บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 กรอบงานโคบิต (CoBIT Framework) [1]

วัตถุประสงค์การควบคุมสำหรับสารสนเทศและเทคโนโลยีที่เกี่ยวข้อง หรือ โคบิต (Control Objective for Information and related Technology : CoBIT) ถูกจัดทำขึ้นโดยมีเนื้อหาเน้นไปในมุมมองทางด้านธุรกิจ โดยได้รับการออกแบบให้สามารถนำไปใช้ได้ไม่เพียงแต่สำหรับผู้ใช้งานในระบบและผู้ตรวจสอบเท่านั้น แต่ยังรวมถึงการให้แนวทางที่สมบูรณ์แก่ผู้บริหารและเจ้าของกระบวนการทางธุรกิจด้วย ซึ่งโดยส่วนใหญ่แล้วผู้บริหารจะมีความคาดหวังค่อนข้างสูงต่อประโยชน์ที่จะได้รับจากระบบเทคโนโลยีสารสนเทศที่นำมาใช้ ทั้งในด้านของการเพิ่มคุณภาพของข้อมูล ความง่ายในการปฏิบัติงาน ตลอดจนการลดระยะเวลาในการส่งมอบข้อมูลและระดับการให้บริการขององค์กรที่ดีขึ้นเรื่อย ๆ ใน ขณะที่สามารถรักษาต้นทุนให้อยู่ในระดับต่ำ ดังนั้นกรอบงานโคบิตจึงเป็นกรอบงานที่ช่วยให้องค์กรสามารถมั่นใจได้ว่าการนำเทคโนโลยีสารสนเทศเข้ามาใช้นั้นจะสามารถตอบสนองความต้องการทางธุรกิจได้อย่างเต็มที่ [7]

โคบิตสามารถตอบสนองความต้องการของผู้บริหาร ในการปิดช่องว่างระหว่างความจำเป็นของการควบคุม ความยุ่งยากด้านเทคนิค และความเสี่ยงของธุรกิจ โดยให้แนวทางการปฏิบัติที่ดีที่สุด (Best Practice) ทั้งในมุมมองด้านเทคโนโลยีและกรอบงานของกระบวนการที่เกี่ยวข้อง ซึ่งนำเสนอในลักษณะของกิจกรรมหรือขั้นตอนการปฏิบัติที่จัดการได้ง่ายและเป็นขั้นตอน เรียกว่าเป็นแนวทางปฏิบัติที่ดีที่สุดของโคบิต ซึ่งได้รับการยอมรับจากผู้ชำนาญงานในด้านการตรวจสอบเทคโนโลยีสารสนเทศทั่วโลก

วัตถุประสงค์อีกอย่างของกระบวนการที่ใช้ในการกำกับดูแลและควบคุมองค์กรที่ดี คือ ความต้องการที่จะเพิ่มมูลค่าให้กับองค์กรไปพร้อม ๆ กับการสร้างสมดุลที่ดีระหว่าง "ความเสี่ยง" และ "ผลตอบแทน" ที่จะได้รับจากเทคโนโลยีสารสนเทศและการปฏิบัติงานที่เกี่ยวข้องทั้งหมด ดังนั้นจำเป็นที่จะต้องมีการสร้างกระบวนการกำกับดูแลและการควบคุมภายในองค์กรที่ดี เพื่อให้แน่ใจได้ว่าสารสนเทศขององค์กรและเทคโนโลยีที่นำมาใช้ในการสนับสนุนวัตถุประสงค์ขององค์กรถูกใช้อย่างเต็มความสามารถ ทำให้เกิดข้อได้เปรียบทางธุรกิจและให้ประโยชน์สูงสุดแก่องค์กร

เพื่อให้การควบคุมภายในขององค์กรอยู่ในระดับที่น่าเชื่อถือและสามารถบรรลุวัตถุประสงค์หลักขององค์กรได้ การจัดการด้านทรัพยากรของเทคโนโลยีสารสนเทศจึงจำเป็นต้องมีการจัดกลุ่มประเภทของกระบวนการ ซึ่งแบ่งได้เป็น 4 โดเมน (Domains) และในแต่ละโดเมนก็จะ

มีการแบ่งออกเป็นวัตถุประสงค์การควบคุมหลัก (High-Level Control Objectives) รวมทั้งหมด 34 หัวข้อดังแสดงในรูปที่ 1 ซึ่งผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศจะนำกรอบงานโคบิตมาใช้ทวนสอบกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่องค์กรใช้งานอยู่ในปัจจุบัน เพื่อควบคุมให้กระบวนการทำงานด้านเทคโนโลยีสารสนเทศดำเนินไปอย่างถูกต้องและปลอดภัย นอกจากนี้กรอบงานโคบิตยังแสดงให้เห็นถึงความสัมพันธ์ต่อปัจจัยหลักที่เกี่ยวข้อง 2 ตัว ได้แก่ **เกณฑ์ของสารสนเทศที่ดี** (Information Criteria) และ **ทรัพยากรด้านเทคโนโลยีสารสนเทศ** (IT Resources) เพื่อให้ผู้ตรวจสอบเข้าใจว่าในแต่ละวัตถุประสงค์การควบคุมหลักมีปัจจัยตัวใดบ้างที่ต้องพิจารณา

รายละเอียดของกลุ่มประเภทกระบวนการทั้ง 4 โดเมน มีดังนี้

1) <u>การวางแผนและการจัดการองค์กร</u> (Planning and Organization)

เป็นการควบคุมในด้านของการวางแผนงานและการจัดการองค์กร โดยจะเน้นไปที่การตรวจสอบและควบคุมแผนงานรวมไปถึงกลยุทธ์ต่าง ๆ ที่ใช้ในองค์กร เพื่อให้การปฏิบัติงานภายในองค์กรสามารถทำให้บรรลุผลเป็นไปตามเป้าหมายหลักที่องค์กรได้วางไว้อย่างมีประสิทธิภาพสูงที่สุด ซึ่งประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 10 ข้อย่อย ดังนี้

- PO1 : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan)
- PO2 : การนิยามสถาปัตยกรรมด้านสารสนเทศ (Define the Information Architecture)
- PO3 : การกำหนดทิศทางด้านเทคโนโลยี (Determine Technological Direction)
- PO4 : การกำหนดโครงสร้างการจัดองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่น (Define the IT Processes, Organization and Relationships)
- PO5 : การจัดการการลงทุนด้านเทคโนโลยีสารสนเทศ (Manage the IT Investment)
- PO6 : การสื่อสารเป้าหมายและทิศทางการจัดการ (Communicate Management aims and Direction)
- PO7 : การจัดการทรัพยากรมนุษย์ (Manage IT Human Resources)
- PO8 : การจัดการคุณภาพ (Manage Quality)
- PO9 : การประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Assess and Manage IT Risks)
- PO10 : การจัดการโครงการ (Manage Projects)

2) <u>การจัดหาและการทำให้เกิดผล</u> (Acquisition and Implementation)

เป็นการควบคุมในด้านการจัดหาระบบงานและอุปกรณ์ต่าง ๆ ที่จะนำมาใช้ในองค์กร รวมถึงขั้นตอนในการนำระบบงานออกใช้งานจริงด้วย โดยจะเน้นไปที่การควบคุมขั้นตอนการจัดหาและการนำออกใช้งานให้สอดคล้องและเป็นไปตามแผนงานหรือนโยบายที่องค์กรได้ตั้งไว้ เพื่อให้สามารถมั่นใจได้ว่าระบบงานใหม่ที่จะนำมาใช้งานนั้นจะสามารถที่ตอบสนองและสอดคล้องกับวัตถุประสงค์หลักขององค์กรที่ได้ตั้งไว้ ซึ่งประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 7 ข้อย่อย ดังนี้

- AI1 : การกำหนดรายละเอียดของระบบที่ทำงานอัตโนมัติ (Identify Automated Solutions)
- AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ (Acquire and Maintain Application Software)
- AI3 : การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี (Acquire and Maintain Technology Infrastructure)
- AI4 : ความสามารถในการปฏิบัติการและการใช้งาน (Enable Operation and Use)
- AI5 : การจัดหาทรัพยากรด้านเทคโนโลยีสารสนเทศ (Procure IT Resources)
- AI6 : การจัดการการเปลี่ยนแปลง (Manage Changes)
- AI7 : การติดตั้งและการรับรองการแก้ปัญหาและการเปลี่ยนแปลง (Install and Accredit Solutions and Changes

3) <u>การส่งมอบและการสนับสนุน</u> (Delivery and Support)

เป็นการควบคุมในด้านการส่งมอบและสนับสนุนระบบงานต่าง ๆ ภายในองค์กร โดยจะเน้นไปที่การควบคุมการจัดการทรัพยากรต่าง ๆ ภายในองค์กร เพื่อให้ระบบเทคโนโลยีและสารสนเทศต่าง ๆ สามารถทำงานได้อย่างต่อเนื่อง รวมถึงการเน้นในด้านของความปลอดภัยของระบบงานที่ใช้งานอยู่ในองค์กรเพื่อให้สามารถมั่นใจได้ว่าระบบงานต่าง ๆ จะปลอดภัยจากการโจมตีของผู้บุกรุก หรือ จากภัยธรรมชาติต่าง ๆ ซึ่งประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 13 ข้อย่อย ดังนี้

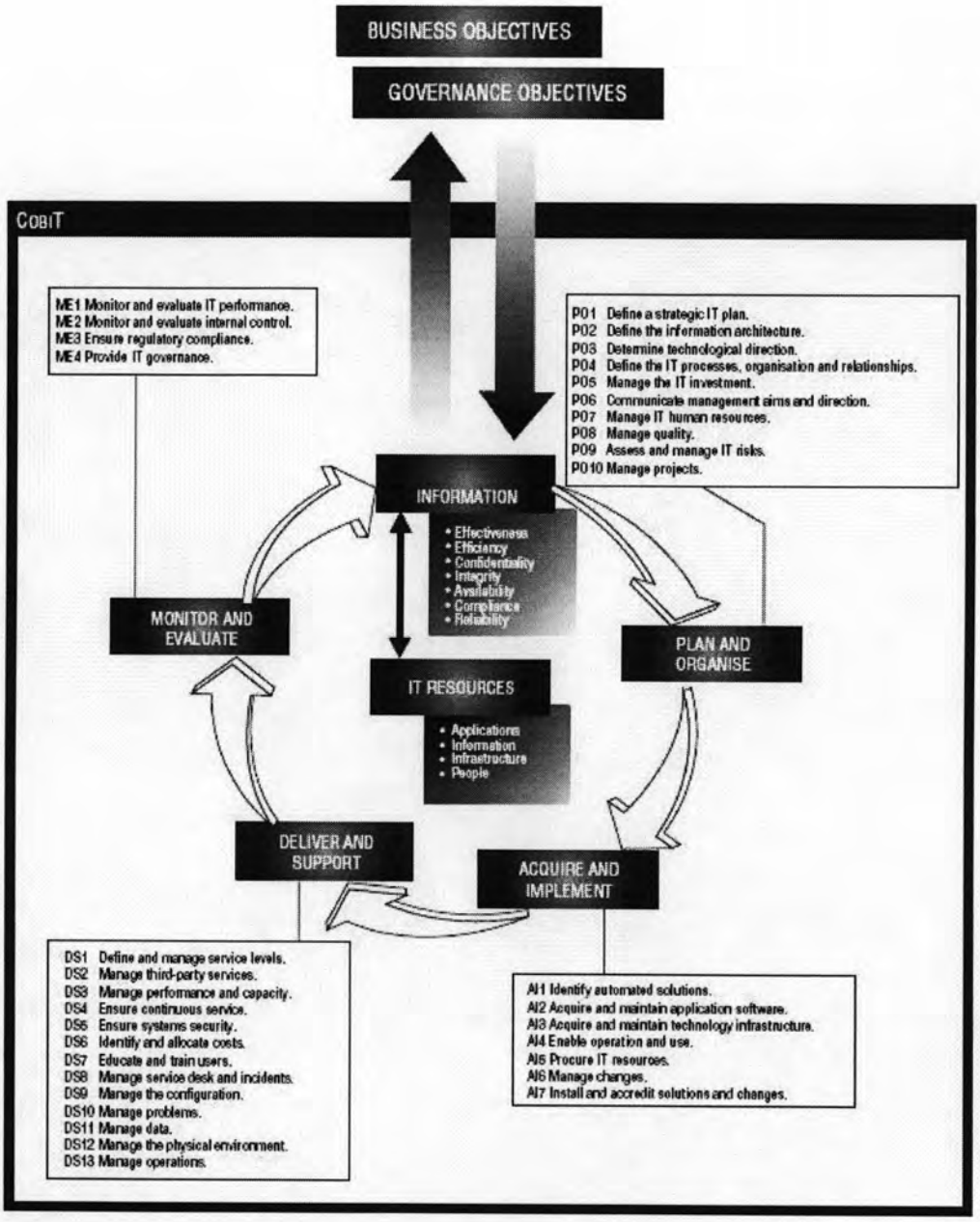
- DS1 : การนิยามและจัดการระดับการให้บริการ (Define and Manage Service Levels)
- DS2 : การการจัดการบริการจากบุคคลที่สาม (Manage Third-Party Services)

- DS3 : การจัดการด้านสมรรถนะและความสามารถของระบบ (Manage Performance and Capacity)
- DS4 : ความต่อเนื่องในการให้บริการ (Ensure Continuous Service)
- DS5 : การรักษาความปลอดภัยระบบ (Ensure Systems Security)
- DS6 : การกำหนดและการจัดสรรต้นทุน (Identify and Allocate Costs)
- DS7 : การให้ความรู้และการฝึกอบรมแก่พนักงาน (Educate and Train Users)
- DS8 : การจัดการด้านการให้ความช่วยเหลือและรับมือเหตุการณ์ (Manage Service Desk and Incidents)
- DS9 : การจัดการรายละเอียดทรัพย์สิน (Manage the Configuration)
- DS10 : การจัดการปัญหา (Manage Problems)
- DS11 : การจัดการข้อมูล (Manage Data)
- DS12 : การจัดการสภาพแวดล้อมด้านกายภาพ (Manage the Physical Environment)
- DS13 : การจัดการการปฏิบัติการ (Manage Operations)

4) <u>การติดตามและประเมินผล</u> (Monitoring and Evaluate)

เป็นการควบคุมในด้านการตรวจสอบและประเมินผลของการปฏิบัติงานในด้านต่าง ๆ ภายในองค์กร โดยจะเน้นไปที่การตรวจสอบและติดตามการทำงานภายในองค์กรเพื่อพัฒนาการปฏิบัติงานให้มีประสิทธิภาพมากขึ้น และเพื่อให้การปฏิบัติงานต่าง ๆ สามารถดำเนินไปได้อย่างสอดคล้องกับนโยบายหรือมาตรฐานสากลต่าง ๆ ทั้งภายในและภายนอกองค์กร ซึ่งประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 4 ข้อย่อย ดังนี้

- ME1 : การติดตามและประเมินประสิทธิภาพของระบบเทคโนโลยีสารสนเทศ (Monitor and Evaluate IT Performance)
- ME2 : การติดตามและประเมินการควบคุมภายใน (Monitor and Evaluate Internal Control)
- ME3 : การแน่ใจว่าองค์กรปฏิบัติตามกฎระเบียบ (Ensure Regulatory Compliance)
- ME4 : การจัดให้องค์กรมีหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (Provide IT Governance)



รูปที่ 1 ภาพรวมของกรอบงานโคบิต

2.1.2 **การประเมินความเสี่ยง** (Risk Assessment)

ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งมีผลทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อองค์กร [2]

การประเมินความเสี่ยงเป็นขั้นตอนที่ระบุอันดับความเสี่ยงของอันตรายทั้งหมดที่เกี่ยวข้องกับการปฏิบัติงานที่มีภายในองค์กร ซึ่งครอบคลุมทั้งในส่วนของสถานที่ เครื่องจักร อุปกรณ์

บุคลากร และขั้นตอนการทำงาน ที่อาจก่อให้เกิดความเสียหายร้ายแรงต่อองค์กรทั้งในด้านของทรัพย์สิน หรือต่อสิ่งแวดล้อมต่าง ๆ ภายในองค์กรได้ [3] ซึ่งขั้นตอนดังกล่าวจะเป็นวิธีที่ใช้ในการประเมินความเสี่ยงของการควบคุมภายในองค์กรว่ามีการปฏิบัติงานในส่วนใดบ้างที่มีความเสี่ยงที่จะเกิดข้อผิดพลาดในการปฏิบัติงานขึ้น เมื่อผู้ตรวจสอบทำการประเมินความเสี่ยงแล้วจะทำให้ทราบได้ว่าควรจะดำเนินการตรวจสอบที่จุดใดก่อน เพื่อป้องกันความเสียหายที่มีโอกาสเกิดขึ้นมากที่สุดหรือร้ายแรงที่สุดก่อน และธนาคารแห่งประเทศไทยได้มีการกำหนดให้ผู้ตรวจสอบต้องทำการประเมินความเสี่ยงก่อนที่จะทำการตรวจสอบในด้านต่าง ๆ เพื่อให้สามารถลดความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นได้อย่างถูกต้อง

วิธีที่ใช้ในการประเมินความเสี่ยงสามารถทำได้หลายวิธี แต่โดยส่วนใหญ่แล้วจะมีลักษณะที่คล้ายคลึงกันโดยกรอบงานการวิเคราะห์ความเสี่ยง (Risk Assessment Framework) จะมีลักษณะเป็นวงจร ดังรูปที่ 2

รูปที่ 2 กรอบงานการวิเคราะห์ความเสี่ยง [4]

รูปที่ 2 แสดงขั้นตอนของวงจรการประเมินความเสี่ยงตามกรอบงานการวิเคราะห์ความเสี่ยงเริ่มต้นด้วยการตีค่าสินทรัพย์ (Asset Valuation) ที่มีอยู่ในองค์กรทั้งหมด (รวมทั้งส่วนที่เป็นทรัพย์สิน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ด้านเทคโนโลยีสารสนเทศต่าง ๆ และส่วนที่ไม่ใช่ทรัพย์สิน เช่น ขั้นตอนการปฏิบัติงาน การควบคุมภายในขององค์กร เป็นต้น) เมื่อประเมินครบทั้งหมดแล้วก็จะมาดูว่าในสินทรัพย์แต่ละตัวยังมีจุดอ่อนหรือข้อบกพร่องอะไรบ้าง (Vulnerability Assessment) ซึ่งการประเมินสินทรัพย์นี้สามารถใช้การประเมินการคุกคาม (Threat Assessment) ต่าง ๆ ว่ามีการกระทำใดบ้างที่จะทำให้เกิดผลเสียต่อสินทรัพย์นั้น ๆ ได้ จากนั้นก็จะเข้าสู่ขั้นตอนการประเมินความเสี่ยง (Risk Assessment) ว่ามีความเสี่ยงใดบ้างที่สามารถเกิดขึ้นได้ แล้วจึงมาทำการประเมินการควบคุมที่มีอยู่ (Control Evaluation) ว่าในปัจจุบันองค์กรมีการ

ควบคุมใดอยู่บ้าง เพื่อให้ได้ความเสี่ยงที่ยังเหลืออยู่ (Residual Risk) จากนั้นจะนำความเสี่ยงดังกล่าวมาทำการวิเคราะห์ตามหลักของกรอบงานโคบิตเพื่อให้ได้ออกมาเป็นแผนการปฏิบัติ (Action Plan) แล้วจึงนำแผนปฏิบัติที่ได้ไปดำเนินการ เพื่อลดความเสี่ยงนั้น ๆ ให้น้อยลง หลังจากนั้นก็จะทำการประเมินตามขั้นตอนข้างต้นใหม่อีกครั้งเพื่อดูว่าความเสี่ยงนั้นลดลงหรือไม่

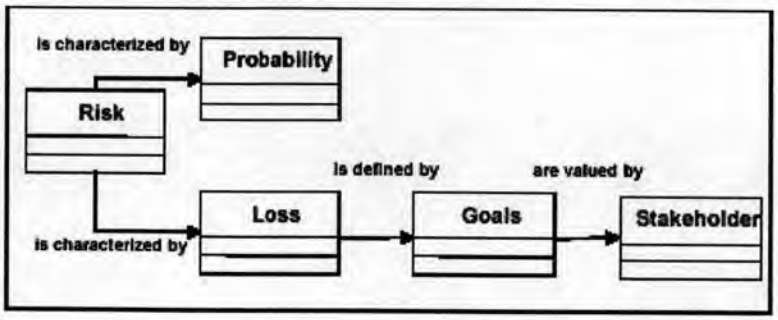
2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 Experiences in improving risk management processes using concepts of the Riskit method [5]

งานวิจัยนี้เป็นการนำเสนอวิธีการที่ใช้ในการจัดการความเสี่ยง (Risk management method) โดยใช้หลักของ Riskit method ซึ่งเป็นวิธีการหนึ่งที่ใช้ในกระบวนการพัฒนาซอฟต์แวร์ วิธีการนี้ถูกออกแบบมาโดยมีวัตถุประสงค์เพื่อให้ผู้ปฏิบัติงานสามารถเข้าใจรายละเอียดหรือส่วนประกอบของความเสี่ยงต่าง ๆ ได้โดยง่าย และวิธีการนี้ยังช่วยในการลดข้อจำกัดหรือปัญหาที่พบในวิธีการจัดการความเสี่ยงแบบอื่น ๆ ได้ เช่น ความไม่เป็นกลางในการจัดอับดับความเสี่ยง (Biased ranking table) เป็นต้น ซึ่งในงานวิจัยชิ้นนี้ได้อธิบายถึงลักษณะเด่นของวิธีการจัดการความเสี่ยงแบบ Riskit method ซึ่งแตกต่างจากวิธีการจัดการความเสี่ยงแบบอื่น ๆ ดังนี้

(1) Riskit method มีวิธีการหรือรูปแบบที่ใช้ในการ "นิยามความเสี่ยง" อย่างเป็นระบบ

(2) Riskit method สามารถทำการวิเคราะห์ได้ว่าผู้ที่มีส่วนเกี่ยวข้อง (Stakeholder) ต่าง ๆ มีความเกี่ยวข้องกับความเสี่ยงต่าง ๆ อย่างไร ซึ่งสามารถสร้างออกมาให้อยู่ในรูปของแผนภาพตามรูปที่ 3 ได้ จากข้อมูลดังกล่าวจะทำให้ทราบถึงรายละเอียดต่าง ๆ ของความเสี่ยงได้ และสามารถสืบกลับไปได้ว่าความเสี่ยงดังกล่าวมีความเกี่ยวข้องกับเป้าหมายใดของผู้ที่เกี่ยวข้องบ้าง เป็นต้น (ซึ่งงานวิจัยชิ้นนี้จะนำรูปแบบในการนิยามความเสี่ยงด้วยวิธีนี้มาประยุกต์ใช้)



รูปที่ 3 การนิยามความเสี่ยงตามวิธีของ Riskit [6]