การบริหารความเสี่ยงและการปรับปรุงคุณภาพระบบกู้ยืมเงินเพื่อการศึกษา ตามหลักการโคบิต 5

นายสุภัทร ปกาสิทธิ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
เอกเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2559

Risk Management and Quality Improvement for e-Studentloan System Based on COBIT5

Mr. Supat Pakasith

A Thesis Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Science in Information and Communication Technology

School of Science and Technology

Sukhothai Thammathirat Open University

2016

หัวข้อวิทยานิพนธ์	การบริหารความเสี่ยงและการปรับปรุงคุณภาพระบบกู้ยืมเงินเพื่อการศึกษาตามหลักการโคบิต 5
ชื่อและนามสกุล	นายสุภัทร ปกาสิทธิ์
แขนงวิชา	เทคโนโลยีสารสนเทศและการสื่อสาร
สาขาวิชา	วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
อาจารย์ที่ปรึกษา	1. ผู้ช่วยศาสตราจารย์ ดร. วฤษาย์ ร่มสายหยุด 2. รองศาสตราจารย์ ดร. พันธุ์ปิติ เปี่ยมสง่า

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 25 สิงหาคม 2559

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. วรลักษณ์ วงศ์โดยหวัง ศิริเจริญ)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. วฤษาย์ ร่มสายหยุด)

.....กรรมการ
(รองศาสตราจารย์ ดร. พันธุ์ปิติ เปี่ยมสง่า)

.....ประธานกรรมการบัณฑิตศึกษา
(รองศาสตราจารย์รสลิน ศิริยะพันธุ์)

ชื่อวิทยานิพนธ์ การบริหารความเสี่ยงและการปรับปรุงคุณภาพระบบกู้ยืมเงินเพื่อการศึกษา ตามหลักการโคบิต 5

ผู้วิจัย นายสุภัทร ปกาสิทธิ์ **รหัสนักศึกษา** 2579600053 **ปริญญา** วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร) **อาจารย์ที่ปรึกษา** (1) ผู้ช่วยศาสตราจารย์ ดร. วฤษาย์ ร่มสายหยุด (2) รองศาสตราจารย์ ดร. พันธุ์ปิติ เปี่ยมสง่า **ปีการศึกษา** 2559

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ (1) เพื่อพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนเงินให้กู้ยืมเพื่อการศึกษาเชื่อมโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5 (2) เพื่อพัฒนาระบบสารสนเทศของกองทุนฯ ตามกระบวนการบริหารความเสี่ยงโคบิต 5 และ (3) เพื่อทดสอบความน่าเชื่อถือของแบบจำลอง สถาณการณ์ความเสี่ยงที่พัฒนาขึ้นและประเมินผลสถานการณ์ความเสี่ยงจากข้อมูลจริง

การดำเนินงานวิจัยประกอบด้วย (1) ศึกษาความเสี่ยงกองทุนเพื่อสร้างแบบจำลองความเสี่ยงกองทุน (2) วิเคราะห์ปัจจัยเสี่ยงกองทุน (3) ออกแบบสถานการณ์ความเสี่ยงกองทุนและสถานการณ์อื่นที่เกี่ยวข้องจากการวิเคราะห์ความเสี่ยงกองทุน (4) เพื่อทดสอบกับรูปแบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลความเสี่ยงและกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (Process) แบ่งเป็น กระบวนการกำกับดูแลความเสี่ยง (EDM03) 3 กระบวนการ และ กระบวนการบริหารความเสี่ยง (APO12) 6 กระบวนการ รวม 9 กระบวนการ (5) ทดสอบแบบจำลองสถานการณ์การความเสี่ยงกับรูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 (6) ผลผลิตกระบวนการบริหารความเสี่ยงกองทุนตามหลักการบริหารความเสี่ยงโคบิต 5 และ (7) ประเมินผลสถานการณ์ความเสี่ยงกองทุนที่ดำเนินตามขั้นตอนหลักการโคบิต 5

ผลการวิจัยแสดงให้เห็นว่าการจัดการความเสี่ยงของกองทุนฯ อยู่บนพื้นฐานของ หลักการโคบิต 5 ได้ดำเนินการบนพื้นฐาน ของหลักการโคบิต 5 มีผลความสำเร็จเป็น 0.02% และมีความเชื่อมั่น 95% ใน หลักการโคบิต 5 ในรูปแบบกระบวนการวัดความสามารถ ผลลัพธ์ที่ได้เปรียบเทียบกับธนาคารกสิกรไทยในกระบวนการความเสี่ยงเป็น 67.35% อย่างไรก็ตาม กองทุนฯควรดำเนินกิจกรรมและกระบวนการขึ้นอยู่กับกระบวนการความเสี่ยง ตามหลักการโคบิต 5 ตามระเบียบวิธีวิจัยสำหรับการเพิ่มประสิทธิภาพและบูรณาการการดำเนินงานของกองทุนฯและไอที

คำสำคัญ กองทุนฯ เงินให้กู้ยืมเพื่อการศึกษา โคบิต 5 การบริหารความเสี่ยงโคบิต 5 (กระบวนการ EDM03 และ APO12)

Thesis title: Risk Management and Quality Improvement for e-Studentloan System Based on COBIT5
Researcher: Mr. Supat Pakasith; **ID:** 2579600053;
Degree: Master of Science (Information and Communication Technology);
Thesis advisors: (1) Dr. Walisa Romsaiyud, Assistant Professor;
(2) Dr. Punpiti Piamsa – nga, Associate Professor; **Academic year:** 2016

Abstract

The purpose of the research were to (1) To develop risk scenario modelling of Student Loan Fund (SLF) align with Cobit5 for Risk processes (2) To develop information system based on Cobit5 for Risk processed and (3) To ensure and evaluate risk scenario of SLF based on real data set.

The research process consists of (1) study a SLF's risk for SLF's risk scenario, (2) analysis a SLF's risk factor analysis, (3) design SLF's risk scenario and other related risk scenario from SLF's risk, (4) test a governance and management risk process capability model divided into risk governance process (EDM03) 3 processes and risk management (APO12) 6 processes, (5) test a SLF's risk scenario model with SLF's process capability model, (6) producea SLF's risk process based on COBIT 5, and (7) evaluate SLF's risk scenario operating based on COBIT 5

The research finding showed that; The SLF's risk management based on COBIT 5 was implemented base on COBIT 5 as 0.02% and the confident 95% base on COBIT 5's capability process model. The result compared with Kasikorn Bank that shown a risk process model as 67.35%. However SLF should implement activities and processes based on COBIT 5's risk process according to a research methodology for increasing effectiveness and integrating the SLF's operation and IT.

Keywords: Student Loan Fund (SLF), Cobit5, Cobit5 for Risk (EDM03 & APO12)

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี ด้วยความกรุณาอย่างยิ่งจาก ผู้ช่วยศาสตราจารย์ ดร. วฤษย์ ร่มสายหยุด กรรมการที่ปรึกษาวิทยานิพนธ์ ที่ได้กรุณาให้คำปรึกษาแนะนำ และตรวจสอบแก้ไขข้อบกพร่องต่างๆ เพื่อให้วิทยานิพนธ์ฉบับนี้สมบูรณ์

นอกจากคณาจารย์ทั้งหลายที่ได้ช่วยให้วิทยานิพนธ์ฉบับนี้นอกจากนี้กลุ่มผู้ให้ข้อมูลและเจ้าหน้าที่กองทุนเงินให้กู้ยืมเพื่อการศึกษา นั้นมีความสำคัญอย่างยิ่งที่ทำให้ข้อมูลในงานวิจัยฉบับนี้สมบูรณ์มากขึ้น ต้องขอขอบคุณผู้บริหารกองทุนเงินให้กู้ยืมเพื่อการศึกษา และเจ้าหน้าที่ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา ทุกท่านที่ให้ความร่วมมือเป็นอย่างดีในการให้ข้อมูลแนะนำและอำนวยความสะดวกในการเก็บรวบรวมข้อมูล

ขอขอบคุณผู้มีส่วนเกี่ยวข้องทุกท่านที่คอยช่วยเหลือ ห่วงใย และให้กำลังใจในการจัดทำวิทยานิพนธ์จนสำเร็จ โดยเฉพาะภรรยาที่รักที่เป็นกังวลและตรวจความถูกต้องก่อนนำเสนอทุกครั้ง และท้ายสุดคุณค่าแห่งงานวิทยานิพนธ์ฉบับนี้ขอมอบให้ ทุกท่านที่มีส่วนเกี่ยวข้องกับข้าพเจ้าที่เห็นความสำคัญของการศึกษาและนำไปปรับใช้ต่อให้เกิดคุณประโยชน์ต่อองค์กรต่อไป

สุภัทร ปกาสิทธิ์

สิงหาคม 2559

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

กองทุนเงินให้กู้ยืมเพื่อการศึกษา ใช้ระบบกู้ยืมเงิน (e-Studentloan) เป็นเครื่องมือทางสารสนเทศที่สนับสนุนการดำเนินงานการให้กู้ยืม ที่มีวัตถุประสงค์เพื่อให้กู้ยืมเงินแก่นักเรียนนักศึกษาที่ขาดแคลนทุนทรัพย์เพื่อเป็นค่าเล่าเรียนและค่าใช้จ่ายที่เกี่ยวเนื่องกับการศึกษาโดยให้เงินกู้ยืมตั้งแต่ระดับมัธยมศึกษาตอนปลาย (สายสามัญและสายอาชีพ) จนถึงระดับปริญญาตรีจึงนับเป็นกลไกสำคัญของรัฐบาลที่ให้การสนับสนุนการขยายโอกาสและพัฒนาการศึกษาของประเทศเพื่อให้เยาวชนไทยได้รับการศึกษาที่มีคุณภาพได้มาตรฐานอย่างเท่าเทียมกัน ซึ่งกระบวนการดำเนินงานในปัจจุบันเป็นการให้บริการในการกู้ยืม โดยการดำเนินงานภายในกองทุนมีการใช้ระบบเทคโนโลยีสารสนเทศเพียงเพื่อบันทึกข้อมูลในการดำเนินงานเท่านั้น ในปีงบประมาณปี 2558 กองทุนฯ ดำเนินการให้กู้ยืมเงินเพื่อการศึกษาแก่ผู้กู้ยืมจำนวน 4,702,996 ราย รวมมูลค่า 503,283,072,970.34 บาท โดยมีผู้กู้อยู่ระหว่างการศึกษาและปลอดหนี้รวม 928,307 ราย ประมาณการผู้ครบกำหนดชำระหนี้ประจำปีงบประมาณ 2558 จำนวน 3,224,467 รายมาชำระหนี้แบบปิดบัญชี 507,689 ราย และเสียชีวิต/พิการ 42,533 ราย คิดเป็นเงินต้นครบกำหนดชำระ 141,177,462,592.23 บาท มาชำระเงินคืนเพียง 75,537,391,850 บาท คิดเป็นร้อยละ 53.51 ยังคงมีเงินที่กองทุนฯ ปล่อยกู้ให้กับผู้กู้ยืมที่ต้องบริหารความเสี่ยงอีกประมาณ 400,000,000,000 บาท ซึ่งเป็นเงินงบประมาณที่ได้จะรัฐบาลและจากการชำระภาษีของประชาชน ดังนั้นกองทุนฯ จึงมีความเสี่ยงในระดับสูงมากในการบริหารการดำเนินงานทั้งการให้กู้ยืมและการรับชำระคืนให้เกิดความสมดุลมากที่สุด

สะท้อนให้เห็นว่ากองทุนฯ ขาดกระบวนการนำเทคโนโลยีมาสนับสนุนการดำเนินงานทั้งหมดอย่างมีระบบเพื่อเพิ่มประสิทธิภาพจึงทำให้การบริหาร การดำเนินงานโครงการ และกิจกรรมต่างๆ ของ กองทุน ไม่ก่อให้เกิดประโยชน์สูงสุด โดยกระบวนการดำเนินงานของกองทุนฯ อาจมีความเสี่ยงที่เกิดขึ้นจากกระบวนการดำเนินงานที่ยังไม่ดำเนินการการกำกับดูแลและบริหารความเสี่ยงจากกองทุน ดังนี้

(1) การคัดกรองคุณสมบัติผู้กู้ยืมของสถานศึกษาไม่ครบถ้วน

(2) ข้อมูลการโอนเงินของผู้กู้ยืมอยู่กับ ผู้บริหารบริหารเงินกู้ยืม (กองทุนไม่สามารถบริหารข้อมูลได้ทันที)

(3) การรับชำระเงินคืน (กองทุนให้ผู้บริหารบริหารเงินกู้ยืมดำเนินการ)

(4) การติดตามการรับชำระเงินคืน

ความเสี่ยงที่เกิดขึ้นดังกล่าวข้างต้นส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลของกระบวนการดำเนินงานของกองทุน ได้แก่

(1) ทำให้กองทุนจัดสรรเงินกู้ยืมกับผู้กู้ยืมที่ขาดคุณสมบัติตามที่กองทุนกำหนด

(2) ทำให้เกิดความล่าช้าในการอนุมัติสัญญาการกู้ยืมและโอนเงินล่าช้า

(3) ทำให้กองทุนไม่สามารถบริหารบริหารข้อมูลผู้กู้ที่ครบกำหนดชำระได้เนื่องจากต้องร้องขอข้อมูลจากผู้บริหารบริหารเงินกู้ยืม

(4) ทำให้กองทุนไม่สามารถเฝ้าติดตามสถานะของผู้กู้ยืมได้ต่อเนื่อง เนื่องจากต้องร้องขอข้อมูลจากผู้บริหารบริหารเงินกู้ยืมทุกครั้งที่ต้องการดำเนินการใดๆ กับข้อมูลผู้กู้ยืม

ทั้งนี้กองทุนเงินให้กู้ยืมเพื่อการศึกษา มีระบบ e-Studentloan เป็นระบบเทคโนโลยีสารสนเทศที่ให้บริการกับผู้กู้ยืมและสถานศึกษาซึ่งระบบ e-Studentloan ประกอบด้วย 2 ฟังก์ชันการทำงานหลัก ได้แก่การรับ - ส่ง ข้อมูลและการบันทึกข้อมูลเท่านั้น ซึ่งทำให้ระบบ e-Studentloan ในปัจจุบันขาดการคัดกรองในประเด็นสำคัญได้แก่

(1) ขาดกระบวนการตรวจสอบคุณสมบัติของผู้กู้ยืม (กองทุนมอบหมายให้สถานศึกษาเป็นผู้คัดกรองคุณสมบัติผู้กู้ยืม)

(2) ขาดกระบวนการทำงานด้านการโอนเงินของผู้กู้ยืมอยู่กับผู้บริหารบริหารเงินกู้ยืมแบบอัตโนมัติ(กองทุนไม่สามารถบริหารข้อมูลได้ทันที)

(3) ขาดกระบวนการบริหารบริหารการรับชำระเงินคืน (กองทุนให้ผู้บริหารบริหารเงินกู้ยืมดำเนินการ)

(4) ขาดกระบวนการติดตามการรับชำระเงินคืน

โดยกองทุนต้องพัฒนาปรับปรุงกระบวนการดำเนินงานต่างๆ เพื่อบริหารความเสี่ยงที่เกิดขึ้นโดยสังเขป ได้แก่

(1) พัฒนาระบบงานหรือกระบวนการดำเนินงานในการคัดกรองคุณสมบัติผู้กู้ยืมให้สามารถคัดกรองตามคุณสมบัติที่กองทุนกำหนดได้

(2) กองทุนต้องมีระบบสารสนเทศเพื่อรองรับการบริหารข้อมูลของผู้กู้ยืม เพื่อให้สามารถดำเนินการต่างๆ ได้แก่ อนุมัติสัญญาโดยผู้บริหารกองทุนได้ โอนเงินโดยเจ้าหน้าที่ของกองทุนผู้ได้รับมอบอำนาจแก่ผู้กู้ยืมได้ เรียกดูข้อมูลผู้กู้ได้เมื่อต้องการใช้งาน เป็นต้น

(3) กองทุนต้องปรับเปลี่ยนสภาพแวดล้อมเดิมของกองทุนเพื่อเตรียมความพร้อมในการปรับเปลี่ยนองค์กรให้สามารถดำเนินงานด้านการกำกับดูแลและบริหารบริหารสารสนเทศของกองทุนตามหลักการโคบิต 5

ดังนั้นในงานวิจัยนี้ขอนำเสนอ การเตรียมใช้สถานการณ์ความเสี่ยงกองทุนสำหรับการนำไปปรับใช้กับกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนเชื่อมโยงกับกรอบการดำเนินงานโคบิต 5 ด้วยปัจจัยเอื้อเพื่อนำดำเนินการตามกระบวนการตามหลักการบริหารความเสี่ยงโคบิต (Cobit5 for Risk Enabling Process) เพื่อช่วยสนับสนุนหรือเป็นเครื่องมือให้กองทุน ฯ สามารถเห็นมุมมอง เข้าใจ ประเด็นความเสี่ยงได้ชัดเจน เพื่อกำหนดวางแผน บริหาร และกำหนดผู้รับผิดชอบ บริหารกับความเสี่ยงที่เกิดขึ้นกับกองทุนได้ตรงกับความเสี่ยงที่เกิดขึ้น

2. วัตถุประสงค์การวิจัย

2.1 เพื่อพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนฯ เงินให้กู้ยืมเพื่อการศึกษาเชื่องโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5

2.2 เพื่อพัฒนาระบบสารสนเทศของกองทุนฯ ตามกระบวนการบริหารความเสี่ยงโคบิต 5

2.3 เพื่อทดสอบความน่าเชื่อถือของแบบจำลองสถานการณ์ความเสี่ยงที่พัฒนาขึ้นและประเมินผลสถานการณ์ความเสี่ยงจากข้อมูลจริง

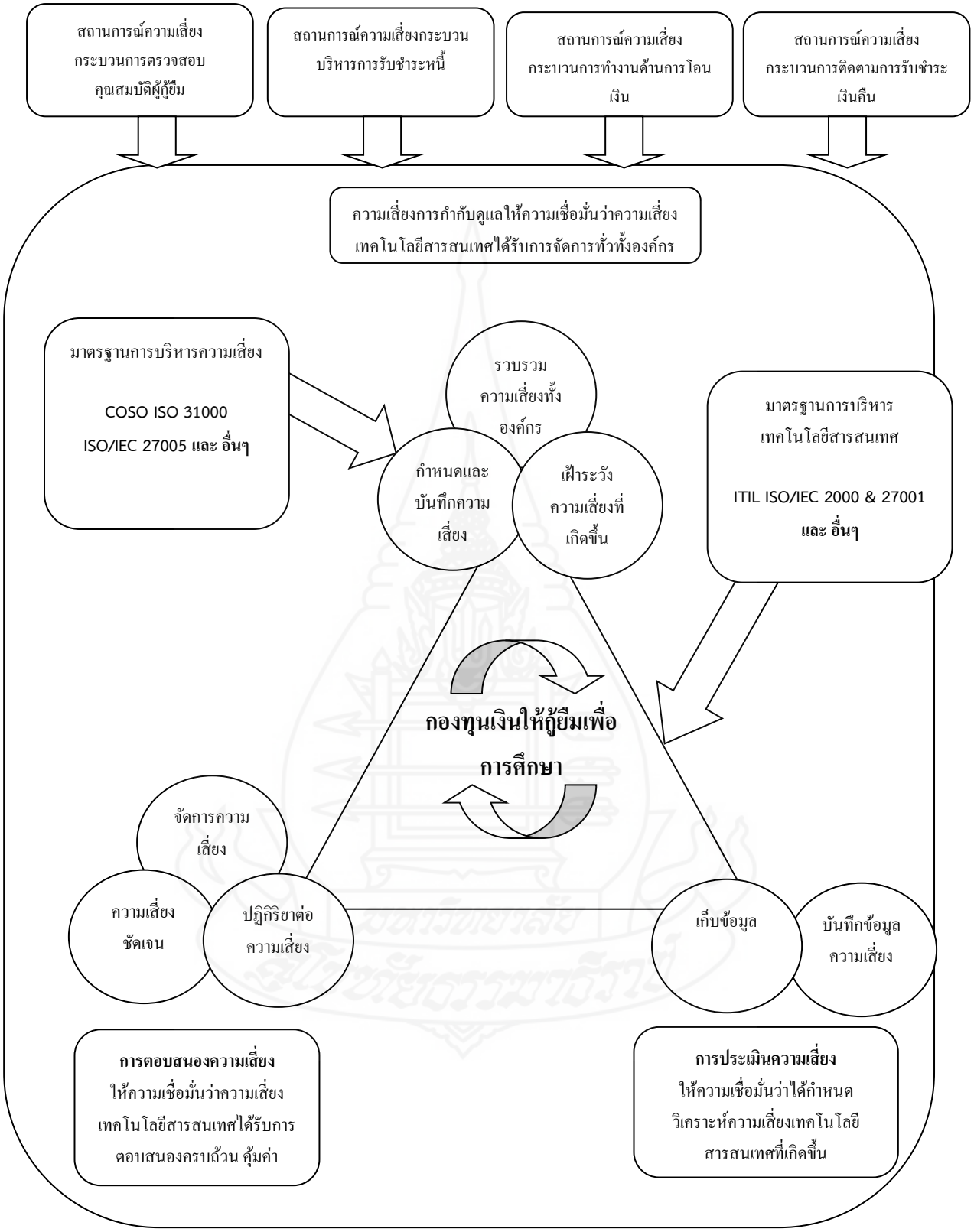
3. ขอบเขตการวิจัย

การวิจัยครั้งนี้ได้กำหนดขอบเขตการศึกษาในการค้นคว้าพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนในเรื่อง (1) กระบวนการตรวจสอบคุณสมบัติของผู้กู้ยืม (2) กระบวนการทำงานด้านการโอนเงิน (3) กระบวนการบริหารบริหารการรับชำระเงินคืน และ (4) กระบวนการติดตามการรับชำระเงินคืน เป็นตัวแปรสถานการณ์ความเสี่ยง ภายใต้กรอบการดำเนินงาน ด้านความเสี่ยงของโคบิต 5 (COBIT 5 for Risk) โดยใช้ข้อมูลการดำเนินงานของกองทุนตาม คู่มือผู้ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา กระบวนการของผู้บริหารบริหารเงินกู้ยืมและกระบวนการดำเนินงานของฝ่ายงานที่

เกี่ยวข้องเพื่อทดสอบแบบจำลองสถานการณ์ความเสี่ยงกองทุนเชื่อมโยงกับกรอบการดำเนินงานด้านความเสี่ยงของโคบิต 5 (COBIT 5 for Risk) เพื่ออธิบายขั้นตอนการบริหารความเสี่ยงกองทุนตามกรอบการดำเนินงานด้านความเสี่ยงของโคบิต 5 (COBIT 5 for Risk: อ้างอิงตามมาตรฐานความเสี่ยง ISO 31000)

4. กรอบแนวคิดการวิจัย

กำหนดสถานการณ์ความเสี่ยงทั้งหมดของกองทุน ได้แก่ (1) สถานการณ์ความเสี่ยงกระบวนการตรวจสอบคุณสมบัติของผู้กู้ยืม (2) สถานการณ์ความเสี่ยงกระบวนการทำงานด้านการโอนเงิน (3) สถานการณ์ความเสี่ยงกระบวนการบริหารการรับชำระเงินคืน และ (4) สถานการณ์ความเสี่ยงกระบวนการติดตามการรับชำระเงินคืน เชื่อมโยงสถานการณ์ความเสี่ยงเข้ากับกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ตามภาพที่ 1.1



ภาพที่ 1.1 กระบวนการบริหารความเสี่ยงโคบิต 5 ของกองทุนฯ

จากภาพที่ 1.1 แสดงสถานการณ์ความเสี่ยงกองทุนเชื่อมกับโมเดลกระบวนการบริหารความเสี่ยงโคบิต 5 ของ กองทุน ประกอบด้วย 5 ส่วนสำคัญได้แก่ (1) การสร้างสถานการณ์ความเสี่ยงของกองทุน ทั่วทั้งองค์กร (2) เชื่อมโยงกับกระบวนการบริหารความเสี่ยงของโคบิต 5 3 องค์ประกอบ โดยมีขั้นตอนดังนี้

(1) ประเมินความเสี่ยงจากสถานการณ์ความเสี่ยงกองทุน

- เก็บข้อมูลความเสี่ยง วิเคราะห์ความเสี่ยง บันทึกข้อมูลความเสี่ยง

(2) ตอบสนองความเสี่ยงจากสถานการณ์ความเสี่ยงกองทุน

- ระบุความเสี่ยงได้ชัดเจน บริหารความเสี่ยง ตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

(3) กำกับดูแลและบริหารบริหารความเสี่ยง

- สั่งการเพื่อบริหารความเสี่ยง ประเมินสถานการณ์ของการบริหารความเสี่ยง เฝ้าติดตามความเสี่ยง

(4) สื่อสาร ให้ความรู้ ความเข้าใจกับเจ้าหน้าที่กองทุน กำหนดความรับผิดชอบในการดำเนินงานเพื่อบริหารบริหารความเสี่ยงกองทุนตามลักษณะหน้าที่ความรับผิดชอบในแต่ละส่วนงาน

(5) นำมาตรฐานการบริหารบริหารความเสี่ยงมาเทียบเคียงกับผลการนำสถานการณ์ความเสี่ยงกองทุนเชื่อมโยงกับกระบวนการบริหารความเสี่ยงของโคบิต 5 และ (5) นำเสนอโมเดลสถานการณ์ความเสี่ยงกับผู้บริหารกองทุน เจ้าหน้าที่ระดับหัวหน้ากลุ่มและผู้มีส่วนเกี่ยวข้องเพื่อสอบถามความพึงพอใจ

5. สมมุติฐานการวิจัย

5.1 สถานการณ์ความเสี่ยงกองทุนที่เชื่องโยงโมเดลกรอบดำเนินงานความเสี่ยงโคบิต 5 สามารถกำหนดทิศทางเพื่อสนับสนุนการบริหารความเสี่ยงของกองทุน

5.2 สถานการณ์ความเสี่ยงกองทุนที่เชื่องโยงโมเดลกรอบดำเนินงานความเสี่ยงโคบิต 5 สามารถกำหนดระดับความเสี่ยงของกองทุน

5.3 กระบวนการบริหารความเสี่ยงของกองทุนตามโมเดลกรอบดำเนินงานความเสี่ยงโคบิต 5 สามารถนำมาใช้ภายใต้สภาวะแวดล้อมของกองทุน

6. นิยามศัพท์

6.1 กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กองทุน) หมายถึง หน่วยงานภาครัฐ มีฐานะเป็นนิติบุคคลกำกับดูแลโดย กระทรวงการคลัง ดำเนินการในลักษณะทุนหมุนเวียน เป็นกลไกสำคัญของรัฐบาลที่ให้การสนับสนุนการขยายโอกาสและพัฒนาการศึกษาของประเทศ เพื่อให้เยาวชนไทยได้รับการศึกษาที่มีคุณภาพได้มาตรฐานเท่าเทียมกัน

6.2 ระบบ e-Studentloan หมายถึง ระบบสารสนเทศเพื่อสนับสนุนกระบวนการให้กู้ยืม

6.3 กระบวนบริหารความเสี่ยงของโคบิต 5 (COBIT for Risk) หมายถึง กรอบการดำเนินงานบริหารความเสี่ยงสารสนเทศ

6.4 ปัจจัยเอื้อเพื่อนำกระบวนการโคบิตไปใช้งาน (Enabling process) หมายถึงองค์ประกอบที่เกื้อหนุนหรือเอื้อประโยชน์ในการนำกระบวนการโคบิตไปใช้งานให้เกิดผลสำเร็จ ประกอบด้วย 7 องค์ประกอบ ได้แก่ (1) หลักการ นโยบาย และกรอบการดำเนินงาน (2) กระบวนการ (3) โครงสร้างองค์กร (4) วัฒนธรรม จริยธรรมและพฤติกรรมขององค์กร (5) สารสนเทศ (6) การบริการโครงสร้างพื้นฐานและโปรแกรมประยุกต์ และ (7) เจ้าหน้าที่ ทักษะและความรู้ความสามารถ

6.5 แบบจำลองสถานการณ์ความเสี่ยงของกองทุน (SLF's Risk scenario) หมายถึง การสร้างสถานการณ์ความเสี่ยงของกองทุนเพื่อเชื่อมโยงกับโมเดลกรอบการบริหารความเสี่ยงโคบิต 5

6.6 กำหนดผู้รับผิดชอบ หมายถึง ระบุเจ้าหน้าที่รับผิดชอบในการดำเนินงานตามกระบวนการต่างๆ ที่โคบิต 5 กำหนด (RACI Charts)

6.7 กระบวนการที่โคบิต 5 กำหนด หมายถึงขั้นตอนการดำเนินงานของกระบวนการต่างๆ ตามคำแนะนำของโคบิต 5

6.8 กำหนดเป้าประสงค์กองทุน หมายถึง การกำหนดเป้าหมายที่ท้าทายของกองทุนเพื่อ สร้างสรรค์ริเริ่ม การดำเนินงานที่ทำให้กองทุนพัฒนาอย่างยั่งยืน

6.9 กำหนดเป้าประสงค์สารสนเทศกองทุน หมายถึง การกำหนดเป้าหมายสารสนเทศที่ท้าทายของกองทุนเพื่อเชื่อมโยง สนับสนุน เป้าประสงค์การพัฒนาการดำเนินงานกองทุน

6.10 กระบวนการบริหารความเสี่ยงกองทุน หมายถึง ขั้นตอนการดำเนินงานบริหารความเสี่ยงของกองทุน

6.11 ทดสอบแบบจำลองสถานการณ์ความเสี่ยง หมายถึง ทดสอบการเชื่อมโยงสถานการณ์ความเสี่ยงกองทุนเข้ากับโมเดลกรอบการดำเนินงานความเสี่ยงของโคบิต 5

6.12 กระบวนการตรวจสอบคุณสมบัติของผู้กู้ยืม หมายถึง ขั้นตอนการคัดกรองคุณสมบัติผู้กู้ยืมตามที่กองทุนกำหนด

6.13 กระบวนการทำงานด้านการโอนเงิน หมายถึง ขั้นตอนการโอนเงินให้กับผู้กู้ยืม

6.14 กระบวนการบริหารการรับชำระเงินคืน หมายถึง ขั้นตอนการดำเนินงานรับชำระเงินคืนจากผู้กู้ยืม

6.15 กระบวนการติดตามการรับชำระเงินคืน หมายถึง ขั้นตอนการติดตามรับชำระเงินคืน

6.16 กรอบการควบคุมภายใน (COSO) หมายถึง กระบวนการปฏิบัติงานที่ถูกกำหนดร่วมกันโดย คณะกรรมการ ผู้บริหารตลอดจนพนักงานขององค์กรทุกระดับชั้น เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า วิธีการหรือการปฏิบัติงานตามที่กำหนดไว้จะทำให้บรรลุวัตถุประสงค์ของการควบคุม

6.17 ระบบการควบคุมภายใน ประกอบด้วย นโยบายและวิธีปฏิบัติงานที่กำหนดขึ้นในองค์กร เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์และเป้าหมายในเรื่องต่อไปนี้

6.17.1 ด้านการดำเนินงาน (Operation) โดยมุ่งหมายให้การปฏิบัติงานเกิดประสิทธิภาพ ประสิทธิผล และคุ้มค่า ด้วยการกำกับการใช้ทรัพยากรทุกประเภทให้เป็นไปอย่างมีประสิทธิภาพ บรรลุเป้าหมายที่ผู้บริหารกำหนดไว้ และให้ปลอดจากการกระทำทุจริตของพนักงาน หรือผู้บริหาร และหากมีความเสียหายเกิดขึ้นก็ช่วยให้ทราบถึงความเสียหายนั้นได้โดยเร็วที่สุด

6.17.2 ด้านการรายงานทางการเงิน (Financial Reporting) รายงานทางการเงินหรืองบการเงินไม่ว่าจะเป็นรายงานที่ใช้ภายในหรือภายนอกองค์กร ต่างต้องมีความเชื่อถือได้และทันเวลา มีคุณภาพเหมาะสมสำหรับการนำไปใช้เป็นข้อมูลประกอบการพิจารณา ตัดสินใจทางธุรกิจของนักบริหาร เจ้าหนี้ ผู้ถือหุ้น และผู้ลงทุนทั่วไป

6.17.3 ด้านการปฏิบัติให้เป็นไปตาม กฎ ระเบียบ และนโยบาย (Compliance with Application Laws and Regulations) การปฏิบัติงานหรือดำเนินธุรกิจให้สอดคล้อง หรือเป็นไปตามบทบัญญัติ ข้อกำหนดของกฎหมาย นโยบาย ข้อบังคับ ระเบียบที่เกี่ยวข้องกับการปฏิบัติงาน หรือการดำเนินธุรกิจนั้น เพื่อป้องกันมิให้เกิดผลเสียหายใดๆ จากการละเว้นการปฏิบัติให้เป็นไปตามกฎระเบียบเหล่านั้น

6.18 มาตรฐานการบริหารความเสี่ยงด้านความปลอดภัยสารสนเทศ (ISO/IEC 27005) หมายถึง คำแนะนำสำหรับการบริหารความเสี่ยงด้านความปลอดภัยสารสนเทศและสนับสนุนมาตรฐานการรักษาความปลอดภัยสารสนเทศด้านการปฏิบัติงานทางเทคนิค

6.19 ITIL V3/ISO/IEC 20000 หมายถึง กรอบการดำเนินงานการบริหารการให้บริการสารสนเทศขององค์กร ประกอบด้วย 5 องค์ประกอบได้แก่

6.19.1 Service Strategy (Core of ITIL V3) (เป็นกลยุทธ์ในด้านบริการเป็นการกำหนดแนวทางโดยให้หลักไว้ว่า Service Management จะเป็นพื้นฐานในการกำหนดและบริหารนโยบายแนวทางปฏิบัติ และกระบวนการในการบริหารการบริการอย่างครบวงจร

6.19.2 Service Design เน้นการออกแบบกิจกรรมที่จะเกิดขึ้น ในกระบวนการให้บริการรวมทั้ง การพัฒนากลยุทธ์และวิธีการบริหารระบบบริการ โดยมีกุญแจหลักอยู่ที่ Availability Management หรือความพร้อมที่จะให้บริการ Capacity Management หรือขีดความสามารถในการให้บริการอย่างรวดเร็วและมีประสิทธิภาพ รวมทั้ง Continuity Management หรือความสามารถในการให้บริการที่ต่อเนื่อง และ การบริหาร (Security Management) หรือการบริหารระบบรักษาความปลอดภัย

6.19.3 Service Transition เน้นที่การดำเนินการเพื่อให้ได้ผลลัพธ์ของการบริการที่ดีที่สุดเป็นบริการที่ส่งมอบเพื่อนำไปใช้ในระบบปฏิบัติงาน การรับข้อมูลจาก Service Design การส่งมอบสถานการณ์ดำเนินงานในทุกรายการเพื่อให้ระบบปฏิบัติการทำงานได้อย่างต่อเนื่อง โดยมีกุญแจหลักของ Service Transition คือ Change Management Configuration Management Release Management และ Service Knowledge Management

6.19.4 Service Operation เน้นไปทางด้านกิจกรรมที่จำเป็นต่อการปฏิบัติงานเพื่อให้บรรลุผลสำเร็จในการดูแลรักษาหน้าที่การทำงานหรือบริการ ที่เป็นไปตามข้อตกลง ว่า ด้วย พันธะสัญญาบริการ) Service Level Agreement (ที่มีต่อลูกค้า กุญแจหลัก Service Operation คือ Incident Management, Problem Management และ Request Fulfillment และ Event Management

6.19.5 Continual Service Improvement เน้นที่ขีดความสามารถที่ทำให้เกิดขีดความสามารถในการปรับปรุงการให้บริการที่มีคุณภาพอยู่แล้ว ให้มีความต่อเนื่อง กุญแจหลักอยู่ที่ Service Reporting Service Measurement และ Service Level Management

6.20 มาตรฐานการรักษาความปลอดภัยสารสนเทศ (ISO/IEC 27001) หมายถึง มาตรฐานด้านการระบบการบริหารความปลอดภัยของข้อมูลสารสนเทศพอความปลอดภัยได้อย่างมีระบบและเพียงเหมาะสมต่อการดำเนินธุรกิจขององค์กร

6.21 การกำกับดูแลความเสี่ยง หมายถึง การเฝ้าติดตาม 2 องค์ประกอบของความเสี่ยง ได้แก่ (1) ความเสี่ยง (Risk) คือ เหตุการณ์ที่จะมีผลกระทบในเชิงลบ (Negative Effect) ซึ่งทำให้องค์กรไม่บรรลุวัตถุประสงค์และสร้างความเสียหายให้กับองค์กร เช่น สินค้าที่ผลิตไม่ได้คุณภาพ ลูกค้าไม่พอใจในสินค้าและบริการ คู่แข่งรายใหม่ พนักงานทุจริต และ (2) โอกาส (Opportunity) หมายถึง เหตุการณ์ที่จะมีผลกระทบในเชิงบวก (Positive Effect) ซึ่งผู้บริหารควรได้นำไปพิจารณาในการกำหนดกลยุทธ์เพื่อนำไปสู่การปฏิบัติให้เกิดเหตุการณ์ที่ต้องการ เช่น การผลิตสินค้าที่มีคุณภาพ

6.22 ประเมินความเสี่ยง หมายถึง การกำหนดเหตุการณ์ความเสี่ยง กำหนดโอกาสการเกิดขึ้น กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยง

6.23 ตอบสนองความเสี่ยง หมายถึง การดำเนินการต่างๆ เพื่อที่จะบริหารกับความเสี่ยงที่เกิดขึ้น ได้แก่ จัดลำดับความเสี่ยงจากสูง-ต่ำ วางแผนการบริหารความเสี่ยง เป็นต้น

7. ประโยชน์ที่ได้รับ

7.1 กองทุนได้มุมมองความเสี่ยงที่เกี่ยวข้องกับสารสนเทศในปัจจุบันและอนาคตอันใกล้อย่างชัดเจน

7.2 กองทุนสามารถนำผลลัพธ์ของสถานการณ์ความเสี่ยงกองทุนที่เชื่อมโยงกรอบการดำเนินงานความเสี่ยงของโคบิต 5 เป็นแนวทางในการบริหารความเสี่ยงสารสนเทศของกองทุน

7.3 กองทุนสามารถจัดสรรงบประมาณเพื่อการลงทุนด้านเทคโนโลยีสารสนเทศเพื่อบริหารบริหารระบบควบคุมภายในของกระบวนการดำเนินงานต่างๆ ของกองทุนได้ประโยชน์สูงสุด

7.4 กองทุนสามารถรวบรวมความเสี่ยงต่างๆ ที่เกิดขึ้นทั้งหมดและสร้างกฎระเบียบเพื่อบริหารกับความเสี่ยงกองทุนที่เกิดขึ้นได้

7.5 ลงทุนมีความสัมพันธ์ระหว่างเจ้าหน้าที่ที่ดีขึ้นเนื่องจากมีการสื่อสารของข้อมูลความเสี่ยงกองทุนในทิศทางเดียวกันทั่วทั้งองค์กร

7.6 ผู้บริหารกองทุนสามารถประเมินผลการดำเนินแก่ผู้ดำเนินงานบริหารความเสี่ยงของกองทุนเพื่อให้รางวัลหรือเลื่อนตำแหน่งอย่างเปิดเผย

7.7 กองทุนสามารถจัดประเภทของความเสี่ยงต่างๆ ที่เกิดขึ้นกับกองทุนได้ชัดเจนเข้าใจง่าย

บทที่ 2
ทบทวนวรรณกรรม

การวิจัยครั้งนี้ได้ทบทวนวรรณกรรมและการวิจัยต่างๆ ที่เกี่ยวข้องๆ ไว้ 3 ประเด็น ได้แก่ (1) กองทุนเงินให้กู้ยืมเพื่อการศึกษา (2) แนวคิดกรอบการดำเนินงานของโคบิต 5 และ (3) แนวคิดกรอบการดำเนินงานความเสี่ยงของโคบิต 5

1. กองทุนเงินให้กู้ยืมเพื่อการศึกษา

1.1 ความเป็นมาและภารกิจตามกฎหมายจัดตั้งหน่วยงาน

กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.) จัดตั้งขึ้นตามมติคณะรัฐมนตรี เมื่อวันที่ 28 มีนาคม พ.ศ. 2538 และมติคณะรัฐมนตรีเมื่อวันที่ 16 มกราคม พ.ศ. 2539 ให้เริ่มดำเนินการกองทุนในลักษณะเงินทุนหมุนเวียนตามนัยมาตรา 12 แห่งพระราชบัญญัติเงินคงคลัง พ.ศ. 2491 ต่อมารัฐบาลได้พิจารณาเห็นความสำคัญของกองทุนเงินให้กู้ยืมเพื่อการศึกษามากขึ้น จึงได้มีการประกาศใช้พระราชบัญญัติกองทุนเงินให้กู้ยืมเพื่อการศึกษา พ.ศ. 2541 มีผลให้กองทุนเงินให้กู้ยืมเพื่อการศึกษามีฐานะเป็นนิติบุคคล โดยอยู่ในการกำกับดูแลของกระทรวงการคลัง กองทุนนับเป็นกลไกสำคัญของรัฐบาลที่ให้การสนับสนุนการขยายโอกาสและพัฒนาการศึกษาของประเทศ เพื่อให้เยาวชนไทยได้รับการศึกษาที่มีคุณภาพได้มาตรฐานอย่างเท่าเทียมกัน

ภารกิจตามกฎหมายจัดตั้งหน่วยงาน ให้กู้ยืมเงินแก่นักเรียนหรือนักศึกษาที่ขาดแคลนทุนทรัพย์ เพื่อเป็นค่าเล่าเรียน ค่าใช้จ่ายเกี่ยวเนื่องกับการศึกษา และค่าใช้จ่ายที่จำเป็นในการครองชีพระหว่างการศึกษา (พระราชบัญญัติกองทุนเงินให้กู้ยืมเพื่อการศึกษา พ.ศ.2541)

กองทุนเงินให้กู้ยืมเพื่อการศึกษาใช้ระบบกู้ยืมเงิน (e-Studentloan) เป็นเครื่องมือทางสารสนเทศที่สนับสนุนการดำเนินงานการให้กู้ยืม ที่มีวัตถุประสงค์เพื่อให้กู้ยืมเงินแก่นักเรียนนักศึกษาที่ขาดแคลนทุนทรัพย์เพื่อเป็นค่าเล่าเรียนและค่าใช้จ่ายที่เกี่ยวเนื่องกับการศึกษาโดยให้เงินกู้ยืมตั้งแต่ระดับมัธยมศึกษาตอนปลาย (สายสามัญและสายอาชีพ) จนถึงระดับปริญญาตรีจึงนับเป็นกลไกสำคัญของรัฐบาลที่ให้การสนับสนุนการขยายโอกาสและพัฒนาการศึกษาของประเทศเพื่อให้เยาวชนไทยได้รับการศึกษาที่มีคุณภาพได้มาตรฐานอย่างเท่าเทียมกัน ซึ่งกระบวนการดำเนินงานในปัจจุบันเป็นการให้บริการในการกู้ยืมโดยการดำเนินงานภายในกองทุนมีการใช้ระบบเทคโนโลยี

สารสนเทศเพียงเพื่อบันทึกข้อมูลในการดำเนินงานเท่านั้นในปีงบประมาณปี 2558 กองทุนฯ ดำเนินการให้กู้ยืมเงินเพื่อการศึกษาแก่ผู้กู้ยืมจำนวน 4,702,996 ราย รวมมูลค่า 503,283,072,970.34 บาท โดยมีผู้กู้อยู่ระหว่างการศึกษาและปลอดหนี้รวม 928,307 ราย ประมาณการผู้ครบกำหนดชำระหนี้ประจำปีงบประมาณ 2558 จำนวน 3,224,467 รายมาชำระหนี้แบบปิดบัญชี 507,689 ราย และเสียชีวิต/พิการ 42,533 ราย คิดเป็นเงินต้นครบกำหนดชำระ 141,177,462,592.23 บาท มาชำระเงินคืนเพียง 75,537,391,850 บาท คิดเป็นร้อยละ 53.51 ยังคงมีเงินที่กองทุนฯ ปล่อยกู้ให้กับผู้กู้ยืมที่ต้องบริหารความเสี่ยงอีกประมาณ 400,000,000,000 บาท ซึ่งเป็นเงินงบประมาณที่ได้จะรัฐบาลและจากการชำระภาษีของประชาชน ดังนั้นกองทุนฯ จึงมีความเสี่ยงในระดับสูงมากในการบริหารการดำเนินงานทั้งการให้กู้ยืมและการรับชำระคืนให้เกิดความสมดุลมากที่สุด

1.2 วิสัยทัศน์ พันธกิจ

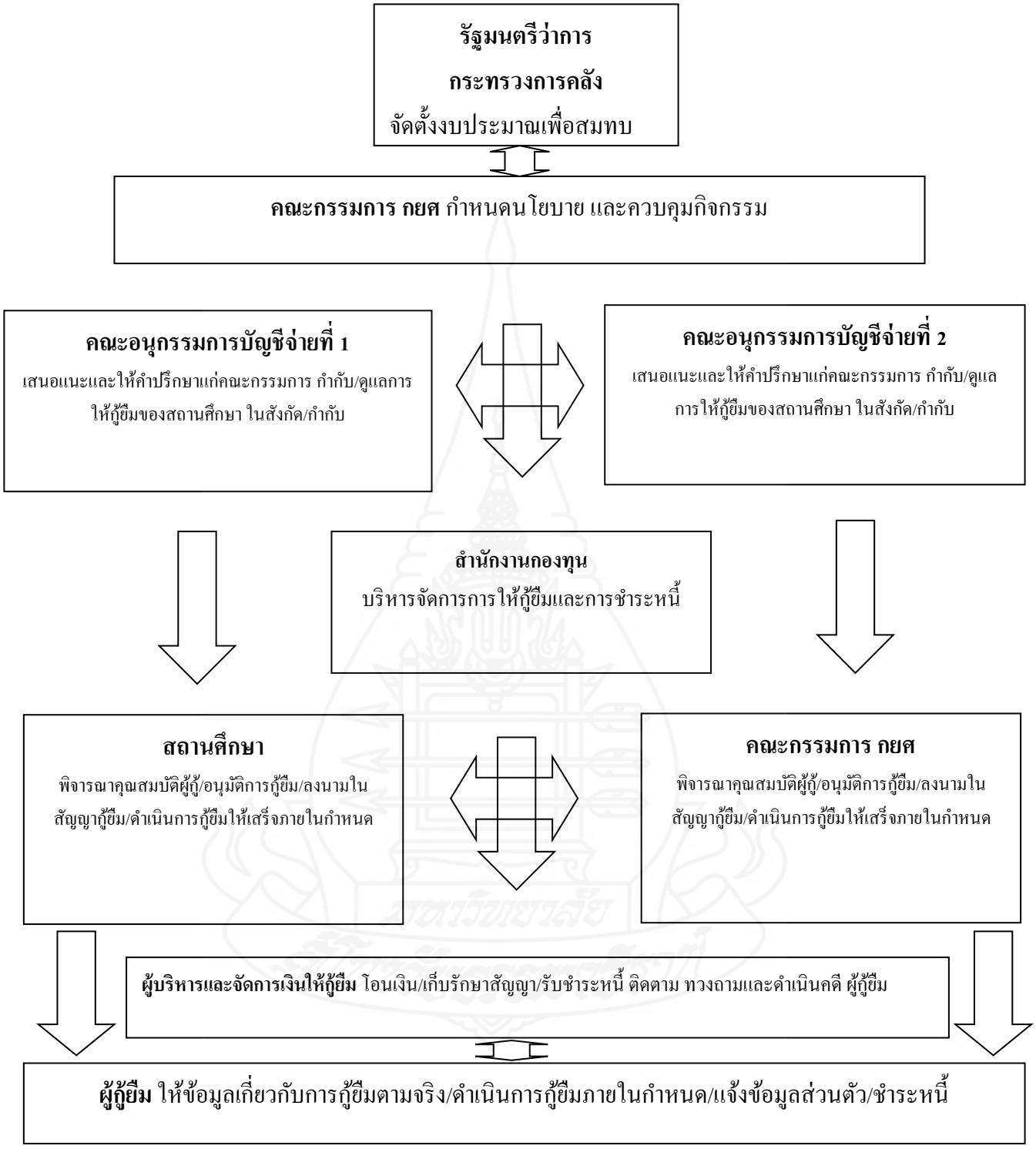
วิสัยทัศน์

“เป็นองค์การที่ให้โอกาสทางการศึกษา เพื่อพัฒนาสังคมไทยให้ยั่งยืน”

พันธกิจ

1.2.1 ให้กู้ยืมกับนักเรียน นักศึกษาที่ขาดแคลนทุนทรัพย์ หรือศึกษาในสาขาที่เป็นความต้องการหลักและมีความจำเป็นต่อการพัฒนาประเทศ

1.2.2 การพัฒนาองค์การสู่ความเป็นเลิศด้านการให้บริหารโดยใช้หลักการบริหารจัดการที่ดี



ภาพที่ 2.1 แสดงโครงสร้างการบริหารงานกองทุนเงินให้กู้ยืมเงินเพื่อการศึกษา
(คู่มือผู้ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา 2558)

จากภาพที่ 2.1 แสดงคำอธิบายต่างๆ ดังต่อไปนี้

1.3 โครงสร้างและอำนาจหน้าที่

พระราชบัญญัติกองทุนเงินให้กู้ยืมเพื่อการศึกษา พ.ศ. 2541 กำหนดให้กองทุนมีคณะกรรมการกองทุนเงินให้กู้ยืมเพื่อการศึกษา ผู้จัดการและคณะอนุกรรม ซึ่งมีอำนาจหน้าที่ดังต่อไปนี้

1.3.1 คณะกรรมการกองทุนเงินให้กู้ยืมเพื่อการศึกษา

อำนาจและหน้าที่ของคณะกรรมการกองทุนเงินให้กู้ยืมเพื่อการศึกษา (มาตรา 18) (กำหนดหน้าที่และความรับผิดชอบ ตามตารางหน้าที่ความรับผิดชอบการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 ในวิธีการดำเนินวิจัย) กำหนดนโยบาย และควบคุมดูแลกิจการของกองทุนให้เป็นไปตามวัตถุประสงค์

แต่งตั้งตามมาตรา 14 ซึ่งประกอบด้วย (1) ปลัดกระทรวงการคลัง เป็นประธานกรรมการ (2) ปลัดกระทรวงศึกษาธิการและเลขาธิการคณะกรรมการการอุดมศึกษา เป็นรองประธานกรรมการ (3) ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง (4) นายกสมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทยและนายกสมาคมสมาพันธ์การศึกษาเอกชนแห่งประเทศไทยเป็นกรรมการ และ (5) กรรมการอื่นอีกไม่เกิน 5 คน ซึ่งรัฐมนตรีแต่งตั้ง โดยในจำนวนนี้อย่างน้อยต้องเป็นผู้ทรงคุณวุฒิด้านเทคโนโลยีสารสนเทศ การเงินหรือการบัญชีหรือกฎหมายด้านละ 1 คน (6) อธิบดีกรมบัญชีกลางเป็นกรรมการและเลขานุการ (7) ผู้จัดการ เป็นกรรมการและผู้ช่วยเลขานุการ ในกรณีจำเป็น ประธานกรรมการจะแต่งตั้งผู้ช่วยเลขานุการเพิ่มขึ้นอีกคนหนึ่งก็ได้

1) ติดตามประเมินผลการดำเนินกิจการของกองทุน และจัดทำรายงานประจำปีเพื่อแพร่ให้ประชาชนทราบ

2) ศึกษาวิเคราะห์และประเมินความต้องการการกู้ยืมเงินของนักเรียน หรือนักศึกษาทั้งในปัจจุบันและอนาคต และเสนอแนะต่อรัฐมนตรีเพื่อดำเนินการจัดตั้งงบประมาณเพื่อสมทบกองทุนตามมาตรา 6 วรรคสอง

3) พิจารณาจัดสรรเงินเพื่อโอนเข้าบัญชีจ่ายที่หนึ่ง บัญชีจ่ายที่สอง และบัญชีจ่ายตามมาตรา 34

4) พิจารณางบประมาณรายจ่ายประจำปีสำหรับการดำเนินการและการบริหารงานของกองทุน

5) กำหนดข้อบังคับเกี่ยวกับการบริหารงานบุคคล การเงิน การพัสดุ การบัญชี การตรวจสอบและสอบบัญชีภายใน และข้อบังคับอื่นที่จำเป็นในการดำเนินการและบริหารงานของกองทุน

6) กำหนดระเบียบ หลักเกณฑ์ และเงื่อนไข เกี่ยวกับการให้นักเรียนหรือนักศึกษากู้ยืมเงินและการชำระคืนเงินกู้ยืม

7) ให้นักเรียน หรือนักศึกษากู้ยืมเงินเพื่อการศึกษาจากกองทุน

8) ประชาสัมพันธ์ให้บุคคลทั่วไปได้เข้าใจถึงวัตถุประสงค์ของกองทุน และคุณค่าของกองทุน

9) ดำเนินการคัดเลือกและทำสัญญาจ้างหรือมีมติเลิกจ้างผู้จัดการและผู้บริหารและจัดการเงินให้กู้ยืม

10) ปฏิบัติงานอื่นใดตามที่กำหนดไว้ในพระราชบัญญัตินี้ หรือเพื่อให้เป็นไปตามวัตถุประสงค์ของกองทุน

คณะกรรมการอาจมอบอำนาจของคณะกรรมการตาม (2) (3) (8) (9) และ (11) เฉพาะในส่วนที่ไม่เกี่ยวกับการกำหนดหลักเกณฑ์ วิธีการ หรือเงื่อนไข ให้ผู้จัดการหรือผู้บริหารและจัดการเงินให้กู้ยืมหรือบุคคลอื่นใดเพื่อกระทำการแทนคณะกรรมการก็ได้

1.3.2 ผู้จัดการ

ตามมาตรา 21 และมาตรา 22 กำหนดให้กองทุนจ้างผู้จัดการคนหนึ่ง ซึ่งต้องเป็นผู้ซึ่งมีความรู้และความเชี่ยวชาญในด้านการบริหารและจัดการ ทั้งต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม

1.3.3 คณะอนุกรรมการบัญชีจ่ายที่หนึ่ง

แต่งตั้ง ตามมาตรา 30 ประกอบด้วย (1) ปลัดกระทรวงศึกษาธิการเป็นประธานอนุกรรมการ เลขาธิการคณะกรรมการการศึกษาขั้นพื้นฐาน (2) เลขาธิการคณะกรรมการการอุดมศึกษา (3) อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคล (4) เลขาธิการคณะกรรมการอาชีวศึกษา (5) ผู้แทนกรมบัญชีกลาง (6) ผู้จัดการ (7) เลขานุการคณะอนุกรรมการบัญชีจ่ายที่สอง และ (8) บุคคลอื่นซึ่งคณะกรรมการแต่งตั้งอีกไม่เกิน 5 คน เป็นอนุกรรมการ

ให้ผู้ช่วยปลัดกระทรวงศึกษาธิการซึ่งปลัดกระทรวงศึกษาธิการมอบหมายคนหนึ่งเป็นอนุกรรมการและเลขานุการ และผู้อำนวยการสำนักนโยบายและแผนการศึกษา ศาสนาและวัฒนธรรม สำนักงานปลัดกระทรวงศึกษาธิการ เป็นอนุกรรมการและผู้ช่วยเลขานุการ

ในกรณีจำเป็น ประธานอนุกรรมการบัญชีจ่ายที่หนึ่งจะแต่งตั้งผู้ช่วยเลขานุการเพิ่มขึ้นอีกคนหนึ่งก็ได้

หน้าที่ของอนุกรรมการบัญชีจ่ายที่หนึ่ง (ตามมาตรา 31)

1) เสนอแนะและให้คำปรึกษาแก่คณะกรรมการในการปฏิบัติหน้าที่ตามมาตรา 18

2) กำกับดูแลการให้กู้ยืมแก่นักเรียนหรือนักศึกษาในโรงเรียน สถานศึกษา หรือสถาบันการศึกษาที่อยู่ในสังกัด ควบคุม หรือกำกับดูแลของกระทรวงศึกษาธิการ หรือโรงเรียน สถานศึกษา หรือสถาบันการศึกษาที่อยู่ในสังกัด ควบคุม หรือกำกับดูแลของส่วนราชการอื่นที่ไม่ใช่สำนักงานคณะกรรมการการอุดมศึกษา ให้เป็นไปตาม นโยบาย ระเบียบและข้อบังคับที่คณะกรรมการกำหนด

3) กำกับดูแลและติดตามการปฏิบัติงานของผู้บริหารและจัดการเงินให้กู้ยืมเฉพาะในส่วนที่เกี่ยวกับบัญชีจ่ายที่หนึ่ง

4) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการมอบหมาย

1.3.4 คณะอนุกรรมการบัญชีจ่ายที่สอง

แต่งตั้งตามมาตรา 32 ประกอบด้วย (1) เลขาธิการคณะกรรมการการอุดมศึกษา เป็นประธานอนุกรรมการ (2) ผู้แทนจากโรงเรียน สถานศึกษา หรือสถาบันการศึกษาที่สำนักงานคณะกรรมการการอุดมศึกษาแต่งตั้งจำนวน 4 คน (3) ผู้แทนกรมบัญชีกลาง (4) ผู้จัดการ (5) เลขานุการอนุกรรมการบัญชีจ่ายที่หนึ่ง และ (6) บุคคลอื่นซึ่งคณะกรรมการแต่งตั้งอีกไม่เกิน 5 คน เป็นอนุกรรมการ

ให้ผู้ช่วยเลขาธิการคณะกรรมการการอุดมศึกษา ซึ่งเลขาธิการคณะกรรมการการอุดมศึกษามอบหมายคนหนึ่ง เป็นอนุกรรมการและเลขานุการ และผู้อำนวยการสำนักส่งเสริมและพัฒนาศักยภาพนักศึกษา สำนักงานคณะกรรมการการอุดมศึกษา เป็นอนุกรรมการและผู้ช่วยเลขานุการ

ในกรณีจำเป็น ประธานอนุกรรมการบัญชีจ่ายที่สองจะแต่งตั้งผู้ช่วยเลขานุการเพิ่มขึ้นอีกคนหนึ่งก็ได้

หน้าที่ของคณะกรรมการบัญชีจ่ายที่สอง (ตามมาตรา 33)

1) เสนอแนะและให้คำปรึกษาแก่คณะกรรมการในการปฏิบัติหน้าที่ตามมาตรา 18

2) กำกับดูแลการให้กู้ยืมเงินแก่นักเรียน หรือนักศึกษาในโรงเรียน สถานศึกษา หรือสถาบันการศึกษาที่อยู่ในสังกัด ควบคุม หรือกำกับดูแลของสำนักงานคณะกรรมการการอุดมศึกษา ให้เป็นไปตามนโยบายของคณะกรรมการ

3) กำกับดูแลและติดตามการปฏิบัติงานของผู้บริหารและจัดการเงินให้กู้ยืมเฉพาะในส่วนที่เกี่ยวข้องกับบัญชีจ่ายที่สอง

4) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการมอบมาย

1.3.5 ผู้บริหารและจัดการเงินให้กู้ยืม

ตามมาตรา 37 ให้คณะกรรมการจ้างบุคคลเพื่อทำหน้าที่รับผิดชอบเป็นผู้บริหารและจัดการเงินให้กู้ยืม โดยหลักเกณฑ์ เงื่อนไข และวิธีการในการคัดเลือก รวมตลอดทั้งคุณสมบัติของผู้บริหารและจัดการเงินให้กู้ยืม ให้เป็นไปตามคณะกรรมการกำหนด

ในปัจจุบัน คณะกรรมการได้จ้าง บมจ.ธนาคารกรุงไทย (KTB) และธนาคารอิสลามแห่งประเทศไทย (IBANK) เป็นผู้บริหารและจัดการเงินให้กู้ยืม

หน้าที่และความรับผิดชอบของผู้บริหารและจัดการเงินให้กู้ยืม (มาตรา 38)

นอกจากหน้าที่และความรับผิดชอบที่กำหนดในสัญญาจ้างแล้ว ผู้บริหารและจัดการเงินให้กู้ยืมมีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

1) ประชาสัมพันธ์ให้ประชาชนทั่วไปได้ทราบถึงนโยบาย ระเบียบ วิธีการในการกู้ยืมเงิน

2) แนะนำ และอำนวยความสะดวกแก่นักเรียน หรือนักศึกษา และสถานศึกษาที่เกี่ยวข้องในการดำเนินการกู้ยืมเงิน

3) เบิกจ่ายเงินกู้ และดำเนินการจัดส่งให้แก่ผู้กู้ยืมเงิน รวมตลอดทั้งเก็บรักษาเอกสารหลักฐานที่เกี่ยวข้อง

4) แจ้งจำนวนหนี้ และสถานะของหนี้ให้ผู้ที่เกี่ยวข้องทราบ

5) รับชำระหนี้เงินกู้ ติดตามทวงถาม และดำเนินคดีเพื่อบังคับชำระหนี้เงินกู้

6) จัดทำรายงานการดำเนินงานให้กู้ยืมเงินเสนอต่อคณะกรรมการ

7) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการมอบหมาย

1.4 งานวิจัยที่เกี่ยวข้องกับกองทุนเงินให้กู้ยืมเพื่อการศึกษา

ทั้งนี้จากการศึกษา ดร.อมรา ติรศรีวัฒน์ (2559) สรุป ปัญหาและแนวทางในการแก้ไข การผิดนัดชำระเงินกู้ยืมเพื่อการศึกษาในประเทศไทย ว่า ผู้กู้ยืมขาดจรรยาบรรณในการชำระเงินคืนให้กับ กยศ อาจเกิดจากสาเหตุปัญหาทางด้านการเงิน เนื่องจากไม่มีงานทำจึงไม่สามารถหาเงินมาชำระคืนได้ รวมทั้งสถานศึกษาที่เกี่ยวข้องในกระบวนการกู้ยืมไม่ตรงไปตรงมาและไม่ปฏิบัติตามกฎ ระเบียบตามที่ กยศ กำหนด สถานศึกษาให้ความสนใจในประโยชน์จากเงินกู้ยืมที่จะได้จาก กยศ มากกว่าให้ความสนใจที่จะได้นักเรียน นักศึกษา ที่มีคุณภาพ ได้เรียนตามสาขาที่ต้อง และเมื่อศึกษาจบหลักสูตรแล้วไม่ได้รับการจ้างงานจากนายจ้าง ในด้านข้อมูลผู้กู้ยืม ขาดการปรับปรุงจากสถานศึกษาเนื่องจากขาดฐานข้อมูลที่เป็นระบบนำไปสู่ปัญหาของการติดตามและขาดการสื่อสาร รวมทั้ง หลักเกณฑ์ นโยบายการจัดสรรและการกระจายเงินกู้ของ กยศ ขาดประสิทธิภาพ อีกทั้งระบบชำระเงินคืนยังขาดความสมบูรณ์ จากสาเหตุดังกล่าวทำให้การดำเนินงานของกองทุนฯ

ไม่เกิดประสิทธิภาพและประสิทธิผลตามวัตถุประสงค์ของกองทุนฯ เนื่องจากกองทุนฯ ไม่ได้ดำเนินการบริหารความเสี่ยงเพื่อระบุสาเหตุของสิ่งต่างๆ ที่เกิดขึ้นเพื่อหาทางแก้ไขปรับปรุงข้อบกพร่องต่างๆ ที่เกิดขึ้นตามกรณีศึกษาข้างต้น โดยในงานวิจัยนี้นำข้อบกพร่องจากกรณีศึกษาข้างต้น (ปัจจัยเสี่ยงต่างๆ ของกองทุนฯ) มาเป็นตัวกำหนดปัจจัยเสี่ยงที่ยังคงมีอยู่ (ความเสี่ยงที่เหลืออยู่) เพื่อเป็นข้อมูลความเสี่ยง (ข้อมูลตั้งต้น) เข้าสู่กระบวนการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 ที่พัฒนาขึ้นในงานวิจัยนี้

นอกจากนี้ สุประพล พาพิโพธิ์ (2557) และอมรา ตันประวัติ (2544) สรุป ปัญหาการค้างชำระหนี้กองทุนเงินให้กู้ยืมเพื่อการศึกษา และ ปัจจัยที่มีผลต่อการชำระคืนเงินกู้โครงการกองทุนเงินให้กู้ยืมเพื่อการศึกษา ในเขตกรุงเทพมหานคร ว่า ปัญหาการค้างชำหนี้กองทุนเงินให้กู้ยืมเพื่อการศึกษาเกิดจากสาเหตุ ดังต่อไปนี้ (1) การบริหารการดำเนินงานของฝ่ายบริหารที่ขาดประสิทธิภาพ โดยเฉพาะเรื่องกระบวนการกู้ยืมคลุมเครือและไม่รัดกุม (2) ปัญหาจากผู้กู้ยืมไม่ชำระหนี้เนื่องจาก หลังจบการศึกษาไม่ได้รับการจ้างงานหรือได้รับการจ้างงานแต่มีหนี้ค้างชำระจากสถาบันการเงินอื่นๆ ที่มีดอกเบี้ยรายเดือนที่สูงกว่าดอกเบี้ยที่กองทุนเงินให้กู้ยืมเพื่อการศึกษาเรียกเก็บ ผู้กู้จึงเลือกที่ชำระให้กับสถาบันการเงินก่อนแล้วให้กองทุน ฟ้องร้องภายหลัง (3) เงื่อนไขชำระหนี้ของกองทุนมีความซับซ้อน ยากต่อการปรับเปลี่ยนเงื่อนไขเพราะเป็นข้อบังคับต้องผ่านหลายขั้นตอนในการอนุมัติเปลี่ยนแปลง เป็นต้น และ ปัจจัยสำคัญที่ส่งผลให้ผู้กู้ชำระเงินคืนคือ เงินเดือนต่อเดือนและจิตสำนึกของผู้กู้ที่จะมาชำระเงินคืน รวมเป็นปัจจัยเสี่ยงของระบบเงินให้กู้ยืมเพื่อการศึกษาตามสมมุติฐานจากงานวิจัยนี้ รวมถึงการขาดประสิทธิภาพและประสิทธิผลในการดำเนินงานต่างๆ ของกองทุนส่งผลให้เกิดผลกระทบต่อกองทุน โดยในงานวิจัยนี้พัฒนาระบบการตรวจสอบและวัดความสามารกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อให้สามารถนำความเสี่ยง (ปัญหาที่ยังคงมีอยู่ในการดำเนินงานต่างๆ ของกองทุนฯ ตามกรณีศึกษาที่กล่าวข้างต้น) มาดำเนินการตามกระบวนและกิจกรรมบริหารความเสี่ยงตามหลักการโคบิต 5 ที่ให้คำอธิบายไว้ในวิธีการดำเนินวิจัย

สอดคล้องกับการศึกษาของ สกุลรัตน์ ธราโสภณ (2554) บุญรอด เสกสรรค์ (2553) สมฤดี วงษ์สมิง (2540) สุรินทร์ บัวงาม (2542) รังษิยา อมาตยคง (2544) เอกภพ ภุมรา (2553) เบญจาภา มุสิกะสินธุ์ (2547) Ziderman, Adrian (2003) สุรัสวดี ชัยรัตน์ (2555) กนกวรา พวงประยงค์ (2554) และ สมชัย ฤชุพันธ์ (2548) สรุปและประเมินการบริหารงานกองทุนเงินให้กู้ยืมเพื่อการศึกษาว่า กองทุนเงินให้กู้ยืมเพื่อการศึกษา ขาดประสิทธิภาพและประสิทธิผลในกระบวนการให้กู้ยืม ตั้งแต่ระดับนโยบาย วัตถุประสงค์ เป้าหมายการดำเนินงานของกองทุน ไม่ชัดเจน กระบวนการให้กู้ยืมขาดความรัดกุม กระบวนการรับชำระหนี้ไม่สามารถทวงถามได้ทันทีเนื่องจาก

ข้อมูลผู้กู้ยืมอยู่ที่ผู้บริหารจัดการเงินให้กู้ยืม การติดตามกระบวนการให้กู้ยืมไม่ต่อเนื่อง รวมทั้งความพึงพอใจในการให้บริการการกู้ยืมของกองทุนยังไม่เป็นที่ประจักษ์ (อยู่ในระดับพอใช้) โดยในงานวิจัยนี้นำแนวทางการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 มาพัฒนาระบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อปรับปรุงกระบวนการกำกับดูแลและบริหารความเสี่ยงของกองทุนฯ โดยเฉพาะเรื่องประสิทธิภาพและประสิทธิผลในกระบวนการให้กู้ยืม ตั้งแต่ ระดับนโยบาย วัตถุประสงค์ เป้าหมายการดำเนินงานของกองทุน ไม่ชัดเจน กระบวนการให้กู้ยืมขาดความรัดกุม และกระบวนการรับชำระหนี้ไม่สามารถทวงถามได้ทันทีเนื่องจากข้อมูลผู้กู้ยืมอยู่ที่ผู้บริหารจัดการเงินให้กู้ยืม เป็นต้น จากกรณีศึกษาข้างต้น มาปรับกระบวนการในส่วนการกำกับดูแล (หน้าที่ความรับผิดชอบของคณะกรรมการตามกระบวนการ EDM03) ตามหลักการบริหารความเสี่ยง โคบิต 5 ที่อธิบายไว้ในกระบวนการและกิจกรรมกำกับดูแลความเสี่ยง (EDM03) นอกจากนี้การตัดสินใจกู้ยืมเงินเพื่อการศึกษาเนื่องจากขาดแคลนรายได้ สอดคล้องกับเขมินทรา อภิภัทรวโรดม (2551)

1.5 บทสรุปงานวิจัยที่เกี่ยวข้องกับกองทุนเงินให้กู้ยืมเพื่อการศึกษา

จากการศึกษางานวิจัยที่เกี่ยวข้องกองทุนเงินให้กู้ยืมเพื่อการศึกษาสรุปได้ว่า (1) กองทุนยังขาดในเรื่อง ประสิทธิภาพในการบริหารการดำเนินงานกระบวนการให้กู้ยืมเงิน ตั้งแต่ต้นจนจบกระบวนการ ได้แก่ นโยบายกับวัตถุประสงค์ไม่สอดคล้องกัน ไม่มีความแน่นอน เป็นต้น (2) ความพึงพอใจของผู้ใช้บริการระบบ e – Studentloan อยู่ในระดับปานกลางในมุมมองของผู้ใช้งาน (ผู้ปฏิบัติงานส่วนสถานศึกษาและนักเรียน นักศึกษา) ส่วนดำเนินงานในระดับนโยบายและวัตถุประสงค์ของกองทุนยังคงขาดประสิทธิภาพในมุมมองของผู้มีส่วนได้เสีย สรุปภาพรวมการดำเนินงานการให้บริการเงินให้กู้ยืมเพื่อการศึกษาของกองทุนยังคงขาดกระบวนการดำเนินงานที่รัดกุมทั้งภายนอกและภายใน ดังนั้นงานวิจัยนี้นำเสนอ แนวทางการปรับปรุงและพัฒนาระบบ e – Studentloan เพื่อเพิ่มประสิทธิภาพให้กับกระบวนการกู้ยืมเงินของกองทุนเงินให้กู้ยืมเพื่อการศึกษาด้วยหลักการบริหารความเสี่ยงโคบิต 5 และพัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อสอบทานกิจกรรมและวัดความสามารถกระบวนการบริหารความเสี่ยงกองทุน

2. แนวคิดตามกรอบการดำเนินงานโคบิต 5 (Cobit5 Business Framework)

โคบิต 5 คือกรอบการดำเนินงานที่สนับสนุนองค์กรในเรื่อง การบรรลุวัตถุประสงค์ในเชิงกำกับดูแลและการบริหารเทคโนโลยีสารสนเทศขององค์กร โดยสนับสนุนในส่วนของการสร้างมูลค่าสูงสุดให้กับองค์กรจากเทคโนโลยีสารสนเทศเพื่อให้การบริหารองค์กรมีการรักษาความสมดุลระหว่าง ประโยชน์ต่างๆ ที่องค์กรจะได้ ระดับความเสี่ยงที่บริหารได้ และบริหารทรัพยากรขององค์กรได้อย่างเหมาะสม ประกอบด้วย 5 หลักการ ตามภาพที่ 2.2 (2.1) ตอบสนองความต้องการของผู้มีส่วนได้เสีย (Meeting Stakeholder Needs) (2.2) ครอบคลุมทั่วทุกส่วนทั้งองค์กร (Covering the Enterprise end – to - end) (2.3) ประยุกต์รวมกรอบดำเนินงานเป็นหนึ่งเดียว (Applying a Single, Integrated Framework) (2.4) นำวิธีการแบบองค์รวมมาใช้ให้เกิดผล (Enabling a Holistic Approach) และ (2.5) แบ่งแยกการกำกับดูแลออกจากการบริหาร (Separating Governance from Management)

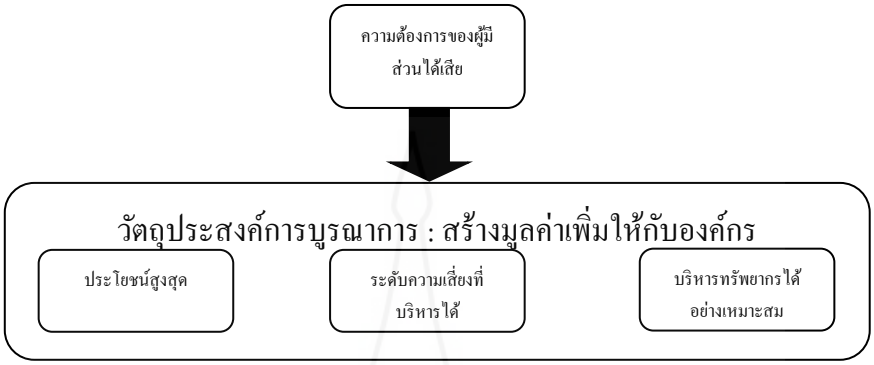
ภาพที่ 2.2 หลักการโคบิต 5

จากภาพที่ 2.2 แสดงคำอธิบายหลักการโคบิต 5 ตั้งแต่ 2.1 – 2.5

2.1 ตอบสนองความต้องการของผู้มีส่วนได้เสีย (Meeting Stakeholder Needs)

โคบิต 5 สนับสนุนการสร้างมูลค่าให้กับองค์กร คือ ตอบสนองความต้องการของผู้ที่มีส่วนเกี่ยวของกับองค์กรทุกภาคส่วน โดยรักษาระดับความสมดุลในส่วนของ ประโยชน์ต่างๆ

ที่องค์กรจะได้ ระดับความเสี่ยงที่บริหารได้ และทรัพยากรที่มีอยู่อย่างจำกัด ขององค์กร ให้มีความเหมาะสม ตามภาพที่ 2.3



ภาพที่ 2.3 วัตถุประสงค์ด้านการกำกับดูแล: การสร้างมูลค่าเพิ่ม

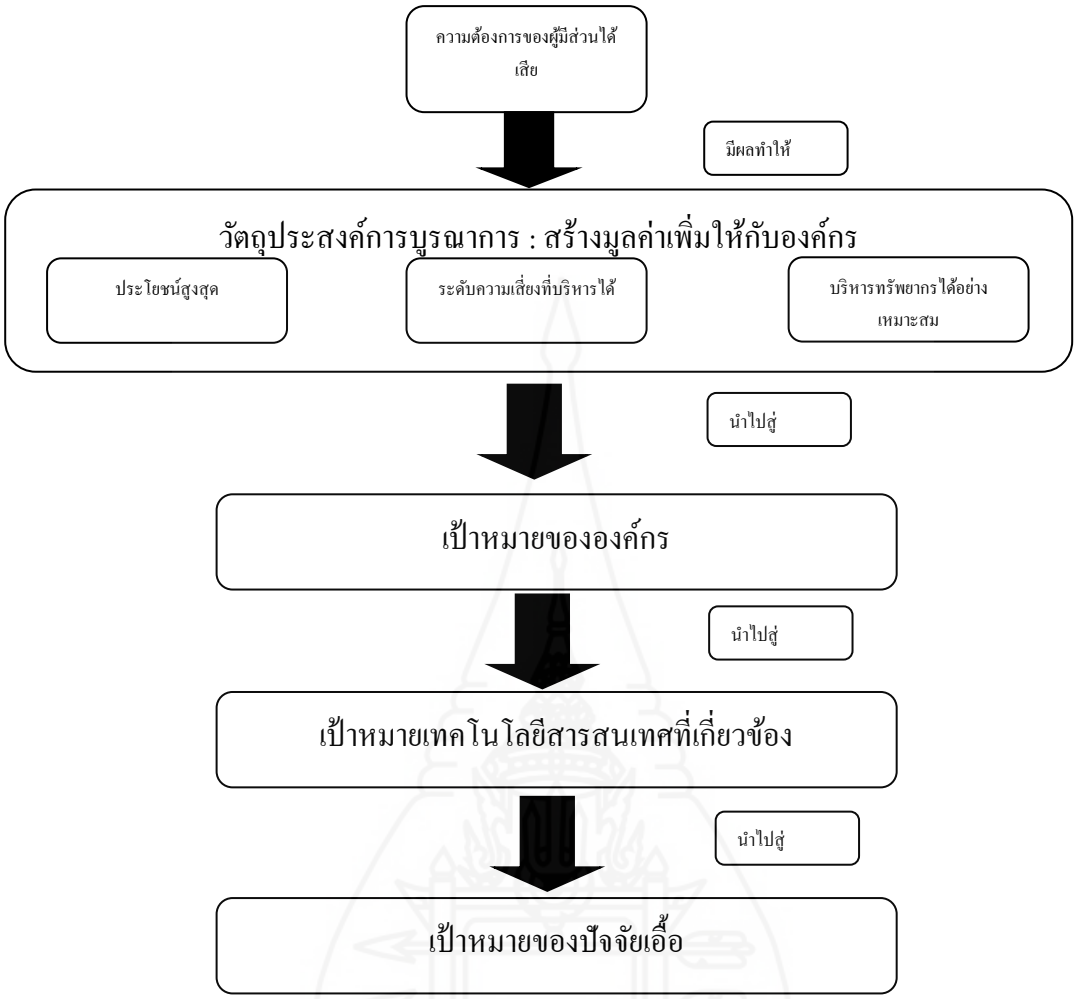
การกำหนดเป้าหมาย (Goal Cascade) ประกอบด้วย 4 ขั้นตอน ตามภาพที่ 2.4

2.1.1 แรงผลักดันจากความต้องการของผู้มีส่วนได้เสียมีผลทำให้เกิด 2.1.2

2.1.2 ความต้องการของผู้มีส่วนได้เสียนำไปสู่เป้าหมายขององค์กร นำไปสู่ 2.1.3

2.1.3 เป้าหมายขององค์กรนำไปสู่เป้าหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้อง นำไปสู่ 2.1.4

2.1.4 เป้าหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้องนำไปสู่เป้าหมายของปัจจัยเอื้อ

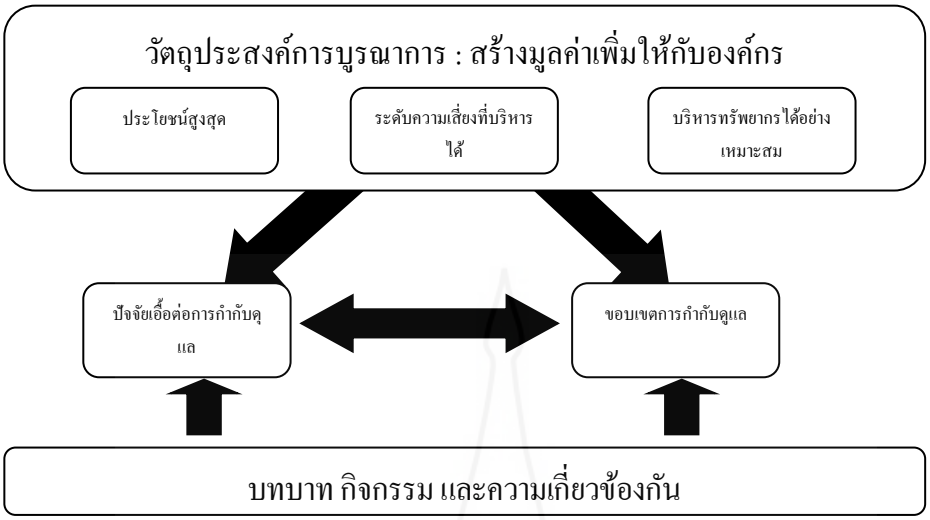


ภาพที่ 2.4 แสดงภาพรวมทิศทางการกำหนดเป้าหมายตามหลักการโคบิต 5

2.2 ครอบคลุมทั่วทุกส่วนทั้งองค์กร (Covering the Enterprise end – to - end)

2.2.1 รวบรวมการกำกับดูแลของเทคโนโลยีสารสนเทศขององค์กรเป็นการกำกับดูแลขององค์กร

2.2.2 ครอบคลุมทุกส่วนการดำเนินงานและกระบวนการที่ต้องกำกับและบริหารสารสนเทศองค์กรและเทคโนโลยีที่เกี่ยวข้อง



ภาพที่ 2.5 การกำกับดูแลและการบริหารตามหลักการโคบิต 5

วิธีการกำกับดูแล (Governance Approach) แบ่งออกเป็น 3 ส่วน ตามภาพที่ 2.5 ดังนี้

2.2.3 ปัจจัยเอื้อต่อการกำกับดูแล (Governance Enablers)

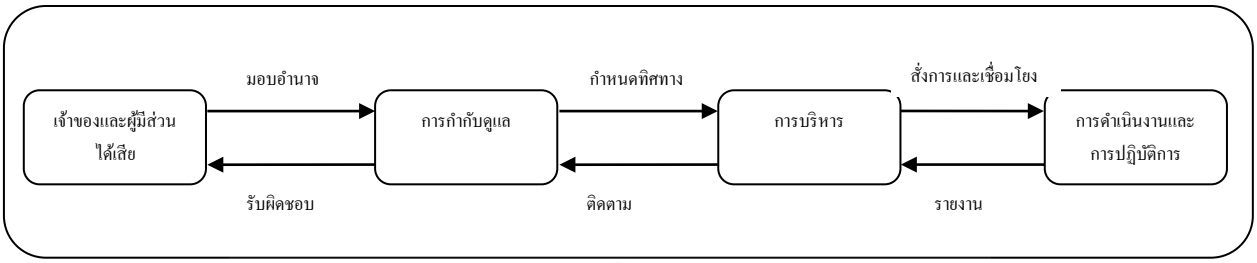
กล่าวถึงทรัพยากรที่เกี่ยวข้องกับองค์กรสำหรับการกำกับดูแล เช่น กรอบการดำเนินงาน หลักเกณฑ์ โครงสร้าง กระบวนการและแนวปฏิบัติด้วยการสั่งการและวัตถุประสงค์ ปัจจัยเอื้อนี้รวมถึงทรัพยากรขององค์กร ได้แก่ ความสามารถทางการบริการ (เช่น โครงสร้างพื้นฐานทางเทคโนโลยีสารสนทเทศ แอปพลเคชั่น เป็นต้น) บุคลากร และสารสนเทศ ดังนั้นการขาดทรัพยากรต่าง ๆ ขององค์กรอาจส่งผลทำให้ไม่สามารถสร้างคุณค่าให้กับองค์กรได้

2.2.4 ขอบเขตการกำกับดูแล (Governance Scope)

การกำกับดูแล หมายถึง องค์กรทั้งหมด หน่วยงานต่างๆ สินทรัพย์ที่จับต้องได้และจับต้องไม่ได้ เป็นต้น

2.2.5 บทบาท กิจกรรม และความเกี่ยวข้องกัน (Role, Activities and Relationships)

หมายถึง ผู้ที่เกี่ยวข้องในการกำกับดูแล มีความเกี่ยวอย่างไร ปฏิบัติหน้าที่อะไร และมีส่วนร่วมอย่างไร ภายใต้ขอบเขตการกำกับดูแลนั้นๆ ตามหลักการโคบิต 5 มีการแบ่งส่วนกิจกรรมหลักของ การกำกับดูแลและการบริหารไว้อย่างชัดเจน รวมทั้งความเกี่ยวเนื่องกันของทั้งสองกิจกรรมและบทบาทของผู้ที่เกี่ยวข้อง โดยจากภาพที่ 5 แสดงรายละเอียดของความสัมพันธ์ของแต่ละบทบาทที่แตกต่างกัน ตามภาพที่ 2.6



ภาพที่ 2.6 หลักของบทบาทหน้าที่ กิจกรรมและความสัมพันธ์กัน

2.3 ประยุกต์รวมกรอบดำเนินงานเป็นหนึ่งเดียว (Applying a Single, Integrated Framework)

โคบิต 5 รวมความรู้หลากหลายแขนงเป็นองค์ความรู้เดียว โดยรวมแนวคิด กรอบการดำเนินงานต่างๆ ของ ISACA เช่น Cobit 4.1 Val IT 2.0 Risk IT BMIS รวมทั้งมาตราต่างๆ และกรอบแนวคิดที่เกี่ยวข้อง เช่น ITIL TOGAF และ ISO เป็นต้น

2.4 นำวิธีการแบบองค์รวมมาใช้ให้เกิดผล (Enabling a Holistic Approach)

กรอบการดำเนินงานโคบิต 5 ให้คำอธิบาย 7 ประเภทของปัจจัยเอื้อ ตามภาพที่ 2.7 ดังนี้

2.4.1 หลักเกณฑ์ นโยบายและกรอบการดำเนินงาน คือ แนวทางการขับเคลื่อนของพฤติกรรมสู่แนวทางการปฏิบัติสำหรับการบริหารการดำเนินงานวันต่อวัน

2.4.2 กระบวนการ อธิบายแนวทางการปฏิบัติและกิจกรรมต่างๆ ที่ทำให้บรรลุวัตถุประสงค์และผลิตผลลัพธ์ที่เอื้อต่อการบรรลุเป้าหมายเทคโนโลยีสารสนเทศทั้งหมด

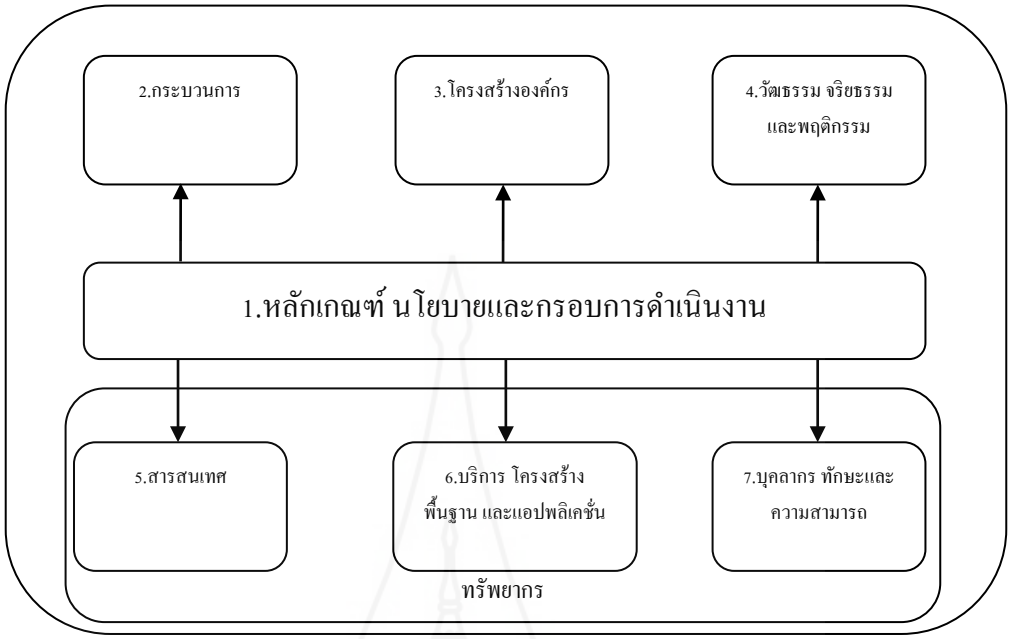
2.4.3 โครงสร้างองค์กร คือ สิ่งที่กำหนดการตัดสินใจในองค์กร

2.4.4 วัฒนธรรม จริยธรรมและพฤติกรรม ของบุคคล องค์กร เป็นตัวกำหนดปัจจัยความสำเร็จในกิจกรรมต่างๆ ของการกำกับดูแลและการบริหาร

2.4.5 สารสนเทศคือ สิ่งที่กระจายอยู่ทั่วทั้งองค์กรและรวมทั้งสารสนเทศที่ถูกผลิตทั้งหมดและใช้โดยองค์กร สารสนเทศคือสิ่งที่ทำให้องค์กรสามารถดำเนินงานได้อย่างต่อเนื่องและอยู่ในการกำกับดูแลที่ดี แต่ในส่วนระดับปฏิบัติการสารสนเทศเป็นสิ่งสำคัญมากสำหรับองค์กร

2.4.6 บริการต่างๆ โครงสร้างพื้นฐานและแอปพลิเคชั่น รวมถึง โครงสร้างพื้นฐานเทคโนโลยี และแอปพลิเคชั่น ที่ทำให้องค์กรสามารถดำเนินการทางเทคโนโลยีสารสนเทศและการบริการได้

2.4.7 บุคลากร ทักษะต่างๆ และความสามารถต่างๆ เป็นสิ่งที่เชื่อมต่อบุคลากรและความต้องการต่อความสำเร็จสมบูรณ์ของทุกๆ กิจกรรม เพื่อการตัดสินใจที่ถูกต้องและการเลือกปฏิบัติที่ถูกต้อง



ภาพที่ 2.7 ปัจจัยเอื้อในการดำเนินงานตามหลักการโคบิต 5

2.4.8 มิติของปัจจัยเอื้อ ตามภาพที่ 2.8 ประกอบด้วย 2 มิติ ดังนี้

2.1.4.1 มิติของปัจจัยเอื้อ (Enabler Dimension) ประกอบด้วย 4 มิติดังนี้

(1) ผู้มีส่วนได้เสีย ประกอบด้วยผู้ที่มีส่วนเกี่ยวข้องกับองค์กรทั้งภายนอกและภายใน

(2) เป้าหมาย ประกอบด้วยเป้าหมายย่อยดังนี้

- คุณภาพทางลักษณะนิสัย (Intrinsic quality) เช่น ปัจจัยเอื้อทางด้าน บุคลากร ทักษะและความสามารถ เป้าหมายในส่วนนี้ คือ มีการศึกษาคุณสมบัติและมีทักษะทางเทคนิคตรงตามความต้องการขององค์กร
- คุณภาพตามสภาวะแวดล้อมที่เกี่ยวข้อง (Contextual quality) ตัวอย่างเดียวกันกับ คุณภาพทางลักษณะนิสัย (Intrinsic quality) บุคลาการต้องมีคุณภาพในส่วนนี้ คือ มีประสบการณ์ มีความรู้และทักษะทางพฤติกรรมที่สอดคล้องกับความต้องการขององค์กร รวมทั้งความพร้อมและการหมุนเปลี่ยนงานด้วย
- การเข้าถึงและความมั่นคงปลอดภัย (Access and security)

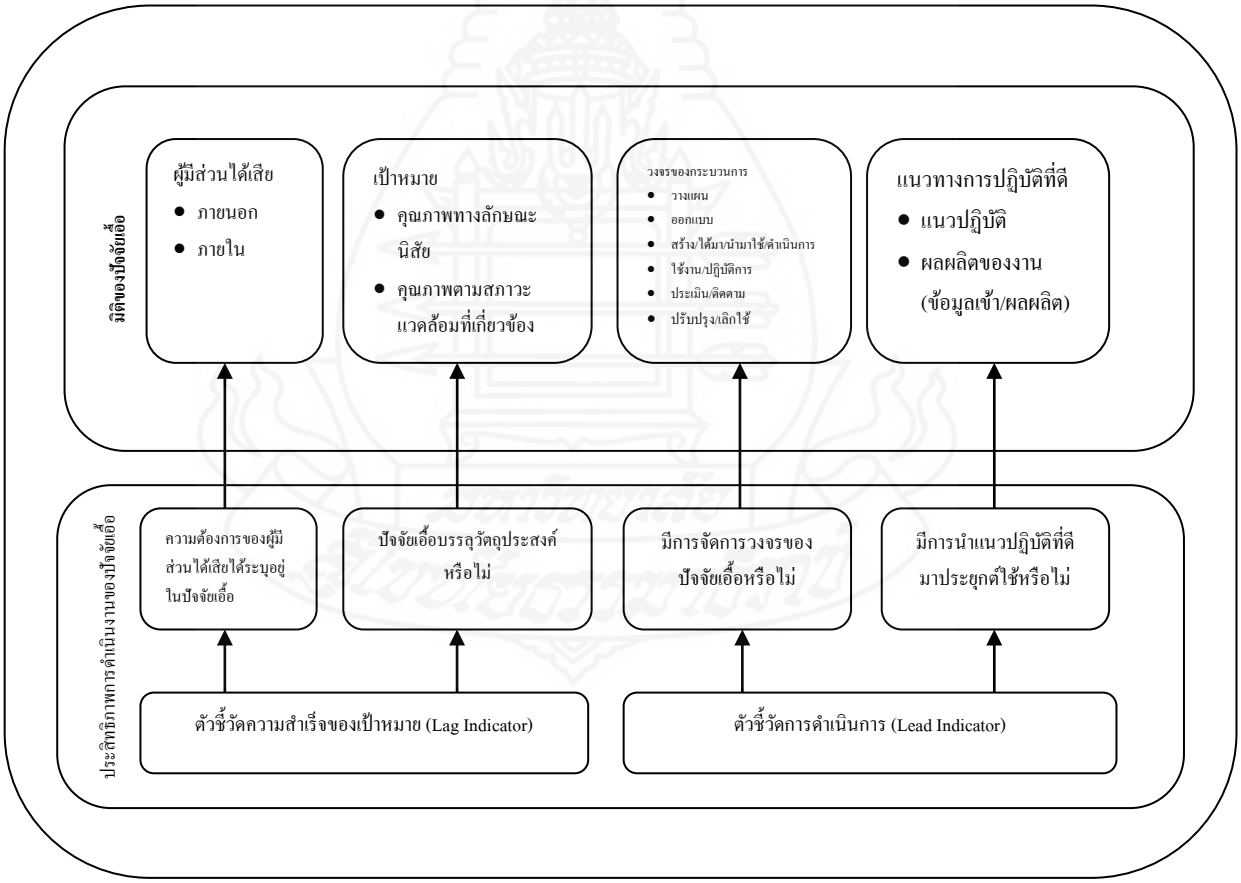
(3) วงจรของกระบวนการประกอบด้วย (1) วางแผน (2) ออกแบบ (3) สร้าง/ได้มา/นำมาใช้/ดำเนินการ (4) ใช้งาน/ดำเนินงานจริง (5) ประเมิน/ติดตาม และ (6) ปรับปรุง/เลิกใช้

(4) แนวทางการปฏิบัติที่ดี ในแต่และปัจจัยเอื้อจะมีแนวทางการปฏิบัติที่ดีช่วยแนะนำให้กับองค์กรปฏิบัติตามเป็นตัวอย่างเพื่อสนับสนุนการดำเนินการของกระบวนการต่างๆ ตามหลักการโคบิต 5

2.1.4.2 ประสิทธิภาพการดำเนินงานของปัจจัยเอื้อ (Enabler Performance Management) ประกอบด้วย 2 ตัวชี้วัดดังนี้

(1) ตัวชี้วัดความสำเร็จของเป้าหมาย (Lag Indicator) คือผลลัพธ์จริงของปัจจัยเอื้อ เช่น ปัจจัยเอื้อบรรลุวัตถุประสงค์หรือไม่ หรือ ความต้องการของผู้มีส่วนได้เสียได้ระบุอยู่ในปัจจัยเอื้อหรือไม่

(2) ตัวชี้วัดการดำเนินการ (Lead Indicator) คือ การดำเนินงานจริงของปัจจัยเอื้อ เช่น มีการจัดการวงจรของปัจจัยเอื้อหรือไม่ หรือ มีการนำแนวปฏิบัติที่ดีมาประยุกต์ใช้หรือไม่



ภาพที่ 2.8 ปัจจัยเอื้อตามหลักการโคบิต 5: ลักษณะการวัดผลของปัจจัยเอื้อ

2.5 แบ่งแยกการกำกับดูแลออกจากการบริหาร (Separating Governance from Management) แบ่งเป็น 2 ส่วน ดังนี้

2.5.1 การกำกับดูแลและการบริหารแยกออกจากกัน ดังนี้

1) การกำกับดูแล (Governance) คือ ให้ความเชื่อมั่นกับผู้มีส่วนได้เสียว่าสิ่งที่ต้องการ สภาพการและทางเลือกต่างๆ ได้รับการความสมดุลในการประเมินเพื่อตัดสินใจเพื่อบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้ โดยกำหนดการสั่งการตามลำดับและการตัดสินใจ รวมทั้ง การติดตามผลการดำเนินการและความสอดคล้องกับคำสั่งการและวัตถุประสงค์ หมายเหตุผู้รับผิดชอบคือประธานคณะกรรมการ โดยมีผู้จัดการหรือผู้อำนวยการเป็นผู้ดำเนินการ

2) การบริหาร (Management) คือ บริหาร การวางแผน การสร้าง การดำเนินงานและติดตามกิจกรรมต่างๆ ขององค์กรให้เชื่อมโยงหรือสอดคล้องกับคำสั่งการที่ได้รับมอบหมายจากส่วนการกำกับดูแล (Governance body)เพื่อบรรลุวัตถุประสงค์ขององค์กร

2.5.2 ปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหาร ตามตารางที่ 2.1

ตารางที่ 2.1 ปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหาร

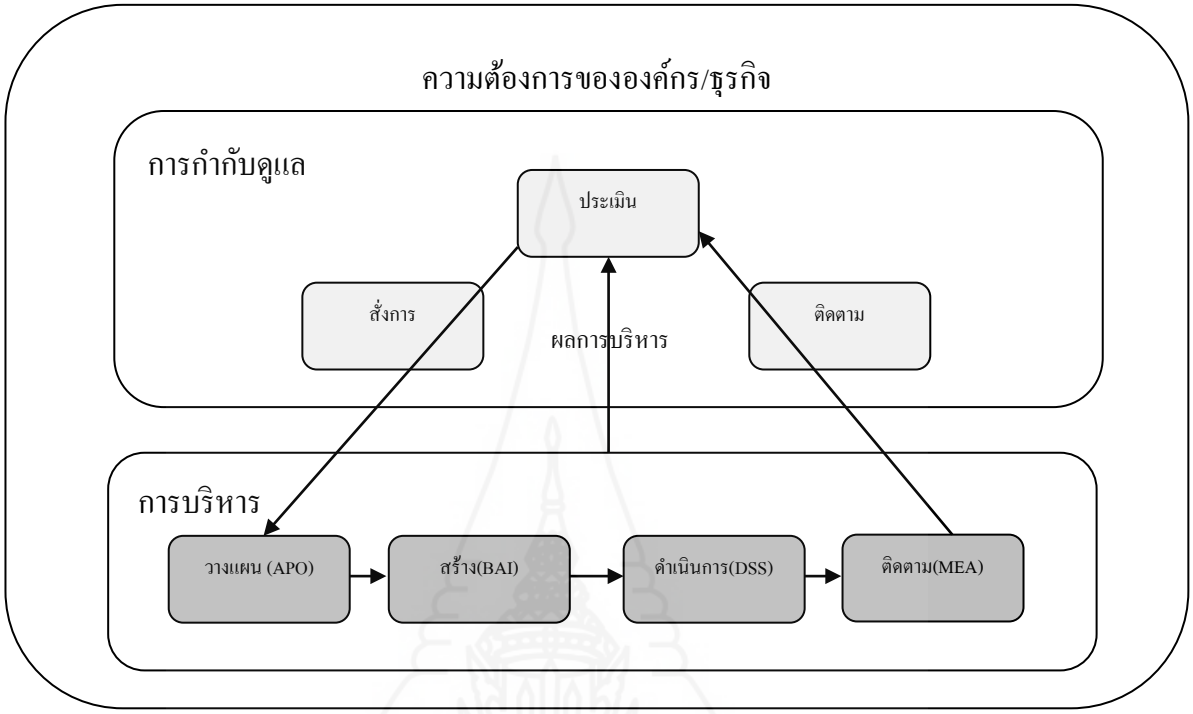
ปัจจัยเอื้อ (Enabler)	ปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหาร
กระบวนการ	รูปแบบกระบวนการตามหลักการโคบิต 5 (Cobit5: Enabling Process)แบ่งแยกกระบวนการกำกับดูแลออกจากการบริหาร รูปแบบกระบวนการกล่าวถึงตารางแบ่งแยกหน้าที่ (RACI Charts)อธิบายถึงความรับผิดชอบสำหรับตำแหน่งงานและบทบาทหน้าที่ต่างๆ ภายในองค์กร
สารสนเทศ	รูปแบบกระบวนการที่อธิบายการรับข้อมูลและการส่งผลลัพธ์จากกระบวนการต่างๆ ที่นำไปปฏิบัติต่อในกระบวนการอื่นๆ ซึ่งรวมถึงสารสนเทศที่แลกเปลี่ยนกันระหว่าง กระบวนการของการกำกับดูแลและการบริหาร สารสนเทศใช้สำหรับการประเมิน การสั่งการและการติดตาม เทคโนโลยีสารสนเทศระดับองค์กรมีการแลกเปลี่ยนกันระหว่าง การกำกับดูแลและการบริหาร
โครงสร้างองค์กร	โครงสร้างองค์กรที่ได้กำหนดขึ้นสำหรับแต่ละองค์กร โครงสร้างหนึ่งๆ อาจอยู่ในส่วนของการกำกับดูแลและการบริหารก็ได้ ขึ้นอยู่กับองค์ประกอบและขอบเขตของการตัดสินใจนั้นๆ เนื่องจากการกำกับดูแลเป็นเรื่องการกำหนดทิศทาง ปฏิสัมพันธ์จึงเกิดขึ้นระหว่างการตัดสินใจที่เกิดขึ้นจากโครงสร้างในส่วนการกำกับดูแล

ตารางที่ 2.1 (ต่อ)

ปัจจัยเอื้อ (Enabler)	ปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหาร
หลักการ นโยบายและกรอบการดำเนินงาน	หลักการ นโยบาย และกรอบการดำเนินงานเป็นสิ่งที่นำไปสู่การตัดสินใจด้านการกำกับดูแลให้เกิดขึ้นภายในองค์กรและด้วยเหตุผลนี้จึงเกิดปฏิสัมพันธ์ระหว่างการตัดสินใจด้านกำกับดูแล (กำหนดทิศทาง) และด้านการบริหาร (การปฏิบัติตามการตัดสินใจ)
วัฒนธรรม จริยธรรมและพฤติกรรม	พฤติกรรมเป็นหนึ่งปัจจัยเอื้อหลักสำหรับการบริหารและการกำกับดูแลที่ดีขององค์กรซึ่งกำหนดขึ้น โดยผู้บริหารระดับสูงด้วยการปฏิบัติให้เห็นเป็นตัวอย่าง ดังนั้นพฤติกรรมจึงเป็นปฏิสัมพันธ์ระหว่างการกำกับดูแลและการบริหาร
บุคลากร ทักษะต่าง ๆ และความสามารถต่าง ๆ	กิจกรรมต่างๆ ในการกำกับดูแลและการบริหารต้องการกลุ่มของทักษะต่างๆที่แตกต่างกัน แต่ทักษะที่จำเป็นสำหรับสมาชิกในหน่วยงานการกำกับดูแลและการบริหารคือ ความเข้าใจในภารกิจทั้งสองด้านและเข้าใจถึงความแตกต่างระหว่างกัน
บริการต่าง ๆ โครงสร้างพื้นฐานและแอปพลิเคชั่น	ต้องการการบริการซึ่งสนับสนุน โดยระบบงานและโครงสร้างพื้นฐานเพื่อให้สารสนเทศเหมาะสมกับหน่วยงานการกำกับดูแลและเพื่อสนับสนุนกิจกรรมการกำกับดูแล ที่รวมถึงการประเมิน การกำหนดทิศทางและการเฝ้าติดตาม

2.5.3 รูปแบบกระบวนการอ้างอิง แบ่งเป็น 2 ส่วน ดังนี้

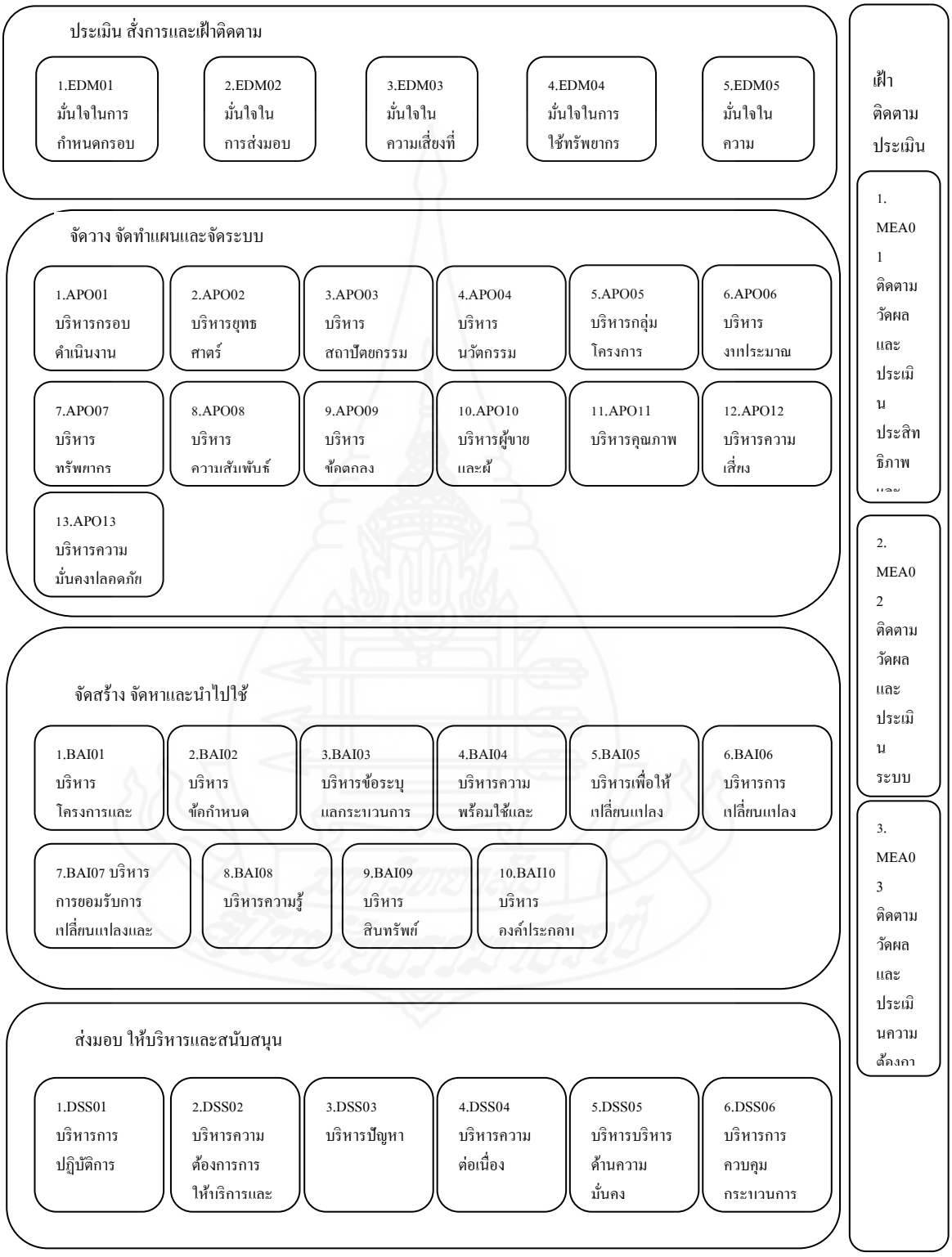
1) รูปแบบการกำกับดูแลและการบริหารตามภาพที่ 2.9



ภาพที่ 2.9 ขอบเขตหลักของการกำกับดูแลและการบริหาร

จากภาพที่ 2.9 แสดงขอบเขตการดำเนินการของการกำกับดูแลและการบริหาร ประกอบด้วย (1) กระบวนการกำกับดูแล (EDM)5 กระบวนการ และ (2) กระบวนการบริหาร แบ่งเป็น 4 กลุ่มหลัก (2.1) จัดวาง ทำแผน วางระบบ (APO) 13 กระบวนการ (2.2) สร้าง จัดหา ดำเนินงาน (BAI) 10 กระบวนการ (2.3) ส่งมอบ บริการและสนับสนุน (DSS)6 กระบวนการ และ (2.4) ติดตาม วัดผล และประเมิน (MEA) 3 กระบวนการ รวมทั้งหมด 32 กระบวนการ รวมกระบวนการตามหลักโคบิต 5 ทั้งหมด 37 กระบวนการ ตามภาพที่ 2.10 แสดงรายการของกระบวนการตามหลักการโคบิต 5

2) กระบวนการการกำกับดูแลและการบริหาร 37 กระบวนการตามภาพที่ 2.10



ภาพที่ 2.10 กระบวนการการกำกับดูแลและการบริหาร 37 กระบวนการ

2.6 แนวทางการแนะนำการดำเนินงาน (Implementation Guidance)

ในส่วนนี้เป็นการแนะนำแนวทางการดำเนินงานและวงจรการพัฒนากระบวนการในระดับสูงสุด และให้ความสำคัญในเรื่องต่างๆ จาก วิธีการดำเนินกระบวนการตามหลักการโคบิต 5 (Cobit5 Implementation) เช่น (1) กรณีศึกษาทางธุรกิจเพื่อดำเนินการและปรับปรุงการกำกับดูแลและการบริหารด้านเทคโนโยลีสารสนเทศ (2) พบจุดอ่อนและสาเหตุที่ทำให้เกิดเหตุการณ์ต่างๆ (3) สร้างสภาพแวดล้อมที่เหมาะสำหรับการดำเนินการ (4) นำโคบิตมาใช้ในการระบุช่องว่างและแนวทางการพัฒนาปัจจัยเอื้อต่างๆ เช่น นโยบาย กระบวนการ หลักการ โครงสร้างองค์กร และบทบาทและความรับผิดชอบ ประกอบด้วย 5 องค์ประกอบ ดังนี้

2.6.1 การพิจารณาสภาพการองค์กร

องค์กรทุกแห่งต้องการการออกแบบแผนการดำเนินงานหรือขั้นตอนการดำเนินงานขององค์กรเองขึ้นอยู่กับปัจจัยภายนอกและภายในที่เฉพาะเจาะจงขององค์กรนั้นๆ เช่น (1) จริยธรรมและวัฒนธรรม (2) เป็นไปตามกฎหมาย ระเบียบและนโยบาย (3) พันธกิจ วิสัยทัศและคุณค่า (4) นโยบายการกำกับดูแลและแนวปฏิบัติ (5) แผนธุรกิจและกลยุทธ์ (6) รูปแบบการปฏิบัติการและระดับความสำเร็จของกระบวนการ (7) ลักษณะการบริหาร (8) การยอมรับความเสี่ยง (9) ความสามารถและความพร้อมใช้ของทรัพยากร และ (10) แนวปฏิบัติของอุตสาหกรรมต่าง ๆ

วิธีการที่ดีที่สุดสำหรับการกำกับดูแลและการบริหารเทคโนโลยีสารสนเทศขององค์กรจะมีความแตกต่างกันสำหรับทุกองค์กรและบริบทขององค์กรต้องการทำความเข้าใจและพิจารณาที่ปรับเปลี่ยนและนำหลักการโคบิตมาใช้ดำเนินการด้านการกำกับดูแลและด้านการบริหารเทคโนโลยีสารสนเทศองค์กรให้เกิดประสิทธิภาพ โคบิตคือกรอบแนวคิดที่สนับสนุนกรอบแนวคิดอื่นๆ แนวทางการปฏิบัติที่ดี มาตรฐานต่างๆ และสิ่งเหล่านี้ต้องการการปรับเปลี่ยนให้มีความเหมาะสมตรงกันกับความต้องการต่างๆ

ปัจจัยสำคัญสู่ความสำเร็จสำหรับการดำเนินการตามหลักการโคบิต 5 ให้ประสบความสำเร็จ ได้แก่

- ผู้บริหารระดับสูงให้คำสั่งการและบทบัญญัติสำหรับกระทำการอย่างอิสระรวมทั้งการให้คำมั่นสัญญาและการสนับสนุนที่เห็นได้อย่างชัดเจน
- ทุกภาคส่วนสนับสนุนกระบวนการกำกับดูแลและการบริหารต่อการทำความเข้าใจองค์กรหรือธุรกิจและวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศ
- เชื่อมั่นว่าการสื่อสารอย่างมีประสิทธิภาพและวิธีการของการเปลี่ยนแปลงต่างๆ ที่จำเป็น

- ออกแบบตามหลักการโคบิต แนวทางการปฏิบัติที่ดีและมาตรฐานต่างๆ ให้เหมาะสมกับสภาพแวดล้อมเดียวกันกับองค์กร
- มุ่งเน้นความสนใจเรื่องที่ได้ประโยชน์มากที่สุดและเลือกดำเนินการปรับปรุงที่ได้ประโยชน์สูงสุดที่มีความง่ายต่อการดำเนินการก่อน

***2.6.2* สร้างสภาพแวดล้อมที่เหมาะสม**

การสร้างสภาพแวดล้อมขององค์กร/ธุรกิจให้เหมาะสมเป็นสิ่งสำคัญในเริ่มดำเนินงานตามหลักการโคบิต 5 เพื่อให้มีการกำกับที่เหมาะและการจัดการที่เพียงพอ การเริ่มต้นดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศส่วนมากล้มเหลวเนื่องมาจากความไม่พร้อมในเรื่อง การสั่งการ การสนับสนุน และความไม่รอบคอบในหลายๆ เรื่องของสิ่งที่ผู้มีส่วนได้เสียต้องการจากองค์กรหรือธุรกิจ เช่นเดียวกันกับการนำหลักการโคบิต 5 มาปรับใช้องค์กรจำเป็นต้องมีการสร้างสภาพแวดล้อมขององค์กรหรือธุรกิจให้พร้อมต่อการดำเนินการดังกล่าว

อีกปัจจัยหนึ่งที่ขาดไม่ได้ในการสร้างแวดล้อมขององค์กร/ธุรกิจเพื่อที่จะดำเนินกระบวนการต่างๆ ตามหลักการโคบิต 5 คือ ความเข้าใจ การให้ความร่วมมือ และการให้คำมั่นสัญญาที่จะดำเนินการตามหลักการโคบิต 5 ของผู้กำกับดูแล (Governance body) และ ผู้บริหาร (Management body) โดยเมื่อสามารถสร้าง/ปรับเปลี่ยนทัศนคติเหล่านั้นได้ และองค์กร/ธุรกิจมีการริเริ่มจาก โยบายหรือแนวปฏิบัติที่จะดำเนินการตามหลักโคบิต 5 จาก ผู้กำกับดูแล ถ่ายทอดลงไปสู่ผู้บริหาร และลงต่อไปถึง ผู้ปฏิบัติงาน องค์กร/ธุรกิจถึงจะสามารถเตรียมความพร้อมเพื่อดำเนินการอีกระดับหนึ่งได้คือ เตรียมทรัพยากรต่างๆ ที่ต้องการเพื่อสนับสนุนโครงการต่างๆ ที่จะต้องเริ่มดำเนินการตามหลักการโคบิต 5 ต่อไป เช่น (1) กำหนดบทบาทหน้าที่และความรับผิดชอบหลักในการดำเนินโครงการ (2) กำหนดโครงสร้างและกระบวนการเพื่อกำกับดูแลและการสั่งการโดยเชื่อมั่นว่าทุกกระบวนการเหล่านี้เชื่อมโยงกับองค์กรและวิธีการบริหารความเสี่ยงทั้งองค์กร (3) มีการให้ความเชื่อมั่นกับผู้มีส่วนได้เสียว่าองค์กร/ธุรกิจ จะสร้างคุณประโยชน์ตามความต้องการของผู้มีส่วนได้เสีย เป็นต้น

2.6.3 พบจุดบกพร่องและสาเหตุที่ทำให้เกิดเหตุการณ์ต่างๆ (Pain Points and Trigger Events)

มีหลายปัจจัยที่อาจบ่งชี้ว่าการกำกับดูแลและการบริหารต้องการการปรับปรุงโดยตามหลักการ โคบิต 5 นำเสนอแนวทางกับองค์กร/ธุรกิจว่าถ้าเกิดพบเห็นหรือเผชิญกับจุดบกพร่อง (Pain Points) ที่เป็นต้นกำเนิดของปัญหา เหล่านี้ องค์กร/ธุรกิจ ควรหรือต้อง ปรับปรุงการดำเนินงานที่เป็นอยู่ใหม่ ยกตัวอย่างดังนี้

- ความซับซ้อนขององค์กร/ธุรกิจกับความล้มเหลวในการเริ่มต้น เช่น ต้นทุนด้านเทคโนโลยีสารสนเทศเพิ่มขึ้นและสถานภาพขององค์กร/ธุรกิจลดลง
- มีเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเกิดขึ้น เช่น ข้อมูลหาย หรือ โครงการไม่เสร็จสิ้น
- การส่งมอบโครงการจากผู้รับจ้างเกิดปัญหา เช่น ผิดข้อตกลงตามสัญญาการให้บริการ
- ไม่ปฏิบัติตามกฎระเบียบ หรือ ไม่ดำเนินการตามความต้องการตามสัญญาที่กำหนด
- เทคโนโลยีสารสนเทศขององค์กร/ธุรกิจ เป็นข้อจำกัดในการดำเนินงานของ องค์กร/ธุรกิจเพื่อสร้างนวัตกรรมและการเปลี่ยนแปลงลักษณะขององค์กร/ธุรกิจ
- การดำเนินการตรวจสอบประจำปีพบว่าศักยภาพของเทคโนโลยีสารสนเทศขององค์กร/ธุรกิจค่อนข้างต่ำหรือคุณภาพการให้บริการเกิดปัญหาในการให้บริการ
- มีการบกปิดและโกงค่าใช้จ่ายทางเทคโนโลยีสารสนเทศ
- มีการดำเนินการซ้ำซ้อนและทับซ้อนกันระหว่างการเริ่มต้นโครงการหรือสิ้นเปลืองทรัพยากร เช่น โครงการถูกยกเลิกเร็วกว่าที่ควรจะเป็น
- คณะกรรมการ คณะผู้บริหารหรือผู้บริหารระดับสูง หลีกเลี่ยงกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือขาดการให้คำมั่นสัญญาและความพอใจในผู้ในการสนับสนุนองค์กร/ธุรกิจสำหรับเทคโนโลยีสารสนเทศ

นอกเหนือจากจุดบกพร่อง มีเหตุการณ์ทั้งภายในและภายนอกสามารถบ่งบอกถึงเหตุการณ์ที่จะเกิดขึ้นได้ (Trigger Events) ยกตัวอย่าง

- การควบรวม การได้มา หรือการถอนทุนทางธุรกิจ
- การเปลี่ยนแปลงของ ตลาดทางธุรกิจ เศรษฐกิจ หรือการแข่งขันทางธุรกิจ
- การเปลี่ยนแปลงรูปแบบการดำเนินงานของธุรกิจ หรือ การจัดวางแหล่งทุน
- กฎระเบียบใหม่ หรือ กฎเกณฑ์ ข้อบังคับใหม่
- เทคโนโลยีที่มีความสำคัญเปลี่ยนแปลง หรือ เปลี่ยนถ่ายยุคสมัย
- ความสนใจการกำกับดูแลขององค์กร หรือ โครงการ
- ผู้บริหารชุดใหม่
- ผู้ตรวจสอบภายนอก หรือ การประเมินจากที่ปรึกษา
- กลยุทธ์ใหม่ของธุรกิจ หรือ การลำดับการดำเนินงาน

2.6.4 ดำเนินการเปลี่ยนแปลง

การดำเนินการตามหลักการโคบิต 5 ให้ประสบความสำเร็จขึ้นอยู่กับการดำเนินการเปลี่ยนแปลงและดำเนินไปในทิศทางที่เหมาะสม (นำปัจจัยเอื้อในเรื่องการกำกับดูแลและการบริหารมาปรับใช้ได้อย่างเหมาะสม) โดยสิ่งสำคัญที่ไม่ควรละเลยในการดำเนินการเปลี่ยนแปลง คือ เรื่อง การจัดการทรัพยากรบุคคล พฤติกรรมและวัฒนธรรมองค์กร ต่อการเปลี่ยนแปลงที่จะเกิดขึ้นกับองค์กร ซึ่งองค์กร/ธุรกิจส่วนมากมุ่งเน้นแต่ในเรื่อง การกำกับดูแลและการบริหารเท่านั้น

2.6.5 วิธีการดำเนินการวงจรชีวิตของกระบวนการ ประกอบด้วย 7 ขั้นตอน ตามภาพที่ 2.11

1) ขั้นตอนที่ 1 เริ่มต้นด้วยความเห็นร่วมกันที่ต้องการเริ่มดำเนินการตามหลักการโคบิต 5หรือเริ่มการปรับปรุงกระบวนการ คือการระบุจุดบกพร่องหรือเหตุการณ์ปัญหาต่างๆ เพื่อก่อให้เกิดการเปลี่ยนแปลงในระดับบริหาร

2) ขั้นตอนที่ 2 กำหนดขอบเขตการดำเนินการและปรับปรุงตามหลักการโคบิต 5 เชื่อมกับเป้าหมายองค์กรและเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขององค์กรเพื่อสนับสนุนกระบวนการด้านเทคโนโลยีสารสนเทศ โดยพิจารณาสถานการณ์ความเสี่ยงต่างๆ ที่เป็นประเด็นสำคัญของกระบวนการนั้นๆ ในส่วนที่ได้ทำการวินิจฉัยว่ามีความสำคัญในระดับสูงที่จะดำเนินการปรับปรุงเป็นอันดับแรกให้นำมากำหนดขอบเขตและทำความเข้าใจเป็นลำดับแรกสุด

3) ขั้นตอนที่ 3 กำหนดเป้าหมายการปรับปรุง โดยวิเคราะห์รายละเอียดตามแนวทางโคบิต 5เพื่อระบุช่องว่างของกระบวนการและการแก้ไข

4) ขั้นตอนที่ 4 วางแผนการดำเนินงานเพื่อทำการแก้ไข โดยกำหนดเป็นโครงการขององค์กร/ธุรกิจ แผนการเปลี่ยนแปลงสำหรับการดำเนินการตามหลักการโคบิต 5 มีการปรับปรุงใหม่

5) ขั้นตอนที่ 5 กำหนดการวัดผลและการติดตาม โดยใช้เป้าหมายความสำเร็จและมาตรวัดตามหลักการโคบิต 5 เพื่อให้ความเชื่อมั่นว่าธุรกิจมีความเชื่อมโยง รักษาแนวทางที่จะบรรลุเป้าหมายและสามารถวัดประสิทธิภาพการดำเนินงานได้

6) ขั้นตอนที่ 6 รักษากระบวนการที่ได้ดำเนินการตามหลักการโคบิต 5 หรือปรับปรุงปัจจัยเอื้อต่างๆ และติดตามผลของความสำเร็จที่คาดหวังไว้

7) ขั้นตอนที่ 7 สอบทานความสำเร็จของการดำเนินการตามหลักการโคบิต 5 กำหนดความต้องการสำหรับ การกำกับดูแลและการบริหารเทคโนโลยีสารสนเทศขององค์กร/ธุรกิจเพิ่มเติม ต้องการแนวทางการปรับปรุงอย่างต่อเนื่อง

ภาพที่ 2.11 วงจรชีวิตของกระบวนการดำเนินงานตามหลักการโคบิต 5 7 ขั้นตอน

2.7 รูปแบบความสามารถของกระบวนการบริหารความเสี่ยงโคบิต 5 (COBIT 5 Process Capability Model) ประกอบด้วยระดับการวัดความสำเร็จ 6 ระดับ ตามภาพที่ 2.12 ดังนี้

2.7.1 ความสำเร็จของกระบวนการระดับ 0 คือ กระบวนการไม่สมบูรณ์ (0 Incomplete Process) : กระบวนการไม่ได้ดำเนินการหรือไม่บรรลุผลตามวัตถุประสงค์ที่กำหนด ตามภาพที่ 2.12 ในวงกลมหมายเลย 0

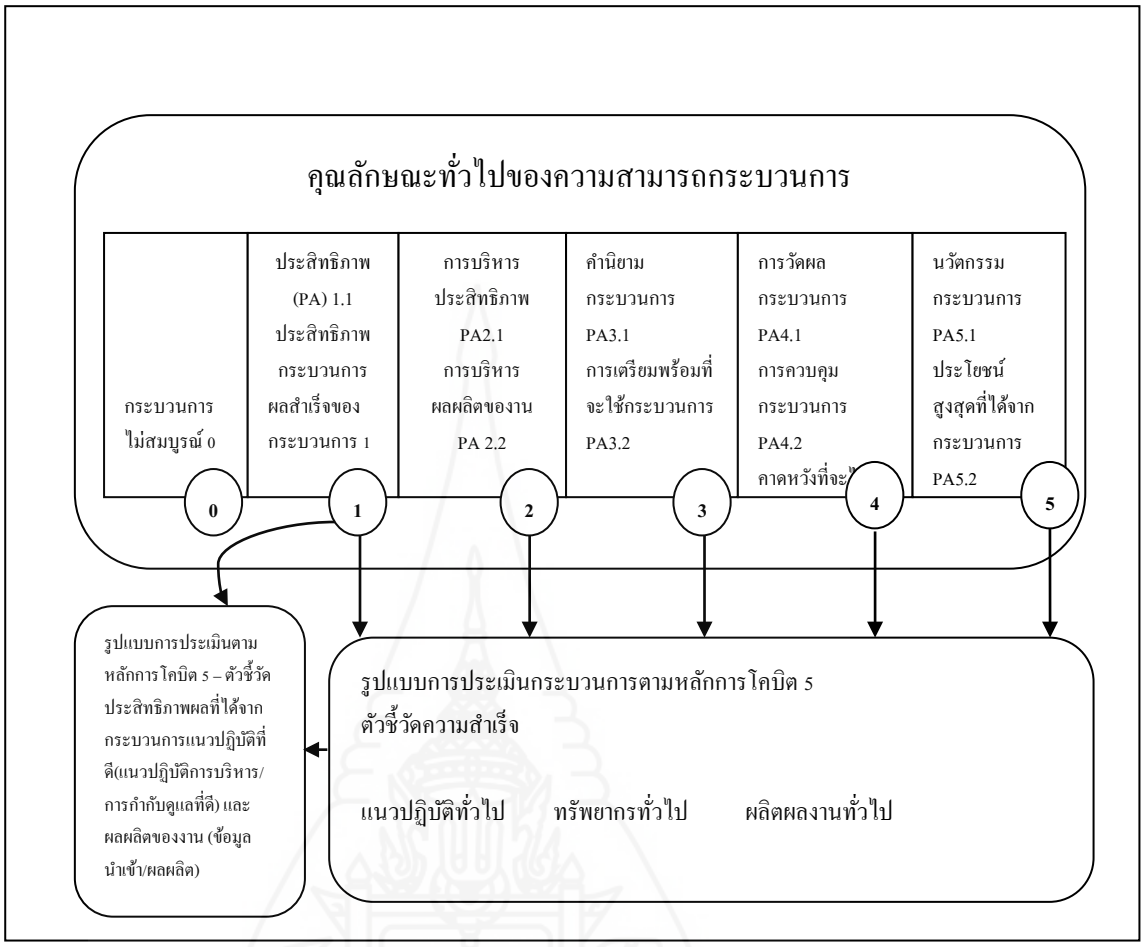
2.7.2 ความสำเร็จของกระบวนการระดับ 1 คือ กระบวนการได้รับการดำเนินการ (1Performed Process) ต้องครอบคลุม 1 คุณลักษณะ (one attribute) : มีการดำเนินกระบวนการสำเร็จตามวัตถุประสงค์ (PA 1.1)ตามภาพที่ 2.12 ในวงกลมหมายเลย 1

2.7.3 ความสำเร็จของกระบวนการระดับ 2 คือ กระบวนการได้รับการบริหาร (2 Managed Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 1 (1Performed Process) (1) ได้รับการดำเนินการบริหารตามรูปแบบ (มีการวางแผน ติดตาม และปรับปรุง) (PA 2.1) และ (2) กระบวนการมีการดำเนินการควบคุม และเก็บรักษาอย่างเหมาะสม (PA 2.2) ตามภาพที่ 2.12 ในวงกลมหมายเลย 2

2.7.4 ความสำเร็จของกระบวนการระดับ 3 คือ กระบวนการได้รับการยอมรับว่ามีจริง (3 Established Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 2 (2 Managed Process) (1) มีการดำเนินการโดยกำหนดกระบวนการ (PA 3.1) (2) นำกระบวนการไปใช้งานโดยกระบวนการสามารถบรรลุผลสำเร็จและได้ผลลัพธ์ (PA 3.2) ตามภาพที่ 2.12 ในวงกลมหมายเลย 3

2.7.5 ความสำเร็จของกระบวนการระดับ 4 คือ กระบวนการสามารถพยากรณ์ได้ (4 Predictable Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 3 (3 Established Process) (1) กระบวนการมีกำหนดมาตราวัดผลลัพธ์ของกระบวนการ (PA 4.1) (2) กระบวนการมีการควบคุม (PA 4.2) ตามภาพที่ 2.12 ในวงกลมหมายเลย 4

2.7.6 ความสำเร็จของกระบวนการระดับ 5 คือ กระบวนการให้ผลลัพธ์และมีคุณประโยชน์สูงสุด (5 Optmising Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 4 (1) มีการพัฒนา คิดค้นนวัตกรรมขึ้นอย่างต่อเนื่อง (PA 5.1) (2) กระบวนการที่กำหนดให้ประโยชน์และคุณค่าสูงสุดต่อองค์กร (PA 5.2) ตามภาพที่ 2.12 ในวงกลมหมายเลย 5



ภาพที่ 2.12 รูปแบบคุณลักษณะความสามารถของกระบวนการ

โดยการวัดผลความสำเร็จของการดำเนินการในแต่ละกระบวนการต้องได้รับการวัดผลความสำเร็จในแต่ละระดับอีกครั้ง ตามเงื่อนไขด้านล่าง จึงจะสามารถเลื่อนระดับ 1 เป็นระดับ 2 ได้ดังนี้

- N (Not achieved) คือ มีเพียงเล็กน้อยหรือไม่มีหลักฐานของการบรรลุผลความสำเร็จตามที่ได้กำหนดไว้ (ค่าความสำเร็จร้อยละ 0 – 15)
- P (Partially achieved) คือ มีหลักฐานบ้างอย่างของวิธีการที่จะดำเนินการและ การบรรลุผลสำเร็จบางอย่างของการกำหนดคุณลักษณะในการประเมินกระบวนการ บางส่วนของการบรรลุผลสำเร็จของคุณลักษณะที่ยังขาดการไม่ได้ (ค่าความสำเร็จร้อยละ 15 – 50)

- L (Largely achieved) คือ มีหลักฐานวิธีการดำเนินการอย่างเป็นระบบและมีนัยสำคัญที่จะบรรลุผลสำเร็จของการกำหนดคุณลักษณะในการประเมินกระบวนการ แต่ยังมีข้อบกพร่องเกิดขึ้นอยู่ในการประเมินกระบวนการ (ค่าความสำเร็จร้อยละ 50 – 85)
- F (Fully achieved) คือ มีหลักฐานวิธีการดำเนินอย่างเป็นระบบสมบูรณ์และมีการบรรลุผลสำเร็จสมบูรณ์ของการกำหนดคุณลักษณะในการประเมินกระบวนการ ไม่พบข้อบกพร่องที่มีนัยสำคัญที่เกี่ยวข้องเหลืออยู่ในคุณลักษณะในการประเมินกระบวนการ (ค่าความสำเร็จร้อยละ 85 – 100)

2.8 งานวิจัยที่เกี่ยวข้องกับแนวทางการศึกษาหลักการโคบิต 5

ทั้งนี้จากการศึกษา ของ Dong &Chao (2014),Azzaoui (2014), Christoph (2011), Razieh andNasser (2012), Felipe &Petar (2011), Petro (2015),Yannick, Frederik &Stefan (2014) และ Kobra (2014) นำเสนอผลงานวิจัยด้านความสัมพันธ์เชิงสถิติของ 7 ปัจจัยเอื้อตามหลักการโคบิต 5 ที่มีผลต่อการดำเนินงานตามกระบวนการที่โคบิตกำหนดขึ้นทั้งหมด 37 กระบวนการ โดย Frederik &Stefan เพิ่มเติมว่าผู้ปฏิบัติงานมีส่วนสำคัญในการดำเนินงานตามหลักการ นโยบายและกรอบการดำเนินงานจากฝ่ายกำกับดูแลเพื่อบรรลุผลสำเร็จตามเป้าหมายองค์กร Deepti & Ashwini Vasant (2013) นำเสนอแนวทางการเชื่อมโยงกฎระเบียบข้อบังคับธนาคารสากล (Basel III) กับหลักการโคบิต5 Rami (2014) และ Fredric, CISSP (2015) นำเสนอผลวิจัยในการเลือกกระบวนการตามหลักการโคบิต 5 เพื่อดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ สามารถเพื่อเพิ่มประสิทธิภาพในการระบุ วิเคราะห์และประเมินความเสี่ยงสารสนเทศขององค์กรให้บรรลุผลสำเร็จในการสร้างกระบวนการด้านความมั่นคงปลอดภัยสารสนเทศจากงานวิจัยของ Shengnan (Sophie) (2013),ShengnanandHans (2013),Yuichi (Rich) (2016) และ Avinash W. (2013) นำเสนอผลการวิจัยว่า แนวทางตามหลักการโคบิต 5 เอื้อประโยชน์ให้กับองค์กรมีความสามารถเพิ่มประสิทธิภาพ ประสิทธิผลและมูลค่าในเรื่อง การกำหนดนโยบาย (กลยุทธ์) และวัตถุประสงค์บริหารกระบวนการดำเนินงานเทคโนโลยีสารสนเทศ การบริหารทรัพยากร การสื่อสารข้อมูลภายในมีประสิทธิภาพมากขึ้นและกระบวนการดำเนินงานขององค์กรสามารถวัดผลได้รวมถึงการเพิ่มมูลค่าให้กับกระบวนการตรวจสอบเทคโนโลยีสารสนเทศและช่วยเพิ่มประสิทธิภาพควบคุมกระบวนการด้านเทคโนโลยีสารสนเทศ นอกจากนี้หลักการโคบิต 5 เป็นปัจจัยเอื้อให้องค์กรบรรลุผลการดำเนินงานด้านเทคโนโลยีสารสนเทศ (IT Governance) โดยเอื้อประโยชน์ให้กับองค์กรบรรลุผลในการดำเนินงานต่างๆ ดังนี้ (1) กลยุทธ์ต่างๆ ขององค์กรเป็นในทิศทางเดียวกัน (2) เพิ่มมูลค่าให้กับองค์กร (3) การบริหารทรัพยากรขององค์กร และ (4) การวัดประสิทธิภาพการดำเนินงานขององค์กร ยิ่งไปกว่านั้นโคบิตเป็นแนวคิดในระดับสูงสุดที่นำมาตรฐานสากลมารวมไว้

เป็นหนึ่งเดียวและง่ายสำหรับการไปปรับใช้งานโดยงานวิจัยนี้นำแนวคิดตามหลักการโคบิต 5 จากแนวทางการศึกษาจากผู้วิจัยต่างๆ ที่กล่าวไว้มาพัฒนาระบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5 ซึ่งกระบวนการบริหารความเสี่ยงกองทุนฯ และ/หรือ องค์กรใดๆ ที่นำแนวทางจากงานวิจัยนี้ไปปรับปรุงกระบวนการดำเนินงานด้านการบริหารความเสี่ยงจะได้ผลลัพธ์ของกระบวนการดำเนินงานที่สอดคล้องกับแนวทางการศึกษาที่กล่าวมาข้างต้น

2.9 บทสรุปงานวิจัยที่เกี่ยวข้องกับกรอบการดำเนินงานตามหลักการโคบิต 5

จากการศึกษางานวิจัยที่เกี่ยวข้องกับหลักการโคบิต 5 สรุปได้ดังนี้ (1) สามารถเพิ่มประสิทธิภาพและปรับปรุงกระบวนการทางธุรกิจได้และเชื่อมโยงความเข้าใจในการดำเนินงานกระบวนการต่างๆ ให้กับทุกฝ่ายงาน (2) เพิ่มมูลค่าให้กับกระบวนการตรวจสอบเทคโนโลยีสารสนเทศ (3) เป็นปัจจัยเอื้อให้องค์กรบรรลุวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศและการดำเนินงานต่างๆ ขององค์กรโดยองค์กรต้องวิเคราะห์สภาวะแวดล้อมที่แท้จริงเพื่อปรับแต่งหลักการโคบิต 5มาใช้กับองค์กร (4) มีมาตรฐานสากลรองรับและง่ายสำหรับนำไปปรับใช้งาน (5) กิจกรรมต่างๆ ที่โคบิต 5 แนะนำให้ดำเนินงานในกระบวนการต่างๆ สามารถส่งเสริมและสนับสนุนให้องค์กรบรรลุวัตถุประสงค์ที่องค์กรตั้งไว้และปรับสถานภาพเทคโนโลยีสารสนเทศองค์กร จาก ไร้ศักยภาพ เป็น อัจฉริยะภาพ งานวิจัยนี้นำแนวคิดตามหลักการโคบิต 5 ที่ได้ทำการศึกษาจากงานวิจัยต่างๆ ที่สนับสนุนองค์กรให้สามารถเพิ่มประสิทธิภาพและประสิทธิผลในการบรรลุวัตถุประสงค์ด้านการดำเนินงานและด้านเทคโนโลยีสานสนเทศ เพื่อมานำเป็นศึกษาเพิ่มเติมเพื่อนำเสนอ แนวทางการปรับปรุงและพัฒนาระบบ e – Studentloan เพื่อเพิ่มประสิทธิภาพให้กับกระบวนการกู้ยืมเงินของกองทุนเงินให้กู้ยืมเพื่อการศึกษาด้วยหลักการบริหารความเสี่ยงโคบิต 5 โดยนำเสนอการพัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

3. แนวคิดตามกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk)

ประกอบด้วย 3 องค์ประกอบ (3.1) ปัจจัยขับเคลื่อนการบริหารความเสี่ยง (3.2) ประโยชน์ที่ได้รับตามแนวทางการดำเนินงาน และ (3.3) สถานการณ์ความเสี่ยง

3.1 ปัจจัยขับเคลื่อนการบริหารความเสี่ยง ประกอบด้วย 2 ปัจจัย ดังนี้

3.1.1 ปัจจัยหลักในการขับเคลื่อนการบริหารความเสี่ยง

1) ผู้มีส่วนได้เสียที่มีความคิดเห็นยึดติดกับสิ่งใดสิ่งหนึ่งต่อสถานะความเสี่ยงขององค์กร

2) แนวทางการดำเนินการบริหารระดับความเสี่ยงที่ยังคงอยู่ในองค์กร

3) แนวทางการดำเนินการกำหนดความเสี่ยงที่เหมาะสมสำหรับองค์กร

4) การประเมินความเสี่ยงในเชิงปริมาณเป็นปัจจัยเอื้อให้ผู้มีส่วนได้เสียให้ความสนใจในค่าใช้จ่ายในการลดและความต้องการแหล่งทรัพยากรเพื่อบริหารความเสี่ยงมากกว่าความสูญเสียที่จะเกิดขึ้น

3.1.2 แนวทางในการบรรลุปัจจัยขับเคลื่อนการบริหารความเสี่ยงตามกรอบการดำเนินงานความเสี่ยงสารสนเทศของโคบิต 5 (COBIT5 for Risk)

1) แนวทางการดำเนินการสร้างการกำกับดูแลและหน้าที่การบริหารความเสี่ยงตามกรอบการดำเนินงานสารสนเทศของโคบิต 5 สำหรับองค์กร

2) แนวทางและวิธีการสร้างการนำหลักการการดำเนินงานสารสนเทศของโคบิต 5 สำหรับองค์กรไปกำกับดูแลและบริหารความเสี่ยงสารสนเทศ

3) แสดงความชัดเจนในเรื่องความเชื่อมโยงของกรอบการดำเนินความเสี่ยงสารสนเทศของโคบิต 5 กับมาตรฐานอื่นที่เกี่ยวข้อง

3.2 ประโยชน์ที่จะได้รับตามแนวทางการดำเนินงาน

3.2.1 แนวทางการบริหารความเสี่ยงเริ่มต้นจนสิ้นสุดกระบวนการ

3.2.2 วิธีการพื้นฐานและยั่งยืนสำหรับการประเมินและตอบสนองความเสี่ยง

3.2.3 ความเสี่ยงที่มีความสำคัญในปัจจุบันและอนาคตทั่วทั้งองค์กรมีความชัดเจนมากขึ้น รวมทั้งผลกระทบจากความเสี่ยงที่มีต่อองค์กรด้วย

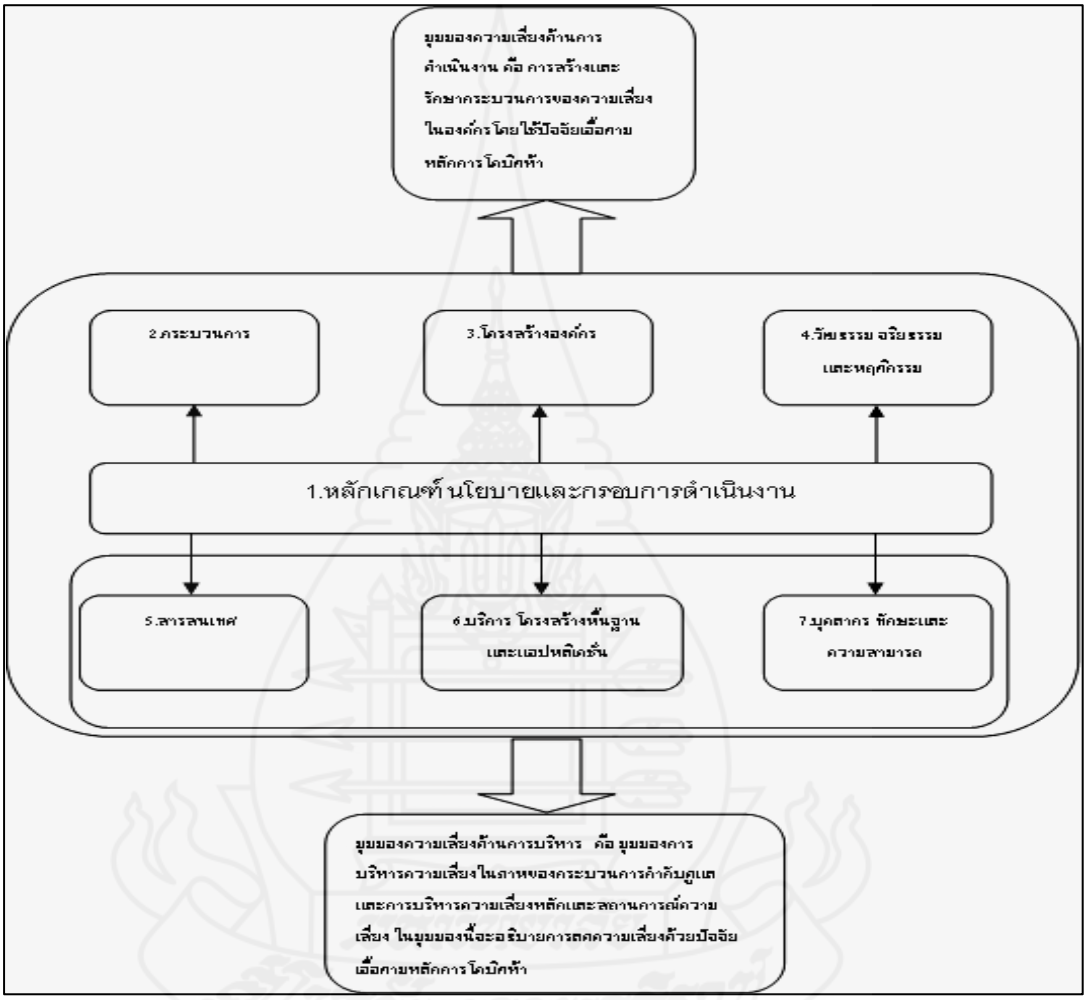
3.2.4 มีความเข้าใจในประสิทธิภาพการบริหารความเสี่ยงสารสนเทศให้ได้ประโยชน์สูงสุดโดยปัจจัยเอื้อของกระบวนการที่มีประสิทธิผลและประสิทธิภาพ

3.2.5 สร้างโอกาสที่จะสามารถรวบรวมการบริหารความเสี่ยงสารสนเทศกับความเสี่ยงทั้งหมดและโครงสร้างกฎระเบียบภายในองค์กร

3.2.6 สร้างการสนับสนุนของบทบาทหน้าความรับผิดชอบต่อความเสี่ยงและการยอมรับความเสี่ยงทั่วทั้งองค์กร

3.2.1 สร้างความเข้าใจในองค์ประกอบของความเสี่ยง แบ่งเป็น 2 องค์ประกอบ ดังนี้

1) มุมมองความเสี่ยง (Risk Perspective) คือ แสดงมุมมองความเสี่ยงรวมขององค์กร



ภาพที่ 2.13 มุมมองความเสี่ยง

จากภาพที่ 2.13 แสดงปัจจัยเอื้อของโคบิต 5 ในมุมมองความเสี่ยง 2 ด้าน ได้แก่

2) มุมมองความเสี่ยงด้านการดำเนินการ แบ่งเป็น 2 มุมมอง ดังนี้

(1) มุมมองความเสี่ยงด้านการดำเนินงาน

อธิบายการกำหนดและดำเนินการความเสี่ยงด้านการดำเนินงานภายในองค์กรโดยปัจจัยเอื้อของโคบิต 5 (COBIT 5 enablers) ซึ่งกระบวนการดำเนินงานความเสี่ยง

โคบิต 5 (COBIT5 for Risk) อธิบายขั้นตอนการดำเนินงานของแต่ละปัจจัยเอื้อที่นำมาใช้ในการกำกับดูแลและบริหารความเสี่ยงด้านการดำเนินงานทั่วทั้งองค์กร ยกตัวอย่าง (1) มีกระบวนการดำเนินงานใดบ้างที่ต้องการระบุและสนับสนุนเพื่อกำกับและบริหารความเสี่ยงด้านการดำเนินงาน (2) สารสนเทศใดบ้างที่ต้องการกำกับและบริหารความเสี่ยง เช่น ความเสี่ยงทั้งหมดขององค์กร หรือ ประเภทความเสี่ยง (3) โครงสร้างองค์กรที่ต้องการกำกับและบริหารความเสี่ยงอย่างมีประสิทธิภาพ และ (4) จัดวางบุคลากรที่มีความรู้ความสามารถดำเนินการบริหารความเสี่ยงด้านดำเนินงานได้อย่างเหมาะสม

ภาพที่ 2.14 หลักการความเสี่ยงโคบิต 5

จากภาพ 2.14 แสดงกรอบการดำเนินงานความเสี่ยงโคบิต 5 กำหนด 7 หลักการบริหารความเสี่ยง ได้แก่ (1) เชื่อมโยงกับเป้าหมายองค์กร (2) เชื่อมโยงกับกรอบการบริหารความเสี่ยงเชิงบูรณการ (COSO ERM) (3) ความสมดุลในการบริหารความเสี่ยงเพื่อลงทุนเทคโนโลยีสารสนเทศ (4) สนับสนุนการสื่อสารทั่วทั้งองค์กร (5) สร้างความร่วมมือจากระดับบริหารถึงระดับปฏิบัติการและความรับผิดชอบในหน้าที่ (6) การปฏิบัติตามหน้าที่เป็นส่วนหนึ่งของกิจกรรมประจำวัน และ (7) วิธีการสมยอม โดยดำเนินการอย่างเป็นระบบ ตรงตามกำหนดการตามแผนบริหารความเสี่ยงทำให้ได้ผลลัพธ์เป็นที่ยอมรับ เปรียบเทียบได้และน่าเชื่อถือ

กรอบการดำเนินงานความเสี่ยงโคบิต 5 กำหนดกระบวนการดำเนินงานตามโคบิต 5ทั้งหมด (COBIT5 processes) เพื่อนำไปใช้สนับสนุนตามความต้องการบริหารความเสี่ยงด้านการดำเนินงาน ตามภาพที่ 2.13 คือการกำกับดูแลหรือให้ความเชื่อมั่นความเสี่ยง (EDM03 Ensure Risk Optimisation) และการบริหารความเสี่ยง (APO12 Manage Risk)

(2) มุมมองความเสี่ยงด้านบริหาร

กำกับดูแลความเสี่ยงหลัก กระบวนการบริหารความเสี่ยงและสถานการณ์ความเสี่ยงขององค์กร ซึ่งอธิบายกระบวนการลดความเสี่ยง โดยปัจจัยเอื้อของโคบิต 5 (COBIT 5 enablers) เป็นแนวทางหลักสำหรับการบริหารความเสี่ยงอย่างมีประสิทธิภาพ ประกอบด้วย 3 สิ่ง ดังนี้

ก. กระบวนการบริหารความเสี่ยงหลักที่มีประสิทธิภาพและประสิทธิผลที่องค์กรนำไปใช้ในการบริหารความเสี่ยง

ข. สำหรับสร้างสถานการณ์ความเสี่ยงเพื่อ กำหนด วิเคราะห์ และตอบสนองความเสี่ยง ซึ่งเป็นสถานการณ์ความเสี่ยงที่เป็นรูปธรรม จับต้องได้และสะท้อนความเสี่ยงที่แท้จริงขององค์กร

ค. โคบิต 5 สามารถตอบสนองกับความเสี่ยงที่ยอมรับไม่ได้

3.3 สถานการณ์ความเสี่ยง (Risk scenario)

ภาพที่ 2.15 สถานการณ์ความเสี่ยง (Risk scenario) แบบจำลองสำหรับความเสี่ยงกองทุน

จากภาพที่ 2.15 แสดงรายละเอียดของสถานการณ์ความเสี่ยงแบบจำลองสำหรับความเสี่ยงกองทุน ดังนี้

3.3.1 สถานการณ์ความเสี่ยง คือ การอธิบายสถานการณ์ต่างๆ ที่อาจจะเกิดขึ้นและเมื่อเกิดขึ้นจะมีผลกระทบต่อความไม่แน่นอนต่อองค์กรที่จะไม่สามารถบรรลุเป้าหมายที่กำหนดไว้ โดยผลกระทบที่เกิดขึ้นอาจจะเป็นผลเชิงบวกหรือเชิงลบได้

3.3.2 สถานการณ์ความเสี่ยงเป็นส่วนสำคัญของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (EDM03 และ APO12 ตามภาพที่ 2.13) ประกอบด้วย 2 วิธีการดังนี้

1) วิธีการแบบบนสู่ล่าง (Top – Down approach) คือ สร้างสถานการณ์ความเสี่ยงสารสนเทศที่ส่งผลกระทบทำให้ไม่สามารถบรรลุเป้าหมายและองค์ประกอบสำคัญที่เกี่ยวข้องทั้งหมดขององค์กร

2) วิธีการแบบล่างสู่บน (Down – Top approach) คือ นำรายการสถานการณ์ต่างๆ มากำหนดรูปแบบปรับแต่งสถานการณ์ที่เกี่ยวข้องให้ใกล้กับความจริงมากที่สุด

(1) วิธีการทั้งสองเป็นวิธีการที่ต้องดำเนินการควบคู่กันรวมทั้งควรดำเนินการในช่วงเวลาเดียวกัน

(2) สถานการณ์ความเสี่ยงต้องมีความสัมพันธ์และเชื่อมโยงกับความเสี่ยงที่แท้จริงขององค์กร

(3) ความเสี่ยงชี้เฉพาะสำหรับแต่ละองค์กรและความต้องการที่จำเป็นของธุรกิจต้องได้รับการพิจารณาในสถานการณ์ความเสี่ยงขององค์กร

(4) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ให้คำอธิบายความหมายรูปแบบสถานการณ์ความเสี่ยงต่างๆ (Generic risks) โดยสามารถใช้เป็นแหล่งอ้างอิงเพื่อลดโอกาสในการมองข้ามทั้งสถานการณ์ความเสี่ยงสูงหรือต่ำได้

3.3.3 การตอบสนองความเสี่ยง (Risk response)

ตอบสนอบความเสี่ยงโดยนำความเสี่ยงที่ถูกกำหนดแปลงเป็นความเสี่ยงขององค์กร

1) การตอบสนองความเสี่ยงจำเป็นต้องได้รับการกำหนดมากที่สุดเท่าที่จะเป็นได้กับความเสี่ยงที่ยังคงมีอยู่ในอนาคต

2) เมื่อการวิเคราะห์ความเสี่ยงแสดงให้เห็นว่าไม่เชื่อมโยงกับการกำหนดความเสี่ยงที่ยอมรับได้และระดับของการยอมรับได้ การตอบสนองความเสี่ยงจึงมีความจำเป็น

3) การตอบสนองความเสี่ยงสามารถเลือกดำเนินการได้ 4 ประเภท ได้แก่ (1) หลีกเลี่ยง(2) ลด (3) แบ่งปัน/โอน และ (4) ยอมรับ

4) การประเมินผลการตอบสนองความเสี่ยงไม่ใช่การดำเนินการเพียงครั้งเดียวแต่เป็นวงจรของกระบวนการบริหารความเสี่ยง (Risk management process cycle)

3.3.4 การดำเนินการลดความเสี่ยง (Risk Mitigation)

1) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ให้จำนวนตัวอย่างของปัจจัยเอื้อของโคบิต 5 (COBIT enablers) ที่สามารถใช้ในการตอนสนองสถานการณ์ความเสี่ยง

2) การดำเนินงานเพื่อลดความเสี่ยงจะเกิดขึ้นเมื่อเทียบเคียงกับการดำเนินการควบคุมระบบเทคโนโลยีสารสนเทศ

3) ตามความหมายของโคบิต 5 การควบคุมระบบเทคโนโลยีสารสนเทศสามารถเป็นได้จากทุกปัจจัยเอื้อ เช่น กำหนดความเหมาะในโครงสร้างขององค์กร กำหนดความเหมาะในการกำกับดูแล หรือการฝึกปฏิบัติการบริหารหรือกิจกรรม

3.3.5 ระดับความเสี่ยงที่สามารถรับได้ (Risk Capacity)

1) ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ จำนวนความเสี่ยงขององค์กรที่ยอมรับได้

2) ความเสี่ยงที่ต้านทานได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนที่ยอมรับได้จากตัววัดผลการดำเนินงานที่เกี่ยวข้องกับการบรรลุเป้าหมาย

3) ระดับความเสี่ยงที่สามารถรับได้ (Risk Capacity) คือ มูลค่าความสูญเสียสะสมขององค์กรที่สามารถต้านทานได้โดยไม่มีความเสี่ยงในการดำเนินงาน ณ ปัจจุบัน

3.3.6 ความสัมพันธ์ของกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) กับมาตรฐานที่เกี่ยงข้อง

1) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) (เป็นกระบวนการตามกรอบการดำเนินงานโคบิต 5 (COBIT5)) คือ วิธีการภายใต้กรอบการดำเนินงานโคบิต 5 (COBIT5) สำหรับดำเนินการในด้านกิจกรรมความเสี่ยง

2) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) กับความสัมพันธ์ในมาตรฐานความเสี่ยงสากลต่างๆ ดังนี้

3.3.7 มาตรฐานการบริหารความเสี่ยง (ISO 31000:2009)

1) หลักเกณฑ์ (Principles) ปัจจัยเอื้อ (Enablers) และรูปแบบปัจจัยเอื้อ (Enabler Model) ของกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ดำเนินการตามหลักเกณฑ์เดียวกับมาตรฐานการบริหารความเสี่ยง (ISO 31000:2009)

2) รูปแบบและกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ครอบคลุมในรายละเอียดที่มีสาระสำคัญตามมาตรฐานการบริหารความเสี่ยง

3) ทุกองค์ประกอบในกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ได้ให้คำอธิบายขยายความในสาระสำคัญตามมาตรฐานการบริหารความเสี่ยง โดยเฉพาะในเรื่องการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

3.3.8 มาตรฐานการบริหารความเสี่ยงความมั่นคงปลอดภัยสารสนเทศขององค์กร (ISO 27005:2011)

1) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ดำเนินการภายใต้คำอธิบายทุกองค์ประกอบตามมาตรฐาน การบริหารความเสี่ยงความมั่นคงปลอดภัยสารสนเทศขององค์กร

2) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) นำภาพรวมของการบริหารความเสี่ยงเทคโนโลยีสารสนเทศเปรียบเทียบกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศขององค์กร (ISO 27005) โดยเน้นในเรื่องการบริหารความมั่นคงปลอดภัยที่เกี่ยวข้องกับความเสี่ยง

3) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ให้ความสำคัญอย่างมากในกระบวนการและการนำไปปฏิบัติเพื่อให้ความเชื่อมั่นในการเชื่อมโยงกับเป้าหมายของธุรกิจ การยอมรับทั่วทั้งองค์กรและความสมบูรณ์ของขอบเขตการดำเนินงานตามปัจจัยต่างๆ

3.3.9 กรอบโครงสร้างการบริหารความเสี่ยงองค์กรเชิงกำกับดูแล (COSO ERM)

1) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ดำเนินการทั้งหมดตามองค์ประกอบของกรอบโครงสร้างการบริหารความเสี่ยงองค์กรเชิงกำกับดูแล COSO ERM

2) กรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) ไม่ได้เน้นหนักในเรื่องการควบคุมแต่มีการเชื่อมโยงไปยังปัจจัยเอื้อต่างๆ (Enablers) ในเรื่องการบริหารการดำเนินงานตามกรอบการดำเนินงานสารสนเทศสำหรับองค์กร (COBIT5 framework)

3) สาระสำคัญทั้งเรื่องที่เกี่ยวกับการควบคุมและการบริหารความเสี่ยงทั่วไปที่กำหนดในกรอบโครงสร้างการบริหารความเสี่ยงองค์กรเชิงกำกับดูแล (COSO ERM) ปรากฏอยู่ในกรอบการดำเนินงานความเสี่ยงโคบิต 5 (COBIT5 for Risk) 2 ส่วนดังนี้

(1) หลักเกณฑ์และการออกแบบกรอบแนวคิด

(2) รูปแบบกระบวนการและการให้แนวทางเพิ่มเติมในกรอบการดำเนินงาน

3.4 งานวิจัยที่เกี่ยวข้อง

ในงานวิจัยนี้นำกระบวนการและกิจกรรมตามหลักการบริหารความเสี่ยงโคบิต 5 มาปรับปรุงการดำเนินงานบริหารความเสี่ยงกองทุนฯ เพื่อให้กองทุนฯ สามารถ ระบุ วิเคราะห์ ประเมินสร้างวิธีการจัดเก็บ สร้างสถานการณ์ความเสี่ยง ปรับสถานการณ์ความเสี่ยงเข้ากับ

สถานการณ์จริงเข้ากับสภาพแวดล้อมกองทุนฯ เป็นต้น สอดคล้องกับการศึกษาของ Karel (2013),Dwi Rosa, Harlili, Afriyan (2014), Bo˘stjan (2008) , Heru (2014), Richards (2013), Vince (2013), Anestis (2012) และ Kristen (2013) พบว่า การระบุ ประเมินและลงทะเบียนความเสี่ยงทางเทคโนโลยีสารสนเทศสามารถสร้างการเชื่อมโยงเป้าหมายขององค์กรกับเป้าหมายด้านเทคโนโลยีสารสนเทศให้บรรลุผลสำเร็จได้ตามที่กำหนดอีกทั้งยังสามารถวางแผนโครงการต่างๆ ได้ครอบคลุมทุกส่วนที่ต้องการแก้ไขและพัฒนา เป็นผลตามความต้องการขององค์กรได้ โดยงานวิจัยครั้งนี้นำแนวทางจากกรณีศึกษาซึ่งเป็นองค์ประกอบในกิจกรรมของกระบวนการบริหารความเสี่ยงโคบิต 5 มาพัฒนาระบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลและบริหารความเสี่ยงตามหลักการโคบิต 5

ในงานวิจัยได้นำเสนอกระบวนการและกิจกรรมที่ติดตั้งอยู่ในระบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลและบริหารความเสี่ยงโคบิต 5 ในเรื่องการระบุความเสี่ยงที่เกี่ยวข้องกับ กฎ ระเบียบ ข้อบังคับ และกฎหมายที่กองทุนฯ ต้องยึดถือปฏิบัติตามข้อกำหนดดังกล่าว รวมทั้งครอบคลุมกระบวนการและกิจกรรมที่เกี่ยวข้องกับการบริหารความเสี่ยงของกองทุนฯ ทั่วทั้งองค์กร ซึ่งสอดคล้องกับการศึกษาของ Maher (2012) ที่เกี่ยวข้องกับความรับผิดทางกฎหมายและสอดคล้องกับการศึกษาของ Matthew (2008) ในเรื่องการดำเนินงานบริหารความเสี่ยงเพื่อนำมา ปรับปรุงและพัฒนาระบบกู้ยืมเงินของกองทุนฯในแบบเชิงบูรณาการ (แบ่งแยกการกำกับดูแลออกจากการบริหาร) และสอดคล้องกับการศึกษาของ Akbar (2014) ในผลสรุปงานวิจัยในเรื่องกระบวนการความเสี่ยงตามหลักการโคบิต 5 ส่งผลให้กระบวนการบริหารความเสี่ยงเกิดประโยชน์ทั่วทั้งองค์กรและ Madhav (2014) ในเรื่องความสามารถในการกำหนดทิศทาง ออกแบบสถานการณ์ความเสี่ยงในการบริหารตามความต้องการขององค์กร รวมทั้งสอดคล้องกับการศึกษาของ Onyeka, Shaun, & Sergey (2014) และ Urs (2011) ในเรื่องเดียวกัน

อีกทั้งการศึกษาจากงานวิจัยนี้สามารถสร้างกระบวนการและกิจกรรมที่เป็นมาตรฐานและนำเสนอแนวทางการบริหารความเสี่ยงตามหลักการโคบิต 5 สำหรับกองทุนฯ ให้บรรลุเป้าหมายที่ตั้งไว้สอดคล้องกับการศึกษาของ Walid & Basil (2015) ในผลงานวิจัยที่กล่าวว่า การบริหารความเสี่ยงตามหลักการโคบิต 5 สามารถกำหนดกระบวนการและกิจกรรมการดำเนินงานขององค์กรให้สามารถบรรลุตามเป้าหมายที่องค์กรตั้งไว้

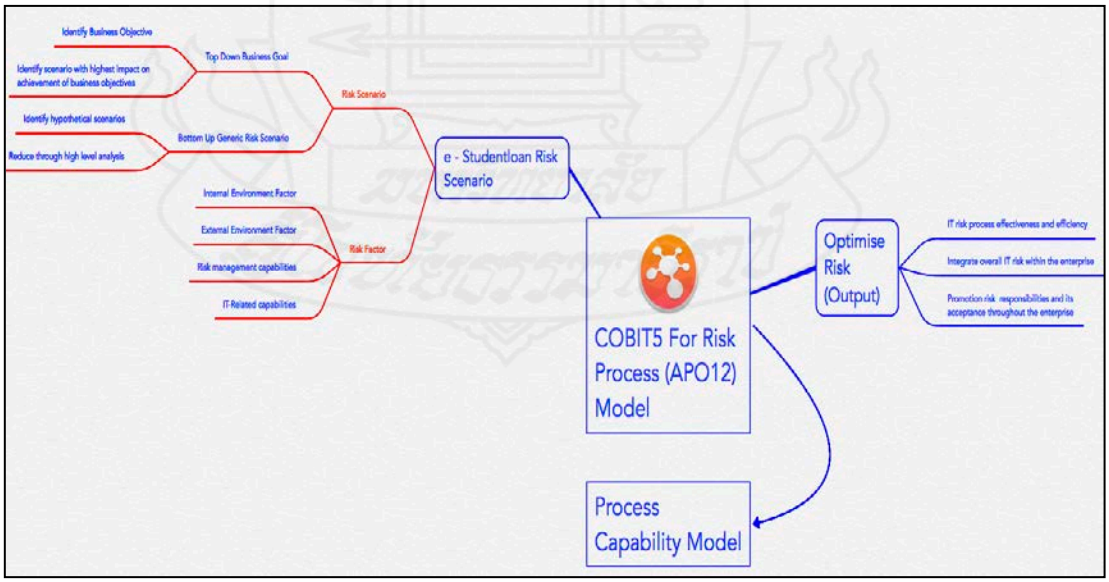
3.5 บทสรุปงานวิจัยที่เกี่ยวข้องกับกรอบการดำเนินงานตามหลักการบริหารความเสี่ยงโคบิต 5

งานวิจัยนี้นำแนวคิดการบริหารความเสี่ยงตามหลักการโคบิต 5 จากการศึกษาจากงานวิจัยที่เกี่ยวข้องในประเด็นของผลงานวิจัยในเรื่อง การระบุ ประเมินและลงทะเบียนความเสี่ยงทางเทคโนโลยีสารสนเทศสามารถสร้างการเชื่อมโยงเป้าหมายขององค์กรกับเป้าหมายด้าน

เทคโนโลยีสารสนเทศให้บรรลุผลสำเร็จได้ ความรับผิดทางกฎหมายการดำเนินงานบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อนำมา ปรับปรุงและพัฒนาระบบแบบเชิงบูรณาการ ความสามารถในการกำหนดทิศทาง ออกแบบสถานการณ์ความเสี่ยงในการบริหารตามความต้องการขององค์กรที่กล่าวข้างต้น สนับสนุนและส่งเสริมองค์กรให้สามารถเพิ่มประสิทธิภาพและประสิทธิผลในการบรรลุวัตถุประสงค์ด้านการดำเนินงานและด้านเทคโนโลยีสานสนเทศ เพื่อมานำเป็นศึกษาเพิ่มเติม โดยนำเสนอ แนวทางการปรับปรุงและพัฒนาระบบ e – Studentloan เพื่อเพิ่มประสิทธิภาพให้กับกระบวนการกู้ยืมเงินของกองทุนเงินให้กู้ยืมเพื่อการศึกษาด้วยหลักการบริหารความเสี่ยงโคบิต 5 และพัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

บทที่ 3
วิธีการดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงประจักษ์ (Empirical research) ตามภาพที่ 3.1 แสดงสถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 ใช้ชุดของข้อมูลจริงจากข้อมูลการดำเนินงานบริหารความเสี่ยงของกองทุนเพื่อสร้างสถานการณ์ความเสี่ยงและกำหนดปัจจัยเสี่ยง (Input) กล่าวในข้อ (1) ศึกษาความเสี่ยงกองทุนเพื่อสร้างแบบจำลองความเสี่ยงกองทุน (Study SLF's riskfor SLF's risk scenario) (2) วิเคราะห์ปัจจัยเสี่ยงกองทุน (3) ออกแบบสถานการณ์ความเสี่ยงกองทุนและสถานการณ์อื่นที่เกี่ยวข้องจากการวิเคราะห์ความเสี่ยงกองทุน (4) เพื่อทดสอบกับรูปแบบตรวจสอบและวัดความสามารถกระบวนการกำกับดูแลความเสี่ยงและกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (Process) แบ่งเป็นกระบวนการกำกับดูแลความเสี่ยง (EDM03) 3 กระบวนการ และ กระบวนการบริหารความเสี่ยง (APO12) 6 กระบวนการ รวม 9 กระบวนการ (5) ทดสอบแบบจำลองสถานการณ์การความเสี่ยงกับรูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 (6) ผลผลิตกระบวนการบริหารความเสี่ยงกองทุนตามหลักการบริหารความเสี่ยงโคบิต 5 และ (7) ประเมินผลสถานการณ์ความเสี่ยงกองทุนที่ดำเนินตามขั้นตอนหลักการโคบิต 5

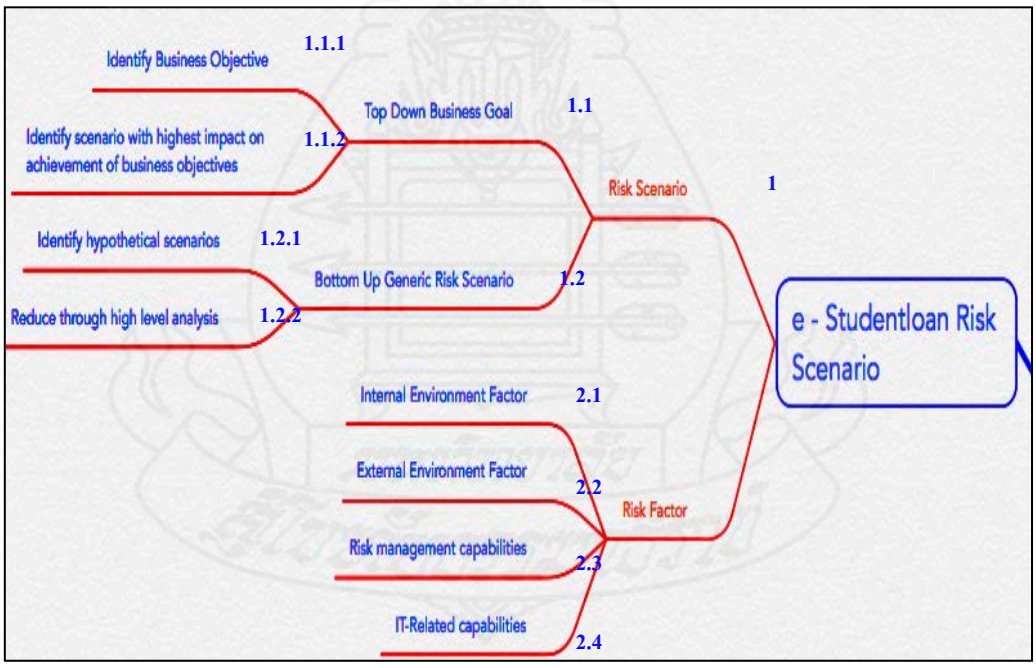


ภาพที่ 3.1 สถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5

งานวิจัยนี้จัดทำเพื่อตอบวัตถุประสงค์ 1) เพื่อพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนเชื่องโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5 2) เพื่อพัฒนาระบบสารสนเทศของกองทุนตามกระบวนการบริหารความเสี่ยงโคบิต 5 และ 3) เพื่อทดสอบแบบจำลองสถานการณ์ความเสี่ยงและประเมินผลสถานการณ์ความเสี่ยงโดยมีวิธีการดำเนินงานและออกแบบรูปแบบกระบวนการวิจัย ดังนี้

1. ศึกษาความเสี่ยงกองทุนเพื่อสร้างแบบจำลองความเสี่ยงกองทุน (Study SLF's riskfor SLF's risk scenario) อธิบาย กระบวนการ 1 2 3

จากภาพที่ 3.1 ศึกษากระบวนการดำเนินงานของระบบ e – Studentloan จากคู่มือผู้ปฏิบัติงาน กองทุนเงินให้กู้ยืมเพื่อการศึกษา ในการระบุความเสี่ยงจากกระบวนการดำเนินงานของระบบ e – studentloan (1) สร้างแบบจำลองความเสี่ยงกองทุน และ (2) วิเคราะห์ปัจจัยเสี่ยงกองทุน



ภาพที่ 3.2 เตรียมข้อมูลความเสี่ยงกองทุนเพื่อเข้าสู่กระบวนการบริหารความเสี่ยงโคบิต 5

จากภาพที่ 3.2 แสดงรายละเอียดการเตรียมข้อมูลความเสี่ยงกองทุนเพื่อเข้าสู่กระบวนการบริหารความเสี่ยงโคบิต 5 (1.1) วิเคราะห์สถานการณ์ความเสี่ยงกองทุน (ระดับนโยบายของกองทุน) และ (1.2) วิเคราะห์สถานการณ์ความเสี่ยงกองทุน (ระดับการปฏิบัติงาน)

1.1 วิเคราะห์สถานการณ์ความเสี่ยงกองทุน (ระดับนโยบายของกองทุน)

1.1.1 กำหนดนโยบายหรือวัตถุประสงค์ของกองทุนจากคณะกรรมการกองทุนเงินให้กู้ยืมเพื่อการศึกษา

1.1.2 กำหนดสถานการณ์ความเสี่ยงที่มีผลกระทบต่อกองทุนมากที่สุดเพื่อกำหนดนโยบายหรือวัตถุประสงค์ของกองทุน

1.2 วิเคราะห์สถานการณ์ความเสี่ยงกองทุน (ระดับการปฏิบัติงาน)

1.2.1 กำหนดสมมุติฐานสถานการณ์ความเสี่ยงของกองทุน

1.2.2 วิเคราะห์การลดระดับความเสี่ยงที่มีความสูงมากของกองทุน

2. วิเคราะห์ปัจจัยเสี่ยงกองทุน

2.1 วิเคราะห์ความเสี่ยงจากปัจจัยแวดล้อมภายในกองทุน

2.1.1 เป้าหมายและวัตถุประสงค์ของกองทุน

2.1.2 ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศที่สำคัญของกองทุน

2.1.3 ความซับซ้อนของเทคโนโลยีสารสนเทศกองทุน

2.1.4 ความซับซ้อนของเอกลักษณ์และระดับความเปลี่ยนแปลงของกองทุน

2.1.5 ความสามารถในการบริหารความเปลี่ยนแปลงของกองทุน

2.1.6 รูปแบบการดำเนินงานของกองทุน

2.1.7 การเรียงลำดับยุทธศาตร์กองทุน

2.1.8 วัฒนธรรมของกองทุน

2.1.9 ความสามารถทางการเงินของกองทุน

2.2 วิเคราะห์ความเสี่ยงจากปัจจัยแวดล้อมภายนอกกองทุน

2.2.1 สถานการณ์ทางการเมือง

2.2.2 ข้อบังคับเกี่ยวกับ กฎหมาย ระเบียบที่เกี่ยวข้อง

2.2.3 สถานภาพและวิวัฒนาการทางเทคโนโลยีสารสนเทศ

2.3 ความสามารถของกองทุนในการบริหารความเสี่ยง

2.3.1 ด้านการกำกับดูแลความเสี่ยง

2.3.2 ด้านการบริหารความเสี่ยง

2.4 ความสามารถของกองทุนในการบริหารเทคโนโลยีสารสนเทศ

2.4.1 ประเมิน สั่งการและติดตาม (EDM)

2.4.2 จัดวาง จัดทำแผนและจัดระบบ (APO)

2.4.3 จัดสร้าง จัดหาและนำไปใช้ (BAI)

2.4.4 ส่งมอบ บริการและสนับสนุน (DSS)

2.4.5 เฝ้าติดตาม วัดผลและประเมิน (MEA)

3. ออกแบบสถานการณ์ความเสี่ยงกองทุนและสถานการณ์อื่นที่เกี่ยวข้องจากการวิเคราะห์ความเสี่ยงกองทุน (3.1) ออกแบบสมมุติสถานการณ์ความเสี่ยงกองทุน และ (3.2) บันทึกสถานการณ์ความเสี่ยงตามรูปแบบที่โคบิต 5 กำหนด

3.1 ออกแบบสมมุติสถานการณ์ความเสี่ยงกองทุน (ระบบ e – Studentloan) ตามสภาพแวดล้อมที่เกิดขึ้น จากกระบวนการให้กู้ยืม ตามคู่มือ ผู้ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษาตามหลักการสถานการณ์ความเสี่ยงโคบิต 5 (Risk scenario Using Cobit5 for Risk, 2014). ตามตารางที่ 3.1 เพื่อเป็นข้อมูลนำเข้าระบบการตรวจสอบและวัดความสามารถการกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5 (Input) ตามภาพที่ 3.2

ตารางที่ 3.1 ตารางสถานการณ์ความเสี่ยงภาพรวมของระบบกู้ยืมเงินกองทุน (Input)

เลขที่อ้างอิง	สถานการณ์ความเสี่ยง	ประเภทความเสี่ยง					ตัวอย่างสถานการณ์	
		สารสนเทศให้ประโยชน์/เพิ่มมูลค่าแก่กองทุนฯ	โปรแกรม/โครงการด้านสารสนเทศ	ของกองทุนฯ ดำเนินการเสร็จ	การดำเนินการ/การให้บริการด้านสารสนเทศของกองทุนฯ ดำเนินการได้		สถานการณ์เชิงลบ	สถานการณ์เชิงบวก
201	การบริหารวงจรโปรแกรม/โครงการ (การเริ่มต้นโปรแกรม/โครงการ เศรษฐกิจการส่งมอบคุณภาพและการยกเลิก)	P	P	S			ความล้มเหลว (ต้นทุน ความล้าช้าขอบเขตไม่แน่นอน และการเปลี่ยนแปลงการลำดับความสำคัญความของกองทุนฯ ฯ/ธุรกิจ) โครงการยกเลิก มีโอกาสที่จะส่งมอบโครงการทางเทคโนโลยีสารสนเทศล้าช้า	ยกเลิกโครงการทันเวลา
203		S	P					โครงการส่งมอบทันเวลา

หมายเหตุ P หมายถึง เป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดผลกระทบต่อกองทุนในระดับสูงสุด

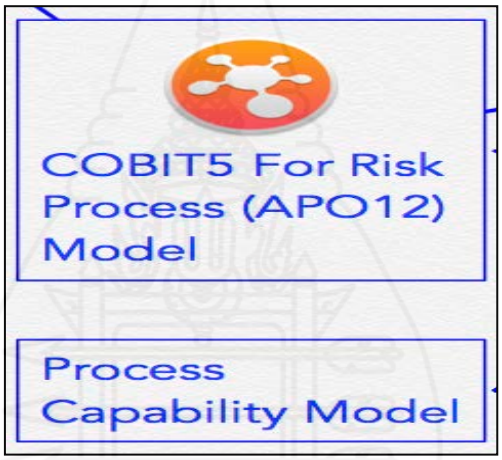
S หมายถึง เป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดผลกระทบต่อกองทุนในระดับต่ำลงมา

ช่องว่าง หมายถึง ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ส่งผลกระทบต่อกองทุน

3.2 บันทึกสถานการณ์ความเสี่ยงตามรูปแบบที่โคบิต 5 กำหนด (ตามตารางที่ 4.2)

4. พัฒนารูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5 (Process: COBIT 5 for riskmodel ของกองทุน ระบบ e – studentloan)

จากภาพที่ 3.3 และรายละเอียดตามตารางที่ 3.2 – 3.14



ภาพที่ 3.3 กระบวนการตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

จากภาพที่ 3.3 ออกแบบและกำหนดรายละเอียดของกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5 ประกอบด้วย 2 กระบวนการหลัก ได้แก่ (4.1) กระบวนการกำกับการดูแลและ (4.2) การบริหารความเสี่ยงของโคบิต 5 (Ensure Risk Optimization EDM03, Manage Risk APO 012) ทั้งหมด 9 กระบวนการ (สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ ภาคพื้นกรุงเทพ, 2555) ดังนี้

4.1 การกำกับดูแลความเสี่ยง (EDM03 Evaluate, Direct, and Monitor)

4.1.1 ประเมินการบริหารความเสี่ยง (EDM03.01 Evaluate risk management)

ตรวจสอบอย่างต่อเนื่องและทำการตัดสินใจกับความเสี่ยงที่คงอยู่ขององค์กรและในอนาคตที่องค์กรจะนำเทคโนโลยีสารสนเทศมาใช้ พิจารณาความเสี่ยงที่องค์กรยอมรับได้และระบุและจัดการความเสี่ยงนั้นๆ ที่เกิดประโยชน์แก่การนำเทคโนโลยีสารสนเทศขององค์กรมาดำเนินงาน โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.2

ตารางที่ 3.2 วิธีการดำเนินการกำกับดูแลด้านการประเมินความเสี่ยง

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.01)				
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต	
ประเมินความเสี่ยง	จาก กระบวนการ	รายละเอียด	รายละเอียด	ไปสู่ กระบวนการ
ประเมินกำรบริหารความเสี่ยง ตรวจสอบและใช้วิจารณญานในการพิจารณาอย่าง ต่อเนื่องถึงผลกระทบของความเสี่ยงด้านการใช้ไอที ในองค์กรทั้งปัจจุบันและอนาคต พิจารณาความ เหมาะสมของระดับความเสี่ยงขององค์กรที่ยอมรับ ได้ และมีการระบุและบริหารจัดการความเสี่ยงที่มีต่อ คุณค่าขององค์กรซึ่งเกี่ยวข้องกับการใช้ไอที	APO12.01	ประเด็นความเสี่ยงที่เกิดขึ้น	แนวทางระดับความเสี่ยงที่ยอมรับได้	APO12.03
			การอนุมัติระดับความเสี่ยงที่องค์กรรับได้	APO12.03
	มาตรฐารอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ	การวัดผลกิจกรรมการบริหารความเสี่ยง	APO12.01
กิจกรรมที่ต้องดำเนินการ				
1. กำหนดระดับของความเสี่ยงด้านไอทีที่กองทุนฯ สามารถยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์				
2.ประเมินและอนุมัติค่าที่นำเสนอสำาหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านไอทีที่ยอมรับได้เทียบกับระดับของความเสี่ยงและโอกาสที่กองทุนฯ ยอมรับได้				
3.พิจารณาว่ายุทธศาสตร์ความเสี่ยงด้านไอทีสอดคล้องกับยุทธศาสตร์ความเสี่ยงระดับกองทุนฯ มากน้อยเพียงใด				
4.ประเมินปัจจัยเสี่ยงด้านไอทีในเชิงรุกสำหรับการตัดสินใจเชิงยุทธศาสตร์ของกองทุนฯ ที่รอดำเนินการ และมั่นใจว่าการตัดสินใจของกงอทุนฯ ได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว				
5.พิจารณาว่ามีการประเมินและวัดผลความเสี่ยงของการใช้ไอทีอย่างเหมาะสม ตามมาตรฐานต่างๆ ที่เกี่ยวข้องทั้งของในประเทศและสากล				
6.ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุนฯ ในการรับความสูญเสียที่เกี่ยวข้องกับไอทีและการยอมรับความสูญเสียของผู้นำ				

4.1.2 การสั่งการเพื่อดำเนินการบริหารความเสี่ยง (EDM03.02 Direct risk managment)

สั่งการในเรื่องการสร้างแนวปฏิบัติการบริหารความเสี่ยงเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผล โดยแนวปฏิบัติการบริหารความเสี่ยงเทคโนโลยีสารสนเทศมีความเหมาะสมที่ให้ความเชื่อมั่นในเรื่องความเสี่ยงเทคโนโลยีสารสนเทศไม่เกินกว่าความเสี่ยงที่ประธานคณะกรรมยอมรับ โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.3

ตารางที่ 3.3 วิธีการดำเนินการกำกับดูแลด้านสั่งการบริหารความเสี่ยง

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.02)				
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต	
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
สั่งการด้านการบริหารความเสี่ยง สั่งการให้จัดทำแนวปฏิบัติสำหรับการบริหารความ เสี่ยงเพื่อให้ความเชื่อมั่นได้ในระดับหนึ่งว่าแนวปฏิบัติในการบริหารความเสี่ยงด้านไอทีมีความเหมาะสม โดยให้มั่นใจว่าความเสี่ยงด้านไอทีที่เกิดขึ้นจริงจะต้องไม่เกินระดับความเสี่ยงที่คณะกรรมการ บริหารยอมรับได้	APO12.03	รวบรวมข้อมูลความเสี่ยง รวมทั้งสถานะการดำเนินการบริหารความเสี่ยง	นโยบายการบริหารความเสี่ยง	APO12.01
			วัตถุประสงค์หลักที่จะติดตามสำหรับการบริหารความเสี่ยง	APO12.01
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ (ข้อมูลความเสี่ยงและแผนการลดความเสี่ยง)	อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	APO12.01

ตารางที่ 3.3 (ต่อ)

กิจกรรมที่ต้องดำเนินการ
1.ส่งเสริมวัฒนธรรมในการตระหนักถึงความเสี่ยงด้านไอที และสร้างเสริมให้กองทุนฯ สามารถระบุถึงความเสี่ยงของไอทีในเชิงรุก ตลอดจนโอกาส และผลกระทบทางธุรกิจที่อาจเกิดขึ้น
2.สั่งการให้บูรณาการยุทธศาสตร์และปฏิบัติการด้านความเสี่ยงของไอที เข้าไปในการตัดสินใจด้านความเสี่ยงเชิงยุทธศาสตร์และปฏิบัติการของกองทุนฯ
3.สั่งการให้มีการพัฒนาแผนการติดต่อสื่อสารด้านความเสี่ยง (ที่ครอบคลุมทุกระดับของกองทุนฯ) และแผนดำเนินการสำหรับความเสี่ยง
4.สั่งการให้นำกลไกที่เหมาะสมมาใช้เพื่อตอบสนองความเสี่ยงที่เปลี่ยนแปลงไปได้อย่างรวดเร็ว และสามารถรายงานไปยังผู้บริหารในระดับที่ เหมาะสมได้ทันที ซึ่งสนับสนุนโดยหลักการในการแจ้งเรื่องตามระดับที่เห็นชอบร่วมกัน (รายงานอะไร เมื่อไหร่ ที่ไหน และอย่างไร)
5.สั่งการให้ทุกคนสามารถรายงานเรื่องความเสี่ยง โอกาส ประเด็นปัญหา และข้อกังวลได้ทุกเมื่อ ความเสี่ยงควรได้รับการบริหารจัดการตาม นโยบายและขั้นตอนการปฏิบัติงานที่เผยแพร่ให้ทราบทั่วกันและได้รับการแจ้งเรื่องตามระดับไปยังผู้ที่มีอำนาจในการตัดสินใจที่เกี่ยวข้อง
6.ระบุเป้าหมายและมาตรวัดหลักของการกำกับดูแลและกระบวนการบริหารความเสี่ยงที่จะต้องเฝ้าติดตามตลอดจนอนุมัติวิธีปฏิบัติ วิธีการ เทคนิค และกระบวนการต่างๆ ที่ใช้เพื่อรวบรวมและรายงานสารสนเทศด้านการวัดผล

4.1.3 การติดตามการบริหารความเสี่ยง (EDM03.03 Monitor risk management)

ติดตามเป้าหมายหลักและมาตรวัดกระบวนการบริหารความเสี่ยงและสร้างแนวทางเพื่อกำหนด การแกะรอยและรายงานแนวโน้มความเปลี่ยนแปลงและปัญหาเพื่อแก้ไขปรับปรุงเรื่องดังกล่าว โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.4

ตารางที่ 3.4 วิธีการดำเนินการกำกับดูแลเฝ้าติดตามการบริหารความเสี่ยง

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.03)				
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต	
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
เฝ้าติดตามการบริหารความเสี่ยง เฝ้าติดตามเป้าหมายหลักและมาตรวัดของกระบวนการในการบริหารความเสี่ยง และกำหนดวิธีการที่จะระบุถึงความเบี่ยงเบนหรือปัญหาต่างๆ ตลอดจนติดตามและรายงานผลสำหรับมาตรการ เยียวยา	APO12.02	ผลการวิเคราะห์ความเสี่ยง	กำหนดมาตรการแก้ไขการบริหารความเสี่ยงที่คาดเคลื่อน	APO12.06
	APO12.04	*โอการที่จะยอมรับความเสี่ยงเพิ่มขึ้น *ผลการประเมินความเสี่ยงบุคคลภายนอก *วิเคราะห์ความเสี่ยงและรายงานข้อมูลความเสี่ยงต่อผู้มีส่วนได้เสีย	ประเด็นบริหารความเสี่ยงสำหรับประธานคณะกรรมการ	EDM05.01
กิจกรรมที่ต้องดำเนินการ				
1.เฝ้าติดตามว่ามีการบริหารจัดการแผนภูมิความเสี่ยง (Risk Profile) ให้อยู่ภายใต้เกณฑ์ของระดับความเสี่ยงที่กองทุนฯ ยอมรับได้มากน้อยเพียงใด				
2.เฝ้าติดตามเป้าหมายหลักและมาตรวัดของการกำกับดูแลและกระบวนการบริหารความเสี่ยงเทียบกับเป้า วิเคราะห์สาเหตุของความเบี่ยงเบนไปจากเป้า และเริ่มดำเนินมาตรการเยียวยาเพื่อจัดการกับสาเหตุดังกล่าว				
3.เอื้อให้ผู้มีส่วนได้เสียหลักสามารถสอบทานความคืบหน้าของกองทุนฯ ที่จะไปสู่เป้าหมายที่ระบุไว้				
4.รายงานประเด็นปัญหาต่างๆ ด้านการบริหารความเสี่ยงไปยังคณะกรรมการบริหารหรือคณะผู้บริหารระดับสูง				

4.1.4 เพื่อความเชื่อมั่นในการดำเนินงานตามหลักการบริหารความเสี่ยงโคบิต 5 อ้างอิงตามมาตรฐานการดำเนินงานที่เป็นสากลตามตารางที่ 3.5

4.1.5 โคบิตห้ากำหนดหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลความเสี่ยงตาม ตารางที่ 3.6

ตารางที่ 3.5 มาตรฐานที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยง

	กรอบการการดำเนินงานมาตรฐานที่เกี่ยวข้องกับ EDM03
มาตรฐานที่เกี่ยวข้อง	รายละเอียดอ้างอิง
COSO/ERM	
ISO/IEC 31000	กรอบมาตฐานการบริหารความเสี่ยง
ISO/IEC 38500	
King III	5.5 เทคโนโลยีสารสนเทศควรควบรวมเป็นส่วนเดี่ยวกับการบริหารความเสี่ยงองค์กร
	5.6 คณะกรรมการความเสี่ยงและคณะกรรมการตรวจสอบควรให้ความช่วยเหลือต่อคณะกรรมการบริหารปฏิบัติหน้าด้านเทคโนโลยีสารสนเทศให้สำเร็จลุล่วง

ตารางที่ 3.6 หน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยง (EDM)

EDM03 ตารางหน้าที่ความรับผิดชอบ (RACI Chart)																														
หลักการบริหารที่ต้องดำเนินการ	คณะกรรมการ	ประธานคณะเจ้าหน้าที่บริหาร	นักบริหารการเงินอาวุโส	นักบริหารการปฏิบัติงานอาวุโส	ผู้บริหารธรกิจ	เจ้าของกระบวนการทางธรกิจ	คณะกรรมการบริหารกลยุทธ์	คณะกรรมการบริหารโครงการ/	เจ้าหน้าที่บริหารโครงการ	เจ้าหน้าที่บริหารคุณค่า	นักบริหารความเสี่ยงอาวุโส	นักบริหารความมั่นคง	คณะกรรมการธรรมาภิบาลไอที	คณะกรรมบริหารความเสี่ยง	ฝ่ายทรัพยากรบุคคล	ฝ่ายกฎ ระเบียบ	ฝ่ายตรวจสอบภายใน	นักบริหารเทคโนโลยี	หัวหน้างานสถาปัตยกรรม	หัวหน้างานพัฒนา	หัวหน้างานปฏิบัติงานด้าน	หัวหน้างานบริหารงานทั่วไป	ผู้อำนวยการบริการ	ผู้อำนวยการความมั่นคง	ผู้อำนวยการความต่อเนื่องทาง	เจ้าหน้าที่ความลับส่วนบุคคล
EDM03.01	A	R	C	C	R	C	R			I	R	C		I	C	C	C	C	R	C							C	
EDM03.02	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	C	R	C	I	I	I	I	I	I	I	
EDM03.03	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	C	R	C	I	I	I	I	I	I	C	

4.2 การบริหารความเสี่ยง (APO12 Align Plan and Organize)

4.2.1 เก็บข้อมูลความเสี่ยง (APO12.01 Collect Data)

ระบุและเก็บข้อมูลที่เกี่ยวข้องเพื่อระบุความเสี่ยงทางเทคโนโลยีสารสนเทศที่เกี่ยวข้อง โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.7

ตารางที่ 3.7 วิธีการดำเนินการรวบรวมข้อมูล

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.01)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
รวบรวมข้อมูล ระบุและรวบรวมข้อมูลที่เกี่ยวข้องที่เอื้อให้เกิดประสิทธิผลในการระบุ การวิเคราะห์และการรายงาน ด้านความเสี่ยงที่เกี่ยวข้องกับไอที	EDM03.01	การวัดผลกิจกรรมการบริหารความเสี่ยง	ข้อมูลของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงาน	ภายใน
	EDM03.02	*อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	ข้อมูลเหตุการณ์ความเสี่ยงและปัจจัยที่ก่อให้เกิดประเด็นความเสี่ยงที่เกิดขึ้นและปัจจัยต่างๆ	ภายใน
	APO02.02	ช่องโหว่หรือความสามารถการบริหารความเสี่ยงปัจจุบัน		EDM03.01 APO01.03 APO02.02
	APO02.05	การประเมินความเสี่ยง		
	APO10.04	ระบุความเสี่ยงจากการส่งมอบของผู้ผลิต		
	DSS02.07	สถานะของเหตุการณ์ที่เกิดและรายงานแนวโน้มของเหตุการณ์		

ตารางที่ 3.7 (ต่อ)

กิจกรรมที่ต้องดำเนินการ
1.กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และการวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับไอทีซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านไอที และปัจจัยเสี่ยง
2.บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมในการปฏิบัติงานของกองทุนฯทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านไอที
3.สำรวจและวิเคราะห์ข้อมูลความเสี่ยงด้านไอทีในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนฯที่มีอยู่จากธุรกิจในประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภทสำหรับ การเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้
4.บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นหรืออาจเป็นสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของไอที ต่อการส่งมอบชุดโครงการและโครงการด้านไอที และ/หรือต่อปฏิบัติการและการส่งมอบบริการด้านไอที จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆที่เกี่ยวข้อง
5.จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณต่างๆ เหล่านั้นมีร่วมกัน
6.ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือที่ไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยง และลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ
7.ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะ เพื่อระบุประเด็นปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่ และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง

4.2.2 วิเคราะห์ความเสี่ยง (APO12.02 Analyze Risk)

วิเคราะห์ข้อมูลที่เป็นประโยชน์เพื่อสนับสนุนในการตัดสินใจต่อปัจจัยความเสี่ยงที่เกี่ยวข้องในธุรกิจโดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.8

ตารางที่ 3.8 วิธีการดำเนินการวิเคราะห์ความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.02)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
วิเคราะห์ความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
พัฒนาสารสนเทศที่มีประโยชน์ต่อกาสนับสนุนการ ตัดสินใจด้านความเสี่ยง ซึ่งได้คำนึงถึงความเกี่ยวเนื่องทางธุรกิจของปัจจัยความเสี่ยงต่างๆ	DSS04.02	วิเคราะห์ผลกระทบกองทุนฯ	ขอบเขตของความพยายามการวิเคราะห์ความเสี่ยง	ภายใน
	DSS05.01	การประเมินผลของภัยคุกคามที่เกิดขึ้น	สถานการณ์ความเสี่ยงเทคโนโลยีสารสนเทศ	ภายใน
	ภายนอกโคบิต	คำแนะนำสำหรับภัยคุกคาม	ผลการวิเคราะห์ความเสี่ยง	EDM03.03 APO01.03 APO02.02 BAI01.10
กิจกรรมที่ต้องดำเนินการ				
1.กำหนดความกว้างและความลึกที่เหมาะสมของความพยายามในการวิเคราะห์ความเสี่ยง โดยพิจารณาถึงทุกปัจจัยเสี่ยงและความสำคัญเชิงธุรกิจของสินทรัพย์ และกำหนดขอบเขตของการวิเคราะห์ความเสี่ยงภายหลังจากการวิเคราะห์ต้นทุน-ผลประโยชน์				
2.จัดทำสถานการณ์ต่างๆ ของความเสี่ยงด้านไอทีและปรับปรุงให้เป็นปัจจุบัน รวมถึงการรวมสถานการณ์ความเสี่ยงที่มีประเภทของภัยคุกคามในลักษณะที่ส่งทอดถึงกันและ/หรือที่เกิดขึ้นพร้อมกันไว้ด้วยกัน แล้วกำหนดความคาดหวังสำหรับกิจกรรมของการควบคุมเฉพาะด้าน ความ สามารถในการตรวจพบ และมาตรการตอบสนองอื่นๆ				

ตารางที่ 3.8 (ต่อ)

กิจกรรมที่ต้องดำเนินการ
3.ประมาณความถี่และความรุนแรงของการสูญเสียหรือประโยชน์ที่สัมพันธ์กับสถานการณ์ต่างๆ ของความเสี่ยงด้านไอที คำนึงถึงปัจจัยเสี่ยงที่เกี่ยวข้องทั้งหมด ประเมินการควบคุมเชิงปฏิบัติการที่มีอยู่และประมาณระดับความเสี่ยงที่เหลืออยู่
4.เปรียบเทียบความเสี่ยงที่เหลืออยู่กับความคลาดเคลื่อนของความเสี่ยงที่ยอมรับได้และระบุโอกาสเสี่ยงภัยที่อาจจำเป็นต้องตอบสนอง
5.วิเคราะห์ ต้นทุน-ผลประโยชน์ของทางเลือกในการตอบสนองความเสี่ยงที่อาจเป็นไปได้ เช่น การหลีกเลี่ยง ลด/บรรเทา โอน/แบ่งปัน และยอมรับและฉวย/คว้าโอกาส เป็นต้น นำเสนอการตอบสนองความเสี่ยงที่เหมาะสมที่สุด
6.ระบุข้อกำหนดความต้องการในภาพรวมสำหรับโครงการหรือชุดโครงการที่นำการตอบสนองความเสี่ยงที่เลือกแล้วไปใช้ ระบุความต้องการ และความคาดหวังต่างๆ สำหรับการควบคุมหลักที่เหมาะสมเพื่อการตอบสนองโดยการบรรเทาความเสี่ยง
7.ตรวจสอบความสมเหตุสมผลของผลการวิเคราะห์ความเสี่ยงต่างๆ ก่อนนำมาใช้ประกอบการตัดสินใจ โดยยืนยันว่าการวิเคราะห์นั้นสอดคล้อง กับข้อกำหนดความต้องการของกองทุนฯ และทวนสอบว่าการประมาณการต่างๆ นั้นมีความเที่ยงตรงและได้พิจารณาถึงอคติที่อาจมี

4.2.3 เก็บรักษาข้อมูลความเสี่ยง (APO12.03 Maintain a risk profile) เก็บรักษาคลังข้อมูลความเสี่ยงและคุณลักษณะของความเสี่ยง (รวมทั้งความถี่ที่ขาดหวัง สิ่งที่อาจเกิดขึ้น ของผลกระทบและการบริหารความเสี่ยง) โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.9

ตารางที่ 3.9 วิธีการดูแลรักษาแผนภูมิความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.03)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
ดูแลรักษาแผนภูมิความเสี่ยง ดูแลรักษาบัญชีรายการความเสี่ยงและคุณลักษณะ ของความเสี่ยงต่างๆ ที่มี (รวมถึงความถี่ที่คาดการณ ไว้ผลกระทบที่อาจเกิดขึ้นและการตอบสนอง) และ บัญชีรายชื่อของทรัพยากร ความสามารถ และกิจกรรมการควบคุมในปัจจุบันที่เกี่ยวข้อง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
	EDM03.01	*อนุมัติระดับความเสี่ยงที่ยอมรับได้ *แนะนำแนวทางการยอมรับความเสี่ยง	ทำเอกสารสถานการณ์ความเสี่ยงตามสายงานของ กองทุนฯ และหน้าที่การดำเนินงาน	ภายใน
	APO10.04	ระบุความเสี่ยงการส่งมอบของผู้ผลิต	รวบรวมข้อมูลความเสี่ยง	EDM03.02 APO02.02
	DSS05.01	การประเมินผลของภัยคุกคามที่อาจเกิดขึ้น	รวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	
กิจกรรมที่ต้องดำเนินการ				
1.จัดทำบัญชีรายการของกระบวนการดำเนินงานต่างๆ รวมถึงบุคลากร ระบบงาน โครงสร้างพื้นฐาน สถานที่และสิ่งอำนวยความสะดวก บันทึก ข้อมูลที่จัดทำด้วยคนที่สำคัญ ผู้ขาย และผู้ให้บริการภายนอกที่สนับสนุนกระบวนการ ตลอดจนจัดทำเอกสารการพึงพากระบวนการบริหาร จัดการบริการด้านไอทีและทรัพยากรโครงสร้างพื้นฐานด้านไอทีต่างๆ				
2.กำหนดและเห็นชอบร่วมกันว่าบริการด้านไอทีและโครงสร้างพื้นฐานด้านไอทีใดที่มีความสำคัญในการสนับสนุนการปฏิบัติงานของ กระบวนการดำเนินงานต่างๆ ให้เกิดขึ้นอย่างต่อเนื่อง วิเคราะห์ระดับการพึ่งพาและระบุจุดอ่อน				
3.รวบรวมสถานการณ์ความเสี่ยงต่างๆ ตามประเภท สายงานดำเนินการ และหน้าที่งานด้านต่างๆ				
4.จัดเก็บสารสนเทศด้านแผนภูมิความเสี่ยงทั้งหมดและนำมารวมเป็นแผนภูมิความเสี่ยงรวมอย่างสม่ำเสมอ				
5.กำหนดชุดของดัชนีความเสี่ยงจากข้อมูลทั้งหมดในแผนภูมิความเสี่ยง ซึ่งจะช่วยให้การระบุและเฝ้าติดตามความเสี่ยงในปัจจุบันและแนว โน้มความเสี่ยงทำได้อย่างรวดเร็ว				
6.จัดเก็บสารสนเทศของเหตุการณ์ความเสี่ยงต่างๆ ด้านไอทีที่เกิดขึ้นจริง เพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ				
7.จัดเก็บสารสนเทศเกี่ยวกับสถานะของแผนดำเนินการด้านความเสี่ยงเพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ				

4.2.4 รายงานความเชื่อมโยงความเสี่ยง (APO12.04 Articulate risk)

เตรียมเปิดเผยสถานะข้อมูลปัจจุบันของเทคโนโลยีสานสนเทศที่เกี่ยวข้องและแจ้งข้อมูลต่างๆ ตามระยะที่เหมาะสมต่อความต้องการของผู้มีส่วนได้เสียโดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.10

ตารางที่ 3.10 วิธีการเชื่อมโยงความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.04)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
เชื่อมโยงความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
นำเสนอสารสนเทศเกี่ยวกับสถานะปัจจุบันของโอกาสเสี่ยงภัยและโอกาสอำนวยประโยชน์ที่เกี่ยวข้องกับไอทีอย่างทันเวลาแก่ผู้มีส่วนได้เสียเพื่อให้มีการตอบสนองอย่างเหมาะสม			วิเคราะห์ความเสี่ยงและรายงานความเสี่ยงต่อผู้มีส่วนได้เสีย	EDM03.03 EDM05.02 APO10.04 MEA02.08
			รวบรวมข้อมูลความเสี่ยง	EDM03.03 APO10.04
			รวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	MEA02.01
			โอกาสต่างๆ สำหรับการยอมรับความเสี่ยงที่เพิ่มขึ้น	EDM03.03
กิจกรรมที่ต้องดำเนินการ				
1.รายงานผลของการวิเคราะห์ความเสี่ยงไปยังผู้มีส่วนได้เสียที่ได้รับผลกระทบทั้งหมดตามเงื่อนไขและรูปแบบที่มีประโยชน์ในการสนับสนุน การตัดสินใจของกองทุนฯ รวมถึงระบุความเป็นไปได้ต่างๆ และขอบเขตของความสูญเสียและผลประโยชน์ พร้อมทั้งระดับความเชื่อมั่นเพื่อเอื้อให้ผู้บริหารสามารถสร้างสมดุลระหว่างความเสี่ยงกับผลตอบแทน หากเป็นไปได้				

ตารางที่ 3.10 (ต่อ)

2.นำเสนอแก่ผู้มีหน้าที่ตัดสินใจ ในเรื่องสถานการณ์ที่สามารถทำให้เข้าใจถึงเหตุการณ์ที่เลวร้ายที่สุดและโอกาสที่เป็นไปได้มากที่สุด ในเรื่องการกระทำโดยระมัดระวังถึงโอกาสเสี่ยงภัย และการคำนึงถึงชื่อเสียง กฎหมาย หรือกฎระเบียบข้อบังคับต่างๆ ที่สำคัญ
3.รายงานถึงแผนภูมิความเสี่ยงในปัจจุบันไปยังผู้มีส่วนได้เสียทุกคน ซึ่งรวมถึงเรื่องของประสิทธิผลของกระบวนการบริหารความเสี่ยงประสิทธิภาพของการควบคุม ช่องว่าง/ความต่าง ความไม่สม่ำเสมอ ความซ้ำซ้อน สถานะของการแก้ไขปรับปรุง และผลกระทบของปัจจัย เหล่านี้ที่มีต่อแผนภูมิความเสี่ยง
4.สอบทานผลการประเมินจากองค์กรภายนอกที่เป็นกลาง การตรวจสอบภายใน และการสอบทานการให้ความเชื่อมั่นด้านคุณภาพ และเชื่อม โยงผลเหล่านั้นเข้ากับแผนภูมิความเสี่ยง สอบทานช่องว่างและโอกาสเสี่ยงภัยที่ได้รับการระบุเพื่อพิจารณาถึงความจำเป็นที่ต้องจัดให้มีการ วิเคราะห์ความเสี่ยงเพิ่มเติม
5.สำหรับในด้านความเสี่ยงสัมพัทธ์ (relative risk) และความเท่าเทียมกันในระดับของความเสี่ยงเพื่อให้ได้ผลประโยชน์ตามที่ต้องการ (riskcapacity parity) นั้น ให้ระบุโอกาสที่เกี่ยวข้องกับไอทีเป็นระยะเพื่อช่วยให้สามารถยอมรับความเสี่ยงได้มากขึ้นและช่วยให้มีการเติบโตและได้รับผลตอบแทนที่ดีขึ้น

4.2.5 กำหนดแนวทางการบริหารความเสี่ยง (APO12.05 Define a risk management action portfolio) บริหารลดระดับความเสี่ยงตามแนวทางการบริหารความเสี่ยงที่กำหนดโดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.11

ตารางที่ 3.11 วิธีการกำหนดกลุ่มของการดำเนินการบริหารความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.05)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ
กำหนดกลุ่มของการดำเนินการ บริหารความเสี่ยงบริหารจัดการโอกาสต่างๆ แบบกลุ่ม (portfolio) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้			นำเสนอโครงการสำหรับการลดความเสี่ยง	APO02.02 APO13.02

ตารางที่ 3.11 (ต่อ)

กิจกรรมที่ต้องดำเนินการ
1.จัดทำบัญชีรายชื่อกิจกรรมการควบคุมที่มีอยู่เพื่อบริหารความเสี่ยงและที่เอื้อให้ความเสี่ยงสอดคล้องกับระดับและช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ จำแนกกิจกรรมการควบคุมต่างๆ และจับคู่กิจกรรมเหล่านั้นกับคำแถลงความเสี่ยงด้านไอทีที่เกี่ยวข้องและ การรวมกลุ่มของความเสี่ยงด้านไอที
2.พิจารณาว่าแต่ละหน่วยงานในกองทุนฯ ได้มีการเฝ้าติดตามความเสี่ยงและยอมรับต่อความรับผิดชอบในผลงานสำหรับการดำเนินงานภายใต้ระดับช่วงความเบี่ยงเบนของความเสี่ยงยอมรับได้ทั้งในระดับหน่วยและในระดับกลุ่ม
3.กำหนดชุดที่มีความสมดุลของข้อเสนอโครงการซึ่งได้ออกแบบมาเพื่อลดความเสี่ยง และ/หรือโครงการที่เอื้อต่อโอกาสต่างๆ ด้านยุทธศาสตร์ของกองทุนฯ พิจารณาถึงต้นทุนและผลประโยชน์ ผลกระทบต่อแผนภูมิความเสี่ยงและกฎระเบียบข้อบังคับต่างๆ ในปัจจุบัน

4.2.6 การตอบสนองต่อความเสี่ยง (APO12.06 Respond to risk)

บริหารความเสี่ยงในระยะเวลาที่เหมาะสมตามการวัดผลอย่างมีประสิทธิภาพ โดยจำกัดขอบเขตต่อความสูญเสียจากเหตุการณ์ทางเทคโนโลยีสารสนเทศที่เกี่ยวข้อง โดยมีแนวปฏิบัติและกิจกรรมที่ต้องดำเนินการตามตารางที่ 3.12

ตารางที่ 3.12 วิธีการตอบสนองต่อความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.06)				
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต	
ตอบสนองต่อความเสี่ยงตอบสนองอย่างทันเวลาด้วยมาตรการที่มีประสิทธิผลในการจำกัดความรุนแรงของความสูญ เสียอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียดดำเนินการปรับปรุงเพื่อบรรจุความคลาดเคลื่อนการบริหารความเสี่ยง	รายละเอียดแผนตอบสนองต่อเหตุการณ์ที่เป็นความเสี่ยง การสื่อสาร ผลกระทบ ความเสี่ยง	ไปสู่กระบวนการ DSS02.05 APO01.04 APO08.04 DSS04.02

ตารางที่ 3.12 (ต่อ)

	โอกาสต่างๆ	DSS02.03
	สำหรับการ	DSS03.01
	ยอมรับความ	DSS03.02
	เสี่ยงที่เพิ่มขึ้น	DSS04.02
		MEA02.04
		MEA02.07
		MEA02.08
กิจกรรมที่ต้องดำเนินการ		
1.จัดเตรียม บำรุงรักษา และทดสอบแผนต่างๆ ที่บันทึกขั้นตอนเฉพาะที่จะนำไปใช้เมื่อเหตุการณ์ความเสี่ยงอาจก่อให้เกิดเหตุการณ์ผิดปกติด้านการปฏิบัติงานหรือด้านการพัฒนาที่มีนัยสำคัญซึ่งส่งผลกระทบต่อกองทุนฯ อย่างรุนแรง ให้มั่นใจว่าแผนดังกล่าวนี้ได้รวมเส้นทางในการแจ้ง เรื่องตามระดับทั่วทั้งกองทุนฯ		
2.จัดหมวดหมู่ของเหตุการณ์ผิดปกติ และเปรียบเทียบโอกาสเสี่ยงภัยที่เกิดขึ้นจริงกับขีดจำกัดของช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ สื่อสารผลกระทบต่อกองทุนฯ ไปยังผู้มีอำนาจตัดสินใจต่างๆ โดยให้เป็นส่วนหนึ่งของการรายงาน และปรับแผนภูมิความเสี่ยงให้เป็น ปัจจุบัน		
3.ประยุกต์ใช้แผนการตอบสนองที่เหมาะสมในการลดผลกระทบให้น้อยที่สุดเมื่อเกิดเหตุการณ์ผิดปกติ		
4.ตรวจสอบเหตุการณ์ไม่พึงประสงค์หรือความเสียหายรวมถึงการสูญเสียโอกาสต่างๆ ในอดีตและวิเคราะห์ถึงต้นเหตุ สื่อสารต้นเหตุ ข้อกำหนดความต้องการในการตอบสนองต่อความเสี่ยงเพิ่มเติม และการปรับปรุงกระบวนการ ไปยังผู้มีอำนาจตัดสินใจในกองทุนฯ ที่เหมาะสม และให้มั่นใจว่าต้นเหตุ ข้อกำหนดความต้องการในการตอบสนอง และการปรับปรุงกระบวนการได้รวมไว้ในกระบวนการกำกับดูแลด้านความเสี่ยง		

4.2.7 เพื่อความเชื่อมั่นในการดำเนินงานตามหลักการบริหารความเสี่ยงโคบิต 5 อ้างอิงตามมาตรฐานการดำเนินงานที่เป็นสากลตามตารางที่ 3.13

4.2.8 โคบิตห้ากำหนดหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลความเสี่ยงตามตารางที่ 3.14

ตารางที่ 3.13 มาตรฐานที่เกี่ยวข้องกับการบริหารความเสี่ยง

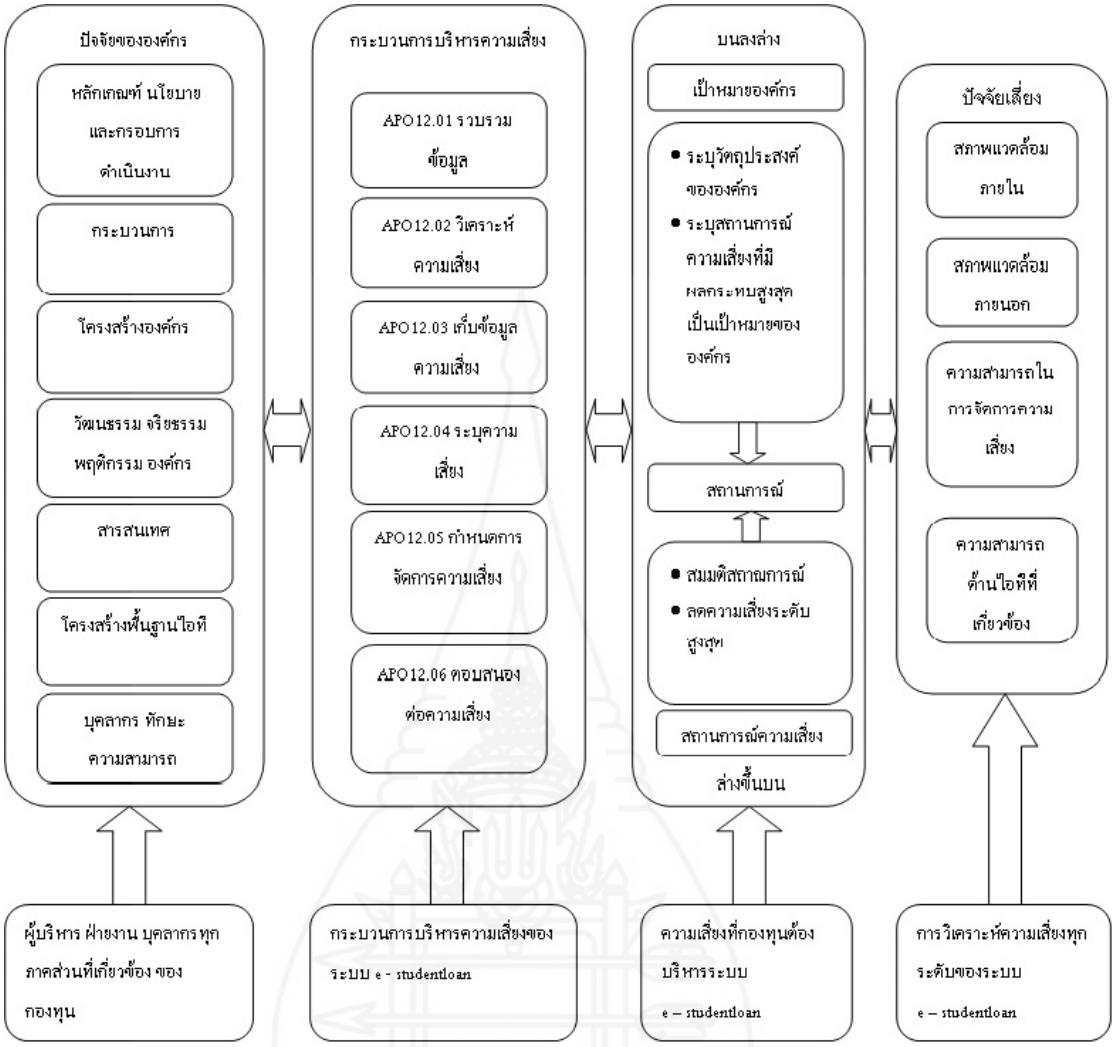
กรอบการการดำเนินงานมาตรฐานที่เกี่ยวข้องกับ APO12	
มาตรฐานที่เกี่ยวข้อง	รายละเอียดอ้างอิง
ISO/IEC 27001:2005	ส่วนที่ 4 เรื่องความต้องการของระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ
ISO/IEC 27002:2011	
ISO/IEC 31000	ข้อ 6 กระบวนการสำหรับการบริหารความเสี่ยง

ตารางที่ 3.14 หน้าที่ความรับผิดชอบในการบริหารความเสี่ยง (APO12)

APO 12 ตารางหน้าที่ความรับผิดชอบ (RACI Chart)																							
หลักการบริหารที่ต้องดำเนินการ	คณะกรรมการ	ประธานคณะเจ้าหน้าที่บริหาร	นักบริหารการเงินอาวุโส	นักบริหารการปฏิบัติงานอาวุโส	ผู้บริหารธุรกิจ	เจ้าของกระบวนการทางธุรกิจ	คณะกรรมการบริหารกลยุทธ์	คณะกรรมการบริหารโครงการ/โปรแกรม	เจ้าหน้าที่บริหารโครงการ	เจ้าหน้าที่บริหารคุณค่า	นักบริหารความมั่นคงสารสนเทศอาวุโส	คณะกรรมการสถาปัตยกรรม	คณะกรรมบริหารความเสี่ยงองค์กร	ฝ่ายทรัพยากรบุคคล	ฝ่ายกฎ ระเบียบ	ฝ่ายตรวจสอบภายใน	นักบริหารเทคโนโลยีสารสนเทศอาวุโส	หัวหน้างานสถาปัตยกรรม	หัวหน้างานพัฒนา	หัวหน้างานปฏิบัติงานด้านเทคโนโลยี	หัวหน้างานบริหารงานทั่วไป	ผู้อำนวยการบริการ	ผู้อำนวยการความมั่นคงปลอดภัย	ผู้อำนวยการความต่อเนื่องทางธุรกิจ	เจ้าหน้าที่ความลับส่วนบุคคล
APO12.01 เก็บข้อมูล	I			R		R		R	R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 วิเคราะห์ความเสี่ยง	I			R		C		R	C	R		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 เก็บรักษาข้อมูลความเสี่ยงทั้งหมด	I			R		C		A	C	R		I		R	R	R	C	C	C	C	C	C	C	C
APO12.06 จัดการความเสี่ยง	I			R		R		R	R	R		I		C	C	A	R	R	R	R	R	R	R	R

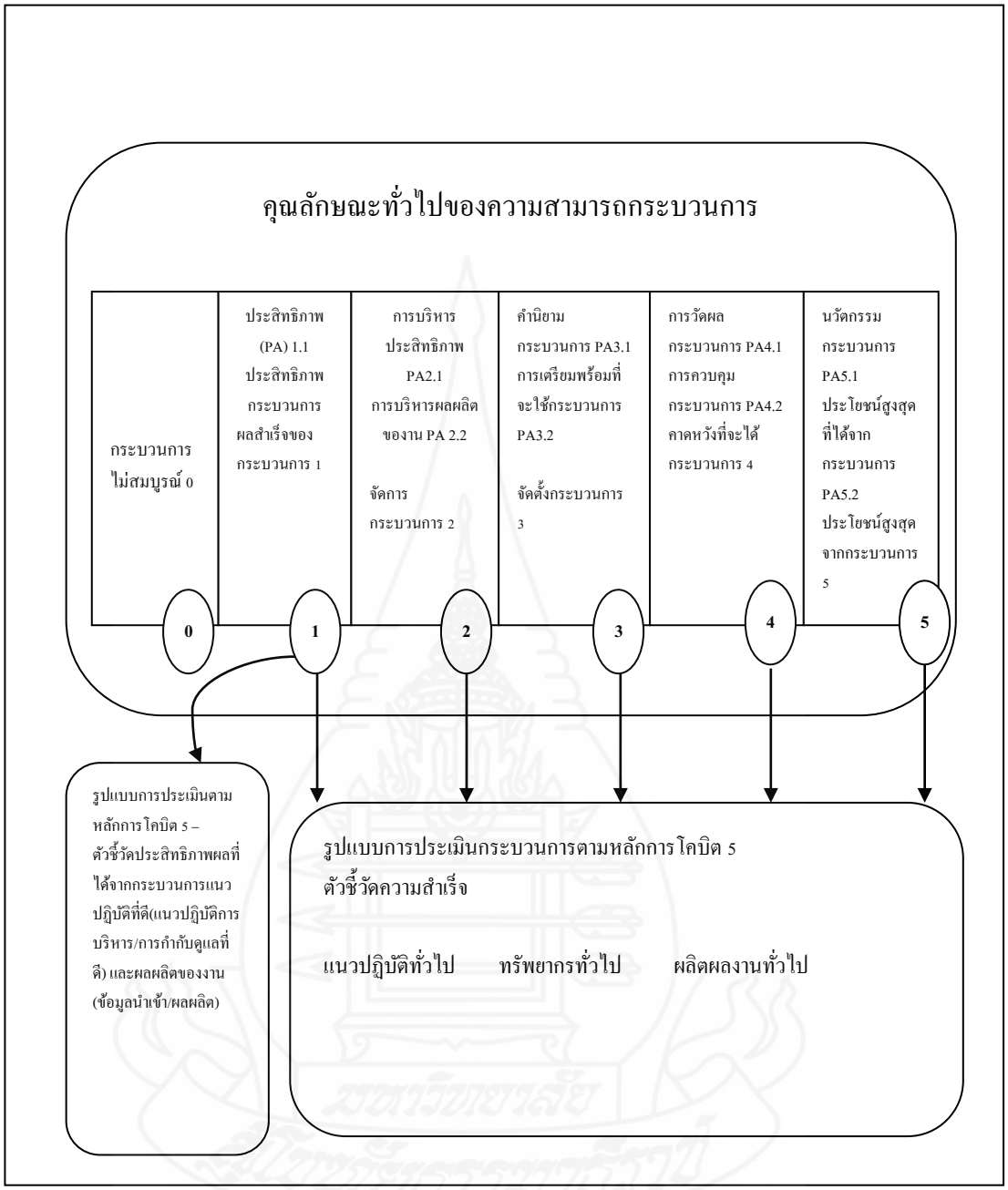
ตารางที่ 3.14 (ต่อ)

APO12.04 แจกแจงความเสี่ยง	I	R	C	R	C	I	C	C	A	C	C	C	C	C	C	C	C	
APO12.05 กำหนดแนวทางการบริหารความเสี่ยง	I	R	C	A	C	I	C	C	R	C	C	C	C	C	C	C	C	
APO12.06 จัดการความเสี่ยง	I	R	R	R	R	I	C	C	A	R	R	R	R	R	R	R	R	



ภาพที่ 3.4 การเชื่อมโยงสถานการณ์ความเสี่ยงกองทุนกับกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5

จากภาพที่ 3.4 แสดงความสัมพันธ์ของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (ซ้ายสุดของภาพ) โดยใช้ปัจจัยเอื้อต่างๆ ตามหลักการโคบิตขององค์กรผลักดันกระบวนการบริหารความเสี่ยง (APO12.01 – 12.06 ตามหลักการโคบิต 5 ที่ 2 จากซ้าย) ดำเนินงานโดยฝ่ายบริหารมีผู้นำที่มีอำนาจในการตัดสินใจสูงสุดคือ นักบริหารอาวุโส (CEO) โดยกระบวนการบริหารความเสี่ยงจะประสบความสำเร็จต้องมีความเชื่อมโยงหรือการสื่อสารในเรื่องการบริหารความเสี่ยงทั่วทั้งองค์กร (ตามภาพที่ 3 จากซ้าย) เพื่อออกแบบสถานการณ์ความเสี่ยงจากสภาพแวดล้อมการดำเนินงานจริงขององค์กรมาปรับใช้ให้เข้ากับทางเลือกสถานการณ์ความเสี่ยงเทคโนโลยีสารสนเทศตามหลักการโคบิต 5 (ภาคผนวก ก) โดยศึกษาและวิเคราะห์จากทุกปัจจัยเสี่ยงทั้งภายนอกและภายใน (ภาพที่ 4 จากซ้าย)



ภาพที่ 3.5 รูปแบบคุณลักษณะความสามารถของกระบวนการ

4.3 พัฒนารูปแบบการตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงโคบิต 5 (COBIT 5 Process Capability Model) ประกอบด้วยระดับการวัดความสำเร็จ 6 ระดับ (ภาพที่ 3.5) ดังนี้

4.3.1 ความสำเร็จของกระบวนการระดับ 0 คือ กระบวนการไม่สมบูรณ์ (0 Incomplete Process) : กระบวนการไม่ได้ดำเนินการหรือไม่บรรลุผลตามวัตถุประสงค์ที่กำหนด ตามภาพที่ 3.3 หมายเลข 0

4.3.2 ความสำเร็จของกระบวนการระดับ 1 คือ กระบวนการได้รับการดำเนินการ (1Performed Process) ต้องครอบคลุม 1 คุณลักษณะ (one attribute) : มีการดำเนินกระบวนการสำเร็จตามวัตถุประสงค์ (PA 1.1) ตามภาพที่ 3.3 หมายเลข 1

4.3.3 ความสำเร็จของกระบวนการระดับ 2 คือ กระบวนการได้รับการบริหาร (2 Managed Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 1 (1Performed Process) (1) ได้รับการดำเนินการบริหารตามรูปแบบ (มีการวางแผน ติดตาม และปรับปรุง) (PA 2.1) และ (2) กระบวนการมีการดำเนินการควบคุม และเก็บรักษาอย่างเหมาะสม (PA 2.2) ตามภาพที่ 3.3 หมายเลข 2

4.3.4 ความสำเร็จของกระบวนการระดับ 3 คือ กระบวนการได้รับการยอมรับว่ามีจริง (3 Established Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 2 (2 Managed Process) (1) มีการดำเนินการโดยกำหนดกระบวนการ (PA 3.1) (2) นำกระบวนการไปใช้งานโดยกระบวนการสามารถบรรลุผลสำเร็จและได้ผลลัพธ์ (PA 3.2) ตามภาพที่ 3.3 หมายเลข 3

4.3.5 ความสำเร็จของกระบวนการระดับ 4 คือ กระบวนการสามารถพยากรณ์ได้ (4 Predictable Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 3 (3 Established Process) (1) กระบวนการมีกำหนดมาตราวัดผลลัพธ์ของกระบวนการ (PA 4.1) (2) กระบวนการมีการควบคุม (PA 4.2) ตามภาพที่ 3.3 หมายเลข 4

4.3.6 ความสำเร็จของกระบวนการระดับ 5 คือ กระบวนการให้ผลลัพธ์และมีคุณประโยชน์สูงสุด (5 Optmising Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute) : กระบวนการในระดับที่ 4 (1) มีการพัฒนา คิดค้นนวัตกรรมขึ้นอย่างต่อเนื่อง (PA 5.1) (2) กระบวนการที่กำหนดให้ประโยชน์และคุณค่าสูงสุดต่อองค์กร (PA 5.2) ตามภาพที่ 3.3 หมายเลข 5

โดยการวัดผลความสำเร็จของการดำเนินการในแต่ละกระบวนการต้องได้รับการวัดผลความสำเร็จในแต่ละระดับอีกครั้ง ตามเงื่อนไขด้านล่าง จึงจะสามารถเลื่อนระดับ 1 เป็นระดับ 2 ได้ดังนี้

- N (Not achieved) คือ มีเพียงเล็กน้อยหรือไม่มีหลักฐานของการบรรลุผลความสำเร็จตามที่ได้กำหนดไว้ (ค่าความสำเร็จร้อยละ 0 – 15)

- P (Partially achieved) คือ มีหลักฐานบ้างอย่างของวิธีการที่จะดำเนินการ และการบรรลุผลสำเร็จบางอย่างของการกำหนดคุณลักษณะในการประเมินกระบวนการ บางส่วนของการบรรลุผลสำเร็จของคุณลักษณะที่ยังขาดการไม่ได้ (ค่าความสำเร็จร้อยละ 15 – 50)
- L (Largely achieved) คือ มีหลักฐานวิธีการดำเนินการอย่างเป็นระบบและมีนัยสำคัญที่จะบรรลุผลสำเร็จของการกำหนดคุณลักษณะในการประเมินกระบวนการ แต่ยังมีข้อบกพร่องเกิดขึ้นอยู่ในการประเมินกระบวนการ (ค่าความสำเร็จร้อยละ 50 – 85)
- F (Fully achieved) คือ มีหลักฐานวิธีการดำเนินอย่างเป็นระบบสมบูรณ์และมีการบรรลุผลสำเร็จสมบูรณ์ของการกำหนดคุณลักษณะในการประเมินกระบวนการ ไม่พบข้อบกพร่องที่มีนัยสำคัญที่เกี่ยวข้องเหลืออยู่ในคุณลักษณะในการประเมินกระบวนการ (ค่าความสำเร็จร้อยละ 85 – 100)

5. ทดสอบแบบจำลองสถานการณ์การความเสี่ยงกับรูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 ตามรูปสถาปัตยกรรมระบบ

5.1 ระบุสถานการณ์ความเสี่ยงจากสภาพแวดล้อมทั้งภายนอกและภายในของระบบe – Studentloan ของกองทุนฯ และสถานการณ์ความเสี่ยงอื่นๆ ที่เกี่ยวข้อง (Risk scenarios) และปัจจัยความเสี่ยงทั้งการดำเนินงานและเทคโนโลยีสารสนเทศที่เกี่ยวข้อง (Risk – related and IT – related risks) เป็นชุดข้อมูลเพื่อเตรียมเข้าสู่กระบวนการบริหารความเสี่ยงโคบิต 5 (APO12)

5.2 เชื่อมข้อมูลด้วยรูปแบบกระบวนการบริหารความเสี่ยงโคบิต 5 (EDM03 และ APO12) โดยในแต่ละกระบวนการต้องผ่านเกณฑ์การประเมินความสำเร็จของกระบวนการตามร้อยละความสำเร็จที่กำหนดไว้

5.3 กระบวนการบริหารความเสี่ยงระบบ e – Studentloan ของกองทุนและสถานการณ์อื่นๆ ที่เกี่ยวข้อง มีการบริหารความเสี่ยงเทคโนโลยีสารสนเทศเชิงบูรณาการ (IT – related risk Governance) อย่างมีประสิทธิภาพและประสิทธิผล (Efficiency and Effectiveness)

5.4 พัฒนารูปแบบระบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 ตามตารางที่ 3.15 - 3.23

ตารางที่ 3.15 กระบวนการประเมินความเสี่ยง (EDM03.01)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.01)								
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต					
ประเมินความเสี่ยง	จาก กระบวนการ	รายละเอียด	รายละเอียด	ไปสู่ กระบวนการ				
ประเมินกำรบริหารความเสี่ยง ตรวจสอบและใช้วิจารณญาน ในการพิจารณาอย่าง ต่อเนื่อง ถึงผลกระทบของความเสี่ยง ด้านการใช้ไอที ในองค์กรทั้ง ปัจจุบันและอนาคต พิจารณา ความ เหมาะสมของระดับ ความเสี่ยงขององค์กรที่ ยอมรับ ได้และมีการระบุและ บริหารจัดการความเสี่ยงที่มี ต่อ คุณค่าขององค์กรซึ่ง เกี่ยวข้องกับการใช้ไอที	APO12.01	ประเด็นความเสี่ยง ที่เกิดขึ้น	แนวทางระดับความ เสี่ยง ที่ยอมรับได้	APO12.03	ค่าถ่วง น้ำหนัก	รายการ ตรวจสอบ กิจกรรมตาม หลักการโค บิตห้า*	สถานะตาม ลำดับ ขั้นตอน (บังคับ ตามลำดับ ต้อง ดำเนินการ เสร็จถึงทำ กิจกรรม ถัดไปได้)	ร้อย ละ ความ สำเร็จ ของ กิจกร รม	สถานะ ความสำเร็จ ของ กระบวนการ
			การอนุมัติระดับความ เสี่ยง ทีองค์กรรับได้	APO12.03				
	มาตรฐารอื่น	หลักการบริหาร ความเสี่ยงเชิงบูรณา การ	การวัดผลกิจกรรม การบริหารความเสี่ยง	APO12.01				
		กิจกรรมที่ต้องดำเนินการ						

ตารางที่ 3.15

1. กำหนดระดับของความเสี่ยงด้านไอทีที่กองทุนฯ สามารถยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์	0.167	0	ERROR	-	Not Achieved
2.ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านไอทีที่ยอมรับได้เทียบกับระดับของความเสี่ยงและโอกาสที่กองทุนฯ ยอมรับได้	0.167	0			
3.พิจารณาว่ายุทธศาสตร์ความเสี่ยงด้านไอทีสอดคล้องกับยุทธศาสตร์ความเสี่ยงระดับกองทุนฯ มากน้อยเพียงใด	0.167	0			
4.ประเมินปัจจัยเสี่ยงด้านไอทีในเชิงรุกสำหรับการตัดสินใจเชิงยุทธศาสตร์ของกองทุนฯ ที่รอดำเนินการ และมั่นใจว่าการตัดสินใจของกองทุนฯได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว	0.167	0			
5.พิจารณาว่ามีการประเมินและวัดผลความเสี่ยงของการใช้ไอทีอย่างเหมาะสม ตามมาตรฐานต่างๆ ที่เกี่ยวข้องทั้งของในประเทศและสากล	0.167	0			
6.ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุนฯ ในการรับความสูญเสียที่เกี่ยวข้องกับไอทีและการยอมรับความสูญเสียของผู้นำ	0.167	0			

ตารางที่ 3.16 กระบวนการสั่งการบริหารความเสี่ยง (EDM03.02)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.02)								
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต					
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ				
สั่งการด้านการบริหารความเสี่ยง สั่งการให้จัดทำแนวปฏิบัติสำหรับการบริหารความ เสี่ยง เพื่อให้ความเชื่อมั่นได้ในระดับหนึ่งว่าแนวปฏิบัติในการบริหารความเสี่ยงด้านไอทีมีความเหมาะสม โดยให้มั่นใจว่าความเสี่ยงด้านไอทีที่เกิดขึ้นจริงจะต้องไม่เกินระดับความเสี่ยงที่คณะกรรมการบริหารยอมรับได้	APO12.03	รวบรวมข้อมูลความเสี่ยงรวมทั้งสถานะการดำเนินการบริหารความเสี่ยง	นโยบายการบริหารความเสี่ยง	APO12.01	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			วัตถุประสงค์หลักที่จะติดตามสำหรับการบริหารความเสี่ยง	APO12.01						
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ(ข้อมูลความเสี่ยงและแผนการลดความเสี่ยง)	อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	APO12.01						

ตารางที่ 3.16 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.ส่งเสริมวัฒนธรรมในการตระหนักถึงความเสี่ยงด้านไอที และสร้างเสริมให้กองทุนฯ สามารถระบุถึงความเสี่ยงของไอทีในเชิงรุก ตลอดจนโอกาส และผลกระทบทางธุรกิจที่อาจเกิดขึ้น	0.167	0	ERROR	-	Not Achieved
2.สั่งการให้บูรณาการยุทธศาสตร์และปฏิบัติการด้านความเสี่ยงของไอที เข้าไปในการตัดสินใจด้านความเสี่ยงเชิงยุทธศาสตร์และปฏิบัติการของกองทุนฯ	0.167	0	ERROR	-	Not Achieved
3.สั่งการให้มีการพัฒนาแผนการติดต่อสื่อสารด้านความเสี่ยง (ที่ครอบคลุมทุกระดับของกองทุนฯ) และแผนดำเนินการสำหรับความเสี่ยง	0.167	0	ERROR	-	Not Achieved
4.สั่งการให้นำกลไกที่เหมาะสมมาใช้เพื่อตอบสนองความเสี่ยงที่เปลี่ยนแปลงไปได้อย่างรวดเร็ว และสามารถรายงานไปยังผู้บริหารในระดับที่ เหมาะสมได้ทันที ซึ่งสนับสนุนโดยหลักการในการแจ้งเรื่องตามระดับที่เห็นชอบร่วมกัน (รายงานอะไร เมื่อไหร่ ที่ไหน และอย่างไร)	0.167	0	ERROR	-	Not Achieved
5.สั่งการให้ทุกคนสามารถรายงานเรื่องความเสี่ยง โอกาส ประเด็นปัญหา และข้อกังวลได้ทุกเมื่อ ความเสี่ยงควรได้รับการบริหารจัดการตาม นโยบายและขั้นตอนการปฏิบัติงานที่เผยแพร่ให้ทราบทั่วกันและได้รับการแจ้งเรื่องตามระดับไปยังผู้ที่มีอำนาจในการตัดสินใจที่เกี่ยวข้อง	0.167	0	ERROR	-	Not Achieved
6.ระบุเป้าหมายและมาตรวัดหลักของการกำกับดูแลและกระบวนการบริหารความเสี่ยงที่จะต้องเฝ้าติดตาม ตลอดจนอนุมัติ วิธีปฏิบัติ วิธีการ เทคนิค และกระบวนการต่างๆ ที่ใช้เพื่อรวบรวมและรายงานสารสนเทศด้านการวัดผล	0.167	0	ERROR	-	Not Achieved
สรุปกระบวนการ 03.02					Not Achieved

ตารางที่ 3.17 กระบวนการติดตามบริหารความเสี่ยง (EDM03.03)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.03)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
เฝ้าติดตามการบริหารความเสี่ยง เฝ้าติดตามเป้าหมายหลักและมาตรวัดของกระบวนการในการบริหารความเสี่ยง และกำหนดวิธี การที่จะระบุถึงความเบี่ยงเบนหรือปัญหาต่างๆ ตลอดจนติดตามและรายงานผลสำหรับมาตรการ เยียวยา	APO12.02	ผลการวิเคราะห์ความเสี่ยง	กำหนดมาตรการแก้ไขการบริหารความเสี่ยงที่คาดเคลื่อน	APO12.06					
	APO12.04	*โอการที่จะยอมรับความเสี่ยงเพิ่มขึ้น *ผลการประเมินความเสี่ยงบุคคลภายนอก *วิเคราะห์ความเสี่ยงและรายงานข้อมูลความเสี่ยงต่อผู้มีส่วนได้เสีย	ประเด็นบริหารความเสี่ยงสำหรับประธานคณะกรรมการ	EDM05.01	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ

ตารางที่ 3.17 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.เฝ้าติดตามว่ามีการบริหารจัดการแผนภูมิความเสี่ยง (Risk Profile) ให้อยู่ภายใต้เกณฑ์ของระดับความเสี่ยงที่กองทุนฯ ยอมรับได้มากน้อยเพียงใด	0.25	0	ERROR	0	Not Achieved
2.เฝ้าติดตามเป้าหมายหลักและมาตรวัดของการกำกับดูแลและกระบวนการบริหารความเสี่ยงเทียบกับเป้า วิเคราะห์สาเหตุของความเบี่ยงเบนไปจากเป้า และเริ่มดำเนินมาตรการเยียวยาเพื่อจัดการกับสาเหตุดังกล่าว	0.25	0	ERROR	0	Not Achieved
3.เอื้อให้ผู้มีส่วนได้เสียหลักสามารถสอบทานความคืบหน้าของกองทุนฯ ที่จะไปสู่เป้าหมายที่ระบุไว้	0.25	0	ERROR	0	Not Achieved
4.รายงานประเด็นปัญหาต่างๆ ด้านการบริหารความเสี่ยงไปยังคณะกรรมการบริหารหรือคณะผู้บริหารระดับสูง	0.25	0	ERROR	0	Not Achieved
สรุปกระบวนการ 03.03					Not Achieved

ตารางที่3.18 กระบวนรวบรวมเก็บข้อมูล (APO12.01)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.01)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
รวบรวมข้อมูล ระบุและรวบรวมข้อมูลที่เกี่ยวข้องที่เอื้อให้เกิดประสิทธิผลในการระบุ การวิเคราะห์และการรายงาน ด้านความเสี่ยงที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	การวัดผลกิจกรรมการบริหารความเสี่ยง	ข้อมูลของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงาน	ภายใน					
	EDM03.02	*อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	ข้อมูลเหตุการณ์ความเสี่ยงและปัจจัยที่ก่อให้เกิด	ภายใน					
	APO02.02	ช่องโหว่หรือความสามารถการบริหารความเสี่ยงปัจจุบัน	ประเด็นความเสี่ยงที่เกิดขึ้นและปัจจัยต่างๆ	EDM03.01 APO01.03 APO02.02					
	APO02.05 APO10.04	การประเมินความเสี่ยง ระบุความเสี่ยงจากการส่งมอบของผู้ผลิต							

ตารางที่ 3.18 (ต่อ)

DSS02.07	สถานะของเหตุการณ์ที่เกิดและรายงานแนวโน้มของเหตุการณ์					
	กิจกรรมที่ต้องดำเนินการ					
1.กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และการวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับไอทีซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านไอที และปัจจัยเสี่ยง		0.143	0	ERRO R	-	Not Achieved
2.บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมในการปฏิบัติงานของกองทุนฯทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านไอที		0.143	0	ERRO R	-	Not Achieved
3.สำรวจและวิเคราะห์ข้อมูลความเสี่ยงด้านไอทีในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนฯที่มีอยู่จากธุรกิจในประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภทสำหรับ การเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้		0.143	0	ERRO R	-	Not Achieved
4.บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นหรืออาจเป็นสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของไอที ต่อการส่งมอบชุดโครงการและโครงการด้านไอที และ/หรือต่อปฏิบัติการและการส่งมอบบริการด้านไอที จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆที่เกี่ยวข้อง		0.143	0	ERRO R	-	Not Achieved

ตารางที่ 3.18 (ต่อ)

5.จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณต่างๆ เหล่านั้นมีร่วมกัน	0.143	0	ERROR	-	Not Achieved
6.ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือที่ไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยง และลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ	0.143	0	ERROR	-	Not Achieved
7.ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะ เพื่อระบุประเด็นปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่ และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.01					Not Achieved

ตารางที่ 3.19 กระบวนการวิเคราะห์ความเสี่ยง (APO12.02)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.02)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
วิเคราะห์ความเสี่ยง พัฒนาสารสนเทศที่มีประโยชน์ต่อกาสนับสนุนการ ตัดสินใจด้านความเสี่ยง ซึ่งได้คำนึงถึงความเกี่ยวเนื่องทางธุรกิจของปัจจัยความเสี่ยงต่างๆ	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
	DSS04.02	วิเคราะห์ผลกระทบกองทุนฯ	ขอบเขตของความพยายามการวิเคราะห์ความเสี่ยง	ภายใน					
	DSS05.01	การประเมินผลของภัยคุกคามที่เกิดขึ้น	สถานการณ์ความเสี่ยงเทคโนโลยีสารสนเทศ	ภายใน	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	ภายนอกโคบิต	คำแนะนำสำหรับภัยคุกคาม	ผลการวิเคราะห์ความเสี่ยง	EDM03.03 APO01.03 APO02.02 BAI01.10					

ตารางที่ 3.19 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.กำหนดความกว้างและความลึกที่เหมาะสมของความพยายามในการวิเคราะห์ความเสี่ยง โดยพิจารณาถึงทุกปัจจัยเสี่ยงและความสำคัญเชิงธุรกิจของสินทรัพย์ และกำหนดขอบเขตของการวิเคราะห์ความเสี่ยงภายหลังจากการวิเคราะห์ต้นทุน-ผลประโยชน์	0.143	0	ERROR	-	Not Achieved
2.จัดทำสถานการณ์ต่างๆ ของความเสี่ยงด้านไอทีและปรับปรุงให้เป็นปัจจุบัน รวมถึงการรวมสถานการณ์ความเสี่ยงที่มีประเภทของภัยคุกคามในลักษณะที่ส่งทอดถึงกันและ/หรือที่เกิดขึ้นพร้อมกันไว้ด้วยกัน แล้วกำหนดความคาดหวังสำหรับกิจกรรมของการควบคุมเฉพาะด้าน ความ สามารถในการตรวจพบ และมาตรการตอบสนองอื่นๆ	0.143	0	ERROR	-	Not Achieved
3.ประมาณความถี่และความรุนแรงของการสูญเสียหรือประโยชน์ที่สัมพันธ์กับสถานการณ์ต่างๆ ของความเสี่ยงด้านไอที คำนึงถึงปัจจัยเสี่ยงที่เกี่ยวข้องทั้งหมด ประเมินการควบคุมเชิงปฏิบัติการที่มีอยู่และประมาณระดับความเสี่ยงที่เหลืออยู่	0.143	0	ERROR	-	Not Achieved
4.เปรียบเทียบความเสี่ยงที่เหลืออยู่กับความคลาดเคลื่อนของความเสี่ยงที่ยอมรับได้และระบุโอกาสเสี่ยงภัยที่อาจจำเป็นต้องตอบสนอง	0.143	0	ERROR	-	Not Achieved
5.วิเคราะห์ ต้นทุน-ผลประโยชน์ของทางเลือกในการตอบสนองความเสี่ยงที่อาจเป็นไปได้ เช่น การหลีกเลี่ยง ลด/บรรเทา โอน/แบ่งปัน และยอมรับและฉวย/คว้าโอกาส เป็นต้น นำเสนอการตอบสนองความเสี่ยงที่เหมาะสมที่สุด	0.143	0	ERROR	-	Not Achieved

ตารางที่ 3.19 (ต่อ)

6.ระบุข้อกำหนดความต้องการในภาพรวมสำหรับโครงการหรือชุดโครงการที่นำการตอบสนองความเสี่ยงที่เลือกแล้วไปใช้ ระบุความต้องการ และความคาดหวังต่างๆ สำหรับการควบคุมหลักที่เหมาะสมเพื่อการตอบสนองโดยการบรรเทาความเสี่ยง	0.143	0	ERROR	-	Not Achieved
7.ตรวจสอบความสมเหตุสมผลของผลการวิเคราะห์ความเสี่ยงต่างๆ ก่อนนำมาใช้ประกอบการตัดสินใจ โดยยืนยันว่าการวิเคราะห์นั้นสอดคล้อง กับข้อกำหนดความต้องการของกองทุนฯ และทวนสอบว่าการประมาณการต่างๆ นั้นมีความเที่ยงตรงและได้พิจารณาถึงอคติที่อาจมี	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.02					Not Achieved

ตารางที่ 3.20 กระบวนดูแลรักษาแผนภูมิความเสี่ยง (APO12.03)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.03)								
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต					
ดูแลรักษำแผนภูมิความเสี่ยง ดูแลรักษาบัญชีรายการความเสี่ยงและคุณลักษณะ ของความเสี่ยงต่างๆ ที่มี (รวมถึงความถี่ที่คาดการณ ไว้ผลกระทบที่อาจเกิดขึ้นและการตอบสนอง) และ บัญชีรายชื่อของทรัพยากร ความสามารถ และกิจกรรมการควบคุมในปัจจุบันที่เกี่ยวข้อง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	*อนุมัติระดับความเสี่ยงที่ยอมรับได้ *แนะนำแนวทางการยอมรับความเสี่ยง	ทำเอกสารสถานการณ์ความเสี่ยงตามสายงานของ กองทุนฯ และหน้าที่การดำเนินงาน	ภายใน					
	APO10.04	ระบุความเสี่ยงการส่งมอบของผู้ผลิต	รวบรวมข้อมูลความเสี่ยง รวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	EDM03.02 APO02.02					
	DSS05.01	การประเมินผลของภัยคุกคามที่อาจเกิดขึ้น							

ตารางที่ 3.20 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.จัดทำบัญชีรายการของกระบวนการดำเนินงานต่างๆ รวมถึงบุคลากร ระบบงาน โครงสร้างพื้นฐาน สถานที่และสิ่งอำนวยความสะดวก บันทึก ข้อมูลที่จัดทำด้วยคนที่สำคัญ ผู้ขาย และผู้ให้บริการภายนอกที่สนับสนุนกระบวนการ ตลอดจนจัดทำเอกสารการพึงพากระบวนการบริหาร จัดการบริการด้านไอทีและทรัพยากรโครงสร้างพื้นฐานด้านไอทีต่างๆ	0.143	0	ERROR	-	Not Achieved
2.กำหนดและเห็นชอบร่วมกันว่าบริการด้านไอทีและโครงสร้างพื้นฐานด้านไอทีใดที่มีความสำคัญในการสนับสนุนการปฏิบัติงานของ กระบวนการดำเนินงานต่างๆ ให้เกิดขึ้นอย่างต่อเนื่อง วิเคราะห์ระดับการพึ่งพาและระบุจุดอ่อน	0.143	0	ERROR	-	Not Achieved
3.รวบรวมสถานการณ์ความเสี่ยงต่างๆ ตามประเภท สายงานดำเนินการ และหน้าที่งานด้านต่างๆ	0.143	0	ERROR	-	Not Achieved
4.จัดเก็บสารสนเทศด้านแผนภูมิความเสี่ยงทั้งหมดและนำมารวมเป็นแผนภูมิความเสี่ยงรวมอย่างสม่ำเสมอ	0.143	0	ERROR	-	Not Achieved
5.กำหนดชุดของดัชนีความเสี่ยงจากข้อมูลทั้งหมดในแผนภูมิความเสี่ยง ซึ่งจะช่วยให้การระบุและเฝ้าติดตามความเสี่ยงในปัจจุบันและแนว โน้มความเสี่ยงทำได้อย่างรวดเร็ว	0.143	0	ERROR	-	Not Achieved
6.จัดเก็บสารสนเทศของเหตุการณ์ความเสี่ยงต่างๆ ด้านไอทีที่เกิดขึ้นจริง เพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	0	ERROR	-	Not Achieved
7.จัดเก็บสารสนเทศเกี่ยวกับสถานะของแผนดำเนินการด้านความเสี่ยงเพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.03					Not Achieved

ตารางที่ 3.21 กระบวนเชื่อมโยงความเสี่ยง (APO12.04)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.04)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
เชื่อมโยงความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
นำเสนอสารสนเทศเกี่ยวกับสถานะปัจจุบันของโอกาสเสี่ยงภัยและโอกาสอำนวยประโยชน์ที่เกี่ยวข้องกับไอทีอย่างทันเวลาแก่ผู้มีส่วนได้เสียเพื่อให้มีการตอบสนองอย่างเหมาะสม			วิเคราะห์ความเสี่ยงและรายงานความเสี่ยงต่อผู้มีส่วนได้เสีย รวบรวมข้อมูลความเสี่ยง รวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง โอกาสต่างๆ สำหรับการยอมรับความเสี่ยงที่เพิ่มขึ้น	EDM03.03 EDM05.02 APO10.04 MEA02.08 EDM03.03 APO10.04 MEA02.01 EDM03.03	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ

ตารางที่ 3.21 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.รายงานผลของการวิเคราะห์ความเสี่ยงไปยังผู้มีส่วนได้เสียที่ได้รับผลกระทบทั้งหมดตามเงื่อนไขและรูปแบบที่มีประโยชน์ในการสนับสนุน การตัดสินใจของกองทุนฯ รวมถึงระบุความเป็นไปได้ต่างๆ และขอบเขตของความสูญเสียและผลประโยชน์ พร้อมทั้งระดับความเชื่อมั่นเพื่อเอื้อให้ผู้บริหารสามารถสร้างสมดุลระหว่างความเสี่ยงกับผลตอบแทน หากเป็นไปได้	0.20	0	ERROR	0	Not Achieved
2.นำเสนอแก่ผู้มีหน้าที่ตัดสินใจ ในเรื่องสถานการณ์ที่สามารถทำให้เข้าใจถึงเหตุการณ์ที่เลวร้ายที่สุดและโอกาสที่เป็นไปได้มากที่สุด ในเรื่องการกระทำโดยระมัดระวังถึงโอกาสเสี่ยงภัย และการคำนึงถึงชื่อเสียง กฎหมาย หรือกฎระเบียบข้อบังคับต่างๆ ที่สำคัญ	0.20	0	ERROR	0	Not Achieved
3.รายงานถึงแผนภูมิความเสี่ยงในปัจจุบันไปยังผู้มีส่วนได้เสียทุกคน ซึ่งรวมถึงเรื่องของประสิทธิผลของกระบวนการบริหารความเสี่ยงประสิทธิภาพของการควบคุม ช่องว่าง/ความต่าง ความไม่สม่ำเสมอ ความซ้ำซ้อน สถานะของการแก้ไขปรับปรุง และผลกระทบของปัจจัย เหล่านี้ที่มีต่อแผนภูมิความเสี่ยง	0.20	0	ERROR	0	Not Achieved
4.สอบทานผลการประเมินจากองค์กรภายนอกที่เป็นกลาง การตรวจสอบภายใน และการสอบทานการให้ความเชื่อมั่นด้านคุณภาพ และเชื่อม โยงผลเหล่านั้นเข้ากับแผนภูมิความเสี่ยง สอบทานช่องว่างและโอกาสเสี่ยงภัยที่ได้รับการระบุเพื่อพิจารณาถึงความจำเป็นที่ต้องจัดให้มีการ วิเคราะห์ความเสี่ยงเพิ่มเติม	0.20	0	ERROR	0	Not Achieved
5.สำหรับในด้านความเสี่ยงสัมพัทธ์ (relative risk) และความเท่าเทียมกันในระดับของความเสี่ยงเพื่อให้ได้ผลประโยชน์ตามที่ต้องการ (riskcapacity parity) นั้น ให้ระบุโอกาสที่เกี่ยวข้องกับไอทีเป็นระยะเพื่อช่วยให้สามารถยอมรับความเสี่ยงได้มากขึ้นและช่วยให้มีการเติบโตและได้รับผลตอบแทนที่ดีขึ้น	0.20	0	ERROR	0	Not Achieved
สรุปกระบวนการ 12.04					Not Achieved

ตารางที่ 3.22 กระบวนการกำหนดกลุ่มของการดำเนินการบริหารความเสี่ยง (APO12.05)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.05)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
กำหนดกลุ่มของการดำเนินการ บริหารความเสี่ยงบริหารจัดการโอกาสต่างๆ แบบกลุ่ม (portfolio) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			นำเสนอโครงการสำหรับการลดความเสี่ยง	APO02.02 APO13.02					
	กิจกรรมที่ต้องดำเนินการ								
1.จัดทำบัญชีรายชื่อกิจกรรมการควบคุมที่มีอยู่เพื่อบริหารความเสี่ยงและที่เอื้อให้ความเสี่ยงสอดคล้องกับระดับและช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ จำแนกกิจกรรมการควบคุมต่างๆ และจับคู่กิจกรรมเหล่านั้นกับคำแถลงความเสี่ยงด้านไอทีที่เกี่ยวข้องและ การรวมกลุ่มของความเสี่ยงด้านไอที					0.333	0	ERROR	-	Not Achieved
2.พิจารณาว่าแต่ละหน่วยงานในกองทุนฯ ได้มีการเฝ้าติดตามความเสี่ยงและยอมรับต่อความรับผิดชอบในผลงานสำหรับการดำเนินงานภายใต้ระดับช่วงความเบี่ยงเบนของความเสี่ยงยอมรับได้ทั้งในระดับหน่วยและในระดับกลุ่ม					0.333	0	ERROR	-	Not Achieved

ตารางที่ 3.22 (ต่อ)

3.กำหนดชุดที่มีความสมดุลของข้อเสนอโครงการซึ่งได้ออกแบบมาเพื่อลดความเสี่ยง และ/หรือ โครงการที่เอื้อต่อโอกาสต่างๆ ด้านยุทธศาสตร์ของกองทุนฯ พิจารณาถึงต้นทุนและผลประโยชน์ ผลกระทบต่อแผนภูมิความเสี่ยงและกฎระเบียบข้อบังคับต่างๆ ในปัจจุบัน	0.333	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.05					Not Achieved

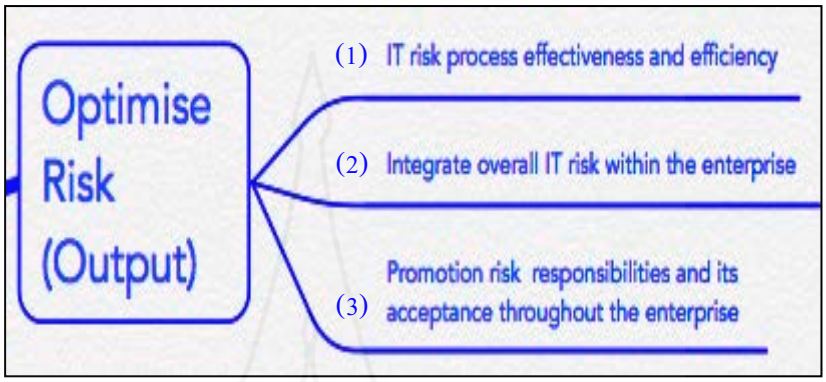
ตารางที่ 3.23 กระบวนการตอบสนองต่อความเสี่ยง (APO12.06)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.06)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
ตอบสนองต่อความเสี่ยง ตอบสนองอย่างทันเวลาด้วยมาตรการที่มีประสิทธิผลในการจำกัดความรุนแรงของความสูญ เสียอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
		ดำเนินการปรับปรุงเพื่อบรรจุความคลาดเคลื่อนการบริหารความเสี่ยง	แผนตอบสนองต่อเหตุการณ์ที่เป็นความเสี่ยง	DSS02.05					
			การสื่อสารผลกระทบความเสี่ยง	APO01.04 APO08.04 DSS04.02	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			โอกาสต่างๆ สำหรับการยอมรับความเสี่ยงที่เพิ่มขึ้น	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08					

ตารางที่ 3.23 (ต่อ)

กิจกรรมที่ต้องดำเนินการ				
1.จัดเตรียม บำรุงรักษา และทดสอบแผนต่างๆ ที่บันทึกขั้นตอนเฉพาะที่จะนำไปใช้เมื่อเหตุการณ์ความเสี่ยงอาจก่อให้เกิดเหตุการณ์ผิดปกติด้านการปฏิบัติงานหรือด้านการพัฒนาที่มีนัยสำคัญซึ่งส่งผลกระทบต่อกองทุนฯ อย่างรุนแรง ให้มั่นใจว่าแผนดังกล่าวนี้ได้รวมเส้นทางในการแจ้ง เรื่องตามระดับทั่วทั้งกองทุนฯ	0.25	0 ERROR	0 Not Achieved	
2.จัดหมวดหมู่ของเหตุการณ์ผิดปกติ และเปรียบเทียบโอกาสเสี่ยงภัยที่เกิดขึ้นจริงกับขีดจำกัดของช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ สื่อสารผลกระทบต่อกองทุนฯ ไปยังผู้มีอำนาจตัดสินใจต่างๆ โดยให้เป็นส่วนหนึ่งของการรายงาน และปรับแผนภูมิความเสี่ยงให้เป็น ปัจจุบัน	0.25	0 ERROR	0 Not Achieved	
3.ประยุกต์ใช้แผนการตอบสนองที่เหมาะสมในการลดผลกระทบให้น้อยที่สุดเมื่อเกิดเหตุการณ์ผิดปกติ	0.25	0 ERROR	0 Not Achieved	
4.ตรวจสอบเหตุการณ์ไม่พึงประสงค์หรือความเสียหายรวมถึงการสูญเสียโอกาสต่างๆ ในอดีตและวิเคราะห์ถึงต้นเหตุ สื่อสารต้นเหตุ ข้อกำหนดความต้องการในการตอบสนองต่อความเสี่ยงเพิ่มเติม และการปรับปรุงกระบวนการ ไปยังผู้มีอำนาจตัดสินใจในกองทุนฯ ที่เหมาะสม และให้มั่นใจว่าต้นเหตุ ข้อกำหนดความต้องการในการตอบสนอง และการปรับปรุงกระบวนการได้รวมไว้ในกระบวนการกำกับดูแลด้านความเสี่ยง	0.25	0 ERROR	0 Not Achieved	
สรุปกระบวนการ 12.06				Not Achieve

6. ผลผลิตกระบวนการบริหารความเสี่ยงกองทุนตามหลักการบริหารความเสี่ยงโคบิต 5 หลังจากทำการทดสอบกับรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5



ภาพที่ 3.6 ผลผลิตจากรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5

จากภาพที่ 3.6 แสดงผลผลิตของกระบวนการกำกับดูแลและบริหารความเสี่ยงของกองทุนตามหลักการบริหารความเสี่ยงโคบิต 5 ในเรื่อง (1) กระบวนการความเสี่ยงด้านเทคโนโลยีสารสนเทศกองทุนมีประสิทธิภาพและประสิทธิผลทั่วทั้งกองทุน (2) กองทุนสามารถรวบรวมความเสี่ยงด้านเทคโนโลยีสารสนเทศครอบคลุมทั้งกองทุน และ (3) สนับสนุนความรับผิดชอบความเสี่ยงและยอมรับความเสี่ยงตลอดทั้งกองทุน

7. ประเมินผลสถานการณ์ความเสี่ยงกองทุนที่ดำเนินตามขั้นตอนหลักการโคบิต 5

ติดตาม วัดผล และประเมินประสิทธิภาพความสอดคล้อง และติดตาม วัดผล และประเมินการควบคุมภายใน ของการดำเนินงานจากการนำสถานการณ์ความเสี่ยงที่สร้างขึ้นไปใช้ของกองทุนฯ

บทที่ 4
ผลการวิจัย

การนำเสนอผลการศึกษาเรื่อง การบริหารความเสี่ยงและการปรับปรุงคุณภาพระบบกู้ยืมเงินเพื่อการศึกษาตามหลักการโคบิต 5 ครั้งนี้ผู้วิจัยจะนำเสนอผลการวิจัยเป็น 3 ตอน (1) แบบจำลองสถานการณ์ความเสี่ยงของกองทุนเชื่อมโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5 (2) พัฒนาระบบสารสนเทศของกองทุนตามกระบวนการบริหารความเสี่ยงโคบิต 5 และ (3) ทดสอบรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อตอบวัตถุประสงค์ของการวิจัยแต่ละข้อดังนี้

ตอนที่ 1 แบบจำลองสถานการณ์ความเสี่ยงของกองทุนเชื่องโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5 แบ่งเป็น 2 ส่วน (1) ศึกษาข้อมูลความเสี่ยงของกองทุนฯ และ (2) ออกแบบสถานการณ์ความเสี่ยงของกองทุนจากปัจจัยเสี่ยงที่กำหนด

1. ศึกษาข้อมูลความเสี่ยงของกองทุนฯ นำข้อมูลความเสี่ยงจากรายงานผลการดำเนินการบริหารความเสี่ยงกองทุน สิ้นสุด 30 มิถุนายน 2559 จากฝ่ายบริหารความเสี่ยง สำนักงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา มาศึกษาการดำเนินการบริหารความเสี่ยงของกองทุนเพื่อปรับปรุงคุณภาพระบบกู้ยืมเงินเพื่อการศึกษา โดยผู้วิจัยเลือกประเด็นความเสี่ยงที่มีผลกระทบต่อการดำเนินงานตามนโยบายจากรัฐบาลของกองทุนฯ ได้แก่ “กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ...ใหม่ทัน” มาศึกษาและทำการเลือกสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 (ภาคผนวก ก) เพื่อออกแบบสถานการณ์ความเสี่ยงของกองทุน(e – Studentloan)

จากการวิเคราะห์ชนิดของสถานการณ์ความเสี่ยง (Risk scenario)ในภาพรวมตามหลักการโคบิต 5 (ภาพที่ 4.1) โดยปัจจัยความเสี่ยงที่อาจเกิดขึ้นอาจจะเกิดจากสภาวะแวดล้อมต่างๆ ของกองทุน ดังต่อไปนี้ (1)ภัยคุกคามต่าง ๆ (ได้แก่ ภัยอันตราย ข้อผิดพลาด ความล้มเหลว ภัยธรรมชาติ เป็นต้น) (2) เหตุการณ์ (ได้แก่ ข้อมูลถูกเปิดเผย การแทรกแซง การดัดแปลง การขโมย เป็นต้น) (3) ทรัพย์สิน/ทรัพยากร (ได้แก่ บุคลากรและทักษะ โครงสร้างองค์กร กระบวนการ สิ่งอำนวยความสะดวก เป็นต้น) (4) ผู้ดำเนินการ (ได้แก่ ภายใน ประด้วย เจ้าหน้าหรือคู่สัญญา ภายนอก ประกอบด้วย กฎหมายและรัฐบาล เป็นต้น) (5) เวลา (ได้แก่ ช่วงเวลา เวลาที่เกิดขึ้น การตรวจจับ เวลาใดเวลาหนึ่ง

เป็นต้น) โดยสถานการณ์ต่างๆ เป็นการตั้งตามสมมติฐานจากสภาพแวดล้อมจริงของการดำเนินงานกองทุน (e - Studentloan) โดยปัจจัยเสี่ยงต่างๆ อาจมีการเปลี่ยนแปลงที่ไม่อาจคาดการได้ทุกเวลาขึ้นอยู่กับสถานการณ์นั้นๆ ซึ่งจากประเด็นความเสี่ยงที่ผู้วิจัยเลือกมาศึกษา ปัจจัยเสี่ยงที่มีผลกระทบต่อ “กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ...ใหม่ทัน” คือ ทรัพย์สิน/ทรัพยากร (กระบวนการ) ผู้ดำเนินการ (ภายใน) นโยบายจากรัฐบาล (ภายนอก) และ เวลา (ช่วงเวลา) ผลลัพธ์ของแบบจำลองสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 คือ ไม่สามารถพัฒนาระบบได้ทันกาล (Ref.0201 และ 0203)

ภาพที่ 4.1 สถานการณ์ความเสี่ยงตามปัจจัยต่างๆ ที่อาจเกิดขึ้นตามสภาพแวดล้อมทั้งภายในและภายนอก

2. ออกแบบสถานการณ์ความเสี่ยงของกองทุนจากปัจจัยเสี่ยงที่กำหนดเพื่อเลือกและกำหนดสถานการณ์ความเสี่ยงจากประเด็นความเสี่ยงและออกแบบสถานการณ์ความเสี่ยงสารสนเทศของกองทุน (e - Studentloan) ตามแนวทางการบริหารความเสี่ยงโคบิต 5 แบ่งออกเป็น 2 ด้านคือ (1) ตัวอย่างสถานการความเสี่ยงด้านลบ และ (2) ตัวอย่างสถานการณ์ด้านบวก โดยประเด็นความเสี่ยงที่ผู้วิจัยเลือกมาศึกษาตรงกับสถานการณ์ความเสี่ยงเลขที่อ้างอิงตามหลักการบริหารความเสี่ยงโคบิต 5 ที่ 0201 และ 0203 โดยผลของการจำลองสถานการณ์ความเสี่ยงของกองทุน (e - Studentloan) เกิดจากการประมาณการตามสภาวะแวดล้อมโดยรวมที่มีโอกาสจะเกิดขึ้นกับกองทุนได้ จากการระบุปัจจัยเสี่ยงข้างต้น โดยกองทุนต้องนำสิ่งปัจจัยเสี่ยงต่างๆ ที่เป็นสาเหตุนำมา ระบุรายละเอียด กำหนดขอบเขต ของความเสี่ยงของ

กองทุน (e – Studentloan) เพื่อสร้างแบบจำลองสถานการณ์ความเสี่ยงที่เหมาะสมกับสภาพแวดล้อมกับกองทุนโดยเลือกสถานการณ์ความเสี่ยงและปรับแต่งให้เหมาะสมกับสภาวะแวดล้อมของกองทุนตามตารางที่ 4.1 และนำสถานการณ์ความเสี่ยงที่ออกแบบมาบันทึกเป็นข้อมูลความเสี่ยงตามรูปแบบของโคบิต 5 ดังตารางที่ 4.2

ตารางที่ 4.1 ผลการออกแบบสถานการณ์ความเสี่ยงของกองทุนตามโคบิต 5 เรื่องการบริหารความเสี่ยง (ความเสี่ยงเทคโนโลยีสารสนเทศเป็นความเสี่ยงหลักในการดำเนินงานของกองทุน (ในประเด็นความเสี่ยง "กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ...ใหม่ทัน")

เลขที่อ้างอิง	สถานการณ์ความเสี่ยง	ประเภทความเสี่ยง				ตัวอย่างสถานการณ์	
		สารสนเทศให้ประโยชน์/เพิ่มมูลค่าแก่กองทุน	โปรแกรม/โครงการด้านสารสนเทศของกองทุนดำเนินการสร้าง	การดำเนินการ/การให้บริการด้านสารสนเทศของกองทุนดำเนินการได้		สถานการณ์เชิงลบ	สถานการณ์เชิงบวก
0201	การบริหารวงจรโปรแกรม/โครงการ (การเริ่มต้นโปรแกรม/โครงการ เศรษฐกิจ การส่งมอบ	P	P	S		ความล้มเหลว (ต้นทุน ความล้าช้า ขอบเขตไม่แน่นอนและการเปลี่ยนแปลงการลำดับความสำคัญความขององค์กร/ธุรกิจ) โครงการยกเลิก	ยกเลิกโครงการทันเวลา
0203	คุณภาพและการยกเลิก)	S	P			มีโอกาสที่จะส่งมอบโครงการทางเทคโนโลยีสารสนเทศล้าช้า	โครงการส่งมอบทันเวลา

หมายเหตุ P หมายถึง เป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดผลกระทบต่อกองทุนในระดับสูงสุด
S หมายถึง เป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดผลกระทบต่อกองทุนในระดับต่ำลงมา
ช่องว่าง หมายถึง ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ส่งผลกระทบต่อกองทุน

ตารางที่ 4.2 ผลจากการเลือกสถานการณ์ความเสี่ยงตามตาราที่ 4.1 มากรอกข้อมูลลงในแบบการลงทะเบียนความเสี่ยงโดยผู้วิจัยนำสถานการณ์ความเสี่ยงที่เลือกจากประเด็นความเสี่ยงจริงของระบบให้กู้ยืมเงินของกองทุนมากรอกลงในแบบลงทะเบียนความเสี่ยง (ประเด็นความเสี่ยง "กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ...ใหม่ทัน")

ส่วนที่ 1 สรุปข้อมูลความเสี่ยง				
คำอธิบายความเสี่ยง	การบริหารวงจรโปรแกรม/โครงการ (การเริ่มต้นโปรแกรม/โครงการ เศรษฐกิจการส่งมอบ คุณภาพและการยกเลิก) อ้างอิงสถานการณ์ความเสี่ยงที่ 0201			
เจ้าของความเสี่ยง	กองทุนเงินให้กู้ยืมเพื่อการศึกษา			
วันสุดท้ายที่ประเมินความเสี่ยง	30 เมษายน พ.ศ. 2559			
วันที่ปรับปรุงการประเมินความเสี่ยง	30 มิถุนายน พ.ศ. 2559			
ประเภทความเสี่ยง	☒P สารสนเทศให้ประโยชน์/เพิ่มมูลค่าแก่กองทุน	☒P โปรแกรม/โครงการด้านสารสนเทศของกองทุนดำเนินการเสร็จ	☑การดำเนินการ/การให้บริการด้านสารสนเทศของกองทุนดำเนินการได้	
จัดระดับความเสี่ยง (นำข้อมูลมาจากการวิเคราะห์ความเสี่ยง)	☐ ต่ำ	☐ปานกลาง	☐ สูง	☐สูงมาก
การตอบสนองต่อความเสี่ยง	☐ยอมรับความเสี่ยง	☑ โอนความเสี่ยง	☐ลดความเสี่ยง	☐หลีกเลี่ยงความเสี่ยง

ตารางที่ 4.2 (ต่อ)

ส่วนที่ 2 คำอธิบายความเสี่ยง						
ชื่อ	กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ... ใหม่ทัน					
สถานการณ์ที่เลือก	(Ref.0201 และ 0203) การบริหารวงจรโปรแกรม/โครงการ (การเริ่มต้นโปรแกรม/โครงการ เศรษฐกิจ การส่งมอบ คุณภาพและการยกเลิก)					
คำอธิบายรายละเอียดของสถานการณ์ – องค์ประกอบสถานการณ์	ผู้ดำเนินการ	ฝ่ายบริหาร				
	ชนิดภัยคุกคาม	ความล้มเหลว				
	เหตุการณ์	ข้อบังคับและกฎระเบียบ				
	สินทรัพย์/ทรัพยากร	กระบวนการ				
	ระยะเวลา	ไม่สามารถดำเนินการได้ทันเวลา				
ข้อมูลสถานการณ์อื่น	กำหนดการบังคับใช้พระราชบัญญัติใหม่ไม่แน่นอน					
ส่วนที่ 3 ผลการวิเคราะห์ความเสี่ยง						
ความถี่ของสถานการณ์ (จำนวนครั้งต่อปี)	0	1	2	3	4	5
	N<=0.01	0.01<N<=0.1	0.1<N<=1	1<N<=10	10<N<=100	100<N
	☑	☐	☐	☐	☐	☐
ผลกระทบของสถานการณ์ต่อองค์กร/ธุรกิจ	0	1	2	3	4	5
	☐	☐	☐	☐	☐	☑
1.ผลผลิต	รายได้ (ขาดทุน) มากกว่า 1 ปี					
ระดับของผลกระทบ	I<=0.1%	0.1%<I<=1%	1%<I<=3%	3%<I<=5%	5%<I<=10%	10%<I
	☐	☐	☐	☐	☐	☑

ตารางที่ 4.2 (ต่อ)

รายละเอียดคำอธิบายของผลกระทบ	ไม่สามารถให้บริการการดำเนินการให้กู้ยืมตามพระราชบัญญัติใหม่ได้					
2.ต้นทุนการตอบสนอง	ค่าใช้จ่ายที่เกี่ยวข้องกับการบริหารเหตุการณ์ที่จะทำให้สูญเสีย					
ระดับของผลกระทบ (บาท)	I<10K	10K<I<=100K	100K<I<=1M	1M<I<=10M	10M<I<=100M	100M<I
	☐	☐	☐	☐	☐	☑
รายละเอียดคำอธิบายของผลกระทบ	ไม่สามารถดำเนินการกระบวนการกู้ยืมเงินภายใต้พระราชบัญญัติใหม่ได้					
3.ความได้เปรียบขององค์กร/ธุรกิจ	ความพึงพอใจของลูกค้า					
ระดับของผลกระทบ	I<0.5	0.5<I<=1	1<I<=1.5	1.5<I<=2	2<I<=2.5	2.5<I
	☐	☐	☐	☐	☐	☑
รายละเอียดคำอธิบายของผลกระทบ	ผู้กู้ยืมไม่สามารถยื่นขอกู้ยืมผ่านระบบเงินให้กู้ยืมได้ และสถานศึกษาไม่มีนักเรียนและนักศึกษามาลงทะเบียนเรียน					
4.ทางกฎหมาย	การปฏิบัติตามกฎหมายกฎระเบียบ – ค่าปรับ (บาท)					

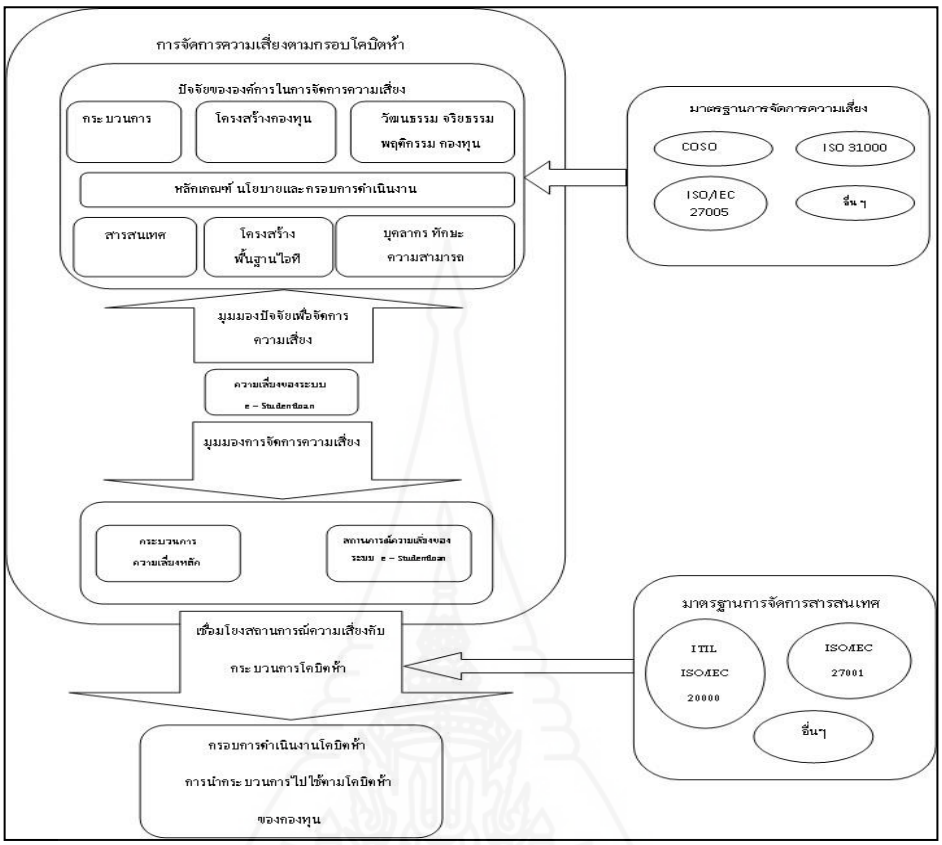
ตารางที่ 4.2 (ต่อ)

ระดับของผลกระทบ	None	< 1 ล้าน	< 10 ล้าน	< 100 ล้าน	< 1000 ล้าน	>1000 ล้าน
	☐	☐	☐	☐	☐	☑
รายละเอียดคำอธิบายของผลกระทบ						
ภาพรวมระดับของผลกระทบ						
ภาพรวมของระดับความเสี่ยงได้มาจากการรวบรวมความถี่และระดับความเสี่ยงจากแผนภูมิความเสี่ยง	☐ ต่ำ		☐ปานกลาง	☐ สูง	☐สูงมาก	
ส่วนที่ 4 การตอบสนองต่อความเสี่ยงการตอบสนองต่อความเสี่ยงนี้	☐ยอมรับความเสี่ยง		☑โอนความเสี่ยง	☐ลดความเสี่ยง	☐หลีกเลี่ยงความเสี่ยง	
การให้เหตุผล	กองทุนไม่สามารถดำเนินการได้เองเนื่องจากขาดบุคลากร ทักษะ ความรู้ความสามารถในการพัฒนาระบบการให้กู้ยืมตามพระราชบัญญัติใหม่					
รายละเอียดของการอธิบายการตอบสนอง (ไม่ต้องอธิบายในกรณียอมรับ)	การดำเนินการตอบสนอง			เสร็จสิ้น	แผนงาน	
	1. จัดจ้างที่ปรึกษาเพื่อพัฒนาระบบให้กู้ยืม			30 กันยายน พ.ศ.2559	1 ปี	
	2.จัดจ้างผู้พัฒนาระบบให้กู้ยืม			1 ตุลาคม พ.ศ. 2559	3 – 5 ปี	
	3.			☐	☐	
	4.			☐	☐	
	5.			☐	☐	
	6.			☐	☐	

ตารางที่ 4.2 (ต่อ)

ภาพรวมทั้งหมดของแผนการดำเนินงาน	
ประเด็นหลักเกี่ยวกับแผนการดำเนินงานความเสี่ยง	
ประเด็นหลักเกี่ยวกับการตอบสนองที่เสร็จสิ้น	
ส่วนที่ 5 ตัวชี้วัดความเสี่ยง	
ตัวชี้วัดความเสี่ยงหลักสำหรับความเสี่ยงนี้	1. 2. 3.

จากตารางที่ 4.2 นำสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 ที่เลือกมากำหนดรายละเอียดความเสี่ยงเพื่อลงทะเบียนลักษณะของความเสี่ยงและเก็บบันทึกข้อมูลความเสี่ยงเป็นฐานข้อมูลความเสี่ยงลงในระบบเทคโนโลยีสารสนเทศของกองทุนและนำข้อมูลความเสี่ยงที่เก็บรักษาไว้ (กระบวนการ APO12.01 กิจกรรมที่ 1) นำมาเป็นข้อมูลนำเข้าเชื่อมโยงกับกระบวนการบริหารความเสี่ยงโคบิต 5 (EDM03 และ APO12) ตามภาพที่ 4.2



ภาพที่ 4.2 การเชื่อมโยงสถานการณ์ความเสี่ยงกับหลักการบริหารความเสี่ยงโคบิต 5

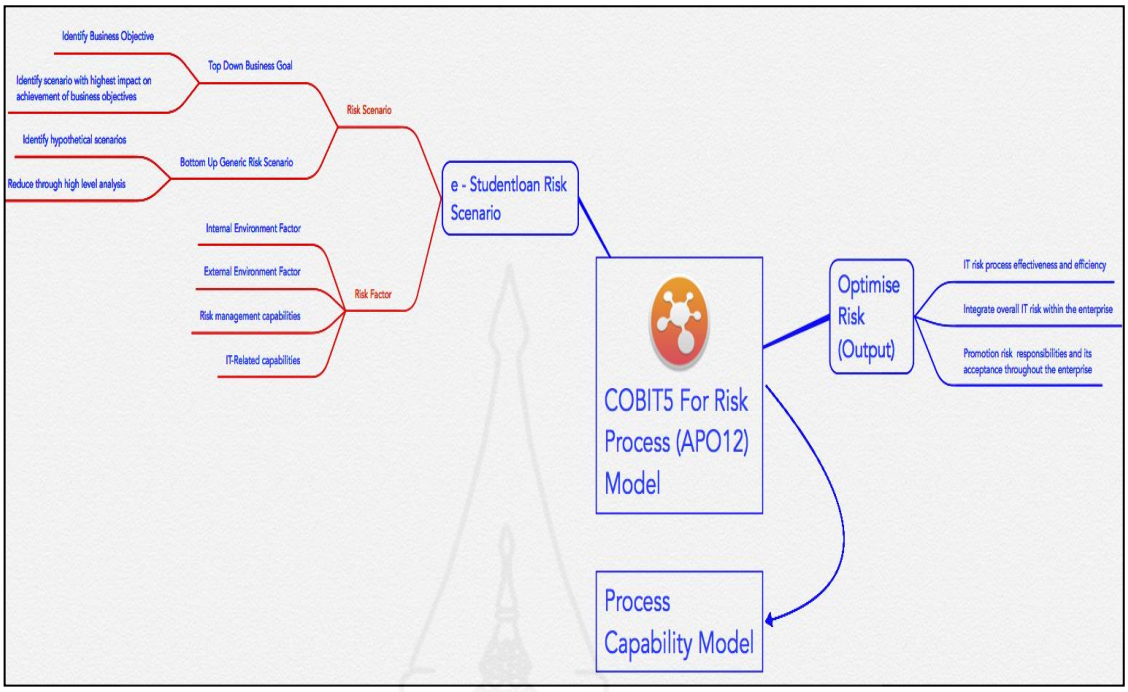
จากภาพที่ 4.2 แสดงการเชื่อมโยงสถานการณ์ความเสี่ยงของกองทุน (e - Stuendtloan) เข้ากับกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5เพื่อสร้างกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (EDM03 และ APO12) โดยจากภาพอธิบายกระบวนการบริหารความเสี่ยงสารสนเทศเชิงบูรณาการ (IT – Governance) และ อ้างอิงตามมาตรฐานสากล ตามคุณลักษณะต่างๆ ดังนี้ (1) รวบรวมความเสี่ยงทั่วทั้งองค์กร กำหนดและบันทึกความเสี่ยงและเฝ้าระวังความเสี่ยงที่เกิดขึ้น (ในส่วนของกระบวนการบริหารความเสี่ยงนี้โคบิตอ้างอิงกระบวนการจาก กรอบแนวคิดการบริหารความเสี่ยงเชิงบูรณาการ (COSOERM) มาตรฐานการบริหารความเสี่ยง (ISO 31000) มาตรฐานการบริหารความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27005) และกรอบแนวคิดและมาตรฐานอื่นๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยง) (2) วิเคราะห์ความเสี่ยง เก็บข้อมูลและบันทึกชุดข้อมูลความเสี่ยง และ (3) จัดการความเสี่ยง แสดงข้อมูลความเสี่ยงและตอบสนองต่อเหตุการณ์หรือความเสี่ยง โดยกระบวนการบริหารความเสี่ยงที่ได้ดำเนินการตามหลักการโคบิต 5

นั้นจะส่งผลให้ระบบให้กู้ยืมของกองทุนหรือองค์กรดำเนินการบริหารความเสี่ยงสารสนเทศแบบเชิงบูรณาการ ดังนี้

- ให้ความเชื่อมั่นได้ว่าสามารถบริหารความเสี่ยงสารสนเทศของระบบให้กู้ยืมเงินของกองทุน (e - Studentloan) ได้ทั่วทั้งองค์กร
- ให้ความเชื่อมั่นได้ว่า กำหนด ประเมินความเสี่ยงสารสนเทศของระบบให้กู้ยืมเงินกองทุน (e - Studentloan) ที่เกิดขึ้นได้
- ให้ความเชื่อมั่นได้ว่า ความเสี่ยงสารสนเทศระบบให้กู้ยืมเงินกองทุน (e - Studentloan) ที่กำหนดได้รับการตอบสนอง จัดการ ครบถ้วนและคุ้มค่า

ตอนที่ 2 พัฒนาระบบสารสนเทศของกองทุนตามกระบวนการบริหารความเสี่ยงโคบิต 5

ผู้วิจัยนำเสนอภาพที่ 4.3 สถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (แสดงรายละเอียดในวิธีการดำเนินวิจัย) โดยใช้ข้อมูลจากรายงานการดำเนินการบริหารความเสี่ยงของกองทุนเงินให้กู้ยืมเพื่อการศึกษา



ภาพที่ 4.3 สถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

จากภาพที่ 4.3 แสดงสถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการการบริหารความเสี่ยงตามหลักการโคบิต 5 โดยมีวิธีการ คือ สร้างสถานการณ์ความเสี่ยงของกองทุน (e -Studentloan)ตามหลักการโคบิต 5 เพื่อนำมาดำเนินกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ซึ่งกระบวนการบริหารความเสี่ยงของกองทุน (e -Studentloan) ต้องมีการประเมินความสำเร็จของกระบวนการจากผู้ประเมินการดำเนินงานตามหลักการโคบิต 5 (Cobit5 Assessor Certified) เพื่อเตรียมนำข้อมูลสถานะของกระบวนการเข้าสู่ รูปแบบตรวจสอบและวัดความสามารถกระบวนการการบริหารความเสี่ยงตามหลักการโคบิต 5 ในตอนที่ 1 มาออกแบบประกอบด้วยขั้นตอน ดังนี้

กำหนดขั้นตอนการตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (APO12) ประกอบด้วย 2 กระบวนการหลักคือ (1) การกำกับดูแลความเสี่ยง และ (2) การบริหารความเสี่ยง โดยแบ่งเป็นกระบวนการย่อยทั้งหมด 9 กระบวนการ ได้แก่ (1.1) EDM03.01 การประเมินความเสี่ยง (1.2) EDM03.02 สั่งการบริหารความเสี่ยง (1.3) EDM03.03 ติดตามการบริหารความเสี่ยง (2.1) APO12.01 รวบรวมข้อมูล (Collect Data)) (2.2) APO12.02 วิเคราะห์ความเสี่ยง (Analyze Risk)) (2.3) APO12.03 จัดเก็บข้อมูลความเสี่ยง (Maintain

a Risk profile)(2.4) APO12.04 ระบุข้อมูลความเสี่ยง (Articulate Risk) (2.5) APO12.05 กำหนดการจัดการความเสี่ยง (Define Risk Management) (2.6)APO12.06 ตอบสนองต่อความเสี่ยง (Respond to Risk) โดยผู้วิจัยได้สร้างรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 (Cobit5 for Risk system model) และอธิบายรายละเอียดกิจกรรมของแต่ละกระบวนการตามตาราง 4.3 – 4.11

ตารางที่ 4.3 กระบวนการประเมินความเสี่ยง (EDM03.01)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.01)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						
ประเมินความเสี่ยง	จาก กระบวนการ	รายละเอียด	รายละเอียด	ไปสู่ กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
ประเมินกำรบริหารความเสี่ยง ตรวจสอบและใช้วิจารณญาณในการพิจารณาอย่าง ต่อเนื่อง ถึงผลกระทบของความเสี่ยงด้านการใช้ไอที ในองค์กรทั้งปัจจุบันและอนาคต พิจารณาความ เหมาะสมของระดับความเสี่ยงขององค์กรที่ยอมรับ ได้และมีการระบุและบริหารจัดการความเสี่ยงที่มีต่อ คุณค่าขององค์กรซึ่งเกี่ยวข้องกับการใช้ไอที	APO12.01	ประเด็นความเสี่ยงที่เกิดขึ้น	แนวทางระดับความเสี่ยงที่ยอมรับได้	APO12.03					
			การอนุมัติระดับความเสี่ยงทีองค์กรรับได้	APO12.03					
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ	การวัดผลกิจกรรมการบริหารความเสี่ยง						

ตารางที่ 4.3 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1. กำหนดระดับของความเสี่ยงด้านไอทีที่กองทุนฯ สามารถยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์	0.167	0	ERROR	-	Not Achieved
2.ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านไอทีที่ยอมรับได้เทียบกับระดับของความเสี่ยงและโอกาสที่กองทุนฯ ยอมรับได้	0.167	0	ERROR	-	Not Achieved
3.พิจารณาว่ายุทธศาสตร์ความเสี่ยงด้านไอทีสอดคล้องกับยุทธศาสตร์ความเสี่ยงระดับกองทุนฯ มากน้อยเพียงใด	0.167	0	ERROR	-	Not Achieved
4.ประเมินปัจจัยเสี่ยงด้านไอทีในเชิงรุกสำหรับการตัดสินใจเชิงยุทธศาสตร์ของกองทุนฯ ที่รอดำเนินการและมั่นใจว่าการตัดสินใจของกองทุนฯได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว	0.167	0	ERROR	-	Not Achieved
5.พิจารณาว่ามีการประเมินและวัดผลความเสี่ยงของการใช้ไอทีอย่างเหมาะสม ตามมาตรฐานต่างๆ ที่เกี่ยวข้องทั้งของในประเทศและสากล	0.167	0	ERROR	-	Not Achieved
6.ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุนฯ ในการรับความสูญเสียที่เกี่ยวข้องกับไอทีและการยอมรับความสูญเสียของผู้นำ	0.167	0	ERROR	-	Not Achieved
สรุปกระบวนการ 03.01					Not Achieved

ตารางที่ 4.4 กระบวนการสั่งการบริหารความเสี่ยง (EDM03.02)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.02)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
สั่งการด้านการบริหารความเสี่ยง สั่งการให้จัดทำแนวปฏิบัติสำหรับการบริหารความ เสี่ยงเพื่อให้ความเชื่อมั่นได้ในระดับหนึ่งว่าแนวปฏิบัติในการบริหารความเสี่ยงด้านไอทีมีความเหมาะสม โดยให้มั่นใจว่าความเสี่ยงด้านไอทีที่เกิดขึ้นจริงจะต้องไม่เกินระดับความเสี่ยงที่คณะกรรมการบริหารยอมรับได้	APO12.03	รวบรวมข้อมูลความเสี่ยงรวมทั้งสถานการณ์ดำเนินการบริหารความเสี่ยง	นโยบายการบริหารความเสี่ยง	APO12.01	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			วัตถุประสงค์หลักที่จะติดตามสำหรับการบริหารความเสี่ยง	APO12.01					
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ (ข้อมูลความเสี่ยงและแผนการลดความเสี่ยง)	อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	APO12.01					

ตารางที่ 4.4(ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.ส่งเสริมวัฒนธรรมในการตระหนักถึงความเสี่ยงด้านไอที และสร้างเสริมให้กองทุนฯ สามารถระบุถึงความเสี่ยงของไอทีในเชิงรุก ตลอดจนโอกาส และผลกระทบทางธุรกิจที่อาจเกิดขึ้น	0.167	0	ERROR	-	Not Achieved
2.สั่งการให้บูรณาการยุทธศาสตร์และปฏิบัติการด้านความเสี่ยงของไอที เข้าไปในการตัดสินใจด้านความเสี่ยงเชิงยุทธศาสตร์และปฏิบัติการของกองทุนฯ	0.167	0	ERROR	-	Not Achieved
3.สั่งการให้มีการพัฒนาแผนการติดต่อสื่อสารด้านความเสี่ยง (ที่ครอบคลุมทุกระดับของกองทุนฯ) และแผนดำเนินการสำหรับความเสี่ยง	0.167	0	ERROR	-	Not Achieved
4.สั่งการให้นำกลไกที่เหมาะสมมาใช้เพื่อตอบสนองความเสี่ยงที่เปลี่ยนแปลงไปได้อย่างรวดเร็ว และสามารถรายงานไปยังผู้บริหารในระดับที่ เหมาะสมได้ทันที ซึ่งสนับสนุนโดยหลักการในการแจ้งเรื่องตามระดับที่เห็นชอบร่วมกัน (รายงานอะไร เมื่อไหร่ ที่ไหน และอย่างไร)	0.167	0	ERROR	-	Not Achieved
5.สั่งการให้ทุกคนสามารถรายงานเรื่องความเสี่ยง โอกาส ประเด็นปัญหา และข้อกังวลได้ทุกเมื่อ ความเสี่ยงควรได้รับการบริหารจัดการตาม นโยบายและขั้นตอนการปฏิบัติงานที่เผยแพร่ให้ทราบทั่วกันและได้รับการแจ้งเรื่องตามระดับไปยังผู้ที่มีอำนาจในการตัดสินใจที่เกี่ยวข้อง	0.167	0	ERROR	-	Not Achieved
6.ระบุเป้าหมายและมาตรวัดหลักของการกำกับดูแลและกระบวนการบริหารความเสี่ยงที่จะต้องเฝ้าติดตาม ตลอดจนอนุมัติวิธีปฏิบัติ วิธีการ เทคนิค และกระบวนการต่างๆ ที่ใช้เพื่อรวบรวมและรายงานสารสนเทศด้านการวัดผล	0.167	0	ERROR	-	Not Achieved
สรุปกระบวนการ 03.02					Not Achieved

ตารางที่ 4.5 กระบวนการติดตามบริหารความเสี่ยง (EDM03.03)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.03)										
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต							
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ						
เฝ้าติดตามการบริหารความเสี่ยง เฝ้าติดตามเป้าหมายหลักและมาตรวัดของกระบวนการในการบริหารความเสี่ยง และกำหนดวิธี การที่จะระบุถึงความเบี่ยงเบนหรือปัญหาต่างๆ ตลอดจนติดตามและรายงานผลสำหรับมาตรการ เยียวยา	APO12.02	ผลการวิเคราะห์ความเสี่ยง	กำหนดมาตรการแก้ไขการบริหารความเสี่ยงที่คาดเคลื่อน	APO12.06						
	APO12.04	*โอการที่จะยอมรับความเสี่ยงเพิ่มขึ้น *ผลการประเมินความเสี่ยงบุคคลภายนอก *วิเคราะห์ความเสี่ยงและรายงานข้อมูลความเสี่ยงต่อผู้มีส่วนได้เสีย	ประเด็นบริหารความเสี่ยงสำหรับประธานคณะกรรมการ	EDM05.01	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิต ห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ	

ตารา'ที่ 4.5 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.เฝ้าติดตามว่ามีการบริหารจัดการแผนภูมิความเสี่ยง (Risk Profile) ให้อยู่ภายใต้เกณฑ์ของระดับความเสี่ยงที่กองทุนฯ ยอมรับได้มากน้อยเพียงใด	0.25	0	ERROR	0	Not Achieved
2.เฝ้าติดตามเป้าหมายหลักและมาตรวัดของการกำกับดูแลและกระบวนการบริหารความเสี่ยงเทียบกับเป้า วิเคราะห์สาเหตุของความเบี่ยงเบนไปจากเป้า และเริ่มดำเนินมาตรการเยียวยาเพื่อจัดการกับสาเหตุดังกล่าว	0.25	0	ERROR	0	Not Achieved
3.เอื้อให้ผู้มีส่วนได้เสียหลักสามารถสอบทานความคืบหน้าของกองทุนฯ ที่จะไปสู่เป้าหมายที่ระบุไว้	0.25	0	ERROR	0	Not Achieved
4.รายงานประเด็นปัญหาต่างๆ ด้านการบริหารความเสี่ยงไปยังคณะกรรมการบริหารหรือคณะผู้บริหารระดับสูง	0.25	0	ERROR	0	Not Achieved
สรุปกระบวนการ 03.03					Not Achieved

ตารางที่ 4.6 กระบวนการรวบรวมข้อมูล (APO12.01)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.01)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
รวบรวมข้อมูล ระบุและรวบรวมข้อมูลที่เกี่ยวข้องที่เอื้อให้เกิดประสิทธิผลในการระบุ การวิเคราะห์และการรายงาน ด้านความเสี่ยงที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่ กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	การวัดผลกิจกรรมการบริหารความเสี่ยง	ข้อมูลของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงาน	ภายใน					
	EDM03.02	*อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	ข้อมูลเหตุการณ์ความเสี่ยงและปัจจัยที่ก่อให้เกิด	ภายใน					
	APO02.02	ช่องโหว่หรือความสามารถการบริหารความเสี่ยงปัจจุบัน	ประเด็นความเสี่ยงที่เกิดขึ้นและปัจจัยต่างๆ	EDM03.01 APO01.03 APO02.02					
	APO02.05	การประเมินความเสี่ยง							
	APO10.04	ระบุความเสี่ยงจากการส่งมอบของผู้ผลิต							

ตารางที่ 4.6 (ต่อ)

DSS02.07	สถานะของเหตุการณ์ที่เกิดและรายงานแนวโน้มของเหตุการณ์					
	กิจกรรมที่ต้องดำเนินการ					
1.กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และการวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับไอทีซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านไอที และปัจจัยเสี่ยง		0.143	0	ERROR	-	Not Achieved
2.บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมในการปฏิบัติงานของกองทุนฯทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านไอที		0.143	0	ERROR	-	Not Achieved
3.สำรวจและวิเคราะห์ข้อมูลความเสี่ยงด้านไอทีในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนฯที่มีอยู่จากธุรกิจในประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภทสำหรับ การเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้		0.143	0	ERROR	-	Not Achieved
4.บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นหรืออาจเป็นสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของไอที ต่อการส่งมอบชุดโครงการและโครงการด้านไอที และ/หรือต่อปฏิบัติการและการส่งมอบบริการด้านไอที จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง		0.143	0	ERROR	-	Not Achieved

ตารางที่ 4.6 (ต่อ)

5.จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณต่างๆ เหล่านั้นมีร่วมกัน	0.143	0	ERROR	-	Not Achieved
6.ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือที่ไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยง และลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ	0.143	0	ERROR	-	Not Achieved
7.ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะ เพื่อระบุประเด็นปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่ และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.01					Not Achieved

ตาราง ที่ 4.7 กระบวนการวิเคราะห์ความเสี่ยง (APO12.02)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.02)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
วิเคราะห์ความเสี่ยง				ไปสู่					
พัฒนาสารสนเทศที่มีประโยชน์ต่อกาสนับสนุนการ ตัดสินใจด้านความเสี่ยง ซึ่งได้คำนึงถึงความเกี่ยวเนื่องทางธุรกิจของปัจจัยความเสี่ยงต่างๆ	จากกระบวนการ DSS04.02	รายละเอียดวิเคราะห์ผลกระทบกองทุนฯ	รายละเอียดขอบเขตของความพยายามการวิเคราะห์ความเสี่ยงสถานการณ์ความเสี่ยงเทคโนโลยีสารสนเทศ	กระบวนการภายใน	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	DSS05.01	การประเมินผลของภัยคุกคามที่เกิดขึ้น		ภายใน					
	ภายนอกโคบิต	คำแนะนำสำหรับภัยคุกคาม	ผลการวิเคราะห์ความเสี่ยง	EDM03.03 APO01.03 APO02.02 BAI01.10					

ตารางที่ 4.7 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.กำหนดความกว้างและความลึกที่เหมาะสมของความพยายามในการวิเคราะห์ความเสี่ยง โดยพิจารณาถึงทุกปัจจัยเสี่ยงและความสำคัญเชิงธุรกิจของสินทรัพย์ และกำหนดขอบเขตของการวิเคราะห์ความเสี่ยงภายหลังจากการวิเคราะห์ต้นทุน-ผลประโยชน์	0.143	0	ERROR	-	Not Achieved
2.จัดทำสถานการณ์ต่างๆ ของความเสี่ยงด้านไอทีและปรับปรุงให้เป็นปัจจุบัน รวมถึงการรวมสถานการณ์ความเสี่ยงที่มีประเภทของภัยคุกคามในลักษณะที่ส่งทอดถึงกันและ/หรือที่เกิดขึ้นพร้อมกันไว้ด้วยกัน แล้วกำหนดความคาดหวังสำหรับกิจกรรมของการควบคุมเฉพาะด้าน ความ สามารถในการตรวจพบ และมาตรการตอบสนองอื่นๆ	0.143	0	ERROR	-	Not Achieved
3.ประมาณความถี่และความรุนแรงของการสูญเสียหรือประโยชน์ที่สัมพันธ์กับสถานการณ์ต่างๆ ของความเสี่ยงด้านไอที คำนึงถึงปัจจัยเสี่ยงที่เกี่ยวข้องทั้งหมด ประเมินการควบคุมเชิงปฏิบัติการที่มีอยู่และประมาณระดับความเสี่ยงที่เหลืออยู่	0.143	0	ERROR	-	Not Achieved
4.เปรียบเทียบความเสี่ยงที่เหลืออยู่กับความคลาดเคลื่อนของความเสี่ยงที่ยอมรับได้และระบุโอกาสเสี่ยงภัยที่อาจจำเป็นต้องตอบสนอง	0.143	0	ERROR	-	Not Achieved
5.วิเคราะห์ ต้นทุน-ผลประโยชน์ของทางเลือกในการตอบสนองความเสี่ยงที่อาจเป็นไปได้ เช่น การหลีกเลี่ยง ลด/บรรเทา โอน/แบ่งปัน และยอมรับและฉวย/คว้าโอกาส เป็นต้น นำเสนอการตอบสนองความเสี่ยงที่เหมาะสมที่สุด	0.143	0	ERROR	-	Not Achieved
6.ระบุข้อกำหนดความต้องการในภาพรวมสำหรับโครงการหรือชุดโครงการที่นำการตอบสนองความเสี่ยงที่เลือกแล้วไปใช้ ระบุความต้องการ และความคาดหวังต่างๆ สำหรับการควบคุมหลักที่เหมาะสมเพื่อการตอบสนองโดยการบรรเทาความเสี่ยง	0.143	0	ERROR	-	Not Achieved

ตารางที่ 4.7 (ต่อ)

7.ตรวจสอบความสมเหตุสมผลของผลการวิเคราะห์ความเสี่ยงต่างๆ ก่อนนำมาใช้ประกอบการตัดสินใจ โดยยืนยันว่าการวิเคราะห์นั้นสอดคล้อง กับข้อกำหนดความต้องการของกองทุนฯ และทวนสอบว่าการประมาณการต่างๆ นั้นมีความเที่ยงตรงและได้พิจารณาถึงอคติที่อาจมี	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.02					Not Achieved

ตารางที่ 4.8 กระบวนการดูแลแผนภูมิความเสี่ยง (APO12.03)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.03)								
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต					
ดูแลรักษาแผนภูมิความเสี่ยง ดูแลรักษาบัญชีรายการความเสี่ยงและคุณลักษณะ ของความเสี่ยงต่างๆ ที่มี (รวมถึงความถี่ที่คาดการณ ไว้ ผลกระทบที่อาจเกิดขึ้น และการตอบสนอง) และ บัญชีรายชื่อของทรัพยากร ความสามารถ และกิจกรรมการควบคุมในปัจจุบันที่เกี่ยวข้อง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการภายใน	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	*อนุมัติระดับความเสี่ยงที่ยอมรับได้ *แนะนำแนวทางการยอมรับความเสี่ยง	ทำเอกสารสถานการณ์ความเสี่ยงตามสายงานของกองทุนฯ และหน้าที่การดำเนินงาน						
	APO10.04	ระบุความเสี่ยงการส่งมอบของผู้ผลิต	รวบรวมข้อมูลความเสี่ยงรวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	EDM03.02 APO02.02					
	DSS05.01	การประเมินผลของภัยคุกคามที่อาจเกิดขึ้น							

ตารางที่ 4.8 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.จัดทำบัญชีรายการของกระบวนการดำเนินงานต่างๆ รวมถึงบุคลากร ระบบงาน โครงสร้างพื้นฐาน สถานที่และสิ่งอำนวยความสะดวก บันทึก ข้อมูลที่จัดทำด้วยคนที่สำคัญ ผู้ขาย และผู้ให้บริการภายนอกที่สนับสนุนกระบวนการ ตลอดจนจัดทำเอกสารการพึงพากระบวนการบริหาร จัดการบริการด้านไอทีและทรัพยากรโครงสร้างพื้นฐานด้านไอทีต่างๆ	0.143	0	ERRO R	-	Not Achieved
2.กำหนดและเห็นชอบร่วมกันว่าบริการด้านไอทีและโครงสร้างพื้นฐานด้านไอทีใดที่มีความสำคัญในการสนับสนุนการปฏิบัติงานของ กระบวนการดำเนินงานต่างๆ ให้เกิดขึ้นอย่างต่อเนื่อง วิเคราะห์ระดับการพึ่งพาและระบุจุดอ่อน	0.143	0	ERRO R	-	Not Achieved
3.รวบรวมสถานการณ์ความเสี่ยงต่างๆ ตามประเภท สายงานดำเนินการ และหน้าที่งานด้านต่างๆ	0.143	0	ERRO R	-	Not Achieved
4.จัดเก็บสารสนเทศด้านแผนภูมิความเสี่ยงทั้งหมดและนำมารวมเป็นแผนภูมิความเสี่ยงรวมอย่างสม่ำเสมอ	0.143	0	ERRO R	-	Not Achieved
5.กำหนดชุดของดัชนีความเสี่ยงจากข้อมูลทั้งหมดในแผนภูมิความเสี่ยง ซึ่งจะช่วยให้การระบุและเฝ้าติดตามความเสี่ยงในปัจจุบันและแนว โน้มความเสี่ยงทำได้อย่างรวดเร็ว	0.143	0	ERRO R	-	Not Achieved
6.จัดเก็บสารสนเทศของเหตุการณ์ความเสี่ยงต่างๆ ด้านไอทีที่เกิดขึ้นจริง เพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	0	ERRO R	-	Not Achieved
7.จัดเก็บสารสนเทศเกี่ยวกับสถานะของแผนดำเนินการด้านความเสี่ยงเพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	0	ERRO R	-	Not Achieved
สรุปกระบวนการ 12.03					Not Achieved

ตารางที่ 4.9 กระบวนการเชื่อมโยงความเสี่ยง (APO12.04)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.04)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
เชื่อมโยงความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
นำเสนอสารสนเทศเกี่ยวกับสถานะปัจจุบันของโอกาสเสี่ยงภัยและโอกาสอำนวยประโยชน์ที่เกี่ยวข้องกับไอทีอย่างทันเวลาแก่ผู้มีส่วนได้เสียเพื่อให้มีการตอบสนองอย่างเหมาะสม			วิเคราะห์ความเสี่ยงและรายงานความเสี่ยงต่อผู้มีส่วนได้เสีย	EDM03.03 EDM05.02 APO10.04 MEA02.08	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			รวบรวมข้อมูลความเสี่ยง รวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	EDM03.03 APO10.04 MEA02.01					
			โอกาสต่างๆ สำหรับการยอมรับความเสี่ยงที่เพิ่มขึ้น	EDM03.03					

ตารางที่ 4.9 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.รายงานผลของการวิเคราะห์ความเสี่ยงไปยังผู้มีส่วนได้เสียที่ได้รับผลกระทบทั้งหมดตามเงื่อนไขและรูปแบบที่มีประโยชน์ในการสนับสนุน การตัดสินใจของกองทุนฯ รวมถึงระบุความเป็นไปได้ต่างๆ และขอบเขตของความสูญเสียและผลประโยชน์ พร้อมทั้งระดับความเชื่อมั่นเพื่อเอื้อให้ผู้บริหารสามารถสร้างสมดุลระหว่างความเสี่ยงกับผลตอบแทน หากเป็นไปได้	0.20	0	ERROR	0	Not Achieved
2.นำเสนอแก่ผู้มีหน้าที่ตัดสินใจ ในเรื่องสถานการณ์ที่สามารถทำให้เข้าใจถึงเหตุการณ์ที่เลวร้ายที่สุดและโอกาสที่เป็นไปได้มากที่สุด ในเรื่องการกระทำโดยระมัดระวังถึงโอกาสเสี่ยงภัย และการคำนึงถึงชื่อเสียง กฎหมาย หรือกฎระเบียบข้อบังคับต่างๆ ที่สำคัญ	0.20	0	ERROR	0	Not Achieved
3.รายงานถึงแผนภูมิความเสี่ยงในปัจจุบันไปยังผู้มีส่วนได้เสียทุกคน ซึ่งรวมถึงเรื่องของประสิทธิผลของกระบวนการบริหารความเสี่ยงประสิทธิภาพของการควบคุม ช่องว่าง/ความต่าง ความไม่สม่ำเสมอความซ้ำซ้อน สถานะของการแก้ไขปรับปรุง และผลกระทบของปัจจัย เหล่านี้ที่มีต่อแผนภูมิความเสี่ยง	0.20	0	ERROR	0	Not Achieved
4.สอบทานผลการประเมินจากองค์กรภายนอกที่เป็นกลาง การตรวจสอบภายใน และการสอบทานการให้ความเชื่อมั่นด้านคุณภาพ และเชื่อม โยงผลเหล่านั้นเข้ากับแผนภูมิความเสี่ยง สอบทานช่องว่างและโอกาสเสี่ยงภัยที่ได้รับการระบุเพื่อพิจารณาถึงความจำเป็นที่ต้องจัดให้มีการ วิเคราะห์ความเสี่ยงเพิ่มเติม	0.20	0	ERROR	0	Not Achieved
5.สำหรับในด้านความเสี่ยงสัมพัทธ์ (relative risk) และความเท่าเทียมกันในระดับของความเสี่ยงเพื่อให้ได้ผลประโยชน์ตามที่ต้องการ (riskcapacity parity) นั้น ให้ระบุโอกาสที่เกี่ยวข้องกับไอทีเป็นระยะเพื่อช่วยให้สามารถยอมรับความเสี่ยงได้มากขึ้นและช่วยให้มีการเติบโตและได้รับผลตอบแทนที่ดีขึ้น	0.20	0	ERROR	0	Not Achieved
สรุปกระบวนการ 12.04					Not Achieved

ตารางที่ 4.10 กระบวนการกำหนดกลุ่มของการดำเนินการบริหารความเสี่ยง (APO12.05)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.05)								
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต		ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
กำหนดกลุ่มของการดำเนินการ บริหารความเสี่ยงบริหารจัดการโอกาสต่างๆ แบบกลุ่ม (portfolio) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	จากกระบวนการ	รายละเอียด	รายละเอียด นำเสนอโครงการสำหรับการลดความเสี่ยง	ไปสู่กระบวนการ APO02.02 APO13.02					
กิจกรรมที่ต้องดำเนินการ									
1.จัดทำบัญชีรายชื่อกิจกรรมการควบคุมที่มีอยู่เพื่อบริหารความเสี่ยงและที่เอื้อให้ความเสี่ยงสอดคล้องกับระดับและช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ จำแนกกิจกรรมการควบคุมต่างๆ และจับคู่กิจกรรมเหล่านั้นกับคำแถลงความเสี่ยงด้านไอทีที่เกี่ยวข้องและ การรวมกลุ่มของความเสี่ยงด้านไอที					0.333	0	ERROR	-	Not Achieved
2.พิจารณาว่าแต่ละหน่วยงานในกองทุนฯ ได้มีการเฝ้าติดตามความเสี่ยงและยอมรับต่อความรับผิดชอบในผลงานสำหรับการดำเนินงานภายใต้ระดับช่วงความเบี่ยงเบนของความเสี่ยงยอมรับได้ทั้งในระดับหน่วยและในระดับกลุ่ม					0.333	0	ERROR	-	Not Achieved

ตารางที่ 4.10 (ต่อ)

3.กำหนดชุดที่มีความสมดุลของข้อเสนอโครงการซึ่งได้ออกแบบมาเพื่อลดความเสี่ยง และ/หรือ โครงการที่เอื้อต่อโอกาสต่างๆ ด้านยุทธศาสตร์ของกองทุนฯ พิจารณาถึงต้นทุนและผลประโยชน์ ผลกระทบต่อแผนภูมิความเสี่ยงและกฎระเบียบข้อบังคับต่างๆ ในปัจจุบัน	0.333	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.05					Not Achieved

ตารางที่ 4.11 กระบวนการตอบสนองต่อความเสี่ยง (APO12.06)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.06)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
ตอบสนองต่อความเสี่ยง ตอบสนองอย่างทันเวลาด้วยมาตรการที่มีประสิทธิผลในการจำกัดความรุนแรงของความสูญ เสียอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
		ดำเนินการปรับปรุงเพื่อบรรจุความคลาดเคลื่อนการบริหารความเสี่ยง	แผนตอบสนองต่อเหตุการณ์ที่เป็นความเสี่ยง	DSS02.05					
			การสื่อสารผลกระทบความเสี่ยง	APO01.04 APO08.04 DSS04.02					
			โอกาสต่างๆ สำหรับการยอมรับความเสี่ยงที่เพิ่มขึ้น	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ

ตารางที่ 4.11 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.จัดเตรียม บำรุงรักษา และทดสอบแผนต่างๆ ที่บันทึกขั้นตอนเฉพาะที่จะนำไปใช้เมื่อเหตุการณ์ความเสี่ยงอาจก่อให้เกิดเหตุการณ์ผิดปกติด้านการปฏิบัติงานหรือด้านการพัฒนาที่มีนัยสำคัญซึ่งส่งผลกระทบต่อกองทุนฯ อย่างรุนแรง ให้มั่นใจว่าแผนดังกล่าวนี้ได้รวมเส้นทางในการแจ้ง เรื่องตามระดับทั่วทั้งกองทุนฯ	0.25	0	ERROR	0	Not Achieved
2.จัดหมวดหมู่ของเหตุการณ์ผิดปกติ และเปรียบเทียบโอกาสเสี่ยงภัยที่เกิดขึ้นจริงกับขีดจำกัดของช่วงความเบี่ยงเบนของความเสี่ยงที่กองทุนฯ ยอมรับได้ สื่อสารผลกระทบต่อกองทุนฯ ไปยังผู้มีอำนาจตัดสินใจต่างๆ โดยให้เป็นส่วนหนึ่งของการรายงาน และปรับแผนภูมิความเสี่ยงให้เป็น ปัจจุบัน	0.25	0	ERROR	0	Not Achieved
3.ประยุกต์ใช้แผนการตอบสนองที่เหมาะสมในการลดผลกระทบให้น้อยที่สุดเมื่อเกิดเหตุการณ์ผิดปกติ	0.25	0	ERROR	0	Not Achieved
4.ตรวจสอบเหตุการณ์ไม่พึงประสงค์หรือความเสียหายรวมถึงการสูญเสียโอกาสต่างๆ ในอดีตและวิเคราะห์ถึงต้นเหตุ สื่อสารต้นเหตุ ข้อกำหนดความต้องการในการตอบสนองต่อความเสี่ยงเพิ่มเติมและการปรับปรุงกระบวนการ ไปยังผู้มีอำนาจตัดสินใจในกองทุนฯ ที่เหมาะสม และให้มั่นใจว่าต้นเหตุ ข้อกำหนดความต้องการในการตอบสนอง และการปรับปรุงกระบวนการได้รวมไว้ในกระบวนการกำกับดูแลด้านความเสี่ยง	0.25	0	ERROR	0	Not Achieved
สรุปกระบวนการ 12.06					Not Achieved

ตอนที่ 3 ทดสอบรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

แบ่งเป็น 2 ส่วน (3.1) ทดสอบกระบวนการบริหารความเสี่ยงกองทุนกับกระบวนการบริหารความเสี่ยงโคบิต 5และ (3.2) สมมุติฐานกระบวนการบริหารความเสี่ยงกองทุนฯ เปรียบเทียบกับการบริหารความเสี่ยงของ บมจ.ธนาคารกสิกรไทย

3.1 ทดสอบกระบวนการบริหารความเสี่ยงกองทุนกับกระบวนการบริหารความเสี่ยงโคบิต 5 นำกระบวนการบริหารความเสี่ยงของกระบวนการให้กู้ยืมเงินของกองทุน (รายงานการบริหารความเสี่ยงการดำเนินงานกองทุนเงินให้กู้ยืมเพื่อเป็น) จากตารางที่ 4.2 ข้อมูลความเสี่ยง มาทำการการทดสอบกระบวนการบริหารความเสี่ยงเดิมที่กองทุนดำเนินงานกับแนวทางตามหลักการโคบิต 5 ด้วยรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการการบริหารความเสี่ยงตามหลักการโคบิต 5 ที่ผู้วิจัยได้พัฒนาขึ้นมา ตามตารางที่ 4.12 – 4.13

ตารางที่ 4.12 ผลทดสอบกระบวนการประเมินความเสี่ยงของกองทุน (EDM03.01)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.01)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						
ประเมินความเสี่ยง	จาก กระบวนการ	รายละเอียด	รายละเอียด	ไปสู่ กระบวนการ					
ประเมินกำรบริหารความเสี่ยง ตรวจสอบและใช้วิจารณญาณในการพิจารณาอย่าง ต่อเนื่องถึงผลกระทบของความเสี่ยงด้านการใช้ไอที ในองค์กรทั้งปัจจุบันและอนาคต พิจารณาความเหมาะสมของระดับความเสี่ยงขององค์กรที่ยอมรับ ได้ และมีการระบุและบริหารจัดการความเสี่ยงที่มีต่อคุณค่าขององค์กรซึ่งเกี่ยวข้องกับการใช้ไอที	APO12.01	ประเด็นความเสี่ยงที่เกิดขึ้น	แนวทางระดับความเสี่ยงที่ยอมรับได้	APO12.03	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			การอนุมัติระดับความเสี่ยงทีองค์กรรับได้	APO12.03					
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ	การวัดผลกิจกรรมการบริหารความเสี่ยง	APO12.01					

ตารางที่ 4.12 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1. กำหนดระดับของความเสี่ยงด้านไอทีที่กองทุนฯ สามารถยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์	0.167	0	ERROR	-	Not Achieved
2.ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านไอทีที่ยอมรับได้เทียบกับระดับของความเสี่ยงและโอกาสที่กองทุนฯ ยอมรับได้	0.167	0	ERROR	-	Not Achieved
3.พิจารณาว่ายุทธศาสตร์ความเสี่ยงด้านไอทีสอดคล้องกับยุทธศาสตร์ความเสี่ยงระดับกองทุนฯ มากน้อยเพียงใด	0.167	0	ERROR	-	Not Achieved
4.ประเมินปัจจัยเสี่ยงด้านไอทีในเชิงรุกสำหรับการตัดสินใจเชิงยุทธศาสตร์ของกองทุนฯ ที่รอดำเนินการ และมั่นใจว่าการตัดสินใจของกงอทุนฯได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว	0.167	0	ERROR	-	Not Achieved
5.พิจารณาว่ามีการประเมินและวัดผลความเสี่ยงของการใช้ไอทีอย่างเหมาะสม ตามมาตรฐานต่างๆ ที่เกี่ยวข้องทั้งของในประเทศและสากล	0.167	0	ERROR	-	Not Achieved
6.ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุนฯ ในการรับความสูญเสียที่เกี่ยวข้องกับไอทีและการยอมรับความสูญเสียของผู้นำ	0.167	0	ERROR	-	Not Achieved
สรุปกระบวนการ 03.01					Not Achieved

ตารางที่ 4.13 ผลทดสอบกระบวนการรวบรวมข้อมูลของกองทุน (APO12.01)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.01)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
รวบรวมข้อมูล ระบุและรวบรวมข้อมูลที่เกี่ยวข้องที่เอื้อให้เกิดประสิทธิผลในการระบุ การวิเคราะห์และการรายงาน ด้านความเสี่ยงที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	การวัดผลกิจกรรมการบริหารความเสี่ยง	ข้อมูลของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงาน	ภายใน					
	EDM03.02	*อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	ข้อมูลเหตุการณ์ความเสี่ยงและปัจจัยที่ก่อให้เกิดประเด็นความเสี่ยงที่เกิดขึ้นและปัจจัยต่างๆ	ภายใน					
	APO02.02	ช่องโหว่หรือความสามารถการบริหารความเสี่ยงปัจจุบัน		EDM03.01 APO01.03 APO02.02					
	APO02.05	การประเมินความเสี่ยง							
	APO10.04	ระบุความเสี่ยงจากการส่งมอบของผู้ผลิต							

ตารางที่ 4.13 (ต่อ)

DSS02.07	สถานะของเหตุการณ์ที่เกิดและรายงานแนวโน้มของเหตุการณ์					
	กิจกรรมที่ต้องดำเนินการ					
	1.กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และการวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับไอทีซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านไอที และปัจจัยเสี่ยง	0.143	0	ERROR	-	Not Achieved
	2.บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมในการปฏิบัติงานของกองทุนฯทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านไอที	0.143	0	ERROR	-	Not Achieved
	3.สำรวจและวิเคราะห์ข้อมูลความเสี่ยงด้านไอทีในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนฯที่มีอยู่จากธุรกิจในประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภทสำหรับ การเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้	0.143	0	ERROR	-	Not Achieved
	4.บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นหรืออาจเป็นสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของไอที ต่อการส่งมอบชุดโครงการและโครงการด้านไอที และ/หรือต่อปฏิบัติการและการส่งมอบบริการด้านไอที จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆที่เกี่ยวข้อง	0.143	0	ERROR	-	Not Achieved

ตารางที่ 4.13 (ต่อ)

5.จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณต่างๆ เหล่านั้นมีร่วมกัน	0.143	0	ERROR	-	Not Achieved
6.ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือที่ไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยง และลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ	0.143	0	ERROR	-	Not Achieved
7.ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะ เพื่อระบุประเด็นปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่ และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง	0.143	0	ERROR	-	Not Achieved
สรุปกระบวนการ 12.01					Not Achieved

จากตารางที่ 4.12 – 4.13 แสดงผลการทดสอบรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการการบริหารความเสี่ยงตามหลักการโคบิต 5 โดยจากการดำเนินงานบริหารความเสี่ยงกองทุนสามารถทดสอบได้เฉพาะกระบวนการรวบรวมข้อมูล (APO12.01) และกระบวนการประเมินความเสี่ยง (EDM03.01) เท่านั้นโดยผลการทดสอบกระบวนการบริหารความเสี่ยงของกองทุนทั้งสองกระบวนการไม่สำเร็จ (Not Achieved) ตามหลักการโคบิต 5 เนื่องด้วยเหตุที่กองทุนไม่ได้ดำเนินงานบริหารความเสี่ยงตามหลักการโคบิต 5 ตั้งแต่แรกเริ่ม คือ อนุมัติการบริหารความเสี่ยงจาก คณะกรรมการกองทุน สั่งการลงมายัง ฝ่ายบริหารในการดำเนินงานรวบรวมข้อมูลต่างๆ เพื่อเตรียมการตามกิจกรรมตามหลักการบริหารความเสี่ยงโคบิต 5 ซึ่งตามหลักการโคบิต 5 ความสำเร็จของแต่ละกระบวนการทั้ง 37 กระบวนการต้องมีการวัดความสามารถของกระบวนการตามที่กล่าวไว้ในวิธีการดำเนินการวิจัยข้อ 4.3 (ต้องดำเนินกิจกรรมให้ครบทุกกิจกรรมจึงจะมีสถานะความสำเร็จเป็นสมบูรณ์ในกระบวนการนั้น) หากไม่ได้ดำเนินการกิจกรรมใดกิจกรรมหนึ่งถือว่าการดำเนินการของกระบวนการที่ดำเนินการอยู่เดิมไม่ตรงตามหลักการโคบิต 5 จากการทดสอบสามารถสรุปผลการทดสอบการดำเนินการบริหารความเสี่ยงของระบบให้กู้ยืมเงินเพื่อการศึกษาตามความเสี่ยงที่ได้เลือกมาข้างต้นกับรูปแบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการโคบิต 5 ตามตารางที่ 4.14

ตารางที่ 4.14 สรุปผลการทดสอบการดำเนินการบริหารความเสี่ยงระบบให้กู้ยืมเงินเพื่อการศึกษากับรูปแบบตรวจสอบและวัดความสามารถของการบริหารความเสี่ยงตามหลักการ โคบิต 5

กระบวนการความเสี่ยงโคบิต 5	ผู้วิจัยประเมินกองทุน	การดำเนินการบริหารความเสี่ยงกองทุน (กำหนดโดยทุนฝ่ายงาน)	กองทุนควรดำเนินการวางแผนความต้องการบริหารความเสี่ยงตามหลักการ โคบิต 5เพื่อบรรลุผลสำเร็จในแต่ละกระบวนการ
EDM03.01	X[1]	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
EDM03.02	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการ

ตารางที่ 4.14 (ต่อ)

กระบวนการความเสี่ยงโคบิต 5	ผู้วิจัยประเมินกองทุน	การดำเนินการบริหารความเสี่ยงกองทุน (กำหนดโดยทุนฝ่ายงาน)	กองทุนควรดำเนินการวางแผนความต้องการบริหารความเสี่ยงตามหลักการโคบิต 5เพื่อบรรลุผลสำเร็จในแต่ละกระบวนการ
			โคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
EDM03.03	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
APO12.01	X	✓[2] ดำเนินการเพียง 1 กิจกรรมจาก 7 กิจกรรม	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
APO12.02	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
APO12.03	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสาร

ตารางที่ 4.14 (ต่อ)

กระบวนการความเสี่ยงโคบิต 5	ผู้วิจัยประเมินกองทุน	การดำเนินการบริหารความเสี่ยงกองทุน (กำหนดโดยทุนฝ่ายงาน)	กองทุนควรดำเนินการวางแผนความต้องการบริหารความเสี่ยงตามหลักการโคบิต 5เพื่อบรรลุผลสำเร็จในแต่ละกระบวนการ
			โคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
APO12.05	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
APO12.06	X	X	นำแนวทางการบริหารความเสี่ยงตามหลักการโคบิตมาปรับใช้สื่อสารให้ทั่วทั้งองค์กรตามข้อเสนอแนะ
สรุปผลความสำเร็จกระบวนการบริหารความเสี่ยง	**ไม่ผ่าน**	**ไม่ผ่าน**	**มีแนวโน้มที่จะผ่าน**

หมายเหตุ [1] เครื่องหมาย X ไม่ได้ดำเนินกิจกรรมตามหลักการบริหารความเสี่ยงโคบิต 5 ที่กล่าวไว้ในระเบียบวิธีวิจัย

[2] ดำเนินกิจกรรมตามหลักการบริหารความเสี่ยงตามหลักการโคบิต 5 ที่กล่าวไว้ในระเบียบวิธีวิจัย

จากตารางที่ 4.14 ผลความสำเร็จของการบริหารความเสี่ยงกองทุนตามหลักการบริหารความเสี่ยงโคบิต 5 คือ ไม่ผ่านด้วยเหตุผล การดำเนินการบริหารความเสี่ยงเดิมของกองทุนไม่เป็นไปตามหลักการบริหารความเสี่ยงโคบิต 5 ดังนั้นกองทุนควรปรับปรุงการดำเนินงานกำกับดูแลและบริหารความเสี่ยงของกระบวนการกู้ยืมในประเด็นความเสี่ยง (กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พ.ร.บ...ใหม่ทัน) ตามหลักการการกำกับดูแลและบริหารความเสี่ยงโคบิต5ดังนี้

3.1.1 ปรับปรุงกระบวนการกำกับดูแลความเสี่ยงของกองทุน ในกิจกรรมต่างๆ ตามตารางที่ 4.12 ดังนี้

1) กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กองทุนสามารถรับได้ เพื่อให้บรรลุวัตถุประสงค์

2) ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่องยอมรับเทียบกับระดับความเสี่ยงและโอกาสที่กองทุนยอมรับได้

3) พิจารณาว่ายุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสอดคล้องกับยุทธศาสตร์บริหารความเสี่ยงของกองทุนมากน้อยเพียงใด

4) ประเมินปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศในเชิงรุกสำหรับการตัดสินเชิงยุทธศาสตร์ที่รอดำเนินการ และ มั่นใจว่าการตัดสินใจของกองทุนได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว

5) พิจารณาว่ามีการประเมินความเสี่ยงและวัดผลความเสี่ยงของการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมตามมาตรฐานต่างๆ ที่เกี่ยวข้อง ทั้งของในประเทศและสากล

6) ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุน ในการรับความสูญเสียที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการยอมรับความสูญเสียของผู้นำ

ข้อแนะนำการดำเนินกิจกรรม (1 – 6):กองทุนควรกำหนด (1) ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กองทุนสามารถรับได้ เพื่อให้บรรลุวัตถุประสงค์ (2) ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่องยอมรับเทียบกับระดับความเสี่ยงและโอกาสที่กองทุนยอมรับได้ (3) พิจารณาว่ายุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสอดคล้องกับยุทธศาสตร์บริหารความเสี่ยงของกองทุนมากน้อยเพียงใด (4) ประเมินปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศในเชิงรุกสำหรับการตัดสินเชิงยุทธศาสตร์ที่รอดำเนินการ และ มั่นใจว่าการตัดสินใจของกองทุนได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว (5) พิจารณาว่ามีการ

ประเมินความเสี่ยงและวัดผลความเสี่ยงของการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมตามมาตรฐานต่างๆ ที่เกี่ยวข้อง ทั้งของในประเทศและสากล (6) ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุน ในการรับความสูญเสียที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการยอมรับความสูญเสียของผู้นำ

3.1.2 ปรับปรุงกระบวนการบริหารความเสี่ยงของกองทุน ในกิจกรรมต่างๆ ตามตารางที่ 4.13 ดังนี้

1) กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านเทคโนโลยีสารสนเทศ และปัจจัยเสี่ยง

ข้อแนะนำการดำเนินกิจกรรม: กำหนดและดูแลวิธีการเก็บรวบรวม จำแนกประเภท วิเคราะห์ข้อมูล จัดหมวดหมู่ ของข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศและปัจจัยเสี่ยงของกองทุน เช่น สร้างฐานข้อมูลความเสี่ยง ฐานข้อมูลปัจจัยเสี่ยงทุกด้านของกองทุน และฐานข้อมูลประเภทของเหตุการณ์ต่างๆ เป็นต้น

2) บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงานของกองทุนทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

ข้อแนะนำการดำเนินกิจกรรม: บันทึกที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงานทั้งภายนอกและภายในของกองทุนลงในฐานข้อมูลปัจจัยความเสี่ยงในระบบเทคโนโลยีสารสนเทศกองทุน

1) สำรวจและวิเคราะห์ข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศในอดีตตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนที่มีอยู่ในธุรกิจประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภท สำหรับการเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้

2) บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นเหตุหรืออาจสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของเทคโนโลยีสารสนเทศ ต่อการส่งมอบชุดโครงการหรือโครงการด้านเทคโนโลยีสารสนเทศ และ/หรือ ต่อการดำเนินงานและการส่งมองบริการ ด้านเทคโนโลยีสารสนเทศ จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง

3) จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณ์ต่างๆ เหล่านั้นมีร่วมกัน

4) ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยงเกิดขึ้นและลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ

5) ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะเพื่อระบุปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง

ข้อแนะนำการดำเนินกิจกรรม (3 – 7): กองทุนควร (1) สำรวจและวิเคราะห์ข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศของกองทุนในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนที่มีอยู่ในธุรกิจประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภท สำหรับการเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้ (2) บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นเหตุหรืออาจสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของเทคโนโลยีสารสนเทศ ต่อการส่งมอบชุดโครงการหรือโครงการด้านเทคโนโลยีสารสนเทศ และ/หรือ ต่อการดำเนินงานและการส่งมองบริการ ด้านเทคโนโลยีสารสนเทศ จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง (3) จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณ์ต่างๆ เหล่านั้นมีร่วมกัน (4) ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยงเกิดขึ้นและลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ (5) ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะเพื่อระบุปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง

3.2 สมมุติฐานกระบวนการบริหารความเสี่ยงกองทุนฯ เปรียบเทียบกับการบริหารความเสี่ยงของบมจ.ธนาคารกสิกรไทย ที่นำกระบวนการบริหารความเสี่ยงตามหลักการ โคบิต 5 มาดำเนินการตามกระบวนการ กิจกรรมและวัดผลความสามารถกระบวนการบริหารความเสี่ยงตามหลักการ โคบิต 5 นำมาทดสอบกับรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการ โคบิต 5 ตามตารางที่ 4.15–4.19

ตารางที่ 4.15 ผลการทดสอบกระบวนการประเมินความเสี่ยง (EDM03.01)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.01)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						สถานะความสำเร็จของกระบวนการ
ประเมินความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ		รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	
ประเมินกำรบริหารความเสี่ยง ตรวจสอบและใช้วิจารณญาณในการพิจารณาอย่าง ต่อเนื่องถึงผลกระทบของความเสี่ยงด้านการใช้ไอที ในองค์กรทั้งปัจจุบันและอนาคต พิจารณาความเหมาะสมของระดับความเสี่ยงขององค์กรที่ยอมรับ ได้และมีการระบุและบริหารจัดการความเสี่ยงที่มีต่อคุณค่าขององค์กรซึ่งเกี่ยวข้องกับการใช้ไอที	APO12.01	ประเด็นความเสี่ยงที่เกิดขึ้น	แนวทางระดับความเสี่ยงที่ยอมรับได้	APO12.03	ค่าถ่วงน้ำหนัก				
			การอนุมัติระดับความเสี่ยงที่องค์กรรับได้	APO12.03					
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ	การวัดผลกิจกรรมการบริหารความเสี่ยง	APO12.01					

ตารางที่ 4.15 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1. กำหนดระดับของความเสี่ยงด้านไอทีที่กองทุนฯ สามารถยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์	0.167	1	Passed	16.67	Partially Achieved
2.ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านไอทีที่ยอมรับได้เทียบกับระดับของความเสี่ยงและโอกาสที่กองทุนฯ ยอมรับได้	0.167	1	Passed	33.33	Partially Achieved
3.พิจารณาว่ายุทธศาสตร์ความเสี่ยงด้านไอทีสอดคล้องกับยุทธศาสตร์ความเสี่ยงระดับกองทุนฯ มากน้อยเพียงใด	0.167	1	Passed	50.00	Partially Achieved
4.ประเมินปัจจัยเสี่ยงด้านไอทีในเชิงรุกสำหรับการตัดสินใจเชิงยุทธศาสตร์ของกองทุนฯ ที่รอดำเนินการ และมั่นใจว่าการตัดสินใจของกงอทุนฯได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว	0.167	1	Passed	66.67	Largely Achieved
5.พิจารณาว่ามีการประเมินและวัดผลความเสี่ยงของการใช้ไอทีอย่างเหมาะสม ตามมาตรฐานต่างๆ ที่เกี่ยวข้องทั้งของในประเทศและสากล	0.167	1	Passed	83.33	Largely Achieved
6.ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุนฯ ในการรับความสูญเสียที่เกี่ยวข้องกับไอทีและการยอมรับความสูญเสียของผู้นำ	0.167	1	Passed	100.00	Fully Achieved
สุรปกระบวนการ 03.01					Fully Achieved

142

จากตารางที่ 4.15 ประธานคณะกรรมการ บมจ.ธนาคารกสิกรไทย ดำเนินกิจกรรมประเมินความเสี่ยงเพื่อการกำกับดูแลความเสี่ยงของ บมจ.ธนาคารกสิกร สมบูรณ์ตามหลักการโคบิต 5 (Fully Achieved)

เงื่อนไข การดำเนินกิจกรรมและวัดความสามารถในกระบวนการนี้ได้ ต้องมีข้อมูลอ้างอิงจากการดำเนินกิจกรรมในกระบวนรวบรวมข้อมูลของ บมจ.ธนาคารกสิกร ในระดับสมบูรณ์ (Fully Achieved) หมายถึง ต้องมีการให้ความเชื่อมั่นจากผู้ประเมินกระบวนการโคบิต 5 ว่า การดำเนินงานในกิจกรรมในกระบวนการประเมินความเสี่ยงครบถ้วน

ตารางที่ 4.16 ผลการทดสอบกระบวนการสั่งการบริหารความเสี่ยง (EDM03.02)

กระบวนการ ประเมิน สั่งการและติดตาม (EDM03.02)									
แนวปฏิบัติการกำกับดูแล	ข้อมูลนำเข้า		ผลผลิต						
	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
สั่งการด้านการบริหารความเสี่ยง สั่งการให้จัดทำแนวปฏิบัติสำหรับการบริหารความ เสี่ยงเพื่อให้ความเชื่อมั่นได้ในระดับหนึ่งว่าแนวปฏิบัติในการบริหารความเสี่ยงด้านไอทีมีความเหมาะสมโดยให้มั่นใจว่าความเสี่ยงด้านไอทีที่เกิดขึ้นจริงจะต้องไม่เกินระดับความเสี่ยงที่คณะกรรมการบริหารยอมรับได้	APO12.03	รวบรวมข้อมูลความเสี่ยงรวมทั้งสถานการณ์ดำเนินการบริหารความเสี่ยง	นโยบายการบริหารความเสี่ยง	APO12.01	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
			วัตถุประสงค์หลักที่จะติดตามสำหรับการบริหารความเสี่ยง	APO12.01					
	มาตรฐานอื่น	หลักการบริหารความเสี่ยงเชิงบูรณาการ (ข้อมูลความเสี่ยงและแผนการลดความเสี่ยง)	อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	APO12.01					

ตารางที่ 4.16 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.ส่งเสริมวัฒนธรรมในการตระหนักถึงความเสี่ยงด้านไอที และสร้างเสริมให้กองทุนฯ สามารถระบุถึงความเสี่ยงของไอทีในเชิงรุก ตลอดจนโอกาส และผลกระทบทางธุรกิจที่อาจเกิดขึ้น	0.167	1	Passed	16.67	Partially Achieved
2.สั่งการให้บูรณาการยุทธศาสตร์และปฏิบัติการด้านความเสี่ยงของไอที เข้าไปในการตัดสินใจด้านความเสี่ยงเชิงยุทธศาสตร์และปฏิบัติการของกองทุนฯ	0.167	1	Passed	33.33	Partially Achieved
3.สั่งการให้มีการพัฒนาแผนการติดต่อสื่อสารด้านความเสี่ยง (ที่ครอบคลุมทุกระดับของกองทุนฯ) และแผนดำเนินการสำหรับความเสี่ยง	0.167	1	Passed	50.00	Partially Achieved
4.สั่งการให้นำกลไกที่เหมาะสมมาใช้เพื่อตอบสนองความเสี่ยงที่เปลี่ยนแปลงไปได้อย่างรวดเร็ว และสามารถรายงานไปยังผู้บริหารในระดับที่ เหมาะสมได้ทันที ซึ่งสนับสนุนโดยหลักการในการแจ้งเรื่องตามระดับที่เห็นชอบร่วมกัน (รายงานอะไร เมื่อไหร่ ที่ไหน และอย่างไร)	0.167	1	Passed	66.67	Largely Achieved
5.สั่งการให้ทุกคนสามารถรายงานเรื่องความเสี่ยง โอกาส ประเด็นปัญหา และข้อกังวลได้ทุกเมื่อความเสี่ยงควรได้รับการบริหารจัดการตาม นโยบายและขั้นตอนการปฏิบัติงานที่เผยแพร่ให้ทราบทั่วกันและได้รับการแจ้งเรื่องตามระดับไปยังผู้ที่มีอำนาจในการตัดสินใจที่เกี่ยวข้อง	0.167	1	Passed	83.33	Largely Achieved
6.ระบุเป้าหมายและมาตรวัดหลักของการกำกับดูแลและกระบวนการบริหารความเสี่ยงที่จะต้องเฝ้าติดตาม ตลอดจนอนุมัติวิธีปฏิบัติ วิธีการ เทคนิค และกระบวนการต่างๆ ที่ใช้เพื่อรวบรวมและรายงานสารสนเทศด้านการวัดผล	0.167	1	Passed	100.00	Fully Achieved
สรุปกระบวนการ 03.02					Fully Achieved

จากตารางที่ 4.16 ประธานคณะกรรมการ บมจ.ธนาคารกสิกรไทย ดำเนินกิจกรรมสั่งการเพื่อกำกับดูแลความเสี่ยงขององค์กรสมบูรณ์ตามหลักการโคบิต 5 (Fully Achieved) **เงื่อนไข** การดำเนินกิจกรรมและวัดความสามารถในกระบวนการนี้ได้ ต้องมีข้อมูลอ้างอิงจากการดำเนินกิจกรรมในกระบวนการดูแลรักษาแผนภูมิความเสี่ยงของ บมจ.ธนาคารกสิกรไทย ในระดับสมบูรณ์ (Fully Achieved)

ตารางที่ 4.17 ผลการทดสอบกระบวนรวบรวมข้อมูล (APO12.01)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.01)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
รวบรวมข้อมูล				ไปสู่					
ระบุและรวบรวมข้อมูลที่เกี่ยวข้องที่เอื้อให้เกิดประสิทธิผลในการระบุ การวิเคราะห์และการรายงาน ด้านความเสี่ยงที่เกี่ยวข้องกับไอที	จากกระบวนการ	รายละเอียด	รายละเอียด	กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	การวัดผลกิจกรรมการบริหารความเสี่ยง	ข้อมูลของความเสี่ยงที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงาน	ภายใน					
	EDM03.02	*อนุมัติกระบวนการสำหรับวัดผลการบริหารความเสี่ยง	ข้อมูลเหตุการณ์ความเสี่ยงและปัจจัยที่ก่อให้เกิด	ภายใน					

ตารางที่ 4.17 (ต่อ)

	APO02.02	ช่องโหว่หรือความสามารถการบริหารความเสี่ยงปัจจุบัน	ประเด็นความเสี่ยงที่เกิดขึ้นและปัจจัยต่างๆ	EDM03.01 APO01.03 APO02.02				
	APO02.05	การประเมินความเสี่ยง						
	APO10.04	ระบุความเสี่ยงจากการส่งมอบของผู้ผลิต						
	DSS02.07	สถานะของเหตุการณ์ที่เกิดและรายงานแนวโน้มของเหตุการณ์						
กิจกรรมที่ต้องดำเนินการ								
1.กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และการวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับไอทีซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านไอที และปัจจัยเสี่ยง					0.143	1	Passed	14.29	Not Achieved

ตารางที่ 4.17 (ต่อ)

2.บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมในการปฏิบัติงานของกองทุนฯทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงด้านไอที	0.143	1	Passed	28.57	Partially Achieved
3.สำรวจและวิเคราะห์ข้อมูลความเสี่ยงด้านไอทีในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนฯที่มีอยู่จากธุรกิจในประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภทสำหรับ การเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้	0.143	1	Passed	42.86	Partially Achieved
4.บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นหรืออาจเป็นสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของไอที ต่อการส่งมอบชุดโครงการและโครงการด้านไอที และ/หรือต่อปฏิบัติการและการส่งมอบบริการด้านไอที จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง	0.143	1	Passed	57.14	Largely Achieved
5.จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณต่างๆ เหล่านั้นมีร่วมกัน	0.143	1	Passed	71.43	Largely Achieved
6.ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือที่ไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยง และลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ	0.143	1	Passed	85.71	Fully Achieved
7.ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะ เพื่อระบุประเด็นปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่ และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง	0.143	1	Passed	100.00	Fully Achieved
สรุปกระบวนการ 12.01					Fully Achieved

จากตารางที่ 4.17 กรรมการผู้จัดการ บมจ.ธนาคารกสิกรไทย มอบหมายความรับผิดชอบให้กับผู้เกี่ยวข้อง (RACI) ดำเนินกิจกรรมในกระบวนรวบรวมข้อมูลสมบูรณ์ (Fully Achieved) จากการอนุมัติการประเมินความเสี่ยงในกิจกรรมการประเมินความเสี่ยงของ บมจ.ธนาคารกสิกรไทย (EDM03.01) และ การสั่งการเพื่อกำกับดูแลความเสี่ยงของ บมจ.ธนาคารกสิกรไทย (EDM03.02) เพื่อนำมาวัดผลกิจกรรมความเสี่ยงต่างๆ

เงื่อนไข การดำเนินกิจกรรมและวัดความสามารถในกระบวนการนี้ได้ ต้องมีข้อมูลอ้างอิงจากการดำเนินกิจกรรมในกระบวนการประเมินความเสี่ยงของ บมจ.ธนาคารกสิกรไทย ในระดับสมบูรณ์ (Fully Achieved) และกิจกรรมในกระบวนการที่เกี่ยวข้องเพิ่มเติมในระดับสมบูรณ์เช่นกันของ บมจ.ธนาคารกสิกรไทย ได้แก่ (1) ประเมินสถานการณ์ปัจจุบัน (APO02.02) (2) กำหนดแผนกลยุทธ์ (APO02.05) (3) ระบุและจัดการความเสี่ยงของผู้ผลิต (APO10.04) และ (4) ตรวจสอบสถานะและผลิตรายงาน DSS02.07

ตารางที่ 4.18 ผลการทดสอบกระบวนการวิเคราะห์ความเสี่ยง (APO12.02)

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.02)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
วิเคราะห์ความเสี่ยง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ					
พัฒนาสารสนเทศที่มีประโยชน์ต่อการสนับสนุนการตัดสินใจด้านความเสี่ยง ซึ่งได้คำนึงถึงความเกี่ยวเนื่องทางธุรกิจของปัจจัยความเสี่ยงต่างๆ	DSS04.02	วิเคราะห์ผลกระทบกองทุนฯ	ขอบเขตของความพยายามการวิเคราะห์ความเสี่ยง	ภายใน	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	DSS05.01	การประเมินผลของภัยคุกคามที่เกิดขึ้น	สถานการณ์ความเสี่ยงเทคโนโลยีสารสนเทศ	ภายใน					
	ภายนอกโคบิต	คำแนะนำสำหรับภัยคุกคาม	ผลการวิเคราะห์ความเสี่ยง	EDM03.03 APO01.03 APO02.02 BAI01.10					
กิจกรรมที่ต้องดำเนินการ									
1.กำหนดความกว้างและความลึกที่เหมาะสมของความพยายามในการวิเคราะห์ความเสี่ยง โดยพิจารณาถึงทุกปัจจัยเสี่ยงและความสำคัญเชิงธุรกิจของสินทรัพย์ และกำหนดขอบเขตของการวิเคราะห์ความเสี่ยงภายหลังจากการวิเคราะห์ต้นทุน-ผลประโยชน์					0.143	1	Passed	14.29	Not Achieved

ตารางที่ 4.18 (ต่อ)

2.จัดทำสถานการณ์ต่างๆ ของความเสี่ยงด้านไอทีและปรับปรุงให้เป็นปัจจุบัน รวมถึงการรวมสถานการณ์ความเสี่ยงที่มีประเภทของภัยคุกคามในลักษณะที่ส่งทอดถึงกันและ/หรือที่เกิดขึ้นพร้อมกันไว้ด้วยกัน แล้วกำหนดความคาดหวังสำหรับกิจกรรมของการควบคุมเฉพาะด้าน ความ สามารถในการตรวจพบ และมาตรการตอบสนองอื่นๆ	0.143	1	Passed	28.57	Partially Achieved
3.ประมาณความถี่และความรุนแรงของการสูญเสียหรือประโยชน์ที่สัมพันธ์กับสถานการณ์ต่างๆ ของความเสี่ยงด้านไอที คำนึงถึงปัจจัยเสี่ยงที่เกี่ยวข้องทั้งหมด ประเมินการควบคุมเชิงปฏิบัติการที่มีอยู่และประมาณระดับความเสี่ยงที่เหลืออยู่	0.143	1	Passed	42.86	Partially Achieved
4.เปรียบเทียบความเสี่ยงที่เหลืออยู่กับความคลาดเคลื่อนของความเสี่ยงที่ยอมรับได้และระบุโอกาสเสี่ยงภัยที่อาจจำเป็นต้องตอบสนอง	0.143	1	Passed	57.14	Largely Achieved
5.วิเคราะห์ ต้นทุน-ผลประโยชน์ของทางเลือกในการตอบสนองความเสี่ยงที่อาจเป็นไปได้ เช่น การหลีกเลี่ยง ลด/บรรเทา โอน/แบ่งปัน และยอมรับและฉวย/คว้าโอกาส เป็นต้น น□าเสนอการตอบสนองความเสี่ยงที่เหมาะสมที่สุด	0.143	1	Passed	71.43	Largely Achieved
6.ระบุข้อกำหนดความต้องการในภาพรวมสำหรับโครงการหรือชุดโครงการที่นำการตอบสนองความเสี่ยงที่เลือกแล้วไปใช้ ระบุความต้องการ และความคาดหวังต่างๆ สำหรับการควบคุมหลักที่เหมาะสมเพื่อการตอบสนองโดยการบรรเทาความเสี่ยง	0.143	1	Passed	85.71	Fully Achieved
7.ตรวจสอบความสมเหตุสมผลของผลการวิเคราะห์ความเสี่ยงต่างๆ ก่อนนำมาใช้ประกอบการตัดสินใจ โดยยืนยันว่าการวิเคราะห์นั้นสอดคล้อง กับข้อกำหนดความต้องการของกองทุนฯ และทวนสอบว่าการประมาณการต่างๆ นั้นมีความเที่ยงตรงและได้พิจารณาถึงอคติที่อาจมี	0.143	1	Passed	100.00	Fully Achieved
สรุปกระบวนการ 12.02					Fully Achieved

จากตารางที่ 4.18 กรรมการผู้จัดการ บมจ.ธนาคารกสิกรไทยมอบหมายความรับผิดชอบให้กับผู้เกี่ยวข้อง(RACI)ดำเนินกิจกรรมในกระบวนการวิเคราะห์ความเสี่ยงสมบูรณ์ (Fully Achieved) จากการนำข้อมูลการวิเคราะห์ผลกระทบ (DSS04.02)การประเมินผลภัยคุกคามที่เกิดขึ้น(DSS05.01)และ การอ้างอิงเรื่องภัยคุกคามเพิ่มเติม มาวิเคราะห์ความเสี่ยงต่างๆที่เกี่ยวข้องกับ บมจ.ธนาคารกสิกรไทย

เงื่อนไข การดำเนินกิจกรรมและวัดความสามารถในกระบวนการนี้ได้ ต้องมีข้อมูลอ้างอิงจากการดำเนินงานกิจกรรมในกระบวนการที่เกี่ยวข้องของ บมจ.ธนาคารกสิกรไทย ในระดับสมบูรณ์ (Fully Achieved) ได้แก่ การวิเคราะห์ผลกระทบ (DSS04.02)การประเมินผลภัยคุกคามที่เกิดขึ้น (DSS05.01)และ การอ้างอิงเรื่องภัยคุกคามเพิ่มเติม

ตารางที่ 4.19 ผลการทดสอบกระบวนการดูแลรักษาแผนภูมิความเสี่ยง

กระบวนการ จัดวาง วางแผน วางระบบ (APO12.03)									
แนวปฏิบัติการบริหาร	ข้อมูลนำเข้า		ผลผลิต						
ดูแลรักษาแผนภูมิความเสี่ยง ดูแลรักษาบัญชีรายการความเสี่ยงและคุณลักษณะของความเสี่ยงต่างๆ ที่มี (รวมถึงความถี่ที่คาดการณ ไว้ ผลกระทบที่อาจเกิดขึ้นและการตอบสนอง) และ บัญชีรายชื่อของทรัพยากร ความสามารถ และกิจกรรมการควบคุมในปัจจุบันที่เกี่ยวข้อง	จากกระบวนการ	รายละเอียด	รายละเอียด	ไปสู่กระบวนการ	ค่าถ่วงน้ำหนัก	รายการตรวจสอบกิจกรรมตามหลักการโคบิตห้า*	สถานะตามลำดับขั้นตอน (บังคับตามลำดับต้องดำเนินการเสร็จถึงทำกิจกรรมถัดไปได้)	ร้อยละความสำเร็จของกิจกรรม	สถานะความสำเร็จของกระบวนการ
	EDM03.01	*อนุมัติระดับความเสี่ยงที่ยอมรับได้ *แนะนำแนวทางการยอมรับความเสี่ยง	ทำเอกสารสถานการณ์ความเสี่ยงตามสายงานของกองทุนฯ และหน้าที่การดำเนินงาน	ภายใน					
	APO10.04	ระบุความเสี่ยงการส่งมอบของผู้ผลิต	รวบรวมข้อมูลความเสี่ยงรวมทั้งสถานะของการดำเนินงานบริหารความเสี่ยง	EDM03.02 APO02.02					
	DSS05.01	การประเมินผลของภัยคุกคามที่อาจเกิดขึ้น							

ตารางที่ 4.19 (ต่อ)

กิจกรรมที่ต้องดำเนินการ					
1.จัดทำบัญชีรายการของกระบวนการดำเนินงานต่างๆ รวมถึงบุคลากร ระบบงาน โครงสร้างพื้นฐาน สถานที่และสิ่งอำนวยความสะดวก บันทึก ข้อมูลที่จัดทำด้วยคนที่สำคัญ ผู้ขาย และผู้ให้บริการภายนอกที่สนับสนุนกระบวนการ ตลอดจนจัดทำเอกสารการพึงพากระบวนการบริหารจัดการบริการด้านไอทีและทรัพยากรโครงสร้างพื้นฐานด้านไอทีต่างๆ	0.143	1	Passed	14.29	Not Achieved
2.กำหนดและเห็นชอบร่วมกันว่าบริการด้านไอทีและโครงสร้างพื้นฐานด้านไอทีใดที่มีความสำคัญในการสนับสนุนการปฏิบัติงานของ กระบวนการดำเนินงานต่างๆ ให้เกิดขึ้นอย่างต่อเนื่อง วิเคราะห์ระดับการพึ่งพาและระบุจุดอ่อน	0.143	1	Passed	28.57	Partially Achieved
3.รวบรวมสถานการณ์ความเสี่ยงต่างๆ ตามประเภท สายงานดำเนินการ และหน้าที่งานด้านต่างๆ	0.143	1	Passed	42.86	Partially Achieved
4.จัดเก็บสารสนเทศด้านแผนภูมิความเสี่ยงทั้งหมดและนำมารวมเป็นแผนภูมิความเสี่ยงรวมอย่างสม่ำเสมอ	0.143	1	Passed	57.14	Largely Achieved
5.กำหนดชุดของดัชนีความเสี่ยงจากข้อมูลทั้งหมดในแผนภูมิความเสี่ยง ซึ่งจะช่วยให้การระบุและเฝ้าติดตามความเสี่ยงในปัจจุบันและแนว โน้มความเสี่ยงทำได้อย่างรวดเร็ว	0.143	1	Passed	71.43	Largely Achieved
6.จัดเก็บสารสนเทศของเหตุการณ์ความเสี่ยงต่างๆ ด้านไอทีที่เกิดขึ้นจริง เพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	1	Passed	85.71	Fully Achieved
7.จัดเก็บสารสนเทศเกี่ยวกับสถานะของแผนดำเนินการด้านความเสี่ยงเพื่อนำมารวบรวมไว้ในแผนภูมิความเสี่ยงของกองทุนฯ	0.143	1	Passed	100.00	Fully Achieved
สรุปกระบวนการ 12.03					Fully Achieved

จากตารางที่ 4.19 กรรมการผู้จัดการ บมจ.ธนาคารกสิกรไทยมอบหมายความรับผิดชอบให้กับผู้เกี่ยวข้อง(RACI)ดำเนินกิจกรรมในกระบวนการเก็บรักษาข้อมูลความเสี่ยงสมบูรณ์ในระดับ 85.71 (Fully Achieved) ซึ่งสามารถเตรียมข้อมูลรองรับการดำเนินการในกระบวนการสั่งการบริหารความเสี่ยง (EDM03.02) แต่ฝ่ายบริหารต้องดำเนินการกิจกรรมการตรวจจับข้อมูลสารสนเทศในสถานะแผนการดำเนินงานบริหารความเสี่ยงเพื่อสรุปเป็นข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศของ บมจ.ธนาคารกสิกรไทย เพื่อที่จะดำเนินการส่งมอบข้อมูลดังกล่าวให้กับ ประธานคณะกรรมการบมจ.ธนาคารกสิกรไทย พิจารณาอนุมัติและสั่งการเพื่อดำเนินการบริหารความเสี่ยงของบมจ.ธนาคารกสิกรไทย ต่อไป

เงื่อนไขความสำเร็จ การดำเนินกิจกรรมและวัดความสามารถในกระบวนการนี้ ต้องมีข้อมูลอ้างอิงจากการดำเนินกิจกรรมในกระบวนการประเมินความเสี่ยงขององค์กรในระดับสมบูรณ์ (Fully Achieved) และกิจกรรมในกระบวนการที่เกี่ยวข้องเพิ่มเติม ได้แก่ การวิเคราะห์ผลกระทบ (APO10.04) การประเมินผลภัยคุกคามที่เกิดขึ้น (DSS05.01)

จากการทดสอบสามารถสรุปผลการเปรียบเทียบการดำเนินการบริหารความเสี่ยงระบบให้กู้ยืมเงินเพื่อการศึกษากับการบริหารความเสี่ยงบมจ.กสิกรไทยตามหลักการโคบิต 5 ตามตาราง 4.19

ตารางที่ 4.20ผลการทดสอบเปรียบเทียบการดำเนินการบริหารความเสี่ยงระบบกู้ยืมเงินเพื่อการศึกษากับการบริหารความเสี่ยงบมจ.กสิกรไทยตามหลักการโคบิต 5

กระบวนการความเสี่ยงโคบิต5	ผู้วิจัยประเมินกระบวนการดำเนินงานบริหารความเสี่ยงกองทุน	การดำเนินงานบริหารความเสี่ยงของบมจ.ธนาคารกสิกรไทย	หมายเหตุ
EDM03.01	X[1]	✓[2]	ที่ประชุมผู้คณะกรรมการบมจ.ธนาคารกสิกรไทยมีมติเห็นชอบการประเมินความเสี่ยงเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินธุรกิจของธนาคาร
EDM03.02	X	✓	ที่ประชุมผู้

ตารางที่ 4.20 (ต่อ)

กระบวนการความเสี่ยงโคบิต 5	ผู้วิจัยประเมินกระบวนการดำเนินงานบริหารความเสี่ยงกองทุน	การดำเนินงานบริหารความเสี่ยงของ บมจ.ธนาคารกสิกรไทย	หมายเหตุ
			คณะกรรมการ บมจ.ธนาคารกสิกรไทยมีมติเห็นชอบการประเมินความเสี่ยงเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินธุรกิจของธนาคาร
EDM03.03	X	X	พิจารณาดำเนินการให้บรรลุผลสำเร็จ
APO12.01	X	✓	ฝ่ายบริหารมอบหมายให้ทุกฝ่ายงานเก็บรักษาข้อมูลความเสี่ยงทั้งหมดตามกิจกรรมโคบิต 5
APO12.02	X	✓	ฝ่ายบริหารมอบหมายให้ทุกฝ่ายงานเก็บรักษาข้อมูลความเสี่ยงทั้งหมดตามกิจกรรมโคบิต 5
APO12.03	X	✓	ฝ่ายบริหารมอบหมายให้ทุกฝ่ายงานเก็บรักษาข้อมูลความเสี่ยงทั้งหมดตามกิจกรรมโคบิต 5
APO12.04	X	X	ฝ่ายบริหารมอบให้ผู้ปฏิบัติงานมานำเสนอแนวทางและประชุมข้อความร่วมมือจากทุกฝ่ายงานเพื่อบรรลุ
APO12.05	X	X	
APO12.06	X	X	

ตารางที่ 4.20 (ต่อ)

กระบวนการความเสี่ยงโคบิต 5	ผู้วิจัยประเมินกระบวนการดำเนินงานบริหารความเสี่ยงกองทุน	การดำเนินงานบริหารความเสี่ยงของ บมจ.ธนาคารกสิกรไทย	หมายเหตุ
			ความสำเร็จของกระบวนการบริหารความเสี่ยงที่เหลือภายในระยะเวลา 1- 3 ปีเพื่อนำเสนอคณะกรรมการในการอนุมัติแผนการดำเนินการ
สรุปผลความสำเร็จกระบวนการบริหารความเสี่ยง	**ไม่ผ่าน**	**ผ่านกระบวนการ EDM03.01-03.02 และ APO12.01-12.03**	มีแนวโน้มที่จะผ่าน

หมายเหตุ [1] เครื่องหมาย X ไม่ได้ดำเนินกิจกรรมตามหลักการบริหารความเสี่ยงโคบิต 5 ที่กล่าวไว้ในระเบียบวิธีวิจัย

[2] ดำเนินกิจกรรมตามหลักการบริหารความเสี่ยงตามหลักการโคบิต 5 ที่กล่าวไว้ในระเบียบวิธีวิจัย

จากตารางที่ 4.20 แสดงผลการดำเนินงานบริหารความเสี่ยงตามหลักการโคบิต 5 ของระบบให้กู้ยืมเงินเพื่อการศึกษาของกองทุนเปรียบกับการดำเนินงานบริหารความเสี่ยงตามหลักการโคบิต 5 (ไม่ผ่าน) ของ บมจ.ธนาคารกสิกรไทย (ผ่านเฉพาะกระบวนการกำกับดูแลความเสี่ยง EDM03.01 - 03.02 และกระบวนการบริหารความเสี่ยง APO12.01 – 12.03)กระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ของ บมจ.ธนาคารกสิกรไทย จะสมบูรณ์ครบทั้ง 9 กระบวนการจะต้องดำเนินการในเรื่อง การมอบหมายการดำเนินจาก ฝ่ายบริหารให้ผู้ปฏิบัติงานมานำเสนอแนวทางและวิธีการตามกิจกรรมของกระบวนการ EDM03.03 APO12.04 APO12.05 และ APO12.06 เพื่อประชุมข้อความร่วมมือจากทุกฝ่ายในการกำหนดแผนการดำเนินงานเพื่อบรรลุความสำเร็จของกระบวนการบริหารความเสี่ยงที่เหลือภายในระยะเวลา 1- 3 ปีและนำเสนอคณะกรรมการ บมจ.ธนาคารกสิกรไทย เพื่ออนุมัติแผนการดำเนินการต่อไป

บทที่ 5
สรุปการวิจัย อภิปรายผล และข้อเสนอแนะ

งานวิจัยนี้นำเสนอบทสรุปการวิจัย แบ่งเป็น (1) สรุปการวิจัย ประกอบด้วย (1.1) วัตถุประสงค์การวิจัย (1.2) วิธีการดำเนินวิจัย และ (1.3) ผลการวิจัยตอบตามวัตถุประสงค์ (2) อภิปรายผล (3) ปัญหาและข้อเสนอแนะ ประกอบด้วย (3.1) ปรับปรุงกระบวนการกำกับดูแลความเสี่ยงของกองทุนและปรับปรุงกระบวนการบริหารความเสี่ยงของกองทุน (4) ข้อเสนอแนะในการทำวิจัย ประกอบด้วย (4.1) ข้อเสนอแนะในการนำวิจัยไปใช้ และ (4.2) ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไปดังนี้

1. สรุปการวิจัย

1.1 วัตถุประสงค์การวิจัย

1.1.1 เพื่อพัฒนาแบบจำลองสถานการณ์ความเสี่ยงของกองทุนเชื่องโยงเข้ากับกระบวนการจัดการความเสี่ยงโคบิต 5

1.1.2 เพื่อพัฒนาระบบสารสนเทศของกองทุนตามกระบวนการจัดการความเสี่ยงโคบิต 5

1.1.3 เพื่อทดสอบแบบจำลองสถานการณ์ความเสี่ยงและประเมินผลสถานการณ์ความเสี่ยง

1.2 วิธีการดำเนินวิจัย

1.2.1 ศึกษาความเสี่ยงกองทุน ระบบ (e – Studentloan) ศึกษากระบวนการดำเนินงานของระบบ e – Studentloan จากคู่มือผู้ปฏิบัติงาน กองทุนเงินให้กู้ยืมเพื่อการศึกษา ในการระบุความเสี่ยงจากกระบวนการดำเนินงานของระบบ (e – Studentloan)

1.2.2 วิเคราะห์สถานการณ์ความเสี่ยงกองทุน (ระบบ e – Studentloan)

1.2.3 ศึกษาและวิเคราะห์ประมาณการสถานการณ์ความเสี่ยงที่คาดการไว้ในช่วงระยะเวลาที่กำหนด ตั้งสมมติฐานความเปลี่ยนแปลงที่อาจเกิดขึ้นในกระบวนการดำเนินงานของระบบ e – Studentloan

1.2.4 ออกแบบสถานการณ์ความเสี่ยงกองทุนและสถานการณ์อื่นที่เกี่ยวข้องสมมติสถานการณ์ความเสี่ยงกองทุน (e - Studentloan) ตามสภาพแวดล้อมที่เกิดขึ้น จากกระบวนการให้กู้ยืม ตามคู่มือ ผู้ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา

1.2.5 พัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5 COBIT 5 for risk model ของกองทุน (e - Studentloan) กระบวนการบริหารความเสี่ยงโคบิต 5 (APO12 Managing Risk) ประกอบด้วย 6 กระบวนการ ดังนี้

1) เก็บข้อมูลความเสี่ยง (APO12.01 Collect Data) ระบุและเก็บข้อมูลที่เกี่ยวข้องเพื่อระบุความเสี่ยงทางเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

2) วิเคราะห์ความเสี่ยง (APO12.02 Analyze risk) วิเคราะห์ข้อมูลที่เป็นประโยชน์เพื่อสนับสนุนในการตัดสินใจต่อปัจจัยความเสี่ยงที่เกี่ยวข้องในธุรกิจ

3) บันทึกข้อมูลความเสี่ยง (APO12.03 Maintain a risk profile) เก็บรักษาคลังข้อมูลความเสี่ยงและคุณลักษณะของความเสี่ยง (รวมทั้งความถี่ที่ขาดหวัง สิ่งที่อาจเกิดขึ้นของผลกระทบและการบริหารความเสี่ยง)

4) รายงานสถานการณ์ความเสี่ยง (APO12.04 Articulate risk) เตรียมเปิดเผยสถานะข้อมูลปัจจุบันของเทคโนโลยีสานสนเทศที่เกี่ยวข้องและแจ้งข้อมูลต่างๆ ตามระยะที่เหมาะสมต่อความต้องการของผู้มีส่วนได้เสีย

5) กำหนดแนวทางการบริหารความเสี่ยง (APO12.05 Define a risk management action portfolio) บริหารลดระดับความเสี่ยงตามแนวทางการบริหารความเสี่ยงที่กำหนด

6) การบริหารความเสี่ยง (APO12.06 Respond to risk) บริหารความเสี่ยงในระยะเวลาที่เหมาะสมตามการวัดผลอย่างมีประสิทธิภาพโดยจากัดขอบเขตต่อความสูญเสียจากเหตุการณ์ทางเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

7) กระบวนการบริหารความเสี่ยง กำหนดผู้มีความรับผิดชอบของกระบวนการตามตาราง RACI

1.2.6 พัฒนารูปแบบการวัดประสิทธิภาพและประสิทธิผลกระบวนการบริหารความเสี่ยงโคบิต 5 (COBIT 5 Process Capability Model) ประกอบด้วยระดับการวัดความสำเร็จ 6 ระดับ

1) ความสำเร็จของกระบวนการระดับ 0 คือ กระบวนการไม่สมบูรณ์ (0Incomplete Process): กระบวนการไม่ได้ดำเนินการหรือไม่บรรลุผลตามวัตถุประสงค์ที่กำหนด

2) ความสำเร็จของกระบวนการระดับ 1 คือ กระบวนการได้รับ การดำเนินการ (1 Performed Process) ต้องครอบคลุม 1 คุณลักษณะ (one attribute): มีการดำเนินกระบวนการสำเร็จตามวัตถุประสงค์ (PA 1.1)

3) ความสำเร็จของกระบวนการระดับ 2 คือ กระบวนการได้รับ การบริหาร (2 Managed Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute): กระบวนการในระดับที่ 1 (1 Performed

Process) (1) ได้รับการดาเนินการบริหารตามรูปแบบ (มีการวางแผน ติดตาม และปรับปรุง) (PA 2.1) และ (2) กระบวนการมีการดำเนินการควบคุม และเก็บรักษาอย่างเหมาะสม (PA 2.2)

4) ความสำเร็จของกระบวนการระดับ 3 คือ กระบวนการได้รับการยอมรับว่ามีจริง (3 Established Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute): กระบวนการในระดับที่ 2 (2 Managed Process) (1) มีการดำเนินการโดยกำหนดกระบวนการ (PA 3.1) (2) นำกระบวนการไปใช้งาน โดยกระบวนการสามารถบรรลุผลสำเร็จและได้ผลลัพธ์ (PA 3.2)

5) ความสำเร็จของกระบวนการระดับ 4 คือ กระบวนการสามารถพยากรณ์ได้ (4 Predictable Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute): กระบวนการในระดับที่ 3 (3 Established Process) (1) กระบวนการมีกำหนดมาตราวัดผลลัพธ์ของกระบวนการ (PA 4.1) (2) กระบวนการมีการควบคุม (PA 4.2)

6) ความสำเร็จของกระบวนการระดับ 5 คือ กระบวนการให้ผลลัพธ์และมีคุณประโยชน์สูงสุด (5 Optmising Process) ต้องครอบคลุม 2 คุณลักษณะ (two attribute): กระบวนการในระดับที่ 4 (1) มีการพัฒนา คิดค้นนวัตกรรมขึ้นอย่างต่อเนื่อง (PA 5.1) (2) กระบวนการที่กำหนดให้ประโยชน์และคุณค่าสูงสุดต่อองค์กร (PA 5.2)

การวัดผลความสำเร็จของการดำเนินการในแต่ละกระบวนการ

7) N (Not achieved) คือ มีเพียงเล็กน้อยหรือไม่มีหลักฐานของการบรรลุผลความสำเร็จตามที่ได้กำหนดไว้ (ค่าความสำเร็จร้อยละ 0– 15)

8) P (Partially achieved) คือ มีหลักฐานบ้างอย่างของวิธีการที่จะดำเนินการและการบรรลุผลสำเร็จบางอย่างของการกำหนดคุณลักษณะในการประเมินกระบวนการ บางส่วนของการบรรลุผลสำเร็จของคุณลักษณะที่ยังขาดการไม่ได้ (ค่าความสำเร็จร้อยละ 15– 50)

9) L (Largely achieved) คือ มีหลักฐานวิธีการดำเนินการอย่างเป็นระบบและมีนัยสำคัญที่จะบรรลุผลสำเร็จของการกำหนดคุณลักษณะในการประเมินกระบวนการ แต่ยังมีข้อบกพร่องเกิดขึ้นอยู่ในการประเมินกระบวนการ (ค่าความสำเร็จร้อยละ 50– 85)

10) F (Fully achieved) คือ มีหลักฐานวิธีการดำเนินอย่างเป็นระบบสมบูรณ์และมีการบรรลุผลสำเร็จสมบูรณ์ของการกำหนดคุณลักษณะในการประเมินกระบวนการ ไม่พบข้อบกพร่องที่มีนัยสำคัญที่เกี่ยวข้องเหลืออยู่ในคุณลักษณะในการประเมินกระบวนการ (ค่าความสำเร็จ ร้อยละ 85– 100)

1.2.7 ทดสอบรูปแบบระบบกระบวนบริหารความเสี่ยงตามกรอบโคบิต 5

1.2.8 ประเมินผล การทดสอบรูปแบบระบบตรวจสอบและวัดผลประสิทธิภาพและประสิทธิผลกระบวนบริหารความเสี่ยงตามหลักการโคบิต 5

1.3 ผลการวิจัย ตอบตามวัตถุประสงค์

1.3.1 แบบจำลองสถานการณ์ความเสี่ยงของกองทุน (e - Studentloan)

1) ปัจจัยเสี่ยงที่มีผลกระทบต่อ “กระบวนการทางานและการพัฒนาระบบอาจเกิดความล่าช้าไม่สามารถรองรับ พรบ ใหม่ได้ทันเวลา” คือ ทรัพย์สิน / ทรัพยากร กระบวนการ ผู้ดำเนินการภายใน และ เวลา ช่วงเวลา ผลลัพธ์ ของแบบจำลองสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 คือไม่สามารถพัฒนาระบบได้ทันกาล (Ref. (0201) และ (0203))

2) ออกแบบสถานการณ์ความเสี่ยงของกองทุนจากปัจจัยเสี่ยงที่กำหนดเพื่อเลือกและกำหนดสถานการณ์ความเสี่ยงจากประเด็นความเสี่ยงและออกแบบสถานการณ์ความเสี่ยงสารสนเทศกองทุน (e - Studentloan) ตามสภาพแวดล้อมจริงของกองทุน ซึ่งสถานการณ์ความเสี่ยงที่ผู้วิจัยเลือกมาตรงกับสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 อ้างอิงที่ 0201 และ 0203 ผลของการจำลองสถานการณ์ความเสี่ยงสามารถกำหนดประเภทความเสี่ยงสารสนเทศและระดับความรุนแรงของความเสี่ยง เพื่อนำไประบุและลงทะเบียนความเสี่ยงกองทุน และจัดเก็บเป็นเอกสารฐานข้อมูล ต่อไป

3) นำสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 ที่เลือกมากำหนดรายละเอียดความเสี่ยงเพื่อลงทะเบียนลักษณะของความเสี่ยงและเก็บบันทึกข้อมูลความเสี่ยงและนำมาเชื่อมโยงเข้ากับกระบวนการบริหารความเสี่ยงโคบิต 5 (EDM03 และ APO12) เพื่อดำเนินการตามกิจกรรมตามหลักการการบริหารความเสี่ยงโคบิต 5 ในแต่ละกระบวนการ

1.3.2 พัฒนาระบบสารสนเทศของกองทุนตามกระบวนการจัดการความเสี่ยงโคบิต 5 ตามสถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

ผู้วิจัยได้นำแนวคิดจากสถาปัตยกรรมมาสร้างรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 เพื่อทำการทดสอบความมีอยู่จริงของกระบวนการบริหารความเสี่ยงกองทุนในปัจจุบันกับรูปแบบระบบตรวจสอบและวัดความสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ผลลัพธ์การทดสอบ คือ กระบวนการบริหารความเสี่ยงกองทุน ไม่สำเร็จตามหลักการโคบิต 5 เนื่องจากขาดกิจกรรมของกระบวนการการกำกับดูความเสี่ยง (EDM03.01) และกิจกรรมของกระบวนการบริหารความเสี่ยง (APO12.01) ทั้งหมด

1.3.3 พัฒนาระบบสารสนเทศของกองทุนตามกระบวนการจัดการความเสี่ยงโคบิต 5 ตามสถาปัตยกรรมรูปแบบระบบตรวจสอบและวัดสามารถของกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5

2. อภิปรายผล

ผู้วิจัย ได้นำประเด็นที่ค้นพบที่น่าสนใจมาอภิปรายตามวัตถุประสงค์ ดังนี้

ระบบเงินให้กู้ยืมเพื่อการศึกษาของกองทุนฯ เปิดให้บริการกู้ยืมเมื่อปีงบประมาณ 2551 เพื่อแก้ปัญหาการกู้ยืม ในเรื่อง ความล่าช้า การคัดกรองคุณสมบัติ ข้อมูลของผู้กู้ยืม เป็นต้น รวมทั้งขาดประสิทธิภาพและประสิทธิผลในการโอนเงินและการรับชำระหนี้ ซึ่งกองทุนฯ จัดจ้างผู้บริหารจัดการเงินให้กู้ยืม เป็นผู้รับผิดชอบดำเนินการ จึงเป็นสาเหตุทำให้กองทุนฯ ไม่สามารถบริหารการดำเนินงานได้ทันกาล (ปัจจุบัน คือ บมจ.ธนาคารกรุงไทยและธนาคารอิสลามแห่งประเทศไทย) จนถึงปัจจุบัน กองทุนฯ ยังคงประสบปัญหาดังกล่าวดังเช่นเดียวกับการดำเนินงานก่อนมีระบบเงินให้กู้ยืม สอดคล้องกับการศึกษาของ Dr.Amara. (2016), Sakulrat (2011) สุประพล พาพิโพธิ์ (2557) บุญรอด เสกสรรค์ (2553) Ziderman, Adrian (2003) อมรา ตันประวัติ (2544) และ สมชัย ฤชุพันธ์ (2548) ในประเด็นเรื่อง กองทุนเงินให้กู้ยืมเพื่อการศึกษา ขาดประสิทธิภาพและประสิทธิผลในกระบวนการให้กู้ยืม ตั้งแต่ระดับนโยบาย วัตถุประสงค์ เป้าหมายการดำเนินงานของกองทุนฯ ไม่ชัดเจน กระบวนการให้กู้ยืมขาดความรัดกุม กระบวนการรับชำระหนี้ไม่สามารถทวงถามได้ทันทีเนื่องจากข้อมูลผู้กู้ยืมอยู่ที่ผู้บริหารจัดการเงินให้กู้ยืม การติดตามกระบวนการให้กู้ยืมไม่ต่อเนื่อง รวมทั้งความพึงพอใจในการให้บริการการกู้ยืมของกองทุนฯ ยังไม่เป็นที่ประจักษ์ (อยู่ในระดับพอใช้)

ดังนั้นการปรับปรุงคุณภาพระบบเงินให้กู้ยืมเพื่อการศึกษาจึงมีความสำคัญสำหรับกองทุนฯ ในการพัฒนากระบวนการให้กู้ยืมให้มีประสิทธิภาพ เพื่อจัดวาง นโยบาย วัตถุประสงค์ เป้าหมายการดำเนินงานและเทคโนโลยีสารสนเทศให้สอดคล้องกัน กองทุนฯ ควรนำแนวทางตามหลักการโคบิต 5 จากการทดสอบตามตารางที่ 2 มาปรับปรุงและพัฒนาระบบเงินให้กู้ยืมเพื่อการศึกษาเพื่อเอื้อประโยชน์ให้กับกองทุนฯ ในการเพิ่มและปรับปรุงประสิทธิภาพและประสิทธิผลให้กับการกำหนดนโยบาย วัตถุประสงค์ และกระบวนการหลักของกองทุนฯ สิ่งสำคัญคือกระบวนการบริหารความเสี่ยงของกองทุนฯ ที่ไม่เป็นไปตามหลักการโคบิต 5 เป็นอีกปัจจัยหลักสำหรับกองทุนฯ ในการปรับปรุงและพัฒนากระบวนการบริหารความเสี่ยง จากปัจจัยต่างๆ เหตุการณ์ ประสบการณ์ย้อนหลัง หรือข้อมูลจากกองทุนฯ /ธุรกิจที่ใกล้เคียงกับกองทุนฯ ทำให้เกิดความไม่มีประสิทธิภาพและประสิทธิผล ตามที่ผู้วิจัยและความสอดคล้องจากการศึกษาของผู้วิจัยต่างๆ ที่กล่าวมาข้างต้น เพื่อนำมากำหนดปัจจัย เหตุการณ์หรือประสบการณ์ความเสี่ยงเพื่อบริหารความเสี่ยงการดำเนินงานด้วยเทคโนโลยีสารสนเทศ สอดคล้องกับ Karel (2013), Dwi Rosa, Harlili, Afriyan (2014), Bo˘stjan (2008) และ Kristen (2013) ในประเด็นเรื่องการระบุ ประเมินและลงทะเบียนความเสี่ยงทางเทคโนโลยีสารสนเทศสามารถสร้างการเชื่อมโยงเป้าหมายของกองทุนฯ กับเป้าหมายด้านเทคโนโลยีสารสนเทศให้บรรลุผลสำเร็จได้ตามที่กำหนด อีกทั้งกองทุนฯ

ยังสามารถ วางแผนโครงการต่างๆ ได้ครอบคลุมทุกส่วนที่ต้องการแก้ไขและพัฒนา เป็นผลตามความต้องการของกองทุนฯ สอดคล้องกับการศึกษาของ Maher (2012) ในเรื่องการกำหนดและวางแผนโครงการและความเสี่ยงกองทุนฯ ในเรื่องความเกี่ยวข้องกับความรับผิดทางกฎหมายของกองทุนฯ สอดคล้องกับการศึกษาของ Matthew (2008) ในเรื่องการกำหนดความเสี่ยงตามข้อบังคับกฎหมาย การดำเนินงานบริหารความเสี่ยงตามข้อเสนอแนะของผู้วิจัยสามารถสนับสนุน ปรับปรุงและพัฒนาระบบเงินให้กู้ยืมของกองทุนฯ ปรับเปลี่ยนเป็นรูปแบบเชิงบูรณาการ (แบ่งแยกการกำกับดูแลออกจากการบริหาร) สอดคล้องกับการศึกษาของ Akbar (2014) ในเรื่องการแบ่งแยกการกำกับดูออกจากการบริหาร ส่งผลให้กระบวนการบริหารความเสี่ยงเกิดประโยชน์ทั่วทั้งกองทุนฯ สอดคล้องกับการศึกษาของ Madhav (2014) กล่าวถึงประโยชน์ในการนำหลักการโคบิต 5 มาปรับใช้กับองค์กรในเรื่องเพิ่มประสิทธิภาพและประสิทธิผลในทุกด้านในกับองค์กร และสามารถกำหนดทิศทาง ออกแบบสถานการณ์ความเสี่ยงในการบริหารตามความต้องการของกองทุนฯ สอดคล้องกับการศึกษาของ Onyeka, Shaun, & Sergey (2014) และ Urs (2011) ในเรื่องความเชื่อมโยงในการกำหนดกลยุทธ์ขับเคลื่อนเทคโนโลยีสารสนเทศขององค์กรไปในทิศทางเดียวกัน รวมทั้งนำเสนอแนวทางการบริหารความเสี่ยงตามหลักการโคบิต 5 สำหรับกองทุนฯ สอดคล้องกับการศึกษาของ Walid& Basil (2015) ในประเด็นเรื่องการเพิ่มประสิทธิภาพและประสิทธิภาพตามหลักการบริหารความเสี่ยงโคบิต 5

3. ปัญหาและข้อเสนอแนะเพื่อบรรลุความสำเร็จของกระบวนการบริหารความเสี่ยงกองทุนตามหลักการโคบิต 5

จากกระบวนการดำเนินงานของกองทุนฯ เงินให้กู้ยืมเพื่อการศึกษายังขาดบุคลากรที่มีความเชี่ยวชาญ การสื่อสารระหว่างฝ่ายงาน ในการดำเนินงานการบริหารความเสี่ยง จึงเป็นสาเหตุหลักทำให้การดำเนินงานด้านการบริหารความเสี่ยงยังขาดประสิทธิภาพส่งผลให้กองทุนฯ ไม่สามารถกำหนด วิเคราะห์ ประเมินและบริหารความเสี่ยงให้เกิดผลประโยชน์สูงสุดกับกองทุนฯ จากการทดสอบกระบวนการบริหารความเสี่ยงของกองทุนฯ กับหลักการโคบิต 5 แสดงให้เห็นว่ากองทุนฯ ยังขาดกระบวนการที่เป็นมาตรฐานเพื่อรองรับการดำเนินงานบริหารความเสี่ยง

ข้อเสนอแนะ กองทุนฯ ควรศึกษาแนวทางจากงานวิจัยนี้ เพื่อปรับแนวทางการบริหารความเสี่ยงกองทุนฯ และพัฒนาระบบเงินให้กู้ยืมเพื่อการศึกษาต่อไป รวมทั้งควรทำศึกษากองทุนฯ จากหน่วยงานที่มีลักษณะกิจกรรมการดำเนินงานที่ใกล้เคียงกับกองทุนฯ ตามหลักการโคบิต 5 มาปรับใช้กับกองทุนฯ เพื่อนำแนวปฏิบัติที่ดี (Best practices) มาปรับใช้กับกองทุนฯ

ดังนั้นกองทุนฯ ควรนำผลจากงานวิจัยนี้เป็นแนวทางในการสร้างสถานการณ์ความเสี่ยงที่เกิดขึ้นจริงกับกองทุนฯ ได้ตามแนวทางรายละเอียดกระบวนการและกิจกรรมการบริหารความเสี่ยงกองทุนฯ ควรกำหนดกิจกรรมต่างๆ ตามหลักการโคบิต 5 กำหนดเพื่อบรรลุผลสำเร็จในกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 สามารถแบ่งแยกเป็นสองส่วน ประกอบด้วย เพิ่มการปรับปรุงกระบวนการกำกับดูแลและปรับปรุงกระบวนการบริหารความเสี่ยง ดังนี้

3.1 ปรับปรุงกระบวนการกำกับดูแลความเสี่ยงของกองทุน ในกิจกรรมต่างๆ ดังนี้

3.1.1 กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กองทุนสามารถรับได้เพื่อให้บรรลุวัตถุประสงค์

3.1.2 ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่องยอมรับเทียบกับระดับความเสี่ยงและโอกาสที่กองทุนยอมรับได้

3.1.3 พิจารณาว่ายุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสอดคล้องกับยุทธศาสตร์บริหารความเสี่ยงของกองทุนมากน้อยเพียงใด

3.1.4 ประเมินปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศในเชิงรุกสำหรับการตัดสินเชิงยุทธศาสตร์ที่รอดำเนินการ และ มั่นใจว่าการตัดสินใจของกองทุนได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว

3.1.5 พิจารณาว่ามีการประเมินความเสี่ยงและวัดผลความเสี่ยงของการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมตามมาตรฐานต่างๆ ที่เกี่ยวข้อง ทั้งของในประเทศและสากล

3.1.6 ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุน ในการรับความสูญเสียที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการยอมรับความสูญเสียของผู้นำ

ข้อแนะนำการดำเนินกิจกรรม (3.1.1 – 3.1.6): กองทุนควรกำหนด (1) ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กองทุนสามารถรับได้ เพื่อให้บรรลุวัตถุประสงค์ (2) ประเมินและอนุมัติค่าที่นำเสนอสำหรับช่วงความเบี่ยงเบนของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่องยอมรับเทียบกับระดับความเสี่ยงและโอกาสที่กองทุนยอมรับได้ (3) พิจารณาว่ายุทธศาสตร์ด้านเทคโนโลยีสารสนเทศสอดคล้องกับยุทธศาสตร์บริหารความเสี่ยงของกองทุนมากน้อยเพียงใด (4) ประเมินปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศในเชิงรุกสำหรับการตัดสินเชิงยุทธศาสตร์ที่รอดำเนินการ และมั่นใจว่าการตัดสินใจของกองทุนได้คำนึงถึงความเสี่ยงดังกล่าวแล้ว (5) พิจารณาว่ามีการประเมินความเสี่ยงและวัดผลความเสี่ยงของการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมตามมาตรฐานต่างๆ ที่เกี่ยวข้อง ทั้งของในประเทศและสากล (6) ประเมินกิจกรรมการบริหารความเสี่ยงเพื่อให้มั่นใจว่าสอดคล้องกับความสามารถของกองทุน ในการรับความสูญเสียที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการยอมรับความสูญเสียของผู้นำ

3.2 ปรับปรุงกระบวนการบริหารความเสี่ยงของกองทุน ในกิจกรรมต่างๆ ดังนี้

3.2.1 กำหนดและดูแลวิธีการในการเก็บรวบรวม การจำแนกประเภท และวิเคราะห์ข้อมูลความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศซึ่งเหมาะสมกับความหลากหลายในประเภทของเหตุการณ์ หมวดหมู่ของความเสี่ยงด้านเทคโนโลยีสารสนเทศ และปัจจัยเสี่ยง

ข้อแนะนำการดำเนินกิจกรรม: กำหนดและดูแลวิธีการเก็บรวบรวม จำแนกประเภท วิเคราะห์ข้อมูล จัดหมวดหมู่ ของข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศและปัจจัยเสี่ยงของกองทุน เช่น สร้างฐานข้อมูลความเสี่ยง ฐานข้อมูลปัจจัยเสี่ยงทุกด้านของกองทุน และฐานข้อมูลประเภทของเหตุการณ์ต่างๆ เป็นต้น

3.2.2 บันทึกข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงานของกองทุนทั้งภายนอกและภายในซึ่งมีบทบาทสำคัญต่อการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

ข้อแนะนำการดำเนินกิจกรรม: บันทึกที่เกี่ยวข้องกับสภาพแวดล้อมการดำเนินงานทั้งภายนอกและภายในของกองทุนลงในฐานข้อมูลปัจจัยความเสี่ยงในระบบเทคโนโลยีสารสนเทศกองทุน

3.2.3 สำรวจและวิเคราะห์ข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศในอดีตตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนที่มีอยู่ในธุรกิจประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภท สำหรับการเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้

3.2.4 บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นเหตุหรืออาจสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของเทคโนโลยีสารสนเทศ ต่อการส่งมอบชุดโครงการหรือโครงการด้านเทคโนโลยีสารสนเทศ และ/หรือ ต่อการดำเนินงานและการส่งมองบริการ ด้านเทคโนโลยีสารสนเทศ จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง

3.2.5 จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณ์ต่างๆ เหล่านั้นมีร่วมกัน

3.2.6 ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยงเกิดขึ้นและลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ

3.2.7 ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะเพื่อระบุปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง

ข้อแนะนำการดำเนินกิจกรรม (3.2.3 – 3.2.7): กองทุนควร (1) สำรวจและวิเคราะห์ข้อมูลความเสี่ยงเทคโนโลยีสารสนเทศของกองทุนในอดีต ตลอดจนประสบการณ์ความสูญเสียที่ได้จากข้อมูลและแนวโน้มภายนอกกองทุนที่มีอยู่ในธุรกิจประเภทเดียวกันผ่านปูมบันทึกเหตุการณ์ ของธุรกิจแต่ละประเภท จากฐานข้อมูล และจากข้อตกลงในธุรกิจแต่ละประเภท สำหรับการเปิดเผยข้อมูลเหตุการณ์ที่สามารถแบ่งปันกันได้ (2) บันทึกข้อมูลเหตุการณ์ความเสี่ยงต่างๆ ที่เป็นเหตุหรืออาจสาเหตุของผลกระทบที่มีต่อประโยชน์และการเอื้อคุณค่าของเทคโนโลยีสารสนเทศ ต่อการส่งมอบชุดโครงการหรือโครงการด้านเทคโนโลยีสารสนเทศ และ/หรือ ต่อการดำเนินงานและการส่งมองบริการ ด้านเทคโนโลยีสารสนเทศ จัดเก็บข้อมูลที่เกี่ยวเนื่องจากประเด็นปัญหา เหตุการณ์ผิดปกติ ปัญหา และการสืบสวนต่างๆ ที่เกี่ยวข้อง (3) จัดระเบียบข้อมูลที่รวบรวมมาและระบุถึงปัจจัยที่เป็นสาเหตุสำหรับเหตุการณ์ต่างๆ ที่มีความคล้ายคลึงกัน ระบุถึงปัจจัยสาเหตุที่เหตุการณ์ต่างๆ เหล่านั้นมีร่วมกัน (4) ระบุสภาวการณ์เฉพาะที่เกิดขึ้นหรือไม่เกิดขึ้นเมื่อมีเหตุการณ์ความเสี่ยงเกิดขึ้นและลักษณะที่สภาวการณ์ดังกล่าวมีผลต่อความถี่และความรุนแรงของความสูญเสียของเหตุการณ์นั้นๆ (5) ดำเนินการวิเคราะห์เหตุการณ์และปัจจัยเสี่ยงเป็นระยะเพื่อระบุปัญหาของความเสี่ยงใหม่ๆ หรือที่เกิดขึ้นใหม่และเพื่อให้เกิดความเข้าใจในปัจจัยเสี่ยงภายในและภายนอกที่เกี่ยวข้อง

ทั้งนี้กองทุนฯ ควรพิจารณากิจกรรมและกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ให้ครบถ้วนตามขั้นตอนข้อ 1 และ 2 ในระเบียบวิธีการวิจัยเพื่อปรับปรุงและเพิ่มประสิทธิภาพกระบวนการบริหารความเสี่ยงให้เกิดประโยชน์สูงสุดสำหรับกองทุนฯ

4. ข้อเสนอแนะในการทำวิจัย

4.1 ข้อเสนอแนะในการนำวิจัยไปใช้

4.1.1 ผลการวิจัยพบว่า การสร้างสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 เป็นแนวทางที่ดีสำหรับกองทุน ดังนั้นกองทุนควรนำแนวทางที่ได้นำเสนอในงานวิจัยนี้ไปดำเนินการประเมินสถานการณ์ความเสี่ยงที่มีอยู่เป็นรายไตรมาส หรือ ทุกครึ่งปีงบประมาณ หรือก่อนสิ้นปีงบประมาณ ขึ้นอยู่กับการวางแผนประจำปีของแต่ละงบประมาณของกองทุน เพื่อปรับเปลี่ยนตามปัจจัยเสี่ยงที่เกิดขึ้นและเลือกสถานการณ์ความเสี่ยงตามหลักการโคบิต 5 ปรับให้เข้าปัจจัยเสี่ยงนั้นๆ เพื่อกำหนด วิเคราะห์และประเมินความเสี่ยงได้ทันกาล

4.1.2 ผลการวิจัยพบว่า การสร้างรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5สามารถตรวจสอบกิจกรรม แสดงสถานะของ

ขั้นตอนแต่ละกระบวนการว่าอยู่ที่ขั้นตอนใดและแสดงผลลัพธ์ความสามารถของกระบวนการตามหลักการโคบิต 5 จากการพัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 เป็นแนวทางสำหรับกองทุนในการกำหนดรูปแบบการบริหารความเสี่ยงกองทุนตามคำอธิบายรายละเอียดในแต่ละกิจกรรมการกำกับดูแลและการบริหารความเสี่ยงตามหลักการโคบิต 5 จึงสามารถนาไปใช้ได้กับทุกองค์กรได้ทันที

4.1.3 ผลการวิจัยพบว่า การทดสอบแบบจำลองสถานการณ์ความเสี่ยงกองทุนกับรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 สามารถแสดงผลสถานะกิจกรรมการกำกับดูแลและการบริหารความเสี่ยงตามหลักการโคบิต 5 กองทุนว่าไม่สำเร็จตามหลักการโคบิต 5 เนื่องจากกองทุนขาดการดำเนินงานกำกับดูแลและการบริหารความเสี่ยงในสาระสำคัญที่โคบิตกำหนด การทดสอบสามารถดำเนินการทดสอบควบคู่กับการดำเนินการตามกิจกรรมที่อธิบายรายละเอียด ขั้นตอนในการดำเนินการ ดังนั้นหากกองทุนจะปรับปรุงกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 กองทุนควรนำแนวทางที่ผู้วิจัยเสนอแนะมาปรับปรุงกระบวนการบริหารความเสี่ยงที่ดำเนินการในปัจจุบันของกองทุน รวมทั้งผู้ที่ต้องการจะนำหลักการบริหารความเสี่ยงโคบิต 5 ไปปรับใช้กับองค์กร สามารถนำรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 เป็นแนวทางในการดำเนินกระบวนการกำกับดูแลและการบริหารความเสี่ยงได้ทันที รวมทั้งยังสามารถวัดความสามารถของกระบวนการต่างๆ ได้พร้อมกันในการดำเนินการในครั้งเดียวกัน

4.2 ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

4.2.1 ควรศึกษาเรื่องการพัฒนารูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 ให้ครบทุกกระบวนการ (ทั้งหมด 17 เป้าหมาย 37 กระบวนการ)

4.2.2 ควรนำรูปแบบระบบตรวจสอบและวัดความสามารถกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 มาศึกษาแนวทางวิธีการดำเนินการเพื่อทดสอบและปรับใช้กับการดำเนินงานจริงของกองทุนฯ ตามวิธีการนำกระบวนการตามหลักการโคบิต 5 ไปใช้ (Cobit5 Enabling Processes) และวิธีการนำไปใช้ตามหลักการโคบิต 5 (Cobit5 Implementing) เพื่อมั่นใจว่านำกระบวนการบริหารความเสี่ยงตามหลักการโคบิต 5 มาปรับใช้ได้อย่างถูกต้อง

4.2.3 ควรศึกษาเรื่องรายละเอียดวิธีการประเมินและเฝ้าติดตามกระบวนการบริหารความเสี่ยงโคบิต 5 ตามหลักการรูปแบบการประเมินกระบวนการโคบิต 5

ภาคผนวก

ภาคผนวก ก

Generic Risk Scenario Using Cobit5 for Risk

GENERIC RISK SCENARIOS

An IT risk scenario is a description of an IT-related event that can lead to a loss event that has a business impact, when and if it should occur. The generic scenarios serve, after customization, as input to risk analysis activities, where the ultimate business impact (among others) needs to be established. This chapter contains a set of generic IT risk scenarios (**figure 14**), built in line with the model described in the previous sections of this guide. The set of generic scenarios contains both negative and positive example scenarios.

A word of warning: The table with generic scenarios does not replace the creative and reflective phase that every scenario-creating exercise should contain. In other words, it is not recommended that an enterprise blindly use this list andassumethatnootherriskscenariosarepossible,orassumethateveryscenariocontainedinthelistisapplicabletothe enterprise. Intelligence and experience are needed to derive a relevant and customized list of scenarios starting from this genericlist.

The generic risk scenarios in **figure 14** include the following information:

- **Riskscenariocategory**—High-leveldescriptionofthecategoryofscenario(e.g.,ITprojectselection).Intotal,there are 20categories.
- **Risktype**—Thetypetowhichscenariosderivedfromthisgenericscenariowillfit,usingthethreeriskty pes explainedearlier:
  - IT benefit/value enablement risk—Associated with (missed) opportunities to use technology to improve the efficiency oreffectivenessofbusinessprocessesorasanenablerfornewbusinessinitiatives
  - ITprogrammeandprojectdeliveryrisk—AssociatedwiththecontributionofITtoneworimprovedbusiness solutions,usuallyintheformofprojectsandprograms
  - IToperationsandservicedeliveryrisk—Associatedwiththeoperationalstability,availability,protectionand recoverabilityofITservices,whichcanbringdestructionorreductionofvaluetotheenterpr ise
- **Risk scenario outcome**—Positive outcomes are scenarios that can result in value creation or preservation. Negative outcomesarescenariosthatcanresultinvaluedestructionorfailuretogain.

A '**P**' indicates a primary (higher degree) fit and an '**S**' represents a secondary (lower degree) fit. Blank cells indicate that the risk category is not relevant for the risk scenario at hand.

- **Examplescenarios**—Foreachscenariocategory,oneorseveralsmallexamplesaregivenofscenarioswithanegative outcome, indicating whether it is more of a value destruction or a failure to gain, and/or positive outcome, indicating valuegain.Intotal,**111riskscenarioexamples**areincludedwithpossiblenegativeand/orpositiveo utcomes.

Figure 14—Example Risk						
Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0201	**Programme/projects life cycle management (programme/projects initiation, economics, delivery, quality and termination)**	P	P	S	Failing (due to cost, delays, scope creep, changed business priorities) projects are not terminated.	Failing or irrelevant projects are stopped on a timely basis.
0202		S	P	S	There is an IT project budget overrun.	The IT project is completed with in agreed-on budgets.
0203		S	P		There is occasional late IT project delivery by an internal development department.	Project delivery is on time.
0204		P	P	S	Routinely, there are important delays in IT project delivery.	The project critical path is managed accordingly and delivery is on time
0205		P	P	S	There are excessive delays in outsourced IT development projects.	Communication with third parties ensures the timely delivery within agreed-on scope and quality.
0206		P	P		Programmes/projects fail due to not obtaining the active involvement throughout the programme/project life cycle of all stakeholders (including sponsor).	Change management is conducted appropriately throughout the life cycle of the programme/project to inform stakeholders on progress and train future users.
0301	**IT investment decision making**	P		S	Business managers or representatives are not involved in important IT investment decision making (e.g., new applications, prioritisation, new technology opportunities).	There is co-ordinated decision making over IT investments between business and IT.
0302		P		S	The wrong software, in terms of cost, performance, features, compatibility, etc., is selected for implementation.	Upfront analysis is performed and a business case is prepared to ensure the adequate selection of software.
0303		P		P	The wrong infrastructure, in terms of cost, performance, features, compatibility, etc., is selected for implementation.	Upfront analysis is performed and a business case is prepared to ensure the adequate selection of infrastructure.
0304		P	P		Redundant software is purchased.	

Figure 14—Example Risk						
Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0401	**IT expertise and skills**	**P**	**P**	**P**	There is a lack of or mismatched IT-related skills within IT, e.g., due to new technologies.	Attracting the appropriate staff increases the service delivery of the IT department.
0402		**P**	**P**	**P**	There is a lack of business understanding by IT staff affecting the service delivery/ projects quality.	Correct staff and skill mix supports project delivery and value delivery.

ภาคผนวก ข

การบริหารความเสี่ยงกองทุนเงินให้กู้ยืมเพื่อการศึกษา

ขั้นตอนที่ 5 และ 6 การเลือกวิธีบริหารจัดการความเสี่ยงและการกำหนดมาตรการควบคุมความเสี่ยง

สำหรับแผนการบริหารความเสี่ยงที่มีระดับความเสี่ยงสูงมากและระดับความเสี่ยงสูงที่ต้องกำหนดมาตรการควบคุมความเสี่ยง มีทั้งหมด 5 เหตุการณ์ ที่คาดว่าจะเกิดความเสี่ยง ซึ่งจำเป็นต้องมีมาตรการควบคุม เพื่อบริหารความเสี่ยงให้ลดระดับความเสี่ยงจากสูงมากและสูงเป็นระดับปานกลางหรือต่ำ โดยมีแนวทางการดำเนินการดังนี้

ประเด็นความเสี่ยง	ผลการประเมิน ณ 1 ตุลาคม 2557			แนวโน้ม ณ 30 กันยายน 2558			แนวทางการบริหารความเสี่ยง ปีงบประมาณ 2558
	โอกาส	ผลกระทบ	ระดับ	โอกาส	ผลกระทบ	ระดับ	
ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)							
1. กระบวนการทำงานและการพัฒนาระบบอาจเกิดความล่าช้า ไม่สามารถรองรับ พรบ. ใหม่ได้ทัน	3	5	สูงมาก	3	1	ต่ำ	จัดเตรียมกระบวนการทำงานและการพัฒนาระบบเพื่อรองรับ พรบ. ใหม่

บรรณานุกรม

บรรณานุกรม

กนกวรา พวงประยงค์. (2554). *การประเมินผลกองทุนเงินให้กู้ยืมเพื่อการศึกษา:กรณีศึกษาสถานศึกษาระดับอาชีวศึกษาในจังหวัดสมุทรสงคราม*. (วิทยานิพนธ์ปริญญาศิลปศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). สถาบันบัณฑิตพัฒนบริหารศาสตร์, กรุงเทพฯ. สืบค้นจาก http://libdcms.nida.ac.th/thesis6/2554/b175246.pdf.

กองทุนเงินให้กู้ยืมเพื่อการศึกษา. (2558). *คู่มือผู้ปฏิบัติงานกองทุนเงินให้กู้ยืมเพื่อการศึกษา ประจำปีการศึกษา 2558.* กรุงเทพฯ: กระทรวงการคลัง.

เขมินทรา อภิภัทรวโรดม. (2551). *ปัจจัยที่ส่งผลต่อการตัดสินใจขอกู้เงินกองทุนเพื่อการศึกษา กรณีศึกษา: มหาวิทยาลัยเอกชน ปีการศึกษา 2547 – 2550*. (วิทยานิพนธ์ปริญญาเศรษฐศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยธุรกิจบัณฑิต, กรุงเทพฯ. สืบค้นจาก http://libdoc.dpu.ac.th/thesis/43619.pdf.

เบญจาภา มุสิกะสินธุ์. (2547). *การดำเนินงานกองทุนเงินให้กู้ยืมเพื่อการศึกษาของสถาบันอุดมศึกษาเอกชน ความคิดเห็นของผู้บริหาร เจ้าหน้าที่และนักศึกษา*. (วิทยานิพนธ์ปริญญาการศึกษามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยศรีนครินทรวิโรฒ, กรุงเทพฯ. สืบค้นจาก http://www.mahalib.msu.ac.th/msu/dublin.php?ID=13399993743.

รังษิยา อมาตยคง. (2544). *องค์ประกอบขององค์การที่ส่งผลต่อประสิทธิผลการบริหารงานกองทุนเงินให้กู้ยืมเพื่อการศึกษาของสถานศึกษาสังกัดกระทรวงศึกษาธิการเขตพื้นที่ภาคตะวันตก*. (วิทยานิพนธ์ปริญญาศิลปศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยศิลปากร, กรุงเทพฯ. สืบค้นจาก http://www.thapra.lib.su.ac.th/thesis/showthesis_th.asp?id=0000000441

สมชัย ฤชุพันธ์. (2548). แนวทางการบริหารจัดการกองทุนเงินให้กู้ยืมเพื่อการศึกษา. กรุงเทพฯ: สกศ.

สมฤดี วงษ์สมิง. (2540). *การวิเคราะห์การดำเนินงานตามนโยบายกองทุนเงินให้กู้ยืมเพื่อการศึกษา*. (วิทยานิพนธ์ปริญญาครุศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ. สืบค้นจาก http://cuir.car.chula.ac.th/browse?type=author&value=%E0%B8%AA%E0%B8%A1%E0%B8%A4%E0%B8%94%E0%B8%B5+%E0%B8%A7%E0%B8%87%E0%B8%A9%E0%B9%8C%E0%B8%AA%E0%B8%A1%E0%B8%B4%E0%B8%87

สุประพล พาพิโพธิ์ (2557).*ปัญหาการค้างชำระหนี้กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.) กรณีศึกษาผู้กู้ยืมที่ค้างชำระ*. (วิทยานิพนธ์ปริญญารัฐประศาสนศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์).

มหาวิทยาลัยเกริก, สืบค้น
จากhttps://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj9uejn36bOAhUIpo8KHW4ACnsQFggfMAA&url=http%3A%2F%2Fmpa.krirk.ac.th%2FThesis%2F24-27%2Fdoc_06.doc&usg=AFQjCNHixuzV0eDDWsn3HMNBrEo8uoxsSw&bvm=bv.128987424,d.c2I.

สุรัสวดี ชัยรัตน. (2552). การศึกษาแนวทางการพัฒนาการบริหารจัดเก็บหนี้กองทุนเงินให้กู้ยืมเพื่อการศึกษา. *วารสารวิชาการมนุษยศาสตร์และสังคมศาสตร์,* 17(27) สืบค้น จาก http://www.db.grad.nu.ac.th/~pornthip/pdf/gradresearch27/full_paper_X.pdf.

สุรินทร์ บัวงาม. (2542). *ปัจจัยที่ส่งผลต่อความสำเร็จของการนำนโยบายกองทุนเงินให้กู้ยืมเพื่อการศึกษาไปปฏิบัติในเขตการศึกษา 5*. (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี. สืบค้น จาก http://www.thaithesis.org/detail.php?id=58926

เสกสรรค์ บุญรอด.(2552). การประเมินผลและความพึงพอใจของนักศึกษาระดับอุดมศึกษาต่อกองทุนเงินให้กู้ยืมเพื่อการศึกษา: กรณีศึกษาสถาบันการศึกษาระดับอุดมศึกษา. (วิทยานิพนธ์ปริญญารัฐประศาสนศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). สถาบันบัณฑิตพัฒนบริหารศาสตร์, กรุงเทพฯ. สืบค้นจาก http://repository.nida.ac.th/handle/662723737/1055

อมราตันประวัติ. (2544). *ปัจจัยที่มีผลต่อการชำระคืนเงินกู้โครงการกองทุนเงินให้กู้ยืมเพื่อการศึกษา : กรณีศึกษา นิสิต นักศึกษาของสถาบันอุดมศึกษา ในเขตกรุงเทพมหานคร*. (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเกษตรศาสตร์, กรุงเทพฯ. สืบค้น
จาก http://research.rdi.ku.ac.th/forest/Search.aspx?keyword=%E0%B8%AD%E0%B8%A1%E0%B8%A3%E0%B8%B2%20%E0%B8%95%E0%B8%B1%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%A7%E0%B8%B1%E0%B8%95%E0%B8%B4

เอกภพ ภุมรา. (2553). *การประเมินผลการดำเนินงานของกองทุนเงินให้กู้ยืมเพื่อการศึกษาระดับอุดมศึกษาในจังหวัดเชียงใหม่*. (วิทยานิพนธ์ปริญญาเศรษฐศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยศรีนครินทรวิโรฒ, กรุงเทพฯ. สืบค้น จาก http://thesis.swu.ac.th/swuthesis/Man_Econ/Ekapop_P.pdf

Abdelbasset, Azzaoui. (2014). *Cobit5 as a mechanism for IT Governance: A case study of Statoil Company*(Master's Thesis).

Retrieved from http://www.stou.ac.th/thai/grad_stdy/masters/%E0%B8%9D%E0%B8%AA%E0%B8%AA/%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%AD%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%AD%E0%B8%B4%E0%B8%87%E0%B9%81%E0%B8%9A%E0%B8%9A%20APA.pdf

Al-Ahmad, Walid& Mohammed, Basil. (2015). A code of practice for effective information security risk management using COBIT 5. InfoSec,

Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7435520

Al-Khazrajy, Maher. (2012). *Risk Based Assessment of IT Control Frameworks: A Case Study*. (Master's Thesis). Retrieved from http://aut.researchgateway.ac.nz/bitstream/handle/10292/3309/Al-KhazrajyM.pdf?sequence=3

Bahrenburg, Matthew. (2008). *Automated processes for Sarbanes-Oxley risk management in a UNIX environment* (Master's Thesis).

Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9397&context=theses

Bartens, Yannick Schulte, Frederik &Vob, Stefan. (2014). E – business IT governance revisited: An attempt towards outlining a novel bi – directional business/IT alignment in Cobit5. *Hawaii International Conference on System Science* (2014). Retrieved from https://www.computer.org/csdl/proceedings/hicss/2014/2504/00/2504e356.pdf

Castillo, Felipe & Stanojevic,Petar. (2011). *An assessment of the IT governance maturity at SL* (Master's Thesis).

Retrieved from https://www.isaca.org/chapters4/Sweden/OmOss/Documents/XR-EE-ICS_2011_008.pdf

Chablani, Madhav. (2014). Using COBIT 5 in IT Governance and Risk Optimization for National Healthcare Delivery, An initiative of The Economic Times. Retrieved from http://health.economictimes.indiatimes.com/news/health-it/using-cobit-5-in-it-governance-and-risk-optimization-for-national-healthcare-delivery-madhav-chablani-consulting-ciotippingedge-consulting-pvt-ltd/45598756

Christoph, Mayer. (2011). *Development of a reference model for an IT governance implementation using Cobit and Val IT* (Bachelor' Degree). Retrieved from https://www.iwi.uni-hannover.de/fileadmin/wirtschaftsinformatik/Abschlussarbeiten/BA_Meyer_K.pdf

Delak, Boˇstjan. (2008). *Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry* (Doctoral dissertation). Retrieved from http://www.doc.ic.ac.uk/~pjm/caisedc2008/delak.pdf

Demopoulos, Anestis. (2012). Assessing & Mapping IT risks: Using ISACA's Cobit & Risk IT frameworks. *20 InfoCom Security Conference* (2012). Retrieved from http://www.infocomsecurity.gr/ppts_2012/demopoulos_isaca.pdf

Dr. Tirasriwat, Amara. (2016) Student Loan Defaults in THAILAND: problems and guidelines for solutions. *วารสารวิชาการบริหารธุรกิจ*, 5(1) Paper no 9 (January - June). Retrieved August 12, 2016 from http://www.vu.ac.th/apheitvu/journal/v5n1/9_Amara_Tirasriwat.pdf

Fischer, Urs. (2011) IT Scenario Analysis in Enterprise Risk Management. ISACA JOURNAL, 2, RetrievedAugust 30, 2016 from http://www.isaca.org/Journal/archives/2011/Volume-2/Documents/jpdf11v2-it-scenario-analysis.pdf.

Fredric Greene. (2015). Selected COBIT 5 Processes for Essential Enterprise Security. ISACA JOURNAL,1(2).

Retrieved from http://www.isaca.org/Journal/archives/2015/Volume-2/Documents/Selected-COBIT-5-Processes-for-Essential-Enterprise-Security_joa_Eng_0315.pdf

Gerber, Petro. (2015). *Addressing the incremental risks associated with social media by using the Cobit5 control framework* (Master's Thesis).

Retrieved from file:///C:/Users/supat/Downloads/gerber_addressing_2015%20(1).pdf

Gibbs, Nelson. (2015). Cobit 5 for risk. The institution of internal auditors: International Conference (July, 6 2015). Retrieved from https://ic.globaliia.org/Documents/MONDAY-CS-3-7-Nelson-Gibbs.pdf

Illoh, Onyeka; Aghili, Shaun; Butakov, Sergey. (2014). Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates. SERVICE-ORIENTED COMPUTING - ICSOC 2014 WORKSHOPS,

Retrieved
from https://vpn.stou.ac.th/+CSCO+00756767633A2F2F6E6363662E6A726F627378616
26A79727174722E70627A++/OneClickSearch.do?product=WOS&search_mode=OneCli
ckSearch&excludeEventConfig=ExcludeIfFromFullRecPage&colName=WOS&SID=Y2
AGF2ou5bM7ks3oz1g&field=TS&value=COBIT+5+for+risk&uncondQuotes=true&cach
eurlFromRightClick=no.

Inaba, Yuichi (Rich). (2016). Creating Value with an Enterprise ITGovernance Implementation Model Using COBIT 5. COBIT Focus, Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-Creating-Value-with-an-Enterprise-IT-Governance-Implementation-Model-Using-COBIT-5_nlt_Eng_0516.pdf.

Indah, Dwi Rosa, Harlili, Mgs & Firdaus, Afriyan. (2014). *Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk* (Master's Thesis). Retrieved from http://download.portalgaruda.org/article.php?article=355937&val=8153&title=Risk%20Management%20for%20Enterprise%20Resource%20Planning%20Post%20Implementation%20Using%20COBIT%205%20for%20Risk.

ISACA, Cobit5. (2012). *A Business Framework for the Governance and Management of Enterprise IT*. 6th ed. United State of America: ISACA publication.

Journal of Theoretical and Applied Information Technology, 60(2), 216 – 221. Retrieved from http://www.jatit.org/volumes/Vol60No2/4Vol60No2.pdf.

Kadam, Avinash W. (2013). Governance and Management of Intelligent Infrastructure. Retrieved fromhttp://csidl.org/bitstream/handle/123456789/488/eCR_CSI_IT1.pdf?sequence=1

Kessinger, Kristen. (2013). Cyberattacks, Insider Threats, Social Media Hacking:
New COBIT 5 for Risk Provides Guidelines to Manage Increased IT Risk. Eastern Daylight Time.

Retrived from http://www.businesswire.com/news/home/20130924006377/en/Cyberattacks-Insider-Threats-Social-Media-Hacking-COBIT.

Khrisna, Akbar. (2014). Risk management framework with COBIT 5 and risk management framework for cloud computing integration.

Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7005923&filter%3DAND%28p_IS_Number%3A7005902%29.

Kohout, Karel. (2013). *IT Risk Register* (Master's Thesis). Retrieved fromhttp://www.diplomovaprace.cz/2013/42/kohout_karel_it_risk_register.pdf.

Kushwaha, Deepti & Gadankush, Ashwini Vasant. (2013). Mapping of BASEL III and Cobit5 framework in banking sector of India: a Futuristic approach. *International Journal of Advanced Research in Computer Science,* 4(8), 81 – 85. Retrieved from http://ijarcs.info/?wicket:bookmarkablePage=:com.genxcellence.journal.pharmacy.web.issue.IssueDetail&target=4941&author=Deepti+Kushwaha,Ashwini+Vasant+Gadankush,Shantanu++Das&country=India&title=Mapping+of+BASEL+III+and+COBIT+5+framework+in+Banking+Sector+of+India:+A+Futuristic+Approach.

Londini, Vince. (2013). *Cobit Case Study: Risk Assessment Management using Cobit5.* Retrieved from http://www.isaca.org/COBIT/Pages/COBIT-Case-Study-Risk-Assessment-Management-Using-COBIT-5.aspx.

Lubbad, R. Rami. (2014). *Towards an abbreviated of IT governance for Palestinian government sector according to Cobit5 framework* (Master's Thesis). Retrieved from http://library.iugaza.edu.ps/thesis/113542.pdf.

Molaeijan, Kobra. (2014). Information Technology governance using Cobit5 approach (Ministry of road and Urban development). *International Journal of Scientific Management and Development,* 2(12), 668 – 675.Retrievedfrom http://www.ijsmd.com/Site/images/2014/December/Information_Technology_governance_using_COBIT_5_approach_Ministry_of_Road_and_Urban_Development.pdf

Nugroho, Heru. (2014). Conceptual model of IT governance for higher education based on Cobit5 framework.

Richards, Clift. (2013). *Information Technology risk assessment Cobit processes PO2, AI3, & DS12.* Retrieved from https://www.cityoftulsa.org/media/298258/itriskassessmentcobit.02.13.pdf.

Sheikhpour, Razieh andModiri, Nasser. (2012). An approach to map Cobit processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications,* 6(2), 13 – 28.

Retrieved from http://www.sersc.org/journals/IJSIA/vol6_no2_2012/2.pdf.

Talasophon, Sakulrat. (2011).*The Analysis and Evaluation of Thai Student Loan Scheme implementation and the deferred debts*(Dissertation's thesis).

Retrieved from http://libdcms.nida.ac.th/thesis6/2011/b171743.pdf.

Zhang, Dong &Zhou, Chao. (2014). *Adoption of Cobit5 and ITIL in small and medium size enterprises in China*(Master's Thesis).

Retrieved fromhttp://www.diva-portal.org/smash/get/diva2:727297/fulltext01.pdf

Zhang, Shengnan (Sophie). (2013). *An Exploratory Examination of the Practicability of COBIT framework*.

(Master's Thesis). Retrieved from http://liacs.leidenuniv.nl/assets/Masterscripties/ICTiB/Zhang-non-confidential.pdf.

Zhang, ShengnanandLe Fever, Hans. (2013). An examination of the pracbility of Cobit framework and the proposal of a Cobit – BSC model. *Journal of Economics, Business and Management,* 1(4), 391 – 395. Retrieved from http://www.joebm.com/papers/84-M021.pdf.

Ziderman, Adrian. (2003). Student Loan in Thailand: Are they effective, equitable, sustainable?. 1st ed. Bangkok: UNESCO.

Retrieved from http://unesdoc.unesco.org/images/0013/001336/133624e.pdf.

ISACA. (2014). *Risk Scenario: Using Cobit5 for Risk*. IL, United State of America: ISACA publication.

ประวัติผู้วิจัย

ชื่อ	นายสุภัทร ปกาสิทธิ์
วัน เดือน ปีเกิด	14 พฤษภาคม 2522
สถานที่เกิด	เขตบางกอกน้อย กรุงเทพมหานคร
ประวัติการศึกษา	ปริญญาตรี มหาวิทยาลัยอัสสัมชัญ ปีการศึกษา 2545
สถานที่ทำงาน	กองทุนเงินให้กู้ยืมเพื่อการศึกษา เขตดินแดง กรุงเทพมหานคร
ตำแหน่ง	เจ้าหน้าที่ตรวจสอบภายใน