

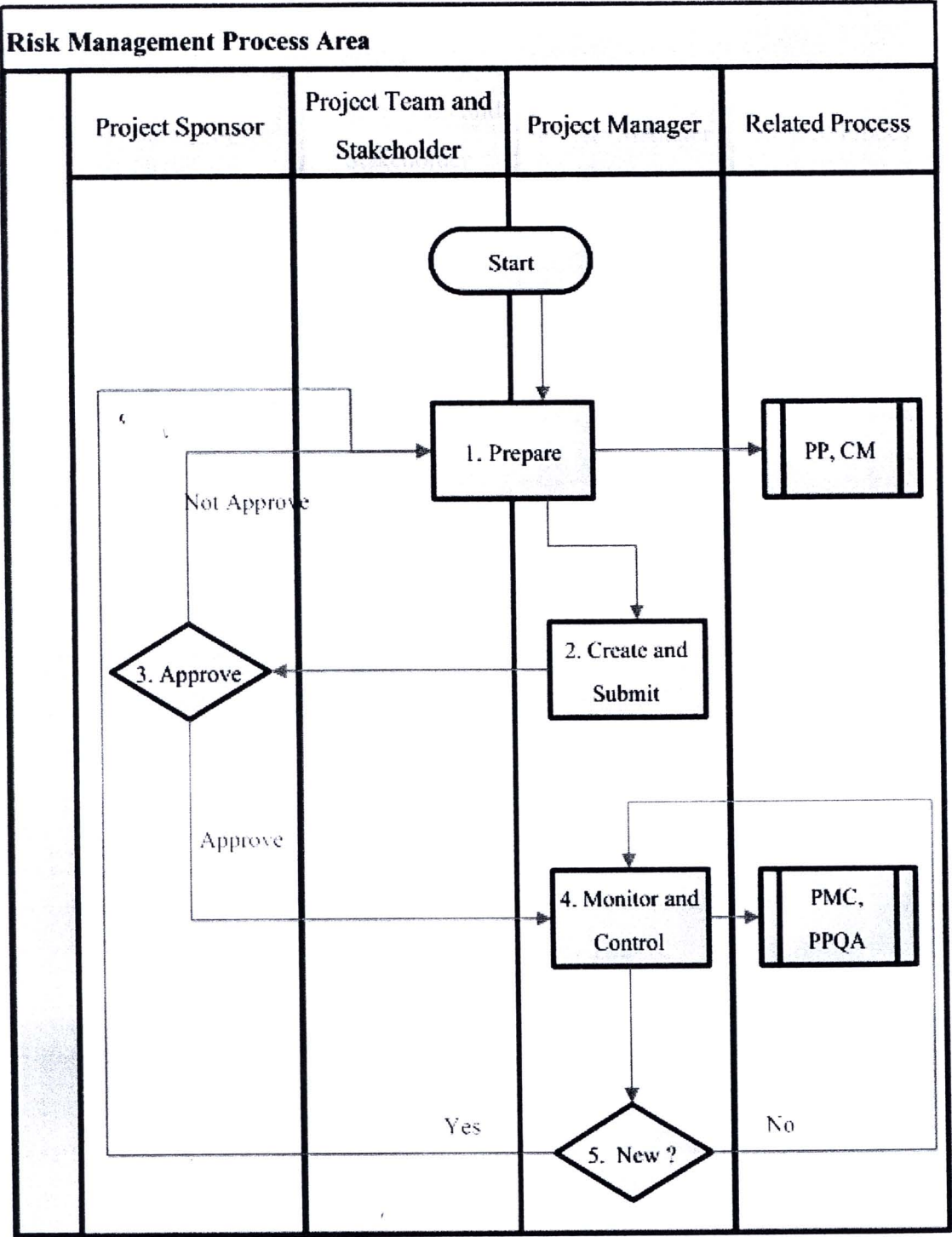
บทที่ 4

ผลการศึกษา

ในบทนี้เป็นการจัดทำ นำเสนอกระบวนการบริหารความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ และเสนอแนะแนวทางในการปฏิบัติสำหรับกระบวนการบริหารความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ และทำการเสนอแนะ การนำเสนอแบบตรวจสอบรายการ (Check Lists) ความเสี่ยงโครงการซอฟต์แวร์ให้เป็นไปตามมาตรฐานซีเอ็มเอ็มไอ สำหรับใช้ในการตรวจสอบรายการการบริหารความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ การศึกษานี้จะมุ่งเน้นศึกษาในด้านการตรวจสอบรายการที่เกี่ยวข้องกับการบริหารความเสี่ยงโครงการซอฟต์แวร์ให้เป็นไปตามมาตรฐานซีเอ็มเอ็มไอ เพื่อให้เข้าใจว่าโครงการซอฟต์แวร์ มีความสามารถในการบริหารความเสี่ยงตามมาตรฐานซีเอ็มเอ็มไอ ได้อย่างไรบ้าง และมีเอกสารอะไรบ้างที่มุ่งเน้นไปยังโครงการซอฟต์แวร์และองค์กร เมื่อองค์กรได้เริ่มจัดทำกระบวนการอย่างมีประสิทธิภาพตลอดทั่วทั้งโครงการซอฟต์แวร์ มีการกำหนดกระบวนการทำงานที่ชัดเจนเป็นมาตรฐานสามารถมองเห็นภาพภายในกระบวนการทำงานในแต่ละขั้นตอนของกระบวนการ โครงสร้างภายในแสดงให้เห็นถึงวิธีการที่เป็นมาตรฐานของกระบวนการได้ถูกนำไปประยุกต์ใช้ภายในโครงการซอฟต์แวร์ ซึ่งงานวิจัยนี้ จะมุ่งเน้นที่องค์ประกอบของการจัดการความเสี่ยง (RSKM)

4.1 กระบวนการจัดการความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ

กระบวนการจัดการความเสี่ยง (Risk Management Process Area) คือ กระบวนการบริหารจัดการความเสี่ยงของโครงการ เพื่อลดโอกาสที่ความเสี่ยงนั้นจะก่อให้เกิดผลกระทบต่อการทำงานของโครงการซอฟต์แวร์ และติดตามควบคุมความเสี่ยงที่เกิดขึ้น ตามแผนการบริหารจัดการความเสี่ยงที่วางไว้ โดยในแผนจะต้องมีการระบุความเสี่ยง (Identify Risks) การวิเคราะห์ความเสี่ยง (Analyze Risks) การจัดลำดับความเสี่ยง (Prioritize Risks) และแผนในการลดความเสี่ยง (Mitigation Plans) ภาพที่ 4.1 แสดงกระบวนการจัดการความเสี่ยงโดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 4.1 Activity Diagram กระบวนการจัดการความเสี่ยง

4.1.1 Process Activities

Project Sponsor หมายถึง ผู้บริหารที่รับผิดชอบโครงการ มีหน้าที่สนับสนุน Project Manager ให้ทำโครงการให้สำเร็จ โดยการให้คำปรึกษา ตัดสินใจ escalate ประเด็น และจัดหาทรัพยากรที่จำเป็นในการพัฒนาโครงการ ทำการทวนสอบความคืบหน้าของโครงการและกำกับการดำเนินงานให้เป็นไปตามกระบวนการที่กำหนด

Project Manager หมายถึง สมาชิกของ Project Team ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ในฐานะผู้จัดการโครงการเพื่อดำเนินการ และรับผิดชอบงานนับตั้งแต่รับคำขอจากผู้ใช้ของหน่วยงาน ส่งมอบงาน จนถึงการปิดโครงการ

Project Team หมายถึง พนักงานที่ได้รับมอบหมายให้ดูแล และรับผิดชอบงานพัฒนาโครงการ นับตั้งแต่รับคำขอจากผู้ใช้ของหน่วยงาน ส่งมอบงาน จนถึงการปิดโครงการตามกระบวนการ

Stakeholder หมายถึง ผู้ที่เกี่ยวข้องกับการพัฒนาโครงการ

สำหรับรายละเอียด Process Activity มีดังต่อไปนี้

1. Prepare for Project Risk Management Plan Activity

การเตรียมพร้อมสำหรับแผนบริหารความเสี่ยง เพื่อเตรียมจัดทำแผนการบริหารจัดการความเสี่ยงโครงการซอฟต์แวร์ โดยการระบุถึงปัจจัยเสี่ยงที่มีผลต่อการดำเนินโครงการ ทำการวิเคราะห์และจัดลำดับของความเสี่ยงเพื่อสร้างแผนสำหรับลดความเสี่ยงที่เกิดขึ้น สำหรับโครงการซอฟต์แวร์ที่จะทำการพัฒนา

การเตรียมพร้อมสำหรับการบริหารความเสี่ยง นับเป็นสิ่งแรกที่ต้องกระทำให้ส่วนของการบริหารความเสี่ยง โดยเตรียมพร้อมสำหรับการบริหารความเสี่ยงนั้นเปรียบเสมือนการค้นหาความเสี่ยงหรือปัญหาเพื่อทำการแก้ไขก่อนปัญหานั้นจะลุกลาม และส่งผลให้โครงการล้มเหลว การเตรียมความพร้อมนั้นประกอบไปด้วย

1.1 ระบุความเสี่ยง (Identify Risks) เป็นการทบทวน พิจารณาแผนทั้งหมดของโครงการซอฟต์แวร์และระบุด้านที่มีความไม่แน่นอนที่โครงการซอฟต์แวร์กำลังเผชิญอยู่ ขั้นตอนนี้จำเป็นต้องอาศัยความรู้ความเข้าใจในโครงการซอฟต์แวร์ สามารถอธิบายได้ดังตารางที่ 4.1

ตารางที่ 4.1 ระบุความเสี่ยง

Description:	การระบุประเด็นความเสี่ยงเป็นงานที่ต้องกระทำอย่างต่อเนื่องตลอดการดำเนินโครงการ โดยเป็นความรับผิดชอบของพนักงานที่ได้รับมอบหมายให้ดูแล และรับผิดชอบงานพัฒนาโครงการนี้ ให้ทำการระบุประเด็นความเสี่ยงที่อาจจะเกิดขึ้นในแต่ละระยะของการพัฒนาโครงการ ซึ่งผู้บริหารโครงการมีหน้าที่หลักในการสนับสนุนกิจกรรมนี้
Activity	- Project Manager
Ower:	- Project Team - Stakeholder
Participants:	N/A
Input:	- Project Management Plan - Risk Taxonomy-Based Questionnaire
Steps:	1. Determine risk sources and categories ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันพิจารณาเพื่อกำหนดแหล่งที่มา และประเภทของความเสี่ยงที่เกี่ยวข้องกับโครงการ โดยใช้ Risk Taxonomy-Based Questionnaire เป็นแนวทางช่วยในการกำหนดแหล่งที่มา และประเภทของความเสี่ยง เพื่อนำประเด็นความเสี่ยงเหล่านั้นไประบุใน Risk Information Form 2. Define risk parameters ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันกำหนดเกณฑ์ในการประเมินความเสี่ยง ระดับค่าขีดแบ่งในการยอมรับความเสี่ยงที่เกิดขึ้น เพื่อบอกว่าประเด็นความเสี่ยงใดบ้างที่ควรจะต้องติดตามและควบคุม 3. Identify the risks ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันระบุประเด็นความเสี่ยงที่คิดว่าจะส่งผลกระทบต่อการดำเนินโครงการ ลงใน Risk Information Form 4. Review all elements of risk ผู้บริหารโครงการ ทบทวนประเด็นความเสี่ยงทั้งหมดที่ระบุ
Output :	- Risk Information Form ในส่วนของ RISK DETAILS

1.2 วิเคราะห์ความเสี่ยง (Analyze Risks) เป็นการนำความเสี่ยงแต่ละประเด็นในส่วนของการระบุความเสี่ยง แล้วนำมาพิจารณาถึงโอกาสและผลกระทบ ที่เกิดขึ้นจากประเด็นความเสี่ยงนั้น แล้วทำการจัดลำดับความเสี่ยง สามารถอธิบายได้ดัง ตารางที่ 4.2

ตารางที่ 4.2 วิเคราะห์ความเสี่ยง

Description:	วิเคราะห์ประเด็นความเสี่ยงแต่ละประเด็น โดยพิจารณาถึงโอกาส และผลกระทบที่เกิดขึ้นจากประเด็นความเสี่ยงนั้น แล้วทำการจัดลำดับความเสี่ยง
Activity ‘	- Project Manager
Owner:	- Project Team - Stakeholder
Participants:	N/A
Input:	- Risk Information Form ในส่วนของ RISK DETAILS
Steps:	1. Evaluate the identified risks ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันประเมินประเด็นความเสี่ยงแต่ละประเด็นว่ามีค่าโอกาสที่จะเกิดความเสี่ยง และผลกระทบต่อโครงการอยู่ในระดับไหน เพื่อจะใช้ในการคำนวณค่า Risk Exposure 2. Categorize and group risks ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันจัดกลุ่มประเด็นความเสี่ยง 3. Prioritize risks ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันจัดลำดับความสำคัญสำหรับประเด็นความเสี่ยงที่ระบุ เพื่อจัดทำแผนลดความเสี่ยง
Output:	- Risk Information Form ในส่วนของ RISK ANALYSIS

1.3 พัฒนาแผนลดความเสี่ยง (Develop Risk Mitigation Plans) เกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยงและการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ผู้บริหารธุรกิจจะต้องเป็นผู้รับผิดชอบการทำงานนี้ด้วยเงื่อนไขในการใช้งบประมาณที่ต่ำที่สุด และใช้วิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผล

กระทบต่อพันธกิจและทรัพยากรขององค์กรให้น้อยที่สุด การพัฒนาความเสี่ยงสามารถอธิบายได้ดังตารางที่ 4.3

ตารางที่ 4.3 พัฒนาแผนลดความเสี่ยง

Description:	จัดทำแผนการลดความเสี่ยงสำหรับประเด็นความเสี่ยงแต่ละประเด็น เพื่อใช้สำหรับควบคุม และติดตามความเสี่ยงให้อยู่ในระดับที่ไม่ส่งผลกระทบต่อการดำเนินโครงการ
Activity Owner:	- Project Manager - Project Team - Stakeholder
Participants:	N/A
Input:	- Risk Information Form ในส่วนของ RISK DETIALS และ RISK ANALYSIS
Steps:	1. Develop risk-handling activities ผู้บริหารโครงการ ทีมพัฒนาโครงการ และผู้ที่เกี่ยวข้องกับโครงการร่วมกันกำหนดแนวทางในการควบคุมแก้ไขสำหรับแต่ละประเด็นความเสี่ยงที่มีระดับความสำคัญที่จะส่งผลกระทบต่อการดำเนินโครงการ 2. Identify the person or group ผู้บริหารโครงการกำหนดผู้รับผิดชอบในการติดตามและควบคุมแต่ละประเด็นความเสี่ยงที่มีระดับความสำคัญที่จะส่งผลกระทบต่อการทำงานโครงการ 3. ส่ง Risk Information Form ให้แก่ ผู้บริหารโครงการเพื่อลงนามอนุมัติ
Output:	- Risk Information Form ฉบับสมบูรณ์

2. Create and Submit Project Risk Management Plan to Project Sponsor Activity

การจัดทำและส่งมอบแผนการบริหารจัดการความเสี่ยงให้โปรเจกต์สปอนเซอร์ สามารถอธิบายได้ดังตารางที่ 4.4

ตารางที่ 4.4 จัดทำและส่งมอบแผนการบริหารจัดการความเสี่ยง

Description:	จัดทำแผนการบริหารจัดการความเสี่ยง และดำเนินการส่ง Project Risk Management Plan ให้กับ Project Sponsor เพื่อทำการพิจารณา
Activity Owner:	Project Manager
Participants:	Project Sponsor
Input:	- Risk Information Form ฉบับสมบูรณ์
Steps:	1. Develop Project Risk Management Plan ผู้บริหารโครงการรวบรวมข้อมูลของประเด็นความเสี่ยงที่ระบุและวิธีการควบคุม สำหรับจัดทำแผนการบริหารจัดการความเสี่ยง 2. ผู้บริหารโครงการทำการทบทวน และตรวจสอบ Project Risk Management Plan 3. ผู้บริหารโครงการดำเนินการส่ง Project Risk Management Plan ให้กับ Project Sponsor เพื่อพิจารณาอนุมัติ
Output:	Project Risk Management Plan



3. Approve Project Risk Management Plan Activity

การอนุมัติแผนบริหารความเสี่ยงโครงการ สามารถอธิบายได้ดังตารางที่ 4.5

ตารางที่ 4.5 อนุมัติแผนบริหารความเสี่ยงโครงการ

Description:	การทบทวน และตรวจสอบความเหมาะสมของ Project Risk Management Plan และทำการอนุมัติ Project Risk Management Plan
Activity:	Project Sponsor
Participants:	Project Manager
Input:	Project Risk Management Plan
Steps:	1. Project Sponsor ทำการทบทวน และตรวจสอบ Project Risk Management Plan และพิจารณาอนุมัติ - กรณี Approve Plan ผู้มีอำนาจลงนาม หรือ ผู้บริหารระดับสูงที่รับผิดชอบโครงการเห็นชอบและลงนามอนุมัติ Project Risk Management Plan - กรณี Reject Plan ผู้มีอำนาจลงนาม หรือ ผู้บริหารระดับสูงที่รับผิดชอบโครงการไม่เห็นชอบและไม่ลงนามอนุมัติ Project Risk Management Plan ให้กลับไปดำเนินการตามข้อ 3.1 2. Baseline Project Risk Management Plan ผู้บริหารโครงการนำ Project Risk Management Plan ที่ได้รับการอนุมัติแล้วมาเป็น Baseline ในการติดตาม และควบคุมความเสี่ยงของโครงการต่อไป
Output:	- Project Risk Management Plan ชุดที่กำหนดเป็น Baseline

4. Continuously Monitor and Control Activity

การดำเนินการติดตามและควบคุมความเสี่ยงที่เกิดขึ้น สามารถอธิบายได้ดังตารางที่ 4.6

ตารางที่ 4.6 ดำเนินการติดตามและควบคุมความเสี่ยงที่เกิดขึ้น

Description:	ดำเนินการติดตาม และควบคุมความเสี่ยงที่เกิดขึ้น ไม่ให้ส่งผลกระทบต่อการดำเนินโครงการ
Activity	Project Manager
Owner:	
Participants:	Project team
Input:	- Project Risk Management Plan - Risk Status Report
Steps:	1. Monitor risk status ผู้บริหารโครงการ และทีมพัฒนาโครงการ ติดตามเก็บรวบรวมข้อมูลสถานะความเสี่ยงที่เกิดขึ้น ว่ามีค่าระดับค่าขีดแบ่งในการยอมรับเกินที่กำหนดหรือไม่ 2. Performance for risk-handling activity ผู้บริหารโครงการ และทีมพัฒนาโครงการดำเนินการควบคุมแก้ไขประเด็นความเสี่ยงที่เกิดขึ้นตามแผนที่วางไว้ 3. Update lists of risk status ผู้บริหารโครงการ และทีมพัฒนาโครงการ ปรับปรุงข้อมูลสถานะของแต่ละประเด็นความเสี่ยงที่ได้ดำเนินการควบคุมแก้ไข
Output:	- Project Risk Management Plan - Risk Status Report

5. Project has new risks Activity

ความเสี่ยงใหม่ที่มีการเกิดขึ้น สามารถอธิบายได้ดังตารางที่ 4.7

ตารางที่ 4.7 ความเสี่ยงใหม่ที่มีการเกิดขึ้น

Description:	ตรวจสอบว่าในการติดตาม และควบคุมความเสี่ยงของโครงการนั้นพบว่ามีความเสี่ยงใหม่เกิดขึ้นหรือไม่ ถ้ามีความเสี่ยงใหม่เกิดขึ้นก็ให้ทำการปรับปรุง Project Risk Management Plan ทันที
Activity:	Project Manager
Owner:	
Participants:	Project Team
Input:	- Project Risk Management Plan - Risk Status Report
Steps:	ผู้บริหารโครงการประเมินว่าในการดำเนินงานโครงการนั้นมีความเสี่ยงใหม่เกิดขึ้นหรือไม่ - กรณีที่มีความเสี่ยงใหม่เกิดขึ้น ผู้บริหารโครงการจะต้องทำการปรับปรุง Project Risk Management Plan แล้วให้กลับไปดำเนินการตาม ข้อ 1 - กรณีที่ไม่มีความเสี่ยงใหม่เกิดขึ้น ผู้บริหาร โครงการจะต้องตรวจสอบผลการติดตามและควบคุมความเสี่ยง แล้วทำการปรับปรุง Risk Status Report
Output:	- Project Risk Management Plan ฉบับปรับปรุง Baseline - Risk Status Report

4.1.2 Process Area Activity Check List

Process Area Activity Check List เป็นรายการสรุปกิจกรรมที่ต้องดำเนินการของแต่ละ Process Area เพื่อให้ผู้รับผิดชอบในการดำเนินการตาม Process Area ใช้สำหรับช่วยในการตรวจสอบกระบวนการทำงานว่าดำเนินการครบถ้วนตามที่ระบุไว้หรือไม่ ตารางที่ 4.8 แสดง Process Area Activity Check List สำหรับกระบวนการจัดการความเสี่ยงที่ออกแบบ

ตารางที่ 4.8 Process Area Activity Check List

Items	Status
Input • Project Management Plan • Risk Taxonomy-Based Questionnaire	
Activities • Create Project Risk Management Plan - Step 1 : Identify Risks - Step 2 : Analyze Risks - Step 3 : Develop Risk Mitigation Plans • Submit Project Risk Management Plan to Project Sponsor - Step 1 : Review Project Risk Management Plan - Step 2 : Submit Project Risk Management Plan to Project Sponsor • Approve Project Risk Management Plan - Step 1 : Review Project Risk Management Plan - Step 2 : Baseline Project Risk Management Plan • Continuously Monitor and Control - Step 1 : Update Lists of Risk Status - Step 2 : Performance for Risk-Handling Activity - Step 3 : Update Lists of Risk Status • Project Have New Risks - Step 1 : Identify and Assess New Risks	
Output • Project Risk Management Plan • Risk Information Form • Risk Status Report	

4.2 แนวทางปฏิบัติสำหรับกระบวนการบริหารความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ

แนวทางปฏิบัติสำหรับกระบวนการบริหารความเสี่ยงโครงการซอฟต์แวร์ เป็นเอกสารที่ระบุขั้นตอนที่จะช่วยให้ผู้บริหารโครงการซอฟต์แวร์สามารถระบุความเสี่ยงที่อาจเกิดขึ้นกับงานโครงการซอฟต์แวร์ที่ดำเนินการ ช่วยพิจารณาผลกระทบ ตลอดจนวางแผนลดความเสี่ยงโดยมีการประเมินความเสี่ยงเป็นระยะตลอดการดำเนินโครงการซอฟต์แวร์ เพื่อให้มั่นใจว่าจะจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้ ตารางที่ 4.9 แสดงเป้าหมายจำเพาะและแนวทางปฏิบัติจำเพาะในกลุ่มกระบวนการบริหารความเสี่ยง และมีความสัมพันธ์กันดังภาพที่ 4.2 โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 4.9 เป้าหมายจำเพาะและแนวทางปฏิบัติจำเพาะในกลุ่มกระบวนการบริหารความเสี่ยง

SG1: เตรียมพร้อมสำหรับการบริหารความเสี่ยง
SP 1.1: กำหนดที่มาของความเสี่ยงและจัดประเภทความเสี่ยง
SP 1.2: กำหนดตัวแปรของความเสี่ยง
SP 1.3: จัดทำกลยุทธ์การบริหารความเสี่ยง
SG2: ระบุและวิเคราะห์ความเสี่ยง
SP 2.1: การระบุความเสี่ยง
SP 2.2: การประเมิน การจัดหมวดหมู่และการจัดลำดับความเสี่ยง
SG3: ลดความเสี่ยง
SP 3.1: การพัฒนาแผนการลดความเสี่ยง
SP 3.2: การดำเนินการตามแผนการลดความเสี่ยง

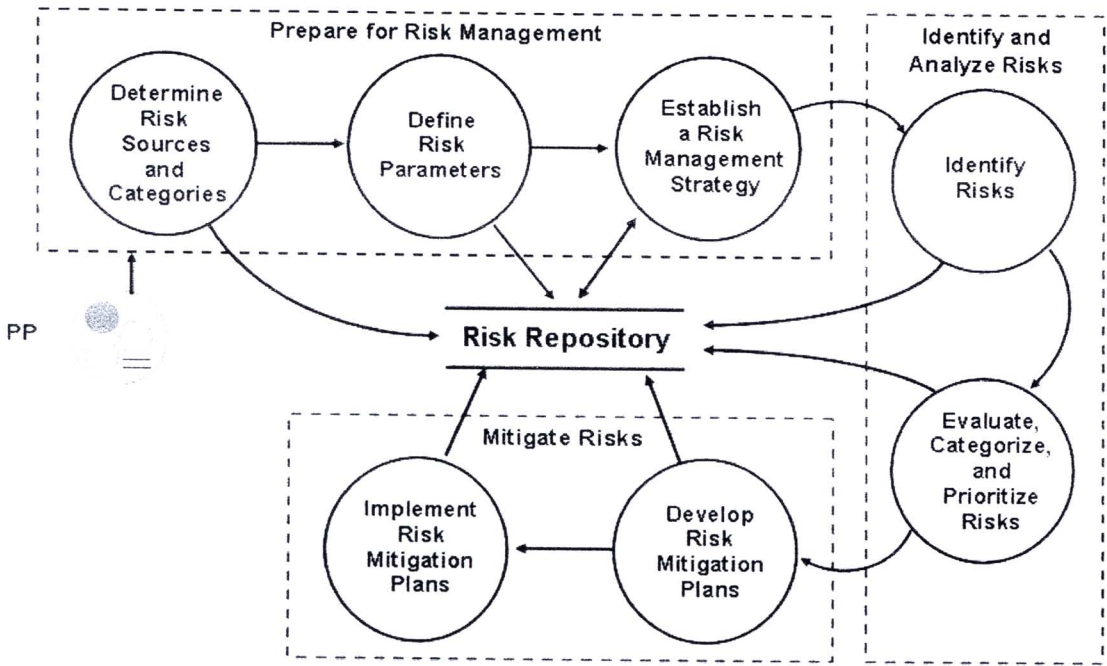
จากตารางที่ 4.9 รายละเอียดเป้าหมายจำเพาะและแนวทางปฏิบัติจำเพาะในกลุ่มกระบวนการบริหารความเสี่ยง ซึ่งการดำเนินการกระบวนการจัดการความเสี่ยงตามมาตรฐานซีเอ็มเอ็มไอ (Risk Management: RSKM) แบ่งเป็น 3 เป้าหมายจำเพาะ โดยมีรายละเอียดดังต่อไปนี้

1. เตรียมความพร้อมสำหรับการบริหารความเสี่ยง โดยกำหนดแหล่งกำเนิดและประเภทของความเสี่ยง เช่น ความต้องการที่ไม่แน่นอนหรือข้อกำหนดความต้องการที่ไม่ชัดเจน และการเปลี่ยนแปลงข้อกำหนดความต้องการหลายครั้ง การออกแบบที่ไม่สามารถกระทำตามได้ การขาดแคลนเทคโนโลยีหรือความต้องการใช้เทคโนโลยีใหม่ (ฮาร์ดแวร์และซอฟต์แวร์) บุคลากรไม่มีทักษะความรู้ความสามารถเพียงพอหรือการขาดแคลนบุคลากร ที่ได้รับการฝึกอบรมทางด้าน

เทคนิค การประมาณเวลาที่ไม่สามารถเป็นจริงได้ การตัดสินใจจากภายนอกที่มีผลต่อโครงการ การเชื่อมโยงกับระบบอื่น สมรรถนะต่ำ และประเด็นปัญหาเรื่องค่าใช้จ่ายและเงินทุน และอื่นกำหนดพารามิเตอร์ของความเสี่ยง เพื่อนำมาประเมินจัดตามประเภทของความเสี่ยง ซึ่งอาจกำหนดได้โดยตาม ผลกระทบ ความรุนแรง ความเป็นไปได้ และลำดับเหตุการณ์ของความเสี่ยงกำหนดกลยุทธ์ ในการจัดการกับความเสี่ยงที่พบ เช่น กำหนดขอบเขตของการจัดการ กำหนดลำดับขั้นตอนวิธีการและเครื่องมือที่นำมาใช้ กำหนดเทคนิควิธีการในการตรวจวัดสถานะของความเสี่ยง และการประเมินความเสี่ยง

2. ระบุและวิเคราะห์ความเสี่ยง โดยทำการประเมินและจัดแบ่งประเภทหมวดหมู่ของความเสี่ยง

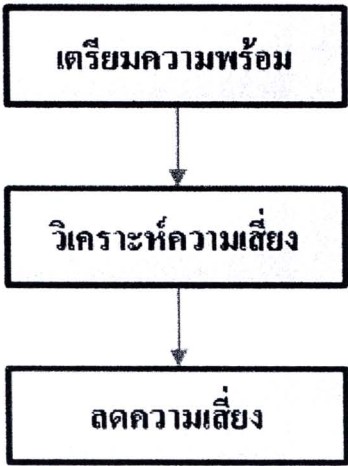
3. ลดความเสี่ยง พัฒนาแผนการจัดการกับความเสี่ยงโดยมุ่ง ประเด็นที่จะลดความรุนแรงต่อผลกระทบที่เกิดกับโครงการ



ภาพที่ 4.2 ความสัมพันธ์ระหว่างเป้าหมายเฉพาะและแนวทางปฏิบัติเฉพาะในกลุ่มกระบวนการบริหารความเสี่ยง (Ray C. Williams, 2006)

4.3 แบบตรวจสอบความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ

แบบตรวจสอบความเสี่ยงโครงการซอฟต์แวร์ตามมาตรฐานซีเอ็มเอ็มไอ จะสร้างขึ้นตามเป้าหมายจำเพาะและแนวทางปฏิบัติจำเพาะในกลุ่มกระบวนการบริหารความเสี่ยงตามมาตรฐานซีเอ็มเอ็มไอ โดยแบบตรวจสอบเหล่านี้ จะถูกใช้ในขั้นตอนการตรวจสอบการจัดการความเสี่ยง ภาพที่ 4.3 และตารางที่ 4.10 แสดงแบบตรวจสอบความเสี่ยงของโครงการซอฟต์แวร์โดยรวม



ภาพที่ 4.3 ขั้นตอนการตรวจสอบการจัดการความเสี่ยง

ตารางที่ 4.10 แบบตรวจสอบความเสี่ยงของโครงการซอฟต์แวร์โดยรวม

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	องค์กรของคุณมีการกำหนดขอบเขตของความเสี่ยง/อันตรายที่อาจจะเกิดขึ้นในการพัฒนาซอฟต์แวร์ในองค์กร หรือไม่		
2	องค์กรของคุณมีการจัดทำเป็นรายการรวบรวมความเสี่ยง/อันตรายที่อาจจะเกิดขึ้นทั้งภายนอกและภายในองค์กร หรือไม่		
3	เมื่อทราบถึงภาวะความเสี่ยงแล้วองค์กรของคุณสามารถระบุได้หรือไม่ว่ามีความรุนแรงมากน้อยเพียงใด		
4	องค์กรของคุณได้ทำการประเมินถึงภาวะเสี่ยงนั้นหรือไม่ว่ามีความรุนแรงมากน้อยเพียงใด		

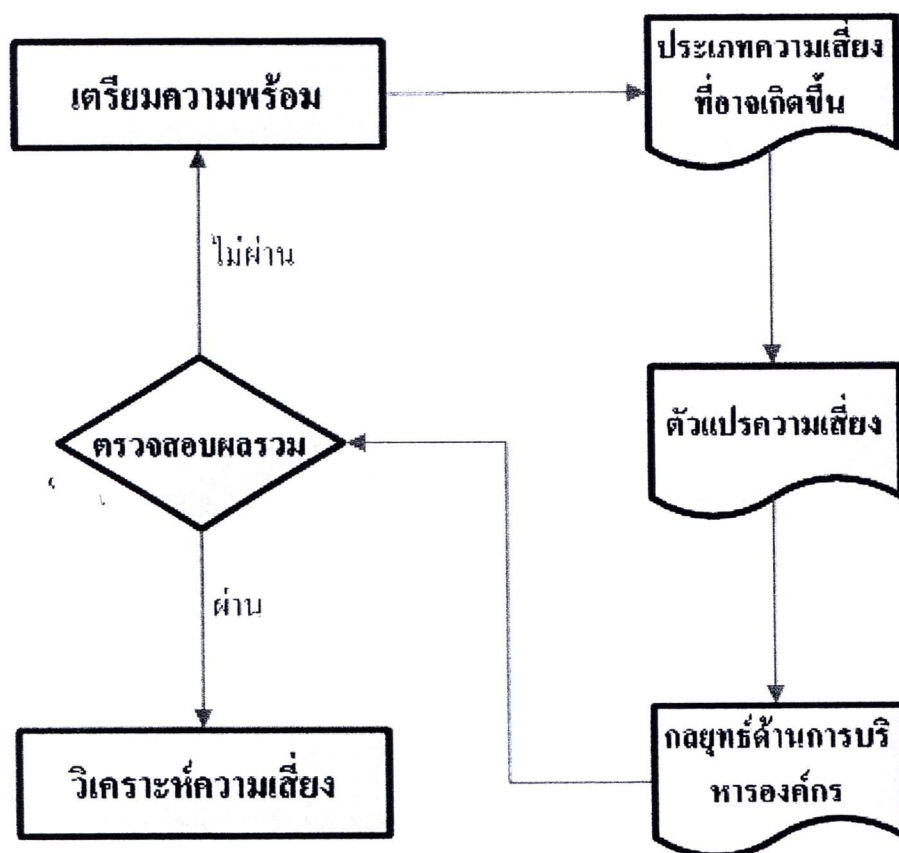
ตารางที่ 4.10 (ต่อ)

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
5	องค์กรของคุณมีหลักการ/วิธีการ/เครื่องมือเตรียมพร้อมรับมือกับภาวะเสี่ยงที่อาจจะเกิดขึ้น หรือไม่		
6	ในกรณีที่ภาวะความเสี่ยงมีจำนวนมาก องค์กรของคุณได้ทำการจัดแบ่งความรุนแรงที่เป็นผลกระทบจากความเสี่ยงตามลำดับหรือไม่เพื่อคัดเลือกและหาแนวทางป้องกันไว้ก่อน		
7	มีหลักฐานอ้างอิงได้หรือไม่ว่า เมื่อทำการแก้ไขไปแล้วจะช่วยลดทอนความเสี่ยงนั้นได้หรือหรือสามารถกำจัดความเสี่ยงนั้นออกไปจากองค์กรนั้นได้		
8	มีการจัดเก็บบันทึกเพื่อเก็บเป็นหลักฐานอ้างอิงต่อไปหรือไม่		
9	มีการจัดฝึกอบรมเทคนิค/วิธีการ ในการแก้ไขและป้องกันภาวะความเสี่ยงนั้นหรือไม่		
10	มีการรายงานผลภาวะเสี่ยงนี้ในที่ประชุมเพื่อให้ผู้บริหารและคณะผู้ทำงานที่เกี่ยวข้องรับทราบ หรือไม่		

1. เตรียมพร้อมสำหรับการบริหารความเสี่ยง

การเตรียมความพร้อม (Preparation) คือ การดำเนินการโดย กลยุทธ์การบำรุงรักษาและการสร้างสำหรับการระบุ การวิเคราะห์ และการลดความเสี่ยง การเตรียมความพร้อมนั้นส่วนใหญ่ มักจะเป็นแผนการในเอกสารของการบริหารความเสี่ยง กลยุทธ์ของการบริหารความเสี่ยงมักอยู่ที่ การกระทำที่เฉพาะเจาะจงและแนวทางการจัดการที่ใช้และควบคุม โปรแกรมการบริหารความเสี่ยง ทั้งนี้รวมไปถึงการระบุแหล่งที่มาของความเสี่ยง โครงการที่ใช้ในการจัดการประเภทความเสี่ยง และตัวแปรที่ใช้ในการประเมิน ข้อจำกัด การควบคุมความเสี่ยงในการจัดการที่มีประสิทธิภาพ

การเตรียมพร้อมสำหรับการบริหารความเสี่ยง ถือเป็นสิ่งแรกที่จะต้องกระทำให้ส่วนของการบริหารความเสี่ยง โดยเตรียมพร้อมสำหรับการบริหารความเสี่ยงนั้นเปรียบเสมือนการ ค้นหาความเสี่ยงหรือปัญหาเพื่อทำการแก้ไขก่อนปัญหานั้นจะลุกลาม และส่งผลให้โครงการ ล้มเหลว ภาพที่ 4.4 แสดงแผนผังการเตรียมพร้อมสำหรับการบริหารความเสี่ยง



ภาพที่ 4.4 แผนผังการเตรียมพร้อมสำหรับการบริหารความเสี่ยง

1.1 กำหนดที่มาของความเสี่ยงและจัดประเภทความเสี่ยง

ในขั้นตอนของการกำหนดความเสี่ยงและจัดประเภทความเสี่ยงนี้ ผู้จัดการโครงการซอฟต์แวร์ มักจะมีประเด็นที่อยู่ในใจว่าเรื่องใดบ้างที่จะนำความเสี่ยงมาสู่โครงการซอฟต์แวร์ โดยประเด็นต่างๆ นั้นมักมาจากประสบการณ์ แต่ในส่วนของการบริหารความเสี่ยงนี้ จำเป็นที่จะต้องจัดหาวิธีที่เป็นรูปธรรมเพื่อนำมาใช้ในการกำหนดความเสี่ยง เช่น จัดทำรายการแบบตรวจสอบ (Checklists) เพื่อทำการตรวจสอบความเสี่ยงที่เกิดขึ้นในโครงการ โดยได้มีการกำหนดแนวทางเพื่อนำไปใช้ในการกำหนดความเสี่ยง

ที่มาของความเสี่ยงเป็นสิ่งสำคัญแรกเริ่มในการเกิดต้นเหตุความเสี่ยงสำหรับโครงการและองค์กรซอฟต์แวร์ ที่มาของความเสี่ยงอาจเกิดได้จากหลายปัจจัย ทั้งภายในและภายนอก และรวมถึงความเสี่ยงในด้านพื้นฐานต่างๆ ภายในองค์กร ดังที่ได้แสดงในแบบตรวจสอบที่ 4.11 โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 4.11 แบบตรวจสอบที่มาของความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีความแน่ใจในความต้องการ		
2	การประมาณการโครงการเป็นที่แน่ใจว่าสามารถใช้งานได้		
3	การออกแบบสามารถปฏิบัติการได้		
4	เทคโนโลยีสามารถหาได้		
5	มีการแบ่งส่วนตารางเวลาที่แน่นอน		
6	บุคลากรมีทักษะเพียงพอ		
7	ค่าใช้จ่ายและการเงินไม่เป็นปัญหา		
8	ผู้ทำสัญญาโครงการมีความสามารถที่เพียงพอและแน่นอน		
9	ผู้ผลิตโครงการมีความสามารถที่เพียงพอและแน่นอน		
10	การสื่อสารกับลูกค้าให้เข้าใจในโครงการมีประสิทธิภาพ		
11	การปฏิบัติงานโครงการมีความต่อเนื่อง		

การจัดประเภทความเสี่ยง เป็นการสะท้อนกลับของขยะภายในองค์กร ให้สามารถช่วยจัดการเกี่ยวกับการจัดประเภทต่างๆภายในองค์กรและ โครงการซอฟต์แวร์ และยังเป็นการช่วยให้ องค์กรซอฟต์แวร์มีความแข็งแกร่งสำหรับกิจกรรมต่างๆในอนาคต ภายในองค์กรและ โครงการ ซอฟต์แวร์ เพื่อที่สามารถนำไปใช้ในแผนการลดความเสี่ยงต่อไปได้

ปัจจัยต่อไปนี้อาจได้รับการพิจารณาเมื่อมีการจัดประเภทความเสี่ยง ดังที่ได้แสดงในแบบตรวจสอบที่ 4.12

ตารางที่ 4.12 แบบตรวจสอบการจัดประเภทของความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีขั้นตอนในรูปแบบวงจรของโครงการซอฟต์แวร์		
2	มีประเภทการใช้ของกระบวนการ		
3	มีประเภทการใช้ของผลิตภัณฑ์		
4	มีการบริหารโปรแกรมความเสี่ยง		

จากตารางที่ 4.12 แบบตรวจสอบการจัดประเภทความเสี่ยง สามารถอธิบายเพิ่มเติมได้ดังต่อไปนี้

ขั้นตอนของรูปแบบวงจรของโครงการซอฟต์แวร์ เช่น ความต้องการ การออกแบบ การผลิต การทดสอบประเมินผล การส่งมอบ และการจำหน่าย เป็นต้น

การบริหารโปรแกรมความเสี่ยง เช่น ความเสี่ยงที่สำคัญ งบประมาณความเสี่ยง ความเสี่ยงด้านเวลา ความเสี่ยงด้านทรัพยากร ความเสี่ยงด้านประสิทธิภาพ และความเสี่ยงด้านการสนับสนุน เป็นต้น

วิทยาศาสตร์หรือเทคนิคเกี่ยวกับการแบ่งประเภทความเสี่ยงสามารถใช้เป็นกรอบสำหรับการกำหนดแหล่งที่มาและประเภทความเสี่ยง

1.2 การกำหนดตัวแปรความเสี่ยง

กำหนดตัวแปรความเสี่ยงที่ใช้ในการวิเคราะห์และจัดประเภทความเสี่ยง และตัวแปรที่ใช้ในการพยายามบริหารความเสี่ยง ตัวแปรสำหรับ การประเมิน การจัดประเภหรือหมวดหมู่ และการจัดลำดับความเสี่ยง มีรายละเอียดในตัวแปรความเสี่ยงดังกล่าว ดังตารางที่ 4.13

ตารางที่ 4.13 แบบตรวจสอบการกำหนดตัวแปรความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีการกำหนดโอกาสที่สามารถเกิดความเสี่ยง		
2	มีการกำหนดผลของความเสี่ยงที่อาจเกิดขึ้น		
3	มีการกำหนดเกณฑ์ในการกระตุ้นการบริหารจัดการกิจกรรม		

จากตารางที่ 4.13 แบบตรวจสอบตัวแปรความเสี่ยงสามารถอธิบายได้ดังนี้

- โอกาสเสี่ยง เช่น ความน่าจะเป็นความเสี่ยงที่เกิดขึ้น
- ผลลัพธ์ของความเสี่ยง เช่น ผลกระทบและความรุนแรงของความเสี่ยงที่เกิดขึ้น
- มีเกณฑ์ในการกระตุ้นการบริหารจัดการกิจกรรม

ตัวแปรความเสี่ยงที่ใช้เป็นหลักเกณฑ์ทั่วไปควรจะมีความสอดคล้องสำหรับการจัดการเปรียบเทียบสิ่งต่างๆ ซึ่งถ้าหากไม่มีตัวแปรเหล่านี้จะเป็นการยากมากที่จะวัดค่าความรุนแรงของการเปลี่ยนแปลงที่ไม่พึงประสงค์อันเกิดจากความเสี่ยงและจัดลำดับความสำคัญ ซึ่งเป็นการกระทำที่จำเป็นสำหรับแผนการลดความเสี่ยง

1.3 จัดทำกลยุทธ์ด้านการบริหารความเสี่ยง

การจัดทำกลยุทธ์ด้านการบริหารความเสี่ยงก็เพื่อให้สามารถรับรู้กับความเสี่ยงประเภทต่างๆและสามารถรู้เกี่ยวกับขั้นตอนและวิธีการบริหารความเสี่ยงที่มีประสิทธิภาพ แบบตรวจสอบด้านการจัดทำกลยุทธ์ด้านการบริหารความเสี่ยงมีรายละเอียดดังตารางที่ 4.14

ตารางที่ 4.14 แบบตรวจสอบการจัดทำกลยุทธ์ด้านการบริหารความเสี่ยง

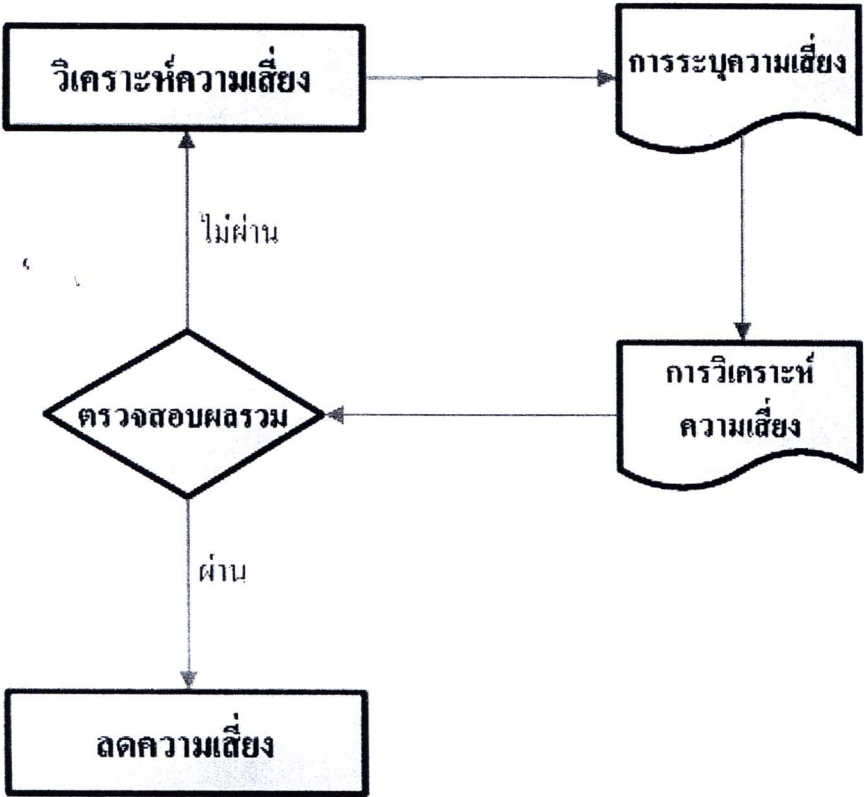
ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีขอบเขตในความพยายามบริหารความเสี่ยง		
2	มีวิธีการและเครื่องมือที่ใช้สำหรับการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การลดความเสี่ยง การตรวจสอบความเสี่ยงและการติดต่อสื่อสาร		
3	มีแหล่งโครงการซอฟต์แวร์เฉพาะความเสี่ยง		
4	มีวิธีการจัดประเภท เปรียบเทียบและรวมเป็นหนึ่ง		
5	มีตัวแปรที่รวมถึง โอกาส ผลลัพธ์และเกณฑ์ สำหรับการดำเนินการในการระบุความเสี่ยง		
6	มีเทคนิคที่จะใช้ลดความเสี่ยง		
7	มีการนิยามหลักเกณฑ์ความเสี่ยงต่อการติดตามความเสี่ยงเริ่มต้น		
8	มีช่วงเวลาสำหรับการตรวจสอบความเสี่ยงหรือการคิดทบทวนใหม่		

กลยุทธ์การบริหารความเสี่ยงควรได้รับคำแนะนำจากวิสัยทัศน์ร่วมกันของความสำเร็จที่อธิบายผลลัพธ์ของโครงการซอฟต์แวร์ในอนาคต ทั้งในแง่ของการจัดส่งโครงการซอฟต์แวร์ ค่าใช้จ่าย และสมรรถภาพในการใช้งานโครงการซอฟต์แวร์ กลยุทธ์ในการบริหารความเสี่ยงของโครงการซอฟต์แวร์บ่อยครั้งได้จัดทำได้ในรูปแบบเอกสารได้หรือโครงการแผนการจัดการความเสี่ยง กลยุทธ์การบริหารความเสี่ยงนี้ คือ การตรวจสอบกับผู้มีส่วนได้ส่วนเสียของโครงการซอฟต์แวร์เพื่อให้เกิดการส่งเสริมและเกิดความเข้าใจ นั่นเอง

2. การระบุและวิเคราะห์ความเสี่ยง

ความเสี่ยงเป็นการระบุและวิเคราะห์เพื่อพิจารณาในสำคัญขององค์กรและโครงการซอฟต์แวร์ ทรัพยากรมีผลกระทบต่ระดับของความเสี่ยงที่ได้กำหนดการจัดการระบุความเสี่ยงและความมุ่งมั่น เมื่อมีความเหมาะสม

การระบุและการวิเคราะห์ความเสี่ยงตามมาตรฐานซีเอ็มเอ็มไอ ประกอบด้วย การระบุความเสี่ยง และการประเมิน การจัดหมวดหมู่และการจัดลำดับความเสี่ยง ดังภาพที่ 4.5 โดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 4.5 แผนผังการระบุและการวิเคราะห์ความเสี่ยง

2.1 การระบุความเสี่ยง

การระบุ (Identify) คือ ทบทวนแผนทั้งหมดของโครงการ ระบุด้านที่มีความไม่แน่นอน การชี้ระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงปัญหาความไม่แน่นอนที่องค์กรเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจขององค์กร การกิจและกิจกรรม สิ่งแวดล้อมด้านกฎหมาย สังคม การเมืองและวัฒนธรรม พัฒนาการและปัจจัยที่มีต่อความสำเร็จขององค์กร รวมทั้งโอกาสและสิ่งคุกคามที่มีต่อองค์กร การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุกๆ ด้านขององค์กร สาเหตุสำคัญของความเสี่ยงคือการมีสิ่งคุกคาม (Threat) ที่อาจส่งผลให้เกิดการละเมิดความมั่นคงสารสนเทศและส่งผลเสียตามมาอาจพิจารณาถึง

เหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับองค์กรนั้น หรือองค์กรอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้

การระบุปัญหาที่อาจเกิดอันตราย ภัยคุกคาม และ ช่องโหว่ การระบุปัญหาเหล่านี้จะมีผลต่อความพยายามในการทำงานหรือเป็นพื้นฐานการวางแผนสำหรับการบริหารความเสี่ยงที่ประสบความสำเร็จ ความเสี่ยงจะต้องถูก อธิบายและระบุในวิธีที่เข้าใจได้ ก่อนที่จะสามารถวิเคราะห์และจัดการอย่างถูกต้อง ความเสี่ยงที่มีเอกสารในข้อความสั้นที่มีเงื่อนไขและผลกระทบของความเสี่ยงที่เกิดขึ้น

การระบุความเสี่ยงควรเป็นวิธีการที่เป็นระเบียบและมีความละเอียด เพื่อหาความน่าจะเป็น เพื่อทำให้บรรลุในวัตถุประสงค์และมีประสิทธิภาพ การระบุความเสี่ยงไม่ควรที่จะทำในทุกเหตุการณ์ที่เป็นไปได้โดยไม่คำนึงถึงวิธีการที่ไม่น่าจะเป็นไปได้ การระบุความเสี่ยงเป็นการพัฒนาแผนกลยุทธ์การบริหารความเสี่ยงโดยใช้การจัดประเภทและตัวแปรพร้อมกับการระบุแหล่งที่มา ความเสี่ยงสามารถให้การปรับปรุงให้กระชับและวินัยที่เหมาะสมกับการระบุความเสี่ยง รูปแบบการระบุความเสี่ยงเป็นพื้นฐานแก่ผู้เริ่มต้นกิจกรรมการบริหารความเสี่ยง กลยุทธ์ความเสี่ยงครั้งล่าสุดควรจะตรวจสอบรายการความเสี่ยงเป็นระยะเพื่อตรวจสอบใหม่แหล่งที่มาของความเป็นไปได้ ของความเสี่ยงและการเปลี่ยนแปลงเงื่อนไข การค้นพบแหล่งที่มาและการมองข้ามความเสี่ยง หรือสิ่งที่ไม่มีอยู่จริง

กิจกรรมระบุความเสี่ยงที่มุ่งเน้นการระบุความเสี่ยง ของการกล่าวโทษคำหาผิดที่ไม่ได้ตำแหน่ง ผลของกิจกรรมระบุความเสี่ยงไม่ได้ใช้เพื่อจัดการประเมินประสิทธิภาพของบุคลากร และในแบบตรวจสอบของการระบุความเสี่ยงของโครงการซอฟต์แวร์ มีรายละเอียดในการตรวจสอบดังตารางที่ 4.15

ตารางที่ 4.15 แบบตรวจสอบการระบุความเสี่ยงโครงการซอฟต์แวร์

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีการระบุความเสี่ยงที่เกี่ยวข้องกับ ค่าใช้จ่าย ตารางเวลาและการปฏิบัติ		
2	มีการทบทวนองค์ประกอบของสิ่งแวดล้อมที่อาจส่งผลกระทบต่อโครงการซอฟต์แวร์		
3	มีการทบทวนองค์ประกอบของโครงสร้างงานที่เสียทั้งหมด เพื่อเป็นส่วนหนึ่งของการระบุความเสี่ยง เพื่อให้มั่นใจว่าทุกด้านที่ได้พยายามทำงานนั้น ได้รับการพิจารณา		
4	มีการทบทวนองค์ประกอบของแผนโครงการว่าได้เป็นส่วนหนึ่งของการระบุความเสี่ยง เพื่อให้มั่นใจว่าทุกโครงการซอฟต์แวร์นั้น ได้รับการพิจารณา		
5	มีเอกสารบริบทเงื่อนไขและผลกระทบที่อาจเกิดขึ้นของความเสี่ยง		
6	มีการระบุผู้ที่มีส่วนได้ส่วนเสียที่เชื่อมโยงกับแต่ละความเสี่ยง		

จากตารางที่ 4.15 แบบตรวจสอบการระบุความเสี่ยงโครงการซอฟต์แวร์นั้น ยังมีหลักการและวิธีการมากมายสำหรับการระบุความเสี่ยง มีดังนี้

- ตรวจสอบองค์ประกอบของโครงสร้างของโครงการหยุดลงแต่ละอันเพื่อเปิดเผยความเสี่ยง
- ดำเนินการประเมินความเสี่ยงโดยใช้วิทยาศาสตร์หรือเทคนิคเกี่ยวกับการแบ่งประเภท (taxonomy) ความเสี่ยงหรืออนุกรมวิธานความเสี่ยง (Taxonomy)
- มีการสัมภาษณ์ผู้เชี่ยวชาญในเรื่องนั้นๆ
- ทบทวนความพยายามจัดการความเสี่ยงจากผลิตภัณฑ์ที่มีความคล้ายคลึงกัน
- ตรวจสอบการเอกสารการเรียนรู้หรือฐานข้อมูล
- ตรวจสอบการออกแบบข้อจำกัดและความต้องการในข้อตกลง

ความเสี่ยงของโครงการเกิดขึ้นในโยงใยที่ซับซ้อนของความเกี่ยวพันในเหตุและผล ซึ่งก่อให้เกิดห่วงโซ่ของการสะท้อนกลับในแต่ละวงจร ความเสี่ยงจึงเกิดขึ้นจากวงจรผลสะท้อนกลับหลากหลายที่อยู่ในระบบของโครงการซอฟต์แวร์

2.2 การประเมิน การจัดหมวดหมู่และการจัดลำดับความเสี่ยง

การประเมินและการจัดประเภทหรือหมวดหมู่แต่ละประเภทใช้กำหนดประเภทของความเสี่ยง ตัวแปร และกำหนดลำดับความสัมพันธ์ที่มีความเกี่ยวข้องกัน

การประเมินความเสี่ยงเป็นสิ่งจำเป็นเพื่อกำหนดความสำคัญในการระบุแต่ละความเสี่ยง และใช้ในการพิจารณาเมื่อมีความสนใจในการจัดการที่เหมาะสมของความต้องการ ประโยชน์ในการรวบรวมความเสี่ยงในก้านความสัมพันธ์กับบุคลากรและการพัฒนาในระดับรวม เมื่อความเสี่ยงรวมเกิดจากการสะสมของความเสี่ยงในระดับต่ำที่ต่ำกว่าการดูแล ควรจะให้ความสำคัญในความเสี่งระดับต่ำ ไม่มีการละเว้น

การประเมิน การจัดหมวดหมู่ และการจัดลำดับความสำคัญของความเสี่ยง บางครั้งเรียกว่า การประเมินความเสี่ยง (Risk assessment) หรือ การวิเคราะห์ความเสี่ยง (Risk Analysis) มีรายละเอียดในการตรวจสอบการประเมินความเสี่ยงดังตารางที่ 4.16

ตารางที่ 4.16 แบบตรวจสอบการประเมินความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	ชื่อความเสี่ยง		
2	ขอบเขต		
3	ลักษณะความเสี่ยง		
4	ผู้ที่มีผลกระทบ		
5	ลักษณะเชิงปริมาณ		
6	การยอมรับความเสี่ยง		
7	การบำบัดและการควบคุม		
8	แนวทางการปรับปรุง		
9	การพัฒนากลยุทธ์และนโยบาย		

การประเมินการระบุความเสี่ยงอาจทำได้โดยการกำหนดตัวแปรดังนี้ Low, Medium High, Negligible, Marginal, Significant, Critical, Catastrophic

การประเมินค่าความเสี่ยง (Risk evaluation) เมื่อได้ความเสี่ยง โดยมีรายละเอียด การประมาณเชิงกึ่งปริมาณแล้ว จึงนำมาประเมินค่าความเสี่ยงโดยการเปรียบเทียบกับหลักเกณฑ์ความเสี่งที่ยอมรับได้ หลักเกณฑ์ยอมรับความเสี่ยง (Risk acceptance criteria) ว่าจะยอมรับได้มากน้อย

เพียงใด เพื่อประกอบการตัดสินใจว่าจะบำบัดความเสี่ยงนั้นๆต่อไปอย่างไร พึงพิจารณาในแง่ต่างๆ ดังต่อไปนี้ เช่น ค่าใช้จ่าย ประโยชน์และความคุ้มทุนที่จะได้รับจากการแก้ไขบำบัดความเสี่ยง (costs and benefits) ข้อกำหนดด้านกฎหมายและกฎระเบียบขององค์กร (legal requirements) ปัจจัยด้านเศรษฐกิจและสังคม (socioeconomic factors) ปัจจัยด้านสิ่งแวดล้อม (environmental factors) ประเด็นสาระสำคัญในมุมมองของผู้มีส่วนได้เสีย (concerns of stakeholders) เป็นต้น

การจัดหมวดหมู่และกลุ่มความเสี่ยงเป็นสิ่งที่เห็นพ้องในการจัดหมวดหมู่ความเสี่ยงได้อย่างชัดเจน ความเสี่ยงได้ถูกจัดหมวดหมู่เพื่อกำหนดหมวดหมู่ความเสี่ยง โดยได้ทำการ จัดหาวิธีที่จะพิจารณาความเสี่ยงที่กำหนดจากแหล่งข้อมูล เทคนิคในการแบ่งหมวดหมู่ และส่วนประกอบของแผนงาน ความเกี่ยวข้องหรือความเสี่ยงที่มีค่าเท่ากันอาจจะเป็นกลุ่มความเสี่ยงที่จะประสบความสำเร็จได้อย่างมีประสิทธิภาพ อย่างไรก็ตามเอกสารเป็นสาเหตุและผลกระทบที่สัมพันธ์กันระหว่างความสัมพันธ์ความเสี่ยง ตารางที่ 4.17 แสดงแบบตรวจสอบการจัดหมวดหมู่ความเสี่ยง

ตารางที่ 4.17 แบบตรวจสอบการจัดหมวดหมู่ความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	องค์กรมีการจัดหาวิธีที่จะพิจารณาความเสี่ยงที่กำหนดจากแหล่งข้อมูล		
2	องค์กรมีเทคนิคในการแบ่งหมวดหมู่		
3	องค์กรมีรายละเอียดในส่วนประกอบของแผนงาน		

จัดลำดับความสำคัญ (Prioritize) แต่ละความเสี่ยงเพื่อกำหนดการปฏิบัติการหรือความพยายามที่ต้องการในการบริหารความเสี่ยง

ความสำคัญที่จะพิจารณาความเสี่ยงตามที่ได้กำหนดในแต่ละค่าความเสี่ยง หลักเกณฑ์ที่ชัดเจนควรที่จะใช้เพื่อกำหนดความเสี่ยงที่มีความสำคัญ เจตนารมณ์ของการจัดลำดับความสำคัญก็เพื่อกำหนดให้บริเวณพื้นที่มีประสิทธิภาพสูงสุดสำหรับลดความเสี่ยงที่ทรัพยากรสามารถแล้วนำมาใช้กับโครงการซอฟต์แวร์ซึ่งได้ผลดีที่สุด,

กำหนดชื่อความเสี่ยงแต่ละข้อโดยย่อ พร้อมระบุเลขที่เพื่อการอ้างอิงต่อไปในอนาคต ผู้ประเมินจะต้องพรรณารายละเอียดของแต่ละความเสี่ยง เพื่อให้เกิดความชัดเจนและเข้าใจความเสี่ยงนั้น โดยสมาชิกทีมงานช่วยกันจัดลำดับความสำคัญแต่ละความเสี่ยงดังตารางที่ 4.18

ตารางที่ 4.18 แบบตรวจสอบการจัดลำดับความสำคัญของความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	ความเสี่ยงจะต้องถูกขจัดให้หมดสิ้นไป หรือลดความเสี่ยงนั้นในทันทีทันใด (ระดับสูงสุด)		
2	ความเสี่ยงที่จำเป็นต้องตรวจสอบอย่างใกล้ชิด และอาจต้องมีแผนปฏิบัติการเพื่อป้องกันไม่ให้เกิดผลกระทบต่อโครงการ		
3	ความเสี่ยงที่จำเป็นต้องตรวจสอบ แต่เข้มนงวดน้อยและแผนการลดความเสี่ยงมีความเร่งด่วนน้อย		
4	ความเสี่ยงในระดับนี้อยู่ในระดับต่ำสุด และต้องการความเอาใจใส่เล็กน้อย แต่ไม่ควรละเลยทั้งหมด		

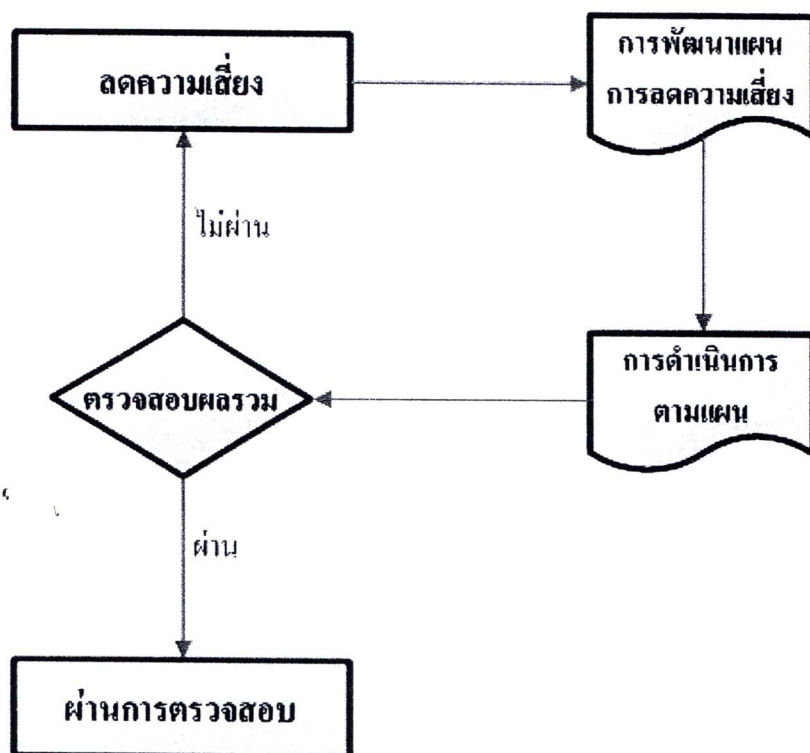
การจัดลำดับความสำคัญของความเสี่ยงช่วยให้การจัดลำดับความสำคัญเพื่อลดความเสี่ยงในลำดับต่อไปและมองเห็นความเสี่ยงในโครงการซอฟต์แวร์เช่น ความเสี่ยงนี้ร้ายแรง มีผลกระทบต่อความสำเร็จของโครงการซอฟต์แวร์และจะต้องดำเนินการแก้ไขทันที เพื่อเป็นประโยชน์แก่ ผู้บริหารจัดการโครงการซอฟต์แวร์ และสมาชิกทีมงานที่ให้ความสนใจหรือเน้นการบริหารความเสี่ยงโครงการซอฟต์แวร์ที่มีผลกระทบต่อโครงการซอฟต์แวร์มากที่สุด

3. การลดความเสี่ยง

ความเสี่ยงได้รับการจัดการและลด ตามความเหมาะสมเพื่อลดผลกระทบทางด้านสิ่งแวดล้อม ซึ่งที่ผลกระทบต่อวัตถุประสงค์

ขั้นตอนในการจัดการความเสี่ยงรวมถึงการพัฒนาตัวเลือกในการจัดการความเสี่ยง การตรวจสอบความเสี่ยง การกำหนดเกณฑ์กิจกรรมการจัดการความเสี่ยงที่มีประสิทธิภาพ เกินแผนการลดความเสี่ยงเป็นการพัฒนาและดำเนินการสำหรับเลือกความเสี่ยงที่มีบทบาทเพื่อลดผลกระทบที่จากความเสี่ยงที่เกิดขึ้น สิ่งเหล่านี้ยังรวมถึงแผนฉุกเฉินเพื่อรับมือกับผลกระทบจากความเสี่งถึงแม้จะพยายามละความเสี่ยงแล้วก็ตาม ตัวแปรความเสี่ยงที่ใช้ในการจัดการกิจกรรมความเสี่ยง ซึ่งมีการกำหนดเป็นกลยุทธ์ในการบริหารความเสี่ยง

การลดความเสี่ยงตามมาตรฐานซีเอ็มเอ็มไอจะทำการพัฒนาแผนการลดความเสี่ยงและการดำเนินการตามแผนการลดความเสี่ยงซึ่ง การออกแบบตรวจสอบจะมีขั้นตอนดังภาพที่ 4.6



ภาพที่ 4.6 แผนผังการลดความเสี่ยง

อย่างไรก็ตามการลดความเสี่ยงสามารถทำได้โดยใช้การควบคุมความเสี่ยงนั้น โดยสามารถเริ่มจากการวางแผนบริหารความเสี่ยง (Risk Management Planning) และ การหาทางแก้ไข ปัญหาความเสี่ยง (Risk Resolution) รวมไปถึงการเฝ้าสังเกตความเสี่ยง (Risk Monitoring) นั่นถือเป็นเรื่องสำคัญ โดยในการควบคุมความเสี่ยงนั้นถือเป็นเรื่องสำคัญเนื่องจากทำให้สามารถที่จะแก้ไขติดตามได้ทันทั่วทั้งที่

ทางเลือกเพื่อลดความเสี่ยงสามารถแบ่งทางเลือกในแผนการลดความเสี่ยงออกเป็น 6 ประเภท ซึ่งจะทำการตรวจสอบ โดยมีรายละเอียดการตรวจสอบดังตารางที่ 4.19

ตารางที่ 4.19 แบบตรวจสอบทางเลือกแผนลดความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	การยอมรับความเสี่ยง		
2	การหลีกเลี่ยงความเสี่ยง		
3	การจำกัดความเสี่ยง		
4	การวางแผนความเสี่ยง		
5	การวิจัยและการรับรู้ความเสี่ยง		
6	การถ่ายโอนความเสี่ยง		

จากตารางที่ 4.19 สามารถอธิบายแบบตรวจสอบในทางเลือกของแผนการลดความเสี่ยงได้โดยมีรายละเอียดดังต่อไปนี้

1. การยอมรับความเสี่ยง (Risk Assumption) คือการยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบข้อมูลสารสนเทศดำเนินงานไปตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ ID และ Password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้การให้ผู้ใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่าโรงพยาบาลอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร
2. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือการหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบัน โรงพยาบาล มีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็มถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการองค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ให้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น
3. การจำกัดความเสี่ยง (Risk Limitation) คือการทำระบบควบคุมเพื่อให้เกิดผลกระทบจากการการถูกคุกคามระบบหรือจากความไม่มั่นคงของระบบให้น้อยที่สุด
4. การวางแผนความเสี่ยง (Risk planning) คือการจัดการความเสี่ยงด้วยการพัฒนาแผนบรรเทาความเสี่ยงที่จัดลำดับความสำคัญ การใช้และการดูแลวิธีการควบคุม

5. การวิจัยและการรับรู้ความเสี่ยง (Research and Acknowledgement) คือการลดความสูญเสียที่เกิดจากความเสี่ยงโดยการตรวจสอบเพื่อรับทราบความอ่อนแอของระบบและค้นคว้าวิจัยให้ได้วิธีการควบคุมเพื่อเสริมความมั่นคงให้แก่ระบบ

6. การถ่ายโอนความเสี่ยง (Risk Transference) คือการถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสียเช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

3.1 การพัฒนาแผนการลดความเสี่ยง

การพัฒนาแผนการลดความเสี่ยงเกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ผู้บริหารธุรกิจจะต้องเป็นผู้รับผิดชอบการทำงานนี้ด้วยเงื่อนไขในการใช้งบประมาณที่ต่ำที่สุด (Least-cost) และใช้วิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผลกระทบต่อพันธกิจและทรัพยากรขององค์กรให้น้อยที่สุด

สำหรับการสร้างแบบตรวจสอบในส่วนของการพัฒนาแผนการลดความเสี่ยงจะมีรายละเอียดหลักๆ ดังตารางที่ 4.20

ตารางที่ 4.20 แบบตรวจสอบการพัฒนาแผนการลดความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีการกำหนดระดับและหลักเกณฑ์ที่กำหนดเมื่อความเสี่ยงเป็นที่ยอมรับไม่ได้และเรียกแผนปฏิบัติการลดความเสี่ยงหรือแผนฉุกเฉิน		
2	มีการระบุ บุคคลหรือกลุ่มบุคคลที่รับผิดชอบในแต่ละความเสี่ยง		
3	มีการกำหนดอัตราค่าใช้จ่ายเอประโยชน์ของการใช้แผนลดความเสี่ยงสำหรับแต่ละความเสี่ยง		
4	มีการพัฒนาแผนการลดความเสี่ยงโดยรวม สำหรับโครงการซอฟต์แวร์ของแต่ละแผนฉุกเฉินและแผนลดความเสี่ยง		
5	มีการพัฒนาแผนฉุกเฉินสำหรับการเลือกความเสี่ยงที่สำคัญในกรณีที่มีผลกระทบจะได้รู้ไว้และตระหนักถึง		

3.2 การดำเนินการตามแผนการลดความเสี่ยง

ในการดำเนินการตามแผนการลดความเสี่ยงนั้นเป็นการตรวจสอบสถานะของแต่ละระยะของความเสี่ยงและดำเนินการตามแผนการลดความเสี่ยงตามความเหมาะสม

การดำเนินการตามแผนการลดความเสี่ยง มีการควบคุมประสิทธิภาพและการบริหารความเสี่ยงในระหว่างการทำงาน เช่น การปฏิบัติตามโปรแกรมเชิงรุกเพื่อความสม่ำเสมอในการตรวจสอบสถานะความเสี่ยงและผลลัพธ์ของการปฏิบัติในการจัดการความเสี่ยง การกำหนดกลยุทธ์ในการบริหารความเสี่ยงเป็นช่วงเวลา สถานะความเสี่ยงควรได้รับการเยี่ยมชมอีกครั้ง กิจกรรมในการบริหารความเสี่ยงนี้อาจทำให้เกิดการค้นพบความเสี่ยงใหม่หรือค้นพบตัวเลือกในการจัดการความเสี่ยงใหม่ การค้นพบเหล่านี้สามารถที่จะเกิดความต้องการในการวางแผนอีกครั้งและการประเมินอีกครั้ง ในกรณีที่ยอมรับเกณฑ์ที่เกี่ยวข้องกับความเสี่ยง ควรจะมีการเปรียบเทียบกับสถานะความเสี่ยง เพื่อพิจารณาความจำเป็นในการดำเนินการตามแผนการลดความเสี่ยง การดำเนินการตามแผนลดความเสี่ยงสามารถปฏิบัติโดยมีรายละเอียดดังตารางที่ 4.21

ตารางที่ 4.21 แบบตรวจสอบการดำเนินการตามแผนการลดความเสี่ยง

ข้อ	คำถาม	ผ่าน	ไม่ผ่าน
1	มีการตรวจสอบสถานะความเสี่ยง		
2	มีการจัดการความเสี่ยงเปิดให้ปิดลงได้		
3	มีตัวเลือกเมื่อความเสี่ยงเกินกว่าเกณฑ์กำหนด		
4	มีการกำหนดเวลาถึงวันที่คาดว่าจะเสร็จ		
5	มีการดำเนินการอย่างต่อเนื่องในแต่ละกิจกรรมความเสี่ยง		
6	มีการจัดเก็บมาตรการที่มีประสิทธิภาพในแต่ละกิจกรรมความเสี่ยง		

จากตารางที่ 4.21 ในแบบตรวจสอบการดำเนินการตามแผนการลดความเสี่ยงสามารถอธิบายรายการตรวจสอบโดยมีรายละเอียดดังนี้

1. การตรวจสอบสถานะความเสี่ยงหลังจากเริ่มแผนลดความเสี่ยง ความเสี่ยงนั้นยังคงต้องมีการติดตามหลักเกณฑ์ ซึ่งหมายถึงการตรวจสอบการดำเนินการศักยภาพของแผนฉุกเฉินว่ามี การติดตามตามระยะกลไกที่ควรจะมีการทำงานอยู่
2. มีวิธีการจัดการความเสี่ยงเปิดและดำเนินการปิด ซึ่งอ้างอิงถึงการติดตามโครงการซอฟต์แวร์และบริเวณกระบวนการควบคุม ข้อมูลเพิ่มเติมเกี่ยวกับการดำเนินการรายการติดตาม

3. เลือกตัวเลือกการจัดการความเสี่ยงเมื่อตรวจสอบว่าความเสี่ยงเกินกว่าเกณฑ์กำหนด
4. กำหนดเวลาหรือระยะเวลาปฏิบัติงานสำหรับแต่ละกิจกรรมการจัดการความเสี่ยงซึ่งตั้งแต่วันเริ่มต้นจนถึงวันที่คาดว่าจะเสร็จ
5. มีความมุ่งมั่นในการดำเนินการที่ต่อเนื่องของแผนทรัพยากรเพื่อให้ประสบความสำเร็จในการดำเนินการ ในแต่ละกิจกรรมการจัดการความเสี่ยง
6. จัดเก็บมาตรการที่มีประสิทธิภาพในกิจกรรมการจัดการความเสี่ยง

