บทที่ 3
ผลการศึกษา

ในการศึกษาเรื่องการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัทลำพูน ซิงเดนเก็น จำกัด มีวัตถุประสงค์ เพื่อ ศึกษากระบวนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ซึ่งผู้ศึกษาได้จัดทำระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล ที่ยึดตามแนวคิด PDCA ซึ่งเป็นไปตามมาตรฐานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ISO/IEC 27001: 2005และแนวปฏิบัติตาม มาตรฐาน ISO/IEC 17799:2005

หลังจากนั้นนำระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลที่จัดทำขึ้นไปใช้ในบริษัท โดยจัดให้มีการตรวจสอบภายใน ตามระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

ผู้ศึกษาได้สรุปผลการศึกษาตามกรอบแนวคิดระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล 6 ขั้นตอน ดังมีรายละเอียดต่อไปนี้

1. จัดตั้งคณะทำงานและวางแผนการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล

ขั้นตอนนี้เป็นขั้นตอนการดำเนินการจัดทำ “ระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล” และการวางแผนการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล ซึ่งประกอบด้วยขั้นตอนรายละเอียดดังต่อไปนี้

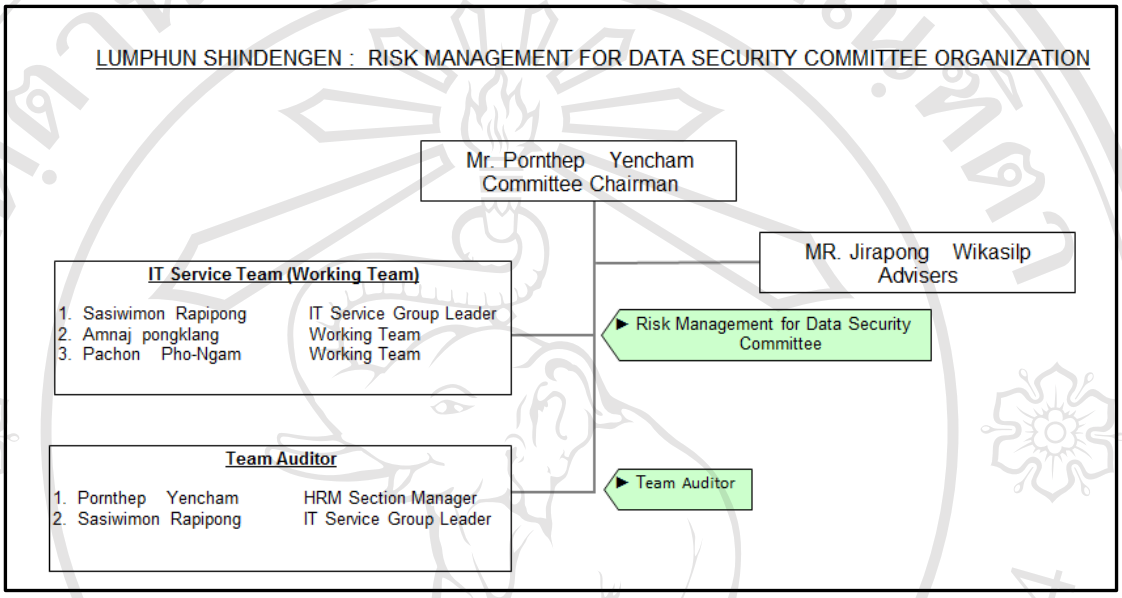
1.1 จัดตั้งคณะทำงาน

ศึกษาได้นำเสนอรายชื่อคณะทำงานด้านบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลแก่ผูบริหาร เพื่อทำการแต่งตั้งคณะทำงานในด้านต่างๆ โดยเชิญผู้เกี่ยวข้องและผู้ที่มีคุณสบบัติที่เหมาะสมเข้าร่วมเป็นคณะทำงานซึ่งแบ่งออกได้เป็น 2 ชุดดังนี้

ชุดที่ 1 คณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล (Team Auditor) ทำหน้าที่เป็นทีมผู้ตรวจ ทำการตวรจสอบด้านความปลอดภัยของข้อมูลและระบุประเด็นที่ไม่เป็นไปตามข้อกำหนดแล้วทำการประมาณค่าความเสี่ยงที่ตรวจพบ เพื่อจัดลำดับความสำคัญเร่งด่วนและแจ้งให้ผู้ที่รับผิดชอบทำการดำเนินการแก้ไขต่อไป

ชุดที่ 2 คณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) คณะทำงานชุดนี้เป็นผู้รับผิดชอบโดยตรงกับข้อมูลที่ระบุไว้ในขอบเขตการตรวจ

ครั้งนี้มีหน้าที่ในการหาแนวทางการแก้ไขหรือควบคุม ป้องกันความเสี่ยงที่ตรวจพบให้อยู่ในระดับที่ยอมรับได้หรือไม่มีความเสี่ยงนั้นๆอีก เพื่อไม่ให้เกิดผลกระทบกับการดำเนินงานของบริษัทโดยโครงสร้างของคณะทำงานทั้ง2 ชุด (ภาพที่ 3-1)



ภาพที่ 3-1 Risk Management For Data Security Committee Organization

ในส่วนของคณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล (Team Auditor) นั้น ผู้ศึกษาได้เชิญบุคคลที่ได้รับการยอมรับว่ามีประสบการณ์ด้านการตรวจสอบภายในและมีความรู้ความสามารถด้านระบบสารสนเทศ โดยมีรายละเอียดดังนี้

1) คุณพรเทพ เย็นฉ่ำ

ตำแหน่ง: ผู้จัดการแผนกบริหารทรัพยากรบุคคล ทำหน้าที่ดูแลด้านฝ่ายงานบุคคลและ ฝ่ายงานเทคโนโลยีสารสนเทศ

ประสบการณ์: LMR. Committee Chairman, Asst. QMR. ผู้ตรวจสอบภายใน ในระบบ ISO 9000, ISO 14000, มรท. (LMR คือ Labour Management Relations, QMR คือ Quality Management Representative, มรท. คือ มาตรฐานแรงงานไทย)

2) คุณศศิวิมล ระพีพงษ์

ตำแหน่ง: หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ประสบการณ์: ผู้ตรวจสอบภายใน ในระบบ ISO 9000, ISO 14000

ในส่วนของคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) เป็นทีมงานวิศวกรด้านระบบคอมพิวเตอร์ของบริษัท ซึ่งเป็นผู้รับผิดชอบโดยตรงกับข้อมูลที่ทำการตรวจสอบครั้งนี้ โดยมีรายละเอียดดังนี้

1) คุณศศิวิมล ระพีพงษ์

ตำแหน่ง: หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

2) คุณอำนาจ พงษ์กลาง

ตำแหน่ง: วิศวกรด้านระบบคอมพิวเตอร์

3) คุณผจญ โพธิ์งาม

ตำแหน่ง: วิศวกรด้านระบบคอมพิวเตอร์

1.2 จัดทำระบบเอกสารภายในระบบบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

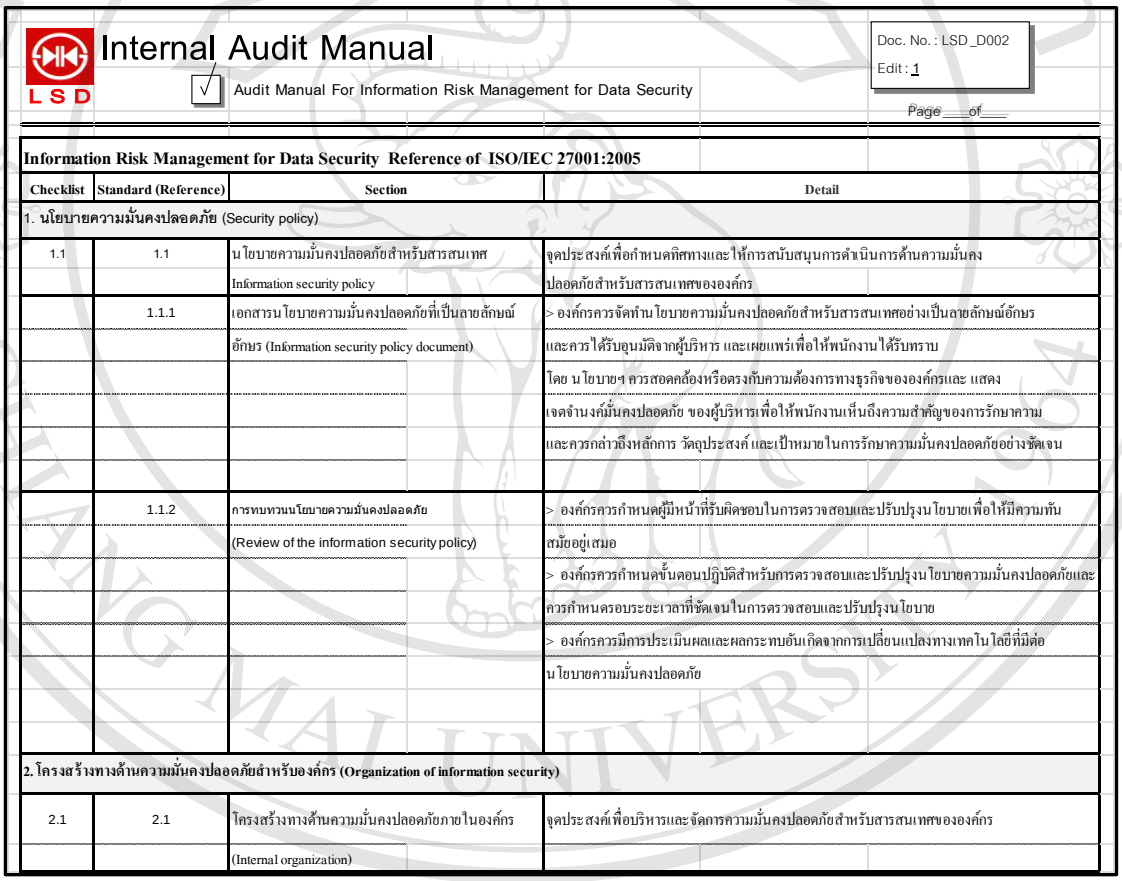
ผู้ศึกษาได้จัดทำเอกสารและแบบฟอร์มต่างๆ สำหรับใช้ในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล โดยนำรูปแบบเอกสารเดิมที่มีใช้งานในบริษัท เช่น เอกสารในระบบ ISO 9000 เป็นต้น มาปรับและเพิ่มเติมเนื้อหาของมาตรฐาน ISO/IEC 27001: 2005

เอกสารที่ใช้ในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลที่ผู้ศึกษาสร้างขึ้นมาใช้งานในระบบ มีดังนี้

1.1.1 Information Risk Management for Data Security Systems Requirements เป็นเอกสารที่นำเอา Requirements ของระบบ ISO 27001: 2005 มาบรรจุไว้เพื่อใช้เป็นกรอบการดำเนินการของระบบที่จัดทำขึ้น ซึ่งผู้ศึกษาได้ประยุกต์เอาข้อกำหนดของ มาตรฐาน ISO/IEC 27001: 2005 มาปรับใช้ในองค์กร โดยตัดส่วนบางส่วนที่ไม่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศโดยตรงและไม่ได้เกี่ยวข้องกับงานด้าน IT Service ออกไปด้วยเหตุผลที่ต้องการเน้นการตรวจเฉพาะขอบเขตงานที่ฝ่ายงานสารสนเทศรับผิดชอบโดยตรงก่อนเพื่อเป็นการนำร่องในการสร้างระบบการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูลของบริษัท แต่ยังคงไว้ซึ่งสาระสำคัญของมาตรฐาน ISO/IEC 27001: 2005 อยู่ ซึ่งทั้งหมดประกอบไปด้วยข้อกำหนด 9 ข้อกำหนดจากทั้งหมด 11 ข้อกำหนดที่มาตรฐาน ISO/IEC 27001: 2005ระบุไว้ โดยข้อกำหนดทั้ง 9 ข้อที่ใช้ในการศึกษาครั้งนี้ได้แสดงรายละเอียดไว้ในเอกสารฉบับนี้ ดังแสดงไว้ใน ภาคผนวก ก

1.1.2 Internal Audit Manual เป็นเอกสารสำหรับใช้เป็นแนวทางปฏิบัติและตรวจสอบด้านความปลอดภัยของข้อมูลให้เป็นไปตามข้อกำหนดของระบบ ซึ่งเอกสารฉบับนี้จะระบุถึงรายละเอียด แนวทางในการปฏิบัติ ที่ถูกต้องตามข้อกำหนด โดยผู้ศึกษาได้ประยุกต์เอาข้อกำหนดตามมาตรฐาน ISO/IEC 27001: 2005 ที่ได้กล่าวถึงข้อกำหนดในภาพกว้างที่เป็น

Requirements ไว้ ดังที่แสดงในเอกสาร Information Risk Management for Data Security Systems Requirements โดยนำมารวมกับข้อกำหนดตามมาตรฐาน ISO/IEC 17799 ที่เป็นการกล่าวถึงข้อกำหนดที่มีรายละเอียดในเชิงเทคนิค หรือเชิงปฏิบัติที่องค์กรควรปฏิบัติในด้านความปลอดภัยของข้อมูลเพื่อเป็นแนวทางสำหรับการตรวจ และการปรับปรุงระบบการจัดการด้านความปลอดภัยของข้อมูลของบริษัทให้เป็นไปตาม Requirements ที่ระบบกำหนดไว้โดยข้อกำหนด และแนวปฏิบัติต่างๆ ดังแสดงตัวอย่างในภาพที่ 3-2 และผู้ศึกษาได้แสดงรายละเอียดของเอกสารฉบับนี้ไว้ใน ภาคผนวก ข



Internal Audit Manual

LSD

√ Audit Manual For Information Risk Management for Data Security

Doc. No. : LSD_D002
Edit : 1
Page ___of___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005

Checklist	Standard (Reference)	Section	Detail
1. นโยบายความมั่นคงปลอดภัย (Security policy)			
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ Information security policy	จุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	> องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร และควรได้รับอนุมัติจากผู้บริหาร และเผยแพร่เพื่อให้พนักงานได้รับทราบ โดย นโยบายฯ ควรสอดคล้องหรือตรงกับความต้องการทางธุรกิจขององค์กรและ แสดงเจตจำนงค์มั่นคงปลอดภัย ของผู้บริหารเพื่อให้พนักงานเห็นถึงความสำคัญของการรักษาความและควรกล่าวถึงหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน
	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	> องค์กรควรกำหนดผู้มีหน้าที่รับผิดชอบในการตรวจสอบและปรับปรุงนโยบายเพื่อให้มีความทันสมัยอยู่เสมอ > องค์กรควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัยและควรกำหนดรอบระยะเวลาที่ชัดเจนในการตรวจสอบและปรับปรุงนโยบาย > องค์กรควรมีการประเมินผลและผลกระทบอันเกิดจากการเปลี่ยนแปลงทางเทคโนโลยีที่มีต่อนโยบายความมั่นคงปลอดภัย
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)			
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)	จุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

ภาพที่ 3-2 ตัวอย่างเอกสาร Internal Audit Manual

1.1.3 Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง) เป็นเอกสารที่ระบุถึงกฎเกณฑ์ในการประมาณความเสี่ยงที่ตรวจพบ เพื่อนำไปจัดลำดับความสำคัญและนำไปสู่การจัดลำดับการแก้ไขหรือมาตรการควบคุมความเสี่ยง โดยมาตรฐานการประเมินระดับความเสี่ยงที่จัดทำขึ้นใช้ในบริษัท ตามหลักการของการประเมินระดับความเสี่ยง มีการระบุระดับความเสี่ยงไว้ทั้งหมด 5 ระดับ คือ VH = มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก), H = มีความเสี่ยงและผลกระทบ (เสี่ยง), M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง), L = มีความเสี่ยงและ

ผลกระทบต่ำ (ต่ำ), VL = มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก) ดังตัวอย่างในภาพที่ 3-3 ซึ่งที่มาของค่าระดับความเสี่ยงได้มาจาก ค่าความรุนแรงและผลกระทบ(Impact) * โอกาสที่ความเสี่ยงจะเกิดขึ้น (Likelihood) โดยผู้ศึกษาได้แสดงรายละเอียดของเอกสารฉบับนี้ไว้ในภาคผนวก ค

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					

VH = มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก)
H = มีความเสี่ยงและผลกระทบ (เสี่ยง)
M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง)
L = มีความเสี่ยงและผลกระทบต่ำ (ต่ำ)
VL = มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก)

Risk Assessment Matrix

20	40	60	80	100
15	30	45	60	75
10	20	30	40	50
5	10	15	20	25
1	2	3	4	5

ภาพที่ 3-3 ตัวอย่างเอกสาร Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง)

จากภาพที่ 3-3 เป็นแนวทางในการวิเคราะห์ความเสี่ยงเพื่อประเมินระดับความเสี่ยง แต่ในทางปฏิบัติฝ่ายบริหารควรพิจารณาถึงปัจจัยอื่นๆประกอบ อาทิ ความเสี่ยงบางประเภทมีระดับความรุนแรงและผลกระทบของความเสี่ยงสูง ถึงแม้ว่าอาจจะมีโอกาสที่จะเกิดน้อยถึงน้อยมาก แต่ในภาพรวมอาจก่อให้เกิดผลเสียหายอย่างร้ายแรงต่อองค์กรได้

1.1.4 Information Risk Management For Data Security Requirement& Audit Scope Matrix เป็นแบบฟอร์มแรกที่ใช้ในกระบวนการวางแผนการตรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล ซึ่งเป็นแบบฟอร์มที่เชื่อมโยงความสัมพันธ์ ระหว่างขอบเขตที่กำหนดขึ้นในการตรวจในแต่ละครั้ง กับข้อกำหนดตามมาตรฐานของระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล โดยมีวัตถุประสงค์เพื่อเป็นแนวทางในการตรวจสอบ เพื่อให้ผู้ตรวจทราบได้ล่วงหน้าว่าขอบเขตที่กำลังจะตรวจสอบมีความเกี่ยวข้องกับข้อกำหนดข้อใดบ้าง เพื่อให้การตรวจสอบเกิดความรวดเร็วและแม่นยำเนื่องจากการตรวจสอบเป็นการตรวจสอบภายใน

และผู้ตรวจก็เป็นบุคคลภายในบริษัท จึงยังขาดความแม่นยำเรื่องของข้อกำหนดของระบบ ผู้ศึกษาจึงสร้างเอกสารฉบับนี้เพื่อสำหรับใช้วางแผนการตรวจ และเป็นข้อมูลสนับสนุนให้กับผู้ตรวจใช้เป็นแนวทางในการตรวจได้อีกทางหนึ่งด้วย ดังแสดงตัวอย่างในภาพที่ 3-4 และผู้ศึกษาได้แสดงรายละเอียดของเอกสารฉบับนี้ไว้ใน ภาคผนวก ต

1.1.5 Internal Audit Checklist เป็นแบบฟอร์มที่ใช้ในกระบวนการวางแผน การตรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลเช่นกัน โดยนำเอาความสัมพันธ์ของขอบเขตการตรวจกับข้อกำหนดตามมาตรฐานของระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลที่ได้จากมาจากการทำ “Audit Scope Matrix” หรือจากเอกสาร Information Risk Management For Data Security Requirement & Audit Scope Matrix นั่นเอง โดยนำมาจัดรูปแบบใหม่ให้อยู่ในแบบฟอร์มของ Internal Audit Checklist ซึ่งในส่วนของ Internal Audit Checklist นี้จะมีการระบุแนวทางของคำถามหรือข้อสังเกตที่เรียกว่า “Audit Question” ไว้ วัตถุประสงค์เพื่อเป็นแนวคำถามหรือข้อสังเกตให้กับผู้ตรวจใช้ ในการตรวจสอบหาประเด็นความเสี่ยง และยังใช้ควบคุมทิศทางของการตรวจให้เป็นไปในทิศทางที่ต้องการอีกด้วย ดังแสดงตัวอย่างในภาพที่ 3-5 และผู้ศึกษาได้แสดงรายละเอียดของเอกสารฉบับนี้ไว้ใน ภาคผนวก ฆ

1.1.6 Internal Audit Report เป็นแบบฟอร์มรายงานความเสี่ยงที่ตรวจพบ พร้อมทั้งการประเมินระดับความเสี่ยงที่ตรวจพบ เพื่อจัดลำดับความเสี่ยงและนำไปสู่การพิจรณาวางแผนแก้ไขความเสี่ยงที่ตรวจพบต่อไป โดยจะใช้งานร่วมกับเอกสาร Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง) LSD_D003 ดังแสดงตัวอย่าง Internal Audit Report ในภาพที่ 3-6 และผู้ศึกษาได้แสดงรายละเอียดของเอกสารฉบับนี้ไว้ใน ภาคผนวก ง

INFORMATION RISK MANAGEMENT FOR DATA SECURITY

REQUIREMENT & AUDIT SCOPE MATRIX

Form. No. : LSD_F001
Edit : 1 Eff.date :

Requirement	1. นโยบายความมั่นคงปลอดภัย (Security policy)	2. ระบบเอกสารส่วนกลาง (File Sharing : LSD DATA SERVER, LSD PS SERVER)	3. Database Server จำนวน 4 Server (ERP. System, MRP. System, HRMS, DB Systems)	4. Active Directory Database	5. ระบบข้อมูลสนับสนุน (Service Support Systems : Mail Server, Web Server)	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
1. นโยบายความมั่นคงปลอดภัย (Security policy)								
1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)	●							
1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	●							
1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	●							
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)								
2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)								
2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการ ทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	●							
2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	●							
2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	●							
2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)	●							
2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality Agreements)	●							
2.1.6 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบ อิสระ (Independent review of information security)	●							
2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)								
2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)	●							
2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers	●							
2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)	●							
3. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)								
3.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)								
3.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)						●	●	
3.1.2 การควบคุมการเข้า-ออก (Physical entry controls)						●	●	

ภาพที่ 3-4 ตัวอย่างแบบฟอร์ม Information Risk Management For Data Security Requirement & Audit Scope Matrix

Internal Audit Checklist

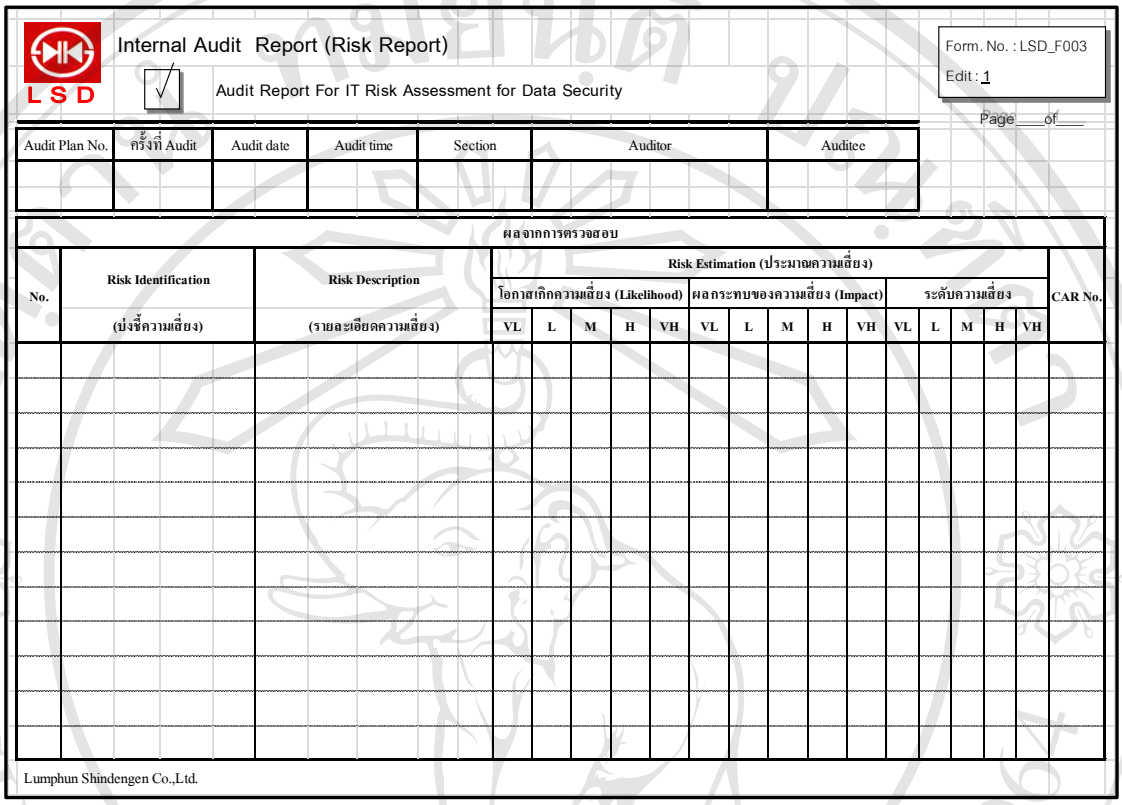
Audit Checklist For Information Risk Management for Data Security

Form. No. : LSD_F002
Edit : 1
Page ___of___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005

Checklist	Standard (Reference)	Section	Audit Question	Audit Scope	Findings (OK / NC)
1. นโยบายความมั่นคงปลอดภัย (Security policy)					
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ Information security policy			
1.1.1	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	องค์กรมีนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากผู้บริหาร และ เผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
1.1.2	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	องค์กรมีการ ทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)					
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)			
2.1.1	2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	ผู้บริหาร มีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง รวมถึงการมอบหมายงานที่เหมาะสมต่อบุคลากร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.2	2.1.2	การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	ผู้บริหาร มีการกำหนด ตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.3	2.1.3	การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	ผู้บริหาร มีการกำหนดหน้าที่ความรับผิดชอบของพนักงานใน การดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	

ภาพที่ 3-5 ตัวอย่างแบบฟอร์ม Internal Audit Checklist



Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1

Page ____of____

Audit Plan No.	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-6 ตัวอย่างแบบฟอร์ม รายงานความเสี่ยงที่ตรวจพบ Internal Audit Report (Risk Report)

1.3 การวางแผนการตรวจสอบภายในด้านความเสี่ยงด้านความปลอดภัยของข้อมูล

ผู้ศึกษาได้ประชุมร่วมกับคณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล โดยในการประชุมมีข้อสรุปให้กำหนดแผนการขั้นตอนเพื่อเตรียมการตรวจสอบภายในด้านความเสี่ยงด้านความปลอดภัยของข้อมูล โดยมีรายละเอียดดังนี้

ตารางที่ 3-1
รายละเอียดขั้นตอนการเตรียม ตรวจสอบภายใน

หัวเรื่อง	รายละเอียด	วันที่/เวลา	สถานที่
1.อบรมผู้ตรวจ (Auditor Training)	1.อธิบายภาพรวมของระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล	วันที่ 20 มีนาคม พ.ศ. 2555	Meeting Room 02
2.ประชุมเปิดการตรวจ (Audit Opening)	1. สรุปขอบเขตการตรวจครั้งนี้ รวมถึงประเด็นหรือพื้นที่ที่ต้องการเน้นเป็นพิเศษ 2.จัดทำ Audit Scope Matrix และ Internal Audit Checklist	วันที่ 20 มีนาคม พ.ศ. 2555 เวลา 13.30-16.30 น.	Meeting Room 02
3.ทำการตรวจสอบภายใน (Internal Audit)	1.ทำการตรวจสอบตามแผนและขอบเขตที่กำหนดไว้	วันที่ 2 เมษายน พ.ศ. 2555 เวลา 09.00 – 16.00 น.	Meeting Room 02
4.ประชุมสรุปและประมาณค่าความเสี่ยงที่ตรวจพบ	1.นำความเสี่ยงหรือประเด็นที่ตรวจพบมาเข้ากระบวนการประมาณค่าความเสี่ยง	วันที่ 23 เมษายน พ.ศ. 2555 เวลา 13.30 – 15.00 น.	Meeting Room 04
5.ส่งรายงานการบริหารความเสี่ยงด้านความด้านความปลอดภัยของข้อมูล	1.จัดทำรายงานเสนอให้ผู้บริหารรับทราบความเสี่ยงและแนวทางการแก้ไขความเสี่ยง	วันที่ 30 เมษายน พ.ศ. 2555	

ในการตรวจครั้งนี้ ได้มีการวางแผนและกำหนดขอบเขตการตรวจให้เป็นไปตามขอบเขตของการศึกษาของผู้ศึกษา ซึ่งผู้ศึกษานำมาจัดทำเป็นขอบเขตการตรวจ (Audit Scope) โดยแบ่งเป็น 7 หัวข้อดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy)
2. ระบบเอกสารส่วนกลาง (File Sharing: LSD DATA SERVER, LSD PS SERVER)
3. Database Server จำนวน4 Server (ERP. System, MRP. System, HRMS, DB Systems)
4. Active Directory Database
5. ระบบข้อมูลสนับสนุน (Service Support Systems: Mail Server, Web Server)
6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (All LSD Server)
7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)

โดยขอบเขตการตรวจ (Audit Scope) นี้ผู้ศึกษาได้นำไปบรรจุไว้ในเอกสารที่จะนำไปเป็นกรอบแนวทางในการตรวจสอบภายในครั้งนี้ คือ

1. Information Risk Management For Data Security Requirement & Audit Scope Matrix (LSD_F001)
2. Internal Audit Checklist (LSD_F002)

(รายละเอียดเอกสารทั้งสองฉบับแสดงไว้ในภาคผนวก ฅ และภาคผนวก ฆ)

2. การตรวจ ประเมินและการวางแผนจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

เป็นการนำเอาระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลและแผนการตรวจสอบภายใน ที่จัดทำขึ้นไปปฏิบัติ โดยทีมผู้ตรวจ (Team Auditor) นำเอา Audit Scope Matrix และ Internal Audit Checklist ซึ่งถือว่าเป็น ขอบเขตและแผนสำหรับการตรวจสอบภายในครั้งนี้ ไปดำเนินการตรวจสอบสายในเพื่อหาจุดบกพร่องประเด็นที่เป็นความเสี่ยง หรือผิดข้อกำหนด ด้านความปลอดภัยของข้อมูล เพื่อนำประเด็นที่เป็นความเสี่ยงที่ตรวจพบ ไปบริหารจัดการตามขั้นตอนที่ระบบได้กำหนดไว้ เพื่อกำจัดหรือควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยมีคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) รับหน้าที่ในส่วนนี้ ดังมีรายละเอียดดังนี้

2.1 การตรวจสอบภายในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

ในการตรวจแต่ละครั้งผู้ตรวจ (Auditor) จะยึดเอา Audit Scope Matrix และ Internal Audit Checklist ที่ได้วางแผนการตรวจไว้เป็นกรอบแนวทางในการตรวจเพื่อควบคุมให้

การตรวจครั้งนั้นๆ อยู่ในประเด็นหรือขอบเขตที่กำหนดไว้ โดยมีขั้นตอนและแผนการตรวจดังแสดงรายละเอียดใน ภาพที่ 3-7

แผนการตรวจสอบภายใน ระบบบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล

หัวเรื่อง	รายละเอียด	วันที่ / เวลา	สถานที่
1. อบรมผู้ตรวจ (Auditor Training)	1. อธิบายภาพรวมของระบบ การบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล	20/03/2555 13.30 - 16.30	Meeting Room02
2. ประชุมเปิดการตรวจ (Audit Opening)	1. สรุปขอบเขตการตรวจครั้งนี้ รวมถึงประเด็นหรือพื้นที่ที่ต้องการเน้นเป็นพิเศษ 2. จัดทำ Audit Scope Matrix และ Internal Audit Checklist		
3. ทำการตรวจสอบภายใน (Internal Audit)	1. ทำการตรวจตามแผนและ ขอบเขตที่กำหนดไว้	2/4/2555 9.00 - 16.00	Meeting Room02
4. ประชุมสรุปและ ประมาณค่าความเสี่ยงที่ตรวจพบ	1. นำความเสี่ยงหรือ ประเด็นที่ตรวจพบ มาเข้ากระบวนการประมาณค่าความเสี่ยง	23/04/2555 13.30 - 15.00	Meeting Room04
5. ส่งรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล	1. จัดทำรายงานเสนอให้ผู้บริหาร รับทราบความเสี่ยงและ แนวทางการแก้ไขความเสี่ยง	30/04/2555	

ภาพที่ 3-7 แผนการตรวจประเมินและการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

1) จากการประชุมเปิดการตรวจ วันที่ 20 มีนาคม พ.ศ.2555 ที่ประชุมประกอบด้วยทีมผู้ตรวจ (Team Auditor) และทีมผู้รับตรวจ (Team Audi tee) ซึ่งเป็นทีมเดียวกับคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) ที่มีผู้ศึกษาร่วมอยู่ในทีมด้วย โดยที่ประชุมเห็นว่าการตรวจครั้งนี้เป็นการตรวจครั้งแรกของบริษัท จึงเห็นว่าควรพิจารณาข้อกำหนดให้ครบทุกข้อ แต่ให้กำหนดขอบเขตการตรวจสอบที่ระบบสารสนเทศ หรือข้อมูลที่จะตรวจสอบตามที่ได้วางแผนการตรวจไว้ ซึ่งได้แสดงรายละเอียดไว้ในเอกสาร Information Risk Management For Data Security Requirement & Audit Scope Matrix (LSD_F001) และInternal Audit Checklist (LSD_F002) โดยรายละเอียดดังกล่าวผู้ศึกษาแสดงไว้ใน ภาคผนวก ฅ และภาคผนวก ฆ

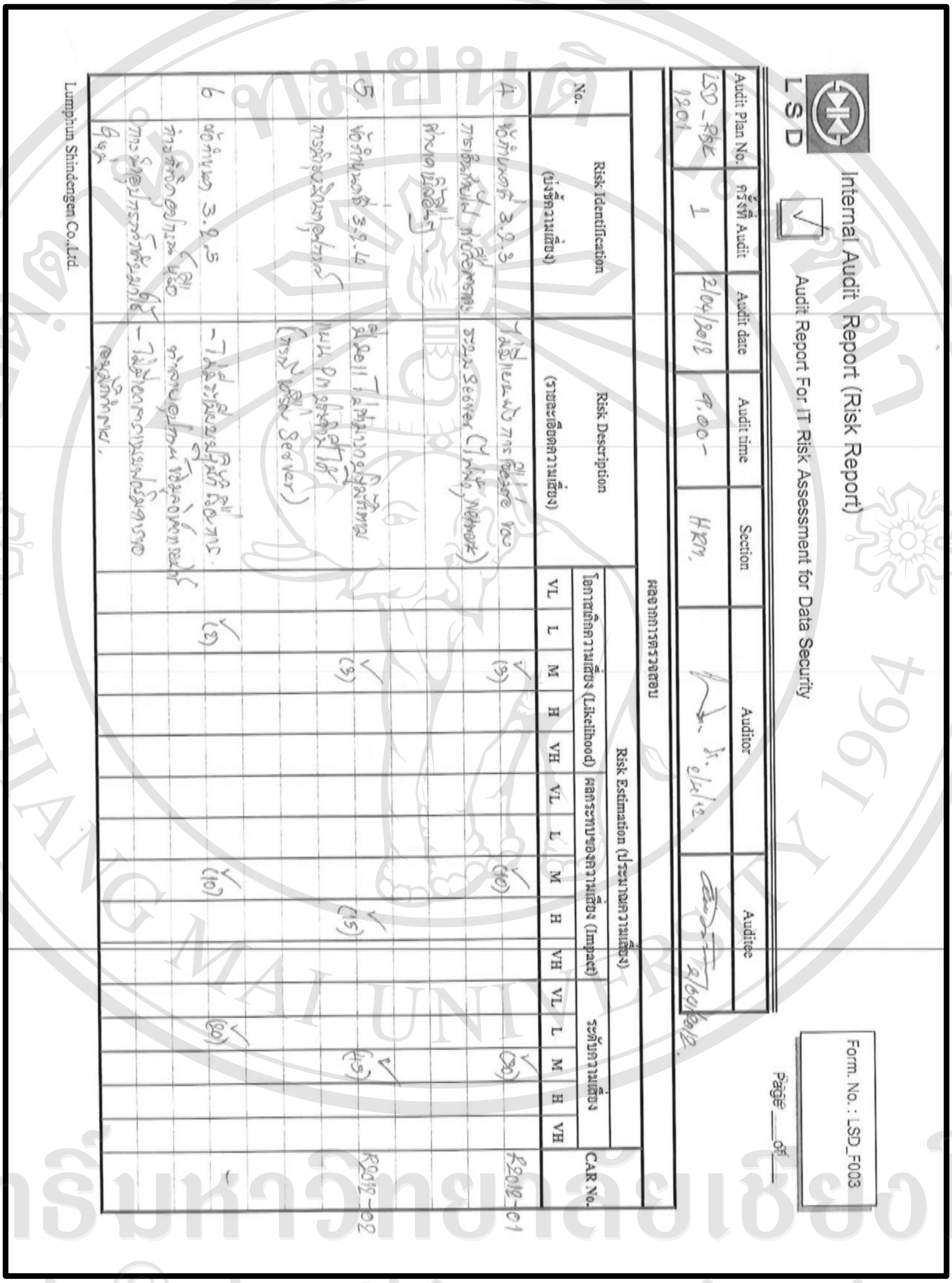
2) วันที่ 2 เมษายน พ.ศ.2555 ทีมผู้ตรวจกำหนดให้มีการตรวจสอบภายในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลขึ้น ซึ่งผลการตรวจภายในครั้งนี้ พบประเด็นความเสี่ยงที่ไม่เป็นไปตามข้อกำหนดทั้งหมด 27 ประเด็นซึ่งประเด็นทั้งหมด ได้ทำการบันทึกลงใน

แบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003 ดังแสดงตัวอย่างในภาพที่ 4-1 แต่ในการตรวจครั้งนี้ หัวหน้าผู้ตรวจแนะนำให้ทำการตรวจหาประเด็นที่เป็นความเสี่ยงเพียงอย่างเดียวก่อน แล้วค่อยประชุมเพื่อสรุปและประมาณค่าความเสี่ยงในภายหลัง

3) วันที่ 23 เมษายน พ.ศ. 2555 ทีมผู้ตรวจนัดประชุมเพื่อสรุปประเด็นความเสี่ยงที่ตรวจพบพร้อมกับร่วมกันประมาณค่าความเสี่ยงในแต่ละประเด็นว่าอยู่ในระดับใด เพื่อนำไปสู่การหาแนวทางการแก้ไข การกำจัดหรือควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยผู้ศึกษาได้สรุปความเสี่ยงที่ตรวจพบและผลการประมาณค่าความเสี่ยง โดยแบ่งตามระดับความเสี่ยง ดังแสดงในตารางที่ 4-1 ซึ่งรายละเอียดของประเด็นความเสี่ยงและแนวทางการแก้ไขทั้งหมด ผู้ศึกษาและคณะทำงานด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) ได้สรุปไว้ในรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล(Risk Management Report For Data Security) ซึ่งแสดงรายละเอียดทั้งหมดไว้ใน ภาคผนวก จ

4) จากประชุมสรุปประเด็นความเสี่ยงและประมาณค่าความเสี่ยงที่ประชุมได้สรุปแนวทางการแก้ไขไว้ว่า ประเด็นที่มีค่าความเสี่ยงตั้งแต่ระดับปานกลางขึ้นไปถึงเสี่ยงมาก ทีมผู้ตรวจทำการบันทึกประเด็นความเสี่ยงลงในเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR.) และกำหนดให้หน่วยงานที่เกี่ยวข้องคือกลุ่มงาน IT Service ที่ผู้ศึกษาสังกัดอยู่นั้นดำเนินการแก้ไขให้แล้วเสร็จภายใน 3 เดือน โดยประมาณ ดังแสดงตัวอย่างเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR.) ในภาพที่ 3-14 ถึงภาพที่ 3-15 และประเด็นที่ถูกประมาณค่าความเสี่ยงให้อยู่ในระดับที่มีความเสี่ยงและผลกระทบต่ำ (L) ทีมผู้ตรวจมีคำสั่งให้หน่วยงานที่เกี่ยวข้องจัดทำแผนการปรับปรุงมานำเสนอและดำเนินการแก้ไขเป็นลำดับถัดไป ส่วนประเด็นที่ประมาณค่าความเสี่ยงอยู่ในระดับต่ำมาก ที่ประชุมถือว่าเป็นประเด็นที่ยอมรับได้และไม่ต้องดำเนินการใดๆ ซึ่งประเด็นความเสี่ยงและแนวทางการดำเนินการแก้ไขทั้งหมด ผู้ศึกษาได้แสดงไว้ในรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล (Risk Management Report For Data Security) ดังแสดงรายละเอียดทั้งหมดไว้ใน ภาคผนวก จ

การตรวจสอบภายในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ของบริษัทลำพูนซิงเด็นเก็น จำกัด ในครั้งนี้ผู้ศึกษามีความตั้งใจที่จะสร้างระบบการตรวจสอบภายในที่มีระดับการตรวจอยู่ 2 ระดับคือ การตรวจประเมินภายในหน่วยงานและการตรวจติดตามภายในโดยคณะกรรมการ ผู้บริหารและบุคคลนอกหน่วยงาน แต่เนื่องจากข้อมูลทางด้านสารสนเทศบางส่วนถือเป็นความลับที่มิอย่างเปิดเผยในวงกว้างได้ ทำให้ผู้จัดการส่วนงานสารสนเทศ มีคำสั่งให้มีการการตรวจสอบภายในเฉพาะการตรวจประเมินภายในหน่วยงานเท่านั้น



ภาพที่ 3-8 ตัวอย่าง การบันทึกประเด็นความเสี่ยงที่ตรวจพบ ลงในแบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003, 2 เมษายน พ.ศ. 2555

จากภาพที่ 3-8 เป็นตัวอย่างรายงานประเด็นความเสี่ยงจากการตรวจสอบภายใน โดยได้แสดงรายละเอียดของประเด็นความเสี่ยงไว้ในรายงานในด้านต่างๆ เช่น

- บ่งชี้ความเสี่ยง (Risk Identification) เป็นการระบุถึงข้อกำหนดที่ ประเด็นความเสี่ยงนั้นเกี่ยวข้อง
- รายละเอียดความเสี่ยง (Risk Description) เป็นการบอกถึงรายละเอียดของประเด็นความเสี่ยง ว่ามีข้อบกพร่องที่ไม่ได้เป็นไปตามข้อกำหนดอย่างไร
- ประมาณความเสี่ยง (Risk Estimation) เป็นการแสดงค่าความเสี่ยงที่ได้รับการประเมินโดยอ้างอิงตามแนวทางในการวิเคราะห์ความเสี่ยงเพื่อประเมินระดับความเสี่ยง ในเอกสาร Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง) ดังแสดงไว้ใน ภาพที่ 3-3

โดยรายงานประเด็นความเสี่ยงจากการตรวจสอบภายในด้านความปลอดภัยของข้อมูลในครั้งนี้ มีประเด็นความเสี่ยงที่ถูกประมาณความเสี่ยงไว้ในระดับต่างๆรวมทั้งหมด 27 ประเด็น ดังแสดงรายละเอียดไว้ใน ภาพที่ 3-9

จากภาพที่ 3-9 ได้แสดงถึงเอกสาร Internal Audit Report โดยเนื้อหาภายในเอกสารฉบับนี้ มีดังนี้

- Risk Identification เป็นการบ่งชี้ความเสี่ยง ว่าไม่ตรงตามข้อกำหนดในข้อใด
- Risk Description เป็นการระบุรายละเอียดความเสี่ยงที่ตรวจพบ
- โอกาสเกิดความเสี่ยง (Likelihood)และผลกระทบของความเสี่ยง (Impact) เป็นคะแนนในการประเมิน ตามเกณฑ์ที่ระบุไว้ในเอกสาร Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง) ดังแสดงวในภาพที่ 3-3
- ระดับความเสี่ยงที่ประมาณได้ โดยเป็นผลมาจากการนำเอาค่า โอกาสเกิดความเสี่ยง (Likelihood) * ผลกระทบของความเสี่ยง (Impact)

LSD

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 1 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง) โอกาสเกิดความเสี่ยง (Likelihood) VL	L	M	H	VH	ผลกระทบของความเสี่ยง (Impact) VL	L	M	H	VH	ระดับความเสี่ยง VL	L	M	H	VH	CAR No.
1	ข้อตกลงการไม่เปิดเผยความลับ (Confidentiality agreements) (2.1.5)	ระเบียบบริษัทไม่ได้ระบุให้มีการลงนาม ระหว่างบริษัทกับพนักงาน ในเรื่องการไม่เปิดเผยความลับ		2						10				20				
2	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Independent review of information security) (2.1.6)	มีการทบทวนนโยบายทุกๆปี ปีละ 1 ครั้ง แต่ไม่ได้ทำการทบทวนทุกประเด็น		2					5				10					
3	การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats) (3.1.3)	ไม่มีเอกสารควบคุมการปฏิบัติของบุคคลภายนอก		2					5				10					

Lumphun Shindengen Co.,Ltd.

LSD

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 2 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง) โอกาสเกิดความเสี่ยง (Likelihood) VL	L	M	H	VH	ผลกระทบของความเสี่ยง (Impact) VL	L	M	H	VH	ระดับความเสี่ยง VL	L	M	H	VH	CAR No.
4	การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ(Cabling security) (3.2.3)	ไม่มีแผนผังการเชื่อมต่อระบบ Server (ไฟฟ้า, Network)			3					10					30			R2012-01
5	การบำรุงรักษาอุปกรณ์ (3.2.4)	ปี 2011 ไม่ได้ปฏิบัติตามแผน PM. ประจำปี (Server)			3						15				45			R2012-02
6	การกำจัดอุปกรณ์และ การนำอุปกรณ์กลับไปใช้ใหม่ (3.2.5)	> ไม่มีระเบียบปฏิบัติการทำลายอุปกรณ์ > ไม่มีระบบการขออนุมัติทำลาย		2						10				20				
7	ขั้นตอนการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร (4.1.1, 4.1.2)	ไม่มีการทบทวน WI. ด้านงาน IT.		2						10				20				

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-9 บันทึกประเด็นความเสี่ยงที่ตรวจพบ ลงในแบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003, 2 เมษายน พ.ศ. 2555

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 3 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง) โอกาสเกิดความเสี่ยง (Likelihood) VL	L	M	H	VH	ผลกระทบของความเสี่ยง (Impact) VL	L	M	H	VH	ระดับความเสี่ยง VL	L	M	H	VH	CAR No.
8	การตรวจรับระบบ	ไม่มีระเบียบและ เอกสารการตรวจ		2						10				20				
	(4.3.2)	รับ Hardware																
9	การสำรองข้อมูล	1. ไม่มีขั้นตอนการปฏิบัติในการกู้			3							20				60		R2012-03
	(4.5.1)	คืนข้อมูลและ ระบบ																
		2. ไม่มีการทดสอบการกู้คืนระบบ																
		สารสนเทศ																
10	การกำจัดสื่อบันทึกข้อมูล	ไม่มีระบบขออนุมัติทำลายสื่อบันทึก		2					5				10					
	(4.5.1)	ข้อมูลที่ไม่ได้ใช้																
11	ข้อกำหนด 4.8.3	ไม่มีระบบขออนุมัติการส่ง		2						10				20				
	การส่งสื่อบันทึกข้อมูลหรือ ข้อมูล	สื่อบันทึกข้อมูลหรือ ข้อมูล																
	ออกนอกบริษัท	ออกนอกบริษัท																

Lumphun Shindengen Co.,Ltd.

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 4 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง) โอกาสเกิดความเสี่ยง (Likelihood) VL	L	M	H	VH	ผลกระทบของความเสี่ยง (Impact) VL	L	M	H	VH	ระดับความเสี่ยง VL	L	M	H	VH	CAR No.
12	ข้อกำหนด 4.10.3	ระบบ LOG ไม่มีระบบป้องกันการ				4				10					40			R2012-10
	การป้องกันข้อมูลบันทึกเหตุการณ์	แก้ไข																
13	นโยบายควบคุมการเข้าถึงระบบ	ไม่มีการทบทวนสิทธิการสิทธิ			3					10					30			R2012-04
	(5.1.1)	พนักงานที่ลาออกหรือ ย้ายสังกัด																
14	การบริหารจัดการการเข้าถึงข้อมูล	1. ไม่มีระเบียบปฏิบัติ ในการจัดการกับ			3					10					30			R2012-05
	(5.2)	พนักงานเข้าใหม่และ พนักงานที่ลาออก																
		2. ไม่มีระบบการทบทวนสิทธิการ																
		เข้าถึงข้อมูล																
15	การจัดการรหัสผ่าน	ละเลยการทบทวนรหัสผ่าน Admin			3					10								R2012-05
	(5.3.1)																	

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-9 บันทึกประเด็นความเสี่ยงที่ตรวจพบ ลงในแบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003, 2 เมษายน พ.ศ. 2555 (ต่อ)

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 5 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	
16	นโยบายการให้บริการเคลือข่าย (5.4.1)	1. นโยบายด้าน IT ไม่ได้ระบุรายละเอียดเรื่องนี้		2					5				10					
17	การควบคุมการเชื่อมต่อทางเครือข่าย (5.4.1)	ไม่มีการทบทวนสิทธิ์ผู้ใช้งาน		2					5				10					
18	การพิสูจน์ตัวตนของผู้ใช้งาน (5.5.2)	LSD PS Serv (file server) ไม่มีการจัดการด้านการพิสูจน์ตัวตนในการเข้าใช้ข้อมูล			3					10					30			R2012-07
19	การแยกระบบสารสนเทศที่มีความสำคัญสูง (5.6.2)	ไม่มีการจัดลำดับความสำคัญของระบบสารสนเทศในบริษัท		2					5				10					

Lumphun Shindengen Co.,Ltd.

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 6 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	
20	การป้องกันอุปกรณ์เครือข่ายแบบพกพา (5.7.1)	ไม่มีนโยบายในการควบคุมการจัดการกับข้อมูล กับการป้องกันอุปกรณ์เครือข่ายแบบพกพา		2						10					20			
21	มาตรการควบคุมช่องโหว่ทางด้านเทคนิค (6.2.1)	ไม่มีระบบและกระบวนการตรวจสอบและจัดการช่องโหว่และการรายงานอย่างเป็นลายลักอักษร			3				5					15				
22	การรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย (7.1.1 และ 7.1.2)	ไม่มีระเบียบปฏิบัติ และขั้นตอนการปฏิบัติ ในการรายงาน ด้านความมั่นคงปลอดภัยด้าน IT			3					10						30		R2012-08

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-9 บันทึกประเด็นความเสียงที่ตรวจพบ ลงในแบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003, 2 เมษายน พ.ศ. 2555 (ต่อ)

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 7 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	
23	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (7.2.1)	ไม่มีขั้นตอนการปฏิบัติ และระบุหน้าที่รับผิดชอบอย่างเป็นลายลักษณ์อักษร เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของ ข้อมูลด้านต่างๆ ในบริษัท		2						10				20				
24	การเก็บรวบรวมหลักฐาน (7.2.3)	ไม่มีการทำรายงาน สรุปเหตุการณ์ที่เกิดขึ้น เพื่อเก็บเป็นข้อมูลในการหาแนวทางการแก้ไข ในเหตุการณ์ในอนาคต		2						10				20				

Lumphun Shindengen Co.,Ltd.

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1 Page 8 of 8

Audit Plan No	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee
IT Risk-01	1	2/4/2555	8:30:00 AM	HRM.	คุณพรเทพ เย็นฉ่ำ	คุณอำนาจ พงษ์กลาง

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	
25	การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (9.2.1)	ไม่มีการกำหนดและข้อปฏิบัติต่างๆ		2						10				20				
26	การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking) (9.2.2)	ไม่มีการตรวจสอบการ ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัย ของเจ้าหน้าที่ ผู้รับผิดชอบ		2						10				20				
27	มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls) (9.3.1)	ไม่มีการตรวจสอบ			3					10					30			R2012-09

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-9 บันทึกประเด็นความเสียงที่ตรวจพบ ลงในแบบฟอร์ม Internal Audit Report (Risk Report): LSD_F003, 2 เมษายน พ.ศ. 2555 (ต่อ)

ตารางที่ 3-2 *ตารางแสดงผลสรุปประเด็นความเสี่ยงที่ตรวจพบ*

ระดับความเสี่ยง	จำนวนประเด็นความเสี่ยง	รูปแบบการแก้ไข
VH= มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก)	0	CAR ทำการร้องขอให้มีการแก้ไข
H = มีความเสี่ยงและผลกระทบ (เสี่ยง)	1	CAR ทำการร้องขอให้มีการแก้ไข
M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง)	9	CAR ทำการร้องขอให้มีการแก้ไข
L = มีความเสี่ยงและผลกระทบต่ำ (ต่ำ)	11	วางแผนแก้ไข
VL= มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก)	6	ความเสี่ยงที่ยอมรับได้

จากภาพที่ 3-9 สามารถนำผลการตรวจสอบภายใน ในครั้งนี้มาสรุปตามกลุ่มของระดับความเสี่ยงได้ ดังแสดงรายละเอียดในตารางที่ 3-2

LSD

Corrective Action Request (System)

Form. No. : LSD_F004
Edit : 1

CAR No. : _____
(หมายเลข CAR)

Auditor

❍ **Information Risk Management for Data Security**

Issue by Auditor : _____ (ผู้ออก CAR) **EMP.Code :** _____ (รหัสพนักงาน) **Issue date :** _____ (วันที่ออก)

Audit plan : _____ (หมายเลขแผนการตรวจ) **Audit Time :** _____ (การตรวจครั้งที่)

Area NC ; (พื้นที่ที่พบข้อบกพร่อง)
❑ SC Div. Sect. _____ ❑ PS Div. Sect. _____
❑ ADM Div. Sect. _____ ❑ Other Sect. _____

Level : VH. H. M. (ระดับ CAR)

Type of CAR : (ประเภท CAR)
❑ Internal Audit
❑ Other NC (ระบุ) _____

Requirement Clause : _____ (ข้อกำหนดที่เกี่ยวข้อง)
Document No : _____ (เอกสารที่เกี่ยวข้อง)

1 **Content of Non-conformity** (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

Due date (กำหนดเสร็จวันที่) : _____ / _____ / _____ ⇨ Responsible action : (ผู้รับผิดชอบแก้ไข) _____ ⇨ Checking by (ผู้ตรวจสอบการแก้ไข / IT Group. GL) _____ ⇨ Approval by (ตัวแทนฝ่ายบริหาร / HRM.Mgr. อนุมัติ) _____

Auditee

2 **Analysis root cause** (การวิเคราะห์หาสาเหตุ)

3 **Take Action** (การแก้ไข) | MGR./GL. Action approve (อนุมัติการแก้ไข โดยผู้จัดการ)

Action for re-occure (การป้องกันการเกิดซ้ำ)

Extension CAR : (ขอต่ออายุ CAR) Extension No. : _____ (หมายเลขเอกสารขอต่ออายุ) Extension to date (ขอต่ออายุถึงวันที่) _____

Auditor

4 **Follow up record** (ผลการติดตามการแก้ไขและป้องกัน) :

❍ In case CAR expired re-issue CAR No. : _____ (ออก CAR ซ้ำ ในกรณีที่เกินกำหนดเสร็จ)

❑ Finished (close) (ทำการแก้ไขแล้วเสร็จ)

Efficiency of implementation (ติดตามผลหลังการดำเนินการแก้ไข)

Evidence (หลักฐานในการแก้ไข)

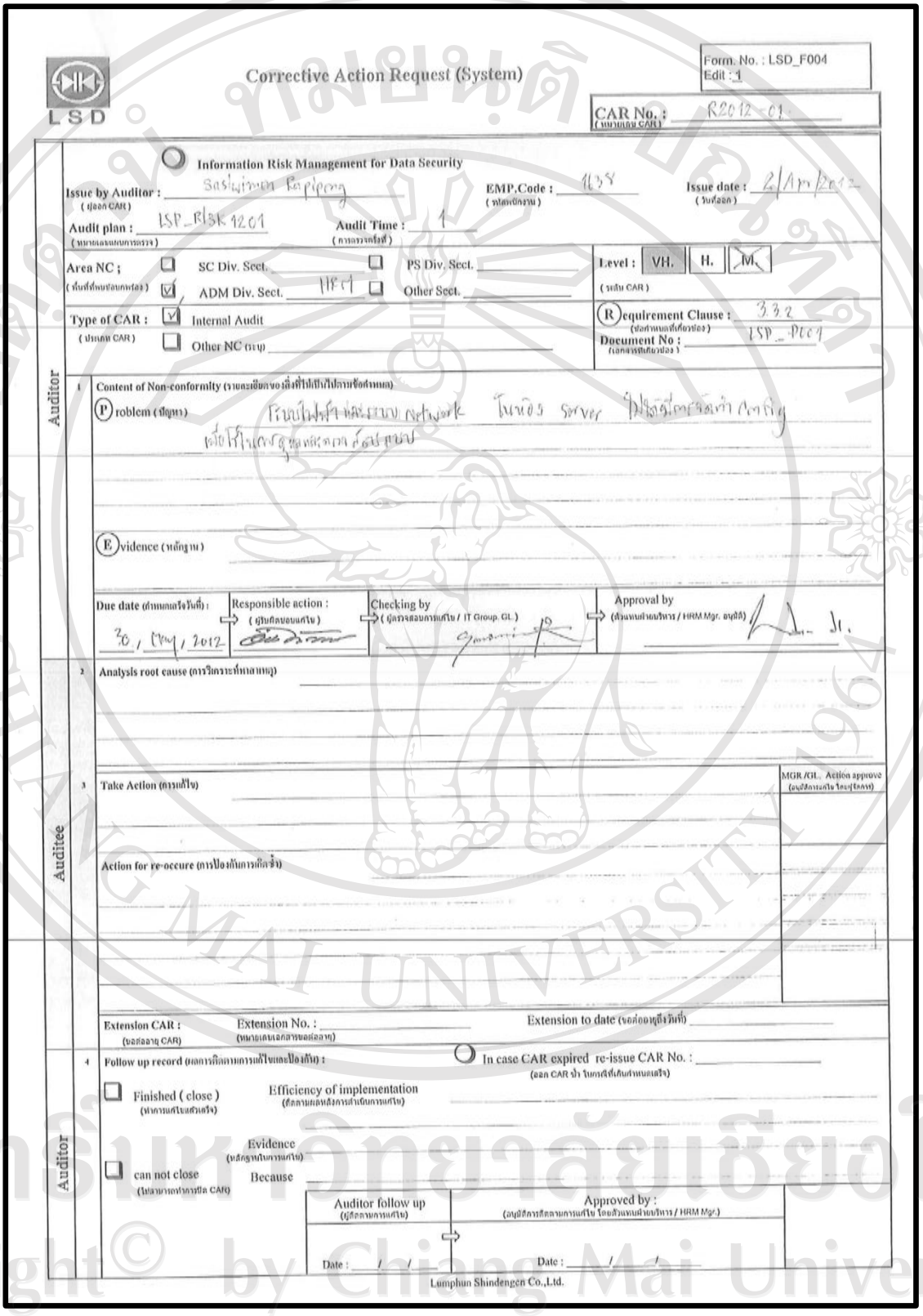
❑ can not close (ไม่สามารถทำการปิด CAR)

Because

Auditor follow up (ผู้ติดตามการแก้ไข)	Approved by : (อนุมัติการติดตามการแก้ไข โดยตัวแทนฝ่ายบริหาร/ HRM Mgr.)
Date : ____/____/____	Date : ____/____/____

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-10 ตัวอย่างที่ 1 แบบฟอร์ม Corrective Action Request (CAR.): LSD_F004



Corrective Action Request (System)

LSD

Form. No. : LSD_F004
Edit : 1

CAR No. : R2012-01

Information Risk Management for Data Security

Issue by Auditor : Sasiwimon Kaipeng
EMP.Code : 1138
Issue date : 2/Apr/2012
Audit plan : ISP_RISK 1201
Audit Time : 1

Area NC ; ☐ SC Div. Sect. ☐ PS Div. Sect.
☑ ADM Div. Sect. HR ☐ Other Sect.

Level : VH. H. M.

Type of CAR : ☑ Internal Audit
☐ Other NC

Requirement Clause : 3.3.2
Document No : ISP_PL01

Auditor

1 Content of Non-conformity

Problem

Evidence

Due date : 30/Apr/2012
Responsible action :
Checking by (IT Group. GL.)
Approval by (HRM Mgr.)

Auditee

2 Analysis root cause

3 Take Action

MGR /GL. Action approve

Action for re-occure

Extension CAR : Extension No. : Extension to date

Auditor

4 Follow up record

☐ Finished (close)
Efficiency of implementation
Evidence
☐ can not close
Because

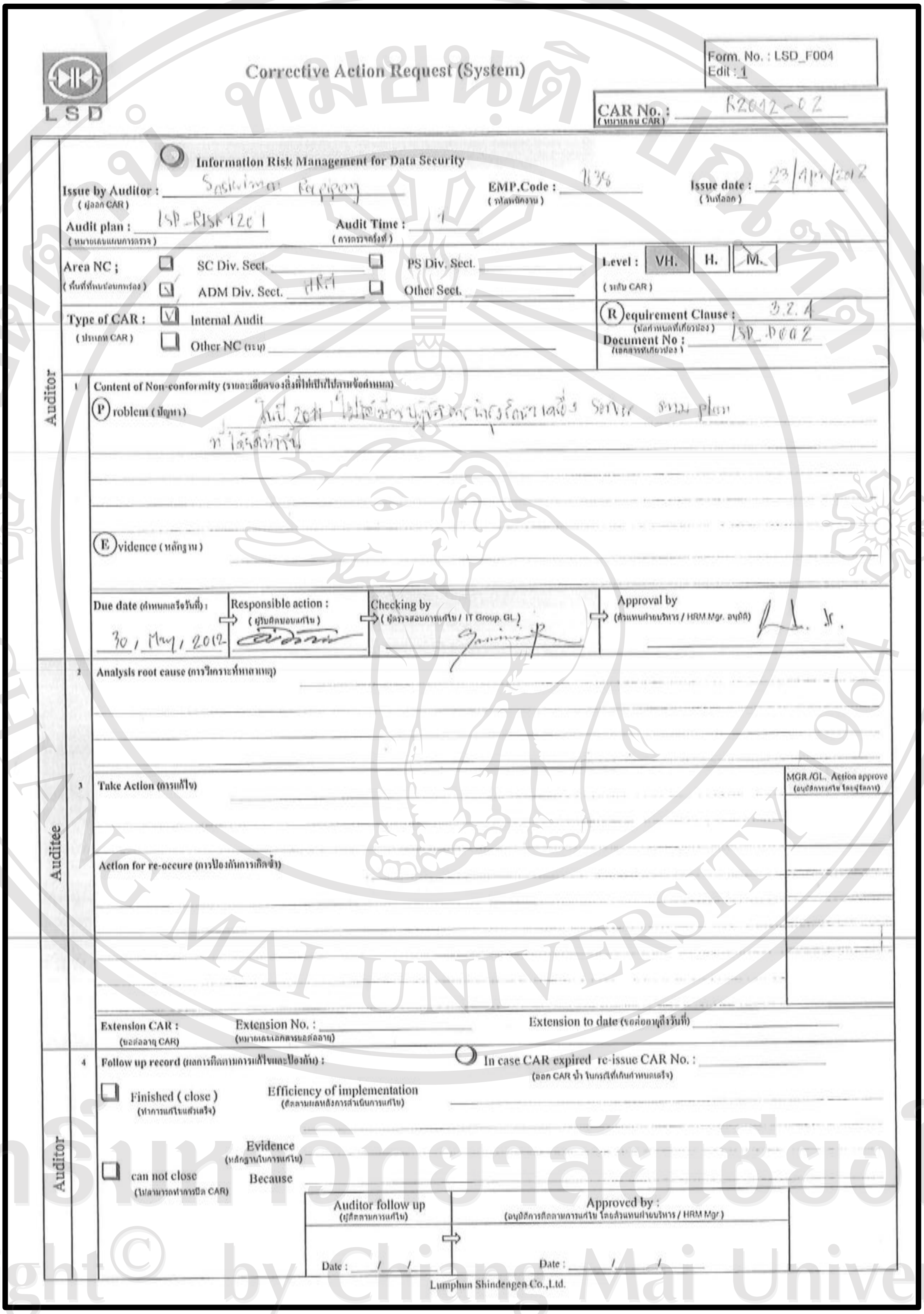
In case CAR expired re-issue CAR No. :

Auditor follow up
Approved by : (HRM Mgr.)

Date : / /
Date : / /

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-11 ตัวอย่างที่ 2 ประเด็นความเสี่ยงที่ถูกออกเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR No. : R2012-01)



Corrective Action Request (System)

Form. No. : LSD_F004
Edit : 1

CAR No. : R2012-02
(หมายเลข CAR)

Information Risk Management for Data Security

Issue by Auditor : (ผู้ออก CAR)
EMP.Code : (รหัสพนักงาน)
Issue date : 23/Apr/2012 (วันที่ออก)

Audit plan : LSP_RISK12-1 (หมายเลขแผนการตรวจ)
Audit Time : 1 (การตรวจครั้งที่)

Area NC : (พื้นที่ที่พบข้อบกพร่อง) SC Div. Sect. / ADM Div. Sect. HRA / PS Div. Sect. / Other Sect.

Level : VH. H. M. (ระดับ CAR)

Type of CAR : (ประเภท CAR) Internal Audit / Other NC (ระบุ)

Requirement Clause : 3.2.4 (ข้อกำหนดที่เกี่ยวข้อง)
Document No : LSP_D002 (เอกสารที่เกี่ยวข้อง)

Auditor

1 Content of Non-conformity (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

Due date (กำหนดแก้ไขวันที่) : 30/May/2012
Responsible action : (ผู้รับผิดชอบแก้ไข)
Checking by (ผู้ตรวจสอบการแก้ไข / IT Group. GL.)
Approval by (ตัวแทนฝ่ายบริหาร / HRM Mgr. อนุมัติ)

Auditee

2 Analysis root cause (การวิเคราะห์หาสาเหตุ)

3 Take Action (การแก้ไข)

MGR./GL. Action approve (อนุมัติการแก้ไข โดยผู้จัดการ)

Action for re-occure (การป้องกันการเกิดซ้ำ)

Extension CAR : (ขอต่ออายุ CAR)
Extension No. : (หมายเลขเอกสารขอต่ออายุ)
Extension to date (ขอต่ออายุถึงวันที่) :

Auditor

4 Follow up record (ผลการติดตามการแก้ไขและป้องกัน) :

In case CAR expired re-issue CAR No. : (ออก CAR ใหม่ ในกรณีที่เกินกำหนดแก้ไข)

Finished (close) (ทำการแก้ไขแล้วเสร็จ)
Efficiency of implementation (ติดตามผลหลังการดำเนินการแก้ไข)

Evidence (หลักฐานในการแก้ไข)

can not close (ไม่สามารถทำการปิด CAR)
Because

Auditor follow up (ผู้ติดตามการแก้ไข)
Approved by : (อนุมัติการติดตามการแก้ไข โดยตัวแทนฝ่ายบริหาร / HRM Mgr)

Date : / /
Date : / /

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-12 ตัวอย่างที่ 3 ประเด็นความเสี่ยงที่ถูกออกเอกสารร้องขอให้มีการแก้ไข Corrective Action Request (CAR No. : R2012-02)

2.2 การวางแผนจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล

จากผลการตรวจสอบภายในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล สามารถแบ่งกลุ่มประเด็นความเสี่ยงที่ต้องดำเนินการแก้ไขได้เป็น 2 กลุ่ม คือ

1) กลุ่มประเด็นความเสี่ยงที่ถูกร้องขอให้มีการแก้ไขหรือถูก CAR. มีจำนวน 10 ประเด็น ซึ่งในขณะที่ผู้ศึกษากำลังทำการสรุปผลการศึกษาอยู่นี้ (15 พฤษภาคม พ.ศ. 2555) ได้ดำเนินการแก้ไขแล้วเสร็จไปแล้วจำนวน 6 ประเด็น ดังแสดงตัวอย่างของเอกสาร Corrective Action Request (CAR.) ที่ดำเนินการแล้วเสร็จ ในภาพที่ 3-14 และภาพที่ 3-15

2) กลุ่มประเด็นความเสี่ยงที่ถูกเสนอแนะให้มีการแก้ไขซึ่งเป็นกลุ่มประเด็นความเสี่ยงที่ ถูกประมาณค่าความเสี่ยงให้อยู่ในระดับที่มีความเสี่ยงและผลกระทบต่ำ (L) ซึ่งส่วนใหญ่จะเป็นประเด็นที่ต้องแก้ไข ระเบียบบริษัทหรือแก้ไขระเบียบขั้นตอนการปฏิบัติงาน โดยที่ประชุมได้กำหนดให้ดำเนินการแล้วเสร็จไม่เกินวันที่ 30 ตุลาคม พ.ศ. 2555 และผู้ศึกษาได้แสดงรายละเอียดไว้ ในรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล (Risk Management Report For Data Security) ภาคผนวก จ

3. การดำเนินการตามแผนการจัดการความเสี่ยง

ผู้ศึกษาจะทำการยกตัวอย่างการดำเนินการแก้ไข โดยนำเอาการดำเนินการแก้ไขประเด็นความเสี่ยงในประเด็นที่ 9 ในรายงานประเด็นความเสี่ยงจากการตรวจสอบภายในด้านความปลอดภัยของข้อมูล ซึ่งเป็นประเด็นที่ได้รับการประมาณค่าความเสี่ยงไว้สูงที่สุด โดยถูกประมาณความเสี่ยงให้อยู่ในระดับที่มีความเสียงและผลกระทบ (เสี่ยง / H) ดังมีรายละเอียดขั้นตอนการดำเนินการดังนี้

ตัวอย่าง การดำเนินการแก้ไขประเด็นความเสี่ยงที่ตรวจพบ

1) รายละเอียดประเด็นความเสี่ยง

- CAR NO : R2012-03
- ข้อกำหนดที่บกพร่อง : ข้อกำหนดที่ 4.5.1 การสำรองข้อมูล
- รายละเอียดความเสี่ยง / ปัญหา
  (1) ไม่มีขั้นตอนการปฏิบัติในการกู้คืนข้อมูลและระบบ
  (2) ไม่มีการทดสอบการกู้คืนระบบสารสนเทศ
- ผู้รับผิดชอบ : นายอำนาจ พงษ์กลาง

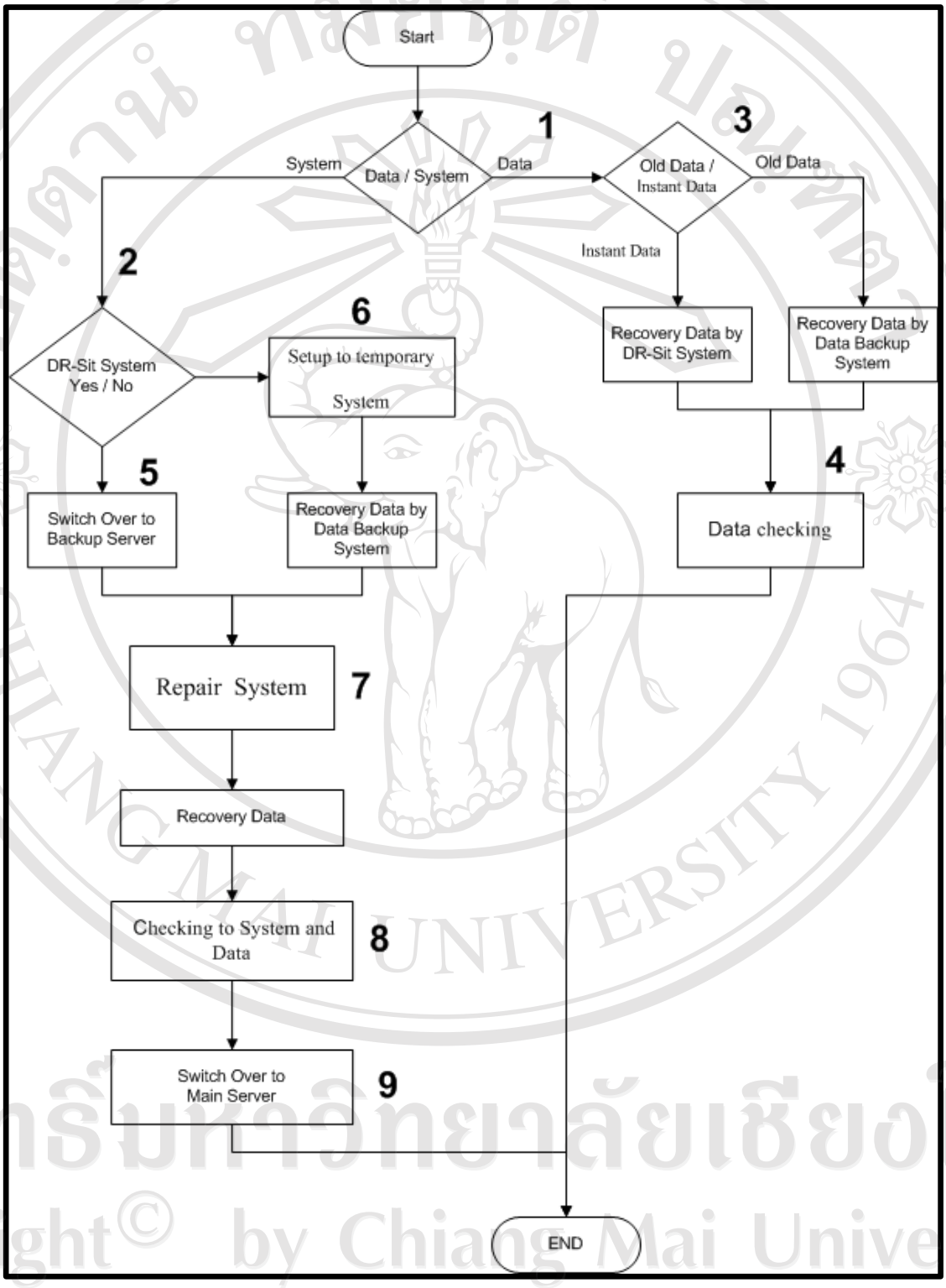
2) การวิเคราห์ถึงผลกระทบที่จะเกิดขึ้นกับบริษัทจากประเด็นความเสี่ยงดังกล่าว สามารถสรุปได้ดังนี้

- ไม่มีขั้นตอนการปฏิบัติในการกู้คืนข้อมูลและระบบ เมื่อเกิดเหตุการณ์ขึ้น อาจจะไม่สามารถกู้คืนระบบได้ตามระยะเวลาที่กำหนดหรือเกิดความผิดพลาดในการกู้คืนระบบทำให้ข้อมูลของบริษัทเกิดการเสียหายหรือส่งผลให้การให้บริการสารสนเทศหยุดให้บริการเป็นเวลานาน
- ไม่มีการทดสอบการกู้คืนระบบสารสนเทศ ทำให้ไม่สามารถยืนยันได้ว่าระบบสำรองข้อมูลที่มีอยู่สามารถใช้งานได้จริงตามที่บริษัทคาดหวัง

ตารางที่ 3-3 *ตารางแสดงการวิเคราะห์ปัญหาและประเด็นความเสี่ยง*

บ่งชี้ความเสี่ยง / ปัญหา	รายละเอียดความเสี่ยง / ปัญหา	แนวทางการแก้ไข	สถานะ
ข้อกำหนดที่ 4.5.1 การสำรองข้อมูล	- ไม่มีขั้นตอนการปฏิบัติในการกู้คืนข้อมูลและระบบ		NG – 1
	- ไม่มีการทดสอบการกู้คืนระบบสารสนเทศ		NG – 1
		- จัดทำ Workflow การกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ	แก้ไข - 1
		-กำหนดให้มีการทดสอบระบบการกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ ประจำเดือน (ใช้การทดสอบผ่าน Software)	แก้ไข - 2
		-กำหนดให้มีการทดสอบระบบการกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ ประจำปี (การย้ายไปใช้งานระบบสำรอง)	แก้ไข - 2

3) การดำเนินการแก้ไข



ภาพที่ 3-13 แสดง Workflow การกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ (Recovery Workflow)

- จำทำ Workflow การกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ (Recovery Workflow) ดังแสดงรายละเอียดในภาพที่ 3-13

รายละเอียด Workflow มีดังนี้

(1) เป็นการวิเคราะห์ว่าสิ่งที่ต้องการกู้คืนนั้นเป็นการกู้คืนระบบหรือเฉพาะข้อมูลบางส่วน โดยหากเป็นการกู้คืนระบบให้ไปทำในข้อ (2) แต่หากเป็นการกู้คืนเฉพาะข้อมูลบางส่วนให้ไปทำข้อ(3)

(2) เป็นการวิเคราะห์ว่าระบบที่ต้องการกู้คืนมีระบบ Server สำรองทำงานแทนหรือไม่ หากมีให้ไปทำข้อ(5) แต่หากไม่มีให้ข้ามไปทำข้อ(6)

(3) เป็นการวิเคราะห์ว่าข้อมูลที่ต้องการกู้คืนเป็นข้อมูลย้อนหลังหรือข้อมูลปัจจุบัน หากเป็นข้อมูลย้อนหลังให้กู้ข้อมูลจากระบบสำรองข้อมูล (Data backup system) แต่หากเป็นข้อมูลปัจจุบันให้สำเนาข้อมูลมาจาก Server สำรอง (DR-Sit System)

(4) ทำการตรวจเช็คข้อมูลที่ได้จากข้อ(3) ก่อนนำไปใช้งาน

(5) เมื่อต้องการกู้คืนระบบ ที่มีระบบ Server สำรองทำงานแทน ให้ทำการสลับให้ Server สำรองใน Backup Sit (DR-Sit) ทำงานให้บริการแทน หลังจากนั้นไปดำเนินการในขั้นตอนข้อ(7) ต่อไป

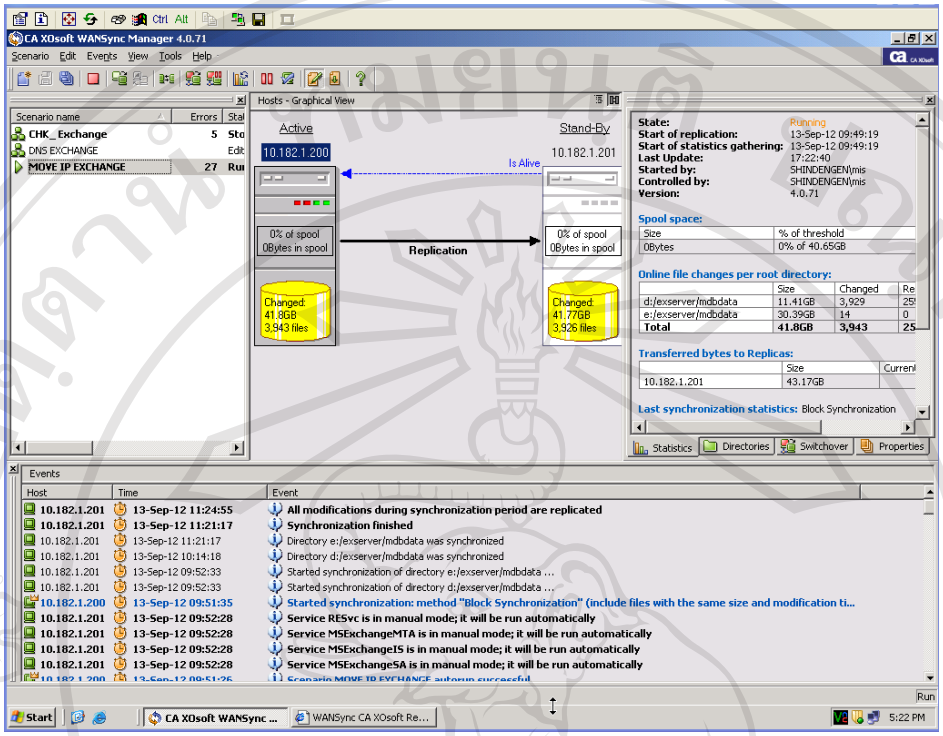
(6) เมื่อต้องการกู้คืนระบบที่ไม่มีระบบ Server สำรองทำงานแทน ให้ทำการสร้างระบบ Server ชั่วคราวให้บริการแทนก่อน หลังจากนั้นไปดำเนินการในขั้นตอนข้อ(7) ต่อไป

(7) ทำการกู้คืนระบบที่ขัดข้อง หลังจากนั้นก็กู้คืนข้อมูลที่เป็นปัจจุบันที่สุด

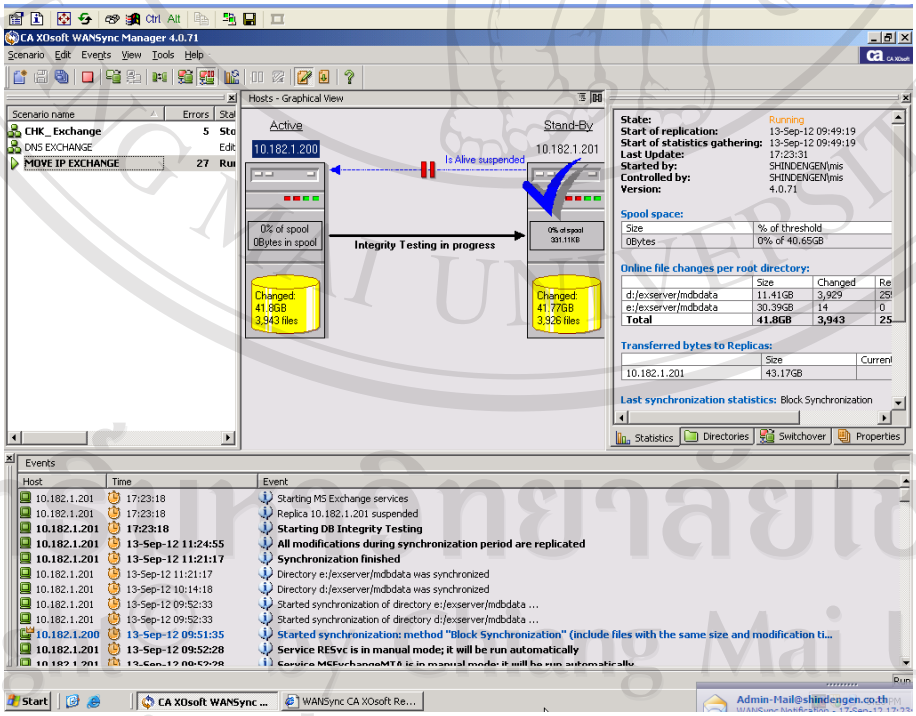
(8) ทำการตรวจเช็คระบบและข้อมูลที่ได้จากข้อ(7)

(9) สลับการทำงานของ Server โดยให้ Server หลักให้บริการตามปรกติ

- กำหนดให้มีการทดสอบระบบการกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศประจำเดือน เดือนละ 1 ครั้งโดยใช้วิธีการทดสอบผ่าน Software
- กำหนดให้มีการทดสอบระบบการกู้คืนข้อมูลสารสนเทศและระบบสารสนเทศ ประจำปี ปีละ 1 ครั้ง โดยการย้ายไปใช้งานระบบ Server สำรอง



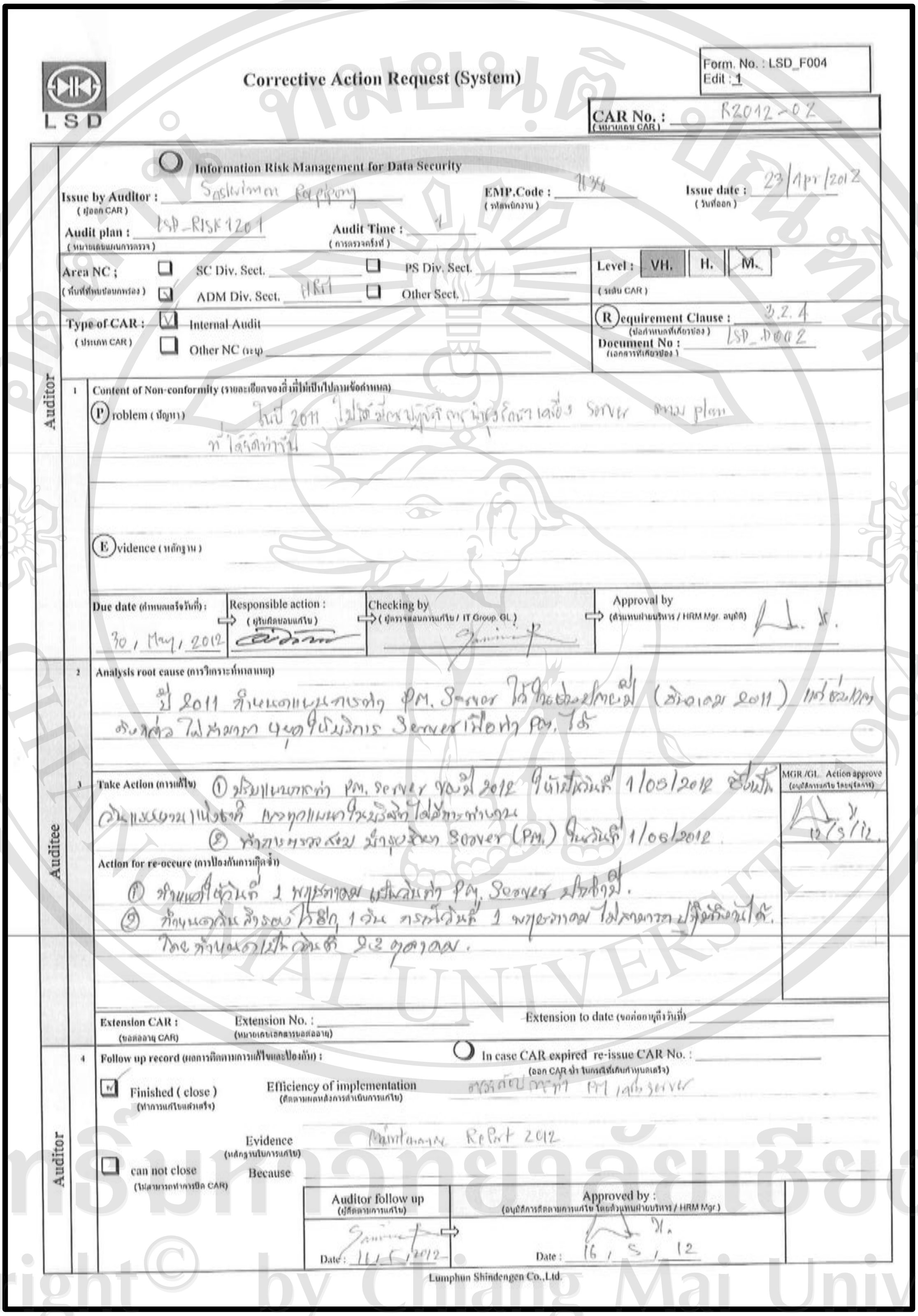
ภาพที่ 3-14 แสดงระบบสารสนเทศ ที่มีระบบ Server สำรองทำงานแทน (DR-Sit System)



ภาพที่ 3-15 แสดงการทดสอบระบบการกู้คืนข้อมูลสารสนเทศโดยใช้วิธีการทดสอบผ่าน Software

4) รายงานผลการแก้ไข

ทำการบันทึกผลการแก้ไขลงในเอกสาร Corrective Action Request (CAR.) จากนั้นส่งเอกสารเสนอผู้บริหารที่มีอำนาจ ทำการปิด Case ปัญหา (Closing CAR.) ดังแสดงตัวอย่างของเอกสาร Corrective Action Request (CAR.) ที่ดำเนินการแล้วเสร็จ ในภาพที่ 3-16 และภาพที่ 3-17



LSD

Corrective Action Request (System)

Form. No. : LSD_F004
Edit : 1

CAR No. : R2012-02 (หมายเลข CAR)

Information Risk Management for Data Security

Issue by Auditor : (ผู้ออก CAR) EMP.Code : (รหัสพนักงาน) Issue date : 23/Apr/2012 (วันที่ออก)

Audit plan : LSD_RISK1201 (หมายเลขแผนการตรวจ) Audit Time : 1 (การตรวจครั้งที่)

Area NC : (พื้นที่พบข้อบกพร่อง) ☐ SC Div. Sect. ☐ PS Div. Sect. ☒ ADM Div. Sect. HR1 ☐ Other Sect.

Level : VH. H. M. (ระดับ CAR)

Type of CAR : (ประเภท CAR) ☑ Internal Audit ☐ Other NC (ระบุ)

Requirement Clause : 3.2.4 (ข้อกำหนดที่เกี่ยวข้อง)

Document No : LSD_D002 (เอกสารที่เกี่ยวข้อง)

Auditor

1 Content of Non-conformity (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

Due date (กำหนดแล้วเสร็จวันที่) : 30/May/2012 | Responsible action : (ผู้รับผิดชอบแก้ไข) | Checking by (ผู้ตรวจสอบการแก้ไข / IT Group GL) | Approval by (ตัวแทนฝ่ายบริหาร / HRM Mgr. อนุมัติ)

Auditee

2 Analysis root cause (การวิเคราะห์หาสาเหตุ)

3 Take Action (การแก้ไข)

MGR/GL Action approve (อนุมัติการแก้ไข โดยผู้จัดการ) 12/5/12

Action for re-occure (การป้องกันการเกิดซ้ำ)

Extension CAR : (ขอต่ออายุ CAR) Extension No. : (หมายเลขเอกสารขอต่ออายุ) Extension to date (ขอต่ออายุถึงวันที่)

Auditor

4 Follow up record (ผลการติดตามการแก้ไขและป้องกัน) :

In case CAR expired re-issue CAR No. : (ออก CAR ใหม่ ในกรณีที่เกินกำหนดแล้วเสร็จ)

☑ Finished (close) (ทำการแก้ไขแล้วเสร็จ) Efficiency of implementation (ติดตามผลหลังการดำเนินการแก้ไข)

Evidence (หลักฐานในการแก้ไข) Maintenance Report 2012

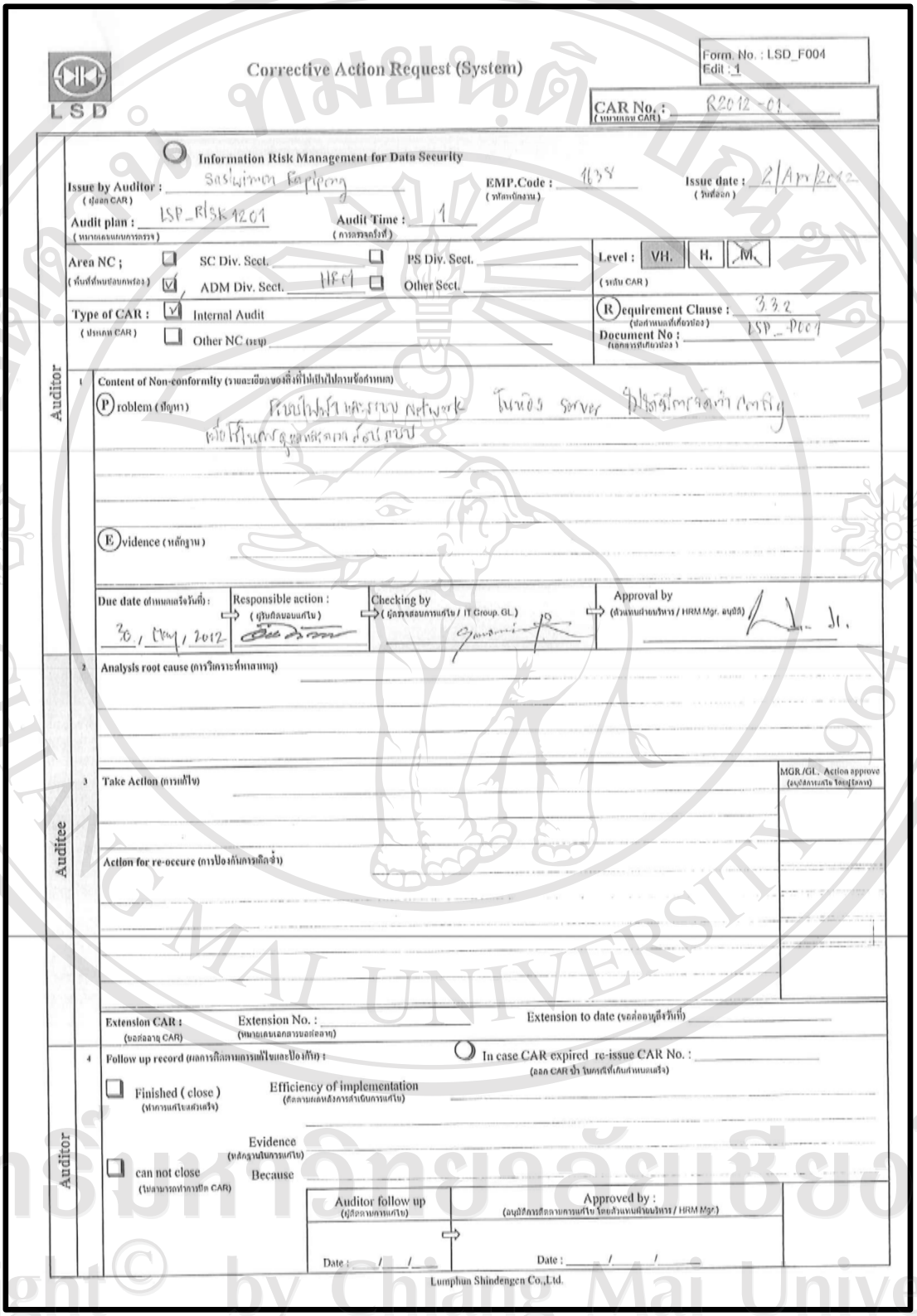
☐ can not close (ไม่สามารถทำการปิด CAR) Because

Auditor follow up (ผู้ติดตามการแก้ไข) Date : 11/5/2012

Approved by : (อนุมัติการติดตามการแก้ไข โดยตัวแทนฝ่ายบริหาร / HRM Mgr.) Date : 16/5/12

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-16 ตัวอย่างที่ 1 ของเอกสาร Corrective Action Request (CAR.) ที่ดำเนินการแล้วเสร็จ (CAR No. : R2012-01)



Corrective Action Request (System)

LSD

Form No. : LSD_F004
Edit : 1

CAR No. : R2012-01

Information Risk Management for Data Security

Issue by Auditor : Sasiwimon Kaipeng
EMP.Code : 1138
Issue date : 2/Apr/2012
Audit plan : LSP_RISK2012
Audit Time : 1

Area NC ; SC Div. Sect. PS Div. Sect.
ADM Div. Sect. HR01 Other Sect.
Level : VH. H. M.

Type of CAR : Internal Audit
Other NC
Requirement Clause : 3.3.2
Document No : LSP_PR01

Auditor

1 Content of Non-conformity
Problem
Evidence

Due date : 30/May/2012
Responsible action :
Checking by
Approval by

Auditee

2 Analysis root cause

3 Take Action
MGR./GL. Action approve
Action for re-occure

Extension CAR :
Extension No. :
Extension to date

Auditor

4 Follow up record
In case CAR expired re-issue CAR No. :
Finished (close)
Efficiency of implementation
Evidence
can not close
Because

Auditor follow up
Approved by :
Date : / /
Date : / /

Lumphun Shindengen Co.,Ltd.

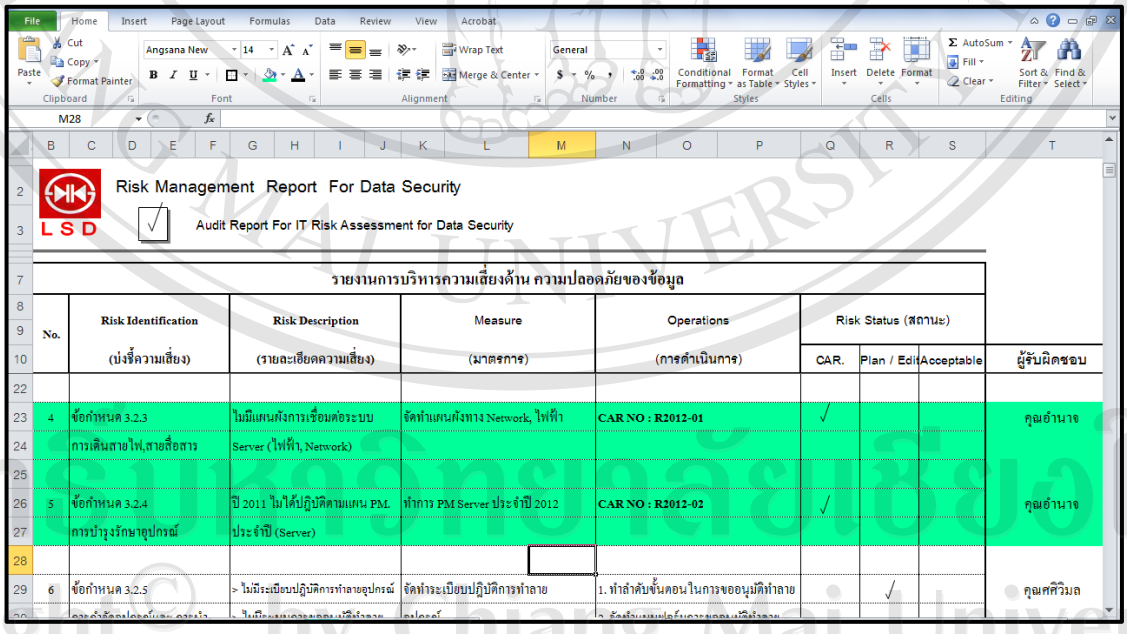
ภาพที่ 3-17 ตัวอย่างที่ 2 ของเอกสาร Corrective Action Request (CAR.) ที่ดำเนินการแล้วเสร็จ (CAR No.: R2012-01)

4. การติดตามผลการแก้ไขการเฝ้าระวังและการรายงานความเสี่ยงตกค้าง

ในส่วนนี้เป็นส่วนของการดำเนินการภายหลังจากมีการตรวจสอบภายในประจำปีแล้ว โดยเป็นการติดตามผลการแก้ไขประเด็นความเสี่ยงที่ตรวจพบในการตรวจภายใน ซึ่งหัวหน้างานสารสนเทศมีหน้าที่รายงานความถืบหน้าต่อผู้บริหารในการประชุมประจำเดือน เป็นประจำทุกๆเดือน และระบบยังกำหนดให้มีการเฝ้าระวังด้านความปลอดภัยของข้อมูล โดยต้องมีการรายงานต่อหัวหน้างานสารสนเทศหากเกิดประเด็นความเสี่ยงใหม่ขึ้นในองค์กร ซึ่งทั้งหมดสามารถสรุปกระบวนการทำงานได้เป็น 3 กระบวนการดังนี้

1) การติดตามผลการแก้ไข

ผู้ศึกษาได้ทำการประยุกต์แนวคิด เรื่องการจัดทำรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล (Risk Management Report For Data Security) โดยปรับให้เป็นเอกสารติดตามสถานะ การปรับปรุงแก้ไข โดยเพิ่มช่องของผู้รับผิดชอบเข้ามา จากนั้นนำข้อมูลเก็บไว้ในไฟล์ที่ผู้เกี่ยวข้องสามารถตรวจสอบได้และให้ผู้รับผิดชอบในแต่ละประเด็น สามารถเข้ามาปรับปรุงสถานะ การแก้ไขประเด็นความเสี่ยงที่ตนรับผิดชอบ ดังแสดงตัวอย่างในภาพที่ 3-16



Risk Management Report For Data Security

Audit Report For IT Risk Assessment for Data Security

รายงานการบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Measure (มาตรการ)	Operations (การดำเนินการ)	Risk Status (สถานะ) CAR.	Plan / Edit	Acceptable	ผู้รับผิดชอบ
4	ข้อกำหนด 3.2.3 การเดินสายไฟ,สายสื่อสาร	ไม่มีแผนผังการเชื่อมต่อระบบ Server (ไฟฟ้า, Network)	จัดทำแผนผังทาง Network, ไฟฟ้า	CAR NO : R2012-01	√			คุณอำนาจ
5	ข้อกำหนด 3.2.4 การบำรุงรักษาอุปกรณ์	ปี 2011 ไม่ได้ปฏิบัติตามแผน PM. ประจำปี (Server)	ทำการ PM Server ประจำปี 2012	CAR NO : R2012-02	√			คุณอำนาจ
6	ข้อกำหนด 3.2.5	> ไม่มีระเบียบปฏิบัติการทำลายอุปกรณ์	จัดทำระเบียบปฏิบัติการทำลาย	1. ทำลำดับขั้นตอนในการขออนุมัติทำลาย		√		คุณศศิวิมล

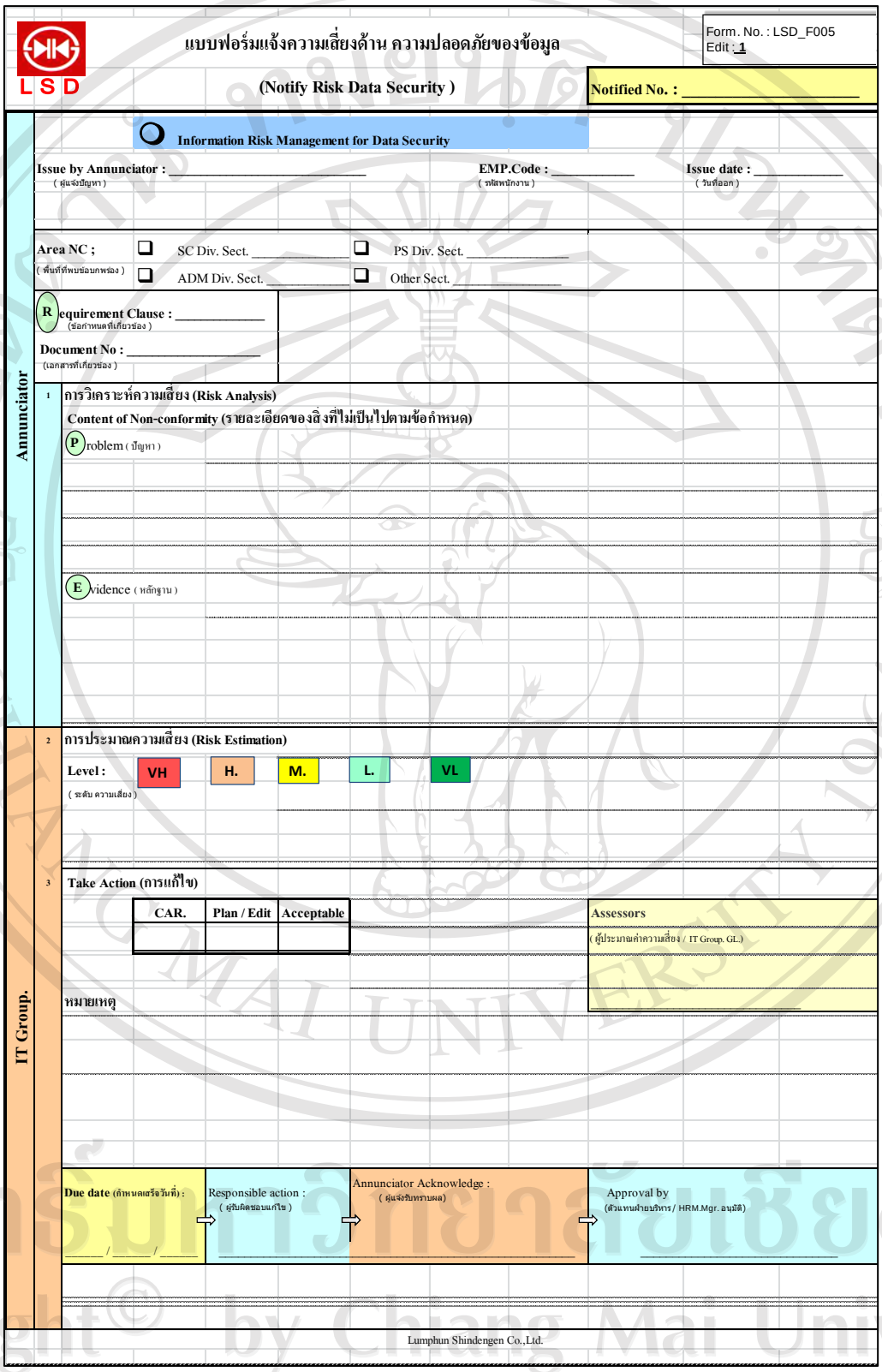
ภาพที่ 3-18 ตัวอย่างการติดตามผลการแก้ไขประเด็นความเสี่ยง

2) การเฝ้าระวัง

การเฝ้าระวัง ในการศึกษาครั้งนี้หมายความถึง การกำหนดให้ผู้ที่เกี่ยวข้องหรือบุคคลในกลุ่มงานที่รับผิดชอบทำการ เฝ้าระวัง สังเกต ระบบสารสนเทศ หรือข้อมูลที่ตนดูแลรับผิดชอบ ว่าพบประเด็นความเสี่ยงเกิดขึ้นเพิ่มหลังจากการตรวจหรือไม่ หากพบประเด็นความเสี่ยงใหม่ ระบบระบุให้ดำเนินการบันทึกประเด็นความเสี่ยงลงในแบบฟอร์มแจ้งความเสี่ยงด้านความปลอดภัยของข้อมูล (Notify Risk Data Security): LSD_F005 โดยจะเป็นการรายงานประเด็นความเสี่ยงด้านความปลอดภัยของข้อมูล มาที่กลุ่มงานสารสนเทศและหัวหน้างานสารสนเทศมีหน้าที่ประมาณค่าความเสี่ยงและกำหนดมาตรการรองรับ แก้ไขหรือควบคุมความเสี่ยงอีกทั้งต้องรายงานให้ฝ่ายบริหารรับทราบ ในประเด็นความเสี่ยงที่พบด้วย โดยรายละเอียดของแบบฟอร์มแจ้งความเสี่ยงด้านความปลอดภัยของข้อมูล (Notify Risk Data Security): LSD_F005 ดังแสดงไว้ในภาพที่ 3-17

3) การรายงานความเสี่ยงตกค้าง

การรายงานความเสี่ยงตกค้าง (Residual Risk Reporting) เป็นรายงานสรุปการปรับปรุงแก้ไขประจำปี ซึ่งจะเป็นข้อมูลสำหรับใช้อ้างอิงในการตรวจสอบภายในปีถัดไป คณะทำงานได้กำหนดให้จัดทำรายงานความเสี่ยงตกค้างใน เดือนธันวาคม พ.ศ. 2555 อีกทั้งเนื่องจากว่าในขณะที่ผู้ศึกษากำลังทำการสรุปผลการศึกษาอยู่นี้ (15 พฤษภาคม พ.ศ. 2555) ประเด็นความเสี่ยงที่ตรวจพบ ส่วนใหญ่กำลังอยู่ในระหว่างดำเนินการ จึงทำให้ผู้ศึกษายังไม่สามารถ สรุปรายงานความเสี่ยงตกค้างประจำปี พ.ศ. 2555 ได้



แบบฟอร์มแจ้งความเสี่ยงด้าน ความปลอดภัยของข้อมูล

(Notify Risk Data Security)

Form. No. : LSD_F005
Edit : 1

Notified No. : _____

Information Risk Management for Data Security

Issue by Annunciator : _____ (ผู้แจ้งปัญหา)

EMP.Code : _____ (รหัสพนักงาน)

Issue date : _____ (วันที่ออก)

Area NC ; (พื้นที่ที่พบข้อบกพร่อง)

❑ SC Div. Sect. _____ ❑ PS Div. Sect. _____

❑ ADM Div. Sect. _____ ❑ Other Sect. _____

Requirement Clause : _____ (ข้อกำหนดที่เกี่ยวข้อง)

Document No : _____ (เอกสารที่เกี่ยวข้อง)

Annunciator

1 การวิเคราะห์ความเสี่ยง (Risk Analysis)

Content of Non-conformity (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

IT Group.

2 การประมาณความเสี่ยง (Risk Estimation)

Level : VH H. M. L. VL (ระดับ ความเสี่ยง)

3 Take Action (การแก้ไข)

CAR.	Plan / Edit	Acceptable

Assessors (ผู้ประมาณค่าความเสี่ยง / IT Group. GL.)

หมายเหตุ

Due date (กำหนดเสร็จวันที่) : ____/____/____ ⇨ Responsible action : (ผู้รับผิดชอบแก้ไข) ⇨ Annunciator Acknowledge : (ผู้แจ้งรับทราบผล) ⇨ Approval by (ตัวแทนฝ่ายบริหาร / HRM.Mgr. อนุมัติ)

Lumphun Shindengen Co.,Ltd.

ภาพที่ 3-19 ตัวอย่างแบบฟอร์มแจ้งความเสี่ยงด้านความปลอดภัยของข้อมูล (Notify Risk Data Security): LSD_F005

5. การจัดทำคู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

ผู้ศึกษาได้จัดทำคู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ประจำปี พ.ศ. 2555 ขึ้นเพื่อเป็นแนวทางให้กับบริษัท สำหรับการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล และเพื่อให้ผู้บริหาร รวมถึงผู้ปฏิบัติงานทุกหน่วยงานได้มีความเข้าใจถึงกระบวนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล จนสามารถดำเนินการตามกระบวนการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลได้และในส่วนท้ายของคู่มือผู้ศึกษาได้แนบ รายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลไว้ด้วยซึ่งในรายงานได้สรุปประเด็นที่เป็นความเสี่ยง รวมถึงแนวทางในการแก้ไข ควบคุมความเสี่ยงต่างๆให้ลดลง อยู่ในระดับที่องค์กรยอมรับได้ เพื่อเป็นตัวอย่างหรือแนวปฏิบัติในลำดับต่อไป โดยรายละเอียด คู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล บริษัทลำพูนซิงเด็นเก็น จำกัด ประจำปี พ.ศ. 2555 ดังแสดงไว้ใน ภาคผนวก ฌ

6. สำรวจและประเมินความเสี่ยง ในรอบต่อไป

ในขั้นตอนนี้เปรียบได้กับการทำ PDCA ในรอบต่อไป ซึ่งจะมีการดำเนินการในปี พ.ศ. 2556 และไม่ถือเป็นส่วนหนึ่งการศึกษาครั้งนี้