บทที่ 1
บทนำ

การศึกษาในครั้งนี้เป็นการนำมาตรฐาน ISO/IEC 27001:2005 (Information Security Management System: ISMS) ซึ่งเป็นมาตรฐานในการบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลมาปรับใช้เพื่อสร้างระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลในบริษัท ลำพูนซิงเดนเก็น จำกัด โดยผู้ศึกษามีความเห็นว่าในปัจจุบันระบบคอมพิวเตอร์และ ระบบสารสนเทศต่างๆ มีความสำคัญอย่างมากต่อองค์กรภาคธุรกิจ ซึ่งก็พบว่ามีภัยคุกคามต่างๆเกิดขึ้นต่อระบบสารสนเทศโดยเฉพาะอย่างยิ่งข้อมูลในระบบสารสนเทศและภัยคุกคามเหล่านี้สร้างผลกระทบโดยตรงต่อการดำเนินธุรกิจ ดังนั้นการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลจึงเปรียบเสมือนภูมิคุ้มกันชนิดหนึ่งที่จะทำให้การดำเนินธุรกิจเป็นไปอย่างต่อเนื่องและปลอดภัยจากภัยคุกคามต่างๆ

หลักการและเหตุผล

จากสภาวะเศรษฐกิจของโลกในปัจจุบันที่มีการแข่งขันกันอย่างรุนแรงและมีแนวโน้มที่จะเพิ่มสูงขึ้นเรื่อยๆทำให้องค์กรภาคธุรกิจต่างพยายามสร้างความได้เปรียบในด้านการแข่งขันและด้านประสิทธิภาพของต้นทุนอยู่ตลอดเวลาทำให้ข้อมูลข่าวสารกลายเป็นหัวใจสำคัญในการทำธุรกิจในยุคนี้โดยหลายองค์กรได้นำเทคโนโลยีสารสนเทศมาช่วยจัดเก็บข้อมูลเพื่อใช้ในการขับเคลื่อนการเปลี่ยนแปลงกระบวนการทำงานที่เกิดขึ้นในองค์กรให้มีประสิทธิภาพมากขึ้นทั้งสร้างความได้เปรียบในด้านการแข่งขัน

สิ่งเหล่านี้ทำให้องค์กรต่างๆมองเห็นความสำคัญของสารสนเทศ (Information) และเทคโนโลยีสารสนเทศ (Information Technology) ในองค์กรอันถือได้ว่าเป็นสินทรัพย์ที่มีค่ายิ่งโดยเฉพาะในโลกของการแข่งขันที่รุนแรงผู้บริหาร ที่ให้ความสำคัญและความคาดหวังกับเทคโนโลยีสารสนเทศมากยิ่งขึ้นโดยเฉพาะการตอบสนองที่รวดเร็วต่อเนื่องตลอดเวลารวมถึงมีคุณภาพสามารถใช้งานได้หลากหลายและสะดวกต่อการใช้งานโดยใช้เวลาน้อยลงเพิ่มระดับการบริการให้ดียิ่งขึ้นและมีต้นทุนที่ต่ำลง

บริษัทลำพูนซิงเดนเก็น จำกัดตั้งอยู่ในเขตนิคมอุตสาหกรรมภาคเหนือ จังหวัดลำพูนดำเนินธุรกิจทางด้านการผลิตชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ประเภท เซมิคอนดักเตอร์และ เพาเวอร์ซัพพลาย

เพื่อส่งออกไปจำหน่ายยังต่างประเทศปัจจุบันบริษัทได้นำเอาระบบและเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและช่วยสนับสนุนการขับเคลื่อนธุรกิจในทุกๆด้านซึ่งปัจจุบันระบบและเทคโนโลยีสารสนเทศได้มีบทบาทสำคัญอย่างยิ่งในการขับเคลื่อนธุรกิจและสร้างความสามารถในการแข่งขันทางธุรกิจให้กับบริษัทซึ่งนั่นย่อมหมายถึงข้อมูล (Data) และสารสนเทศ (Information)ในแต่ละส่วนหรือแต่ละระบบก็ย่อมมีความสำคัญต่อธุรกิจมากเช่นกัน

จากเหตุผลขั้นต้นจะเห็นได้ว่าข้อมูลสารสนเทศนั้นมีความสำคัญกับบริษัทลำพูนซิงเดนเก็น จำกัดเป็นอย่างมาก โดยบริษัทนั้นมีความต้องการใช้ข้อมูลสารสนเทศอย่างต่อเนื่องตลอดเวลาเห็นว่าบริษัทจะได้รับผลกระทบอย่างมากหากการให้บริการข้อมูลสารสนเทศเกิดหยุดชะงัก ข้อมูลเสียหายหรือรั่วไหลไปยังบริษัทคู่แข่ง ซึ่งการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลเป็นเรื่องที่สำคัญเรื่องหนึ่งที่บริษัทควรให้ความสำคัญและพิจารณาจัดการบริหารอย่างเป็นระบบ รวมถึงควรอ้างอิงจากมาตรฐานสากลที่มีการกำหนดกรอบการปฏิบัติไว้อย่างชัดเจนและการพิจารณาปรับปรุงกระบวนการจัดการระบบสารสนเทศด้านความปลอดภัยของข้อมูล โดยนำเอามาตรฐานการบริหารจัดการด้านเทคโนโลยีสารสนเทศมาแก้ปัญหาหรือสร้างระบบป้องกันความเสี่ยงเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ดังนั้นผู้ศึกษาจึงมีความสนใจที่จะศึกษาและดำเนินการในเรื่อง “การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทลำพูนซิงเดนเก็น จำกัด”เพื่อให้บริษัทสามารถมีข้อมูลและระบบสารสนเทศในการขับเคลื่อนธุรกิจซึ่งเป็นข้อมูลสารสนเทศที่ถูกต้องและปลอดภัย อีกทั้งมีระบบและเทคโนโลยีสารสนเทศที่สามารถให้บริการได้อย่างต่อเนื่องตลอดเวลา

วัตถุประสงค์ของการศึกษา

1. ศึกษาความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทลำพูนซิงเดนเก็น จำกัดในปัจจุบัน
2. จัดทำมาตรฐานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทลำพูนซิงเดนเก็น จำกัดตามมาตรฐาน ISO/IEC 27001:2005และมาตรฐาน ISO/IEC 17799:2005

ประโยชน์ที่ได้รับจากการศึกษา

1. สามารถประยุกต์ใช้มาตรฐานด้านการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลเพื่อใช้ในการประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่จะส่งผลกระทบต่อธุรกิจของบริษัทลำพูนซิงเดนเก็นจำกัด ได้อย่างถูกต้องและเหมาะสม

2. สามารถประยุกต์ใช้มาตรฐานด้านการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลเพื่อให้ได้มาซึ่งระบบหรือแผนป้องกันความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ต่ำและยอมรับได้

ขอบเขตของการศึกษา

1. ขอบเขตการศึกษา

1.1 ประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทลำพูนซิงเดนเก็น จำกัด โดยใช้มาตรฐาน ISO/IEC 27001:2005(Information Security Management System: ISMS) และมาตรฐาน ISO/IEC 17799:2005 (Information Technology Security Techniques Code of practice for information security management)

1.2 ออกแบบมาตรฐานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัทลำพูนซิงเดนเก็น จำกัด โดยประยุกต์ตามมาตรฐานของ ISO/IEC 27001:2005 และมาตรฐาน ISO/IEC 17799:2005 ซึ่งการค้นคว้าแบบอิสระครั้งนี้มีขอบเขตด้านข้อมูลและวิธีการดำเนินการดังนี้

1.2.1 ขอบเขตด้านข้อมูล

ขอบเขตของข้อมูลสารสนเทศของบริษัทลำพูนซิงเดนเก็น จำกัดที่ใช้ในงานวิจัยครั้งนี้มีรายละเอียด ดังต่อไปนี้

บริษัทลำพูนซิงเดนเก็น จำกัด มีกลุ่มงานที่ดูแลงานทางด้านสารสนเทศประกอบด้วย 2 กลุ่มงานคือกลุ่มงาน IT Serviceและกลุ่มงาน IT Development โดยในการศึกษาครั้งนี้ผู้ศึกษาจะจัดทำระบบบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลเฉพาะข้อมูลที่กลุ่มงาน IT Service Group รับผิดชอบเท่านั้นซึ่งเป็นกลุ่มงานที่ให้บริการและดูแลด้านระบบสารสนเทศทั่วทั้งองค์กรและมีส่วนเกี่ยวข้องโดยตรงกับข้อมูลที่บริษัทต้องใช้งาน โดยสามารถเป็นต้นแบบให้กับกลุ่มงานอื่นๆต่อไปได้ซึ่งมีการแบ่งหน้าที่รับผิดชอบโดยสังเขปดังนี้

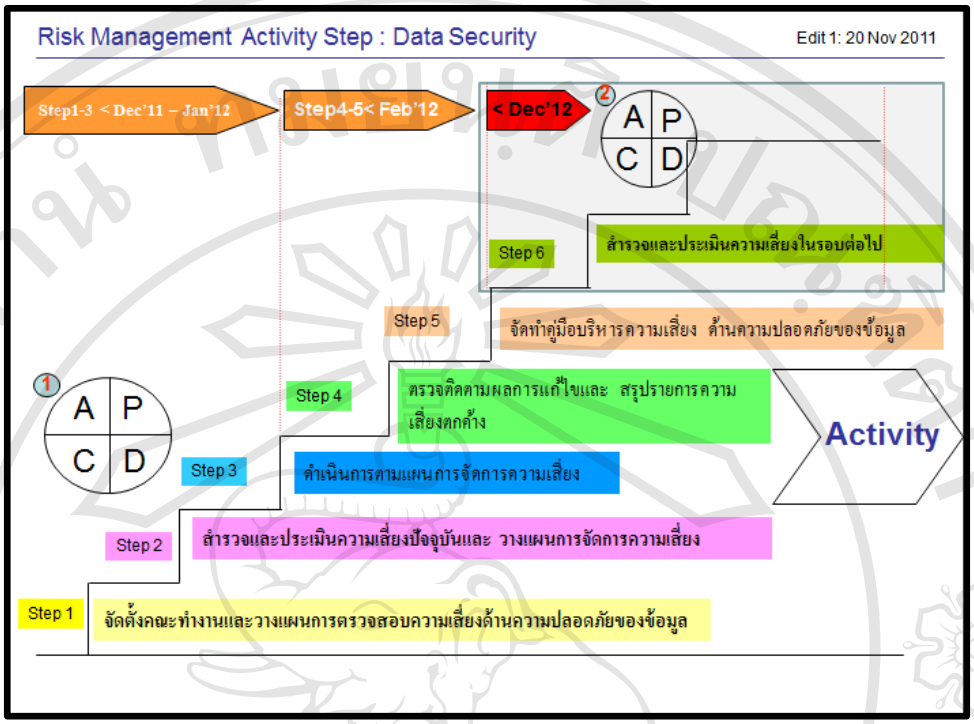
ตารางที่ 1-1

ตารางแสดงหน้าที่รับผิดชอบด้านข้อมูลใน บริษัท ลำพูนซิงเดนเก็น จำกัด

กลุ่มงาน	หน้าที่รับผิดชอบด้านข้อมูล
กลุ่มงาน IT Service	ทำงานด้านดูแลระบบเป็นหลักโดยมีข้อมูลสารสนเทศที่อยู่ในความรับผิดชอบและอยู่ในขอบเขตงานวิจัย คือ 1. ระบบข้อมูลส่วนกลาง (Data Center) ประกอบด้วย 1.1 ระบบเอกสารส่วนกลาง (File Sharing) ซึ่งมี File Server จำนวน 2 Server 1.2 ระบบฐานข้อมูล (Data Base Systems) มี Database Server จำนวน 4 server (ERP. System, MRP. System, HRMS, DB System Active Directory Database) 2. ระบบข้อมูลสนับสนุน (Service Support Systems) 2.1 ระบบจดหมายอิเล็กทรอนิคส์ (E-Mail) Mail Server จำนวน 1 Server 2.2 เว็บไซต์ภายในองค์กร 3. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง 3.1 ระบบเครื่องแม่ข่าย คอมพิวเตอร์แม่ข่าย จำนวน 8 เครื่อง 3.2 ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร
กลุ่มงาน IT Development	ทำงานทางด้านวิเคราะห์และพัฒนาระบบ และดูแลในส่วนของ Application Development

1.2.2 วิธีการดำเนินการ

จากการศึกษากรอบแนวคิดของระบบประกันคุณภาพทั่วทั้งองค์กร (Total Quality Management :TQM) สามารถนำเอาแนวคิดของ TQMมาประยุกต์ใช้ร่วมกับแนววิธีปฏิบัติเพื่อนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยในองค์กร ที่ระบุไว้ในมาตรฐาน ISO/IEC 17799: 2005 โดยมีแนววิธีปฏิบัติที่สอดคล้องตาม มาตรฐาน ISO/IEC27001: 2005 ทำให้สามารถออกแบบ “แผนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท ลำพูนซิงเดนเก็น จำกัด” โดยแบ่งขั้นตอนออกเป็น 6 ขั้นตอน (ภาพที่ 1-1)



ภาพที่ 1-1 ขั้นตอนการทำงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทลำพูนซิงเคนเก็น จำกัด

1. ขั้นตอนที่ 1

1.1 จัดตั้งคณะทำงานบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล โดยแบ่งออกเป็น 2 ชุด คือ คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล และคณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล

1.2 จัดทำแบบฟอร์มการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล โดยยึดตามมาตรฐาน ISO/IEC 27001: 2005

2. ขั้นตอนที่ 2

2.1 คณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูลดำเนินการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูลที่มีอยู่ในปัจจุบัน

2.2 จัดทำรายงานสรุปรายการความเสี่ยงด้านความปลอดภัยของข้อมูลที่ตรวจพบ

2.3 จัดทำแผนการจัดการความเสี่ยง

3. ขั้นตอนที่ 3

3.1 ดำเนินการปรับปรุงแก้ไขข้อบกพร่อง ที่ก่อให้เกิดความเสี่ยงด้านความปลอดภัยของข้อมูล ตามแผนการจัดการความเสี่ยง

4. ขั้นตอนที่ 4

4.1 ตรวจติดตามผลการแก้ไขและสรุปรายการความเสี่ยงด้านความปลอดภัยที่ตกค้าง

4.2 จัดทำรายงานสรุปรายการความเสี่ยงด้านความปลอดภัยที่ตกค้าง

5. ขั้นตอนที่ 5

5.1 จัดทำคู่มือบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

5.2 ทบทวนและปรับปรุงแบบฟอร์มการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูลเพื่อให้มีความชัดเจนมากขึ้น โดยยังคงยึดตาม มาตรฐาน ISO/IEC 27001: 2005

6. ขั้นตอนที่ 6

6.1 ทำการเฝ้าระวัง (Monitor) ความเสี่ยงที่อาจเกิดขึ้น

6.2 ประชุมวางแผนสำหรับการตรวจในรอบต่อไปหรือปีต่อไป (ขั้นตอนการเฝ้าระวัง (Monitor) และการติดตาม PDCA ในรอบต่อไปหรือปีต่อไป ไม่รวมในการศึกษาครั้งนี้) สำหรับการประยุกต์ใช้มาตรการในการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ISO/IEC 27001: 2005 และ ISO/IEC 17799: 2005 ในการศึกษาครั้งนี้ได้ประยุกต์ใช้ หัวข้อสำคัญในมาตรฐาน จำนวน 9 หัวข้อ ดังรายละเอียดของมาตรฐานตามที่ระบุในภาคผนวก ก

วิธีการศึกษา (การเก็บข้อมูลและการวิเคราะห์ข้อมูล)

จากการศึกษาและรวบรวมข้อมูลทางด้านมาตรฐานการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลตามมาตรฐาน ISO/IEC 27001: 2005 ซึ่งยึดตามแนวคิดของหลักการ PDCA (Plan-Do-Check-Act) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและสามารถพัฒนาขึ้นได้อย่างต่อเนื่องนั้น สามารถสรุปแนววิธีการศึกษา เรื่องการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลได้ 7 ขั้นตอนรายละเอียดดังต่อไปนี้

1. ศึกษาระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล จากมาตรฐาน ISO/IEC 27001: 2005และมาตรฐาน ISO/IEC 17799: 2005 เพื่อศึกษาหาแนวทางการสร้างวิธีปฏิบัติงานของ ระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท โดยนำแนวคิดหลักการปฏิบัติที่ได้ มาวิเคราะห์และสร้างเป็นวิธีการดำเนินการ 6 ขั้นตอน ดังที่แสดงไว้ในขอบเขตการศึกษา

2. ศึกษาและออกแบบระบบเอกสาร เพื่อใช้สำหรับการสำรวจและประเมินความเสี่ยงตามมาตรฐานการสำรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลเพื่อปรับใช้เฉพาะใน

องค์กร โดยผู้ศึกษาได้ศึกษาระบบเอกสารที่สำหรับใช้ในระบบการบริหารความเสี่ยงเพื่อเก็บเป็นข้อมูลทุติยภูมิรายละเอียดได้ดังนี้

2.1 ศึกษาเอกสาร แบบฟอร์มต่างๆที่ใช้ในระบบ ISO/IEC 27001: 2005 เช่น ISO/IEC 27001 Router Security Audit Checklist, ISO/IEC 27001 Audit question เป็นต้น เพื่อศึกษารูปแบบแนวทางในการนำเอาข้อกำหนดต่างๆ ของระบบมาใช้ในการบวนการตรวจสอบภายใน รวมถึงรูปแบบในการประเมินความเสี่ยงและการรายงานความเสี่ยงด้วย

2.2 ศึกษาเอกสาร แบบฟอร์มต่างๆ ที่มีใช้งานในบริษัท เช่นเอกสารระบบ ISO 9000 เพื่อนำรูปแบบของเอกสารมาปรับใช้ ในระบบการจัดการความเสี่ยงเทคโนโลยีสารสนเทศด้านความปลอดภัยของข้อมูล โดยผู้ศึกษาได้นำเนื้อหา สาระสำคัญและ ข้อกำหนดของมาตรฐาน ISO/IEC 27001: 2005 มาใส่ลงในแบบแบบฟอร์มเดิม ที่มีใช้งานอยู่ในบริษัท เพื่อให้ง่ายต่อการนำไปใช้งานเนื่องจากเป็นรูปแบบที่คุ้นเคย แต่อาจมีการปรับรูปแบบบ้างเพื่อให้สามารถคงไว้ซึ่งสาระสำคัญของมาตรฐาน ISO/IEC 27001: 2005

หลังจากการศึกษาและเก็บข้อมูลในทั้งสองส่วนแล้ว ผู้ศึกษาจึงนำข้อมูลที่ได้มาทำการวิเคราะห์โดยการนำเอารูปแบบของเอกสาร แบบฟอร์มต่างๆที่ใช้ในระบบISO/IEC 27001: 2005 กับเอกสาร แบบฟอร์มต่างๆ ที่มีใช้งานในบริษัทมาปรับและผสมผสาน ซึ่งผู้ศึกษาพยายามปรับให้มีรูปแบบที่ใกล้เคียงกับเอกสาร แบบฟอร์มที่ใช้งานในบริษัท เพื่อความสะดวกและง่ายต่อการทำความเข้าใจของผู้ใช้งาน แต่ยังคงสาระสำคัญและข้อกำหนดต่างๆตามที่มาตรฐาน ISO/IEC 27001: 2005 ระบุไว้ เพื่อใช้เป็นเอกสารแบบฟอร์มของระบบบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท

3. สำรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลตามแบบสำรวจความเสี่ยงที่ได้ออกแบบไว้ ดังนี้

ผู้ศึกษาทำการประชุมกลุ่มกับ 2 ส่วนงาน เพื่อเก็บเป็นข้อมูลปฐมภูมิโดยมีวัตถุประสงค์เพื่อเก็บข้อมูลสำหรับเตรียมการตรวจภายใน และวางแผนการแก้ไขประเด็นความเสี่ยงที่ตรวจพบ โดยมีสาระสำคัญดังต่อไปนี้

1) ส่วนงานที่ 1 ผู้ศึกษาในฐานะเป็นผู้จัดทำระบบบริหารความเสี่ยงด้านความปลอดภัยข้อมูลของบริษัทประชุมร่วมกับทีมผู้ตรวจสอบของบริษัท (Auditors) ที่มีคุณสมบัติเหมาะสมในการเป็นทีมผู้ตรวจสอบ ทั้งนี้เนื่องจากมีประสบการณ์ด้านการเป็นผู้ตรวจสอบภายในของระบบ ISO 9000, ISO 14000 ของบริษัท จำนวน 2 ท่าน ซึ่งเป็นการประชุม เพื่อวางแผน และกำหนดกรอบการตรวจ โดยมีจุดประสงค์หลัก 2 ส่วนกล่าวคือ

ส่วนแรกการอบรมผู้ตรวจ (Auditors Training) เป็นการชี้แจงให้เกิดความเข้าใจที่ตรงกันในสาระสำคัญของระบบการจัดการความเสี่ยงเทคโนโลยีสารสนเทศด้านความปลอดภัยของข้อมูล และยังเป็นการชี้แจงแบบฟอร์มต่างๆ ที่มีใช้ในระบบนี้ด้วย

ส่วนที่สองเป็นการกำหนดกรอบการตรวจในแต่ละครั้ง โดยในครั้งนี้ได้กำหนดกรอบให้เป็นไปตามขอบเขตการศึกษาที่ผู้ศึกษาได้กล่าวไว้ในข้างต้น

2) ส่วนงานที่ 2 ผู้ศึกษาในฐานะเป็นผู้จัดทำระบบบริหารความเสี่ยงด้านความปลอดภัยข้อมูลของบริษัท และเป็นหนึ่งในคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) ประชุมร่วมกับกลุ่มงาน IT Service ซึ่งทั้งหมดเป็นสมาชิกใน Working Team ซึ่งประชุมภายหลังจากตรวจสอบภายในแล้วเสร็จ โดยการประชุมเป็นการวางแผนการปฏิบัติขจัด หรือลดระดับความเสี่ยงในประเด็นที่ตรวจพบ การดำเนินการจะยึดตามกรอบปฏิบัติที่ระบบการจัดการความเสี่ยงเทคโนโลยีสารสนเทศด้านความปลอดภัยของข้อมูลที่ได้ระบุไว้ (ตามกรอบของมาตรฐาน ISO/IEC 27001: 2005)

การเก็บข้อมูลภาคสนาม เป็นการเก็บข้อมูลจากการตรวจสอบและประเมินความเสี่ยงเทคโนโลยีสารสนเทศด้านความปลอดภัยของข้อมูลภายในบริษัท โดยทำการตรวจสอบและประเมินตามกรอบการตรวจสอบภายในที่ได้วางแผนไว้ เพื่อตรวจหาจุดที่ไม่เป็นไปตามข้อกำหนดของระบบ หรือจุดที่มีความเสี่ยงที่จะส่งผลกระทบกับการดำเนินงานของบริษัท ซึ่งผู้ศึกษามีบทบาทในส่วนของทีมผู้รับการตรวจในการตรวจครั้งนี้

จากการเก็บข้อมูลภาคสนาม ผู้ศึกษาได้นำข้อมูลที่ได้มาวิเคราะห์ เพื่อประเมินความเสี่ยงที่ตรวจพบ กล่าวคือ ในการศึกษาการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัทลำพูน-ซิงเดนเก็น จำกัด ผู้ศึกษามุ่งศึกษากระบวนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001: 2005 โดยยึดตามแนวคิดของหลักการ PDCA ในการปฏิบัติจะวิเคราะห์ในมุมมองด้านความเสี่ยงที่จะมีผลกระทบกับธุรกิจของบริษัท อันเนื่องมาจากสาเหตุด้านความปลอดภัยของข้อมูล ด้วยการนำเอาข้อกำหนดการปฏิบัติงานตามมาตรฐาน ISO/IEC 27001: 2005 มาทำการตรวจสอบภายใน เน้นการจัดการด้านความปลอดภัยของข้อมูลของบริษัทและการวิเคราะห์ประเด็นความเสี่ยง โดยการจัดหมวดหมู่ความเสี่ยงที่ตรวจพบทั้งหมด ซึ่งพิจารณาจากความน่าจะเป็น (Likelihood) ของการเกิดความเสี่ยงและผลกระทบ (Impact) ที่มีต่อธุรกิจของบริษัท และใช้ตารางแมททริก (ภาพที่ 1-2) ช่วยในการวิเคราะห์ความเสี่ยงรวมทั้งการจัดลำดับความสำคัญของความเสี่ยงต่างๆ

Doc. No. : LSD_D003
Edit : 1

Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง)

ความรุนแรงและ ผลกระทบของความเสี่ยง (Impact)	โอกาสที่ความเสี่ยงจะเกิดขึ้น (Likelihood)				
	น้อยมาก (1),(VL)	น้อย (2), (V)	ปานกลาง (3), (M)	บ่อย (4), (H)	บ่อยมาก (5), (VH)
รุนแรงมาก (20) = VH					
รุนแรง (15) = V					
ปานกลาง (10) = M					
น้อย (5) = V					
น้อยมาก (1) = VL					

Risk Assessment Matrix

VH = มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก)	20	40	60	80	100
H = มีความเสี่ยงและผลกระทบ (เสี่ยง)	15	30	45	60	75
M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง)	10	20	30	40	50
L = มีความเสี่ยงและผลกระทบต่ำ (ต่ำ)	5	10	15	20	25
VL = มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก)	1	2	3	4	5

ภาพที่ 1-2 ตารางเมตริกซ์การประมาณความเสี่ยง (Risk Estimation)

4. จัดทำรายงานด้านความเสี่ยงด้านความปลอดภัยของข้อมูล

หลังจากขั้นตอนการประมาณความเสี่ยง (Risk Estimation) ผู้ศึกษาได้นำข้อมูลจากผลการประมาณความเสี่ยง (Risk Estimation) มาทำการวิเคราะห์ในขั้นตอนต่อไปเพื่อจัดทำรายงานด้านความเสี่ยงด้านความปลอดภัยของข้อมูลโดยมีขั้นตอนดังนี้

4.1 พิจารณาว่ามีหรือไม่มีความเสี่ยงในองค์กร

4.2 หากมีการตรวจพบประเด็นความเสี่ยงให้นำผลการประมาณความเสี่ยง (Risk Estimation) มาจัดลำดับความสำคัญ (เรียงตามระดับผลกระทบ*โอกาสที่ความเสี่ยงจะเกิดขึ้น) เพื่อจัดลำดับ ก่อนและหลัง สำหรับการดำเนินการขจัดความเสี่ยง หรือลดระดับความเสี่ยง เพื่อเป็นข้อมูลให้กับคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) นำไปดำเนินการ

5. นำเสนอแผนวิธีการควบคุมและป้องกันความเสี่ยงด้านความปลอดภัยของข้อมูลให้แก่ผู้บริหาร

6. ดำเนินการตามแผนวิธีการควบคุมและป้องกันความเสี่ยงด้านความปลอดภัยของข้อมูลตามที่ผู้บริหารเห็นชอบ

7. จัดทำรายงานความเสี่ยงตกค้างเสนอผู้บริหาร

แผนการดำเนินการ

แผนการดำเนินการของการค้นคว้าแบบอิสระครั้งนี้มีขั้นตอนในการดำเนินการดังต่อไปนี้

1. เสนอแนวความคิดต่อผู้บังคับบัญชาเพื่อให้เกิดการตระหนักและยอมรับการดำเนินงานในเบื้องต้นและให้การสนับสนุนในการดำเนินงาน

2. ดำเนินการตาม“แผนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท ลำพูนซิงเดนเก็น จำกัด” ทั้ง 6 ขั้นตอน ดังที่แสดงไว้ในขอบเขตการศึกษา

3. จัดทำรายงานการค้นคว้าอิสระ