บทที่ 4

สรุปผลการศึกษา อภิปรายผลการศึกษา ข้อค้นพบและข้อเสนอแนะ

การศึกษาเรื่อง “การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท ลำพูนซิงเดนเก็น จำกัด ” มีวัตถุประสงค์เพื่อศึกษาความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัท ลำพูนซิงเดนเก็น จำกัด ในปัจจุบันและจัดทำมาตรฐานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลขึ้นใช้ในบริษัท โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001:2005และมาตรฐาน ISO/IEC 17799:2005 ซึ่งผู้ศึกษาได้มีการศึกษาขั้นตอนวิธีการและเอกสารที่เกี่ยวข้อง ในการจัดทำระบบที่เป็นมาตรฐานตามแบบฉบับของมาตรฐาน ISO จนทำให้ได้มาซึ่งระบบที่เป็นมาตรฐานใช้สำหรับการ บริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ตลอดจนได้มีการนำเอาระบบที่ได้จัดทำขึ้นไปใช้ในการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัทและกำหนดแนวทางการแก้ไข ตามที่มาตรฐานได้ระบุไว้ เพื่อขจัดความเสี่ยงหรือลดระดับความเสี่ยงให้อยู่ในระดับที่ควบคุมได้หรือรับได้นั่นเอง เพื่อป้องกันไม่ให้เกิดผลกระทบต่อการดำเนินกิจการของบริษัทอันเนื่องมาจากการขัดข้องหรือหยุดให้บริการด้านข้อมูลสารสนเทศ ซึ่งนั่นเองเปรียบเสมือนจุดหมายปลายทางของการบริหารความเสี่ยง โดยสามารถสรุปผลการศึกษาได้เป็น 2 ส่วนดังนี้

ส่วนที่ 1 การจัดทำระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

ส่วนที่ 2 การตรวจ ประเมินและการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

สรุปผลการศึกษา

ในการศึกษาครั้งนี้ ทำการดำเนินการตามกรอบแนวคิดระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล 6 ขั้นตอน โดยสามารถสรุปผลการศึกษาได้

1. จัดตั้งคณะทำงานและวางแผนการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล

การจัดทำระบบบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ผู้ศึกษาได้แบ่งงานออกเป็น 2 ขั้นตอนดังนี้

ขั้นตอนที่1 เป็นการจัดตั้งคณะทำงานภายในระบบ ซึ่งเป็นการวางโครงสร้างด้านบุคคลภายในระบบ โดยแบ่งออกเป็น 2 ชุดคือ

1) คณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล (Team Auditor) ทำหน้าที่เป็นทีม ผู้ตรวจ ทำการตรวจสอบภายในเพื่อหาประเด็นความเสี่ยงหรือประเด็นที่ไม่เป็นไปตามมาตรฐานที่ระบบได้ระบุไว้ โดยได้มีการแต่งตั้ง ผู้ตรวจ (Auditor) ไว้จำนวน 2 ท่าน

โดยทั้ง 2 ท่านนั้นมีประสบการณ์ในการเป็นผู้ตรวจ (Auditor) ภายในของระบบ ISO 9000 และISO 14000 และยังเป็นผู้เชี่ยวชาญงานทางด้านสารสนเทศของบริษัท ซึ่งถือได้ว่าทั้ง 2 ท่านนั้นมีคุณสมบัติเหมาะสมตามที่ระบบต้องการ

2) คณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) ทำหน้าที่เป็นทีมงานในการ วางแผน กำหนดแนวทางการแก้ไขและ ดำเนินการ ขจัดความเสี่ยงหรือลดระดับความเสี่ยงให้อยู่ในระดับที่ควบคุมได้หรือยอมรับได้ (คะแนนอยู่ในระดับ 1-10 ถูกประมาณค่าความเสี่ยงอยู่ในระดับต่ำมาก (VL.)) โดยคณะทำงานนี้มีสมาชิกทั้งหมด 3 ท่าน ซึ่งทั้งหมดสังกัดอยู่ในกลุ่มงาน IT Service รวมถึงผู้ศึกษาเอง ก็เป็นหนึ่งในทีมงานด้วยเช่นกัน

ขั้นตอนที่2 เป็นส่วนของการจัดทำระบบ เอกสาร แบบพอร์มต่างๆ ที่ใช้ในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลโดยมีรายละเอียดต่างๆ ของเอกสารดังแสดงไว้ในตารางที่ 4-1

ตารางที่ 4-1 *สรุปรายละเอียดเอกสาร แบบพอร์มในระบบบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล*

หมายเลขเอกสาร	ชื่อเอกสาร	รายละเอียดและคำอธิบาย
LSD_D001	Information Risk Management for Data Security Systems Requirements	เป็น Requirements ของระบบโดยอ้างอิงมาจาก มาตรฐาน ISO/IEC 27001:2005
LSD_D002	Internal Audit Manual	เป็นแนวทางปฏิบัติและตรวจสอบด้านความปลอดภัยของข้อมูลตามมาตรฐาน ISO/IEC 17799 โดยทำการเรียบเรียงให้แนวทางปฏิบัติมีความสอดคล้องกับข้อกำหนดตามมาตรฐาน ISO/IEC 27001:2005
LSD_D003	Risk Estimation	เป็นกฎเกณฑ์ในการใช้ประมาณความเสี่ยงที่ตรวจพบ เพื่อนำไปจัดลำดับความสำคัญและวางแผนกการขจัดความเสี่ยงต่อไป

(ต่อ)

หมายเลขเอกสาร	ชื่อเอกสาร	รายละเอียดและคำอธิบาย
LSD_F001	Information Risk Management For Data Security Requirement & Audit Scope Matrix	เป็นแบบฟอร์มที่ใช้วางแผนการตรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล โดยเป็นเชื่อมโยงความสัมพันธ์ระหว่างขอบเขตที่การตรวจกับข้อกำหนด
LSD_F002	Internal Audit Checklist	เป็นแบบฟอร์มที่เชื่อมโยงความสัมพันธ์ระหว่างขอบเขตที่การตรวจกับข้อกำหนดที่ต้องตรวจสอบในอีกรูปแบบหนึ่งและมีเพิ่มในส่วนของแนวทางของคำถามหรือข้อสังเกตที่เรียกว่า (Audit Question) เพื่อเป็นแนวทางให้กับผู้ตรวจ
LSD_F003	Internal Audit Report	เป็นแบบฟอร์มรายงานความเสี่ยงที่ตรวจพบ พร้อมทั้งแสดงการประเมินระดับความเสี่ยง
LSD_F004	Corrective Action Request	เอกสารร้องขอให้มีการแก้ไขประเด็นความเสี่ยงที่ตรวจพบ
LSD_F005	Notify Risk Data Security	แบบฟอร์มแจ้งความเสี่ยงด้าน ความปลอดภัยของข้อมูล โดยใช้เมื่อพบประเด็นความเสี่ยงเพิ่มเติมหลังการตรวจ

2. การตรวจ ประเมินและการวางแผนจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

จากการตรวจสอบภายในด้านความปลอดภัยของข้อมูลในครั้งนี้ สามารถสรุปกระบวนการในการดำเนินการได้ดังนี้

2.1 ประชุมร่วมระหว่างผู้ตรวจและผู้รับการตรวจ เพื่อเป็นการทำความเข้าใจในขอบเขตของการตรวจครั้งนี้

2.2 ผู้ตรวจทำการตรวจสอบภายในด้านความปลอดภัยของข้อมูลตามขอบเขตที่ได้ตกลงร่วมกับผู้รับการตรวจไว้ โดยในการตรวจครั้งนี้ผู้ตรวจ ตรวจพบประเด็นความเสี่ยงทั้งหมด 27 ประเด็น

2.3 ผู้ตรวจทำการนัดประชุมร่วมเพื่อทำการประมาณค่าความเสี่ยงที่ตรวจพบ โดยปรากฏที่ประชุมประมาณค่าความเสี่ยงที่อยู่ในระดับ ปานกลางและเสี่ยง จำนวน 11 ประเด็น โดยผู้ตรวจได้ทำการออกเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR.) ใน 11 ประเด็นความเสี่ยงดังกล่าวจึงทำให้ผู้รับผิดชอบต้องดำเนินการแก้ไขโดยทันที ต่อมาที่ประชุมได้ประมาณค่าความเสี่ยงที่อยู่ในระดับ ต่ำ ไว้จำนวน 10 ประเด็นโดยแจ้งให้มีการนำเสนอแผนในการดำเนินการในลำดับถัดไปและสุดท้ายที่ประชุมได้ประมาณค่าความเสี่ยงที่อยู่ในระดับ ต่ำมาก จำนวน 6 ประเด็นซึ่งถือได้ว่าประเด็นดังกล่าวเป็นความเสี่ยงที่ยอมรับได้

3. ดำเนินการตามแผนการจัดการความเสี่ยง

การดำเนินการแก้ไขประเด็นความเสี่ยงที่ตรวจพบ โดยทำการดำเนินการในประเด็นที่ได้รับการออกเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR.)ก่อนส่วนในประเด็นอื่นให้ทำการวางแผนการแก้ไขและดำเนินการเป็นลำดับถัดไป

4. การติดตามผลการแก้ไขการเฝ้าระวังและการรายงานความเสี่ยงตกค้าง

การติดตามผลการแก้ไข ขั้นตอนนี้จัดให้มีระบบติดตามการดำเนินการ โดยให้ผู้รับผิดชอบสามารถรายงานความถืบหน้าในประเด็นที่ตนรับผิดชอบและผู้บริหารสามารถติดตามความถืบหน้าได้โดยตลอด

การเฝ้าระวัง ขั้นตอนนี้ได้ทำการแจ้งให้ผู้เกี่ยวข้องได้ทราบโดยทั่วกันว่าหากพบประเด็นความเสี่ยงเพิ่มเติมนอกเหนือจากการตรวจ ให้รายงานผู้บริหารให้รับทราบโดยใช้แบบฟอร์มแจ้งความเสี่ยงด้าน ความปลอดภัยของข้อมูล (Notify Risk Data Security)

5. การจัดทำคู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

จัดทำคู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ประจำปี พ.ศ. 2555 เพื่อเป็นแนวทางให้สำหรับให้หน่วยงานอื่นๆ ในบริษัทนำระบบดำเนินการต่อไป

6. สำรวจและประเมินความเสี่ยง ในรอบต่อไป

ในขั้นตอนนี้เปรียบได้กับการทำ PDCA ในรอบต่อไป ซึ่งจะมีการดำเนินการในปี พ.ศ. 2556 และไม่ถือเป็นส่วนหนึ่งการศึกษาครั้งนี้

อภิปรายผลการศึกษา

เมื่อนำกระบวนการดำเนินการที่ได้ดำเนินการตามกรอบแนวคิดในการศึกษาและผลการศึกษามาวิเคราะห์เทียบเปรียบเทียบกับกรอบแนวคิด PDCA พบว่าในการศึกษาครั้งนี้สามารถดำเนินการตามกรอบแนวคิดของ PDCA ในรอบที่ 1 ได้ ซึ่งในการศึกษาครั้งนี้จะเน้นในเรื่องของการจัดสร้างระบบและการนำระบบที่สร้างขึ้นไปตรวจสอบภายในเพื่อหาประเด็นความเสี่ยงในด้านความปลอดภัยของข้อมูล ตลอดจนการดำเนินการแก้ไขหรือขจัดความเสี่ยงที่ตรวจพบและจากการศึกษาจะเห็นได้ว่าในขั้นตอนของการ ติดตาม เฝ้าระวังความเสี่ยงนั้น เป็นเพียงการสร้างระบบเตรียมรอไว้เท่านั้น เนื่องจากยังไม่มีการพบประเด็นความเสี่ยงเพื่อเติมภายหลังการตรวจสอบภายใน

จากการศึกษาครั้งนี้จะเห็นว่า ระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ที่สร้างขึ้นสามารถเพิ่มคุณภาพ ในด้านการให้บริการด้านข้อมูลสารสนเทศขององค์กร ให้มีความถูกต้อง เป็นปัจจุบันและให้บริการอย่างต่อเนื่อง อีกทั้งยังมีการปรับปรุงงานอย่างต่อเนื่อง เพื่อให้สามารถตอบสนองต่อความต้องการใช้ข้อมูลของทั้งองค์กร ซึ่งก็สอดคล้องกับหลักการของ TQM (Total Quality Management) ที่มุ่งเน้นการพัฒนาและปรับปรุงคุณภาพอย่างต่อเนื่องในทุกๆ กิจกรรม

จากผลการศึกษาพบว่า การจัดทำระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001: 2005 นั้น จำเป็นต้องนำเอาแนวปฏิบัติตาม มาตรฐาน ISO/IEC17799: 2005 มาปรับใช้คู่กันเสมอ เนื่องจากมาตรฐาน ISO/IEC 27001: 2005 นั้นเป็นการวางโครงสร้างของระบบ ด้วยการวางมาตรการหรือข้อกำหนดในการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศไว้ แต่ไม่ได้ระบุแนวทางการปฏิบัติไว้ จึงเป็นการยากที่องค์กรจะหาแนวทางการปฏิบัติที่ถูกต้องได้

จากผลการศึกษาพบว่า การนำเอาระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001: 2005 มาใช้นั้น สามารถตรวจสอบระบบสารสนเทศในด้านความปลอดภัยของข้อมูลได้อย่างครบทุกแง่มุม (กิจกรรม, Software, Hardware, บุคลากร) ซึ่งในบางแง่มุมทีมงานที่ดูแลระบบสารสนเทศของบริษัท ยอมรับกันว่าเป็นเรื่องใกล้ตัวที่ถูกมองข้ามไป ทำให้มีความเสี่ยงเกิดขึ้น อาทิเช่นกรอบระยะเวลาของการเปลี่ยน Password Administrator ที่ไม่ได้ปฏิบัติตาม เป็นต้น

จากผลการศึกษาในด้านระบบเอกสารพบว่า ระบบเอกสารมีความคล้ายคลึงกับระบบเอกสารของระบบ ISO 9000 ที่บริษัทมีอยู่และในเอกสารบางฉบับสามารถนำรูปแบบมาปรับใช้งานในระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลได้

ในขั้นตอนของการประมาณค่าความเสี่ยง เพื่อจัดลำดับความสำคัญ ความจำเป็นเร่งด่วน ในการดำเนินการแก้ไขประเด็นความเสี่ยงนั้น อาจมีประเด็นความเสี่ยงบางประเด็นที่ผลการประมาณค่าความเสี่ยงแล้วได้คะแนนที่เท่ากัน โดยในกรณีนี้ผู้บริหารของบริษัทจะพิจารณาให้ดำเนินการแก้ไขในประเด็นที่มีความเสี่ยงและผลกระทบสูงก่อนเป็นอันดับแรก แต่หากประเด็นดังกล่าวมีค่าความเสี่ยงและผลกระทบสูงในระดับที่เท่ากัน ผู้บริหารของบริษัทจะพิจารณาระบบป้องกันที่มีอยู่ในปัจจุบันของทั้งสองประเด็นเพื่อประกอบการตัดสินใจ

จากผลการศึกษาพบว่า ประเด็นที่มีการผิดข้อกำหนดของมาตรฐาน ISO/IEC 27001: 2005 หลายๆ ประเด็นเป็นเรื่องของการกำหนดนโยบายและการทบทวนนโยบาย เนื่องจากเดิมการกำหนดนโยบายด้านความปลอดภัยของข้อมูลของผู้บริหารเป็นการกำหนดตามที่ผู้บริหารเห็นควรและจำเป็นต่อองค์กร โดยไม่มีกรอบมาตรฐานที่ชัดเจน อีกทั้งการทบทวนนโยบายก็ไม่ได้ทำการทบทวนครบทุกประเด็น โดยจะทบทวนแต่ประเด็นที่เป็นที่สนใจในขณะนั้นหรือในปีนั้นๆ เท่านั้น

จากการศึกษาครั้งนี้ผู้ศึกษาได้นำเอากระบวนการตรวจติดตามภายใน (Internal Audit) มาปรับใช้ในการตรวจสอบและประเมินความเสี่ยง โดยจะเห็นว่าการตรวจสอบเป็นการตรวจสอบจากบุคคลภายในหน่วยงานสารสนเทศเอง ซึ่งจะแตกต่างจากหลักการของการตรวจติดตามภายใน (Internal Audit) ที่จะใช้ทีมผู้ตรวจเป็นบุคคลที่อยู่ภายนอกหน่วยงาน แต่เนื่องจากข้อมูลทางด้านระบบสารสนเทศเป็นข้อมูลเฉพาะที่ต้องใช้ความรู้ความชำนาญเฉพาะด้าน อีกทั้งยังเป็นข้อมูลที่ความลับของบริษัท ดังนั้นผู้จัดการแผนกสารสนเทศจึงไม่อนุญาตให้ผู้ตรวจที่เป็นบุคคลนอกหน่วยงานสารสนเทศเข้าร่วมในทีมผู้ตรวจ แต่เนื่องจากต้องการติดตามผลการแก้ไขและให้มีการตรวจสอบอย่างต่อเนื่อง การนำเอาหลักการของกระบวนการตรวจติดตามภายใน (Internal Audit) มาปรับใช้ในการศึกษาครั้งนี้จึงถือว่ามีความเหมาะสมกับองค์กรและวัฒนธรรมองค์กรของ บริษัท ลำพูนซิงเด็นเก็น จำกัดเท่านั้น

จากผลการศึกษาเมื่อนำไปเปรียบเทียบกับ การค้นคว้าแบบอิสระของ พัทธ์ธีรา โอศิริ (2549) ที่ได้ทำการค้นคว้าแบบอิสระ เรื่องระบบประเมินและวิเคราะห์ความเสี่ยงในการจัดการด้านระบบสารสนเทศ พบว่ามีการนำกรอบแนวคิดของ มาตรฐาน ISO/IEC 27001: 2005 และ มาตรฐาน ISO/IEC17799: 2005 มาปรับใช้ในการศึกษาเช่นเดียวกัน แต่มีความแตกต่างกันที่จุดมุ่งหมายหรือวัตถุประสงค์การศึกษา ซึ่งการค้นคว้าแบบอิสระของ พัทธ์ธีรา โอศิริ เน้นการสร้างระบบสารสนเทศที่เป็นโปรแกรมช่วยในการ ประเมินและวิเคราะห์ความเสี่ยง ซึ่งพบปัญหาว่าคำแนะนำที่ได้จากระบบนั้นไม่สามารถแก้ปัญหาได้จริง เนื่องจากปัญหาหรือประเด็นความเสี่ยงที่ตรวจพบมีความหลากหลายและมีคุณสมบัติเฉพาะของแต่ละองค์กร แต่ในการศึกษาของผู้ศึกษาครั้งนี้ มุ่งเน้นในการสร้างระบบขึ้นมาใช้งานจริงโดยมุ่งที่จะดำเนินการแก้ไขประเด็นความเสี่ยงให้ได้ผลจริง ซึ่ง

การประเมินความเสี่ยง การวิเคราะห์ความเสี่ยงและการเลือกแนวทางการแก้ไขนั้นมาจากความเห็นของคณะทำงานในโครงสร้างของระบบที่ได้รับการแต่งตั้ง ซึ่งทุกท่านมีความเข้าใจในกระบวนการของระบบสารสนเทศของบริษัทและยังเข้าใจกระบวนการดำเนินการทางธุรกิจของบริษัทเป็นอย่างดี ทำให้การประเมินความเสี่ยง การวิเคราะห์ความเสี่ยงและการเลือกแนวทางการแก้ไขนั้นมีความเหมาะสมและสามารถแก้ปัญหาได้จริงกับบริษัท ลำพูนซิงเด็นเก็น จำกัด

จากการศึกษาครั้งนี้ทำให้ทราบว่า ข้อมูลสารสนเทศของบริษัทนั้นมีความสำคัญต่อการดำเนินกิจการภายในเป็นอย่างมากและยังพบว่าการดูแลข้อมูลสารสนเทศในปัจจุบันนั้นยังมีจุดที่ต้องทำการปรับปรุงในหลายๆจุดเพื่อนำไปสู่การบริหารจัดการด้านความปลอดภัยของข้อมูล ที่เป็นไปตามมาตรฐานสากลหรือให้เป็นไปตามมาตรฐาน ISO/IEC 27001:2005 ที่นำมาใช้ในการศึกษาครั้งนี้ ซึ่งทั้งหมดก็เพื่อเป้าหมายใหญ่คือการให้บริการข้อมูลสารสนเทศภายในองค์กรได้อย่างต่อเนื่องตลอดเวลารวมถึงมีการกำกับดูแลที่ดีตามมาตรฐานสากล

ข้อค้นพบ

จากการศึกษาเรื่อง “ การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัท ลำพูน ซิงเดนเก็น จำกัด ” มีข้อค้นพบที่น่าสนใจดังนี้

1. การดำเนินการต้องเริ่มต้นจากความเห็นชอบจากผู้บริหารอีกทั้งยังต้องได้รับการสนับสนุนจากบริหารด้วย เนื่องจากการดำเนินการเกี่ยวข้องกับหลายส่วนงาน การได้รับการสนับสนุนจากบริหาร จะเป็นแรงผลักดันที่สำคัญมากที่จะทำให้ระบบประสบความสำเร็จ
2. ในการศึกษาครั้งนี้ในขั้นตอนการประเมินความเสี่ยงและการประมาณค่าความเสี่ยงเป็นขั้นตอนที่สำคัญอย่างมาก แต่จากผลการศึกษาพบว่า การประเมินความเสี่ยงและการประมาณค่าความเสี่ยงนั้นอาศัยการวินิจฉัยของทีมผู้ตรวจเป็นหลัก ดังนั้นการเลือกทีมผู้ตรวจสอบภายใน จึงต้องเลือกบุคคลที่มีคุณสมบัติตรงและเหมาะสมกับระบบที่สร้างขึ้น เช่นต้องเป็นผู้มีความรู้ในด้านการตรวจสอบภายใน ต้องมีความเข้าใจในกระบวนการทำงานภายในองค์กรและต้องมีความรู้ในด้านระบบสารสนเทศ เป็นต้น ซึ่งจะส่งผลไปถึงเรื่องของผลสำเร็จของการบริหารจัดการด้านความปลอดภัยของข้อมูลขององค์กร
3. การประชุม อบรม ชี้แจง ทีมผู้ตรวจถือเป็นขั้นตอนที่สำคัญขั้นตอนหนึ่ง เพราะนอกเหนือจากเป็นการ ชี้แจงขอบเขตในการตรวจสอบภายในแล้ว ยังเป็นการชี้แจงทำความเข้าใจในระบบที่สร้างขึ้น รวมถึงการชี้แจงการนำเอกสาร แบบฟอร์มไปใช้งาน

ด้วย เนื่องจากการตรวจสอบเป็นการตรวจสอบครั้งแรก ถึงแม้ว่าทีมผู้ตรวจจะมีประสบการณ์ในด้านการเป็นผู้ตรวจสอบภายในระบบอื่นๆมาแล้วก็ตาม เพราะมีรายละเอียดหลายจุดที่มีความแตกต่างกันจึงต้องมีการทำความเข้าใจก่อนการตรวจจริง

4. จากการศึกษาพบว่า การตรวจสอบภายในและการตรวจพบประเด็นความเสี่ยงนั้น ถือเป็นการพิจารณาในมุมมองที่มาจากกิจกรรมและการดำเนินงานภายในบริษัท ลำพูนซิงเด็นเก็น จำกัดเท่านั้น ซึ่งในแต่ละประเด็น เมื่อนำระบบหรือข้อกำหนดไปทำการตรวจสอบภายในกับองค์กรอื่นๆ ผลของการพิจราณาอาจมีความเห็นที่แตกต่างกันออกไป
5. จากการศึกษาครั้งนี้ การประมาณค่าความเสี่ยงเป็นการพิจารณาจากผลกระทบที่อาจจะเกิดขึ้นกับธุรกิจของ บริษัทลำพูนซิงเด็นเก็น จำกัด เท่านั้นซึ่งจะเห็นว่าผลของค่าความเสี่ยงที่มีการประมาณค่าความเสี่ยงและจัดลำดับไว้นั้น ก็เป็นข้อสรุปจากความเห็นของทีมผู้ตรวจ ดังนั้นหากมีการเปลี่ยนแปลงทีมผู้ตรวจสอบภายใน ผลของการประมาณค่าความเสี่ยงก็อาจมีข้อแตกต่างกันออกไป
6. การติดตาม เฝ้าระวังความเสี่ยง จากการศึกษาครั้งนี้พบว่ายังไม่มีการพบประเด็นความเสี่ยงเพื่อเติมภายหลังการตรวจสอบภายใน เนื่องจากระบบที่สร้างขึ้นเป็นระบบนำร่องและยังไม่มีการนำไปใช้อย่างเป็นทางการในระดับบริษัท จึงอาจทำให้ผู้เกี่ยวข้องเมื่อพบประเด็นความเสี่ยงแล้ว แต่ไม่ทำการแจ้งประเด็นความเสี่ยงตามที่ระบบได้กำหนดไว้ ทำให้มีประเด็นความเสี่ยงที่ไม่มีการตรวจพบและไม่มีการควบคุมเกิดขึ้นในบริษัทได้
7. ในการศึกษาครั้งนี้ สามารถสร้างระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ขึ้นใช้งานในบริษัทได้ โดยสามารถตรวจสอบความเสี่ยงด้านความปลอดภัยและมีระบบควบคุมดูแลด้านความปลอดภัยของข้อมูลที่เป็นมาตรฐานสากล ถึงแม้ว่าการดำเนินการแก้ไขหรือขจัดความเสี่ยง จะยังคงมีความล่าช้าอยู่บ้างเนื่องจากเหตุผลด้านเวลาในการดำเนินการหรืองบประมาณในการดำเนินการ แต่ก็สามารถนำไปบรรจุไว้ในแผนงานในปีถัดไปได้ ซึ่งระบบที่สร้างขึ้นก็มีขั้นตอนรองรับอยู่แล้วในส่วนของการรายงานความเสี่ยงตกค้างแก่ผู้บริหาร
8. จากการศึกษาครั้งนี้ พบว่าบุคลากรในองค์กรมีความเข้าใจในมุมมองด้านการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลและมุมมองด้านความสำคัญของข้อมูลสารสนเทศที่มีต่อองค์กรดีขึ้น โดยเฉพาะอย่างยิ่งทำให้ผู้บริหารเกิดความตระหนักและให้ความสำคัญในด้านความปลอดภัยของข้อมูลมากขึ้น อีกทั้งยังทำให้ผู้บริหารทราบ

ถึงประเด็นความเสี่ยงที่มีในองค์กร อันจะนำไปสู่การดำเนินการแก้ไขและขจัดความเสี่ยง รวมถึงการวางแผนด้านงบประมาณสำหรับการดำเนินการแก้ไขและขจัดความเสี่ยงต่อไป

9. จากการศึกษาครั้งนี้ ในขั้นตอนของ Management Review ยังไม่สามารถทำได้ในภาพรวมขององค์กร เนื่องจากผู้ศึกษายังไม่สามารถนำเอาผู้บริหารระดับสูง ที่มีอำนาจในการตัดสินใจในองค์กรมาร่วมในโครงการได้
10. ในการสร้างระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลแบบสมบูรณ์ ยังต้องมีการศึกษาเพิ่มเติมและปรับปรุงอีกมาก ซึ่งอาจจะต้องให้ผู้เชี่ยวชาญมาช่วยในการตรวจประเมินความเสี่ยงและให้คำแนะนำในการปรับปรุงระบบ

ข้อเสนอแนะ

จากการศึกษาเรื่อง “ การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัท ลำพูน ซิงเคนเก็น จำกัด ” มีข้อเสนอแนะที่น่าสนใจดังนี้

1. หากต้องการให้ระบบประสบความสำเร็จอย่างแท้จริงในระดับองค์กร การสร้างระบบหรือการดำเนินการต่างๆ ควรเป็นการสั่งการหรือเป็นนโยบายของผู้บริหาร ลงมาสู่ผู้ปฏิบัติงานหรือผู้เกี่ยวข้อง จึงจะได้มาซึ่งความร่วมมือกันทั้งองค์กร โดยจะเห็นได้จากปัญหาที่เกิดในการศึกษาครั้งนี้คือ การดำเนินการแก้ไขประเด็นความเสี่ยงเกิดความล่าช้า ซึ่งส่วนหนึ่งมาจากการไม่ได้ถูกสั่งการมาจากระดับนโยบายนั่นเอง โดยการติดตามของผู้บริหารในแต่ละเดือนเป็นเพียงการสอบถามความก้าวหน้าเท่านั้น
2. การติดตามการดำเนินการแก้ไขหรือขจัดความเสี่ยง ควรเป็นการติดตามจากผู้บริหารเพื่อให้ผู้เกี่ยวข้องเกิดการตื่นตัวในการดำเนินการแก้ไข
3. ระบบเอกสารที่ออกแบบและใช้งานในการศึกษาครั้งนี้ควรจะมีการปรับปรุงตามความเหมาะสมในการใช้งานภายในองค์กร โดยควรมีการดัดแปลงรูปแบบของเอกสารให้มีความใกล้เคียงกับเอกสารที่มีใช้ในบริษัท เพื่อสะดวกในเรื่องของการทำความเข้าใจและการนำไปปฏิบัติ แต่ต้องคงไว้ซึ่งเนื้อหาหรือข้อกำหนดของมาตรฐาน ISO/IEC 27001:2005 ให้ครบถ้วน เนื่องจากรายละเอียดการตรวจสอบอาจมีความแตกต่างกันตามลักษณะการใช้งานระบบสารสนเทศและข้อมูลในแต่ละองค์กร
4. ขั้นตอนของการเลือกบุคคลเข้ามาอยู่ในคณะทำงาน ถือว่าเป็นส่วนสำคัญมาก โดยควรเลือกบุคคลให้เหมาะสมกับที่ระบบต้องการ เนื่องจากจะเห็นได้ว่าผลการดำเนินงานในแต่ละขั้นตอน ทั้งขั้นตอนการตรวจสอบภายในและการเลือกแนวทางการแก้ไข

ประเด็นความเสี่ยงนั้น ล้วนแต่ต้องอาศัยความเห็นและการตัดสินใจของคณะทำงานทั้งสิ้น

5. การรายงานประเด็นความเสี่ยงให้กับผู้บริหารเป็นส่วนที่สำคัญเช่นกัน ควรรายงานประเด็นความเสี่ยงให้ครบถ้วนในทุกประเด็นที่ตรวจพบ เพื่อให้ผู้บริหารรับทราบในประเด็นความเสี่ยงที่เกิดขึ้นในองค์กร รวมทั้งยังสามารถขอการสนับสนุนในการดำเนินการแก้ไขประเด็นความเสี่ยงจากผู้บริหารได้อีกด้วย เนื่องจากการปรับปรุงแก้ไขความเสี่ยงบางเรื่องเกี่ยวข้องกับระดับนโยบายด้วย
6. การชี้แจงให้คนในองค์กร เข้าใจและตระหนัก ในเรื่องความเสี่ยงและการจัดความความเสี่ยง เป็นเรื่องที่ไม่สามารถทำสำเร็จในเวลาอันสั้น จึงครรมีการชี้แจงอย่างต่อเนื่องในหลายๆ โอกาส
7. สำหรับผู้ที่นำเอาการศึกษาในครั้งนี้ ไปปรับใช้ในการสร้างระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล ตามมาตรฐาน ISO/IEC 27001: 2005 กับองค์กรอื่นๆนั้น สามารถนำเอาการศึกษาครั้งนี้ไปเป็นแนวทางในการนำไปใช้ได้ แต่ผู้ศึกษาเห็นว่า มีรายละเอียดปลีกย่อยบางประเด็นที่มีความแตกต่างกันในแต่ละองค์กร อาทิ เช่น ข้อกำหนดบางข้อที่ในการศึกษาครั้งนี้ผู้ศึกษาไม่ได้นำมาบรรจุไว้ เนื่องจากเห็นว่าไม่มีความจำเป็นกับบริษัทลำพูนซิงเด็นเก็น จำกัด เป็นต้น