# บทที่ 2
# แนวคิด ทฤษฎี เอกสาร และงานวิจัยที่ข้อง

ในการศึกษาเรื่องการบริหารความเสี่ยงของคณะพยาบาลศาสตร์ มหาวิทยาลัยเชียงใหม่ ผู้ศึกษาได้ศึกษาจาก บทความทางวิชาการเกี่ยวกับการบริหารความเสี่ยง เอกสารแนวทางการบริหารความเสี่ยง คู่มือเกี่ยวกับการบริหารความเสี่ยง คู่มือเกี่ยวกับการประกันคุณภาพการศึกษา เอกสารแผนการบริหารจัดการเชิงกลยุทธ์ งานวิจัยที่เกี่ยวข้อง และข้อมูลออนไลน์ มาประกอบการศึกษา ดังนี้

2.1 ความหมายและคำจำกัดความของการบริหารความเสี่ยง

2.2 การบริหารความเสี่ยงด้านการบริหารจัดการ

2.3 การบริหารความเสี่ยงด้านการปฏิบัติการ

2.4 แนวคิดทฤษฎีการบริหารความเสี่ยงตามแนวทางของ COSO (Committee of Sponsorin Organization of the Treadway Commission)

2.5 งานวิจัยที่เกี่ยวข้อง

2.6 กรอบแนวคิด

2.7 นิยามศัพท์ปฏิบัติการ

## 2.1 ความหมายและคำจำกัดความของการบริหารความเสี่ยง

2.1.1 ความหมายของความเสี่ยง

ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กร
(คู่มือการบริหารความเสี่ยงมหาวิทยาลัยเชียงใหม่, 2553)

ความเสี่ยง หมายถึง เหตุการณ์หรือสถานการณ์ที่มีความไม่แน่นอน ซึ่งอาจเกิดขึ้นและมีผลทำให้หน่วยรับตรวจเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า ไม่สามารถดำเนินงานให้บรรลุผลสำเร็จตามวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้ได้ (สำนักงานการตรวจเงินแผ่นดิน, 2544)

ความเสี่ยง หมายถึง สถานการณ์ที่มีความเป็นไปได้ที่จะเปิดเหตุการณ์ที่ไม่พึงประสงค์ไปจากผลลัพธ์ที่คาดหวังไว้ (Vaughan, 1997)

ความเสี่ยง หมายถึง โอกาสที่จะประสบกับการบาดเจ็บหรือความเสียหาย เหตุร้าย อันตราย ความสูญเสีย รวมทั้งโอกาสที่จะเผชิญกับความไม่แน่นอน หรือการเปิดเผยต่าง ๆ ซึ่งเป็นสิทธิส่วนบุคคล (กฤษดา แสวงดี, 2542)

ความเสี่ยง หมายถึง แนวโน้มของการเกิดผลลัพธ์ไม่ต้องการ และไม่คาดหวัง ที่อาจเป็นอันตรายต่อความเป็นอยู่ที่ดี หรือสุขภาพที่ดี อันตรายต่อทรัพย์สินขององค์กร และบุคคล (Wilson, 1999)

ความเสี่ยง หมายถึง โอกาสที่จะประสบกับความสูญเสีย หรือสิ่งที่ไม่พึงประสงค์ (อนุวัฒน์ ศุภชุติกุล, 2543)

ความเสี่ยง จำแนกได้เป็น 4 ลักษณะ ดังนี้ (คู่มือการบริหารความเสี่ยง มหาวิทยาลัยเชียงใหม่, 2553)

1) ความเสี่ยงด้านยุทธศาสตร์ (Strategic Risk) หมายถึง ความเสี่ยงทีเกี่ยวข้องในระดับยุทธศาสตร์

2) ความเสี่ยงด้านปฏิบัติงาน (Operational Risk) หมายถึง ความเสี่ยงที่ เกี่ยวข้องในระดับปฏิบัติการ

3) ความเสี่ยด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงที่เกี่ยวข้องกับด้านการเงิน

4) ความเสี่ยงด้านความปลอดภัยจากอันตรายต่อชีวิตและทรัพย์สิน (Hazard Risk) หมายถึง ความเสี่ยงที่เกี่ยวข้องในด้านความปลอดภัยจากอันตรายต่อชีวิตและทรัพย์สิน

โดยสรุป ความเสี่ยง หมายถึง โอกาสที่จะเกิดความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ถ้าหากเกิดขึ้นแล้วและเกิดผลกระทบจะทำให้ไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าประสงค์ขององค์กรได้

2.1.2 คำจำกัดความการบริหารความเสี่ยง

ซูลีแวน และเดคเคอร์ (Suliivan & Decker, 1992) กล่าวว่า การบริหารความเสี่ยง หมายถึง โปรแกรมที่จัดทำเพื่อป้องกัน และควบคุมการสูญเสียที่อาจเกิดขึ้นขององค์กร

วิลสัน (Wilson, 1992) กล่าว่า การบริหารความเสี่ยง หมายถึง ความพยายามที่จะลดจำนวนและความรุนแรงของอุบัติเหตุ และเหตุการณ์ที่เกิดขึ้น เพื่อป้องกันการเสียทรัพย์สินและจำกัดความเสียหายที่จะเกิดขึ้นต่อบุคลากร ระบบการปฏิบัติงาน และผู้รับบริการ รวมทั้งการลดการถูกฟ้องร้องทางกฎหมาย และการเสื่อมเสียชื่อเสียงขององค์กร

อนุวัฒน์ ศุภชุติกุล (2543) กล่าวว่า การบริหารความเสี่ยง หมายถึง การรับรู้และจำกัดความเสี่ยง เพื่อลดโอกาส และปริมาณของความสูญเสียที่เกิดขึ้น

ไพร้ซวอเตอร์เฮาส์คูเปอร์ส (2547) กล่าวว่า การบริหารความเสี่ยง หมายถึง กระบวนการที่ปฏิบัติโดยคณะกรรมการบริษัท ผู้บริหาร และบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

ชัยเสฏฐ์ พรหมศรี (2550) การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบและได้รับการวางแผน เพื่อใช้ในการลด หรือขจัดความน่าจะเป็น หรือโอกาสที่ความสูญเสียจะเกิดขึ้นในสถานที่ใดสถานที่หนึ่ง อาจกล่าวได้ว่า การบริหารความเสี่ยง คือหลักเกณฑ์ที่ใช้รับมือกับความเป็นไปได้ของเหตุการณ์ในอนาคตที่เป็นสาเหตุของภัยและอันตรายต่าง ๆ

กล่าวโดยสรุป การบริหารความเสี่ยง หมายถึง กระบวนการที่เป็นระบบและได้รับการวางแผน อย่างเป็นระบบ โดยผู้บริหาร และบุคลากรทุกคนในองค์กร เพื่อลดหรือป้องกันความผิดพลาดหรือความสูญเสียที่เกิดขึ้นจากการปฏิบัติงาน ซึ่งจะส่งผลให้เกิดการบาดเจ็บหรืออันตรายต่อบุคคลและองค์กร

ความเสี่ยงเป็นส่วนหนึ่งขององค์กรเช่นเดียวกับการเป็นส่วนหนึ่งของชีวิตของคนเรา เราจึงไม่สามารถหลีกเลี่ยงความเสี่ยงได้ทั้งหมด ซึ่งการบริหารความเสี่ยง มีหลายวิธี ดังนี้

1. การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

2. การลด/การควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบ ให้อยู่ในระดับที่องค์กรยอมรับได้

3. การกระจายความเสี่ยง หรือการโอนความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบไป

4. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงมาก และหน่วยงานไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมนั้นไป

2.1.2 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

2.1.3 การประเมินความเสี่ยง ( Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยงโดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

ผลกระทบ (Impact) หมายถึงขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้น หากเกิดเหตุความเสี่ยง

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น 4 ระดับคือ สูงมาก สูง ปานกลาง และน้อย

2.1.4 การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่าง ๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่องค์กรจะเกิดความเสียหาย ให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้ อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมาย ทั้งในด้านกลยุทธ์ การปฏิบัติตามกฎระเบียบ การเงิน และชื่อเสียงเกียรติภูมิขององค์กรเป็นสำคัญ โดยได้รับการสนับสนุนและการมีส่วนร่วมในการบริหารความเสี่ยงจากหน่วยงานทุกระดับทั่วทั้งองค์กร ได้แก่

1) การควบคุมเพื่อป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

2) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้น เพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

3) การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

4) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น เพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

(คู่มือการบริหารความเสี่ยงมหาวิทยาลัยเชียงใหม่, 2553)



**2.2 การบริหารความเสี่ยงด้านการบริหารจัดการ และการบริหารความเสี่ยงด้านปฏิบัติการ**

(วิฑูรย์ สมโต, 2551)

2.2.1 การบริหารความเสี่ยงด้านการบริหารจัดการ

การบริหารความเสี่ยงด้านการบริหารจัดการ คือ การบริหารความเสี่ยงที่เกิดจากการไม่สามารถบริหารกระบวนการดำเนินงานขององค์กรที่เป็นระบบและต่อเนื่อง เพื่อช่วยให้กิจการลดความสูญเสียที่อาจเกิดขึ้นจากความเสี่ยงต่าง ๆ ให้เหลือน้อยที่สุดหรืออยู่ในระดับที่ยอมรับได้ และเพิ่มโอกาสให้แก่ธุรกิจมากที่สุด ตลอดจนเป็นองค์ประกอบสำคัญในการกำกับดูแลองค์กรที่ดี ที่จะช่วยให้กิจการบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้อย่างมีประสิทธิภาพ และประสิทธิผล ความเสี่ยงที่ทำให้องค์กรไม่บรรลุตามวัตถุประสงค์และเป้าหมาย อย่างเช่น

- ความผิดพลาด เรื่อง การกำหนดนโยบาย การกำหนดโครงสร้างการจัดการ
- การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี
- ความเสี่ยงจากการบริหารจัดการในกระบวนการทำงานต่างๆ ที่ไม่มีประสิทธิภาพ
- การจัดสรรบุคลากรที่ขาดทักษะในการทำงาน และมีอัตราการเข้า – ออกสูง
- การไม่มีระบบการควบคุมภายในในกิจการ

ในอดีตสภาพแวดล้อมการแข่งขันไม่รุนแรง องค์กรต่าง ๆ เพียงแต่ดำเนินงานให้บรรลุเป้าหมายก็เพียงพอ แต่ความรุนแรงของการแข่งขันและความผันผวนของสภาพแวดล้อมในปัจจุบันและจะมีความซับซ้อนมากขึ้นในอนาคต ทำให้ธุรกิจต้องดำเนินงานอย่างมีประสิทธิภาพและมีทิศทางที่ชัดเจน การจัดการจึงเป็นเครื่องมือหนึ่งในการแก้ปัญหา และสร้างความก้าวหน้าแก่ธุรกิจ แต่ถึงแม้จะมีกระบวนการทางด้านการจัดการซึ่งกำหนดขึ้นโดยผู้บริหาร ก็ไม่จำเป็นเสมอไปว่าธุรกิจนั้นจะสามารถประสบผลสำเร็จ เนื่องจากมีปัจจัยความเสี่ยงด้านการบริหารจัดการหลายๆด้านทั้งภายนอกและภายในองค์กร ที่มีผลกระทบต่อการบริหารจัดการผู้บริหารและคณะกรรมการจะต้องใช้ความสามารถในการกำหนดกระบวนการจัดการจัดการในหน้าที่ที่สำคัญ 5 หน้าที่ ได้แก่

การวางแผน (Planning) เป็นหน้าที่ทางการจัดการหน้าที่แรกที่กำหนดทิศทางภารกิจ เป้าหมาย และวัตถุประสงค์ขององค์กร ตลอดจดกรอบความคิด แนวทาง และวิธีปฏิบัติ เพื่อให้ดำเนินงานบรรลุผลสำเร็จตามที่ต้องการ

การจัดองค์กร (Organizing) เป็นการจัดทำโครงสร้างองค์กร และกำหนดระบบงาน บทบาท อำนาจหน้าที่ความรับผิดชอบ และหน้าที่ของบุคลากร เพื่อให้การปฏิบัติงานเป็นระบบและสอดคล้องกันภายในหน่วยงาน ซึ่งจะทำให้องค์กรสามารถดำเนินงานสู่เป้าหมายร่วมกัน และใช้ทรัพยากรอย่างมีประสิทธิภาพ

การจัดบุคคลเข้าทำงาน (Staffing) เป็นการจัดบุคคลให้เหมาะสมกับงานทั้งในด้านคุณภาพ ได้แก่ ความรู้ ทักษะความสามารถ ประสบการณ์ และปริมาณแรงงานที่ต้องการ หรือเรียกว่า “การจัดคนให้เหมาะสมกับงาน (Put the right man on the right job)” ตลอดจนธำรงรักษาและพัฒนาแรงงานที่มีคุณภาพให้อยู่กับองค์กรอย่างต่อเนื่อง

การนำ (Leading) เป็นการใช้อิทธิพลและความสัมพันธ์ระหว่างผู้นำและผู้ตาม ในการบ่งชี้เป้าหมาย ชักจูงและเปลี่ยนแปลงผู้ติดตามหรือผู้ใต้บังคับบัญชาให้ปฏิบัติงานอย่างเต็มความสามารถด้วยความเต็มใจซึ่งจะก่อให้เกิดประโยชน์แก่องค์กรอย่างเต็มที่

การควบคุม (Controlling) เป็นกระบวนการในการกำหนดเกณฑ์และมาตรฐานขั้นตอนการติดตามตรวจสอบ ประเมิน และแก้ไขให้การดำเนินงานสามารถบรรลุเป้าหมาย หรือปรับปรุงแผนและการดำเนินงานให้สอดคล้องกับข้อจำกัดของเหตุการณ์ และสภาพแวดล้อมจริงนอกจากการจัดกระบวนการบริหารจัดการผู้บริหารและคณะกรรมการยังมีหน้าที่ในการควบคุม และรับผิดชอบการดำเนินงาน โดยรวมขององค์กร ดังนั้น จะต้องมีการกำหนดวิธีการควบคุม อย่างเช่น ระบบการบริหารความเสี่ยง ระบบการควบคุมภายใน ระบบการรายงาน ระบบการสอบทาน การวิเคราะห์ และระบบประเมินผลการดำเนินงาน เป็นต้น ซึ่งระดับความเสี่ยงจะมีลักษณะตรงกันข้ามกับการควบคุมภายใน คือ ถ้าพื้นที่ใดมีการควบคุมภายในที่เหมาะสมความเสี่ยงจะมีระดับต่ำ แต่ถ้าพื้นที่ใดมีจุดอ่อนของระบบควบคุมภายในหรือมีข้อบกพร่องโอกาส โอกาสที่จะเกิดความเสี่ยงย่อมมีสูง ดังนั้นจึงควรจะมีการประเมินสม่ำเสมอและรายงานผลให้ทราบทั้งองค์กร เพื่อใช้เครื่องมือเหล่านี้เป็นช่วยในการควบคุมความเสี่ยงที่อาจจะเกิดขึ้น และนำสิ่งที่ได้มาทำการปรับปรุงแก้ไข และใช้ในการวางแผนเพื่อรองรับกับสภาพแวดล้อมการดำเนินธุรกิจมีการเปลี่ยนแปลงเสมอ

กล่าวโดยสรุป การที่ผู้บริหารจะบริหารความเสี่ยงด้านการบริหารจัดการขององค์กร ให้ประสบผลสำเร็จได้นั้น ผู้บริหารจะต้องมีความสามารถในการบริหารจัดการหลาย ๆ ด้านทั้งภายนอกและภายในองค์กร โดยจะต้องมีการวางแผน การจัดการองค์กร การจัดบุคคลเข้าทำงาน จากนั้นจึงใช้ความเป็นผู้นำขององค์กร สุดท้ายก็คือการควบคุมความเสี่ยงที่อาจจะเกิดขึ้นในองค์กร

2.2.2 การบริหารความเสี่ยงด้านการปฏิบัติการ

การบริหารความเสี่ยงด้านการปฏิบัติการ คือ การบริหารความเสี่ยงจากการปฏิบัติงาน ที่เกิดจากความผิดพลาดในการกระบวนการดำเนินงาน และก่อให้เกิดความเสียหายแก่องค์กร โดยข้อผิดพลาดอาจเนื่องมาจากทางเทคนิคหรือจากผู้ปฏิบัติงาน ที่มีการละเมิดกฎระเบียบ กฎหมาย ระเบียบข้อบังคับและข้อกำหนดของทางการหรือเกิดการทุจริตของบุคลากรในองค์กร ความเสี่ยงด้านการปฏิบัติงาน อย่างเช่น

- พนักงานขาดความรับผิดชอบในหน้าที่ที่ได้รับมอบหมาย
- พนักงานไม่เข้าใจในระเบียบการปฏิบัติงานอย่างแท้จริง
- พนักงานฝ่าฝืนกฎระเบียบ ข้อบังคับโดยจงใจ
- พนักงานทุจริต และขาดระบบการตรวจสอบภายใน

-ไม่มีการควบคุมการจัดทำรายงานของเจ้าหน้าที่และไม่จัดส่งรายงานภายในเวลากำหนด

- แบบรายงานที่จัดทำขาดการควบคุมและติดตามอย่างใกล้ชิด

เนื่องจากการบริหารความเสี่ยงด้านปฏิบัติการ เป็นความเสี่ยงที่สามารถควบคุมได้ภายใต้การบริหารจัดการที่ดี และทำให้เกิดความพึงพอใจแก่ผู้ปฏิบัติงาน ซึ่งจะส่งผลต่อผลงานที่ได้รับในองค์กร ดังนั้น องค์กรควรมีระบบการควบคุมภายใน และมีการประเมินความเสี่ยงที่อาจเกิดขึ้น และทำให้ติดตาม ตรวจสอบ และสรุปผลการปฏิบัติงานของแต่ละบุคคล ว่าเป็นไปตามวัตถุประสงค์และเป้าหมายขององค์กรที่กำหนดไว้ เพื่อเป็นข้อมูลย้อนกลับในการปฏิบัติงานของบุคคล และจัดให้มีอบรมและพัฒนาฝ่ายปฏิบัติงาน ให้มีความรู้ ทักษะ และความสามารถในการทำงานเหมาะสมกับงานที่กำหนด และควรกำหนดผลตอบแทนให้แก่พนักงานอย่างเหมาะสม เพื่อไม่ให้เกิดการเข้า-ออกของพนักงานในอัตราที่สูง ซึ่งจะทำให้องค์กรสูญเสียทรัพยากรเพิ่มขึ้นและการดำเนินงานขาดความต่อเนื่อง

กล่าวโดยสรุป การบริหารความเสี่ยงด้านปฏิบัติการ เป็นความเสี่ยงที่ควบคุมได้ภายใต้การบริหารจัดการที่ดี พร้อมทั้งทำให้เกิดความพึงพอใจแก่ผู้ปฏิบัติงาน ทั้งนี้ทั้งนั้นองค์กรก็จะต้องมีระบบการควบคุมภายในที่ดี พร้อมทั้งมีการประเมินความเสี่ยงที่อาจจะเกิดขึ้น ติดตาม ตรวจสอบตลอดจนสรุปผลการปฏิบัติงานของผู้ปฏิบัติงานแต่ละคน ให้เป็นไปตามวัตถุประสงค์และเป้าหมายขององค์กร

**2.3 แนวคิดทฤษฎีการบริหารความเสี่ยงตามแนวทางของ** COSO (Committee of Sponsoring Organization of the Treadway Commission) (ดารณี ชัยวัฒนาโรจน์, 2550)

COSO ได้กำหนดนิยามของการบริหารความเสี่ยง (Enterprise Risk Management) ไว้ว่าเป็นกระบวนการที่ปฏิบัติโดยคณะกรรมการบริษัทผู้บริหารและบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร และสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้ ซึ่งประกอบด้วยแนวคิดพื้นฐาน คือ

1) กระบวนการ การบริหารความเสี่ยงเป็นเครื่องมือซึ่งนำไปสู่จุดหมาย มิใช่เป็นจุดหมายด้วยตัวเอง การบริหารความเสี่ยงขององค์กรไม่ได้จำกัดสำหรับเหตุการณ์ใดเหตุการณ์หนึ่ง แต่เป็นกระบวนการที่สามารถปรับเปลี่ยนอยู่ตลอดเวลา เพื่อให้สอดคล้องกับการใช้ทรัพยากร และการปฏิบัติงานขององค์กร

2) เกิดจากบุคคล การบริหารความเสี่ยงมิใช่เป็นเพียงนโยบาย การสำรวจความคิดเห็น หรือเป็นเอกสาร แต่เกิดจากการปฏิบัติโดยพนักงานในทุกระดับขององค์กร

3) ประยุกต์ใช้ในการกำหนดกลยุทธ์องค์กร ผู้บริหารต้องพิจารณาความเสี่ยงที่เกี่ยวข้องกับกลยุทธ์ต่างๆ ขององค์กร

4) นำไปใช้ทั่วทั้งองค์กร การบริหารความเสี่ยงควรได้รับการปฏิบัติในทุกระดับและทุกหน่วยงานรวมถึงการมองความเสี่ยงในระดับภาพรวมขององค์กร

5) ความเสี่ยงที่ยอมรับได้ การบริหารความเสี่ยงได้รับการออกแบบเพื่อจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้เพื่อความสำเร็จของพันธกิจ หรือวิสัยทัศน์ขององค์กร

6) ให้ความมั่นใจอย่างสมเหตุสมผล การบริหารความเสี่ยงให้ความมั่นใจแก่คณะกรรมการและผู้บริหารในระดับหนึ่งแต่มิใช่การรับประกันโดยสมบูรณ์ และ

7) การบรรลุวัตถุประสงค์ การบริหารความเสี่ยงเป็นเครื่องมือนำไปสู่การบรรลุวัตถุประสงค์เรื่องใดเรื่องหนึ่ง หรือในหลายเรื่อง ได้แก่ วัตถุประสงค์ด้านกลยุทธ์ ด้านปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎหมายและกฎระเบียบ

ซึ่งองค์ประกอบของการบริหารความเสี่ยงของ COSO ประกอบด้วยองค์ประกอบแปดประการ ซึ่งสัมพันธ์กับการดำเนินทั้งทางด้านธุรกิจและด้านกระบวนการบริหารงานโดยจัดแบ่งออกเป็น 3 หมวดหมู่ ดังนี้ (วิฑูรย์ สมโต, 2551)

2.3.1 สภาพแวดล้อมภายในองค์กร (Internal Evironment) รากฐานสำคัญของกรอบการบริหารความเสี่ยง คือ สภาพแวดล้อมภายในองค์กรซึ่งจะมีอิทธิพลต่อผู้บริหารองค์กรในการกำหนดเป้าหมายองค์กร และกลยุทธ์ในการดำเนินกิจกรรมทางธุรกิจ การกำหนดเหตุการณ์บ่งชี้หรือกิจกรรมบ่งชี้ การประเมินความเสี่ยงและการจัดการความเสี่ยงประเภทต่าง ๆ ได้แก่ จริยธรรมองค์กร ปรัชญา และวัฒนธรรมองค์กรในการบริหารความเสี่ยง วิธีการทำงานของผู้บริหาร วิธีการและขั้นตอนการปฏิบัติงานของบุคลากรฝ่ายต่าง ๆ ในองค์กรโดยเฉพาะในเรื่องที่เกี่ยวกับการดูแลความเสี่ยงที่อาจเกิดขึ้นต่อองค์กร ดังนั้น ผู้บริหารควรพิจารณาถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appeite) จึงจำเป็นที่ผู้บริหารควรจัดให้มีความชัดเจนด้วยการทำเป็นแนวทางปฏิบัติที่ดี เช่น การมีคู่มือพนักงานในการทำงานที่กล่าวถึง จริยธรรมที่ดี ๆ ขององค์กร และปรัชญาในการบริหารงาน เป็นต้น

2.3.2 กระบวนการในการบริหารความเสี่ยง (Risk Management Process)

การบริหารความเสี่ยงให้ประสบความสำเร็จได้ดีนั้นผู้บริหารจำเป็นต้องวางแผนและปฏิบัติตามขั้นตอนต่าง ๆ อย่างเหมาะสมโดยมีการกำหนดขั้นตอนต่าง ๆ ดังนี้

2.3.2.1 การกำหนดวัตถุประสงค์ขององค์กร (Objective Setting) ผู้บริหารต้องกำหนดวัตถุประสงค์ทางธุรกิจให้ชัดเจน ต้องสร้างความมั่นใจว่าวัตถุประสงค์ที่กำหนดนั้น มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ (Strategic Objective) รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้ โดยหลักการแล้วผู้บริหารจำเป็นต้องจัดให้มีการบันทึกทั้งวัตถุประสงค์และกลยุทธ์ไว้เป็นลายลักษณ์อักษร เพื่อให้เกิดความชัดเจนกับทุกฝ่ายที่เกี่ยวข้อง

2.3.2.2 เหตุการณ์บ่งชี้ (Event Identification) ผู้บริหารควรพิจารณาเหตุการณ์หรือกิจกรรมบ่งชี้ความเสี่ยงที่อาจเกิดขึ้น ไม่ว่าจะเป็นแหล่งภายในหรือแหล่งภายนอกทุกด้านอันได้แก่ ด้านกลยุทธ์ ด้านการเงิน ด้านบุคลากร ด้านปฏิบัติการและระบบงาน ด้านภายีอากร ด้านกฎระเบียบต่างๆ และปัจจัยเกี่ยวกับสิ่งแวดล้อม รวมทั้งพิจารณาความสัมพันธ์ระหว่างเหตุการณ์ ต่าง ๆ ที่อาจเกิดขึ้น ทั้งนี้เพื่อให้ผู้บริหารเข้าใจความสัมพันธ์ของเหตุการณ์ต่างๆ ตลอดจนมีข้อมูลเพียงพอสำหรับใช้ในการบริหารความเสี่ยง โดยการประเมินความเสี่ยงเบื้องต้นได้อย่างเหมาะสมและทันเวลา

2.3.2.3 การประเมินความเสี่ยง (Risk Assessment) เป็นขั้นตอนที่ผู้บริหารประเมินทั้งความเสี่ยงและโอกาสขององค์กร รวมทั้งผลกระทบในทางลบที่อาจเกิดจากความเสี่ยง ผลในทางบวกของโอกาส และประเมินเหตุการณ์ที่อาจเกิดขึ้นว่าจะมีผลกระทบต่อวัตถุประสงค์องค์กรที่ได้ตั้งไว้ ผู้บริหารต้องประเมินให้ได้ว่าผลกระทบดังกล่าวอยู่ในระดับต่ำหรือสูง โอกาสที่เหตุการณ์นั้นจะเกิดขึ้นมากน้อยเพียงใด และหากเหตุการณ์นั้นเกิดขึ้นจริง จะส่งผลกระทบต่อกิจการอย่างไร การประเมินดังกล่าว ทำได้ทั้งในเชิงคุณภาพและหรือเชิงปริมาณ ในการประเมินความเสี่ยงนั้น ผู้บริหารควรให้ความสนในเรื่องต่างๆ เช่นโครงสร้างทางธุรกิจ กระบวนการปฏิบัติงานของผู้บริหารและพนักงาน การวัดผลการปฏิบัติงานและการติดตามผลการปฏิบัติงานกระบวนการรายงาน วิธีการติดต่อสื่อสารภายในองค์กร รวมทั้งกระบวนการรายงานทัศนคติของผู้บริหารเกี่ยวกับความเสี่ยงและแนวทางในการจัดการความเสี่ยง พฤติกรรมองค์กรในปัจจุบันและที่คาดว่าจะเกิดขึ้น ตลอดจนสัญญากับคู่ค้าหรือสัญญาต่างๆ ที่ผูกพันองค์กรและพันธมิตรทางธุรกิจขององค์กร เป็นต้น

2.3.2.4 การตอบสนองความเสี่ยง (Risk Response) เมื่อผู้บริหารสามารถบ่งชี้ความเสี่ยงและประเมินความเสี่ยงแล้ว ผู้บริหารต้องตัดสินใจว่าจะใช้วิธีการใดจัดการกับความเสี่ยงเหล่านั้น แต่ต้องแน่ใจว่า เป็นวิธีการที่สามารถนำไปปฏิบัติได้และวัดผลของการปฏิบัติหรือการจัดการความเสี่ยงนั้นได้ด้วย โดยที่ผู้บริหารต้องพิจารณาความเสี่ยงที่ยอมรับได้ควบคู่กันกับต้นทุนที่คาดว่าจะ

เกิดขึ้น และผลประโยชน์ที่คาดว่าจะได้รับ จากการจัดการหรือการบริหารความเสี่ยงเพื่อให้เกิดการบริหารที่มีประสิทธิภาพและประสิทธิผลมากที่สุดคือ การพิจารณาว่าใช้วิธีการบริหารความเสี่ยงอย่างคุ้มค่าการลงทุนนั่นเอง ดังนั้นผู้บริหารอาจเลือกใช้เพียงวิธีการเดียวหรือหลายวิธี ในการบริหารความเสี่ยงแต่ละเรื่องภายในองค์กรควบคู่กับการบริหารความเสี่ยงในภาพรวมขององค์กรให้ความเสี่ยงต่าง ๆ นั้นอยู่ในระดับที่ผู้บริหารประเมินได้ว่าจะเกิดความเสี่ยงแก่องค์กรน้อยที่สุดคืออยู่ในระดับที่องค์กรยอมรับได้ (Risk Tolerance Rate) หมายถึง การที่องค์กรทนรับกับแรงเสียดทานความเสี่ยงนั้นได้โดยไม่ล้มทั้งยืน หลักการที่ผู้บริหารอาจเลือกพิจารณาในการบริหารความเสี่ยงมี 4 หลักการ คือ

ก. ยอมรับความเสี่ยงที่อาจเกิดขึ้น (Accept the Risk) : เมื่อผู้บริหารพิจารณาแล้วว่าองค์กรจะประสบกับความเสี่ยงในระดับต่ำจนยอมรับได้ผู้บริหารก็อาจจะไม่ดำเนินการเพิ่มเติมอีกแล้วทั้งนี้อาจเนื่องจากต้นทุนการดำเนินการที่เพิ่มขึ้นไม่คุ้มกับค่าความเสี่ยงที่มีอยู่ในระดับที่ต่ำอยู่แล้ว

ข. ลดความเสี่ยง (Reduce the Risk): ผู้บริหารอาจดำเนินการเพิ่มเติมเพื่อลดโอกาสที่อาจเกิดผลเสียหายเพื่อทำให้ระดับความเสี่ยงอยู่ในเกณฑ์ที่ยอมรับได้

ค. การร่วมรับความเสี่ยง (Share the Risk) : ผู้บริหารอาจตัดสินใจร่วมแบ่งความรับผิดชอบกับองค์กรอื่นในการบริหารจัดการความเสี่ยงที่คาดว่าจะเกิดขึ้น

ง. การหลีกเลี่ยงความเสี่ยง (Avoid the Risk) : ผู้บริหารอาจตัดสินใจดำเนินดำเนินการบางอย่างเพื่อหลีกเลี่ยงบางเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงแก่องค์กร เพื่อเป็นการลดความเสียหายที่อาจเกิดขึ้นก็ได้ ผู้บริหารสามารถเลือกข้อใดข้อหนึ่งตอบสนองต่อความเสี่ยงประเภทต่างๆ ตามความเหมาะสมและต้องประเมินความเสี่ยงที่เหลืออยู่อย่างสม่ำเสมอ เพื่อสร้างความมั่นใจว่าสามารถควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับผลเสียหายที่อาจเกิดขึ้นได้

2.3.2.5 กิจกรรมการควบคุม (Control Activities) กิจกรรมการควบคุมรวมถึงนโยบาย วิธีการปฏิบัติงานและกระบวนการปฏิบัติงานขององค์กร ที่ฝ่ายบริหารจัดให้มีขึ้นภายในองค์กรเพื่อให้กิจกรรมการควบคุมต่าง ๆ เหล่านั้น ทำให้ผู้บริหารมั่นใจว่าได้มีการบริหารจัดการกับความเสี่ยง ซึ่งเป็นเครื่องมือที่ผู้บริหารกำหนดขึ้น ในทิศทางที่เหมาะสมกับวัตถุประสงค์ขององค์กร โดยที่ผู้บริหารแต่ละองค์กรจะมีเทคนิคในการนำไปปฏิบัติได้ซึ่งในทางปฏิบัติแล้วจะพบว่ากิจกรรมการควบคุมนั้นมีความแตกต่างกันในแต่ละองค์กร ตามลักษณะของธุรกิจภายใต้สภาพแวดล้อมที่องค์กรดำเนินธุรกิจอยู่ รวมทั้งโครงสร้างองค์กรและวัฒนธรรมภายในองค์กรด้วย นอกจากนี้แล้วกิจกรรมการควบคุมต่างๆจะเป็นภาพสะท้อนของสภาพแวดล้อมภายในองค์กรด้วยเช่นกัน

2.3.2.6 การตรวจสอบและติดตามดูแล (Monitoring) การตรวจสอบและติดตามผลถือเป็นมาตรการในการควบคุมดูแลคุณภาพของการบริหารจัดการความเสี่ยงโดยที่ผู้บริหารอาจพิจารณาถึงความเหมาะสมของการบริหารจัดการความเสี่ยงด้วย เนื่องจากธุรกิจมีความเปลี่ยนแปลงได้ตลอดเวลา ดังนั้นผู้บริหารจึงควรพิจารณากำหนดมาตรการติดตามตรวจสอบที่เหมาะสมโดยกำหนดให้มีการรายงานตามลำดับขั้นความรับผิดชอบอย่างเหมาะสม ทั้งนี้การติดตามตรวจสอบอาจเป็นลักษณะต่อเนื่องหรือเป็นครั้งคราว ซึ่งการติดตามอย่างต่อเนื่องจะทำให้ผู้บริหารหรือบุคลากรที่รับผิดชอบสามารถสนองตอบอย่างต่อเนื่อง และสนองตอบต่อการเปลี่ยนแปลงได้ทันท่วงทีซึ่งหากมีการติดตามอย่างสม่ำเสมอแล้วอาจถือว่าการติดตามตรวจสอบเป็นส่วนหนึ่งของการปฏิบัติงาน ในขณะที่การติดตามเป็นครั้งคราวนั้น จะมีการดำเนินการหลังจากเกิดเหตุการณ์แล้ว การจัดทำรายงาน จะช่วยให้ผู้บริหารใช้เป็นเครื่องมือในการติดตามการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพและประสิทธิผล

2.3.3. สารสนเทศและการสื่อสาร (Information & Communication) การสื่อสารอย่างมีประสิทธิภาพภายใต้ระบบสารสนเทศที่เหมาะสม จะช่วยให้ผู้บริหารบ่งชี้ประเมินและบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพประสิทธิผลและคุ้มค่าเม็ดเงินที่ลงทุนผู้บริหารควรกำหนดให้มีการบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กร ไม่ว่าจะมาจากแหล่งภายนอกหรือภายในองค์กรและกำหนดให้มีการสื่อสารอย่างเหมาะสมและทันต่อเวลา เพื่อให้บุคลากรในองค์กรตอบ-สนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพบางครั้ง หรือบางโอกาสมีการแลกเปลี่ยนข้อมูลกับบุคลากรภายนอก

กล่าวโดยสรุป การบริหารความเสี่ยงที่ดีจะต้องมีการสอบทานและตรวจสอบอยู่ตลอดเวลาและอย่างต่อเนื่อง ซึ่งการบริหารความเสี่ยงคือการที่ไม่สามารถประกันผลลัพธ์ที่จะเกิดขึ้นได้ แต่ถ้าหากองค์กรมีการนำองค์ประกอบแปดประการตามแนวทางของ COSO ไปปฏิบัติ จะช่วยเพิ่มความเชื่อมั่นในด้านกลยุทธ์และดำเนินงานให้กับองค์กรได้ พร้อมทั้งสามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กร ตลอดจนสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

**2.4 งานวิจัยที่เกี่ยวข้อง**

วันเพ็ญ สายชล (2549) ศึกษาความรู้ความเข้าใจในความเสี่ยงด้านปฏิบัติการของพนักงานธนาคารไทยพาณิชย์ จากการตอบคำถามเกี่ยวกับความรู้ความเข้าใจเกี่ยวกับความเสี่ยงด้านปฏิบัติการของพนักงานธนาคารไทยพาณิชย์พบว่า ผู้ตอบแบบสอบถามมีความรู้ความเข้าใจระดับปานกลางถึงสูง คือ ตอบคำถามถูกต้องได้มากกว่าร้อยละ 60.1 ขึ้นไปของคำถามแต่ละข้อ สามารถจำแนกได้ว่าผู้ตอบแบบสอบถามทราบดีถึงความหมายของความเสี่ยงด้านปฏิบัติการ การกำหนด

นโยบายและภาพรวมในการบริหารความเสี่ยงด้านปฏิบัติการในองค์กร ระบบการบริหารความเสี่ยงด้านปฏิบัติการในองค์กร และวิธีการจัดการความเสี่ยงด้านปฏิบัติการที่เกิดขึ้นในองค์กร

เมื่อนำคำตอบมาประเมินความรู้ความเข้าใจ โดยผู้ที่มีความรู้ความเข้าใจในเรื่องดังกล่าวถูกต้องได้ 1 คะแนนแต่หากไม่สามารถตอบได้จะได้คะแนน 0 คะแนน ปรากฏว่าผู้ตอบแบบสอบถามมีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงด้านปฏิบัติการอยู่ในระดับสูง ในคำถามที่ควรมีการกำหนดนโยบายและภาพรวมในการบริหารความเสี่ยงด้านปฏิบัติการในองค์กร (ร้อยละ 100.0) หน่วยบริหารความเสี่ยงทำหน้าที่ช่วยเหลือในด้านการดำเนินการ สนับสนุนในด้านการนำการบริหารความเสี่ยงมาปฏิบัติ และพัฒนาความสามารถในการบริหารความเสี่ยงด้านปฏิบัติการของพนักงาน(ร้อยละ 93.7) ระบบการบริหารความเสี่ยงด้านปฏิบัติการ ประกอบด้วย การระบุ ประเมิน ติดตาม รายงาน และการควบคุม (ร้อยละ 95.7) ควรกำหนดหรือทบทวนแนวทาง และวิธีการในการประเมินความเสี่ยงด้านปฏิบัติการให้มีความเหมาะสมกับการดำเนินการธุรกิจอยู่เสมอ (ร้อยละ 98.0) การประเมินความเสี่ยงด้านปฏิบัติการต้องครอบคลุมถึงโอกาสที่เหตุการณ์อาจเกิดขึ้น และผลกระทบที่เหตุการณ์นั้นมีต่อองค์กร (ร้อยละ 98.3) การติดตามผลและการรายงานความเสี่ยงด้านปฏิบัติการ เป็นเครื่องมือที่ช่วยให้ ผู้บริหารใช้ประเมินความสามารถของระบบการควบคุมความเสี่ยงด้านปฏิบัติ(ร้อยละ 93.0) และระบบข้อมูลสารสนเทศจะช่วยให้การจัดเก็บข้อมูลที่เกี่ยวข้องและจำเป็นต่อการบริหารความเสี่ยงด้านปฏิบัติการได้อย่างครบถ้วนและเหมาะสม (ร้อยละ 89.3)

ผู้ตอบแบบสอบถามส่วนใหญ่ มีความรู้ความเข้าใจการบริหารความเสี่ยงด้านปฏิบัติการ อยู่ในระดับปานกลาง ในคำถามที่การบริหารจัดการ และการควบคุมความเสี่ยงด้านปฏิบัติการ เป็นหน้าที่ของหน่วยบริหารความเสี่ยงเท่านั้น (ร้อยละ 79.7) การระบุและทบทวนควรจัดทำเมื่อองค์กรมีความพร้อมเท่านั้น และไม่จำเป็นต้องระบุและทบทวนทุกครั้งที่มีการเปลี่ยนแปลงของปัจจัยเสี่ยงด้านการปฏิบัติการ (ร้อยละ 79.0) การคาดคะเนถึงความเสี่ยงด้านปฏิบัติการที่อาจเกิดขึ้นในอนาคตไม่ได้ช่วยให้มีการปรับตัวและป้องกันได้ก่อนที่ความเสี่ยงจะเกิดขึ้น (ร้อยละ79.0) กระบวนการสอบยันหรือคู่มือการปฏิบัติงาน ไม่ได้ลดโอกาสที่จะเกิดความเสี่ยงด้านปฏิบัติการลงได้ (ร้อยละ 68.3) สามารถมอบให้บุคคลหรือตำแหน่งใด ๆ มีอำนาจในการอนุมัติการจ่ายเงิน ตรวจสอบ และกระทบยอดรายการที่เกี่ยวเนื่องในคราวเดียวกันได้ (ร้อยละ 73.0) ความเสี่ยงด้านกลยุทธ์ ด้านเครดิต ด้านการตลาด ด้านสภาพคล่อง เป็นสาเหตุที่ทำให้เกิดความเสี่ยงด้านปฏิบัติการ (ร้อยละ 76.3) รางวัลหรือสิ่งจูงใจที่ผูกติดกับผลการดำเนินงานที่สูงกว่ามาตรฐาน ไม่ได้ก่อให้เกิดความเสี่ยงด้านปฏิบัติการขึ้นได้ (ร้อยละ 75.0) และวิธีการจัดการความเสี่ยงด้านปฏิบัติการขึ้นได้ (ร้อยละ 75.0) และวิธีการจัดการความเสี่ยงด้านปฏิบัติการ ได้แก่ การควบคุม การโอนย้าย การหลีกเลี่ยง แต่จะไม่มีการยอมรับความเสี่ยง (ร้อยละ 67.3)

ข้อเท็จจริงของการบริหารความเสี่ยงด้านปฏิบัติการในองค์กร ของผู้ตอบแบบสอบถาม ผู้ตอบแบบสอบถามส่วนใหญ่ระบุว่า องค์กรของตนมีการบริหารความเสี่ยงด้านการปฏิบัติการ ความเสี่ยงด้านปฏิบัติการสามารถเกิดขึ้นได้กับพนักงานระดับล่างมากที่สุด ประเภทความเสี่ยงด้านปฏิบัติการที่เกิดขึ้นมากที่สุด จากกระบวนการทำงานความเสี่ยงด้านปฏิบัติการที่เกิดจากการทุจริตจากบุคคลภายนอกที่เกิดขึ้นบ่อยที่สุดคือ ลูกค้าเสนอให้สินบนแก่พนักงาน ความเสี่ยงด้านปฏิบัติการที่เกิดจากพนักงานทุจริตที่เกิดขึ้นบ่อยคือ พนักงานนำข้อมูลของลูกค้าไปหาประโยชน์ ความเสี่ยงด้านปฏิบัติการที่เกิดจากผู้บริหารซึ่งเกิดขึ้นบ่อยที่สุดคือ ขาดความรู้ความเข้าใจในความเสี่ยงด้านปฏิบัติการและความเสี่ยงด้านปฏิบัติการจากการจ้างงานที่เกิดขึ้นได้บ่อยที่สุดคือ การลาออกของพนักงานที่เกิดขึ้นบ่อยและมีแนวโน้มเพิ่มสูงขึ้น

ข้อมูลความคิดเห็นเกี่ยวกับความเสี่ยงด้านปฏิบัติการ ของพนักงานธนาคารไทยพาณิชย์ ผู้ตอบแบบสอบถามส่วนใหญ่ มีความคิดเห็นอยู่ในระดับมาก ของความเหมาะสมในการใช้เพื่อควบคุมการปฏิบัติการขององค์กร คือสามารถส่งเสริมให้มีการควบคุมภายในที่ดี สามารถส่งเสริมให้มีการจัดสถานที่ทำงานให้มีความปลอดภัยสำหรับพนักงาน สามารถส่งเสริมให้มีการปฏิบัติงานอยู่ในอำนาจหรืออำนาจอนุมัติ สามารถส่งเสริมให้มีการปฏิบัติงานที่สามารถตรวจสอบรายการระหว่างกันได้ สามารถส่งเสริมให้มีระบบการสำรองข้อมูล สามารถส่งเสริมให้มีการปฏิบัติตามกฎหมายและกฎระเบียบภายในบริษัท สามารถส่งเสริมให้มีการเก็บรักษาความลับของลูกค้า มิให้นำไปหาผลประโยชน์ส่วนตน สามารถส่งเสริมให้มีการซักซ้อมแผนสำรองฉุกเฉินอยู่เป็นประจำทุกปี และสามารถนำแผนสำรองฉุกเฉินไปปฏิบัติได้จริงกรณีเหตุการณ์วิกฤต

ปัญหาและข้อเสนอแนะถ้าหากขาดการควบคุมความเสี่ยงด้านปฏิบัติการ จะมีระดับความรุนแรงมากน้อยของปัญหาในด้านต่าง ๆ คือ ผู้ตอบแบบสอบถามส่วนใหญ่ มีความคิดเห็นอยู่ในระดับมากของปัญหาในการควบคุมความเสี่ยงด้านปฏิบัติการคือการควบคุมภายในขาดประสิทธิภาพ การทุจริตของบุคคลกรในองค์กร เช่น เจ้าหน้าที่ และผู้บริหาร การทุจริตของบุคคลภายนอกองค์กร คือ ลูกค้า และผู้มุ่งหวังผลประโยชน์ ความปลอดภัยของสถานที่ทำงาน การปรับเปลี่ยนโครงสร้างขององค์กร การจัดการที่ขาดประสิทธิภาพ ความบกพร่องของระบบงาน และคอมพิวเตอร์ พนักงานขาดความรู้ความเข้าใจในการทำงาน ไม่มีคู่มือในการปฏิบัติงานที่ดีหรือนำมาใช้ได้จริง มีคู่มือปฏิบัติงานแต่พนักงานไม่ปฏิบัติตามคู่มือนั้น ไม่มีแผนสำรองฉุกเฉินหรือไม่มีการซักซ้อม หากมีกรณีวิกฤตเกิดขึ้น และการนำข้อมูลความลับของลูกค้าไปหาประโยชน์ส่วนตน

วัชรี พรรณเรืองรอง (2549) ศึกษาการประเมินผลการดำเนินงานตามระบบการควบคุมภายในของมหาวิทยาลัยเชียงใหม่ ได้อภิปรายประเด็นสำคัญได้ดังนี้

1. การวิเคราะห์ปัจจัยการดำเนินงานตามระบบการควบคุมภายใน

1.1 ด้านสภาพแวดล้อมการควบคุม การดำเนินงานด้านสภาพแวดล้อมการควบคุม ในภาพรวมดำเนินการอยู่ในระดับดี เนื่องจากผู้บริหารของมหาวิทยาลัยเชียงใหม่ ได้ให้ความสำคัญกับการดำเนินงานตามระบบการควบคุมภายในเป็นอย่างมาก เห็นได้จากการกำหนดนโยบายและการมอบหมายอำนาจหน้าที่ให้บุคลากรรับผิดชอบในการควบคุมภายในอย่างชัดเจน นอกจากนี้ผู้บริหารหรือผู้รับตรวจมีหน้าที่รับผิดชอบโดยตรงที่จะต้องจัดให้มีการควบคุมภายใน และประเมินผลการควบคุมภายใน รวมทั้งในระดับองค์กหรือทั้งหน่วยรับตรวจ โดยต้องรับผิดชอบให้มีระบบการควบคุมภายใน ของหน่วยงานที่รับผิดชอบให้มีประสิทธิภาพ ประสิทธิผล ในระดับที่น่าพอใจอยู่เสมอ รวมทั้งการสร้างบรรยากาศเพื่อให้เกิดสภาพแวดล้อมของการควบคุมที่ดี และกำหนดบทบาทในการปฏิบัติตนให้เป็นตัวอย่างในเรื่องความซื่อสัตย์ ความมีคุณธรรมและจริยธรรมของผู้บริหาร และผู้บริหารจะต้องมีทัศนคติที่ดีและสนับสนุนการปฏิบัติหน้าที่เกี่ยวกับการเงิน การบัญชี ระบบการบริหารสารสนเทศ ทรัพยากรมนุษย์ การติดตามผล และการประเมินผล สนับสนุนมีการจัดโครงสร้างองค์กรและสายงานการบังคับบัญชาที่ชัดเจนและเหมาะสมกับขนาด และลักษณะการดำเนินงานขององค์กรซึ่งมหาวิทยาลัยได้จัด แนวทางการปฏิบัติงานตามระบบควบคุมภายในเพื่อให้บุคลากรได้จัดวางระบบการควบคุมภายในให้เหมาะสมแก่หน่วยงานซึ่งส่งผลให้การดำเนินงานมีประสิทธิภาพและประสิทธิผล

1.2 ด้านการประเมินความเสี่ยง การดำเนินการด้านประเมินความเสี่ยง โดยรวมดำเนินการอยู่ในระดับปานกลาง เนื่องจากความเสี่ยงในแต่ละหน่วยงานมีความแตกต่างกัน ซึ่งสาเหตุมาจากปัจจัยทั้งภายในและภายนอกองค์กร ในการปฏิบัติงานด้านการประเมินความเสี่ยงของหน่วยงานจึงเป็นเกณฑ์ความเสี่ยงที่เกี่ยวกับการควบคุมภายใน โดยเน้นการป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้นได้ ซึ่งผู้บริหารสามารถควบคุมความเสี่ยงดังกล่าวได้ ดังนั้น หน่วยงานจึงต้องระบุปัจจัยเสี่ยงและประเมินความเสี่ยงที่อาจเกิดขึ้นจากปัจจัยภายใน เช่น การปรับลดบุคลากร การใช้เทคโนโลยีสมัยใหม่ การปรับเปลี่ยนโครงสร้างองค์กร โดยผู้บริหารทุกระดับควรมีส่วนร่วมในการระบุปัจจัยเสี่ยงและประเมินความเสี่ยง และมีการวิเคราะห์ประเมินระดับความสำคัญหรือผลกระทบของความเสี่ยงและความถี่ที่จะเกิดขึ้น หรือโอกาสที่จะเกิดความเสี่ยง

1.3 กิจกรรมควบคุม การดำเนินการด้านกิจกรรมควบคุม โดยรวมดำเนินการอยู่ในระดับดี เนื่องจากหน่วยรับตรวจจะต้องปฏิบัติตามมาตรฐานการควบคุมภายในที่สำนักงานตรวจเงินแผ่นดินกำหนดไว้อยู่แล้ว รวมทั้งผู้บริหารและบุคลากรของมหาวิทยาลัยเชียงใหม่มีความรู้ และความเข้าใจในระดับของกิจกรรมการควบคุมเป็นอย่างดี เพราะเป็นกิจกรรมการควบคุมในเรื่องเกี่ยวกับการปฏิบัติงานตามความจำเป็นอย่างเหมาะสม รวมเป็นส่วนหนึ่งของการปฏิบัติงานประจำ

เมื่อพิจาณาถึงกิจกรรมการควบคุมที่หน่วยงานต่าง ๆ ได้ดำเนินการพบว่า มีการแบ่งแยกหน้าที่ในการอนุมัติ การบันทึกบัญชี และการดูแลรักษาทรัพย์สินออกจากกันโดยเด็ดขาด มีมาตรการป้องกันและดูแลรักษาทรัพย์สินอย่างรัดกุมและเพียงพอ มีการดำเนินการกำหนดขอบเขตอำนาจหน้าที่และวงเงินอนุมัติของผู้บริหารแต่ละระดับไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร มีการวางแผนการปฏิบัติงานตามระบบควบคุมภายในประจำปี และมีการปฏิบัติงานตามแผนการปฏิบัติงานตามระบบการควบคุมภายในประจำ ดังนั้น หน่วยงานหรือองค์กรต่าง ๆ ควรจัดให้มีกิจกรรมควบคุมอย่างต่อเนื่อง นอกจากนี้ การจัดให้มีกิจกรรมควบคุมควรคำนึงถึงความจำเป็น และความคุ้มค่าคุ้มทุนของการจัดกิจกรรมควบคุมด้วย เพื่อก่อให้เกิดการใช้ประโยชน์จากทรัพยากรขององค์กรหรือหน่วยงานให้เกิดประโยชน์สูงสุด

1.4 ด้านสารสนเทศและการสื่อสาร การดำเนินงานด้านสารเทศและการสื่อสาร โดยรวมพบว่า อยู่ในระดับปานกลาง เนื่องจากการสื่อสารภายในหน่วยงานเกี่ยวกับการดำเนินงานตามระบบการควบคุมภายในยังไม่ครอบคลุมหรือชัดเจนเท่าที่ควร รวมทั้งจากระดับผู้บริหารลงมาสู่ผู้ปฏิบัติงานจริง หรือจากผู้ปฏิบัติงานไปสู่ผู้บริหาร หรือบุคลากรภายในมหาวิทยาลัย แต่การดำเนินงานตามระบบควบคุมภายในของทุกหน่วยงาน ได้มีการแต่งตั้งคณะกรรมการเพื่อรับผิดชอบเกี่ยวกับการดำเนินงานดังกล่าวประจำหน่วยงานอยู่แล้ว รวมทั้งมีการมอบหมายหน้าที่ให้บุคลากรที่รับผิดชอบในเรื่องเกี่ยวกับระบบการควบคุมภายในให้ทุกคนทราบและเข้าใจบทบาทหน้าที่ของตน แต่จากการที่แต่ละฝ่ายมีความเข้าใจเกี่ยวกับการควบคุมภายในไม่ตรงกันบ้าง จึงทำให้ระดับการปฏิบัติงานด้านการสื่อสารอยู่ในระดับปานกลาง เมื่อพิจารณาด้านสารสนเทศและการสื่อสารในแต่ละประเด็นพบว่า การดำเนินงานด้านสารสนเทศและการสื่อสารมีความเหมาะสม และมีระบบการติดต่อสื่อสารทั้งภายในและภายนอกอย่างเพียงพอ เชื่อถือได้ และทันเวลา มีระบบสารสนเทศและสายการรายงานสำหรับการบริหารและตัดสินใจของฝ่ายบริหาร

การดำเนินการดังกล่าวมีความสอดคล้องกับการศึกษาของ นพวรรณ ฟูติตระกูล (2544) ซึ่งได้ทำการศึกษาเรื่อง การศึกษาเปรียบเทียบแนวคิดด้านการควบคุมภายในของ COSO และระบบการควบคุมภายในของธนาคารออมสิน ที่พบว่า ธนาคารออมสิน และ COSO ต่างให้ความสำคัญกับการมีระบบสารสนเทศและการสื่อสาร มีการจัดระบบสื่อสารทั้งภายในและภายนอกที่มีประสิทธิภาพและประสิทธิผลผู้ที่ต้องการใช้ข้อมูลสามารเข้าถึงข้อมูลที่ต้องการได้ สามารถนำข้อมูลไปใช้ให้เกิดประโยชน์ในการตัดสินใจต่าง ๆ ได้ทันเวลา นอกจากนี้ทางหน่วยงานหรือองค์การควรจัดทำระบบการควบคุมภายในที่เป็นเอกสาร แล้วสื่อสารให้ฝ่ายบริหารและบุคลากรที่เกี่ยวข้องทราบทั่วกัน ทั้งนี้เพื่อให้บุคลากรของหน่วยงานหรือองค์การที่เกี่ยวข้องสื่อสารและเข้าใจตรงกัน

1.5 ด้านการติดตามประเมินผล การดำเนินงานด้านการติดตามประเมินผลโดยรวมดำเนินการอยู่ในระดับปานกลาง เนื่องจากการติดตามผลการปฏิบัติงานตามระบบตรวจสอบภายในเป็นกิจกรรมการบริหารและการกำกับดูแลโดยปกติของหน่วยงาน และเป็นกิจกรรมการปฏิบัติงานตามหน้าที่ของบุคลากรอยู่แล้ว และทุกหน่วยงานจะต้องปฏิบัติตามระเบียบคณะกรรมการตรวจเงินแผ่นดิน เมื่อพิจารณาในแต่ละประเด็นด้านการติดตามประเมินผลพบว่า มีการดำเนินงานติดตามประเมินผลการแก้ไขข้อบกพร่องที่พบจากการประเมิน ผลการประเมินผลการควบคุมด้วยตนเอง มีการเปรียบเทียบแผนและผลการดำเนินงานและรายงานให้ผู้กำกับดูแลทราบเป็นลายลักษณ์อักษรอย่างต่อเนื่องและสม่ำเสมอ และในกรณีผลการดำเนินงานไม่เป็นไปตามแผนมีการดำเนินการแก้ไขอย่างทันการณ์

การติดตามประเมินผลการควบคุมภายในจะประสบผลสำเร็จได้นั้น ฝ่ายบริหารและผู้ที่มีส่วนเกี่ยวข้อง ควรจัดให้มีการตรวจสอบการปฏิบัติตามระบบการควบคุมภายใน โดยใช้กลไกต่าง ๆ เช่น การติดตามผลในขณะการปฏิบัติงานหรือขณะมีการนำระบบการควบคุมภายในที่กำหนดไปสู่การปฏิบัติอย่างต่อเนื่อง การตรวจสอบโครงสร้างการควบคุมภายในเป็น ระยะ ๆ เพื่อให้ทราบถึงปัญหาและอุปสรรคในการดำเนินงาน และนำปัญหาและอุปสรรคนั้นมาปรับปรุงแก้ไขให้ดียิ่งขึ้นเพื่อก่อให้เกิดความการดำเนินงานการควบคุมภายในที่มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

**2.5 กรอบแนวคิดที่ใช้ในการศึกษา**

จากการศึกษา ทบทวน แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องในประเด็นต่าง ๆ ผู้ศึกษาจึงได้กำหนดกรอบแนวคิดในการศึกษา โดยใช้แนวคิดทฤษฎีการบริหารความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization of the Treadway Commission) ประกอบด้วย


**รูป 1 กรอบแนวคิดการบริหารความเสี่ยงของ** COSO

**2.6 นิยามศัพท์เฉพาะ**

**ผู้บริหาร** หมายถึง ผู้ดำรงตำแหน่งเป็นคณบดีคณะพยาบาลศาสตร์ รองคณบดี คณะพยาบาลศาสตร์

**หัวหน้างาน** หมายถึง ผู้ที่ได้รับแต่งตั้งให้เป็นหัวหน้างาน ณ หน่วยงานต่าง ๆ ในคณะพยาบาลศาสตร์ ซึ่งประกอบด้วย ข้าราชการ และพนักงานมหาวิทยาลัย-พนักงานปฏิบัติการ

**หัวหน้าหน่วย** หมายถึง ผู้ที่ได้รับแต่งตั้งให้เป็นหัวหน้าหน่วย และผู้ที่ได้รับมอบหมาย ซึ่งประกอบด้วย ข้าราชการพลเรือนในมหาวิทยาลัย และพนักงานมหาวิทยาลัย-พนักงานปฏิบัติการ

**พนักงานมหาวิทยาลัย-พนักงานปฏิบัติการ** หมายถึง ผู้ปฏิบัติงานในตำแหน่ง พนักงานในกำกับของรัฐ

**พนักงานส่วนงาน** หมายถึง ผู้ปฏิบัติงานในตำแหน่ง พนักงานเงินรายได้

**สภาพแวดล้อมภายในองค์กร** (Internal Environment) หมายถึง วัฒนธรรมของคณะพยาบาลศาสตร์ จริยธรรมของบุคลากร โครงสร้างการจัดการองค์กร นโยบาย วิธีการทำงานของผู้บริหารและบุคลากร สภาพแวดล้อมในการทำงาน มุมมองและทัศนคติที่มีต่อความเสี่ยงรวมถึงระดับความเสี่ยงที่คณะพยาบาลศาสตร์ มหาวิทยาลัยเชียงใหม่ ยอมรับได้

**การกำหนดวัตถุประสงค์** (Objective Setting) หมายถึง การกำหนดวัตถุประสงค์โดยรวมของคณะพยาบาลศาสตร์ ในรูปพันธกิจ จุดมุ่งหมายหรือเป้าประสงค์ เช่น จุดมุ่งหมายเชิงยุทธศาสตร์และแผนปฏิบัติการประจำปี การกำหนดวัตถุประสงค์ระดับกิจกรรม

**เหตุการณ์บ่งชี้หรือการระบุความเสี่ยง** (Event Identification) หมายถึง การที่ผู้บริหาร คณะพยาบาลศาสตร์สามารถระบุความเสี่ยงทุกกิจกรรมที่สำคัญได้อย่างครอบคลุม หน่วยงานมีกลไกที่เพียงพอในการระบุความเสี่ยงจากปัจจัยภายนอกและปัจจัยภายใน

**การประเมินความเสี่ยง** (Risk Assessment) หมายถึง การวิเคราะห์การจัดลำดับความเสี่ยงโดยมีการพิจารณาการประเมินโอกาสที่จะเกิดความเสี่ยง ความรุนแรงของผลกระทบจากเหตุการณ์ที่ความเสี่ยง ทั้งปัจจัยภายในและปัจจัยภายนอกคณะพยาบาลศาสตร์ ซึ่งปัจจัยที่ใช้การพิจารณาอาจจะประกอบด้วย การปฏิบัติงานของผู้บริหารและบุคลากร กระบวนการปฏิบัติงาน กิจกรรมการควบคุมภายใน โครงสร้างขององค์กร การวัดผลการปฏิบัติงานและการติดตามผล วิธีการติดต่อสื่อสาร ทัศนคติและแนวทางของผู้บริหารเกี่ยวกับความเสี่ยง

**การตอบสนองความเสี่ยง** (Risk Response) หมายถึง เมื่อมีการบ่งชี้ว่ามีการเกิดความเสี่ยงขึ้นในคณะพยาบาลศาสตร์ในด้านใดด้านหนึ่งหรือหลาย ๆ ด้าน ผู้บริหารต้องเลือกวิธีการจัดการกับความเสี่ยงที่เกิดขึ้น

**กิจกรรมการควบคุม** (Control Activities) ในที่นี้หมายถึง นโยบายและกระบวนการหรือขั้นตอนการปฏิบัติงานเพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ระบบเทคโนโลยีสารสนเทศ เช่น การจัดซื้อโปรแกรมสำเร็จรูป การพัฒนาโปรแกรม การบำรุงรักษา และการกำหนดให้บุคลากรภายในคณะพยาบาลศาสตร์ รับผิดชอบการควบคุมแต่ละกิจกรรม ระยะเวลาในการปฏิบัติงาน พร้อมทั้งต้องมีการควบคุมและชี้แจงเกี่ยวกับกฎหมายการเข้าถึงเทคโนโลยีสารสนเทศ ของคณะพยาบาลศาสตร์

**การตรวจสอบและติดตามดูแล** (Monitoring) ในที่นี้หมายถึง การนำแผนการจัดการความเสี่ยงไปใช้อย่างถูกต้องและมีประสิทธิภาพทราบถึงข้อผิดพลาดที่อาจเกิดขึ้นหลังจากใช้แผนการ

จัดการความเสี่ยงสามารถปรับปรุงแก้ไขแผนจัดการความเสี่ยงให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป หลังจากนั้นมีการรายงานผลต่อผู้บริหารที่ได้รับมอบหมาย ภายในคณะพยาบาลศาสตร์

**สารสนเทศและการสื่อสาร** (Information & Communication) หมายถึง การวางแผนและการบริหารความปลอดภัย ระบบข้อมูลสามารถสืบค้นและรายงานข้อมูลต่าง ๆ ที่เกี่ยวข้องกับสถานะของคณะพยาบาลศาสตร์ในปัจจุบัน ได้แก่ ข้อมูลนักศึกษา เช่น จำนวนรับเข้าศึกษา จำนวนผู้สำเร็จการศึกษา ช่องการสื่อสารที่มีประสิทธิภาพเพื่อให้บุคลากรทุกระดับสามารถสื่อสารได้ และมีการแลกเปลี่ยนข้อมูลระหว่างกัน ผู้ปฏิบัติงานสามารถเข้าใจบทบาทหน้าที่ของตนเอง และผู้บริหารได้ทราบปัญหาที่เกิดขึ้นจากการปฏิบัติงานจริง