บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การค้นคว้าแบบอิสระเรื่อง “การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัท ลำพูนซิงเดนเก็น จำกัด” ผู้ศึกษาได้ศึกษาค้นคว้าเอกสารทฤษฎีและงานวิจัยที่เกี่ยวข้องสาระสำคัญได้ดังนี้

1. มาตรฐานที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. ความหมายและกระบวนการบริหารจัดการความเสี่ยง
3. เอกสารและงานวิจัยที่เกี่ยวข้อง
4. กรอบแนวคิดในการศึกษา

ในการศึกษาครั้งนี้ ผู้ศึกษาได้พยายามชี้ถึงความสำคัญของข้อมูลสารสนเทศและการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ว่ามีความสำคัญต่อการดำเนินการทางธุรกิจของบริษัทเป็นอย่างมากอันเป็นการนำไปสู่แนวคิดเรื่องของการบริหารจัดการระบบสารสนเทศให้เป็นไปในทิศทางเดียวกับธุรกิจของบริษัทอย่างมีประสิทธิภาพ ซึ่งมีกรอบแนวคิดต่างๆมากมายที่องค์กรควรนำมาประยุกต์ใช้ ไม่ว่าจะเป็นมาตรฐานISO 9000, ISO/IEC 27001, ISO/IEC 20000, ITIL, CobiT Framework โดยแต่ละมาตรฐานหรือ Best Practices นั้นมีความเหมาะสมในการนำไปใช้ในที่แตกต่างกัน แต่เมื่อพิจารณาลึกไปในด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลจะเห็นได้ว่ากระบวนการของ Information Security Management System: ISMS ตามมาตรฐาน ISO/IEC 27001 นั้นมีมุมมองด้านความเสี่ยงในเรื่องการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลเป็นหลัก โดยเน้นไปที่การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นกระบวนการ ด้วยการนำแนวคิดของศาสตราจารย์ Deming ตามหลักการ Plan-Do-Check-Act หรือ Deming Cycle มาใช้ในการทำ “Continual Process Improvement:กระบวนการปรับปรุงอย่างต่อเนื่อง” โดยมาตรฐานที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ใช้ในการศึกษาครั้งนี้ ผู้ศึกษาจะได้กล่าวในรายละเอียดต่อไป

มาตรฐานที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

มาตรฐาน ISO/IEC 27001:2005 (Information Security Management System: ISMS)

เศรษฐพงค์ มะลิสุวรรณ (2552) อธิบายว่า มาตรฐานที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่หลายองค์กรนำมาใช้ในการบริหารจัดการความเสี่ยง คือ มาตรฐาน ISO/IEC 27001: 2005 มาตรฐาน ISO/IEC 17799: 2005 และมาตรฐาน ISO/IEC 27002: 2005 นอกจากนี้ยังมีมาตรฐานอื่นๆ ที่สถาบันที่มีชื่อเสียงเป็นผู้กำหนดเพื่อเป็นแนวทางในการปฏิบัติ ได้แก่ มาตรฐาน ISO/IEC TR 13335มาตรฐาน ISO/IEC 15408: 2005มาตรฐาน ITIL (IT Infrastructure Library) มาตรฐาน FIPS PUB 200 มาตรฐาน NIST 800-14 และมาตรฐาน IT Baseline Protection Manual

ISO/IEC 27001: 2005 คือ มาตรฐานสากลด้านการบริหารความมั่นคงของข้อมูลซึ่งเน้นความสำคัญที่ “ระบบการบริหารจัดการ” (Management System) โดยมีข้อกำหนดต่างๆที่องค์กรพึงปฏิบัติ ในการรักษาความมั่นคงของข้อมูล เพื่อปกป้องข้อมูลทางธุรกิจและทรัพย์สินด้านสารสนเทศที่สำคัญ ให้พ้นจากภัยคุกคามและความเสี่ยงในรูปแบบต่างๆ รวมถึงกำหนดให้มีการจัดทำแผนรับมือเหตุฉุกเฉิน ที่อาจเกิดขึ้นเพื่อลดความสูญเสียและคงไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกระทรวงวิทยาศาสตร์และเทคโนโลยี (2550) ได้อธิบายรายละเอียดของ มาตรฐานที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่อ้างอิงจากมาตรฐาน ISO/IEC 27001:2005 ซึ่งผู้ศึกษาได้นำมาใช้เป็นมาตรฐานอ้างอิงในการศึกษาครั้งนี้ โดยแบ่งออกเป็นสองส่วนหลักๆ ดังนี้

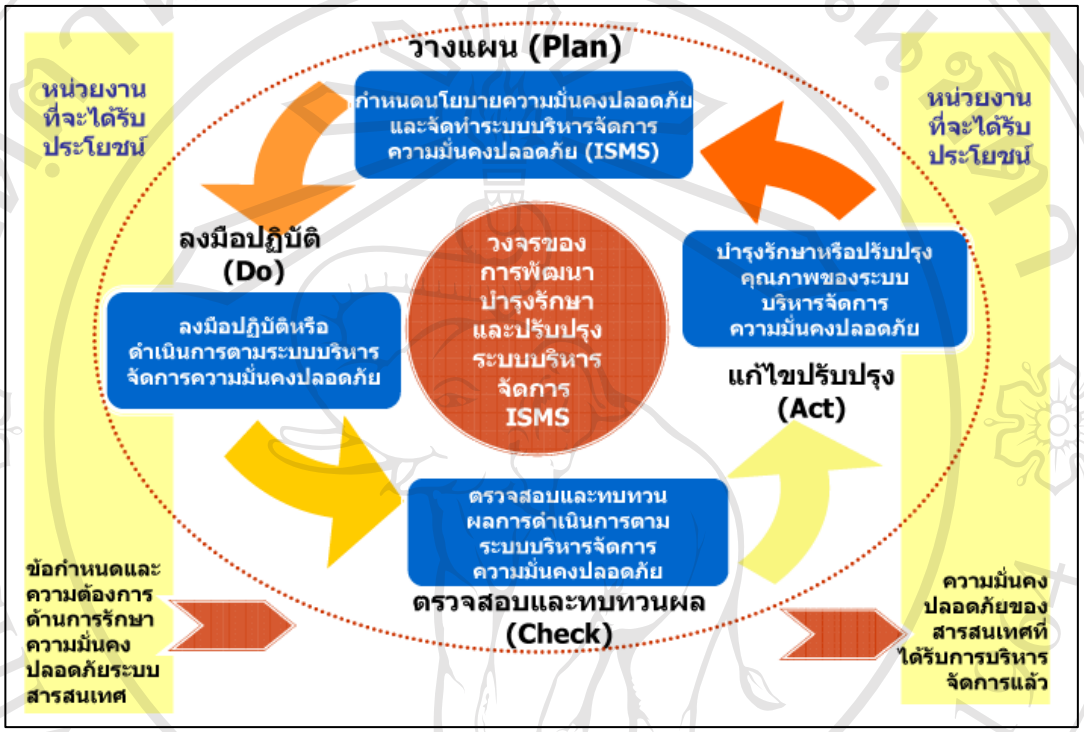
ส่วนที่ 1 กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1. ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1.1 ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนดลงมือปฏิบัติดำเนินการเฝ้าระวังทบทวนบำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย ตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษรภายใน

กรอบกิจกรรมการดำเนินการทางธุรกิจต่างๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ (ภาพที่2-1)



ภาพที่ 2-1 วงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอนPlan-Do-Check-Act

1.2 การกำหนดและบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัย

1.2.1 กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

1) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาถึงลักษณะของธุรกิจองค์กรสถานที่ตั้งทรัพย์สินและเทคโนโลยี

2) กำหนดนโยบายความมั่นคงปลอดภัย

3) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมสำหรับองค์กร

4) ระบุความเสี่ยง

5) วิเคราะห์และประเมินความเสี่ยง

6) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยง

7) เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยเพื่อจัดการกับความเสี่ยง

8) ขอการอนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

9) ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

1.2.2 ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Do)

1) จัดทำแผนการจัดการความเสี่ยงซึ่งกล่าวถึงการดำเนินการเชิงบริหารจัดการทรัพยากรที่จำเป็น หน้าที่ความรับผิดชอบและลำดับการดำเนินการ เพื่อบริหารจัดการความเสี่ยงที่พบ

2) ลงมือปฏิบัติตามแผนจัดการความเสี่ยง เพื่อให้บรรลุวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

3) ลงมือปฏิบัติตามมาตรการที่เลือกไว้

4) กำหนดวิธีการในการวัดความสัมฤทธิผลของมาตรการที่เลือกมาใช้

5) จัดทำและลงมือปฏิบัติตามแผนการอบรม

6) บริหารการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

7) บริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

8) จัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติซึ่งจะช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

1.2.3 เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Check)

1) ลงมือปฏิบัติตามขั้นตอนปฏิบัติ สำหรับการเฝ้าระวังและทบทวนเพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสามารถ

2) ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ

3) วัดความสัมฤทธิ์ผลของมาตรการทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

4) ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนด

5) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยภายในองค์กรตามรอบระยะเวลาที่ได้กำหนดไว้

6) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหารอย่างสม่ำเสมอ

7) ปรับปรุงแผนทางด้านความมั่นคงปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่างๆมาพิจารณาร่วมด้วย

8) บันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

1.2.4 บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Act)

1) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้

2) ใช้มาตรการเชิงแก้ไขและป้องกัน

3) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

4) ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

1.3 ข้อกำหนดทางด้านการจัดทำเอกสาร

1.3.1 ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร

1.3.2 การบริหารจัดการเอกสาร เป็นเอกสารตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุมขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร

1.3.3 การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่างๆ องค์กรจะต้องมีการกำหนดจัดทำและบำรุงรักษาบันทึกข้อมูล หรือฟอร์มต่างๆเพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนด

2. หน้าที่ความรับผิดชอบของผู้บริหาร

2.1 การให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติ การดำเนินการการเฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

2.2การบริหารจัดการทรัพยากร

2.2.1 การจัดสรรทรัพยากร

2.2.2 การอบรมการสร้างความตระหนักและการเพิ่มขีดความสามารถ

3. การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย โดยองค์กรควรดำเนินการตรวจสอบภายในตามรอบระยะเวลาที่กำหนด เพื่อตรวจสอบว่าวัตถุประสงค์ มาตรการ กระบวนการและขั้นตอนปฏิบัติ ของระบบบริหารจัดการความมั่นคงปลอดภัยดังนี้

3.1 สอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมายระเบียบข้อบังคับหรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องหรือไม่

3.2 สอดคล้องกับข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือไม่

3.3 ได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิ์ผลหรือไม่

3.4 เป็นไปตามที่คาดหมายไว้หรือไม่

4. การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร ซึ่งผู้บริหารต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ตามรอบระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิผล

5. การดำเนินการเพื่อบำรุงรักษาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

5.1 การปรับปรุงอย่างต่อเนื่อง โดยองค์กรจะต้องปรับปรุงความสัมฤทธิ์ผลของระบบบริหารความมั่นคงปลอดภัยอย่างต่อเนื่อง

5.2 การดำเนินการเชิงแก้ไข โดยองค์กรต้องดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนดสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อป้องกันการเกิดขึ้นอีก

5.3 การดำเนินการเชิงป้องกัน โดยองค์กรต้องดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนด สำหรับระบบบริหารจัดการความมั่นคงปลอดภัย ที่มีโอกาสเกิดขึ้นเพื่อป้องกันการเกิดขึ้น

ส่วนที่ 2 มาตรการหรือข้อกำหนดด้านการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

มาตรการหรือข้อกำหนด ที่เป็นหัวข้อหลักๆซึ่งมักถูกเรียกว่า11 โดเมนหลักของมาตรฐาน ISO/IEC 27001: 2005 ดังนี้

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
2. โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and Operations Management)

7. การควบคุมการเข้าถึง (Access Control)

8. การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition Development and Maintenance)

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

11. การปฏิบัติตามข้อกำหนด (Compliance)

อย่างไรก็ตามจะเห็นได้ว่า มาตรการหรือข้อกำหนดในการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ที่กล่าวไว้ในมาตรฐาน ISO/IEC 27001: 2005 นั้นไม่มีการแนะนำแนวทางปฏิบัติที่เป็นรายละเอียดขยายความว่า องค์กรควรจะปฏิบัติในแนวทางใดจึงจะถูกต้องตามข้อกำหนด ผู้ศึกษาจึงศึกษาเพิ่มเติมในส่วนของมาตรฐาน ISO/IEC 17799: 2005 Information Technology Security Techniques Code of Practice for Information Security Management ซึ่งในรายละเอียดได้กล่าวถึง แนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับข้อกำหนดตามมาตรฐาน ISO/IEC 27001: 2005

มาตรฐาน ISO/IEC 17799: 2005 Information Technology Security Techniques Code of Practice for Information Security Management

วชิราพร ปัญญาพินิจนุกูร (2552) อธิบายว่า มาตรฐาน ISO/IEC 17799 เป็นมาตรฐานที่กล่าวถึง เรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัย ที่องค์กรได้จัดทำขึ้นซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติ ในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการหรือเลือกใช้วิธีการที่มีความมั่นคงปลอดภัย เพียงพอหรือเหมาะสมตามที่องค์กรได้ประเมินไว้ โดยแนววิธีปฏิบัติดังกล่าว ได้ถูกจัดให้มีความสอดคล้องกันกับ มาตรฐาน ISO/IEC 27001: 2005 ดังแสดงรายละเอียดเป็นไว้ใน ตัวอย่างที่ 2-1

ตัวอย่างที่ 2-1

แสดงความสอดคล้องกันระหว่าง ISO/IEC 17799 กับ ISO/IEC 27001:2005

ข้อกำหนดตามมาตรฐานISO/IEC 27001: 2005

1. นโยบายความมั่นคงปลอดภัย (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document) (ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร อย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy) (ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

แนววิธีปฏิบัติตามมาตรฐานISO/IEC 17799

1. นโยบายความมั่นคงปลอดภัย (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

1) องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร

2) นโยบายฯควรได้รับการอนุมัติหรือรับรองอย่างเป็นทางการโดยผู้บริหาร

3) นโยบายฯควรได้รับการตีพิมพ์และเผยแพร่เพื่อให้พนักงานได้รับทราบ

4) นโยบายฯควรสามารถอ่านทำความเข้าใจได้โดยง่าย

5) นโยบายฯควรสอดคล้องหรือตรงกับความต้องการทางธุรกิจขององค์กร

6) นโยบายฯควรมีการแสดงเจตจำนงของผู้บริหารเพื่อให้พนักงานเห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

7) นโยบายฯควรกล่าวถึงหลักการวัตถุประสงค์และเป้าหมายในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน

8) นโยบายฯควรมีการให้คำนิยามคำว่า “การรักษาความปลอดมั่นคงปลอดภัยสำหรับสารสนเทศ” (Information security)

9) นโยบายฯควรมีการกล่าวถึงขอบเขตของการรักษาความมั่นคงปลอดภัย

10)นโยบายฯควรกล่าวถึงหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย

11)นโยบายฯควรกล่าวถึงหน้าที่และความรับผิดชอบของพนักงานในการรายงานเหตุการณ์ความมั่นคงปลอดภัยที่เกิดขึ้น

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)

1) องค์กรควรกำหนดผู้มีหน้าที่รับผิดชอบในการตรวจสอบและปรับปรุงนโยบายเพื่อให้มีความทันสมัยอยู่เสมอ

2) องค์กรควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัย

3) องค์กรควรกำหนดรอบระยะเวลาที่ชัดเจนในการตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัย

4) องค์กรควรมีการประเมินประสิทธิภาพและประสิทธิผลโดยภาพรวมของนโยบายความมั่นคงปลอดภัย

5) องค์กรควรมีการประเมินผลและผลกระทบอันเกิดจากการเปลี่ยนแปลงทางเทคโนโลยีที่มีต่อนโยบายความมั่นคงปลอดภัย

อย่างไรก็ตามจะเห็นได้ว่าทั้ง มาตรฐานISO/IEC 27001: 2005 และมาตรฐาน ISO/IEC 17799 นั้นจะมุ่งเน้นไปในด้านของกระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ และข้อกำหนดด้านการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ รวมถึงแนววิธีปฏิบัติที่จะทำให้องค์กรสามารถปฏิบัติตามข้อกำหนดได้ แต่ยังขาดรายละเอียดในเรื่องของ ขั้นตอนการสร้างระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลในบริษัท ผู้ศึกษาจึงได้ศึกษาในเรื่อง กระบวนการทำระบบประกันคุณภาพทั่วทั้งองค์กร (Total Quality Management: TQM) ร่วมด้วย

เพื่อนำหลักการของ TQM. โดยเฉพาะขั้นตอนตามทฤษฎี PDCAมาปรับใช้ในการสร้างระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลของการศึกษาครั้งนี้

ระบบประกันคุณภาพทั่วทั้งองค์กร (Total Quality Management: TQM)

TQM มาจากคำว่า TQC (Total Quality Control) ของญี่ปุ่นหรือบางทีญี่ปุ่นก็เรียกว่า CWQC (Company-Wide Quality Control) หรืออาจแปลว่า “การควบคุมคุณภาพทั่วบริษัท” (เรืองวิทย์ เกษสุวรรณ, 2549) TQM ได้รับการนิยามว่าเป็น “กิจกรรมที่เป็นระบบ เป็นวิทยาศาสตร์ และครอบคลุมทุกส่วนขององค์กรโดยให้ความสำคัญที่ลูกค้า” (จำลักษณ์ ขุนพลแก้วและศุภชัย อาชีวระงับโรค, 2548)

เมื่อกล่าวโดยสรุปในภาพรวมสำหรับความหมายของ TQM นั้น Witcher (1390 อ้างถึงใน สุนทร พูนพิพัฒน์, 2542) กล่าวว่า

T (Total) หมายถึง การยินยอมให้ทุกคนปฏิบัติงานอยู่ภายในองค์การได้เข้ามามีส่วนร่วมในการจัดตั้งและบริหารงานระบบคุณภาพซึ่งเกี่ยวกับทั้งลูกค้าภายนอก (External Customer) และลูกค้าภายใน (Internal Customer) โดยตรง

Q (Quality) หมายถึง การสร้างความพึงพอใจของลูกค้าต่อการใช้ประโยชน์จากสินค้าและบริการเป็นหลัก นอกจากนี้คุณภาพยังมีส่วนเกี่ยวข้องกับแนวความคิดเชิงระบบของการจัดการ (Systematic Approach of Management) กล่าวคือ การกระทำสิ่งใด ๆ อย่างเป็นระบบที่ต่อเนื่องและตรงตามแนวความคิดดั้งเดิมของวงจรคุณภาพที่เรียกว่า PDCA cycle ซึ่งเสนอรายละเอียดโดย W. Edwards Deming เพราะฉะนั้นถ้าหมุนวงจรคุณภาพเช่นนี้อย่างต่อเนื่องขึ้นภายในแต่ละหน่วยงานย่อยขององค์การหนึ่งๆ ก็ย่อมจะเกิดระบบคุณภาพโดยรวมทั้งหมดที่เรียกว่า TQM ขึ้นมาได้ในประการสุดท้าย

M (Management) หมายถึง ระบบของการจัดการหรือบริหารคุณภาพขององค์การ ซึ่งดำเนินการและควบคุมด้วยผู้บริหารระดับสูงสุด ซึ่งประกอบด้วย วิสัยทัศน์ (Vision) การประกาศพันธกิจหลัก (Mission statement) และกลยุทธ์ของการบริหาร (Strategic Management) รวมถึงการแสดงสภาวะของความเป็นผู้นำ (Leadership) ที่จะมุ่งมั่นปรับปรุงและพัฒนาระบบคุณภาพขององค์การอย่างสม่ำเสมอและต่อเนื่องตลอดระยะเวลา (Continuous Quality Improvement)

การบริหารจัดการธุรกิจภายใต้สภาพแวดล้อมทางธุรกิจที่มีความซับซ้อน การแข่งขันทวีความรุนแรง มีการเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้นผู้บริหารจึงจำเป็นต้องอาศัยแนวคิดเกี่ยวกับการบริหารความเสี่ยงมาช่วยให้เกิดความมั่นใจมากยิ่งขึ้นในการจัดการกับความเปลี่ยนแปลงและ

ความไม่แน่นอน ดังนั้นจึงปฏิเสธไม่ได้ว่าหน้าที่สำคัญอีกอย่างหนึ่งของผู้บริหารคือ การควบคุมภายใน (Internal Audit) เพื่อให้นโยบายของผู้บริหารถูกนำไปสู่การปฏิบัติ

การตรวจติดตามภายใน (Internal Audit) คือกระบวนการซึ่งร่วมกันทำให้บังเกิดผลโดยคณะกรรมการ ผู้บริหารและบุคคลอื่น ๆ ขององค์กรถูกออกแบบขึ้นมาเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ ซึ่งมี 3 ประการ ดังต่อไปนี้

1. ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน (Effectiveness and Efficiency of Operations)
2. ความเชื่อถือได้ของรายงานทางการเงิน (Reliability of financial reporting)
3. การปฏิบัติตามกฎหมายและกฎระเบียบ (Compliance with applicable laws and regulations)

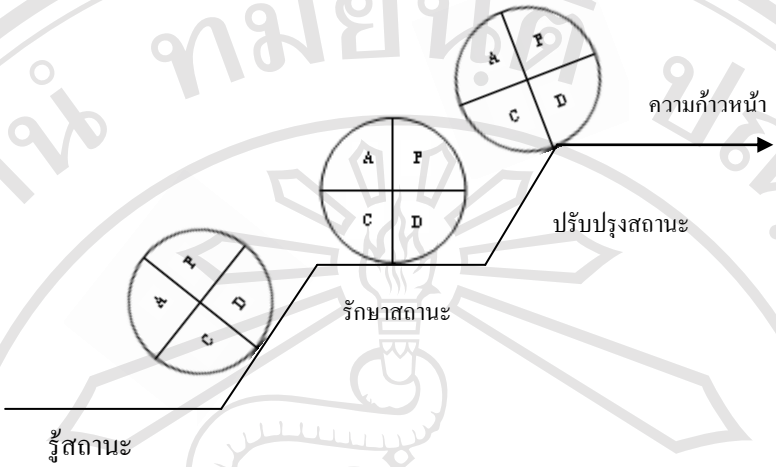
การตรวจติดตามภายใน (Internal Audit) ประกอบด้วยองค์ประกอบที่สำคัญ 5 ประการ ที่มีความเกี่ยวเนื่องสัมพันธ์กัน โดยองค์ประกอบเหล่านี้ มาจากแนวทางที่ผู้บริหารดำเนินธุรกิจและมีการเชื่อมโยงเข้ากับกระบวนการทางการบริหาร ดังมีรายละเอียดดังนี้

1. สภาพแวดล้อมการควบคุม (Control Environment)
2. การประเมินความเสี่ยง (Risk Assessment)
3. กิจกรรมการควบคุม (Control Activities)
4. สารสนเทศและการสื่อสาร (Information and Communication)
5. การติดตามประเมินผล (Monitoring)

การตรวจติดตามภายใน (Internal Audit) มีการแบบระดับการตรวจออกเป็น 3 ระดับ ดังนี้

1. การตรวจประเมินภายในหน่วยงาน
2. การตรวจติดตามภายในโดยคณะกรรมการ ผู้บริหารและบุคคลนอกหน่วยงาน
3. การตรวจติดตามภายในโดยผู้ตรวจสอบจาก Certification Body (CB) ที่มีหน้าที่ตรวจสอบตามมาตรฐาน ISO/IEC เช่น มาตรฐาน ISO/IEC 27001 เป็นต้น

อย่างไรก็ตามจะเห็นได้ว่า ทั้ง 3 มาตรฐานที่ได้กล่าวมานี้ ไม่ได้มีการกล่าวเจาะลึกไปถึงกระบวนการบริหารจัดการความเสี่ยงและการประเมินความเสี่ยงไว้ แต่หลักการดังกล่าวนี้ถือเป็นส่วนสำคัญอีกส่วนหนึ่งในการศึกษาครั้งนี้ ซึ่งผู้ศึกษาก็ได้ศึกษาเพิ่มเติมในส่วนนี้ด้วย และจะได้กล่าวรายละเอียดของ กระบวนการบริหารจัดการความเสี่ยงและการประเมินความเสี่ยงในลำดับต่อไป



P = Plan	คือ การสำรวจสภาพปัจจุบันเพื่อนำมาวางแผนในการแก้ไขปัญหา
D = Do	คือ การปฏิบัติ ตามแผนที่วางไว้
C = Check	คือ การตรวจสอบ ผลที่ได้จากการปฏิบัติงานตามแผน
A = Act	คือ การปฏิบัติการแก้ไข ถ้าไม่ได้ตามเป้าหมาย นำเข้าสู่วงจรเดมิ่งใหม่ (PDCA) ถ้าทำได้ตามเป้าหมายก็ตั้งเป็นมาตรฐานต่อไป

ภาพที่ 2-2 วงจรคุณภาพที่เรียกว่า PDCA CYCLE

หมายเหตุ. แหล่งที่มา. Deming, 1986 อ้างถึงใน สุนทร พูนพิพัฒน์, 2542

ความหมาย และกระบวนการบริหารจัดการความเสี่ยง

เศรษฐพงค์ มะลิสุวรรณ (2552) อธิบายว่า การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบและควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรมหน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยง อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งให้มากที่สุด

กระบวนการบริหารจัดการความเสี่ยงแบ่งเป็น 5 ขั้นตอนดังนี้

1. การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วยกระบวนการวิเคราะห์ความเสี่ยงและการประเมินค่าความเสี่ยง

1.1 การวิเคราะห์ความเสี่ยง (Risk Analysis) ประกอบด้วย 3 ขั้นตอนดังนี้

1.1.1 การชี้หรือระบุความเสี่ยง (Risk Identification) คือ การชี้ให้เห็นถึงปัญหาความไม่แน่นอน หรือประเด็นความเสี่ยงที่องค์กรกำลังเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัย

ความรู้ความเข้าใจองค์กรภารกิจและกิจกรรม สิ่งแวดล้อมด้านกฎหมายสังคม การเมืองและวัฒนธรรมพัฒนาการ และปัจจัยที่มีต่อความสำเร็จขององค์กร รวมทั้งโอกาสและสิ่งคุกคามที่มีต่อองค์กร การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุกๆด้านขององค์กร

1.1.2 ลักษณะรายละเอียดของความเสี่ยง (Risk Description) คือ เมื่อระบุความเสี่ยงแล้ว ควรบรรยายรายละเอียดและลักษณะของความเสี่ยงนั้น เช่นชื่อความเสี่ยง (Name) ขอบเขต (Scope) ลักษณะความเสี่ยง (Nature) ผู้ที่มีผลกระทบลักษณะเชิงประมาณเป็นต้น

1.1.3 การประมาณความเสี่ยง (Risk Estimation) ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรง หรือเสียหายมากน้อยเพียงใดโอกาสหรือความน่าจะเป็น (Probability) หรือความบ่อยครั้งของการเกิดเหตุหรือเหตุการณ์อาจแบ่งแบบง่ายๆ เป็น 5 ระดับจากน้อยไปหามาก เช่น บ่อย (Frequent) พบได้บ่อยครั้งเป็นประจำประปราย (Probable) ตามโอกาส (Occasional) น้อยครั้งมาก (Remote) แทบไม่เกิดเลย (Improbable) และความรุนแรงของสิ่งที่เกิดขึ้นตามมา (Severity of Consequence) อาจแบ่งเป็น 4 ระดับ คือ สูงมาก (Severe) สูง (High) ปานกลาง (Moderate) ต่ำ (Low)

1.2 การประเมินค่าความเสี่ยง (Risk Evaluation)

เมื่อได้ประเด็นความเสี่ยงที่มีการระบุรายละเอียดความเสี่ยง (Risk Description) และมีการประมาณความเสี่ยง (Risk Estimation) แล้วจึงนำประเด็นความเสี่ยงนั้นๆ มาประเมินค่าความเสี่ยงโดยการเปรียบเทียบกับหลักเกณฑ์ความเสี่ยงที่ยอมรับได้ เช่นหลักเกณฑ์ยอมรับความเสี่ยง (Risk Acceptance Criteria) ว่าจะยอมรับได้มากน้อยเพียงใด เพื่อประกอบการตัดสินใจว่าจะบำบัดความเสี่ยงนั้นๆ ต่อไปอย่างไร โดยควรพิจารณาในแง่ต่างๆ ดังต่อไปนี้ เช่น ค่าใช้จ่ายประโยชน์และความคุ้มทุนที่จะได้รับจากการแก้ไขบำบัดความเสี่ยง (Costs and Benefits) ข้อกำหนดด้านกฎหมายและกฎระเบียบขององค์กร (Legal Requirements) ปัจจัยด้านสิ่งแวดล้อม (Environmental Factors) เป็นต้น

2. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk Reporting) เป็นการรายงานสรุปประเด็นความเสี่ยงที่ตรวจพบทั้งหมด โดยทำการจัดกลุ่มความเสี่ยงตามระดับความรุนแรงตามที่ทำการประเมินค่าความเสี่ยงไว้และอีกทั้งเป็นเอกสารที่ใช้ในการสื่อสารกับฝ่ายบริหารและบุคลากรในองค์กรได้รับรู้ถึงความเสี่ยงที่องค์กรเผชิญอยู่โดยในรายงานควรประกอบด้วยรายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง

3. การบรรเทาและควบคุมความเสี่ยง (Risk Mitigationand Control) เมื่อฝ่ายบริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณาจากหลักเกณฑ์การยอมรับความเสี่ยง ที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัดความเสี่ยงเพื่อลดความเสี่ยง (Reduction) ให้อยู่ในระดับที่ยอมรับได้หรือจัดทำระบบควบคุม เพื่อให้เกิดผลกระทบต่อองค์กรจากความเสี่ยงนั้นๆ

4. การรายงานความเสี่ยงตกค้าง (Residual Risk Reporting) เมื่อมีการบำบัดความเสี่ยงแล้วจำเป็นต้องมีการรายงานและทบทวนอยู่เสมอ เพื่อดูว่ามีการประเมินและการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมา ใช้ได้ผลหรือไม่เพียงไรหรือมีความเสี่ยงใดที่ยังไม่ได้รับการบำบัดบ้าง

5. การเฝ้าสังเกต (Monitoring) กระบวนการเฝ้าสังเกตเป็นหลักประกันว่าองค์กรมีมาตรการต่างๆที่จำเป็น และเหมาะสมสำหรับการบริหารความเสี่ยงต่างๆและมาตรการเหล่านั้นมีผู้ปฏิบัติตามและบังเกิดผลจริง

เอกสารและงานวิจัยที่เกี่ยวข้อง

พัทธ์ธีรา โอศิริ (2549) ได้ทำการค้นคว้าแบบอิสระ เรื่องระบบประเมินและวิเคราะห์ความเสี่ยงในการจัดการด้านระบบสารสนเทศ โดยมีวัตถุประสงค์ในการพัฒนาระบบสารสนเทศ เพื่อใช้ประเมินและวิเคราะห์ความเสี่ยงในการจัดการด้านระบบสารสนเทศ ซึ่งนำเอาแนวปฏิบัติของมาตรฐาน ISO/IEC 17799 มาเป็นกรอบวิธีการให้องค์กรดำเนินการตามกรอบที่มาตรฐานกำหนด โดยพัฒนาเป็นระบบสารสนเทศผ่านทางเว็บแอพพลิเคชั่น ซึ่งภายหลังการทำการค้นคว้าแบบอิสระทำให้ได้เครื่องมือสำหรับใช้ในการดำเนินกิจกรรมการบริหารความเสี่ยงด้านสารสนเทศที่เป็นเว็บแอพพลิเคชั่นสำหรับองค์กร

จากการพัฒนาระบบประเมินและวิเคราะห์ความเสี่ยงในการจัดการด้านระบบสารสนเทศ โดยระบบมีความสามารถในการประเมินและวิเคราะห์ความเสี่ยง ในการจัดการด้านระบบสารสนเทศและจัดทำรายงานผลการประเมิน พร้อมทั้งคำแนะนำและจัดลำดับหัวข้อเรื่องที่ต้องกระทำก่อนหลัง ซึ่งหลังจากทำการดำเนินการเสร็จแล้ว พบปัญหาและอุปสรรค คือ ระบบยังไม่รองรับการแบ่งเกณฑ์ประเมินโดยผู้ใช้งานเองและการสร้างแบบสอบถามก็ขาดความยืดหยุ่นและที่สำคัญที่สุด พบว่าคำแนะนำที่ได้จากระบบนั้นไม่สามารถแก้ปัญหาได้จริง เนื่องจากปัญหาหรือประเด็นความเสี่ยงที่ตรวจพบมีความหลากหลายและแนวทางการแก้ไขในบางกรณีต้องใช้วิธีการ

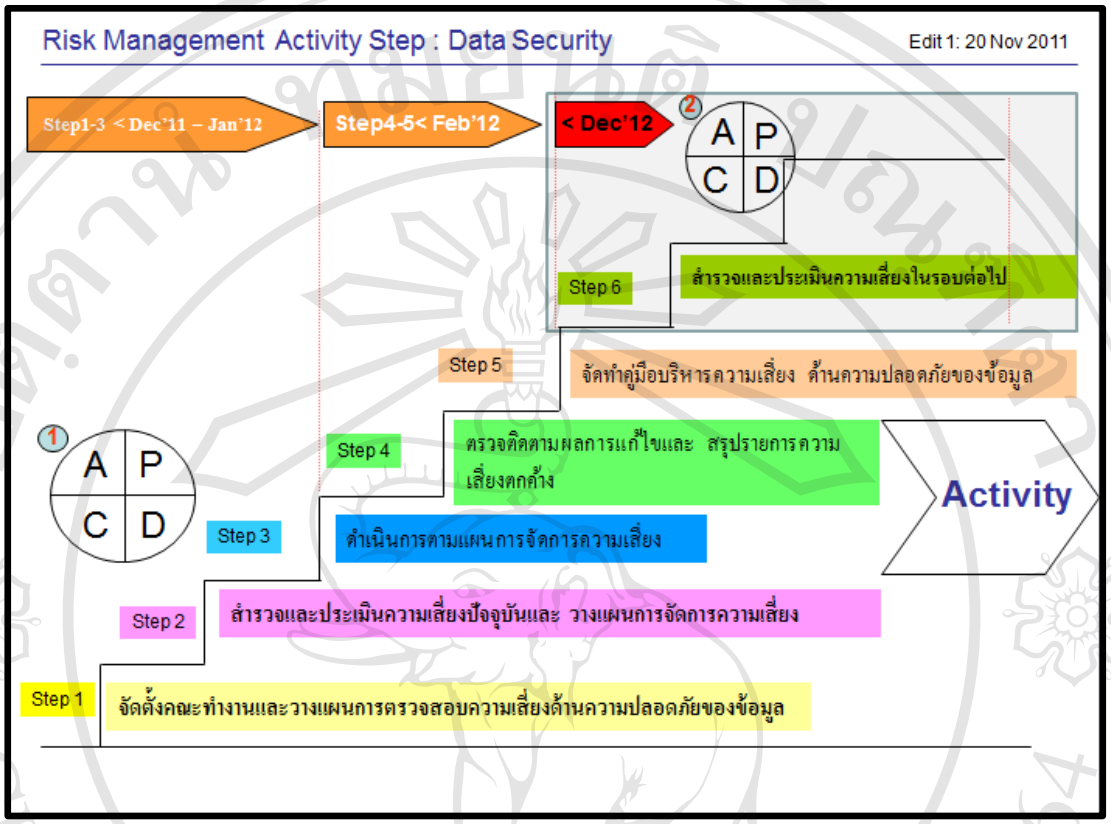
ดำเนินการเฉพาะทางหรือต้องใช้ความรู้ทางเทคนิคมาแก้ปัญหา จึงทำให้คำแนะนำที่ได้จากระบบนั้น คำตอบที่ได้ยังไม่ครอบคลุมกับประเด็นปัญหาที่ตรวจพบและไม่สามารถแก้ปัญหาได้จริง

กรอบแนวคิดในการศึกษา

ในการศึกษาครั้งนี้ ผู้ศึกษาต้องการจัดทำระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล โดยการปรับใช้ มาตรฐาน ISO/IEC 27001: 2005 ซึ่งเป็นมาตรฐานที่นำแนวคิดของหลักการ PDCA มาเป็นโครงสร้างหลักในระบบการบริหารจัดการ เพื่อให้องค์กรมีระบบที่จะสามารถ ตรวจสอบ วิเคราะห์ประเมินดูแลและควบคุมความเสี่ยงที่มีหลักปฏิบัติเป็นมาตรฐานสากล ดังนั้นผู้ศึกษาจึงได้สร้างกรอบแนวคิดของระบบบริหารจัดการความเสี่ยงขึ้น เพื่อที่จะให้เห็นภาพของระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ในรูปแบบกรอบแนวคิด PDCA ได้ชัดเจน โดยจะเป็นการแสดงถึงขั้นตอนการทำงาน การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ที่แสดงให้เห็นว่ามีขั้นตอนการทำงานทั้งหมด 6 ขั้นตอน ซึ่งในแต่ละขั้นตอนจะเป็นการแสดงลำดับการทำงานดังนี้

1) จัดตั้งคณะทำงานและวางแผนการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล
2) สำรวจประเมินความเสี่ยงปัจจุบันและวางแผนการจัดการความเสี่ยง
3) ดำเนินการตามแผนการจัดการความเสี่ยง
4) ตรวจติดตามผลการแก้ไขและสรุปรายการความเสี่ยงตกค้าง
5) จัดทำคู่มือบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล
6) สำรวจและประเมินความเสี่ยง ในรอบต่อไป

อย่างไรก็ตามในการศึกษาครั้งนี้ จะดำเนินการถึงเพียงขั้นตอนที่ 5 เท่านั้น ในส่วนของขั้นตอนที่ 6 เปรียบได้กับการทำ PDCA ในรอบต่อไป ซึ่งจะมีการดำเนินการในปีถัดไปโดยจะไม่นำมากล่าวถึงในการศึกษาครั้งนี้ (ภาพที่ 2-3)



ภาพที่ 2-3 กรอบแนวคิดระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ตามรูปแบบแนวคิด PDCA.

จากกรอบแนวคิดระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ตามรูปแบบแนวคิด PDCA จะเห็นว่าใน Step 1-5 นั้นเป็นขั้นตอนกระบวนการที่เริ่มตั้งแต่ การสร้างระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล จนถึงการจัดทำคู่มือบริหารความเสี่ยง ซึ่งทั้งหมดมาจากการนำเอาหลักการของการบริหารจัดการความเสี่ยง (Risk Management) ทั้ง 5 ข้อ รวมกับการนำเอาหลักการแนวคิด PDCA มาใช้จนทำให้เกิดกระบวนการดังกล่าวขึ้น และยังได้นำเอาเนื้อหาหรือข้อกำหนดของมาตรฐาน ISO/IEC 27001: 2005 มาเป็นแนวทางในการสำรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล