการอย่างเหมาะสม ดังนี้

1) ผลการประเมินที่มีผลลัพธ์ความเสี่ยงสูง (High Risk)

ผู้ศึกษาโครงการ แนะนำให้ควรมีการตอบสนองต่อความเสี่ยงอย่างรวดเร็ว เช่น มี Action Plan การดำเนินการโดยเร็วเพื่อให้ความเสี่ยงที่ตรวจพบ หรือมีอยู่ในปัจจุบันมีการควบคุม ติดตามได้อย่างเหมาะสม ป้องกันความเสียหายหรือผลกระทบที่อาจเกิดขึ้นกับเทคโนโลยีสารสนเทศของธนาคารได้ ดังต่อไปนี้

ตารางที่ 6.3.2.1 ข้อเสนอแนะสำหรับผลลัพธ์ความเสี่ยงสูง

รายละเอียดความเสี่ยงที่ขาดการความคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารยังไม่มีการกำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ในส่วนของการ (Detective Control) ในการตรวจสอบ ตรวจเช็ค ควบคุม ติดตามการเปิดพอร์ตที่มีความเสี่ยงของระบบเครือข่ายของธนาคาร	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการกำหนดกระบวนการตรวจสอบหรือตรวจเช็คพอร์ตที่ใช้งาน เช่น จัดทำกระบวน Hardening ระบบเครือข่าย ซึ่งการเป็นกระบวนการทบทวนการกำหนดค่า (Parameter) บนระบบเครือข่ายเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันผู้บุกรุกและช่องโหว่ความปลอดภัยอื่น ๆ ของระบบเครือข่ายเป็นประจำอย่างน้อยไตรมาสละครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ เช่น ➢ File Transfer Protocal (FTP) ที่มีการกำหนดให้เค้าถึงโดยไม่มีการควบคุม (Anonymous) หรือคาดเดารหัสผ่านได้ง่าย หรือกำหนดพอร์ตให้ใช้งานให้ปลอดภัยทดแทนด้วยการใช้ Secure File Tranfer Protocal (SFTP)

ตารางที่ 6.3.2.1 (ต่อ)

รายละเอียดความเสี่ยงที่ขาดการความคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
	➢ Telnet ที่เป็นการทำงานผ่านทางอินเทอร์เน็ตรูปแบบหนึ่ง ซึ่งเป็นการขอเข้าใช้เครื่องคอมพิวเตอร์จากระยะไกล ผู้ใช้นั้นสามารเข้าถึงได้โดยการติดต่อเครือข่ายที่ได้รับอนุญาต
1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารยังไม่มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ในส่วนของการ (Detective Control) ควบคุม ติดตาม อย่างต่อเนื่อง และเหมาะสม	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการกำหนดกระบวนการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานที่มีสิทธิการใช้ระบบงานที่มีสิทธิเฉพาะ (Privilege User) เช่น Administrator, Root, Sys, System เป็นต้น หรือมีการทบทวน Log การเข้าถึงระบบงาน โดยดำเนินการเปลี่ยนรหัสผ่าน นำรหัสผ่านดังกล่าวจัดเก็บเข้าซองและมีการนำฝากในห้องมั่นคง (Custodian) ตลอดจนมีการควบคุม เบิกใช้งานการเข้าถึงอย่างเหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบ ตรวจเช็คระบบงานได้อย่างทันทีหากมีการดำเนินการเปลี่ยนแปลงใด ๆ เกิดขึ้นกับระบบงานสารสนเทศของธนาคารเป็นประจำอย่างน้อยปีละครั้ง หรือเมื่อมีการพบเข้าถึงที่สำคัญ
1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารยังไม่มีกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการกำหนดกระบวนการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานที่มีสิทธิการใช้งานอุปกรณ์เคลื่อนที่สื่อสารประเภทพกพา ที่สามารถระบบงาน Core Bank ของธนาคารได้ เช่น ผู้ใช้งานที่สิทธินอกเหนือมาตรฐาน (Exception User) ผู้บริหารหน่วยงาน และผู้ดูแลระบบงานที่สำคัญ เป็นต้น หรือมีการ

ตารางที่ 6.3.2.1 (ต่อ)

รายละเอียดความเสี่ยงที่ขาดการความคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
สอบทานสิทธิ หรือ log ของผู้ใช้งานและผู้ดูและระบบสารสนเทศของธนาคารผ่านอุปกรณ์สื่อสารพกพา	ทบทวน Log การเข้าถึงระบบงานที่สำคัญของธนาคารเป็นประจำอย่างน้อยปีละครั้ง หรือเมื่อมีการพบเข้าถึงที่สำคัญ
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ในส่วนของการ (Detective Control) ในการตรวจเช็ค ตรวจสอบ สอบทานสิทธิ หรือ Log ของผู้ใช้งานและผู้ดูแลระบบงานในการเข้าถึงระบบสารสนเทศจากภายนอกสำนักงานอย่างเหมาะสม	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการกำหนดกระบวนการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานที่มีสิทธิเข้าถึงระบบงาน Core Bank ของธนาคารจากภายนอกสำนักงานได้ เช่น ผู้ใช้งานที่ขอสิทธิเข้าถึง Citrix ที่เป็นช่องทาง VPN ของธนาคาร และผู้ดูแลระบบงานที่สามารถเข้าถึงระบบสารสนเทศได้ด้วยวิธีการอื่น ๆ เช่น Remote to Server เป็นต้น หรือมีการทบทวน Log การเข้าถึงระบบงานที่สำคัญของธนาคารเพื่อดูพฤติกรรมการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล มีการอนุมัติรายการ หรือโอนรายการเป็นประจำอย่างน้อยปีละครั้ง หรือเมื่อมีการพบเข้าถึงที่สำคัญ

2) ผลการประเมินที่มีผลลัพธ์ความเสี่ยงระดับปานกลาง (Medium Risk)

ผู้ศึกษาโครงการ แนะนำให้ควรมีการตอบสนองต่อความเสี่ยงโดยการให้ความสำคัญกับส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญก่อน เพื่อควบคุม ติดตาม และป้องกันได้อย่างทันเหตุการณ์ โดยผู้ศึกษาโครงการแนะนำให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศของธนาคารดำเนินการจัดทำในส่วนแนวทางปฏิบัติที่เป็น Detective Control ก่อน เนื่องจากเป็นการควบคุมภายในแบบตรวจหาหรือทำการตรวจสอบ ตรวจเช็ค ค้นหาข้อผิดพลาดหรือความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของธนาคารเป็นลำดับต่อมา ดังนี้

2.1) แนวทางปฏิบัติที่มีความเสี่ยงที่ต้องใช้เทคนิคด้านเทคโนโลยีสารสนเทศ

เป็นแนวทางปฏิบัติที่ผู้ศึกษาโครงการแนะนำให้ผู้ปฏิบัติงานดำเนินการพิจารณาในการควบคุม ติดตาม และดำเนินการป้องกันการเกิดความเสี่ยงที่อาจทำให้ระบบสารสนเทศของธนาคารมีการเข้าถึงได้อย่างเหมาะสมก่อน เนื่องจากจากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเห็นได้ว่า มีความเสี่ยงระดับปานกลาง ที่มีโอกาสหากขาดการควบคุมที่มีเป็นความเสี่ยงสูงได้ จึงควรมีการกำหนดแนวทางการปฏิบัติงาน ดังนี้

ตารางที่ 6.3.2.2 ข้อเสนอแนะด้านเทคนิคสำหรับผลลัพธ์ความเสี่ยงระดับปานกลาง

รายละเอียดความเสี่ยงที่ขาดการความคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารยังไม่มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ในส่วนของการ (Detective control) ในการควบคุมติดตามการป้องกันการละเมิดการติดตั้งโปรแกรมประเภทยูทิลิตี้ต่าง ๆ ที่ไม่เหมาะสมกับธนาคาร	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการติดตั้งโปรแกรมประเภทยูทิลิตี้ หรือมีการกำหนดสิทธิให้ผู้ใช้งานเข้าถึงผ่านเครื่องคอมพิวเตอร์ของธนาคารที่มีการกำหนดสิทธิเป็น User ไม่ให้สามารถดำเนินการติดต้งโปรแกรมใด ๆ เองได้ ซึ่งเป็นการกำหนดให้อุปกรณ์เครื่องคอมพิวเตอร์ Detect สิทธิตามการเข้าถึง
1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ในส่วนของการ (Detective Control) เพื่อให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ให้มีความเหมาะสม	ธนาคารควรมีการควบคุม ติดตาม การตรวจสอบการกำหนดให้ระบบงานมีวิธีการปฏิบัติในการให้พนักงานทำการเลือกเปลี่ยนรหัสผ่านเองได้ตั้งแต่ครั้งแรกที่เข้าระบบ หรือตามความบ่อยครั้งที่ต้องการ โดยทำให้ระบบ Detect การ Force Change Password เพื่อให้ผู้ใช้งานเลือกใช้รหัสผ่านได้อย่างเหมาะสม เช่น ➢ การให้เปลี่ยนรหัสผ่านตั้งแต่ครั้งแรกที่เข้าใช้ ➢ การกำหนดให้เปลี่ยนรหัสผ่านทุก 90 วัน ตามนโยบายด้านเทคโนโลยีสารสนเทศของธนาคาร

2.2 แนวทางปฏิบัติที่มีความเสี่ยงที่ต้องกำหนดให้มีความชัดเจนเป็นลายลักษณ์อักษร

เป็นแนวทางปฏิบัติที่ผู้ศึกษาโครงการแนะนำให้ผู้ปฏิบัติงานดำเนินการพิจารณาในการจัดหาแนวทางป้องกัน ด้วยวิธีการกำหนดกระบวนการต่าง ๆ ให้มีความชัดเจน เป็นลายลักษณ์อักษรป้องกันการเกิดความเสี่ยงที่อาจทำให้ระบบสารสนเทศของธนาคารมีการเข้าถึงได้ ซึ่งการกำหนดวิธีการแก้ปัญหาดังกล่าวอาจใช้การกำหนดแนวทางการป้องกันลักษณะชั่วคราว (Interim solution) เช่น การวางแผนการทบทวนนโยบายประจำปี โดยกำหนด Gap Analysis ของนโยบายด้านเทคโนโลยีสารสนเทศไว้ อาทิ การบริหารจัดการทางด้านเครือข่าย ควรมีการจัดทำคู่มือปฏิบัติงานชั่วคราวของระบบเครือข่าย ระบบปฏิบัติการ เพื่อกำหนด Port / Service ที่ธนาคารควรเปิดเพื่อการเข้าถึงหรือใช้งานให้มีความเหมาะสม สอดคล้องกับมาตรฐานการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น โดยควรมีการกำหนดแนวทางการปฏิบัติงาน ดังนี้

ตารางที่ 6.3.2.3 ข้อเสนอแนะด้านกระบวนการสำหรับผลลัพธ์ความเสี่ยงระดับปานกลาง

รายละเอียดความเสี่ยงที่ขาดการควบคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารยังไม่มีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ในส่วนของ (Preventive Control) ในการระบุ หรือกำหนดอย่างเป็นลายลักษณ์อักษรเพื่อเป็นแนวปฏิบัติในการป้องกันระบบเครือข่ายในกรณีต่าง ๆ ไม่ว่าเป็นการหยุดชะงัก หรือเหตุฉุกเฉินที่ระบบเครือข่ายไม่สามารถใช้งานได้อย่างเหมาะสม	ธนาคารควรมีการรวบรวม จัดเก็บข้อมูลเส้นทางบนเครือข่ายที่สำคัญของธนาคาร เช่น BOT , NCB Link ซึ่งเป็นเส้นทางที่เชื่อมต่อกับระบบงานของหน่วยงานรัฐบาล หรือเส้นทางระบบเครือข่ายที่มีความสำคัญ เช่น ระบบงานเงินฝาก ซึ่งเป็นธุรกรรมหลักของธนาคาร (Core Bank) เพื่อทำการกำหนดแนวทางปฏิบัติในการกำหนดการป้องกันการเกิดเหตุการณ์ต่าง ๆ อย่างเป็นลายลักษณ์อักษรว่า เส้นทางเครือข่ายใดสำคัญ เป็นเส้นทางหลัก (Primary Linkage) หรือเส้นทางสำรอง ให้ชัดเจน อย่างถูกต้อง และเหมาะสม
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ในส่วนของการ (Preventive Control)	ธนาคารควรมีการมีการรวบรวม จัดเก็บข้อมูลการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เป็น Core Bank ที่เหมาะสมที่สุด ตามที่ระบบ Detect ไว้ เพื่อจัดทำเป็นแนวทางการปฏิบัติอย่างชัดเจนเป็นลาย

ตารางที่ 6.3.2.3 (ต่อ)

รายละเอียดความเสี่ยงที่ขาดการความคุมภายใน	ข้อเสนอแนะของผู้ศึกษาโครงการ
	ลักษณ์อักษร ให้สอดคล้องกันในทุกระบบงาน เช่น ระยะเวลาที่เหมาะสมที่สุดของการจำกัดการเชื่อมต่อระบบงานหรือระบบเครือข่าย 30 นาที เพื่อกำหนดเป็นนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศในรอบการทบทวนถัดไป หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารยังไม่มีการทบทวนการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ในส่วนของการ (Detective Control) เพื่อควบคุมติดตามการเข้าถึงระบบเครือข่ายได้อย่างเหมาะสม	ธนาคารควรมีการมีการรวบรวม จัดเก็บข้อมูลนโยบายการใช้งานบริการเครือข่ายเพื่อการวางแผนการทบทวนนโยบายประจำปี โดยกำหนด Gap Analysis ของนโยบายด้านเทคโนโลยีสารสนเทศ ว่าในนโยบาบด้านเทคโนโลยีสารสนเทศควรมีการกำหนดการใช้งานเครือข่ายใดได้บ้าง เช่น กำหนดให้เข้าระบบเครือข่ายด้วยวิธีการทำ VLan ตาม IP Address ของเครื่องคอมพิวเตอร์และ Mac Address เป็นต้น ในกรณี Outsouce หรือบุคคลภายนอกธนาคารมีนโยบายให้แบ่งแยกระบบเครือข่ายออกจากผู้ใช้งานปกติ (แบ่งแยกตาม VLan) และไม่ให้เข้าถึงระบบงานสารสนเทศของธนาคารที่ระดับ Production เป็นต้น

บทที่ 7
การทดสอบแบบจำลอง (หลังทำโครงการ)

จากการทดสอบแบบจำลอง (ก่อนทำโครงการ) แสดงให้เห็นว่าการดำเนินการที่มีอยู่ในปัจจุบันมีบางส่วนที่ยังไม่มีการดำเนินการอย่างเพียงพอและเหมาะสม ซึ่งจากการประเมินความเสี่ยงแล้วทำให้เห็นถึงความสำคัญของการดำเนินการก่อนและหลังทำโครงการ ตามความเสี่ยงขององค์กร (Risk base Approach) ซึ่งองค์กรสามารถจัดลำดับความสำคัญของการพัฒนาปรับปรุงกระบวนการให้มีความเหมาะสม และมีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสอดคล้องกับมาตรฐาน (ISO/IEC 27001) ได้

7.1 การประเมินผลการจัดทำโครงการ (หลังทำโครงการ)

จากขอบเขตการพัฒนาแบบจำลองความเสี่ยงและการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศ นำมาสู่การประเมินผลการโครงการ โดยทำการประเมินผลโครงการที่มีการปฏิบัติงานในปัจจุบันของธนาคารพาณิชย์แห่งหนึ่ง เพื่อแสดงให้เห็นการบริหารจัดการความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศตามมาตรฐาน (ISO/IEC 27001) ซึ่งได้ทำการประเมินผลการบริหารจัดการส่วนที่เกี่ยวข้องกับระบบงานด้านเงินฝาก อันเป็นธุรกิจหลัก (Core Business) ของธนาคารพาณิชย์ (ก่อนทำโครงการ) เพื่อให้ผู้ปฏิบัติงานได้ทราบถึงการดำเนินการที่มีในปัจจุบันว่ามีความเสี่ยง และการขาดการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างไรไปแล้วนั้น ผู้ปฏิบัติงานได้นำไปพิจารณาในการดำเนินการวางแผน หรือจัดทำแนวทางปฏิบัติดังคำแนะนำของผู้ศึกษาโครงการ ซึ่งสามารถประเมินผลการจัดดำเนินาร (หลังทำโครงการ) ได้ดังนี้

7.1.1 ผู้ปฏิบัติงานนำแนวทางข้อเสนอแนะไปบริหารการจัดการความมั่นคงปลอดภัย

ผู้ศึกษาโครงการได้ให้ผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศ นำแนวทางที่ผู้ศึกษาโครงการได้แนะนำไปปฏิบัติ หรือสามารถวางแผน ค้นคว้าข้อมูลด้านการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ดีจากแนวทางปฏิบัติงานอื่น ๆ เองได้ จาก Framework of IT Best Practice โดยกำหนดให้เมื่อดำเนินการใด ๆ หรือมีแนวทางการปฏิบัติงานแล้ว ให้มีการจัดส่งหลักฐาน (Evidence) ต่าง ๆ ให้กับผู้ศึกษาโครงการอย่างเป็นลายลักษณ์อักษร ดังนี้ ตามภาคผนวก ค

ตารางที่ 7.1.1 แบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายในโดยการประเมินตนเอง (หลังทำโครงการ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (Use access management 2) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การบริหารจัดการสิทธิผู้ใช้งานและรหัสผ่าน ข้อ 5.1.2 (2.1) สำหรับการกำหนดสิทธิสำหรับบุคคล กรณีขอใช้สิทธินอกเหนือมาตรฐาน (Exception) 3) เอกสาร Authorization matrix ขั้นตอนการร้องขอผู้ใช้สิทธิพิเศษ	1) ธนาคารมีนโยบายฯ การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) การจัดการสิทธิเฉพาะในการใช้งานระบบตามความจำเป็นในการใช้งานของผู้ใช้ในแต่ละบัญชีผู้ใช้ (UserID) 2) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย และได้รับสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม โดยกรณีขอใช้สิทธินอกเหนือมาตรฐาน (Exception) โดยทั่วไประบบสารสนเทศต่าง ๆ ไม่อนุญาตให้มีการกำหนดสิทธินอกเหนือมาตรฐานเว้นแต่มีความจำเป็น โดยจะต้องทำเรื่องขออนุมัติเป็นกรณีไป 3) ในระบบงานที่เป็น Core Business ธนาคารมีการกำหนด Role and Matrix เพื่อให้ทราบถึงอำนาจอนุมัติในระบบงานในแต่ละสิทธิที่ได้รับอย่างเหมาะสม

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
	☑ Detective Control	เอกสารขั้นตอนกระบวนการปฏิบัติงานเพื่อการบริหารจัดการสิทธิเฉพาะ (Flow Privilege User) และการทบทวน Log ภาคผนวก ง 1.2.2(1)	ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการให้มี การเบิกใช้ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิเฉพาะ (Privilege User) ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาซองรหัสผ่านดังนี้ *ตัวอย่างรายละเอียดการสอบทาน* *"สอบทาน Access Log โดยมีการใช้ Privilege user เข้า Log in เมื่อวันที่ 25 ธันวาคม 2556 เวลา 18.18 น. และ Log out ออกจากระบบเมื่อวันที่ 25 ธันวาคม 2556 เวลา 20.20 น"*
	☑ Corrective Control	เอกสารการขอเบิกใช้ Privilege User ของระบบงานเงินฝาก	ธนาคารมีการกำหนดเอกสารแบบฟอร์มเอกสารการขอเบิกใช้สิทธิเฉพาะ (Privilege User) เพื่อให้ผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศนำไปใช้ในการแก้ไขปัญหาระบบงานที่เกิดขึ้น กรณีที่สิทธิของพนักงานปฏิบัติงานไม่สามารถดำเนินการได้
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารมีการกำหนดวิธีปฏิบัติที่มั่นคงปลอดภัยสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	ธนาคารมีนโยบายฯ การใช้งานรหัสผ่าน สำหรับผู้ใช้งาน (Password use) พนักงานที่มีสิทธิในระบบสารสนเทศใด ๆ ของกลุ่มธุรกิจทางการเงิน ต้องเก็บรักษารหัสผ่านเป็นความลับ และกำหนดรหัสผ่านให้ยากต่อการคาดเดา
	☑ Detective Control	ผู้ศึกษาโครงการใช้วิธีการเข้าถึงหน้าจอการกำหนดให้ระบบงาน Force Change Password เพื่อให้ผู้ใช้งานทำการเลือกใช้รหัสผ่าน ภาคผนวก ง 1.3.1(1)	ธนาคารดำเนินการกำหนดให้ระบบงานเงินฝาก (Flexcute) ให้ผู้ใช้งานสามารถดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)
	☑ Corrective Control	เอกสาร IT Request การขอปลดล็อกรหัสผ่าน	ธนาคารมีวิธีการกำหนดให้ผู้ใช้งานสามารถร้องขอผ่านทาง IT Request ในกรณีไม่สามารถใช้งานรหัสผ่านที่ตนเองเปลี่ยน หรือเกิดปัญหาการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนด โดยต้องมีการอนุมัติผ่านระบบงาน IT Request ของหัวหน้างาน และเจ้าของข้อมูลในระบบงานอย่างเหมาะสม ซึ่งทางผู้ปฏิบัติงานจะดำเนินการ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
			Generate รหัสผ่านและส่งมอบให้ตามกระบวนการ
1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)			
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารมีการจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ***ใช่หรือไม่อย่างไร***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ การควบคุมการใช้งานบริการเครือข่าย (Policy on use of network services) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ รวมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ หรือบริการใดไม่สามารถใช้งานได้
	☐ Detective Control	เอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ภาคผนวก ง 1.1.4 (1) ซึ่งยังคงดำเนินการไม่แล้วเสร็จ(มีความเสี่ยง)	ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet เป็นต้น
	☑ Corrective Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) บทที่เกี่ยวกับนโยบายการรักษาความ	ธนาคารมีการกำหนดให้มีการทบทวนปรับปรุงนโยบายด้านเทคโนโลยีสารสนเทศ ครอบคลุมถึง การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ เนื่องจากระบบ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
		มั่นคงปลอดภัยทางสารสนเทศ	เครือข่ายสื่อสารมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจในปัจจุบัน หากไม่มีการบริหารจัดการที่ดี จะส่งผลกระทบต่อการดำเนินธุรกิจ จึงมีการแบ่งหน้าที่ความรับผิดชอบ การเฝ้าระวังทั้งที่เป็นการทำงานของอุปกรณ์ การเฝ้าระวังการบุกรุก และการกำหนดขั้นตอนการปฏิบัติงาน ตลอดจนสร้างกระบวนการบริหารจัดการ การให้บริการของผู้ให้บริการภายนอก ซึ่งต้องสอดคล้องนโยบายฯฉบับใหม่
1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการ	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)	ธนาคารมีนโยบายฯ กำหนดให้มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) มาตรการการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
	☑ Detective Control	หน้าจอการ Configuration เพื่อเปิดปิด Port การเข้าถึงผ่านระบบเครือข่าย ภาคผนวก ง 1.4.4(2)	ธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงและยังคงไม่มั่นคงปลอดภัย เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
ป้องกันการเข้าถึงโดยผ่านทางเครือข่าย ***ใช่หรือไม่อย่างไร***	☑ Corrective Control	เอกสาร Request For Change (RFC) Network	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลงโดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสมก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงที่อุปกรณ์เครือข่ายเพื่อป้องกันความมั่นคงปลอดภัย
1.4.7การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารมีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ***ใช่หรือไม่อย่างไร***	☐ Preventive Control	ผู้ศึกษาโครงการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ พบว่า ยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด ซึ่งยังคงดำเนินการไม่แล้วเสร็จ(มีความเสี่ยง)	ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)
	☑ Detective Control	อ้างอิงเอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการกำหนด Mac Address, IP Address แยกสำหรับแต่ละอุปกรณ์ ตลอดจนเส้นทางที่ธนาคารจำเป็นต้องมีการเชื่อมต่อบนเครือข่ายเพื่อให้ข้อมูลสารสนเทศสามารถติดต่อสื่อสารได้กับ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
			หน่วยงานรัฐ และหน่วยงานกำกับ เช่น Site VOIP conference กับธนาคารแห่งประเทศไทย
	☑ Corrective Control	อ้างอิงเอกสาร Network Diagram แสดงการแบ่งแยกเครือข่าย	ธนาคารมีการกำหนดเส้นทางการติดตั้งระบบเครือข่ายสำหรับกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถรองรับการดำเนินการของธุรกรรมอิเล็กทรอนิกส์ (Core Bank) ได้อย่างต่อเนื่อง โดยอุปกรณ์ Switch สามารถ Manage เส้นทางการไหลข้อมูลเปลี่ยนอัตโนมัติ เป็น สาขา > ISP > ศูนย์ DC สำรอง ตลอดจนผู้ดูแลระบบเครือข่ายจะดำเนินการปรับ configuration firewall ของศูนย์ DC สำรองให้ธนาคารสามารถรับส่งข้อมูลได้อย่างต่อเนื่อง เพื่อให้สามารถรองรับการดำเนินการของธุรกรรมอิเล็กทรอนิกส์ (Core Bank) ได้อย่างต่อเนื่อง
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารมีการจำกัดและ	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.5. การควบคุมการเข้าถึง	ธนาคารมีนโยบายฯ การใช้งานโปรแกรมประเภท Utility (Use of system utilities) การจำกัดและควบคุมการใช้งานโปรแกรมประเภท Utility เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคง

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
ควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ***ใช่หรือไม่อย่างไร***		ระบบปฏิบัติการ (Operating system access control)	ปลอดภัยที่ได้กำหนดไว้
	☑ Detective Control	ผู้ศึกษาโครงการทำการเข้าถึงหน้าจอของเครื่องคอมพิวเตอร์ผู้ใช้งาน (พนักงานธนาคาร) ที่มีการกำหนดสิทธิระดับ OS เป็น User โดยมีการควบคุมไม่ให้ติดตั้งโปรแกรมใด ๆ ภาคผนวก ง 1.4.4(1)	ธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคาร มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใด ๆ ของธนาคารได้ หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม
	☑ Corrective Control	เอกสารการร้องขอสิทธิ ผ่านระบบ IT Request	ธนาคารมีการจำกัดการติดตั้งโปรแกรมประเภทยูทิลิตี้ โดยกำหนดให้ผู้ใช้งานต้องการใช้งาน ต้องมีการร้องขอผ่าน IT Request เพื่อให้ผู้ดูและระบบงานทำการติดตั้งระบบงานให้อย่างเหมาะสม เพื่อป้องกันความปลอดภัยในการติดตั้ง Software ใด ๆ
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	☐ Preventive Control	ผู้ศึกษาโครงการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ พบว่า ยังไม่ครบถ้วน คิดเป็น 1-2%	ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
ธนาคารมีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ***ใช่หรือไม่อย่างไร***		ของระบบเงินฝากทั้งหมด ซึ่งยังคงดำเนินการไม่แล้วเสร็จ(มีความเสี่ยง)	2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (เน้น Core Bank ลำดับแรก) มีการกำหดนให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)
	☑ Detective Control	อ้างอิงตามเอกสารแนบของผู้ศึกษา โครงการใช้เทคนิคในการเข้าถึง Server ดูค่า configuration การตั้งความมั่นคงปลอดภัย ภาคผนวก ค 1.3.2(1)	ธนาคารมีการกำหนดให้ระบบที่มีความสำคัญ (Core Bank) มีการควบคุมให้ระบบงานมีจำกัดระยะเวลาเชื่อมต่อ โดยกำหนดเป็นระยะเวลา หรือถ้ามีการใส่รหัสผ่านผิดระบบงานจะล็อก ดังนี้ - Reset account Lockout counter after คือ ระยะเวลาที่คีย์ผิดตั้งแต่ผิดครั้งแรก แล้วนับไปอีกกี่นาทีถึง reset จำนวนที่นับ ถ้าคีย์ผิดครบตามจำนวนครั้งที่กำหนดแล้วอยู่ในเวลาก็จะล็อก แต่ถ้าคีย์ผิดแต่ยังไม่ครบ แล้วเวลานับถึงที่ตั้งแล้ว ก็จะเริ่มนับที่ 0 ใหม่ (ธนาคารกำหนดไว้ = 30 นาที) จากการดำเนินการกำหนดค่า ดังกล่าว จะทำให้การใช้งานโปรแกรมจำพวกสุ่มรหัสผ่าน เช่น Flickr หรือ Brute force ในการเข้าถึงระบบงานธนาคารระดับ OS ได้ยาก เมื่อเปิด Log ของเครื่อง

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
			OS จะพบว่าแหล่งต้นทางมาจากที่ใด และสามารถทำการ log account ต้นทางดังกล่าวไม่ให้มีการใช้งานเพื่อความปลอดภัย
	☑ Corrective Control	อ้างอิงเอกสาร Request For Change (RFC) ระบบงาน Core Bank ระดับ OS	ธนาคารมีการกำหนดให้หากมีการเปลี่ยนแปลงค่ามาตรฐานความมั่นคงปลอดภัยใด ๆ ต้องทำการการร้องขอ ควบคุมการเปลี่ยนแปลงโดยผู้ดูแลระบบงานต้องมีการขออนุมัติหัวหน้างานอย่างเหมาะสมก่อนดำเนินการใด ๆ โดยจัดทำเอกสาร Request for Change (RFC) ก่อนเปลี่ยนแปลงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันความมั่นคงปลอดภัย
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารมีการต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น	☑ Preventive Control	1) นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile computing and teleworking)	1) ธนาคารมีนโยบายฯ การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communication) อุปกรณ์สื่อสารประเภทพกพา คือ อุปกรณ์สื่อสารที่สามารถประมวลผล บันทึกข้อมูล และเชื่อมต่อเครือข่ายได้ เช่น Notebooks, Tablet, Smart-Phones และอุปกรณ์อื่น ๆ ที่สามารถทำงานลักษณะคล้ายคลึงอุปกรณ์เหล่านี้ ให้พิจารณาเพิ่มขั้นตอนปฏิบัติงานที่มีความมั่นคงปลอดภัยมากกว่า

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ***ใช่หรือไม่อย่างไร***		2) ระเบียบการใช้งานทรัพย์สินสารสนเทศธนาคาร ข้อ 3.2 การใช้งานอุปกรณ์สื่อสารเคลื่อนที่ 3) บันทึกความเข้าใจกระบวนการในการปฏิบัติงานระหว่างหน่วยงาน (Sign Off) เรื่อง การใช้งานอุปกรณ์สื่อสารเคลื่อนที่ และเครือข่ายคอมพิวเตอร์ (Mobile Device and Network) ข้อ 5 เนื้อหา ขั้นตอนการปฏิบัติงาน ตั้งแต่การขอใช้งาน	อุปกรณ์สารสนเทศทั่วไป โดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์ที่ใช้เชื่อมต่อ 2) ธนาคารมีการกำหนดระเบียบในการใช้งานทรัพย์สินสารสนเทศ เพื่อให้ผู้ใช้งานและผู้ปฏิบัติงานตระหนักในหน้าที่ความรับผิดชอบของตนเอง เช่น ผู้ใช้งานต้องขอลงทะเบียนอุปกรณ์สื่อสารเคลื่อนที่กับผู้ดูแลระบบงานผ่าน IT Request และขออนุมัติเป็นลายลักษณ์อักษร ตามความจำเป็นของการใช้งาน และส่งคืนอุปกรณ์หรือแจ้งการถอดถอนสิทธิเมื่อสิ้นสุดความจำเป็นในการใช้งาน 3) ธนาคารมีการจัดทำ Sign Off กับหน่วยงานต่าง ๆ เพื่อกำหนดเป็นข้อตกลงอย่างเป็นลายลักษณ์อักษร ในการป้องกันการเข้าถึงระบบงานอย่างมั่นคงปลอดภัย ผ่านการใช้งานด้วยอุปกรณ์เคลื่อนที่พกพา และสิทธิตามที่ได้รับอนุญาตอย่างเหมาะสม ดังนี้ - การขอใช้งาน ลงทะเบียน และอนุมัติกลุ่มผู้ใช้งานที่ได้รับสิทธิโดยมาตรฐาน กรณีพนักงานธนาคารมีความประสงค์จะใช้งาน ให้ส่งคำร้องขอ หรือ “IT Request” ต่อสายเทคโนโลยีสารสนเทศ และ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
		ลงทะเบียน และอนุมัติ	ต้องผ่านการอนุมัติจากหัวหน้าฝ่ายผู้ขอใช้งาน ซึ่งจะพิจารณาคำขอเป็นรายบุคคล ตามหน้าที่ปฏิบัติงาน และความจำเป็น พร้อมทั้งพิจารณารับทราบความเสี่ยง และผลกระทบต่อธนาคาร - การปฏิบัติเมื่อเปลี่ยนอุปกรณ์สื่อสารเคลื่อนที่ หรืออุปกรณ์สูญหายให้ผู้ใช้งานแจ้งสายเทคโนโลยีสารสนเทศผ่านทาง “IT Request” ทุกครั้ง เพื่อลบโปรแกรมและข้อมูลสารสนเทศจากอุปกรณ์ ติดตั้งโปรแกรมใหม่ ปรับปรุงทะเบียนอุปกรณ์ให้ถูกต้องและเป็นปัจจุบัน - การปฏิบัติเมื่อโอนย้าย ลาออกสายเทคโนโลยีสารสนเทศจะได้รับแจ้งจากสายบริหารทรัพยากรบุคคล เพื่อปฏิบัติงานถอดถอนสิทธิของผู้ใช้งานที่มีการใช้อุปกรณ์ฯ เพื่อเชื่อมต่อหรือใช้งานระบบของธนาคาร ทั้งนี้สายเทคโนโลยีสารสนเทศจะนำข้อมูลที่ได้รับมาตรวจสอบกับทะเบียนอุปกรณ์ฯ
	☑ Detective Control	รายงานการทบทวนบัญชีผู้ใช้งานที่ได้รับสิทธิใช้งานอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงาน	ธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
		จากภายนอกองค์กร ภาคผนวก ง 1.7.1 (1)	1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ
	☑ Corrective Control	เอกสารหน้าจอ Firewall Setup อุปกรณ์มือถือของผู้บริหาร Nokia ผ่าน Firewall	ธนาคารมีการกำหนด Firewall ในการตรวจสอบอุปกรณ์เคลื่อนที่พกพา (Mobile) ที่ได้รับอนุญาตเท่านั้นที่เข้าถึงระบบงานธนาคารได้ตลอดจนหากมีการเปลี่ยนแปลงใด ๆ กับค่าอุปกรณ์ต้องมีการกำหนดเปลี่ยนแปลง เช่น IMEI มือถือผ่านการร้องขอ IT Request
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ***<u>ใช่หรือไม่อย่างไร</u>***	☑ Preventive Control	นโยบาย เทคโนโลยีสารสนเทศของกลุ่มธุรกิจทางการเงิน(2012) ข้อ 2.7.7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile computing and teleworking)	ธนาคารมีนโยบายฯ การปฏิบัติงานภายนอกสำนักงาน (Teleworking) คือ การปฏิบัติงานโดยเชื่อมต่อระบบเครือข่ายจากสถานที่ภายนอกกลุ่มธุรกิจทางการเงิน เข้าสู่ระบบเครือข่ายภายในกลุ่มธุรกิจทางการเงินโดยทั่วไปแล้วจะทำผ่านอินเทอร์เน็ต โดยมีการใช้งานการเชื่อมต่อที่มีความมั่นคงปลอดภัย เช่น เครือข่ายเสมือนส่วนตัว (VPN)
	☑ Detective Control	รายงานการทบทวนบัญชีผู้ใช้งานที่ได้รับสิทธิใช้งานอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงาน	ธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำ

ตารางที่ 7.1.1 (ต่อ)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
		จากภายนอกองค์กร ภาคผนวก ง 1.7.2 (1)	อย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก
	☑ Corrective Control	อ้างอิงเอกสารหน้าจอระบบงาน IT Request การร้องขอสิทธิเพื่อการขอปฏิบัติงานจากภานอกสำนักงาน	ธนาคารมีการกำหนดการขอร้องขอการขอปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยการขอผ่านระบบงาน IT Request เพื่อให้หัวหน้างานทำการอนุมัติ ก่อนการใช้งาน Lotus note บน Mobile เพื่อควบคุมสิทธิการร้องขอเข้าใจ เปลี่ยนแปลงแก้ไขข้อมูลใด ๆ ที่ไม่เหมาะสม
ความเห็นเพิ่มเติม			
.....			
ขอรับรองว่าข้อมูลที่ได้ให้ไว้ในแบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายใน โดยการประเมินตนเอง (Control Self Assessment: CSA) ถูกต้องตรงกับการปฏิบัติงานจริงทุกประการ			

7.1.2 การประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

จากการทดสอบแบบจำลองการความคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) ผู้ศึกษาโครงการพบว่า การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่องค์กร (ธนาคาร) มีการจัดการเพิ่มเติมขึ้น ส่งผลให้การควบคุมภายในมีความมั่นคงปลอดภัย และเป็นลายลักษณ์อักษรแสดงถึงการกำหนดแนวทางการปฏิบัติงานด้านการบริหารจัดการเพื่อการเข้าถึงระบบสารสนเทศที่มากขึ้น และมีความเหมาะสม อยู่ในระดับที่องค์กรยอมรับได้ตาม (Risk base Approach) โดยทำการ Plot คำชี้แจงและหลักฐานการจัดการตามคำชี้แจงจากประเมินตนเอง (Control Self Assessment : CSA) เฉพาะในขอบเขตที่การควบคุมภายในยังไม่เพียงพอ และผู้ดูแลระบบงานมีการปรับปรุง เพิ่มเติมการควบคุมภายในและมีการตอบคำชี้แจงกลับมายังผู้ศึกษาโครงการ โดยขั้นตอนในการพิจารณาหลักฐาน คำชี้แจง ตลอดจนเทคนิคในการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อยืนยันผลการดำเนินการที่มีการปรับปรุงการควบคุมภายในให้มีความเหมาะสมมากขึ้น ผู้ศึกษาโครงการยังคงใช้เทคนิคที่ได้กล่าวมาแล้วในข้อ 6.1.2 การใช้เทคนิคในการใช้ดุลพินิจประกอบเพื่อพิจารณา ซึ่งจากรายละเอียดดังที่กล่าวมาแล้วนั้นทำให้ผู้ศึกษาโครงการสามารถจำมาใช้ในการเป็นข้อมูลนำเข้า (Input) เพื่อประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้ (หลังทำโครงการ) ได้ดังต่อไปนี้

ตารางที่ 7.1.2.1 แบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)		**เพื่อควบคุมการเข้าถึงสารสนเทศ**				**100.00**
1.1.1	นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ	Yes	Yes	Yes	
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)		**เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต**				**100.00**
1.2.1	การลงทะเบียนพนักงาน (User registration)	ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น	Yes	Yes	Yes	

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.2.2	การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน	Yes	Yes	Yes	
1.2.3	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย	Yes	Yes	Yes	
1.2.4	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้	Yes	Yes	Yes	
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		**เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ**				**100.00**
1.3.1	การใช้งานรหัสผ่าน (Password use)	ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน	Yes	Yes	Yes	
1.3.2	การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)	ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล	Yes	Yes	Yes	

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective Access Control	Questions	Compliance			Percentage
			Preventive Control	Detective Control	Corrective Control	
1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)		**เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต**				**90.48**
1.4.1	นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้	Yes	No	Yes	
1.4.2	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	Yes	Yes	Yes	
1.4.3	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ซึ่งได้รับอนุญาตแล้ว	Yes	Yes	Yes	
1.4.4	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย	Yes	Yes	Yes	

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.4.5	การแบ่งแยกเครือข่าย (Segregation in networks)	ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ	Yes	Yes	Yes	
1.4.6	การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้	Yes	Yes	Yes	
1.4.7	การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง	No	Yes	Yes	
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)		**เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต**				**94.44**
1.5.1	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ	Yes	Yes	Yes	

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.5.2	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ	Yes	Yes	Yes	
1.5.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ	Yes	Yes	Yes	
1.5.4	การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว	Yes	Yes	Yes	
1.5.5	การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้	Yes	Yes	Yes	
1.5.6	การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง	No	Yes	Yes	

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)		**เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต**				**100.00**
1.6.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน	Yes	Yes	Yes	
1.6.2	การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ	Yes	Yes	Yes	
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)		**เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**				**100.00**

ตารางที่ 7.1.2.1 (ต่อ)

หัวข้อ	Control Objective	Questions	Compliance			Percentage
	Access Control		Preventive Control	Detective Control	Corrective Control	
1.7.1	การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้	Yes	Yes	Yes	
1.7.2	การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติบุคลากรที่จำเป็นต้องปฏิบัติงานจากภายนอกสำนักงาน	Yes	Yes	Yes	

ซึ่งจากการประเมินผลการควบคุมภายในด้านเทคโนโลยีสาสนเทศ (หลังทำโครงการ) จะทำให้ผู้ปฏิบัติงาน ผู้บริหารสายงานเทคโนโลยีสารสนเทศทราบว่า ระบบงานเทคโนโลยีสารสนเทศของธนาคารที่มีการเพิ่มเติม ปรับปรุง การบริหารจัดการการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศในระดับต่าง ๆ มีความเพียงพอที่องค์กรสามารถยอมรับได้อย่างเหมาะสม สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) สามารถสรุปได้ดังตาราง

ตารางที่ 7.1.2.2 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

A.1	Access Control (ก่อนดำเนินโครงการ)	Indicator Organize	Overall Score	Overall Rating
			97.85	Good
A.1.1	Business Requirement for Access Control	85.39	100.00	Excellent
A.1.2	User Access Management	85.39	100.00	Excellent
A.1.3	User Responsibilities	85.39	100.00	Excellent
A.1.4	Network Access Control	85.39	90.48	Marginal
A.1.5	Operating System Access Control	85.39	94.44	Good
A.1.6	Application and Information Access Control	85.39	100.00	Excellent
A.1.7	Mobile Computing and Teleworking	85.39	100.00	Excellent

โดยผู้ศึกษาโครงการได้ทำการสรุปผลแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) และนำมาจัดทำเป็นแผนภูมิภาพให้เห็นถึงข้อมูลการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน (ISO/IEC 27001) และระดับที่องค์กรยอมรับได้ (หลังทำโครงการ) พบว่า จากแผนภูมิภาพแสดงให้เห็นถึงตามแนวปฏิบัติที่องค์การมีการปฏิบัติงานที่ธนาคาร(โดยสายเทคโนโลยีสารสนเทศ) ได้พัฒนาและปรับปรุงประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศของธนาคารให้มีความมั่นคงปลอดภัยอย่างเหมาะสมนั้นสามารถแบ่งเป็น 2 รูปแบบที่เป็นการดำเนินการที่ดีเป็นไปตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ในเฉพาะขอบเขตเรื่องการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) ดังนี้

1) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับดีมาก (Excellent) โดยประกอบด้วยการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่มีการบริหารจัดการที่มั่นคงปลอดภัยจากการเข้าถึงเดิมอยู่แล้ว และการพัฒนาปรับปรุงการควบคุมภายในด้านการเข้าถึงระบบเทคโนโลยีสารสนทเศของธนาคารให้มีความเหมาะสมมากยิ่งขึ้น อันได้แก่

- ✓ การจัดการด้านข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)
- ✓ การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)
- ✓ การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)
- ✓ การจัดการที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)
- ✓ การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

ซึ่งมีลักษณะเป็นการที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ดำเนินการเพิ่มเติม ปรับปรุงกระบวนการของการควบคุมภายในด้านเทคโนโลยีสารสนเทศเพื่อการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เช่น การทำการเพิ่มกระบวนการในการเบิกใช้และทบทวนการใช้งาน Privilege User อย่างเหมาะสม เป็นต้น

2) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับดี (Good) โดยประกอบด้วยการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่มีการบริหารจัดการที่มั่นคงปลอดภัยจากการเข้าถึงเดิมอยู่แล้ว และการพัฒนาปรับปรุงการควบคุมภายในด้านการเข้าถึงระบบเทคโนโลยีสารสนทเศของธนาคารให้มีความเหมาะสมอยู่ในระดับที่องค์กรยอมรับได้ ทำให้โดยภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยอยู่ในระดับของการบริหารจัดการที่ดี อันได้แก่

- ❖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

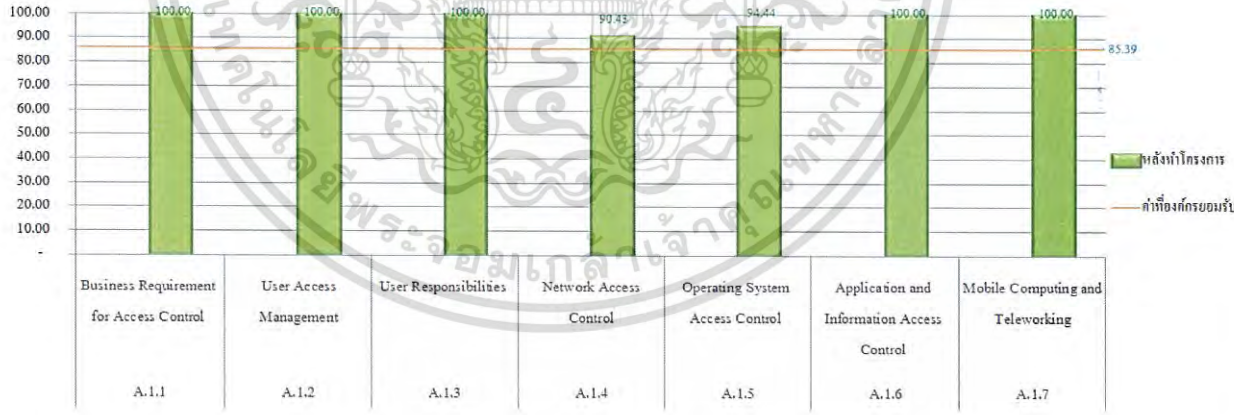
ซึ่งมีลักษณะเป็นการที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ดำเนินการเพิ่มเติม ปรับปรุงกระบวนการบางประการของการควบคุมภายในด้านเทคโนโลยีสารสนเทศเพื่อการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร เช่น การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารอยู่ระหว่างการเก็บรวบรวมข้อมูล และทบทวนการกำหนดระยะเวลาให้เหมาะสมสำหรับการเชื่อมต่อระบบธนาคารให้ถูกต้องเหมาะสมกับความมั่นคงปลอดภัย โดยปัจจุบันได้ทำการกำหนดที่ 30 นาที เป็นต้น

3) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับพอใช้ (Marginal) ประกอบด้วย

- การควบคุมการเข้าถึงเครือข่าย (Network access control)

ซึ่งมีลักษณะเป็นการที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ดำเนินการเพิ่มเติม ปรับปรุงกระบวนการบางประการของการควบคุมภายในด้านเทคโนโลยีสารสนเทศเพื่อการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร เช่น การมีแนวนโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารมีการกำหนดให้ปฏิบัติงานชั่วคราว ระหว่างการเก็บรวบรวมข้อมูล และทบทวนนโยบายฉบับปี 2557 ให้มีเนื้องหาครอบคลุมเพื่อให้ผู้ปฏิบัติงานสามารถดำเนินการได้อย่างถูกต้องเหมาะสมกับความมั่นคงปลอดภัย

จากการที่มีการบริหารจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารดังที่กล่าวมาข้างต้น ผู้ศึกษาโครงการสามารถแสดงให้เห็นถึงแผนภูมิภาพรายละเอียดการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งมีการควบคุมภายในที่เพิ่มมากขึ้น ส่งผลทำให้ภาพรวมของการบริหารจัดการในการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารเพิ่มมากขึ้นด้วย จนมีค่ามากกว่าระดับที่องค์กรคาดหวังหรือยอมรับได้ ดังต่อไปนี้



รูปที่ 7.1.2 แผนภูมิแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

7.2 การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

จากการประเมินผลแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) ตามมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) เฉพาะในขอบเขตที่พิจารณาศึกษาด้านการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) แล้วนั้น พบว่า สายเทคโนโลยีสารสนเทศ ซึ่งเป็นผู้ดูแลระบบงานมีการเพิ่มเติม ปรับปรุงบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศให้อยู่ในระดับที่องค์กรยอมรับได้ และเป็นไปตามมาตรฐานที่ดี ซึ่งสามารถนำมาประเมินความเสี่ยงการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ดี นำไปสู่การลดระดับความเสี่ยงของธนาคารที่กำหนดไว้ได้จึงนำมาสู่การประเมินความเสี่ยงจากแบบจำลองที่จัดสร้างเพื่อให้เห็นภาพว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งสอดคล้องกับความเสี่ยงขององค์กรมีการตอบสนองเพื่อลดความเสี่ยงลงมาอย่างเหมาะสมเรียบร้อยแล้ว ดังนี้

1) ผู้ศึกษาโครงการ นำหัวข้อเรื่องจากการประเมินการควบคุมภายในด้านระบบเทคโนโลยีสารสนเทศที่พบว่า ยังไม่มีการควบคุมภายในอย่างเหมาะสม และได้มีการเพิ่มเติม ปรับปรุงการดำเนินการบางประการไปแล้วนั้น ทำให้การควบคุมภายในมีแนวทางการบริหารจัดการอยู่ในระดับที่องค์กรยอมรับได้ โดยผู้ศึกษาโครงการต้องนำรายละเอียดในหัวข้อที่มีการเพิ่มเติม หรือปรับปรุง มาประเมินว่ามีความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งสอดคล้องกับความเสี่ยงขององค์กรที่มีการปรับลดความเสี่ยงในประเภทใด โดยมีรายละเอียดของความเสี่ยง ดังต่อไปนี้

ตารางที่ 7.2.1 การกำหนดประเภทความเสี่ยงในแบบจำลอง (หลังทำโครงการ)

Risks		
#	Risk Category	Risk Description
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มีการเบิกใช้บัญชีผู้ใช้งานสิทธิเฉพาะ (Privilege User) ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาซองรหัสผ่าน

ตารางที่ 7.2.1 (ต่อ)

#	Risk Category	Risk Description
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุงกระบวนการ (Detective Control) โดยกำหนดให้ระบบงานเงินฝากสามารถให้ผู้ใช้งานดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet เป็นต้น (ตามเอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงที่ไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบหลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนดอย่างยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด

ตารางที่ 7.2.1 (ต่อ)

#	Risk Category	Risk Description
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคารให้มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆของธนาคารได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ ควบคุมการปฏิบัติงานอย่างเหมาะสม
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงาน IT ที่ทำหน้าที่กำกับ (Detective Control)
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)

RRAM - RISK OVERVIEW

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control (หลังทำโครงการ)

วันที่ประเมิน : 07-12-2013

Risks

#	Risk Category	Risk Description
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มี การเบิกใช้ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง (Privilege User) ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาซองรหัสผ่าน
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุง (Detective Control) การดำเนินการกำหนดให้ระบบงานเงินฝาก (Flexcute) ให้ผู้ใช้งานสามารถดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet, (เอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)
4	Operational Risk	1.4.4 การป้องกันพอร์ทที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ทที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงและยังคงไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ) ยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิ์ผู้ใช้งานการเข้าถึงระบบปฏิบัติงาน (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคาร มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆของธนาคารได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control เช่น Core Bank ลำดับแรก) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)

รูปที่ 7.2.1 แสดงการระบุประเภทความเสี่ยงในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)

2) ผู้ศึกษาโครงการทำการประเมิน Likelihood ซึ่งเป็นโอกาสหรือความถี่ของการเกิดเหตุการณ์ เพื่อประเมินสถานการณ์ของโอกาสเกิดขึ้น (หลังทำโครงการ) ที่มีการเพิ่มเติม ปรับปรุงขั้นตอนการปฏิบัติงานให้มีการควบคุมภายในการเข้าถึงระบบสารสนเทศของธนาคารที่มากขึ้น โดยผู้ศึกษาโครงการใช้การประมาณการของโอกาสที่อาจจะเกิดขึ้นเมื่อมีการควบคุมภายในด้านเทคโนโลยีสารสนเทศแล้วให้ได้มากที่สุด (จำนวนเท่าไรต่อปีที่สามารถมีโอกาสเกิดเหตุการณ์ได้)

ซึ่งจากการประเมินการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงขององค์กร (หลังทำโครงการ) หากผู้ศึกษาโครงการร่วมประเมินความเสี่ยงกับผู้เชี่ยวชาญด้านการควบคุมภายในท่านอื่น มีความคิดเห็นในการประเมินความเสี่ยงในส่วนโอกาสหรือความถี่ของการเกิดเหตุการณ์ที่ยังคงคิดเห็นแตกต่างกัน ก็คงยังสามารถทำการประเมินความเสี่ยงได้โดยระบุในช่องความเห็นในแต่ละ Paticipant โดยแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศจะทำการเฉลี่ยความเสี่ยงตามความคิดเห็นของผู้ร่วมศึกษาโครงการ ดังนี้

ตารางที่ 7.2.2 การประเมินโอกาสหรือความถี่ของการเกิดเหตุการณ์ (หลังทำโครงการ)

LIKELIHOOD						
#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มีการเบิกใช้บัญชีผู้ใช้งานสิทธิเฉพาะ (Privilege User) ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาซองรหัสผ่าน	Yes	3		**3.00**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุงกระบวนการ (Detective Control) โดยกำหนดให้ระบบงานเงินฝากสามารถให้ผู้ใช้งานดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)	Yes	2		**2.00**
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet เป็นต้น (ตามเอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	Yes	5		**5.0**

ตารางที่ 7.2.2 (ต่อ)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงที่ไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	Yes	2		**2.00**
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนดอย่างยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด	Yes	5		**5.00**
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคารให้มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	Yes	2		**2.00**

ตารางที่ 7.2.2 (ต่อ)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	ค่าเฉลี่ยความเสี่ยง
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)	Yes	5		**5.0**
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง ต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)	Yes	2	2	**2.00**
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	Yes	2		**2.00**

RRAM - RISK ASSESSMENT (LIKELIHOOD)

ชื่อการตรวจสอบ : *ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control (หลังทำโครงการ)*

วันที่ประเมิน : *07-12-2013*

LIKELIHOOD (score 1-5)

#	Risk Category	Risk Description	Plot	Participant 1	Participant 2	AVRG
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มี การเปิดใช้ใส่ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง (Privilege User) ทุกครั้งที่มีการเปิดใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเปิดใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาของรหัสผ่าน	Yes	3		3.0
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุง (Detective Control) การดำเนินการกำหนดให้ระบบงานเงินฝาก (Flexcute) ให้ผู้ใช้งานสามารถดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)	Yes	2		2.0
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินการทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet, (เอกสาร E-mail การกำกับแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	Yes	5		5.0
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงและยังคงไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP, TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	Yes	2		2.0
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นกฎมือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ) ยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด	Yes	5		5.0
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคาร มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆของธนาคารได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	Yes	2		2.0
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control เช่น Core Bank ลำดับแรก) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)	Yes	5		5.0
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์คือสารประเภทคอมพิวเตอร์ (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)	Yes	2	2	2.0
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	Yes	2		2.0

รูปที่ 7.2.2 การประเมินโอกาสของการเกิดเหตุการณ์ในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)

3) ผู้ศึกษาโครงการทำการประเมิน Impact ซึ่งเป็นผลกระทบหรือความเสียหายของการเกิดเหตุการณ์เพื่อประเมินสถานการณ์ความเสียหายที่มากที่สุดที่อาจเกิดขึ้นได้ ทั้งในด้านความเสียหายที่เป็นตัวเงิน ผลกระทบที่ไม่เป็นตัวเงิน เช่น ด้านกฎหมาย กฎระเบียบ ด้านชื่อเสียง หรือลูกค้า โดยการใช้การประมาณการของความเสียหายที่มากที่สุด (จำนวนเท่าไรต่อการเกิดเหตุการณ์ขึ้น)

ซึ่งจากการประเมินการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงขององค์กร (หลังทำโครงการ) หากผู้ศึกษาโครงการร่วมประเมินความเสี่ยงกับผู้เชี่ยวชาญด้านการควบคุมภายในท่านอื่น มีความคิดเห็นในการประเมินความเสี่ยงของผลกระทบหรือเสียหายการเกิดเหตุการณ์ที่ยังคงคิดเห็นแตกต่างกัน ก็คงยังสามารถทำการประเมินความเสี่ยงได้โดยระบุในช่องความเห็นในแต่ละ Paticipant โดยแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศจะทำการเฉลี่ยความเสี่ยงตามความคิดเห็นของผู้ร่วมศึกษาโครงการ ดังนี้

ตารางที่ 7.2.3 การประเมินผลกระทบหรือความเสียหายของการเกิดเหตุการณ์ (หลังทำโครงการ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มีการเบิกใช้บัญชีผู้ใช้งานสิทธิเฉพาะ (Privilege User) ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาซองรหัสผ่าน	Yes	6	2	5	8					**5.25**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุงกระบวนการ (Detective Control) โดยกำหนดให้ระบบงานเงินฝากสามารถให้ผู้ใช้งานดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)	Yes	6	2	1	5					**3.50**

ตารางที่ 7.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet เป็นต้น (ตามเอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	Yes	1	2	1	2					**1.50**
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงที่ไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	Yes	6	3	5	8					**5.50**

ตารางที่ 7.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่กำหนดอย่างยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด	Yes	1	2	2	5					**2.50**
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคารให้มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	Yes	1	1	1	3					**1.5**

ตารางที่ 7.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบหลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)	Yes	1	2	1	3					**1.75**
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง ต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่กำกับ (Detective Control)	Yes	6	2	3	8	6	2	5	8	**5.00**

ตารางที่ 7.2.3 (ต่อ)

IMPACT				Participant1				Participant2				ค่าเฉลี่ยความเสี่ยง
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	Yes	6	2	3	5					**4.00**

RRAM - RISK ASSESSMENT (IMPACT)

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ขอบเขต Access Control (หลังทำโครงการ)

วันที่ประเมิน : 07-12-2013

IMPACT (score 1-11)				Participant1				Participant2				
#	Risk Category	Risk Description	Plot	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	ด้านการเงิน	ด้านกฎระเบียบ	ด้านชื่อเสียง	ด้านลูกค้า	AVRG
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารกำหนดการปรับปรุงกระบวนการ (Detective Control) ให้มี การเปิดใช้ได้ไม่เกิน 60 วันทำการ และต้องมีการลอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง (Privilege User) ทุกครั้งที่มีการเปิดใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเปิดใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาของรหัสผ่าน	Yes	6	2	5	8					5.25
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุง (Detective Control) การดำเนินการกำหนดให้ระบบงานเงินฝาก (Flexcute) ให้ผู้ใช้งานสามารถดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)	Yes	6	2	1	5					3.50
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet, เอกสาร E-mail การกำกับเน้นแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	Yes	1	2	1	2					1.50
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงและยังคงไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	Yes	6	3	5	8					5.50
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นผู้ปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ) ยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเส้นทางทั้งหมด	Yes	1	2	2	5					2.50
6	Operational Risk	1.5.4 การใช้งาน โปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงาน (OS) ที่มีการใช้งานกับอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคาร มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆของธนาคารได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	Yes	1	1	1	3					1.50
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน ในปัจจุบันในระดับ OS บางระบบงาน (Preventive Control เช่น Core Bank กำหนดแรก) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)	Yes	1	2	1	3					1.75
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)	Yes	6	2	3	5	6	2	5	8	5.00
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	Yes	6	2	3	5					4.00

รูปที่ 7.2.3 การประเมินผลกระทบของเหตุการณ์ที่เกิดในแบบจำลองที่จัดสร้าง (หลังทำโครงการ)

4) ผู้ศึกษาโครงการได้นำผลลัพธ์ของการแสดงแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ มาจากการมูลค่าความเสียหายที่อาจจะเกิดขึ้นได้หลังทำโครงการ (Risk Value) ซึ่งเกิดขึ้นได้จากการที่โอกาสหรือความถี่ของการเกิดเหตุการณ์ขึ้น คูณผลกระทบหรือความเสียหายที่เกิดขึ้น ซึ่งจะเห็นได้ว่า หากผู้บริหาร และผู้ปฏิบัติงานมีการนำแนวทางการรักษาความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศให้เหมาะสมสอดคล้องกับมาตรฐาน ISO/IEC 27001 เมื่อดำเนินการแล้วมาประเมินความเสี่ยงอีกครั้ง พบว่า ความเสี่ยงด้านเทคโนโลยีสารสนเทศหลังทำโครงการจะลดลงกว่าก่อนทำโครงการ โดยสามารถคิดคำนวณได้ดังนี้

ตารางที่ 7.2.4 การคำนวณมูลค่าความเสียหายที่อาจเกิดขึ้น (หลังทำโครงการ)

Risk Value (Likelihood X Impact)					
#	**Risk Category**	**Risk Description**	**Likelihood**	**Impact**	**Risk Value**
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มีการเบิกใช้บัญชีผู้ใช้งานสิทธิเฉพาะ (Privilege User) ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลซองรหัสผ่าน	3.00	5.25	**15.75**
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุงกระบวนการ (Detective Control) โดยกำหนดให้ระบบงานเงินฝากสามารถให้ผู้ใช้งานดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วัน อย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งผ่านมา)	2.00	3.50	**7.00**

ตารางที่ 7.2.4 (ต่อ)

#	Risk Category	Risk Description	Likeli hood	Impact	Risk Value
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet เป็นต้น (ตามเอกสาร E-mail การกำกับแนวแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	5.00	1.50	**7.50**
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงที่ไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	2.00	5.50	**11.00**
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบหลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยัง	5.00	2.50	**12.50**

ตารางที่ 7.2.4 (ต่อ)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
		ไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนดอย่างยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด			
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงการ (OS) ที่มีการใช้งานผ่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคารให้มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขออนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	2.00	1.50	**3.00**
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวมข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด	5.00	1.75	**8.75**
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1	2.00	5.00	**10.00**

ตารางที่ 7.2.4 (ต่อ)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
		ครั้ง ต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)			
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารผ่านทางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	2.00	4.00	**8.00**

RRAM - RISK ASSESSMENT (RISK VALUE)

ชื่อการตรวจสอบ : ระบบธุรกรรมอิเล็กทรอนิกส์ (ธนาคารพาณิชย์) ตามมาตรฐาน (ISO/IEC 27001) ของเขต Access Control (หลังทำโครงการ)

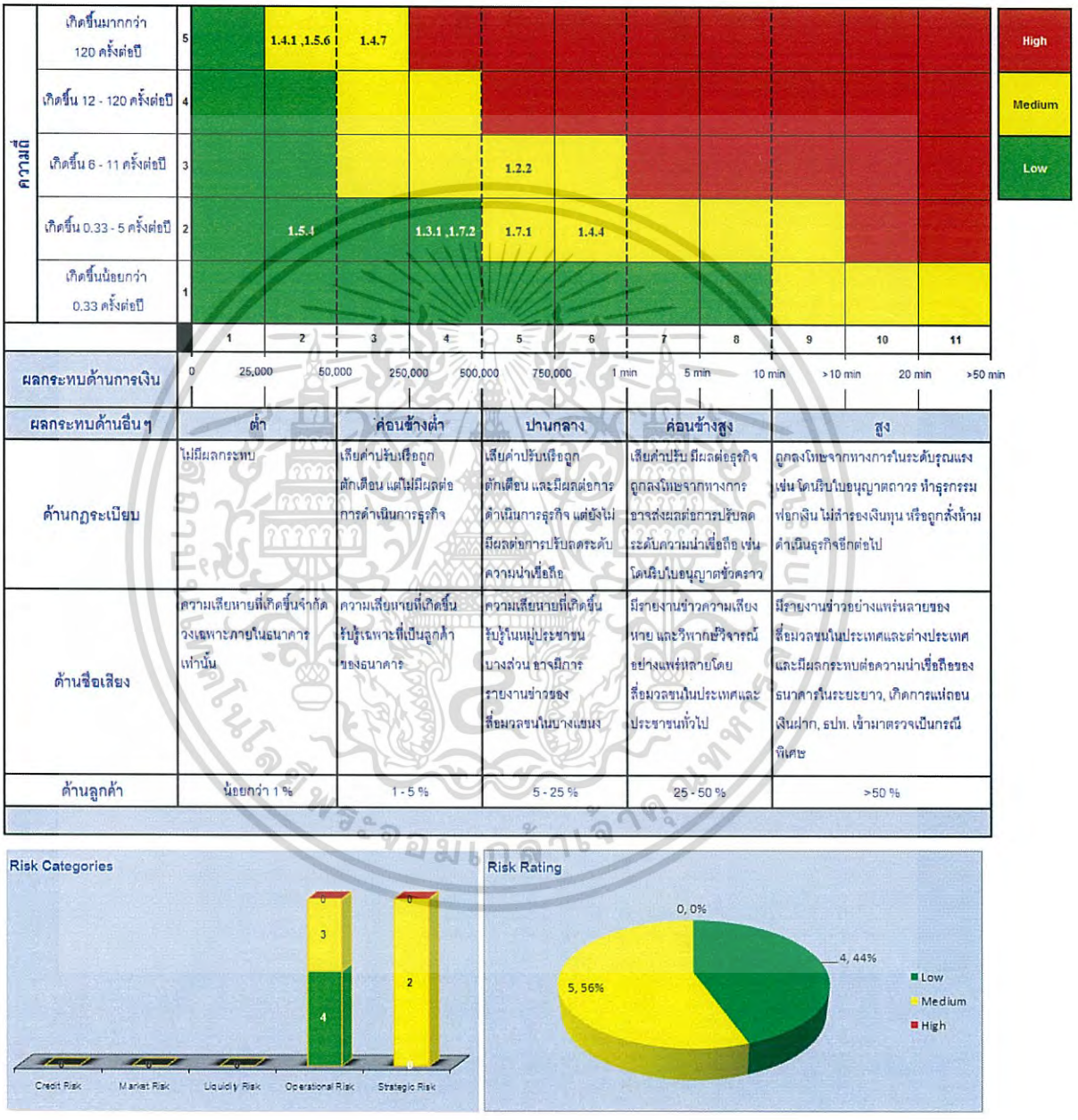
วันที่ประเมิน : 07-12-2013

Risk Value (Likelihood X Impact)

#	Risk Category	Risk Description	Likelihood	Impact	Risk Value
1	Operational Risk	1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ปัจจุบันธนาคารดำเนินการปรับปรุงกระบวนการ (Detective Control) ให้มีการเบิกใช้ได้ไม่เกิน 60 วันทำการ และต้องมีการสอบทาน Log การใช้งานรหัสผ่านของผู้มีสิทธิสูง (Privilege User) ทุกครั้งที่มีการเบิกใช้งาน โดยทันทีที่ส่งคืน โดยกำหนดให้มีการระบุในเอกสารการขอเบิกใช้งานรหัสผ่าน และส่งมอบคืนผู้ดูแลรักษาของรหัสผ่าน	3.00	5.25	15.75
2	Operational Risk	1.3.1 การใช้งานรหัสผ่าน (Password use) ปัจจุบันธนาคารมีการเพิ่มเติม ปรับปรุง (Detective Control) การดำเนินการกำหนดให้ระบบงานเงินฝาก (Flexcute) ให้ผู้ใช้งานสามารถดำเนินการเปลี่ยนรหัสผ่านเป็นของตนเองได้ตั้งแต่ครั้งแรกที่มีการ Log in เพื่อการใช้งาน โดยต้องมีความมั่นคงปลอดภัยอย่างเพียงพอ และอยู่ภายใต้นโยบายเทคโนโลยีสารสนเทศในการให้เปลี่ยนรหัสผ่านทุก 90 วันอย่างเหมาะสม (ห้ามใช้รหัสผ่านซ้ำ 4 ครั้งที่ผ่านมา)	2.00	3.50	7.00
3	Operational Risk	1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารอยู่ระหว่างการดำเนินทบทวนนโยบายด้านเทคโนโลยีสารสนเทศประจำปี 2557 (Detective Control) ซึ่งจะดำเนินการให้สอดคล้องกับนโยบายการใช้งานบริการเครือข่าย (Policy of Network Service) โดยระหว่างการดำเนินการกำหนดให้ผู้ปฏิบัติงานดำเนินการปิดบริการเครือข่ายที่สามารถเข้าถึงภายนอกที่ไม่มั่นคงปลอดภัย เช่น FTP, Telnet, (เอกสาร E-mail การกำกับแนวทางการปฏิบัติงานให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)	5.00	1.50	7.50
4	Operational Risk	1.4.4 การป้องกันพอร์ตที่ใช้สำหรับการวินิจฉัยและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ปัจจุบันธนาคารได้ทำการกำหนดพอร์ตที่ใช้งานเพื่อเป็นการป้องกันการเข้าถึงผ่านระบบเครือข่ายที่มีความเสี่ยงและยังคงไม่มั่นคงปลอดภัย (Detective Control) เช่น FTP , TFTP, Telnet โดยเปิดให้ผู้ดูแลระบบงานเปิดให้เข้าถึงระบบเครือข่ายได้เฉพาะการ Log in	2.00	5.50	11.00
5	Strategic Risk	1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวน นโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบด้วน (Preventive Control) โดยปัจจุบันมีการกำหนดเป็นผู้มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ) ยังไม่ครบด้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด	5.00	2.50	12.50
6	Operational Risk	1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ปัจจุบันธนาคารทำการกำหนดให้สิทธิผู้ใช้งานการเข้าถึงระบบปฏิบัติงาน (OS) ที่มีการใช้งานด่านอุปกรณ์เครื่องคอมพิวเตอร์ของธนาคาร มีสิทธิเป็น User ซึ่งไม่สามารถทำการติดตั้งโปรแกรมประเภทยูทิลิตี้ใดๆของธนาคารได้ (Detective Control) หากจำเป็นต้องติดตั้งต้องมีการร้องขอ อนุมัติ และควบคุมการปฏิบัติงานอย่างเหมาะสม	2.00	1.50	3.00
7	Strategic Risk	1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ปัจจุบันธนาคารอยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศที่เหมาะสม เพื่อใช้ในการทบทวน นโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบด้วน โดยปัจจุบันในระดับ OS บางระบบงาน (Preventive Control เช่น Core Bank กำหนดแรก) มีการกำหนดให้เชื่อมต่อ 30 นาทีเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ)	5.00	1.75	8.75
8	Operational Risk	1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารเฉพาะผู้บริหาร หรือผู้ที่ได้รับอนุมัติ โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ (Detective Control)	2.00	5.00	10.00
9	Operational Risk	1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ปัจจุบันธนาคารได้กำหนดการให้สิทธิและตรวจสอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารที่นางการปฏิบัติงานภายนอกสำนักงาน (Teleworking) โดยกำหนดการทบทวนสิทธิเป็นประจำอย่างน้อยไตรมาสละ 1 ครั้ง โดยต้องมีการลงนามเป็นลายลักษณ์อักษรจากผู้บริหารสายงานเทคโนโลยีที่ทำหน้าที่กำกับ ซึ่งเนื้อหาในการทบทวน Log เพื่อสอบทานเวลาการเข้าถึงที่ผิดปกติ เช่น ยามวิกาล การโอนเงินข้ามบัญชีจำนวนมาก (Detective Control)	2.00	4.00	8.00

รูปที่ 7.2.4.1 การคำนวณมูลค่าความเสียหาย (Risk Value) หลังทำโครงการ

ซึ่งจากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโครงการแล้วนั้น ผู้ศึกษาโครงการสามารถแสดงเป็นแผนภาพแบบจำลองความเสี่ยงที่แสดงให้เห็นระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความเสี่ยงขององค์กร (หลังทำโครงการ) ได้ดังแผนภาพ Risk Rating Matrix ดังต่อไปนี้



รูปที่ 7.2.4.2 ผลลัพธ์จากแบบจำลองความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ)

บทที่ 8
สรุปผลการดำเนินโครงการ

จากการศึกษาการสร้างแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ ทำให้ผู้ปฏิบัติงาน (สายเทคโนโลยีสารสนเทศ) ได้ทราบถึงแนวทางการดำเนินการที่ได้ปฏิบัติงานอยู่ในปัจจุบันว่าสอดคล้องกับมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) มากน้อยอย่างไรในลักษณะรูปแบบการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ที่แสดงผลในลักษณะเชิงปริมาณ มากกว่าการใช้ดุลพิจนิจการดำเนินการ

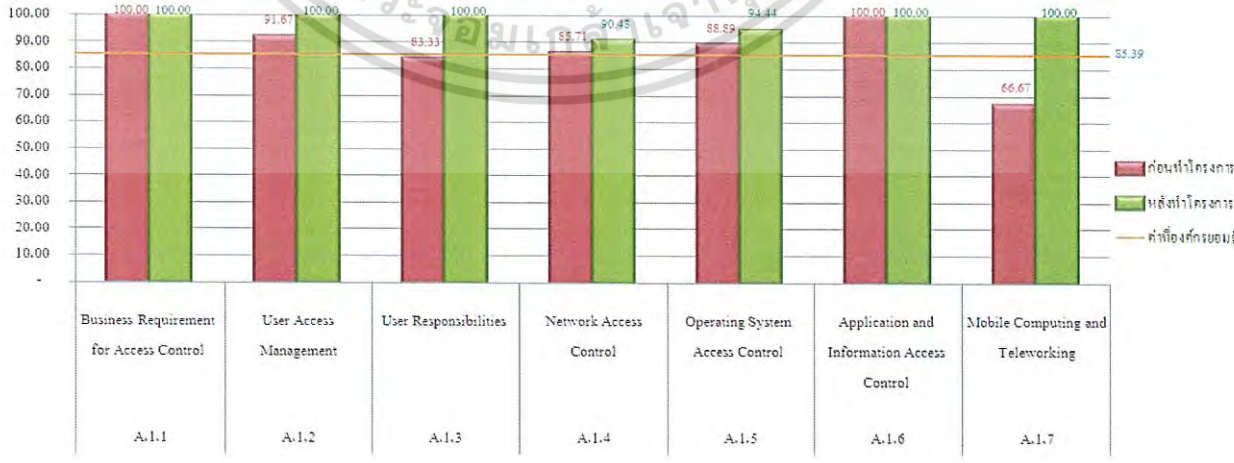
8.1 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนและหลังทำโครงการ)

จากการดำเนินการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ในขอบเขตของการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) โดยผู้ศึกษาโครงการนำแบบจำลองการควบคุมภายในด้านเทคโนโลยีสารสนเทศมาใช้ประเมินการบริหารจัดการที่ปัจจุบันธนาคารพาณิชย์มีการดำเนินอยู่ (ก่อนทำโครงการ) ทำให้เห็นถึงภาพรวมว่า การจัดการความมั่นคงปลอดภัยด้านการเข้าถึงระบบสารสนเทศของธนาคารยังคงมีการควบคุมภายในที่ไม่เพียงพอ ส่งผลต่อความสอดคล้องกับมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001)ที่ดีซึ่งองค์กรควรมีการกำหนดไว้ ซึ่งผู้ศึกษาโครงการได้ให้คำแนะนำในเบื้องต้นในการเป็นแนวปฏิบัติเพื่อการควบคุมภายในที่ดี โดยหลังจากที่องค์กรรับทราบ และตระหนักถึงการควบคุมภายในที่มีจุดอ่อนที่สำคัญในบางประการแล้วนั้น ก็ได้นำไปเพิ่มเติม ปรับปรุงแนวทางการควบคุม (Contorl) อย่างเหมาะสมส่งผลต่อระดับการควบคุมภายในที่มีประสิทธิภาพมากยิ่งขึ้น จนทำให้ภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยการเข้าถึงระบบสารสนเทศของธนาคาร (หลังทำโครงการ) มีการบริหารจัดการที่อยู่ในระดับที่องค์กรยอมรับได้ และเป็นไปตามมาตรฐาน (ISO/IEC 27001) อย่างเหมาะสม ซึ่งสามารถชี้วัดได้ ดังนี้

ตารางที่ 8.1.1 สรุปผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากแบบจำลอง

A.1	Access Control	Indicator Organize	ก่อนทำโครงการ		หลังทำโครงการ	
			Overall Score	Overall Rating	Overall Score	Overall Rating
			88.04	Marginal	97.85	Good
A.1.1	Business Requirement for Access Control	85.39	100.00	Excellent	100.00	Excellent
A.1.2	User Access Management	85.39	91.67	Marginal	100.00	Excellent
A.1.3	User Responsibilities	85.39	83.33	Poor	100.00	Excellent
A.1.4	Network Access Control	85.39	85.71	Marginal	90.48	Marginal
A.1.5	Operating System Access Control	85.39	88.89	Marginal	94.44	Good
A.1.6	Application and Information Access Control	85.39	100.00	Excellent	100.00	Excellent
A.1.7	Mobile Computing and Teleworking	85.39	66.67	At Risk	100.00	Excellent

ซึ่งเมื่อผู้ศึกษาโครงการทำการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศก่อนและหลังทำโครงการแล้วนั้น สามารถนำมาแสดงได้เป็นแผนภูมิภาพการประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ตามมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001) ได้ดังภาพ



รูปที่ 8.1.1 แผนภูมิการควบคุมภายในด้านเทคโนโลยีสารสนเทศก่อนและหลังทำโครงการ

8.2 สรุปผลประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนและหลังทำโครงการ)

จากการดำเนินการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ในขอบเขตของการจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) แล้วนั้นผู้ศึกษาโครงการนำแบบจำลองการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศมาใช้ประเมินผลความเสี่ยงการจัดการควบคุมภายในที่ยังคงขาดการดำเนินการ เพื่อให้ผู้บริหารและผู้ปฏิบัติงานเห็นถึงการดำเนินการที่มีความเสี่ยงสอดคล้องกับความเสี่ยงขององค์กรที่มีการกำหนดไว้ได้ โดยทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) ทำให้เห็นถึงภาพรวมว่า ความเสี่ยงที่สำคัญของธนาคารที่ควรดำเนินการจัดการมีอะไรบ้าง ซึ่งผู้ศึกษาโครงการได้จัดลำดับความเสี่ยงระดับสูง ปานกลาง และต่ำ เพื่อให้ผู้ปฏิบัติงานเห็นถึงลำดับสำคัญในการเพิ่มเติม ปรับปรุงการปฏิบัติงานการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขอบเขตการควบคุมการเข้าถึง (Access Control) ที่เหมาะสมสอดคล้องกับมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001)ที่ดี

ทั้งนี้ผู้ศึกษาโครงการได้ให้คำแนะนำ หรือแนวทางในการปฏิบัติงานที่ช่วยเพิ่มเติมปรับปรุงการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ส่งผลให้ทิศทางของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศลดลง ย่อมเป็นผลดีและสอดคล้องกับทิศทางความเสี่ยงขององค์กรที่มีการตอบสนองที่ดีขึ้นด้วย โดยการประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) เป็นตัวชี้วัดผลการตอบสนองความเสี่ยงที่ผู้บริหารหรือผู้ปฏิบัติงานสายเทคโนโลยีสารสนเทศนำไปปรับใช้ปฏิบัติ ทำให้ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) สามารถสรุปได้ดังนี้

ตารางที่ 8.2.1 ผลลัพธ์จากการประเมินความเสี่ยงและทิศทาง

ความเสี่ยง (Risk Heat Map)	ทิศทางความเสี่ยง (Risk Direction)
ลดลง	ลดลง ⬇
คงที่	ลดลง ⬇
	คงที่ ⟺

1) **การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับความเสี่ยงลดลง (Reduction Risk Heat Map) และทิศทางความเสี่ยงการดำเนินการปรับลดลง (Reduction Risk Direction)**

ซึ่งเป็นการบริหารจัดการความเสี่ยงที่ทุกส่วนคาดหวังอยากให้การดำเนินการหลังทำโครงการ เมื่อมีการพัฒนา ปรับปรุง กระบวนการใด ๆ ไปแล้วส่งผลให้ความเสี่ยงการบริหารจัดการด้านเทคโนโลยีสารสนเทศของธนาคารลดลงตามลำดับ จนอยู่ในระดับที่องค์กรยอมรับได้ หรือน่าพอใจ เช่น ผู้ศึกษาแนะนำแนวทางการปฏิบัติงานในการบริหารจัดการผู้ใช้งานที่มีสิทธิเฉพาะ (Privilege user) ให้ผู้ปฏิบัติงานเพิ่มกระบวนการควบคุมการเบิกใช้งาน และทบทวน Log การเข้าถึง หรือ Log เหตุการณ์ดำเนินการใด ๆ ที่ผู้ดูแลระบบงานไปใช้งาน เพื่อป้องกันการเข้าถึงที่ไม่เหมาะสม หรือการเกิดทุจริตได้อย่างทันต่อเหตุการณ์ เป็นต้น ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศจากการเข้าถึงที่ไม่เหมาะสมจากระดับความเสี่ยงสูง (ก่อนทำโครงการ) ปรับลดเป็นระดับ ปานกลาง อย่างเหมาะสม ในระดับที่องค์กรยอมรับได้

2) **การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับความเสี่ยงคงที่ (Residual Risk Heat Map) แต่ทิศทางความเสี่ยงการดำเนินการปรับลดลง (Reduction Risk Direction)**

ซึ่งเป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของธนาคารแล้ว ยังคงพบว่ามีความเสี่ยงอยู่ในองค์กร โดยอาจมีสาเหตุมาจากการอยู่ระหว่างการดำเนินการที่ยังไม่แล้วเสร็จ ครบถ้วนในทุกส่วน แต่โดยภาพรวมการบริหารจัดการในบางประการสามารถปรับลดความเสี่ยงในบางระดับไปบ้างแล้ว และทิศทางการดำเนินการยังคงหามาตรการ หรือแนวทางมาใช้ในการควบคุมความเสี่ยงเพิ่มเติมอย่างต่อเนื่อง เช่น ผู้ศึกษาโครงการแนะนำให้ผู้บริหาร หรือผู้ดูแลระบบสารสนเทศ ควรมีการรวบรวม จัดเก็บข้อมูลเส้นทางบนเครือข่าย (Network Routing control) ที่สำคัญของธนาคาร เช่น BOT , NCB Link ซึ่งเป็นเส้นทางที่เชื่อมต่อกับระบบงานของหน่วยงานรัฐบาล หรือเส้นทางระบบเครือข่ายที่มีความสำคัญ เช่น ระบบงานเงินฝาก ซึ่งเป็นธุรกรรมหลักของธนาคาร (Core Bank) เพื่อทำการกำหนดแนวทางปฏิบัติในการกำหนดการป้องกันการเกิดเหตุการณ์ต่าง ๆ อย่างเป็นลายลักษณ์อักษรว่า เส้นทางเครือข่ายใดสำคัญ เป็นเส้นทางหลัก (Primary Linkage) หรือเส้นทางสำรอง ให้ชัดเจน อย่างถูกต้อง และเหมาะสม ซึ่งสายเทคโนโลยีสารสนเทศ อยู่ระหว่างการจัดเก็บรวบรวม ข้อมูลการกำหนดเส้นทางระบบเครือข่าย เพื่อใช้ในการทบทวนนโยบาย ระเบียบ หลักเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี 2557 ให้มีความครบถ้วน โดยปัจจุบันมีการกำหนดเป็นคู่มือปฏิบัติงานเฉพาะ Link VOIP ธนาคารแห่งประเทศไทยเท่านั้น ซึ่งยังไม่ครอบคลุมทุก Routing Control ที่ธนาคารกำหนด (อยู่ระหว่างดำเนินการ) ผู้ศึกษาโครงการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ พบว่า ยังไม่ครบถ้วน คิดเป็น 1-2% ของระบบเงินฝากทั้งหมด ซึ่งจะเห็นได้ว่าทิศทางความเสี่ยงจากการดำเนินการลดลง (Reduction Risk Direction) อย่างเหมาะสม เป็นต้น

3) **การประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับความเสี่ยงคงที่ (Residual Risk Heat Map) และทิศทางความเสี่ยงการดำเนินการปรับลดลง (Residual Risk Direction)**

ซึ่งเป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของธนาคารแล้ว ยังคงพบว่ามีความเสี่ยงอยู่ในองค์กร โดยไม่ว่าจะดำเนินการอย่างไรความเสี่ยงยังคงอยู่ในระดับเท่าเดิม และทิศทางการดำเนินการก็ยังไม่สามารถปรับลดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ ซึ่งผู้บริหารหรือผู้ปฏิบัติงานควรพิจารณาแนวทางในการตอบสนองการดำเนินการอื่น เช่น การถ่ายโอนความเสี่ยงออกไปยังผู้ให้บริหาร (Vendor or Outsoucing) หรือการซื้อประกันภัยเพิ่มเติม เพื่อช่วยในการบริหารจัดการความเสี่ยงและศึกษาการตอบสนองว่าช่วยในการปรับลดความเสี่ยงต่อไปหรือไม่ ตลอดจนหากไม่สามารถดำเนินการใด ๆ ได้ควรยกเลิกหรือหลีกเลี่ยง (Avoid) การดำเนินกิจกรรมดังกล่าว หรือการปฏิบัติงานเพื่อการเข้าถึงดังกล่าวให้มีความเหมาะสม ซึ่งจากการศึกษาโครงการก่อนและหลังทำโครงการแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษาระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ดังกล่าวนี้ ยังไม่พบประเด็นของการประเมินผลความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับความเสี่ยงคงที่ (Residual Risk Heat Map) และทิศทางความเสี่ยงการดำเนินการปรับลดลง (Residual Risk Direction) ดังกล่าว

จากรายละเอียดการสรุปผลการดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนและหลังทำโครงการ ตามที่กล่าวมาแล้วนั้น ทำให้ผู้นำแนวทางการปฏิบัติตามแบบจำลองการจัดการความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ กรณีศึกษาระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ สามารถสรุปได้ดังนี้

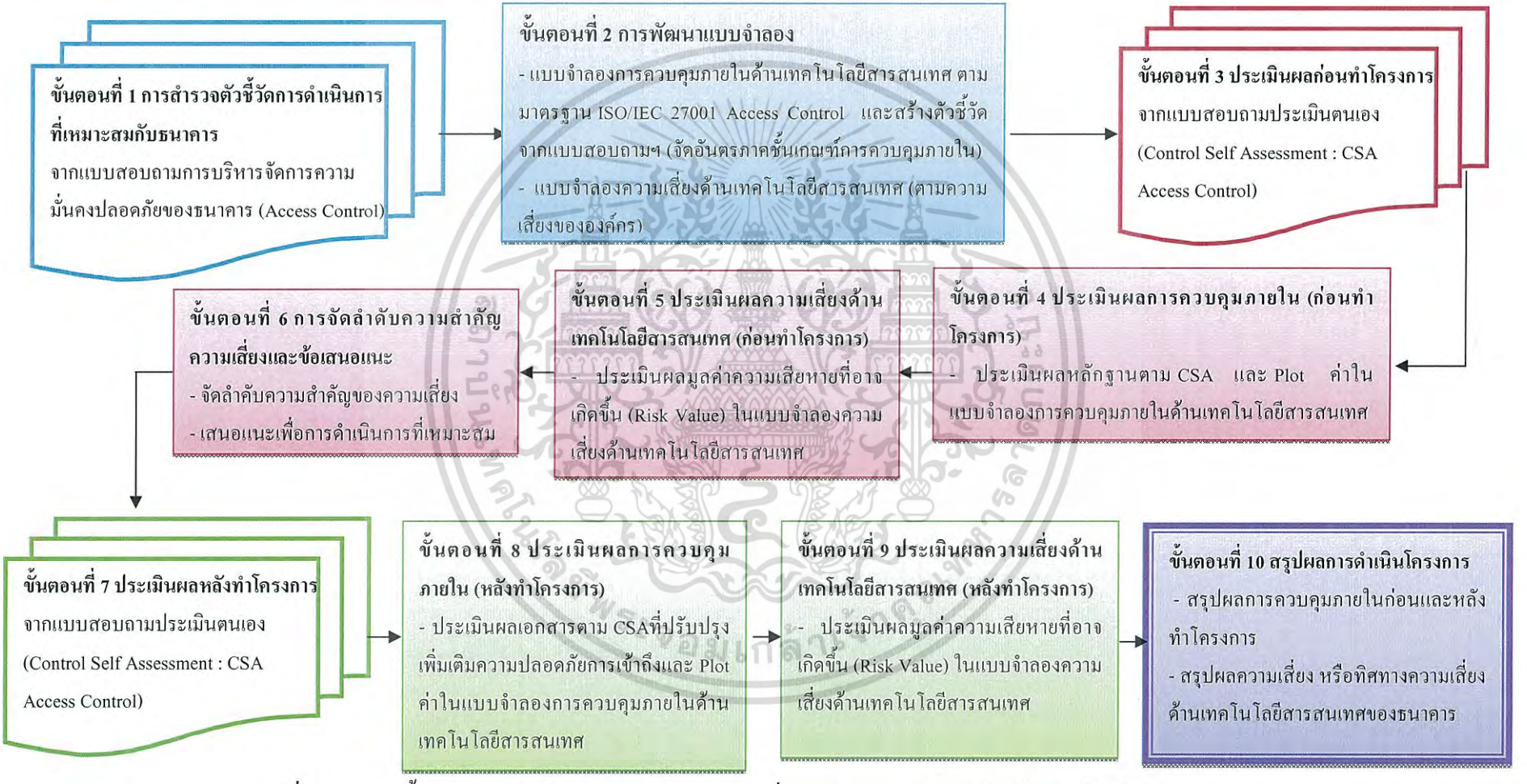
ตารางที่ 8.2.2 สรุปผลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ก่อนหลังทำโครงการ

รายละเอียดความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ก่อนทำโครงการ				หลังทำโครงการ			
	ผลประเมิน Likelihood	ผลประเมิน Impact	ผลลัพธ Risk Value	ระดับความเสี่ยง	ผลประเมิน Likelihood	ผลประเมิน Impact	ผลลัพธ Risk Value	ระดับความเสี่ยง
1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	5.00	7.25	**36.25**	High	2.00	5.50	**11.00**	Medium
1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	5.00	6.00	**30.00**	High	3.00	5.25	**15.75**	Medium
1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	5.00	6.25	**31.25**	High	2.00	5.00	**10.00**	Medium
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	5.00	5.25	**26.25**	High	2.00	4.00	**8.00**	Low
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	5.00	3.25	**16.25**	Medium	2.00	1.50	**3.00**	Low
1.3.1 การใช้งานรหัสผ่าน (Password use)	4.00	4.00	**16.0**	Medium	2.00	3.50	**7.00**	Low
1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	5.00	2.75	**13.75**	Medium	5.00	2.50	**12.50**	Medium
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	5.00	2.00	**10.00**	Medium	5.00	1.75	**8.75**	Medium
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	5.0	1.75	**8.75**	Medium	5.00	1.50	**7.50**	Medium

ตารางที่ 8.2.3 สรุปผลความเสี่ยงและทิศทางของความเสี่ยง (Risk Heat Map)

รายละเอียดความเสี่ยงด้านเทคโนโลยีสารสนเทศ	Risk Heat Map	Risk Direction
1.4.4การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	Medium High	ลดลง ⬇
1.2.2การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	Medium High	ลดลง ⬇
1.7.1การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	Medium High	ลดลง ⬇
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	Low High	ลดลง ⬇
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	Low Medium	ลดลง ⬇
1.3.1 การใช้งานรหัสผ่าน (Password use)	Low Medium	ลดลง ⬇
1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	Medium Medium	ลดลง ⬇
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	Medium Medium	ลดลง ⬇
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	Medium Medium	ลดลง ⬇

8.3 สรุปขั้นตอนดำเนินการแบบจำลองความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ



รูปที่ 8.3 สรุปขั้นตอนการดำเนินการแบบจำลองความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

บรรณานุกรม

เจนเนตร มณีนาค, กรกนก วงศ์พาณิชย์, ปัญจมน แก้วมีแสง และดรุณรัตน์ พึ่งตน. 2548. **การบริหารจัดการความเสี่ยงระดับองค์กร จากหลักผู้บริหารสู่ภาคปฏิบัติ**. กรุงเทพฯ: ซัมซิสเท็ม.

ชัยเสฏฐ์ พรหมศรี. 2550. **การบริหารความเสี่ยง**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: เอ็กซเปอร์เน็ท.

ตลาดหลักทรัพย์แห่งประเทศไทย. 2556. **การใช้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก.** พิมพ์ครั้งที่ 1. กรุงเทพฯ: เมจิกเพรส.

ตลาดหลักทรัพย์แห่งประเทศไทย. 2556. **การตรวจสอบการกำกับดูแลเทคโนโลยีสารสนเทศ.** พิมพ์ครั้งที่ 1. กรุงเทพฯ: เมจิกเพรส.

ประกาศธนาคารแห่งประเทศไทย. 2552. **สรข. 3/2552 เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์**. [Online] Available: http://www.etcommission.go.th/laws.html.

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย. 2556. **แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) : Phase: ธุรกรรมฝาก ถอน และโอน.** [Online] Available: http://www2.bot.or.th/FIPCS/thai/PFIPCS_List.aspx

พระราชกฤษฎีกา. 2553. **ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์**. [Online] Available: http://www.etcommission.go.th/laws.html

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. 2550. **มาตรฐานการรักษาความมั่นคงปลอดภัย (เวอร์ชั่น 2.5)**. พิมพ์ครั้งที่ 1. ปทุมธานี: หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทยและตลาดหลักทรัพย์แห่งประเทศไทย. 2551. **กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ : บทสรุปสำหรับผู้บริหารและกรอบโครงสร้าง**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง.

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทยและตลาดหลักทรัพย์แห่งประเทศไทย. 2551. **กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ : แนวทางปฏิบัติ**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง.

สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย. 2546. **คู่มือตรวจสอบความเสี่ยงสถาบันการเงิน**. [Online] Available: http://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/Pages/ExaminationManual.aspx.

S.H.von Solms and R.von Solms. 2009. **Information Security Governance**. New York: Springer.

The Institute of Internal Auditors 2005. **Information Technology Control**. [Online] Available: http://www.iiacolombia.com/resource/guias/GTAG1.pdf

The Institute of Internal Auditors 2011. **Three Lines of Defense Model**. [Online] Available: http://www.theiia.org/chapters/pubdocs/303/2_Jean_Pierre_Garitte_Advocacy_Achievements_and_the_3_lines_of_Defense_Model.pdf.

the International Organization for Standardization (ISO). 2005. **ISO/IEC 27001 Information technology – Security techniques - Information security management systems – Requirements**. [Online] Available: http://www.iso.org.

ภาคผนวก

ภาคผนวก ก

แบบสอบถามผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และการควบคุมภายในเกี่ยวกับเกณฑ์การบริหารจัดการความมั่นคงปลอดภัยขององค์กร ตามมาตรฐาน ISO/IEC 27001 ในขอบเขตการเข้าถึงระบบสารสนเทศของธนาคาร (Acess Control)

แบบสอบถาม

เรื่อง แบบสอบถามผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และการควบคุมภายในเกี่ยวกับเกณฑ์การบริหารจัดการความมั่นคงปลอดภัยขององค์กร ตามมาตรฐาน ISO/IEC 27001 ในขอบเขตการเข้าถึงระบบสารสนเทศของธนาคาร (Acess Control)

เรียน ผู้เชี่ยวชาญที่เกี่ยวข้องกับระบบงาน และการจัดการงานตรวจสอบภายใน

เนื่องด้วยดิฉันนางสาวจิรวณี สิริประภาสวัสดิ์ อยู่ระหว่างการศึกษาอิสระ กรณีศึกษาด้านความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ เพื่อใช้ไปประกอบกับวิชาการศึกษาอิสระ 2 ระดับปริญญาโท สาขาเทคโนโลยีสารสนเทศ แขนงเทคโนโลยีสารสนเทศและการจัดการ หลักสูตรวิทยาศาสตร์มหาบัณฑิต มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง จึงใคร่ขอความกรุณาจากผู้ที่เกี่ยวข้องในการตอบแบบสอบถามให้ครบถ้วนในส่วนที่ 1 และ 2

คำชี้แจง :

โปรดแสดงความคิดเห็นของท่านในแต่ละข้อโดยทำเครื่องหมาย ✓ ลงในช่อง เพื่อให้การศึกษาในครั้งนี้สามารถนำ ไปใช้ให้เกิดประโยชน์สูงสุด ขอความกรุณาตอบแบบสอบถามทุกข้อตามความเป็นจริง โดยคำตอบจากแบบสอบถามจะถูกเก็บเป็นความลับและใช้เพื่อการศึกษาเท่านั้น

ส่วนที่ 1 แบบสอบถามเกี่ยวกับความถูกต้องของตำแหน่งหน้าที่ การทำงาน

1.1 ท่านเคย หรืออยู่ระหว่างทำงานในธนาคารพาณิชย์แห่งหนึ่ง ใช่หรือไม่

☐ ใช่ ☐ ไม่ใช่

1.2 ท่านดำรงตำแหน่ง อยู่ในส่วนงานเทคโนโลยีสารสนเทศ หรือการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์แห่งหนึ่ง ใช่หรือไม่

☐ ใช่ ☐ ไม่ใช่

1.3 ท่านดำรงตำแหน่ง อยู่ในส่วนงานเทคโนโลยีสารสนเทศ หรือการควบคุมภายในด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์แห่งหนึ่ง ระยะเวลากี่ปี

☐ 1-2 ☐ 3-5 ☐ มากกว่า 5 ปี

ส่วนที่ 2 แบบสอบถามความเห็นเพื่อการบริหารจัดการความมั่นคงปลอดภัยขององค์กรในขอบเขตการเข้าถึงระบบสารสนเทศของธนาคาร (Acess Control) ที่ดีสำหรับองค์กร (กรุณา ✓ ระดับความเห็น)

No	Control Objective	ระดับ 5 เห็นด้วยอย่างยิ่ง	ระดับ 4 ค่อนข้างเห็นด้วย	ระดับ 3 มีหรือไม่มีก็ได้	ระดับ 2 ค่อนข้างไม่เห็นด้วย	ระดับ 1 ไม่เห็นด้วย
7.1	**ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)** ท่านคิดว่า ธนาคารควรมีการกำหนดนโยบายการควบคุมการเข้าถึงระบบ (Access control policy) หรือไม่					
7.2	**การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีการจัดการเพื่อการเข้าถึงของผู้ใช้งาน ตั้งแต่การกำหนดให้มีการลงทะเบียนพนักงาน บริหารจัดการสิทธิ และรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการทบทวนสิทธิผู้ใช้งานอย่างครบถ้วน หรือไม่					
7.3	**หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีการใช้งานรหัสผ่านในทุกส่วนของระบบเทคโนโลยีสารสนเทศ ตลอดจนมีวิธีการป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล หรือไม่					
7.4	**การควบคุมการเข้าถึงเครือข่าย (Network access control)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีนโยบายการใช้งานระบบเครือข่าย การพิสูจน์ตัวตนจากภายนอกและบนอุปกรณ์บนระบบเครือข่าย ตลอดจนการป้องกันพอร์ต การควบคุมการเชื่อมต่อ และการแบ่งแยกระบบเครือข่ายให้มีความมั่นคงปลอดภัย หรือไม่					

No	Control Objective	ระดับ 5 เห็นด้วยอย่างยิ่ง	ระดับ 4 ค่อนข้างเห็นด้วย	ระดับ 3 มีหรือไม่มีก็ได้	ระดับ 2 ค่อนข้างไม่เห็นด้วย	ระดับ 1 ไม่เห็นด้วย
7.5	**การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on) การพิสูจน์ตัวตนหรือการบริหารจัดการรหัสผ่าน การกำหนดระยะเวลาการใช้งานหรือจำกัดการใช้ระบบงาน ตลอดจนกำหนดให้มีการใช้งานโปรแกรมยูทิลิตี้อย่างมั่นคงปลอดภัย หรือไม่					
7.6	**การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีการจำกัดการเข้าถึงสารสนเทศที่สำคัญของธนาคาร หรือการแบ่งแยกระบบสารสนเทศที่มีความสำคัญสูงให้มีความมั่นคงปลอดภัยมากขึ้น หรือไม่					
7.7	**การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)** ท่านคิดว่า ธนาคารควรมีการกำหนดให้มีการป้องกันอุปกรณ์สื่อสารประเภทพกพาที่ใช้กับธนาคาร หรือการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ให้มีความมั่นคงปลอดภัย หรือไม่					

ภาคผนวก ข

แบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายในโดยการประเมินตนเอง (Control Self Assessment: CSA)

แบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายใน
โดยการประเมินตนเอง
(Control Self Assessment: CSA)
เรื่อง มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ
กรณีศึกษา ระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์ โดยสายงาน IT

<u>เกณฑ์การประเมิน Control Self Assessment</u>

กรุณาทำเครื่องหมาย ✓ ในช่อง ☐ เพื่อทำการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ที่ปัจจุบันธนาคารมีการกำหนด พร้อมทั้งอธิบาย อ้างอิงเอกสารที่มีการดำเนินการดังนี้

☐ **Preventive Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในแบบป้องกัน หรือลดความเสี่ยงจากความผิดพลาด ความเสียหายจากเหตุการณ์ที่เกิดขึ้น หรือการรักษาความปลอดภัย เช่น กำหนดนโยบาย ระเบียบ หลักเกณฑ์ให้ชัดเจนเป็นลายลักษณ์อักษร การแบ่งแยกหน้าที่การงาน การควบคุมการเข้าถึงทรัพย์สินธนาคารไว้อย่างเหมาะสม

☐ **Detective Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในแบบตรวจหา หรือทำการตรวจสอบ ตรวจเช็ค ค้นหาข้อผิดพลาดหรือความเสียหายที่เกิดขึ้นแล้ว เช่น การติดตาม (Monitor) ด้วยคนหรือเครื่องมือ (Tools) ใด ๆ ในการการสอบทานงาน ยืนยันสิทธ์การเข้าถึงอย่างสม่ำเสมอ ตลอดจดการใช้เครื่องมือเทคโนโลยีสารสนเทศทำการตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ผิดปกติ หรือไม่เหมาะสม

☐ **Corrective Control** หมายถึง ธนาคารมีการกำหนดแนวทางปฏิบัติ เพื่อประเมินว่ามีการควบคุมภายในเพื่อแก้ไขข้อผิดพลาดหรือเหตุการณ์ที่เกิดขึ้นให้ถูกต้อง จากการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร สำหรับการหาแนวทางการแก้ไขปัญหาไม่ให้เกิดข้อผิดพลาดซ้ำอีกภายในองค์กรไว้

ขอบเขตการตรวจสอบ

การจัดการความมั่นคงปลอดภัยของการเข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคาร (Access Control) โดยระบบงานที่เป็นธุรกรรมอิเล็กทรอนิกส์ของกลุ่มตัวอย่าง (Sampling System) ได้แก่ ระบบงานเงินฝาก Flexcute (FCR)

เนื่องมาจากเป็นธุรกรรมหลักด้านเงินฝากสำหรับสนับสนุนธุรกิจหลัก (Core Business Financial Bank) ที่มีฐานข้อมูลการทำธุรกรรมทางการเงินของลูกค้า เพื่อควบคุมการเข้าถึงอย่างมั่นคงปลอดภัยเป็นไปตามมาตรฐานความมั่นคงปลอดภัย (ISO/IEC 27001)

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)			
1.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy) ธนาคารกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
1.2.1 การลงทะเบียนพนักงาน (User registration) ธนาคารกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) ธนาคารจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ธนาคารกำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ธนาคารกำหนดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			
1.3.1 การใช้งานรหัสผ่าน (Password use) ธนาคารมีการกำหนดวิธีปฏิบัติที่มั่นคงปลอดภัยสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment) ธนาคารมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.4. การควบคุมการเข้าถึงเครือข่าย (Network access control)			
1.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารมีการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ธนาคารกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอก โดยองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) ธนาคารมีการกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ซึ่งได้รับอนุญาตแล้ว ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ธนาคารมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุม	☐ Preventive Control		
	☐ Detective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
ทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครื่องข่าย ***ใช่หรือไม่อย่างไร***	☐ Corrective Control		
1.4.5 การแบ่งแยกเครือข่าย (Segregation in networks) ธนาคารมีการจัดทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ธนาคารมีการจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ธนาคารมีการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
1.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures) ธนาคารมีการจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการ	☐ Preventive Control		
	☐ Detective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
เข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ ***ใช่หรือไม่อย่างไร***	☐ Corrective Control		
1.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication) ธนาคารมีการจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system) ธนาคารมีการจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ธนาคารมีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out) ธนาคารมีการกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
1.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ธนาคารมีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)			
1.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ธนาคารมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) ธนาคารมีการแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ ***ใช่หรือไม่อย่างไร***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
1.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications) ธนาคารมีการต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกัน	☐ Preventive Control		
	☐ Detective Control		

การตรวจสอบ	หน่วยงานประเมินตนเอง		ความเห็นผู้รับการตรวจสอบ / ผู้ตรวจสอบ
	ใช่ / ไม่ใช่	อ้างอิงเอกสาร	
อุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ ***<u>ใช่หรือไม่อย่างไร</u>***	☐ Corrective Control		
1.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ธนาคารมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน ***<u>ใช่หรือไม่อย่างไร</u>***	☐ Preventive Control		
	☐ Detective Control		
	☐ Corrective Control		
ความเห็นเพิ่มเติม.....			
.....			
ขอรับรองว่าข้อมูลที่ได้ให้ไว้ในแบบสอบถามกระบวนการปฏิบัติงานและการควบคุมภายใน โดยการประเมินตนเอง (Control Self Assessment: CSA) ถูกต้องตรงกับการปฏิบัติงานจริงทุกประการ			

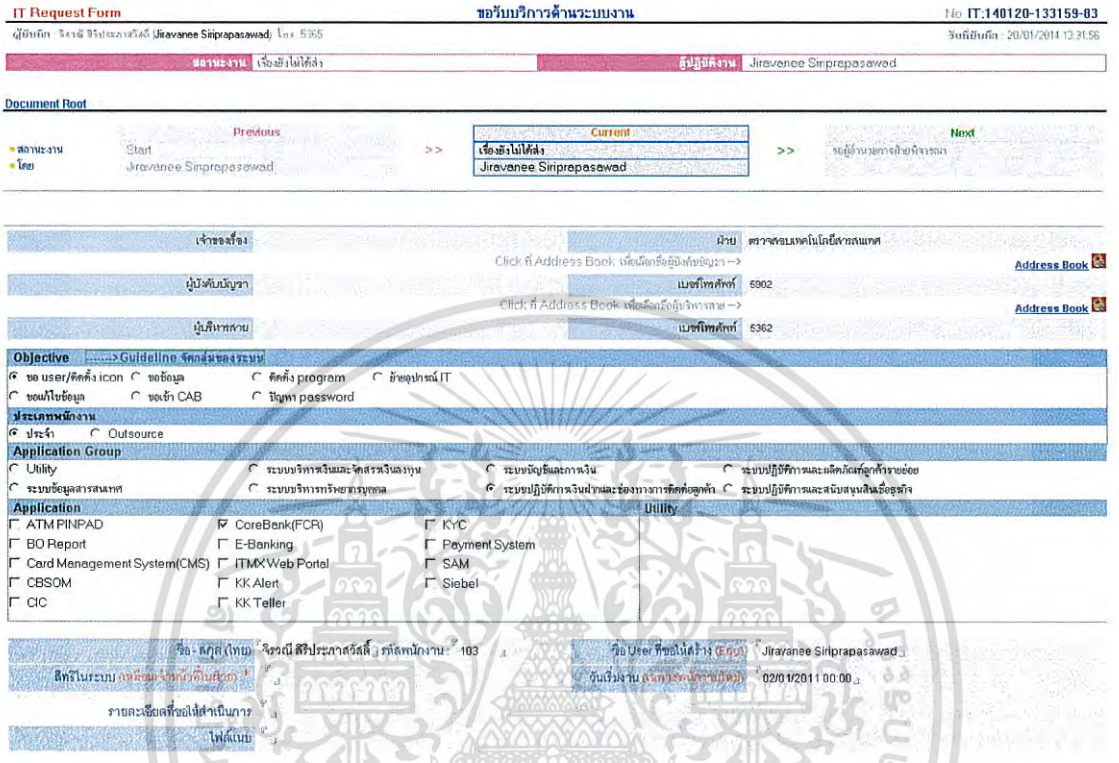
ที่มา...มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001)

ภาคผนวก ค

เอกสารประกอบการดำเนินการเพื่อประเมินผลความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (ก่อนทำโครงการ) กรณีศึกษาระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์

1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

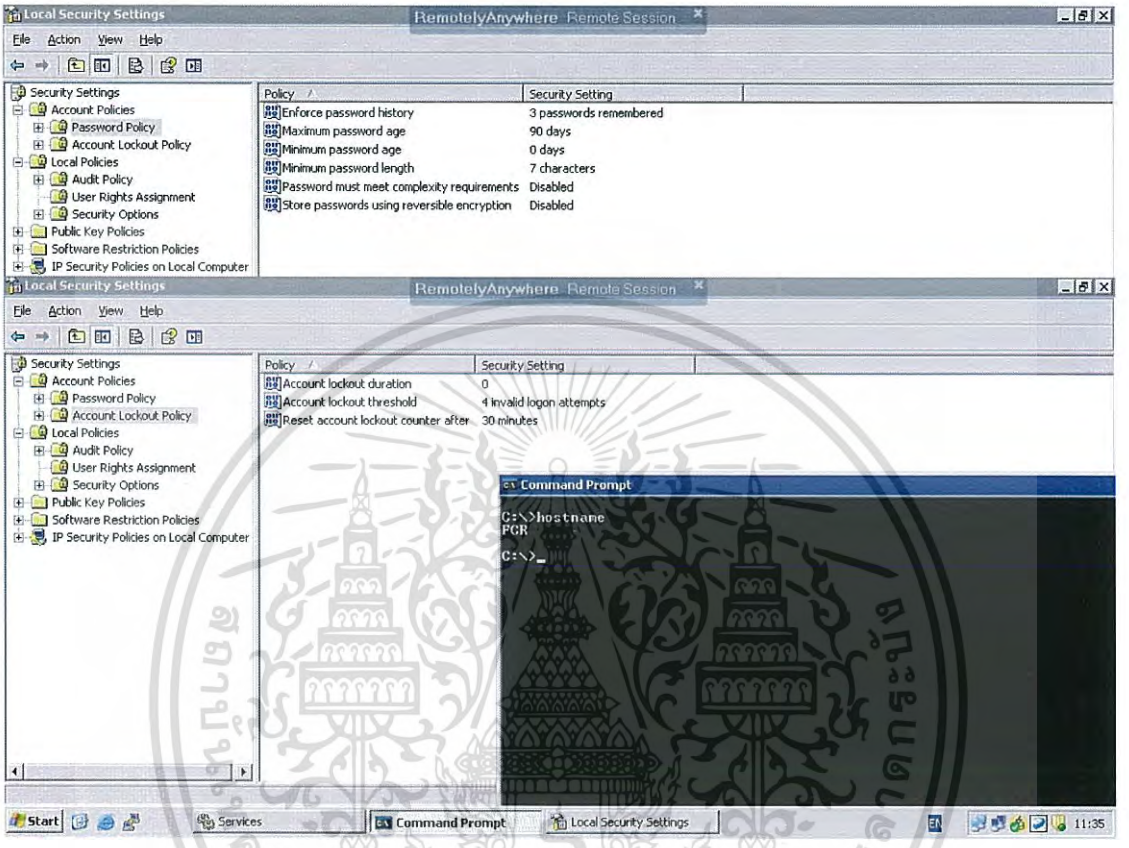
1.2.1(2) เอกสาร IT Request การร้องขอสิทธิเข้าถึงระบบงานธนาคารในการควบคุมการเข้าถึงระบบสารสนเทศธนาคารอย่างเหมาะสม



รูปที่ 1.2.1 เอกสารแนบหน้าจอ IT Request การร้องขอสิทธิเข้าถึงระบบงาน

1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

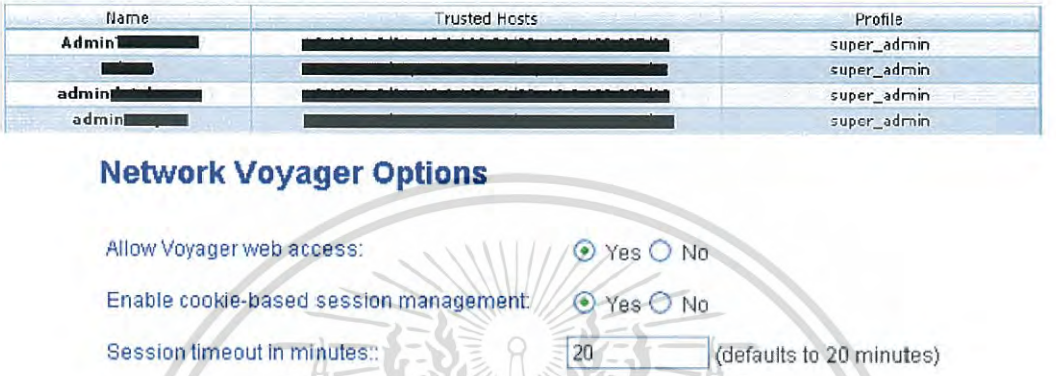
1.3.2(1) ผู้ศึกษาโครงการใช้เทคนิคในการ Remote เพื่อเข้าถึง Server ดูค่า Configuration ที่ใช้ในระบบงานเงินฝาก (Core Bank) ในการบริหารจัดการการเข้าถึงระบบงานอย่างเหมาะสม



รูปที่ 1.3.2 เอกสารแนบหน้าจอการกำหนดค่า Configuration การเข้าถึงระบบงานระดับ Server

1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

1.4.3(1) หน้าจอ Firewall กำหนด Admin เข้าถึงอุปกรณ์ตาม IP Address Manage Permitted IP Address ที่ Firewall ในการให้ Administrator เข้าถึง Host ของระบบงานเงินฝาก ตลอดจนการกำหนดค่าการเข้าถึงระบบงานเครือข่ายมีการกำหนด Session Time out อย่างมั่นคงปลอดภัย



Name	Trusted Hosts	Profile
Admin[redacted]	[redacted]	super_admin
[redacted]	[redacted]	super_admin
admin[redacted]	[redacted]	super_admin
admin[redacted]	[redacted]	super_admin

Network Voyager Options

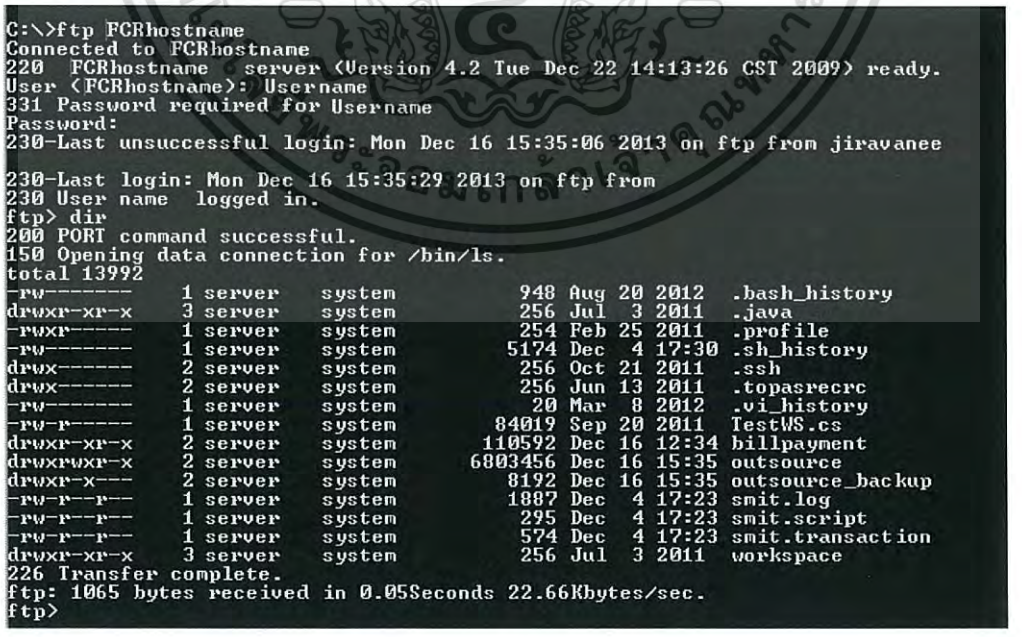
Allow Voyager web access: (•) Yes ( ) No

Enable cookie-based session management: (•) Yes ( ) No

Session timeout in minutes:: 20 (defaults to 20 minutes)

รูปที่ 1.4.3 หน้าจอการกำหนดค่า IP Address ให้เข้าถึงระบบเครือข่ายได้เฉพาะผู้ดูแลระบบ

1.4.4(1) ผู้ศึกษาโครงการใช้เทคนิคในการเข้าถึงพอร์ตระบบเครือข่ายที่ทำการเปิดไว้อย่างไม่มั่นคงปลอดภัยมากเพียงพอ อาจส่งผลต่อการเข้าถึงระบบสารสนเทศที่ไม่ถูกต้องได้



```
C:\>ftp FCRhostname
Connected to FCRhostname
220  FCRhostname  server (Version 4.2 Tue Dec 22 14:13:26 CST 2009) ready.
User (FCRhostname): Username
331 Password required for Username
Password:
230-Last unsuccessful login: Mon Dec 16 15:35:06 2013 on ftp from jiravanee

230-Last login: Mon Dec 16 15:35:29 2013 on ftp from
230 User name  logged in.
ftp> dir
200 PORT command successful.
150 Opening data connection for /bin/ls.
total 13992
-rw-------    1 server   system         948 Aug 20 2012  .bash_history
drwxr-xr-x    3 server   system         256 Jul  3 2011  .java
-rwxr-----    1 server   system         254 Feb 25 2011  .profile
-rw-------    1 server   system        5174 Dec  4 17:30 .sh_history
drwx------    2 server   system         256 Oct 21 2011  .ssh
drwx------    2 server   system         256 Jun 13 2011  .topasrecrc
-rw-------    1 server   system          20 Mar  8 2012  .vi_history
-rw-r-----    1 server   system       84019 Sep 20 2011  TestWS.cs
drwxr-xr-x    2 server   system      110592 Dec 16 12:34 billpayment
drwxrwxr-x    2 server   system     6803456 Dec 16 15:35 outsource
drwxr-x---    2 server   system        8192 Dec 16 15:35 outsource_backup
-rw-r--r--    1 server   system        1887 Dec  4 17:23 smit.log
-rw-r--r--    1 server   system         295 Dec  4 17:23 smit.script
-rw-r--r--    1 server   system         574 Dec  4 17:23 smit.transaction
drwxr-xr-x    3 server   system         256 Jul  3 2011  workspace
226 Transfer complete.
ftp: 1065 bytes received in 0.05Seconds 22.66Kbytes/sec.
ftp>
```

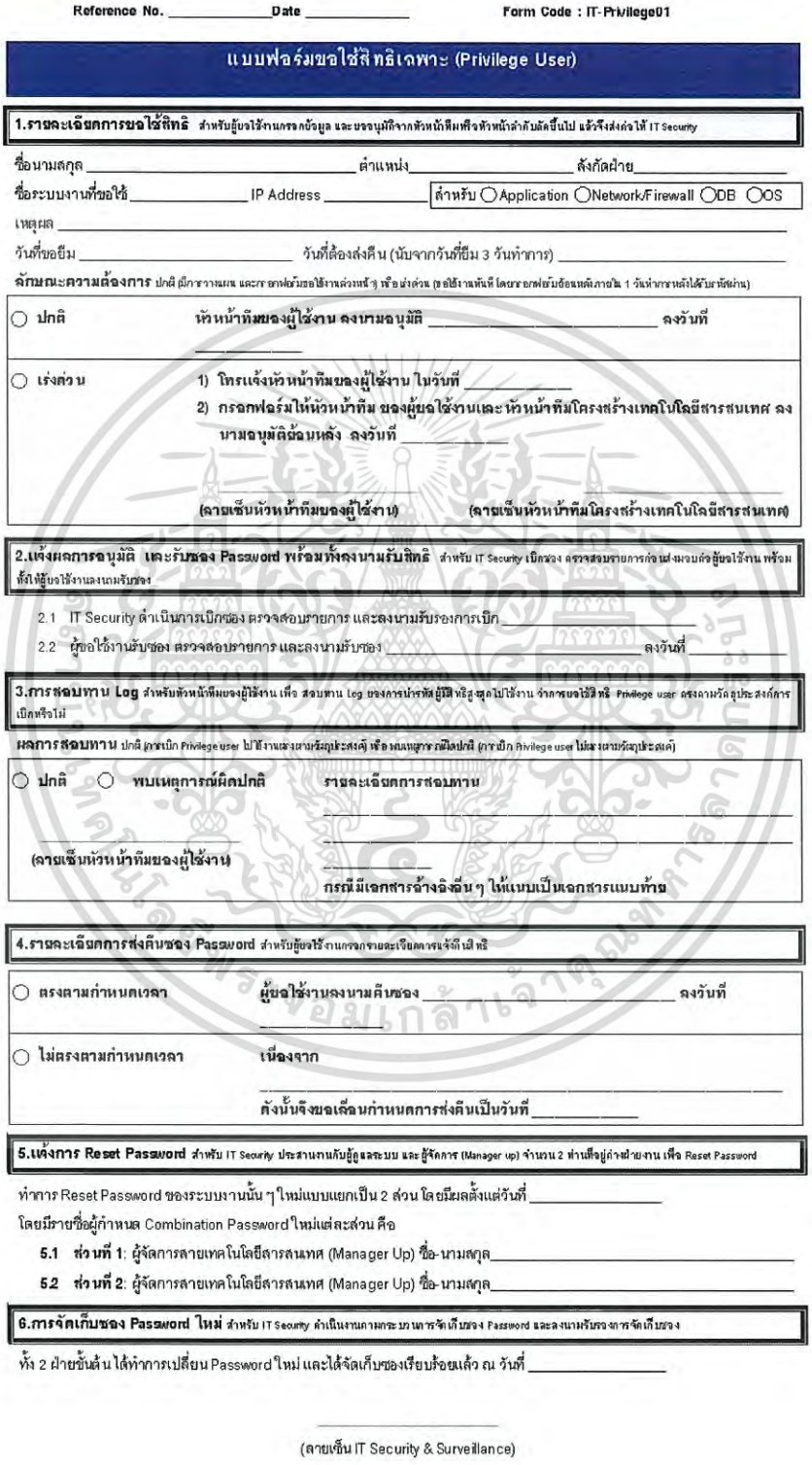
รูปที่ 1.4.4.1 เอกสารแนบหน้าจอการเปิดพอร์ตการเข้าถึงระบบเครือข่าย

ภาคผนวก ง

เอกสารประกอบการดำเนินการเพื่อประเมินผลความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หลังทำโครงการ) กรณีศึกษาระบบธุรกรรมอิเล็กทรอนิกส์ของธนาคารพาณิชย์

1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

1.2.2 (1) แบบฟอร์มเพื่อให้ผู้ปฏิบัติงานดำเนินการจัดการสิทธิการใช้งานระบบ (Privilege management) การขอใช้สิทธิเฉพาะ (Privilege User) และการทบทวน Log เมื่อมีการเบิกใช้งาน



Reference No. _____Date _____ Form Code : IT-Privilege01

แบบฟอร์มขอใช้สิทธิเฉพาะ (Privilege User)

1.รายละเอียดการขอใช้สิทธิ สำหรับผู้ขอใช้งานกรอกข้อมูล และขออนุมัติจากหัวหน้าทีมหรือหัวหน้าลำดับถัดขึ้นไป แล้วจึงส่งต่อให้ IT Security

ชื่อนามสกุล _____ตำแหน่ง_____สังกัดฝ่าย_____

ชื่อระบบงานที่ขอใช้_____ IP Address _____ สำหรับ ○ Application ○ Network/Firewall ○ DB ○ OS

เหตุผล _____

วันที่ขอยืม _____ วันที่ต้องส่งคืน (นับจากวันที่ยืม 3 วันทำการ) _____

ลักษณะความต้องการ ปกติ (มีการร่างแบบ และกรอกฟอร์มขอใช้งานล่วงหน้า ๆ หรือส่งล่วง (ขอใช้งานทันที โดยกรอกฟอร์มย้อนหลังภายใน 1 วันทำการหลังได้รับสิทธิ์ผ่าน)

○ ปกติ — **หัวหน้าทีมของผู้ใช้งาน ลงนามอนุมัติ** _____ **ลงวันที่** _____

○ เร่งด่วน — 1) **โทรแจ้งหัวหน้าทีมของผู้ใช้งาน ในวันที่** _____
2) **กรอกฟอร์มให้หัวหน้าทีม ของผู้ขอใช้งานและ หัวหน้าทีมโครงสร้างเทคโนโลยีสารสนเทศ ลงนามอนุมัติย้อนหลัง ลงวันที่** _____

(ลายเซ็นหัวหน้าทีมของผู้ใช้งาน) **(ลายเซ็นหัวหน้าทีมโครงสร้างเทคโนโลยีสารสนเทศ)**

2.แจ้งผลการอนุมัติ และรับของ Password พร้อมทั้งลงนามรับสิทธิ สำหรับ IT Security เบิกของ ตรวจสอบรายการก่อนส่งมอบก่อผู้ขอใช้งาน พร้อมทั้งให้ผู้ขอใช้งานลงนามรับของ

2.1 IT Security ดำเนินการเบิกของ ตรวจสอบรายการ และลงนามรับรองการเบิก _____

2.2 ผู้ขอใช้งานรับของ ตรวจสอบรายการ และลงนามรับของ _____ ลงวันที่ _____

3.การสอบทาน Log สำหรับหัวหน้าทีมของผู้ใช้งาน เพื่อ สอบทาน Log ของการนำรหัสผู้มีสิทธิสูงสุดไปใช้งาน ว่าการขอใช้สิทธิ Privilege user ตรงตามวัตถุประสงค์การเบิกหรือไม่

ผลการสอบทาน ปกติ (การเบิก Privilege user ไปใช้งานตรงตามวัตถุประสงค์) หรือพบเหตุการณ์ผิดปกติ (การเบิก Privilege user ไม่ตรงตามวัตถุประสงค์)

○ ปกติ ○ พบเหตุการณ์ผิดปกติ — **รายละเอียดการสอบทาน** _____

(ลายเซ็นหัวหน้าทีมของผู้ใช้งาน)

กรณีมีเอกสารอ้างอิงอื่น ๆ ให้แนบเป็นเอกสารแนบท้าย

4.รายละเอียดการส่งคืนของ Password สำหรับผู้ขอใช้งานกรอกรายละเอียดการแจ้งคืนสิทธิ

○ ตรงตามกำหนดเวลา — **ผู้ขอใช้งานลงนามคืนของ** _____ **ลงวันที่** _____

○ ไม่ตรงตามกำหนดเวลา — **เนื่องจาก** _____

ดังนั้นจึงขอเลื่อนกำหนดการส่งคืนเป็นวันที่ _____

5.แจ้งการ Reset Password สำหรับ IT Security ประสานงานกับผู้ดูแลระบบ และผู้จัดการ (Manager up) จำนวน 2 ท่านขึ้นไปเพื่อทำการ Reset Password

ทำการ Reset Password ของระบบงานนั้น ๆ ใหม่แบบแยกเป็น 2 ส่วน โดยมีผลตั้งแต่วันที่ _____

โดยมีรายชื่อผู้กำหนด Combination Password ใหม่แต่ละส่วน คือ

5.1 ส่วนที่ 1: ผู้จัดการสายเทคโนโลยีสารสนเทศ (Manager Up) ชื่อ-นามสกุล _____

5.2 ส่วนที่ 2: ผู้จัดการสายเทคโนโลยีสารสนเทศ (Manager Up) ชื่อ-นามสกุล _____

6.การจัดเก็บของ Password ใหม่ สำหรับ IT Security ดำเนินงานตามกระบวนการจัดเก็บของ Password และลงนามรับรองการจัดเก็บของ

ทั้ง 2 ฝ่ายขั้นต้น ได้ทำการเปลี่ยน Password ใหม่ และได้จัดเก็บของเรียบร้อยแล้ว ณ วันที่ _____

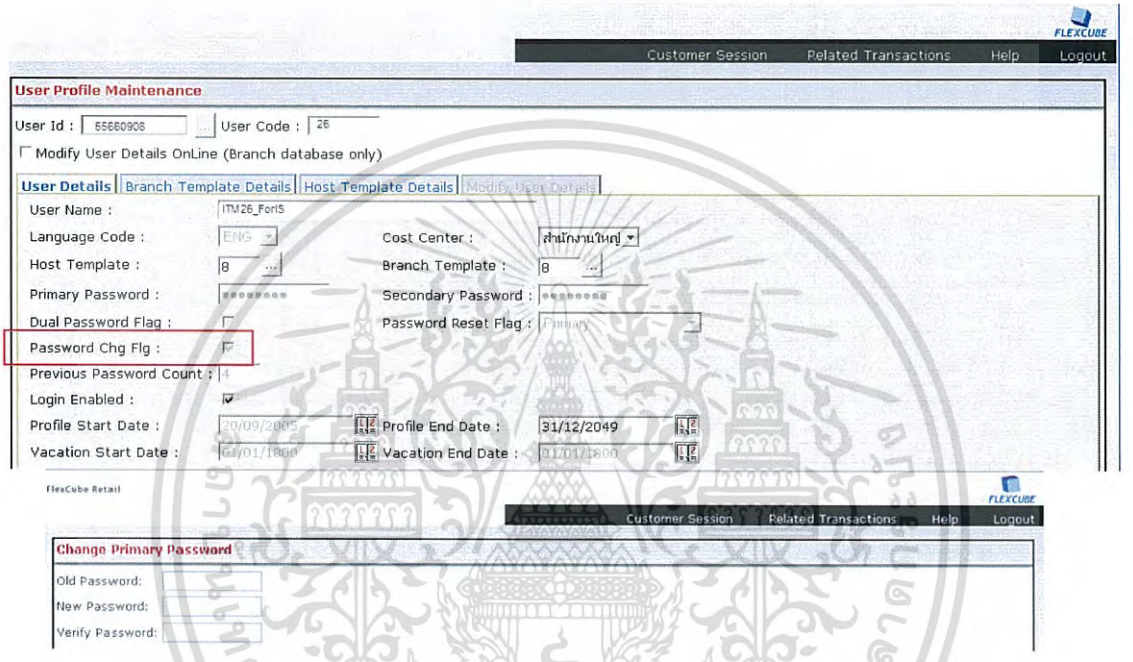
_____

(ลายเซ็น IT Security & Surveillance)

รูปที่ 1.2.2 เอกสารแนบตัวอย่างแบบฟอร์มขอใช้สิทธิเฉพาะ(Privilege User)และการทบทวน Log

1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

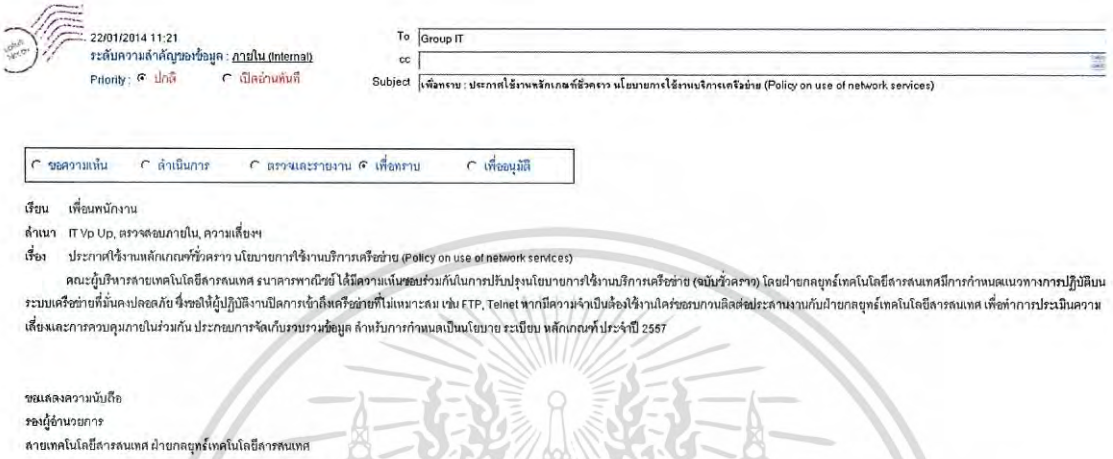
1.3.1 (1) ผู้ศึกษาโครงการใช้วิธีการเข้าถึงหน้าจอการกำหนดให้ระบบงาน Force Change Password เพื่อให้ผู้ใช้งานทำการเลือกการใช้งานรหัสผ่าน (Password use) ที่มีความมั่นคงปลอดภัย และผู้ศึกษาทดสอบเปลี่ยนรหัสผ่าน เมื่อ Login เข้าใช้งานครั้งแรก ระบบงานเงินฝาก กำหนดให้ต้องเปลี่ยนรหัสผ่านอย่างมั่นคงปลอดภัย ซึ่งหากไม่เปลี่ยน จะไม่สามารถข้ามขั้นตอนไปใช้งานในระบบ



รูปที่ 1.3.1 เอกสารแนบหน้าจอการกำหนดค่า Configuration การเลือกใช้งานรหัสผ่าน

1.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

1.4.1 (1) นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ธนาคารมีการกำหนดให้ปฏิบัติงานชั่วคราว ระหว่างการเก็บรวบรวมข้อมูล และทบทวนนโยบายฉบับปี 2557 ให้มีเนื่องหาครอบคลุม



22/01/2014 11:21
ระดับความสำคัญของข้อมูล : ภายใน (Internal)
Priority : ปกติ เปิดอ่านทันที

To Group IT
cc
Subject เพื่อทราบ : ประกาศใช้งานหลักเกณฑ์ชั่วคราว นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

ขอความเห็น ดำเนินการ ตรวจและรายงาน เพื่อทราบ เพื่ออนุมัติ

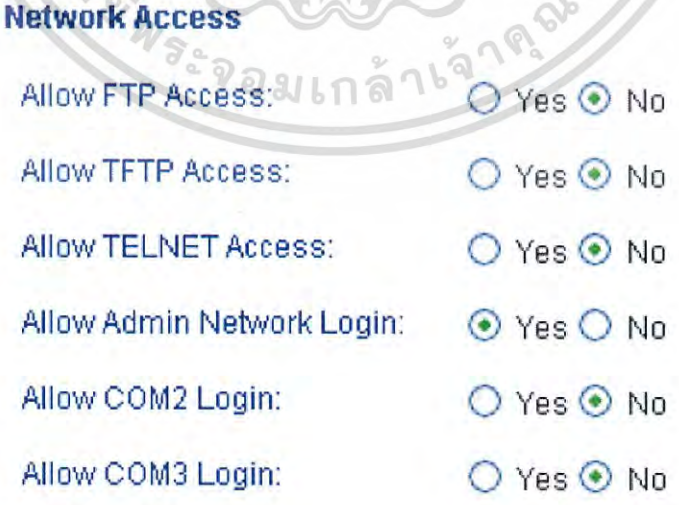
เรียน เพื่อนพนักงาน
ตำแหน่ง IT Vp Up, ตรวจสอบภายใน, ความเสี่ยงฯ
เรื่อง ประกาศใช้งานหลักเกณฑ์ชั่วคราว นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

คณะผู้บริหารสายเทคโนโลยีสารสนเทศ ธนาคารพาณิชย์ ได้มีความเห็นชอบร่วมกันในการปรับปรุงนโยบายการใช้งานบริการเครือข่าย (ฉบับชั่วคราว) โดยฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศมีการกำหนดแนวทางการปฏิบัติบนระบบเครือข่ายที่มั่นคงปลอดภัย ซึ่งขอให้ผู้ปฏิบัติงานปิดการเข้าถึงเครือข่ายที่ไม่เหมาะสม เช่น FTP, Telnet หากมีความจำเป็นต้องใช้งานโดยขอรับอนุมัติส่งประสานงานกับฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศ เพื่อทำการประเมินความเสี่ยงและการควบคุมภายในร่วมกัน ประกอบการจัดเก็บรวบรวมข้อมูล สำหรับการกำหนดเป็นนโยบาย ระเบียบ หลักเกณฑ์ ประจำปี 2557

ขอแสดงความนับถือ
รองผู้อำนวยการ
สายเทคโนโลยีสารสนเทศ ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศ

รูปที่ 1.4.1.1 เอกสารแนบตัวอย่างประกาศใช้งานนโยบายใช้บริการเครือข่าย(Network Policy)

1.4.4 (2) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ผู้ศึกษาเข้าถึงการตั้งค่า Configuration Firewall เพื่อการศึกษาการบริหารจัดการความมั่นคงระบบเครือข่ายให้สอดคล้องกับมาตรฐาน ISO/IEC 27001



Network Access

Allow FTP Access:	○ Yes ◉ No
Allow TFTP Access:	○ Yes ◉ No
Allow TELNET Access:	○ Yes ◉ No
Allow Admin Network Login:	◉ Yes ○ No
Allow COM2 Login:	○ Yes ◉ No
Allow COM3 Login:	○ Yes ◉ No

รูปที่ 1.4.4.2 เอกสารแนบการกำหนดค่าป้องกันพอร์ตความมั่นคงปลอดภัยระบบเครือข่าย

1.4.7 (1) การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) ปัจจุบันมีการกำหนดการควบคุมเส้นทางแค่ Link ที่ธนาคารเชื่อมต่อธนาคารแห่งประเทศไทย แต่ยังไม่ครอบคลุมทุกระบบเครือข่ายที่สำคัญของธนาคาร เช่น ระบบเงินฝาก , Link หน่วยงานรัฐบาล ฯลฯ โดยอยู่ระหว่างการรวบรวมและดำเนินการ คาดว่าแล้วเสร็จธันวาคม 2557

คู่มือการติดตั้งระบบ

BOT Conference

วันที่:	
ฉบับที่:	
เจ้าของเอกสาร:	

Configure Firewall and Web Proxy File (หากใช้งานผ่าน Broadband, ADSL, 3G ข้ามขั้นตอนนี้ได้)

ข้อนี้ต้องแจ้งให้ ทีม Data Center ดำเนินการ Config firewall Ports

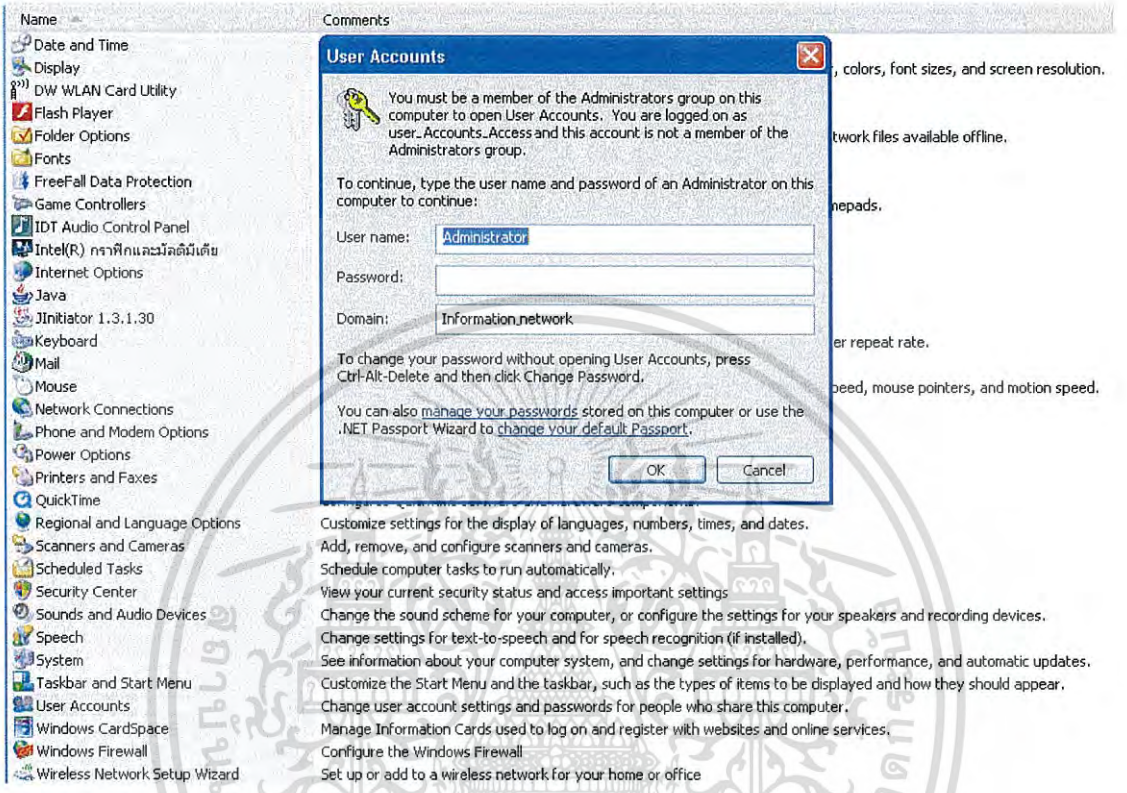
- แจ้ง IP Address ของเครื่องที่ใช้งาน
- Allow TCP/443 on Firewall
- Allow HTTPS access on Forward Web Proxy
- Allow DNS Lookup (TCP/UDP/53) to resolve external DNS record

Firewall Rule	Source Address	Destination Address	Services/Protocol
Allow SIP	<Bank Client's Fixed IP Address>	XXX.XX.X.XXX	TCP/443
Allow Audio/Video	< Bank Client's Fixed IP Address>	XXX.XX.X.XXX	TCP/443, UDP/3478
Allow App Sharing	< Bank Client's Fixed IP Address>	XXX.XX.X.XXX	TCP/443
Allow Lync Web Services	<Bank Client's Fixed IP Address>	XXX.XX.X.XXX	HTTPS/TCP/443

รูปที่ 1.4.7 เอกสารแนบการควบคุมการกำหนดเส้นทางบนเครือข่ายที่สำคัญ

1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

1.5.4 (1) การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) การกำหนดสิทธิระดับระบบปฏิบัติการให้ผู้ใช้งานเป็น User เพื่อป้องกันไม่ได้ผู้ใช้งานติดตั้งโปรแกรมยูทิลิตี้ได้



รูปที่ 1.5.4 เอกสารแนบการกำหนดสิทธิไม่ให้ผู้ใช้งานติดตั้งโปรแกรมยูทิลิตี้

1.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

1.7.1 (1) และ 1.7.2 (1) การทบทวนบัญชีผู้ใช้งานที่ได้รับสิทธิใช้งานอุปกรณ์สื่อสารประเภทพกพาอย่างเหมาะสมและการปฏิบัติงานจากภายนอกองค์กรให้มีความเหมาะสม

รายงานการทบทวนบัญชีผู้ใช้งานได้รับสิทธิใช้งานอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

Mobile Device		
ระดับชั้น: Mobile	รายงานประจำไตรมาส: 1/2557	วันที่ออกรายงาน: 31/01/2557

ส่วนที่ 1: อนุมัติผลการทบทวนบัญชีผู้ใช้งาน

ลายเซ็นผู้ทบทวนบัญชีผู้ใช้งาน (_____) (สังกัดส่วนงาน IT Security) ลงวันที่ 31/01/2557	ลายเซ็นผู้ดูแลระบบ (IT Security) (_____) (สังกัดส่วนงาน IT Security) ลงวันที่ 31/01/2557
ลายเซ็นผู้บริหาร IT Security (_____) (สังกัดส่วนงาน IT Security) ลงวันที่ 31/01/2557	

ส่วนที่ 2: สรุปผลการทบทวนบัญชีผู้ใช้งาน

จำนวนบัญชีผู้ใช้งาน ทั้งหมดในระบบ:	33 บัญชี
จำนวนบัญชีผู้ใช้งาน ที่มีสถานะ Active ในระบบ :	32 บัญชี
รายละเอียด	จากบัญชีผู้ใช้งานที่ได้รับสิทธิสามารถเข้าถึงระบบงานธนาคารผ่านอุปกรณ์พาพาหรืออุปกรณ์สื่อสารเคลื่อนที่ได้ จำนวน 33 ท่าน พบรายละเอียดดังนี้ 1. เป็นผู้บริหารระดับสูง (กรรมการผู้จัดการธนาคาร ผู้ช่วยกรรมการผู้จัดการ และประธานสายงานต่างๆ จำนวน 20 ท่าน ซึ่งมีการร้องขอเข้าใช้งานผ่าน IT Request ทุกท่าน 2. เป็นผู้บริหารระดับกลาง จำนวน 13 ท่าน ซึ่งมีการร้องขอเข้าใช้งานผ่าน IT Request ทุกท่าน โดยมี 1 ท่านได้รับการแจ้งเลียชีวิต ทรัพยากรบุคคลแจ้งเรื่องผ่าน IT Request แล้ว

รูปที่ 1.7.1 เอกสารแนบทบทวนบัญชีผู้ใช้งานที่ได้รับสิทธิ Mobile computing and Teleworking

รายงานการทบทวนบัญชีผู้ใช้งานได้รับสิทธิใช้งานอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

Mobile Device		
ระดับชั้น: Mobile	รายงานประจำไตรมาส: 1/2557	วันที่ออกรายงาน: 31/01/2557

สรุปผลการทบทวนบัญชีผู้ใช้งาน โดยพิจารณาแบ่งตามขอบเขต ดังนี้

1. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ซ้ำกัน หรือ ไม่มีความจำเป็นในการใช้งาน (Redundant User Account)
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ซ้ำกัน หรือ ไม่มีความจำเป็นในการใช้งาน

2. ตรวจสอบและทบทวนบัญชีผู้ใช้งานของพนักงานที่พ้นสภาพพนักงานแล้ว แต่ยังคงมีสถานะ Active อยู่ในระบบ
   ผลการดำเนินงาน: **พบ**บัญชีผู้ใช้งานของพนักงานที่พ้นสภาพพนักงาน แต่ยังคงมีสถานะ Active อยู่ในระบบ จำนวน 1 รายการ (User : Lead Operation) เนื่องจากเสียชีวิต สายทรัพยากรบุคคลรับมอบทรัพย์สินแล้วและทำการ Disable รายการแล้ว ณ วันที่ 31 มกราคม 2557

3. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ไม่กำหนดวันครบอายุของรหัสผ่าน (Password never expired)
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ไม่กำหนดวันครบอายุของรหัสผ่าน

4. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ไม่มีการเข้าใช้งานระบบเป็นเวลามากกว่า 90 วัน
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ไม่มีการเข้าใช้งานระบบเป็นเวลามากกว่า 90 วัน

5. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ไม่สามารถระบุถึงผู้ใช้งานได้ (Unidentified Owner)
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ไม่สามารถระบุถึงผู้ใช้งานได้

6. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ไม่กำหนด Password, มี Password เป็น NULL หรือ Blank Password
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ไม่กำหนด Password หรือ มี Password เป็น Blank Password

7. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่ถูกกำหนดรหัสผ่านมาพร้อมกับระบบสารสนเทศ (Default Password)
   ผลการดำเนินงาน: **ไม่พบ**บัญชีผู้ใช้งานที่ไม่กำหนด Password หรือ มี Password เป็น Blank Password

8. ตรวจสอบและทบทวนบัญชีผู้ใช้งานที่มีการใช้งานผิดปกติ เช่น ยามวิกาล หรือมีการอนุมัติรายการที่ไม่เหมาะสม (เฉพาะกรณีการปฏิบัติงานจากภายนอกสำนักงาน)
   ผลการดำเนินงาน: - (ระดับชั้น Mobile Device ไม่มีรายการดังกล่าว)

รูปที่ 1.7.2 เอกสารแนบรายละเอียดทบทวนบัญชีผู้ใช้งาน Mobile computing and Teleworking

ประวัติผู้เขียน

ชื่อผู้จัดทำโครงการ	นางสาวจิรวณี สิริประภาสวัสดิ์
วันเดือนปีเกิด	12 มีนาคม 2527
สถานที่เกิด	กรุงเทพฯ
ประวัติการศึกษา	
มัธยมศึกษาตอนต้น	โรงเรียนเบญจวรรณศึกษา
มัธยมศึกษาตอนปลาย	โรงเรียนยานนาเวศวิทยาคม
อุดมศึกษา (ปริญญาตรี)	มหาวิทยาลัยราชภัฏสวนสุนันทา
อุดมศึกษา (ปริญญาโท)	สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ประวัติการทำงาน	
พ.ศ.2550-2552	บริษัทเว็บสตาร์ดอทคอม (ไทยแลนด์) จำกัด ตำแหน่งโปรแกรมเมอร์ และนักวิเคราะห์ระบบงาน
พ.ศ.2552-2554	บริษัทเอ็ม บี เค จำกัด (มหาชน) ตำแหน่งผู้ตรวจสอบเทคโนโลยีสารสนเทศ
พ.ศ.2554-2556	ธนาคารเกียรตินาคิน จำกัด (มหาชน) ตำแหน่งผู้ช่วยผู้จัดการตรวจสอบเทคโนโลยีสารสนเทศ