คู่มือการตรวจสอบ
ด้าน Electronic Banking

คำนำ

คู่มือการตรวจสอบด้าน Electronic-Banking (E-Banking) เป็นผลงานจากการดำเนินงานของโครงการกำกับ E-Banking ตามแผนกลยุทธ์ของธนาคารแห่งประเทศไทย และของสายกำกับสถาบันการเงิน (สกส.) ในการกำกับดูแลความเสี่ยงที่เกิดขึ้นจากการดำเนินธุรกรรมด้าน E-Banking ของสถาบันการเงินต่างๆ โดยมีวัตถุประสงค์ เพื่อช่วยให้ผู้ตรวจสอบสถาบันการเงินด้านเทคโนโลยีสารสนเทศ สามารถประเมินความเพียงพอของระบบการรักษาความปลอดภัย ในการดำเนินงาน รวมทั้งการบริหารและควบคุมความเสี่ยงด้าน E-Banking ว่าสถาบันการเงินแต่ละแห่ง ได้มีการบริหารความเสี่ยงในทุกด้านอย่างเพียงพอที่จะเชื่อมั่นได้ว่าจะไม่เกิดปัญหาใดที่จะกระทบกับชื่อเสียงและฐานะการดำเนินงานของสถาบันการเงินนั้นๆ และไม่ส่งผลกระทบกับความเชื่อถือที่มีต่อระบบสถาบันการเงินในประเทศไทย โดยรวม ซึ่งจะสอดคล้องกับแผนกลยุทธ์โดยรวมของธนาคารแห่งประเทศไทยที่มุ่งจะเสริมสร้างความมั่นคงของสถาบันการเงินเป็นสำคัญ

การจัดทำคู่มือการตรวจสอบด้าน E-Banking ฉบับนี้ได้อาศัยแนวทางของธนาคารกลางประเทศสหรัฐอเมริกา และ BIS เป็นหลัก และยังได้รับความช่วยเหลือจาก Office of the Comptroller of the Currency (OCC) และ Federal Reserve Banks (FRB) จากประเทศสหรัฐอเมริกา และ ธนาคารโลก (World Bank) ในการส่งผู้เชี่ยวชาญมาให้ความรู้ คำแนะนำ และแลกเปลี่ยนประสบการณ์ที่เป็นประโยชน์ นอกจากนี้ทีมงานได้ไปศึกษาดูงานที่ธนาคารกลาง ธนาคารพาณิชย์และองค์กรเอกชนที่เกี่ยวข้องในประเทศสิงค์โปร์และประเทศเกาหลี เมื่อจัดทำคู่มือฉบับร่างเสร็จแล้วได้นำไปทดลองใช้ปฏิบัติงานตรวจสอบที่ธนาคารพาณิชย์ในประเทศ 2 แห่ง และได้นำประสบการณ์ภาคปฏิบัติมาปรับปรุงคู่มืออีกครั้งหนึ่ง

คู่มือการตรวจสอบด้าน E-Banking ฉบับนี้ สามารถจัดทำสำเร็จขึ้นได้ โดยได้รับการสนับสนุนจากผู้บริหารและพนักงาน ในสายกำกับสถาบันการเงินโดยเฉพาะพนักงานในส่วนตรวจสอบเทคโนโลยีสารสนเทศ และคณะทำงานจากสายนโยบายสถาบันการเงิน สายระบบชำระเงิน สายเทคโนโลยีสารสนเทศ และสายตรวจสอบกิจการภายใน ในการเข้าร่วมให้ความคิดเห็นและข้อเสนอแนะที่เป็นประโยชน์

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

บทสรุป

ปัจจุบันเทคโนโลยีเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันและการดำเนินธุรกิจมากขึ้น บทบาทของเทคโนโลยีจะไม่ได้จำกัดอยู่ที่ระดับของธุรกิจเท่านั้น แต่ได้แผ่ขยายเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันของบุคคลทั่วไป ดังจะเห็นได้จากการมีโทรศัพท์มือถือ การใช้เครือข่ายอินเตอร์เน็ตเพื่อการติดต่อสื่อสาร เป็นต้น ธุรกิจหลากหลายประเภทได้เริ่มหันมาเน้นการใช้ประโยชน์จากเทคโนโลยีกันมากขึ้น ไม่เว้นแม้แต่สถาบันการเงินที่กำลังเริ่มขยายช่องทางการให้บริการผ่านเครือข่ายอิเล็กทรอนิกส์ เช่น การให้บริการ Internet Banking การให้บริการ Mobile Bankingหรือ ATM เป็นต้น ลักษณะการให้บริการ Electronic Banking (E-Banking) ในประเทศไทย มี 2 ลักษณะ คือ เพื่อการประชาสัมพันธ์ ข้อมูลข่าวสาร และเพื่อการทำธุรกรรมทางการเงินกับธนาคาร จึงทำให้สถาบันการเงินสามารถเข้าถึงฐานลูกค้าได้อย่างกว้างขวางขึ้น สามารถให้บริการแก่ลูกค้าได้รวดเร็วขึ้น และสามารถลดค่าใช้จ่ายในระยะยาวและเป็นการสร้างรายได้ค่าธรรมเนียมได้อีกทางหนึ่ง

อย่างไรก็ตาม ถึงแม้ว่าการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ ไม่ได้ก่อให้เกิดความเสี่ยงรูปแบบแปลกใหม่เกิดขึ้น แต่กลับจะเป็นการเพิ่มปริมาณความรุนแรงของความเสี่ยงประเภทเดิมๆที่สถาบันการเงินประสบอยู่แล้วให้มากขึ้นได้ เนื่องจากการเข้าถึงลูกค้าทำได้อย่างไร้พรมแดน และ ข้อมูลธุรกรรมทางการเงินของลูกค้าจะถูกส่งผ่านสื่ออิเล็กทรอนิกส์ ตัวอย่างเหตุการณ์ที่จะทวีความรุนแรงของความเสี่ยง ได้แก่ การปล่อยสินเชื่อไม่มีคุณภาพ การโจรกรรมข้อมูลลูกค้า รูปแบบบริการอาจไปขัดต่อกฎหมายของประเทศที่มีการนำเสนอบริการนั้น เป็นต้น ซึ่งเหตุการณ์เหล่านี้จะทำให้เพิ่มความเสี่ยง เช่น ความเสี่ยงต่อการเสียชื่อเสียง ความเสี่ยงจากการดำเนินงาน และความเสี่ยงด้านกลยุทธ์ ดังนั้นเพื่อให้ลูกค้าเกิดความเชื่อมั่นในการทำธุรกรรมทางการเงินผ่านสื่ออิเล็กทรอนิกส์ ฝ่ายบริหารควรจะมีการกำหนดนโยบายและวางแผนกลยุทธ์ทั้งในเชิงธุรกิจและด้านเทคโนโลยีสำหรับการดำเนินธุรกิจด้าน E-Banking โดยเฉพาะเพื่อให้มีความสอดคล้องกันระหว่างแผนกลยุทธ์และแผนการปฏิบัติงานของสถาบันการเงิน รวมไปถึงความเพียงพอของระบบการควบคุมภายในและระบบการรักษาความปลอดภัยที่มีประสิทธิภาพ และส่งเสริมให้มีระบบการบริหารความเสี่ยงที่ดีดังกล่าว

ในการนี้ ธปท. โดยสายกำกับสถาบันการเงิน (สกส.) ได้พัฒนาแนวคิดของหลักการบริหารความเสี่ยงด้าน E-Banking ที่สถาบันการเงินพึงปฏิบัติ โดยอ้างอิงจาก Risk Management Principles for Electronic Banking ซึ่งพัฒนาโดย Bank for International Settlements ฉบับเดือนพฤษภาคม 2001 ซึ่งได้มีการปรับปรุงเนื้อหาให้มีความเหมาะสมเข้ากับสถานการณ์ของธุรกิจ E-Banking ในระบบสถาบันการเงินไทย หลักการบริหารความเสี่ยงมีทั้งหมด 14 ข้อ แบ่งเป็น 3 กลุ่มหลัก

ได้แก่ การกำกับดูแลด้าน E-Banking ของคณะกรรมการและผู้บริหาร (Board and Management Oversight) การควบคุมการรักษาความปลอดภัย (Security Controls) และการบริหารความเสี่ยงเกี่ยวกับเรื่องกฎหมายและชื่อเสียง (Legal and Reputational Risk Management)

ในการตรวจสอบการดำเนินธุรกิจด้าน E-Banking ของสถาบันการเงิน มีวัตถุประสงค์เพื่อประเมินความเสี่ยงของการทำธุรกิจในด้านดังกล่าวซึ่งอาจส่งผลกระทบต่อฐานะและความสามารถในการดำเนินงานของสถาบันการเงิน รวมทั้งให้ข้อเสนอแนะในการแก้ไขปัญหาหรือลดความเสี่ยงในการประกอบธุรกิจ E-Banking ก่อนที่จะเกิดความเสียหายแก่สถาบันการเงินเป็นสำคัญ ซึ่งแนวทางการตรวจสอบจะใช้แบบเดียวกับแนวทางการตรวจสอบความเสี่ยง กล่าวคือ จะเริ่มตั้งแต่ขั้นเตรียมการออกตรวจสอบ ขั้นดำเนินการตรวจสอบสถาบันการเงิน และขั้นการสรุปผลและออกรายงาน โดยมีขอบเขตของการตรวจสอบ ดังนี้

1. การตรวจสอบเพื่อประเมินความเสี่ยงเชิงปริมาณ โดยพิจารณาจาก โครงสร้างระบบเครือข่าย ลักษณะของบริการ และปริมาณรายการธุรกรรม

2. การตรวจสอบเพื่อประเมินความเสี่ยงเชิงคุณภาพ จะเป็นการตรวจสอบเพื่อประเมินการจัดการและบริหารความเสี่ยงด้าน E-Banking โดยจะคำนึงถึงปัจจัย 5 ด้าน ดังนี้

2.1 นโยบายและการจัดการ

2.2 การควบคุมภายในและการรักษาความปลอดภัย

2.3 การตรวจสอบและสอบทาน

2.4 การติดตามในระบบสารสนเทศและสื่อสาร

2.5 การบริหารจัดการทางเทคโนโลยีโดยองค์กรภายนอก

ลักษณะการตรวจสอบเพื่อประเมินความเสี่ยงเชิงคุณภาพแบ่งเป็น 2 ระดับ คือ การตรวจสอบหลัก (Core Analysis) และการตรวจสอบเพิ่มเติม (Expanded Analysis) โดยในกรณีที่ผู้ตรวจสอบพบจุดอ่อนของระบบการบริหารและการจัดการที่มีผลกระทบเป็นนัยสำคัญต่อบริการE-Banking หรือมีข้อบกพร่องในผลการดำเนินงานซึ่งส่งผลกระทบที่เป็นนัยสำคัญต่อฐานะความมั่นคงของสถาบันการเงินให้ผู้ตรวจสอบดำเนินการตามแนวทางการตรวจสอบเพิ่มเติม

3. การตรวจสอบเพื่อการประเมินการปฏิบัติตามกฎหมาย

ส่วนที่ 1 รูปแบบ ลักษณะและคำนิยามของ E-Banking

การนำเสนอบริการทางการเงินผ่านสื่ออิเล็กทรอนิกส์ (E-Banking) ของสถาบันการเงินมีหลายรูปแบบ ซึ่งมักจะตั้งชื่อของบริการตามช่องทางที่ให้บริการหรือประเภทของเครื่องมือที่ใช้ในการชำระเงิน สำหรับในประเทศไทยสามารถแบ่งประเภทบริการตามลักษณะของเครือข่ายอิเล็กทรอนิกส์ได้ ดังนี้

1. บริการทางการเงินโดยผ่านเครือข่ายแบบส่วนตัว เป็นการอาศัยเครือข่ายส่วนตัว เช่น คู่สายโทรศัพท์ (leased line) หรือ เครือข่ายส่วนตัวแบบเสมือนจริง(VPN :Virtual Private Network) ซึ่งผู้ที่จะสามารถเชื่อมโยงถึงเครือข่ายนี้ได้ คือ ผู้ที่ได้รับสิทธิจากธนาคารเท่านั้น โดยบริการส่วนใหญ่เป็นบริการที่สถาบันการเงินได้เปิดให้บริการกับลูกค้ามานานแล้ว ได้แก่

1.1 บริการ Office Banking / Corporate Banking เป็นบริการที่ให้แก่ลูกค้านิติบุคคล สามารถเข้ามาใช้บริการทางการเงินที่ธนาคารเปิดให้บริการอยู่ได้โดยใช้คอมพิวเตอร์เชื่อมต่อผ่านสายโทรศัพท์จากที่ทำการของลูกค้าเข้ามาที่หมายเลขโทรศัพท์ที่ธนาคารกำหนดไว้ โดยลูกค้าจะต้องป้อนรหัสผ่านที่ธนาคารออกให้

1.2 บริการ Home Banking / PC Banking จะมีลักษณะการเชื่อมต่อเช่นเดียวกันกับ Office Banking แต่จะให้บริการกับลูกค้าประเภทบุคคลธรรมดา

1.3 บริการเอทีเอ็ม (ATM) เป็นการให้บริการทางการเงินของธนาคารผ่านเครื่อง ATM ซึ่งในปัจจุบันมีการให้บริการที่หลากหลายขึ้น นอกเหนือจากจะให้บริการถอนเงินอัตโนมัติ แล้วยังให้บริการโอนเงินรายย่อยระหว่างธนาคารแบบออนไลน์ (ORFT- On-line Retail Funds Transfer) และบริการจ่ายชำระค่าสินค้าและบริการ เป็นต้น

1.4 บริการบัตรเครดิต (Credit Card) เป็นสื่อการชำระเงินในลักษณะซื้อก่อนจ่ายทีหลัง (Pay Later)

1.5 บริการบัตรเดบิต (Debit Card) / บัตรเอทีเอ็ม (ATM Card) เป็นบัตรพลาสติกประเภทหักเงินในบัญชีของผู้ถือบัตรทันทีเมื่อซื้อสินค้าและบริการ (Pay Now) บัตรเดบิตที่นิยมใช้กันอยู่ในปัจจุบัน ได้แก่ บัตร Visa Electron Card ซึ่งสามารถนำไปใช้ที่ร้านค้าในต่างประเทศได้

1.6 บริการ E-Money เช่น สมาร์ทการ์ด (Smart Card) หรือกระเป๋าสตางค์อิเล็กทรอนิกส์ (E-Purse) เป็นบัตรที่ผู้ถือบัตรได้จ่ายเงินล่วงหน้า (Pay Before) ให้แก่ผู้ออกบัตร เพื่อใช้ชำระค่าสินค้าหรือบริการที่มีมูลค่าทางการเงินไม่สูงนัก

2. บริการทางการเงินโดยผ่านเครือข่ายแบบสาธารณะ เป็นการอาศัยเครือข่ายสาธารณะ เช่น เครือข่ายโทรศัพท์สาธารณะ เครือข่ายโทรศัพท์มือถือ และเครือข่ายอินเตอร์เน็ต เป็นต้น มาให้บริการธุรกรรมบางอย่างของธนาคาร ได้แก่

2.1 บริการธนาคารผ่านเครือข่ายโทรศัพท์บ้าน (Phone Banking หรือ Tele Banking) เป็นบริการให้ลูกค้าทำธุรกรรมทางการเงินโดยใช้โทรศัพท์ธรรมดาติดต่อไปที่หมายเลขโทรศัพท์ที่แต่ละธนาคารกำหนดขึ้น โดยนำเสนอทั้งในรูปแบบบริการตอบรับอัตโนมัติ (Interactive Voice Response: IVR) และศูนย์บริการลูกค้า (Call Center) ซึ่งมีเจ้าหน้าที่คอยให้บริการ

2.2 บริการธนาคารผ่านโทรศัพท์มือถือ (Mobile Banking / M-Banking) เป็นบริการที่ให้ลูกค้าสามารถทำธุรกรรมทางการเงินด้วยตนเองผ่านโทรศัพท์มือถือ โดยต้องมีรหัสผ่านที่ออกโดยธนาคารเช่นกันและใช้ระบบรักษาความปลอดภัยแบบ End-to-End Encryption

2.3 บริการธนาคารผ่านเครือข่ายอินเตอร์เน็ต (Internet Banking) เป็นบริการที่ให้ลูกค้าสามารถทำธุรกรรมทางการเงินผ่านทางเครือข่ายอินเตอร์เน็ตด้วยตนเองจากทุกที่ที่สามารถใช้อินเตอร์เน็ตได้ โดยอาศัยช่องทางในการติดต่อสื่อสารที่เป็นอุปกรณ์อิเล็กทรอนิกส์ที่มีอยู่มากมายหลากหลายรูปแบบ เช่น PCs, ATM, KIOSKs, Mobile Phone , PDAs, Cable TVs, หรือสื่อชนิดอื่นๆ ที่จะช่วยให้ลูกค้าสามารถทำรายการทางการเงินในลักษณะโต้ตอบกับระบบงานของธนาคารหรือสถาบันการเงินได้เองโดยอัตโนมัติ ในส่วนของบริการธนาคารบนเครื่องคอมพิวเตอร์มือถือ (PDA Banking : Personal Digital Assistant Banking) ซึ่งวิวัฒนาการของ PDA มี 3 รูปแบบ คือ Palm, Pocket PC และ Smart Phone โดยมีวิธีการเชื่อมต่อได้ 2 วิธี คือ ต่อผ่านโทรศัพท์มือถือผ่าน port infrared หรือ ต่อกับสายโทรศัพท์ที่บ้านด้วยอุปกรณ์ต่อพ่วงที่มากับ PDA

1. ลักษณะการให้บริการ E-Banking ในประเทศไทย

การให้บริการ E-Banking ในประเทศไทยนั้นสามารถแบ่งลักษณะการให้บริการในภาพกว้างได้เป็น 2 ลักษณะ ดังนี้

1.1 บริการในลักษณะของการให้ข้อมูลข่าวสาร (Information Services) เป็นบริการที่สถาบันการเงินใช้วิธีการทางอิเล็กทรอนิกส์มาเป็นช่องทางในการให้ข้อมูลข่าวสารของสถาบันการเงินแก่ลูกค้า เช่นเดียวกับการโฆษณา หรือเผยแพร่ธุรกิจที่ให้บริการ เช่น ประกาศอัตราดอกเบี้ย อัตราแลกเปลี่ยน ขั้นตอนปฏิบัติในการขอสินเชื่อ ข่าวสารความเคลื่อนไหวของธนาคาร เป็นต้น

1.2 บริการในการทำธุรกรรมกับสถาบันการเงิน (Transaction Services) เป็นการใช้วิธีการทางอิเล็กทรอนิกส์มาเป็นช่องทางให้ลูกค้าสามารถทำธุรกรรมทางการเงินที่นอกเหนือจากการให้ข้อมูลข่าวสารตามข้อ 1.1 ในลักษณะโต้ตอบกับระบบงานของสถาบันการเงิน ซึ่งประเภทและขอบเขตของธุรกรรมทางการเงินที่ให้บริการจะต้องเป็นธุรกรรมที่ได้รับอนุญาตจากธนาคารแห่ง

ประเทศไทย ตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่จะแก้ไขเพิ่มเติมต่อไป (ผู้ตรวจสอบ ควรศึกษารายละเอียดเกี่ยวกับการให้บริการธนาคารผ่านเครือข่าย Internet ทั้งในประเทศไทย และต่างประเทศ เพิ่มเติม ได้ในภาคผนวก 2)

2. ผู้ที่เกี่ยวข้องในระบบ E-Banking

ในระบบ หรือ วงจรของ E-Banking จะมีผู้ที่เกี่ยวข้อง ดังนี้

2.1 ลูกค้าของสถาบันการเงิน มีบทบาทในฐานะผู้ใช้บริการ แบ่งเป็น

- ประเภทบุคคลธรรมดา
- ประเภทนิติบุคคล

2.2 สถาบันการเงิน ซึ่งจะมีบทบาทเป็นผู้ให้บริการทางการเงิน

2.3 สถาบันอื่น แบ่งเป็น

- บริษัทผู้เชี่ยวชาญทางเทคโนโลยี เช่น ผู้ให้บริการทางอินเตอร์เน็ต (Internet Service Providers-ISP) ผู้แทนจำหน่ายระบบงาน (Vendor) เป็นต้น
- องค์กรอื่นที่มิใช่สถาบันการเงิน เช่น ผู้ประกอบการต่างๆ

2.4 ผู้ให้บริการเกี่ยวกับการรับรอง (Trusted Third Party)

- Certificate Authority (CA) เป็นองค์กรกลางที่มีหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Digital certificates) เพื่อก่อให้เกิดความมั่นใจแก่ผู้ที่เกี่ยวข้องทั้งสองฝ่ายในระบบ ได้แก่ ผู้ใช้บริการและ ผู้ให้บริการ เพื่อยืนยันว่าบุคคลที่ทั้งสองฝ่ายติดต่ออยู่ คือ บุคคลนั้นจริง ซึ่งใบรับรองอิเล็กทรอนิกส์นั้นอาจอยู่ในรูปของสื่อกลาง (media) ในรูปแบบใดก็ได้ ขึ้นอยู่กับระดับของความปลอดภัยที่ต้องการ ส่วนมากจะเป็นสื่อกลางประเภทสมาร์ทการ์ด
- Registration Authority (RA) เป็นหน่วยงานที่ทำหน้าที่นายทะเบียนเพื่อตรวจสอบความถูกต้องของข้อมูลหลักฐานต่าง ๆ ก่อนที่จะเชื่อมโยงระบบมาที่ CA

2.5 กระทรวงการคลัง ซึ่งได้มอบหมายให้ธนาคารแห่งประเทศไทยกำกับดูแลสถาบันการเงินแทน

3. คำนิยามของ E-Banking

ปัจจุบัน พบว่าองค์กรต่าง ๆ ได้ให้คำนิยามของ E-Banking ซึ่งมีความหลากหลายไปตามแต่ละองค์กร ดังที่ระบุไว้ในภาคผนวก 1 อย่างไรก็ตาม คำนิยามที่ได้กำหนดโดยแต่ละองค์กรนั้นไม่ได้แตกต่างกันอย่างเป็นนัยสำคัญ โดยความแตกต่างจะขึ้นอยู่กับขอบเขตความครอบคลุมของประเภทสื่ออิเล็กทรอนิกส์ ลักษณะระบบเครือข่าย หรือประเภทธุรกรรม เป็นต้น

อย่างไรก็ดี คู่มือฉบับนี้ให้ความหมายของ E-Banking ไว้ดังนี้

การให้บริการ E-Banking หมายถึง “การนำเสนอบริการหรือผลิตภัณฑ์ของสถาบันการเงินผ่านเครือข่ายอิเล็กทรอนิกส์ ซึ่งหมายรวมถึงบริการในลักษณะของการให้ข้อมูลข่าวสาร และบริการในการทำธุรกรรมทางการเงินผ่านช่องทางหรือเครือข่ายอินเทอร์เน็ต (Internet)”

ส่วนที่ 2 ความเสี่ยงและแนวทางการบริหารความเสี่ยงด้าน E-Banking

1. ประเภทของความเสี่ยงที่เกี่ยวข้องกับการให้บริการ E-Banking

1.1 นิยามของความเสี่ยง

ความเสี่ยง ก็คือ การดำเนินกิจกรรมใดๆ ในสถาบันการเงินแล้วก่อให้เกิดความเป็นไปได้ ที่จะทำให้เกิดความเสียหายต่อรายได้ (Earning) หรือเงินกองทุน (Capital) ของสถาบันการเงิน [1]

ทั้งนี้ ไม่ว่าระบบงานอิเล็กทรอนิกส์จะมีระดับของความสลับซับซ้อนอยู่ในระดับใดก็ตามเราก็จะพบว่ายังมีความเสี่ยงในการให้บริการอยู่เสมอ เช่น Web Site ที่ให้บริการในระดับ Information-Only ก็อาจจะพบกับปัญหาในเรื่องที่ Web Site ดังกล่าวอาจจะถูกผู้ประสงค์ร้ายเข้ามาเปลี่ยนแปลงข้อมูลโดยมิได้รับอนุญาตได้ ในขณะที่ยังมีความเสี่ยงที่อาจจะมีการส่งจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นความลับหรือเป็นเนื้อหาที่เป็นของส่วนตัวจะถูกส่งไปผิดตัวถึงผู้ที่ไม่ควรจะได้รับข้อมูล หรือระบบฐานข้อมูลของธนาคารจะถูกเข้าถึงโดยผู้ไม่มีสิทธิซึ่งประสงค์จะเข้าไปดูข้อมูลหรือระบบงานที่เป็นความลับ หรือเกิดการหยุดชะงักในการดำเนินงานของระบบคอมพิวเตอร์เพราะว่าระบบไฟฟ้าขัดข้อง หรือระบบงานเกิดทำงานบกพร่อง

1.2 ประเภทของความเสี่ยงที่เกี่ยวข้องกับ E-Banking

ด้วยลักษณะการทำธุรกรรมทางการเงินผ่านเครือข่ายอิเล็กทรอนิกส์ โดยเฉพาะ Internet จะทำให้สถาบันการเงินสามารถเข้าถึงลูกค้าได้อย่างไร้พรมแดน ลูกค้าไม่ต้องเดินทางมาทำรายการที่สำนักงานหรือสาขาที่ตั้งของสถาบันการเงิน และข้อมูลรายการธุรกรรมของลูกค้าจะถูกส่งผ่านทางสื่ออิเล็กทรอนิกส์ นั้น ล้วนเป็นการท้าทายต่อการบริหารและควบคุมความเสี่ยงของสถาบันการเงิน ถึงแม้ว่าด้วยลักษณะดังกล่าว จะไม่ก่อให้เกิดความเสี่ยงประเภทใหม่ๆขึ้นต่อสถาบันการเงินก็ตาม แต่อาจจะเป็นการเพิ่มโอกาสของการเกิดความเสี่ยงในแต่ละประเภทที่สถาบันการเงินประสบอยู่แล้วให้มากขึ้นและอาจส่งผลเสียหายต่อฐานะทางการเงินและชื่อเสียงของสถาบันการเงินให้รุนแรงขึ้นได้

ทั้งนี้ การพิจารณาความเสี่ยง จะเป็นไปตามประเภทความเสี่ยงที่ระบุในคู่มือการตรวจสอบความเสี่ยงของธนาคารแห่งประเทศไทย ที่จัดทำโดยส่วนตรวจสอบความเสี่ยง ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ สายกำกับสถาบันการเงิน ซึ่งแบ่งเป็น 5 ด้าน ดังนี้

[1] "Risk : Any activity within the financial institution that creates exposure of loss to earnings and/or capital.", from the courtesy of the Federal Reserve Banking System

- ความเสี่ยงด้านกลยุทธ์
- ความเสี่ยงด้านเครดิต
- ความเสี่ยงด้านตลาด
- ความเสี่ยงด้านสภาพคล่อง
- ความเสี่ยงด้านปฏิบัติการ

การตรวจสอบด้าน E-Banking จะมีความเกี่ยวข้องและเชื่อมโยงกับการตรวจสอบความเสี่ยงตามที่กล่าวข้างต้น ดังนั้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศ จึงจำเป็นที่จะต้องมีพื้นฐานความรู้ของการตรวจสอบตามความเสี่ยงแต่ละประเภทด้วย

ความเสี่ยงด้านกลยุทธ์

ความเสี่ยงด้านกลยุทธ์เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์ด้าน E-Banking อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย เป้าหมาย กลยุทธ์ โครงสร้างองค์กร สภาพแวดล้อมขององค์กร สภาวะการแข่งขัน และทรัพยากร เช่น บุคลากร ช่องทางการสื่อสาร ระบบการปฏิบัติการ และระบบเครือข่าย ผู้บริหารจะต้องมีความเข้าใจในความเสี่ยงต่างๆที่เกี่ยวข้องกับ E-Banking ก่อนที่จะตัดสินใจดำเนินการใดๆด้าน E-Banking และจัดให้มีเทคโนโลยีและระบบสารสนเทศเพื่อการบริหารที่เพียงพอ นโยบายด้าน E-Banking ควรมีความสอดคล้องกับนโยบายภาพรวมของสถาบันการเงินและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ของสถาบันการเงินนั้น สินค้าและบริการที่เสนอผ่านช่องทางด้าน E-Banking ควรสอดคล้องกับแผนการดำเนินธุรกิจโดยรวมของสถาบันการเงินด้วย นอกจากนี้จะต้องคำนึงถึงการบังคับใช้กฎหมายที่เกี่ยวข้องกับธุรกรรม E-Banking เช่น การบังคับใช้ Two Factor Authentication หรือ การใช้ Digital Signature และ Certificate Authority ในการพิสูจน์ตัวตนของบุคคลที่เข้ามาทำรายการ รวมทั้งการเพิ่มมาตรการในการรักษาความลับของข้อมูลของลูกค้า และการป้องกันการฟอกเงินอีกด้วย เพราะนอกจากสถาบันการเงินจะต้องรับผิดชอบตามกฎหมายแล้ว ยังจะได้รับผลกระทบต่อชื่อเสียงของสถาบันการเงินได้ในที่สุด

ความเสี่ยงด้านเครดิต

E-Banking สามารถทำให้สถาบันการเงินขยายฐานลูกค้าได้อย่างไร้พรมแดน และลูกค้าไม่ต้องทำรายการกับเจ้าหน้าที่ของสถาบันการเงินแบบตัวต่อตัว เป็นการเพิ่มระดับความเสี่ยงด้านเครดิตต่อสถาบันการเงินในแง่ของ

- การพิสูจน์ความสุจริตใจของลูกค้าซึ่งเป็นองค์ประกอบสำคัญในการตัดสินใจอนุมัติสินเชื่อ
- การพิสูจน์หลักประกันของลูกค้าที่อยู่นอกพื้นที่ (out-of-area borrower)

- การบริหาร portfolio สินเชื่อ ซึ่งหากไม่มีการบริหารที่ดีแล้ว อาจเพิ่มโอกาสการเกิดการกระจุกตัวของสินเชื่อได้ง่ายขึ้น

ความเสี่ยงด้านตลาด

ความเสี่ยงด้านตลาด คือ ความเสี่ยงที่เกิดจากความผันผวนของราคา อัตราดอกเบี้ย และอัตราแลกเปลี่ยน E-Banking ทำให้ระดับความเสี่ยงด้านตลาดของสถาบันการเงินสูงขึ้นได้ เนื่องจากรูปแบบการทำรายการกับธนาคารพาณิชย์ของลูกค้าจะเปลี่ยนแปลงไป โดยลูกค้าสามารถเลือกใช้บริการหรือทำรายการกับสถาบันการเงินที่ให้ราคาหรืออัตราที่ดีกว่า ทำให้สถาบันการเงินที่ให้บริการ E-Banking ต้องพยายามปรับราคาหรืออัตราให้เป็นไปตามสถานะของตลาดได้อย่างรวดเร็วทันการณ์ และคิดค้นรูปแบบการให้บริการให้หลากหลายตรงกับความต้องการของลูกค้าที่มีอย่างกว้างขวางขึ้น เพื่อไม่ให้เกิดความเสียเปรียบในเชิงแข่งขันได้ รูปแบบเงินฝาก สินเชื่อที่หลากหลายและมีปริมาณมากขึ้นอาจเป็นการเพิ่มความเสี่ยงทางด้านอัตราดอกเบี้ยให้แก่สถาบันการเงิน และเนื่องจากธนาคารสามารถเข้าถึงลูกค้าได้อย่างไร้พรมแดน โอกาสที่สถาบันการเงินจะมีการทำรายการที่เป็นสกุลเงินตราต่างประเทศก็จะเพิ่มขึ้น ซึ่งนำไปสู่ความเสี่ยงทางด้านอัตราแลกเปลี่ยนที่สูงขึ้นได้

ความเสี่ยงด้านสภาพคล่อง

E-Banking ทำให้สถาบันการเงินมีความเสี่ยงด้านสภาพคล่องสูงขึ้น เนื่องจากการฝากถอน หรือโอนเงินทำได้โดยง่ายและสะดวกสบายขึ้น ทำให้ปริมาณเงินฝากจากลูกค้ามีความผันผวนมากขึ้น หากเกิดวิกฤติการขาดความเชื่อมั่นในสถาบันการเงิน การแห่ถอนเงินก็ทำได้ง่าย สะดวกสบายและรวดเร็วขึ้น นอกจากนี้ถ้าระบบขัดข้องทั้งๆที่มีสภาพคล่องดี แต่ลูกค้าไม่สามารถใช้บริการได้ก็ทำให้ขาดสภาพคล่องได้ ดังนั้น สถาบันการเงินควรมีวิธีการรองรับและจัดการกับสภาพคล่องทั้งในภาวะปกติและวิกฤติการณ์

ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงด้านปฏิบัติการเป็นความเสี่ยงที่เกิดจากความผิดพลาด หรือความไม่เพียงพอของกระบวนการทำงาน พนักงาน ระบบงาน หรือระบบเทคโนโลยีสารสนเทศ และเหตุการณ์หรือปัจจัยภายนอก ซึ่งอาจเป็นช่องทางหรือส่งผลให้เกิดการทุจริต การปฏิบัติงานผิดพลาด และการไม่สามารถส่งมอบสินค้าและบริการให้ลูกค้าได้ ความล้มเหลวในการรักษาสถานภาพเชิงการแข่งขันและความผิดพลาดในการบริหารข้อมูล E-Banking จะทำให้ระดับความเสี่ยงประเภทนี้สูงขึ้นมากถ้าสถาบันการเงินขาดระบบการวางแผน การบริหาร การปฏิบัติงานและการติดตามที่ดีและเพียงพอ การบุกรุกระบบงานหรือระบบเครือข่ายก็เป็นอีกปัจจัยหนึ่งที่เพิ่มความเสี่ยงประเภทนี้ให้กับสถาบันการเงิน ดังนั้น สถาบันการเงินควรมีระบบการควบคุมและติดตามที่มีประสิทธิภาพเพื่อปกป้องระบบงานภายในจากการบุกรุกทั้งภายในและภายนอกองค์กร นอกจากนั้นการมีแผนสำรองเพื่อรองรับ

สถานการณ์ฉุกเฉินต่างๆ เช่น ระบบงานหรือระบบเครือข่ายล้มเหลวจะช่วยลดความเสี่ยงจากการดำเนินงานได้ทางหนึ่ง เพราะจะทำให้สถาบันการเงินสามารถนำเสนอสินค้าและบริการทาง E-Banking ได้อย่างต่อเนื่องและตลอดเวลา ทั้งนี้ในการพัฒนาแผนสำรองดังกล่าวควรคำนึงประเด็นในเรื่องการรักษาความปลอดภัยด้วย มิเช่นนั้นสถาบันการเงินก็จะไม่สามารถปฏิเสธความรับผิดชอบทางกฎหมายต่อลูกค้าหรือบุคคลอื่นที่เข้ามาทำรายการได้เมื่อเกิดการละเมิดกฎหมาย กฎระเบียบ วิธีปฏิบัติ รวมทั้งมาตรฐานจริยธรรมต่างๆ อันจะก่อให้เกิดความเสี่ยงที่สถาบันการเงินจะต้องเสียค่าปรับ หรือค่าเสียหายอื่นๆ ซึ่งจะมีผลกระทบกับชื่อเสียงของสถาบันการเงินได้ในที่สุด

เพราะฉะนั้นเมื่อผู้ตรวจสอบคนใดได้รับมอบหมายให้รับผิดชอบในการพิจารณาและประเมินภาพรวมของความเสี่ยงทางด้าน E-Banking แล้ว ผู้ตรวจสอบคนนั้นก็จะต้องประเมินประเด็นของความเสี่ยงที่จะมีผลกระทบต่อฐานะและการดำเนินงานของสถาบันการเงินก่อน หลังจากนั้นถ้าพบประเด็นที่จะมีผลกระทบต่อฐานะและการดำเนินงานของสถาบันการเงิน ก็ให้รวบรวมประเด็นดังกล่าวให้ผู้ตรวจสอบด้านอื่นติดตามต่อไป นอกจากนั้นผู้ตรวจสอบจะต้องพิจารณาและประเมินความเสี่ยงด้าน IT[2] ซึ่งแบ่งออกได้เป็น 5 ประเภทตามวิธีการประเมินความเสี่ยงของ Federal Reserve System, SR 98-9 IT Risks ทั้งนี้เพราะว่าการดำเนินธุรกรรมด้าน E-Banking เป็นการดำเนินธุรกรรมโดยอาศัยเครือข่ายการสื่อสารด้วยระบบเทคโนโลยีสารสนเทศเป็นหลัก จึงจำเป็นที่จะต้องพิจารณาความเสี่ยงจาก IT ประกอบด้วย

ประเภทของความเสี่ยงด้าน IT ที่สถาบันการเงินประสบอยู่มีองค์ประกอบดังนี้ คือ

- ความเสี่ยงด้านกระบวนการบริหาร (Management Process)
- ความเสี่ยงด้านสถาปัตยกรรมคอมพิวเตอร์ (Architecture)
- ความเสี่ยงด้านระบบการรักษาความปลอดภัย (Security)
- ความเสี่ยงด้านความสมบูรณ์ ถูกต้อง ครบถ้วนและน่าเชื่อถือได้ (Integrity)
- ความเสี่ยงด้านสภาพพร้อมใช้งาน (Availability)

<u>ความเสี่ยงด้านกระบวนการบริหาร</u> (Management Process)

ความเสี่ยงด้านกระบวนการบริหารเป็นความเสี่ยงที่เกิดขึ้นจากการวางแผน การลงทุน การพัฒนาและการใช้เทคโนโลยีสารสนเทศของสถาบันการเงิน และครอบคลุมไปถึงการวางแผนเพื่อรองรับความเสี่ยงทางด้านระบบการรักษาความปลอดภัย (Security) ความสมบูรณ์ ถูกต้อง ครบถ้วนและน่าเชื่อถือได้ (Integrity) และสภาพพร้อมใช้งาน (Availability) ซึ่งมีองค์ประกอบย่อยๆ ดังต่อไปนี้ คือ

[2] Supervisory Program (SR98-9), IT Risks, Federal Reserve System (FRB)

- การบริหารโครงการ (Project Management)

- การพัฒนาระบบงาน&โปรแกรม รวมทั้งการจัดซื้อระบบงาน (SDLC & Acquisition)

- การบำรุงรักษาระบบงานและการบริหารการเปลี่ยนแปลง (System maintenance & Change Control)

- การรับประกันคุณภาพของการให้บริการ (Quality Assurance)

- การบริหารความต่อเนื่องในการให้บริการและการจัดทำแผนฉุกเฉิน (Business Continuity & Contingency Planning)

- การบริหารการใช้บริการจากหน่วยงานภายนอก (Management of Outsourcing)

<u>ความเสี่ยงด้านสถาปัตยกรรมคอมพิวเตอร์</u> (Architecture)

ความเสี่ยงด้านสถาปัตยกรรมคอมพิวเตอร์ เป็นความเสี่ยงที่เกิดขึ้นจากการวางรูปแบบของเทคโนโลยีสารสนเทศและองค์ประกอบอื่นๆ ที่เกี่ยวข้อง คือ

- เครือข่ายการสื่อสารและระบบปฏิบัติการ (Network Telecommunication & Operating Systems)

- ระบบการจัดการและบริหารฐานข้อมูล (Database Management Systems)

- ซอฟท์แวร์ระบบงานสำคัญที่สถาบันการเงินใช้ในการให้บริการ (Business Line Software Application)

นอกจากนี้ยังครอบคลุมถึงสภาพแวดล้อมในการทำงานทั้งด้านกายภาพและตรรกะ และการจัดโครงสร้างของข้อมูลเพื่อช่วยอำนวยความสะดวกในการติดต่อสื่อสารระหว่างระบบงานที่ต่างกัน เพื่อให้เกิดความมั่นใจของระบบการรักษาความปลอดภัย ความสมบูรณ์ ถูกต้อง และน่าเชื่อถือได้ (Integrity) และสภาพพร้อมใช้งาน (Availability)

<u>ความเสี่ยงด้านระบบการรักษาความปลอดภัย</u> (Security)

ความเสี่ยงด้านระบบการรักษาความปลอดภัยเป็นความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูลและทรัพย์สิน รวมทั้งสภาพแวดล้อมในการประมวลผลทั้งด้านกายภาพและตรรกภาพ โดยจัดการป้องกันให้มีความเหมาะสมทั้งคุณค่าและความสำคัญของข้อมูล โดยมีหลักเกณฑ์ในการวัดที่ว่าระบบการรักษาความปลอดภัยที่ดีจะต้องสามารถป้องกันการเข้าถึง การเข้าไปแก้ไขเปลี่ยนแปลง การทำลาย หรือการเปิดเผยข้อมูลหรือทรัพย์สิน ระหว่างที่กำลังสร้าง จัดส่ง ประมวลผล หรือจัดเก็บรักษาข้อมูล

<u>ความเสี่ยงด้านความสมบูรณ์ ถูกต้อง ครบถ้วน และน่าเชื่อถือได้</u> (Integrity)

ความเสี่ยงด้านความสมบูรณ์ ถูกต้อง ครบถ้วน และน่าเชื่อถือได้ เป็นความเสี่ยงที่

เกี่ยวข้องกับการส่งมอบข้อมูลที่มีความสมบูรณ์ ถูกต้อง ครบถ้วน และน่าเชื่อถือได้ ให้กับผู้ที่ต้องการใช้ข้อมูล (End User) ทั้งนี้ การบริหารความเสี่ยงด้านนี้จะมีผลกระทบทั้งกับโครงสร้างของการควบคุมองค์กร และโครงสร้างของสายงานการให้บริการทั้งหมด

ความเสี่ยงด้านสภาพพร้อมใช้งาน (Availability)

ความเสี่ยงด้านสภาพพร้อมใช้งาน เป็นความเสี่ยงในเรื่องของการจัดส่งข้อมูลไปให้ผู้ที่ต้องการใช้ข้อมูล ซึ่งความเสี่ยงนี้ถ้ามีการควบคุมในระดับที่เหมาะสมแล้ว ก็จะต้องสามารถให้ข้อมูลได้อย่างต่อเนื่องในเวลาที่เหมาะสมเพื่อให้สามารถสนับสนุนกระบวนการบริหารธุรกิจและการตัดสินใจ โดยอาศัยข้อมูลทั้งจากแหล่งภายในและจากแหล่งภายนอก พร้อมทั้งจัดให้มีแผนฉุกเฉินในการแก้ไขหรือหาแหล่งประมวลผลทดแทน และการจัดทำสินทรัพย์ประเภทข้อมูลขึ้นมาใหม่ การดำเนินกิจกรรมต่างๆ เพื่อให้สามารถดำเนินงานได้อีกครั้งหนึ่งหลังจากการหยุดชะงักของการให้บริการข้อมูลไปแล้ว

อย่างไรก็ดี ความเสี่ยงด้าน IT ทั้ง 5 ด้าน ดังกล่าวสามารถจัดได้เป็น 2 กลุ่มใหญ่ๆ คือ

- ความเสี่ยงจากกระบวนการบริหารการจัดการ (Management Process)
- ความเสี่ยงจากกระบวนการปฏิบัติงาน (Operational Process)

เนื่องจากความเสี่ยงด้าน IT ทุกด้านก็ประกอบด้วยความเสี่ยงที่เกิดจากการบริหารการจัดการและความเสี่ยงจากการดำเนินงานทั้งสิ้น

1.3 ผลกระทบสำคัญที่เกิดจากความเสี่ยงด้าน E-Banking ของสถาบันการเงิน[3]

เหตุการณ์ / สถานการณ์ ซึ่งมีผลกระทบในด้านลบต่อการหารายได้ หรือ ส่วนของผู้ถือหุ้นของสถาบันการเงิน มีตัวอย่างดังต่อไปนี้ คือ

- สถาบันการเงินไม่ได้รับความเชื่อถือจากลูกค้า
- สถาบันการเงินไม่สามารถส่งมอบบริการให้ลูกค้าได้
- สถาบันการเงินเกิดความผิดพลาดในการปฏิบัติซึ่งไม่เป็นไปตามระเบียบวิธีปฏิบัติทั้งของสถาบันการเงินเองหรือการปฏิบัติตามกฎหมาย
- สถาบันการเงินเกิดความผิดพลาดในระบบข้อมูลเพื่อการจัดการและการบริหาร (MIS)
- สถาบันการเงินไม่สามารถตรวจจับการทุจริตได้
- สถาบันการเงินไม่สามารถดำเนินธุรกิจไปได้ตามปกติ

[3] "Information Technology School" , OCC, IS & E-banking Training, March 27-Apr 3-2001 at BOT

- สถาบันการเงินมีการคำนวณ (ตัวเลขทางการเงิน) ผิดพลาดและมีการดำเนินขั้นตอนการทำงานที่ผิดพลาด

2. แนวทางการบริหารความเสี่ยงด้าน E-Banking

จากการศึกษาพบว่าหลายองค์กรได้จัดทำแนวทางการบริหารความเสี่ยงด้านE-Banking ซึ่งมีกรอบแนวคิดที่คล้ายๆกัน โดยจะครอบคลุมเรื่อง การบริหาร การปฏิบัติงาน การควบคุมและการรักษาความปลอดภัย การบริหารจัดการกับองค์กรภายนอก (Outsourcing Relationship Management) สำหรับคู่มือฉบับนี้ จะนำเสนอแนวทางที่สกส.ได้พัฒนาขึ้น โดยอ้างอิงมาจากแนวทางของ Risk Management Principles for Electronic Banking ของ Basel Committee on Banking Supervision, Bank for International Settlements ฉบับเดือนพฤษภาคม 2001 ซึ่งประกอบด้วยหลักการ 14 ข้อ ที่สถาบันการเงินพึงปฏิบัติสำหรับการดำเนินการด้าน E-Banking ซึ่งมีจุดมุ่งหมายเพื่อเป็นแนวทางให้กับสถาบันการเงินในการบริหารความเสี่ยงต่างๆ ที่เกี่ยวข้องกับการดำเนินงานด้าน E-Banking โดยเฉพาะอย่างยิ่งความเสี่ยง 2 ประเภทหลัก อันได้แก่ ความเสี่ยงเชิงกลยุทธ์ และความเสี่ยงจากการดำเนินงาน นอกจากนี้ยังครอบคลุมถึงความเสี่ยงด้าน IT ที่ได้กล่าวมาแล้ว ทั้งนี้หลักการบริหารความเสี่ยงของ BIS ทั้ง 14 ข้อนี้เป็นเพียงข้อแนะนำโดยกว้างที่พึงปฏิบัติแต่มิใช่ Best Practice เนื่องจาก BIS เชื่อว่าการที่จะกำหนดแนวทางการบริหารความเสี่ยงหรือมาตรฐานทางด้านเทคนิคสำหรับการดำเนินการด้าน E-Banking นั้นจะล้าสมัยได้ง่ายเพราะพัฒนาการทางด้านเทคโนโลยีสารสนเทศและการพัฒนาผลิตภัณฑ์บริการใหม่ๆ ทางด้าน E-Banking เปลี่ยนแปลงไปอย่างรวดเร็ว BIS จึงเห็นควรให้เป็นหน้าที่ของผู้บริหารของสถาบันการเงินเองที่จะต้องเป็นผู้กำหนดนโยบายและขั้นตอนการดำเนินการบริหารและจัดการความเสี่ยงในรายละเอียดให้เหมาะสมกับสถานการณ์ของแต่ละสถาบันต่อไป สำหรับแนวทางการบริหารความเสี่ยงด้าน E-Banking ในคู่มือนี้ได้มีการปรับปรุงเนื้อหาในบางข้อเพื่อให้มีความเหมาะสมและเข้ากับสถานการณ์ของธุรกิจ E-Banking ในระบบสถาบันการเงินของไทย อีกทั้งยังได้แนบส่วนของการบริหารความเสี่ยงด้าน E-Banking ซึ่งเป็นส่วนหนึ่งของเอกสารเรื่อง Internet Banking Comptroller's Handbook ของ OCC ฉบับเดือนตุลาคม 1999 ไว้ในภาคผนวก 3

หลักการบริหารความเสี่ยงทั้ง 14 ข้อ จำแนกเป็น 3 กลุ่ม คือ

(1) การกำกับดูแลด้าน E-Banking ของคณะกรรมการและผู้บริหาร (Board and Management Oversight)

(2) การควบคุมการรักษาความปลอดภัย (Security Controls)

(3) การบริหารความเสี่ยงเกี่ยวกับเรื่องกฎหมายและชื่อเสียง (Legal and Reputation Risk Management)

2.1 การกำกับดูแลด้าน E-Banking ของคณะกรรมการและผู้บริหาร (Board and Management Oversight)

เนื่องจากคณะกรรมการและผู้บริหารระดับสูงมีความรับผิดชอบต่อการพัฒนากลยุทธ์การดำเนินธุรกิจและจัดให้มีการติดตามดูแลความเสี่ยงของฝ่ายบริหารอย่างมีประสิทธิภาพ ฉะนั้นการตัดสินใจเชิงกลยุทธ์เพื่อกำหนดว่าสถาบันการเงินควรดำเนินธุรกิจ E-Banking หรือไม่และอย่างไร จะต้องกระทำด้วยความชัดเจน มีข้อมูลสนับสนุน และเป็นลายลักษณ์อักษร การตัดสินใจเบื้องต้นควรจะรวมถึงการกำหนดผู้รับผิดชอบ นโยบาย และการควบคุมเกี่ยวกับความเสี่ยง รวมทั้งดูเรื่องการค้าข้ามชาติที่กำลังเพิ่มขึ้นด้วย การติดตามของฝ่ายบริหารที่มีประสิทธิภาพควรครอบคลุมถึงการทบทวนและการอนุมัติเกี่ยวกับเรื่องสำคัญ ๆ ของกระบวนการควบคุมรักษาความปลอดภัยของสถาบันการเงิน เช่น การพัฒนา และการบำรุงรักษาโครงสร้างพื้นฐานของการควบคุมรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันระบบ E – Banking และข้อมูลจากการคุกคามทั้งภายในและภายนอก นอกจากนั้น กระบวนการติดตามควรจะครอบคลุมถึงการบริหารความเสี่ยงที่เกิดจากการพึ่งพาความสัมพันธ์กับผู้ให้บริการภายนอก และการพึ่งพาองค์กรภายนอก (third parties) อื่นๆ เพื่อการดำเนินงานที่สำคัญๆ ของ E–Banking

ในเรื่องของการกำกับดูแลด้าน E-Banking ของคณะกรรมการและผู้บริหาร จะแยกเป็น 3 หลักการที่สถาบันการเงินพึงปฏิบัติ โดยมีรายละเอียดดังนี้

<u>หลักการข้อที่ 1</u> คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินควรกำหนดให้มีการบริหาร/ จัดการองค์กรสำหรับการดำเนินงานด้าน E-Banking ที่มีประสิทธิภาพ

(1) ควรดำเนินการจัดทำนโยบาย แผนกลยุทธ์ ด้าน E-Banking มีการทบทวนก่อนนำไปใช้งาน และทำการประเมินความสมเหตุสมผลของนโยบายและแผนฯ อย่างต่อเนื่องเป็นระยะ ๆ หรือในเวลาอันควร

(2) ควรจัดทำนโยบายและแผนงานด้าน E-Banking ให้มีความสอดคล้องกับนโยบายและแผนงานโดยรวมของสถาบันการเงิน

(3) ควรมีการประเมินความเสี่ยงของธุรกรรม E-Banking และ/หรือระบบงานและ/หรือโปรแกรมระบบงานที่พัฒนาขึ้นใหม่ก่อนนำไปใช้ทุกครั้ง

(4) ควรกำหนดความสามารถในการรองรับความเสี่ยงของสถาบันการเงิน (Risk Appetite) ทางด้าน E-Banking

(5) ควรระบุปัจจัยเสี่ยงต่อความปลอดภัย ความถูกต้อง และเสถียรภาพในการให้บริการทาง E-Banking และกำหนดให้บริษัทภายนอกที่สถาบันการเงินว่าจ้าง ให้ดำเนินการในทำนองเดียวกันกับของสถาบันการเงินเอง

(6) ควรจัดให้มีการควบคุมภายในที่มีประสิทธิภาพ

(7) ควรจัดให้มีกระบวนการติดตามของผู้มีอำนาจจัดการที่มีลักษณะยืดหยุ่น (Dynamic) เพียงพอที่จะสามารถเข้าไปแก้ไขปัญหาที่เกิดขึ้นกับระบบงาน E-Banking ได้อย่างทันท่วงที

(8) ควรจัดสายการบังคับบัญชาบุคลากรและการรายงานผลเพื่อรองรับต่อเหตุการณ์ที่จะมีผลกระทบต่อเสถียรภาพความมั่นคงและชื่อเสียงของสถาบันการเงิน

<u>หลักการข้อที่ 2</u> คณะกรรมการและผู้บริหารระดับสูงควรทบทวนและอนุมัติหลักเกณฑ์ (key aspects) สำหรับกระบวนการควบคุมระบบรักษาความปลอดภัยของสถาบันการเงิน

(1) ควรจัดทำและเก็บรักษาข้อมูลของการรักษาความปลอดภัย (Security Profile) ซึ่งเกี่ยวข้องกับการกำหนดสิทธิอำนาจแก่ผู้ใช้ระบบงาน E-Banking ทุกคน ซึ่งต้องสนับสนุนระบบการแบ่งแยกอำนาจหน้าที่อย่างเหมาะสม

(2) ควรจัดให้มีการประเมินจุดแข็งและจุดอ่อนของระบบการรักษาความปลอดภัยโดยผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยอิสระ หรือผู้ตรวจสอบภายใน ก่อนการใช้งานจริง และอย่างน้อยปีละครั้ง

(3) ควรกำหนดขอบเขตของการเข้าถึงหรือเรียกดูข้อมูลในระบบงาน E-Banking ตามความพิเศษและความสำคัญ (Sensitivity and importance) ของข้อมูลและระบบงานนั้น พร้อมกำหนดมาตรการป้องกันไม่ให้เรียกดูข้อมูลสำคัญสำหรับบุคคลที่ไม่ได้มีอำนาจหน้าที่

(4) ควรจัดให้มีการควบคุมทางกายภาพ (physical control) อย่างเพียงพอ เพื่อหลีกเลี่ยงการเข้าถึงระบบงาน server ฐานข้อมูล และโปรแกรมระบบงาน E-Banking จากบุคคลที่ไม่ได้รับอนุญาต

(5) ควรหลีกเลี่ยงการจัดเก็บข้อมูลที่ต้องใช้ความระมัดระวังเป็นพิเศษหรือที่มีความเสี่ยงสูงไว้บน Desktop และ laptop systems และควรใช้เทคนิคที่เหมาะสมสำหรับการปกป้องข้อมูลดังกล่าว

(6) ควรจัดเก็บรายละเอียดของ configuration ของ Application และ System ไว้ในที่ปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต

(7) ควรใช้เครื่องมือที่เหมาะสมในการลดภัยคุกคามจากภายนอกต่อระบบงาน E-Banking เช่น

-ใช้ Software เพื่อตรวจจับ virus ณ จุดที่มีความเสี่ยง

-ใช้ Software เพื่อตรวจจับการบุกรุก กิจกรรมที่น่าสงสัย/ผิดปกติ (Intrusion Detection System)

- ติดตั้ง Firewalls, Packet-filtering firewalls และ Denial of service filters

- พิจารณาแนวทางการแบ่งระดับชั้นของเครือข่าย (Demilitarized Zone หรือ DMZ) ตามความเหมาะสม

(8) ควรกำหนดมาตรการรักษาความปลอดภัยในการแจกจ่ายโปรแกรมต่างๆ ผ่านทางเครือข่าย Internet เพื่อป้องกันการแพร่กระจายของไวรัส

- ไม่ควรแจกจ่าย Access Code ของ Users หรือข้อมูลสำคัญ ผ่านทาง Internet หรือ Web-based distribution system

- ควรให้ความรู้แก่ลูกค้าถึงความเสี่ยงต่างๆที่อาจเกิดขึ้นจากการ download โปรแกรม ผ่านทางเครือข่าย Internet หรือ Web-based distribution system

(9) ควรกำหนดให้นำมาตรการรักษาความปลอดภัยมาใช้อย่างเข้มงวดและบังคับใช้ทั้งกับพนักงานและบุคคลภายนอกทุกรายที่สามารถเข้าถึงระบบงาน E-Banking โดยเท่าเทียมกัน

(10) ควรปรับปรุงมาตรการ เครื่องมือและอุปกรณ์การรักษาความปลอดภัยและการควบคุมให้ทันสมัยอย่างต่อเนื่องเป็นประจำ

(11) ควรติดตามการปรับปรุงแก้ไขโปรแกรม เพื่อทำการ upgrade (รวมถึง Service Patch) ของโปรแกรมที่ใช้งานอยู่เสมอ

<u>หลักการข้อที่ 3</u> คณะกรรมการและผู้บริหารระดับสูงควรกำหนดให้มีการจัดทำ due diligence และกระบวนการติดตามอย่างต่อเนื่องและครอบคลุมทั่วถึง เพื่อการบริหารจัดการ ดูแลความสัมพันธ์ระหว่างสถาบันการเงินกับบริษัทผู้ให้บริการภายนอกและ/หรือองค์กรภายนอกอื่นๆที่สนับสนุนงานด้าน E-Banking ของสถาบันการเงิน (Outsourcing relationship)

(1) ควรจัดให้มีกระบวนการเพื่อช่วยในการตัดสินใจเลือกใช้ระบบงาน E-Bankingที่พัฒนาโดยหน่วยงานภายนอก ให้สัมพันธ์กับแผนกลยุทธ์และแผนการดำเนินธุรกิจ โดยคำนึงถึงความเสี่ยงและจะต้องทำการสื่อสารให้ส่วนงานที่เกี่ยวข้องภายในองค์กรเกิดความเข้าใจถึงผลกระทบจากการใช้บริการของหน่วยงานภายนอกนั้น

(2) ควรทำการประเมินความเสี่ยงและจัดทำ due diligence ก่อนตัดสินใจเลือกใช้บริการของหน่วยงานภายนอก และดำเนินการทบทวนอย่างสม่ำเสมอ

(2.1) กระบวนการตัดสินใจคัดเลือกหน่วยงานภายนอก ควรมีปัจจัยขั้นต่ำที่ใช้ในการพิจารณา ดังนี้

- ขอบเขตหรือระดับการให้บริการ
- การวิเคราะห์ความเสี่ยงทางการเงิน
- ชื่อเสียง

- นโยบายการบริหารความเสี่ยง การควบคุมความเสี่ยง
- ความสามารถในการปฏิบัติตามข้อตกลง/สัญญา/ข้อบังคับ
- ระบบรักษาความปลอดภัย ทั้งด้านการป้องกัน (Preventive) ตรวจติดตาม (Detective) และ การแก้ไขปัญหา (Corrective)
- แผนสำรองฉุกเฉิน

(2.2) กระบวนการทบทวนหลังการว่าจ้าง ควรพิจารณาดำเนินการ ดังนี้

- ควรจัดให้มีบุคคลหรือทีมงานรับผิดชอบในการติดตามดูแลการให้บริการ E-Banking ของหน่วยงานภายนอก
- ควรทบทวนและจัดทำ due diligence เพื่อประเมินประสิทธิภาพและความสามารถของผู้ให้บริการในการปฏิบัติตามสัญญาว่าจ้าง พร้อมทั้งจัดทำ exit strategy เพื่อรองรับความเสี่ยงในการที่จะต้องยกเลิกสัญญาว่าจ้างการให้บริการกับหน่วยงานภายนอก

(3) ควรกำหนดเงื่อนไขขั้นต่ำในสัญญาว่าจ้างหน่วยงานภายนอกให้ชัดเจน ดังนี้

- ขอบเขตของการให้บริการ
- ข้อผูกพันตามสัญญาและความรับผิดชอบของทุกฝ่าย รวมถึงการทำสัญญาว่าจ้างบริษัทอื่นอีกทอดหนึ่งในลักษณะของ subcontracting
- ความรับผิดชอบในการจัดหาและขอรับข้อมูลจากบริษัทผู้ให้บริการ
- ข้อกำหนดเกี่ยวกับการคุ้มครองประกันภัย สิทธิความเป็นเจ้าของข้อมูลใน server หรือฐานข้อมูลของบริษัทผู้ให้บริการ และสิทธิของสถาบันการเงินในการเรียกข้อมูลกลับคืนเมื่อสัญญาหมดอายุหรือถูกยกเลิก
- แนวทางการดำเนินงานภายใต้สถานการณ์ปกติและสภาวะฉุกเฉิน
- การค้ำประกัน การชดใช้ความเสียหายที่เหมาะสมหากบริษัทผู้ให้บริการไม่สามารถปฏิบัติตามสัญญา
- วิธีการเข้าแทรกแซงและแก้ไขสถานการณ์ที่ทันการณ์และมีลำดับขั้นตอนที่เหมาะสม ในกรณีที่บริษัทผู้ให้บริการ (service provider) ปฏิบัติงานได้ต่ำกว่ามาตรฐานที่ระบุในสัญญา
- ในการว่าจ้างบริษัทผู้ให้บริการภายนอกซึ่งอยู่ต่างประเทศ จะต้องพิจารณาในเรื่องที่เกี่ยวกับการบังคับใช้กฎหมาย รวมทั้งนโยบายการคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองผู้บริโภค
- การเข้าตรวจสอบของสถาบันการเงิน ธนาคารแห่งประเทศไทย และผู้ตรวจสอบหรือผู้ประเมินจากภายนอก

(4) ควรจัดให้มีการตรวจสอบการดำเนินงานในส่วน Outsource โดยผู้ตรวจสอบภายในและภายนอกเป็นประจำและจะต้องมีความเป็นอิสระ โดยใช้ขอบเขตและมาตรฐานในการตรวจสอบขั้นต่ำเท่ากับที่สถาบันการเงินเป็นผู้ดำเนินการเอง (in-house operation) แต่ในกรณีที่เป็นระบบงานสำคัญและมีความซับซ้อนทางเทคโนโลยี สถาบันการเงินจะต้องจัดให้มีการตรวจสอบผลการดำเนินงานและการรักษาความปลอดภัยของหน่วยงานภายนอกดังกล่าวโดยผู้เชี่ยวชาญทางด้านเทคโนโลยี (บุคคลที่ 3) เป็นประจำ

(5) ควรปรับปรุงแผนสำรองฉุกเฉินทางด้าน E-Banking ให้ครอบคลุมถึงการดำเนินงานโดยหน่วยงานภายนอก

(6) ควรกำหนดลักษณะของการดำเนินงาน ความรับผิดชอบ และพันธะผูกพันของสถาบันการเงินเองให้ชัดเจน ในกรณีที่สถาบันการเงินเป็นผู้ดำเนินการให้บริการ E-Banking แก่หน่วยงานภายนอก

2.2 การควบคุมการรักษาความปลอดภัย (Security Controls)

คณะกรรมการจัดการมีความรับผิดชอบในการทำให้มั่นใจว่ากระบวนการควบคุมการรักษาความปลอดภัยของธุรกรรม E – Banking มีความเหมาะสม สาระสำคัญของกระบวนการต่างๆ นี้ต้องการความสนใจของฝ่ายจัดการเป็นพิเศษ เพราะว่าความท้าทายของการรักษาความปลอดภัยที่มีเพิ่มขึ้น ได้แก่การกำหนดสิทธิของผู้ได้รับมอบอำนาจ/ได้รับอนุญาตอย่างเหมาะสม การควบคุมทางกายภาพและทางตรรกภาพ (Physical and Logical) การรักษาความปลอดภัยที่เพียงพอที่จะรักษาเขตแดนและการจำกัดวงของกิจกรรมของผู้ใช้งานทั้งจากภายในและภายนอกอย่างเหมาะสม และความถูกต้องของข้อมูลในการทำรายการ เช่น การบันทึก และข้อมูลข่าวสารต่างๆ และควรจะมีความมั่นใจว่าร่องรอยการทำรายการที่มีอยู่สำหรับการใช้ติดตามและตรวจสอบในภายหลัง สามารถปกป้องความน่าเชื่อถือของธุรกรรม E – Banking ได้

แม้ว่าการปกป้องลูกค้า และนโยบายคุ้มครองข้อมูลส่วนบุคคล จะผันแปรไปในแต่ละประเทศที่ใช้กรอบกฎหมายที่แตกต่างกัน แต่โดยทั่วไปแล้ว สถาบันการเงินจะต้องกำหนดความรับผิดชอบอย่างชัดเจนที่จะทำให้ลูกค้ามีความสบายใจในเรื่องการเปิดเผยข้อมูล การปกป้องข้อมูลของลูกค้า และความมีเสถียรภาพในการใช้งาน ซึ่งไม่ควรต่ำกว่าระดับที่ลูกค้าคาดหวังจากการใช้บริการด้วยช่องทางการให้บริการแบบดั้งเดิมของสถาบันการเงิน เพื่อที่จะลดความเสี่ยงทางด้านกฎหมาย และความเสี่ยงต่อชื่อเสียงของสถาบันการเงิน ที่อาจเกิดจากการทำธุรกรรม E – Banking ทั้งในประเทศและจากต่างประเทศ สถาบันการเงินควรจะเปิดเผยข้อมูลข่าวสารที่พอเพียงบน Web Site ของตนเอง และดำเนินมาตรการที่เหมาะสมเพื่อให้มั่นใจว่ามีการปฏิบัติตามข้อกำหนดในเรื่องความคุ้มครองข้อมูล

ส่วนบุคคลของลูกค้าที่บังคับใช้ภายใต้กรอบของกฎหมายของประเทศที่มีการนำเสนอบริการ E – Banking ของสถาบันการเงินนั้นๆ

ในเรื่องของการควบคุมการรักษาความปลอดภัย จะแยกเป็น 7 หลักการที่สถาบันการเงินพึงปฏิบัติ โดยมีรายละเอียดดังนี้

<u>หลักการข้อที่ 4</u> สถาบันการเงินควรจัดให้มีมาตรการที่เหมาะสมในการพิสูจน์ตัวตน (Authentication) เพื่อให้สามารถแยกแยะตัวบุคคลและสิทธิของลูกค้าที่เข้ามาทำธุรกรรมบนเครือข่าย internet ได้

(1) ควรมีนโยบายและขั้นตอนการดำเนินงานอย่างเป็นลายลักษณ์อักษรในการเลือกใช้วิธีการพิสูจน์ตัวตนให้เหมาะสมกับลักษณะ ปริมาณ และความเสี่ยงของธุรกรรมที่เกิดขึ้นและความสำคัญของข้อมูลที่จัดเก็บอยู่ ทั้งนี้ สถาบันการเงินอาจเลือกใช้วิธีการหรือเครื่องมือที่เป็นที่ยอมรับโดยทั่วไป เช่น PINs, password, smartcards, security tokens, biometric และใบรับรองอิเล็กทรอนิกส์ (digital certificate) วิธีใดวิธีหนึ่ง หรือใช้หลายวิธีร่วมกันก็ได้

(2) ควรมีมาตรการที่เหมาะสมเพื่อควบคุมการเชื่อมต่อเข้าสู่ระบบงาน E-Banking ให้สามารถป้องกันการแอบอ้างใช้สิทธิเข้าถึงระบบ โดยอาศัยกลไกในการรักษาความปลอดภัย (security mechanisms) ที่ได้รับการยอมรับโดยทั่วไป

(3) ควรทำการพิสูจน์ความถูกต้องของบุคคลที่เข้ามาในระบบงานตั้งแต่ช่วงเริ่มเข้าใช้ระบบงาน (Account origination) ทุกครั้ง ซึ่งเครื่องมือและกระบวนการที่ใช้ในการระบุตัวตนบุคคลจะต้องสามารถป้องกันการเปลี่ยนแปลงใดๆในระบบฐานข้อมูลที่ใช้ในการพิสูจน์ตัวตน (Authentication database) โดยไม่ได้รับอนุญาตได้

(4) ควรจัดให้ระบบ Authentication สามารถพิสูจน์ความถูกต้องของบุคคลที่เข้ามาทำรายการอย่างต่อเนื่องตั้งแต่เริ่มต้นจนออกจากระบบงาน และเมื่อเกิดกรณีที่การเชื่อมต่อหยุดชะงักหรือขาดหายไป ระบบจะต้องจัดให้มีการพิสูจน์ความถูกต้องของบุคคลที่เข้ามาใหม่ทุกครั้ง

(5) ควรป้องกันฐานข้อมูลที่ใช้สำหรับการตรวจสอบสิทธิการเข้าใช้งานในระบบ E-Banking ให้ปลอดภัยจากการถูกเข้าไปแก้ไขดัดแปลงหรือข้อมูลไม่มีความถูกต้องหลังจากการใช้งาน ควรมีระบบตรวจสอบและเก็บร่องรอยความผิดพลาดที่อาจเกิดขึ้น

<u>หลักการข้อที่ 5</u> สถาบันการเงินควรเลือกใช้วิธีการพิสูจน์ความถูกต้องของรายการธุรกรรม (Transaction authentication) เพื่อป้องกันการปฏิเสธความรับผิดชอบ (non-repudiation) และทำให้รายการธุรกรรมนั้นมีความถูกต้องและเชื่อถือได้

(1) ควรออกแบบระบบงาน E-Banking ให้มีความรัดกุม เพื่อป้องกันความเสี่ยงจากการที่ลูกค้าทำรายการโดยพลั้งเผลอ/ไม่ได้ตั้งใจ

(2) ควรเลือกใช้วิธีการระบุตัวตนบุคคลที่สามารถป้องกันการปฏิเสธความรับผิดชอบของบุคคลที่เข้ามาทำรายการผ่านระบบงาน E-Banking ได้

(3) เครื่องมือที่ใช้ป้องกันการปฏิเสธความรับผิดชอบ ควรเป็นไปตามมาตรฐานซึ่งเป็นที่ยอมรับโดยทั่วไป และควรที่จะสามารถตรวจจับการเปลี่ยนแปลงใดๆในข้อมูลธุรกรรมทางการเงินที่เกิดขึ้นได้

<u>หลักการข้อที่ 6</u> สถาบันการเงินควรจัดให้มีมาตรการควบคุมภายในที่ดีสำหรับการปฏิบัติงานกับระบบงาน ฐานข้อมูลและโปรแกรมระบบงานด้าน E-Banking

(1) ควรมีการแบ่งแยกหน้าที่ความรับผิดชอบเพื่อไม่ให้บุคคลใดบุคคลหนึ่ง (ไม่ว่าจะเป็นพนักงานของสถาบันการเงินหรือบุคลากรจากหน่วยงานภายนอกองค์กร) สามารถทำรายการธุรกรรมที่มีความสำคัญตั้งแต่เริ่มต้นจนเสร็จสิ้นกระบวนการ

(2) ควรแบ่งแยกหน้าที่ระหว่างกลุ่มผู้พัฒนาระบบงาน ผู้ปฏิบัติงาน และผู้ตรวจสอบให้ชัดเจน

(3) ควรมีการทบทวนการแบ่งแยกหน้าที่ดังกล่าวอย่างสม่ำเสมอ

(4) ควรจัดให้มีการหมุนเวียนสลับเปลี่ยนหน้าที่และการฝึกอบรมพนักงานเป็นประจำ

(5) สำหรับขั้นตอนการดำเนินงานที่ต้องการความระมัดระวังเป็นพิเศษ ควรจัดให้มีบุคลากรเข้าไปร่วมทำงานนั้นมากกว่า 1 คน

<u>หลักการข้อที่ 7</u> สถาบันการเงินควรดำเนินการควบคุมเกี่ยวกับการอนุญาต และการให้สิทธิในการเข้าถึงระบบงาน และระบบฐานข้อมูล อย่างเหมาะสม (authorization control)

(1) ควรพิจารณาอนุญาตและให้สิทธิในการเข้าถึงระบบงานแก่ผู้ใช้งานตามหน้าที่ความรับผิดชอบและความเกี่ยวข้องกับงาน โดยให้เป็นอิสระต่อสายอำนาจการบังคับบัญชาตามปกติ

(2) ไม่ควรให้สิทธิอำนาจบุคคลหนึ่งบุคคลใดสามารถเข้าถึงได้ทุกระบบงาน ระบบฐานข้อมูล หรืออุปกรณ์ที่เกี่ยวข้องกับระบบงาน E-Banking ไม่ว่าบุคคลนั้นจะเป็นผู้บริหารระดับสูง หรือผู้ถือหุ้นของสถาบันการเงินนั้นก็ตาม

(3) ควรสร้างระบบงาน E-Banking ที่สามารถปฏิบัติงานสัมพันธ์กับระบบฐานข้อมูลในการให้สิทธิ (authorization database)

(4) ผู้ใช้ระบบงาน (ระดับ User) จะต้องไม่สามารถดำเนินการเปลี่ยนแปลงแก้ไขอำนาจและสิทธิในการเข้าถึงระบบฐานข้อมูลที่เกี่ยวกับการให้สิทธิด้วยตนเอง

(5) การเปลี่ยนแปลงใดๆเกี่ยวกับระบบงาน และระบบฐานข้อมูล ต้องได้รับอนุญาตจากผู้มีอำนาจ และควรจัดให้มีการบันทึกร่องรอยการทำธุรกรรมเพื่อการตรวจสอบ (audit trail) ได้อย่างทันเวลาและเหมาะสม

(6) ฐานข้อมูลที่ใช้ในการให้สิทธิ จะต้องได้รับการปกป้องจากการรบกวนซึ่งอาจจะทำให้เกิดการทำงานที่ผิดพลาดหรือเสียหายจนหยุดชะงักไปได้ และควรจัดให้มีกระบวนการติดตามอย่างต่อเนื่อง รวมทั้งบันทึกร่องรอยการทำธุรกรรมเพื่อการตรวจสอบจะต้องสามารถแสดงให้เห็นถึงรายละเอียดของการที่ฐานข้อมูลถูกรบกวนได้

(7) ควรระงับการใช้ฐานข้อมูลเกี่ยวกับการให้สิทธิที่ประสบภัยจากการถูกคุกคาม/บุกรุกจนกว่าจะมีการแก้ไขให้ฐานข้อมูลนั้นมีความถูกต้องเสียก่อน

(8) ควรป้องกันการเปลี่ยนแปลงระดับการให้สิทธิ (Authorization level) ในช่วงที่มีการทำธุรกรรม และการเปลี่ยนแปลงการให้สิทธิใดๆจะต้องถูกบันทึกลงในทะเบียนทางคอมพิวเตอร์ (log) และจัดทำรายงานให้ระดับบริหารรับทราบ

<u>หลักการข้อที่ 8</u> สถาบันการเงินควรดำเนินมาตรการที่จะรักษาความถูกต้องครบถ้วนของข้อมูลที่เกี่ยวกับการทำธุรกรรมและข้อมูลอื่นๆที่เกี่ยวข้อง (Data Integrity)

(1) ระบบงานควรมีความสามารถในการป้องกันการรบกวนหรือเข้ามาเปลี่ยนแปลงแก้ไขข้อมูลการทำธุรกรรมตั้งแต่ช่วงเริ่มต้นจนจบขั้นตอนการทำธุรกรรม

(2) การจัดเก็บ การเข้าถึงและการเปลี่ยนแปลงข้อมูลเกี่ยวกับ E-Banking ควรที่จะมีความรัดกุมและสามารถป้องกันภัยจากการรบกวนหรือเปลี่ยนแปลงแก้ไขได้

(3) ควรออกแบบกระบวนการทำธุรกรรม E-Banking และการจัดเก็บข้อมูล ให้สามารถตรวจจับการเปลี่ยนแปลงใดๆที่ไม่ได้รับอนุญาตได้

(4) ควรกำหนดนโยบายควบคุมการเปลี่ยนแปลง (Change Control Policy) ซึ่งหมายรวมถึง ขั้นตอนการติดตามและดำเนินการทดสอบอย่างเพียงพอ

(5) ควรสามารถตรวจจับการรบกวนต่างๆที่เกิดขึ้นกับธุรกรรมและข้อมูล ในกระบวนการประมวลผลรายการธุรกรรม กระบวนการติดตามการทำธุรกรรมและกระบวนการจัดเก็บข้อมูล

<u>หลักการข้อที่ 9</u> สถาบันการเงินควรจัดให้มีบันทึกร่องรอยการทำรายการ เพื่อการตรวจสอบที่ชัดเจน (Audit Trails)

(1) ควรจัดให้มีทะเบียนรายละเอียดการเข้าทำธุรกรรม (log) อย่างชัดเจนและเพียงพอ เพื่อนำไปใช้ในการติดตาม ตรวจสอบ และแก้ไขปัญหาข้อขัดแย้งต่างๆได้

(2) ควรออกแบบและติดตั้งระบบงาน E-Banking เพื่อให้สามารถเก็บรวบรวมหลักฐานที่จะนำมาใช้ในการดำเนินคดีทางกฎหมาย และจัดเก็บหลักฐานให้ปลอดภัยจากการรบกวนและการปลอมแปลงเอกสาร

(3) ในกรณีที่การประมวลผลและการจัดทำบันทึกร่องรอยเพื่อการตรวจสอบดำเนินการโดยหน่วยงานภายนอก สถาบันการเงินจะต้องสามารถเข้าถึงบันทึกร่องรอยเพื่อการตรวจสอบที่เกี่ยวข้องทั้งหมด รวมทั้งการจัดทำและเก็บบันทึกร่องรอยฯ โดยหน่วยงานภายนอกนั้นจะต้องเป็นไปตามมาตรฐานที่กำหนดโดยสถาบันการเงิน

<u>หลักการข้อที่ 10</u> สถาบันการเงินควรดำเนินมาตรการที่เหมาะสมในการรักษาความลับของข้อมูลสำคัญด้าน E-Banking และมาตรการที่ใช้ควรมีความสอดคล้องกับความอ่อนไหว (sensitivity) ของข้อมูลที่ถูกส่งและจัดเก็บในฐานข้อมูล

(1) ควรจัดให้ระบบป้องกันผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลลับของสถาบันการเงิน

(2) ควรป้องกันการเรียกดู/ใช้ หรือเปลี่ยนแปลงแก้ไขในระหว่างที่ส่งข้อมูลผ่านเครือข่ายจากผู้ไม่ได้รับอนุญาต

(3) ควรกำหนดมาตรฐานและการควบคุมการใช้ข้อมูลโดยให้ครอบคลุมถึงหน่วยงานภายนอกที่ให้บริการ (Outsource)

(4) ควรจัดทำทะเบียนบันทึกทางคอมพิวเตอร์ (log) สำหรับข้อมูลที่ถูกจัดลำดับชั้นให้เป็นข้อมูลหวงห้าม เพื่อให้เกิดความมั่นใจว่าทะเบียนดังกล่าวสามารถป้องกันการรบกวนและเปลี่ยนแปลงแก้ไขได้

(5) ควรเลือกใช้เทคนิคการเข้ารหัสข้อมูลที่ได้มาตรฐานเป็นที่ยอมรับโดยทั่วไปและสามารถสนับสนุนมาตรการในการรักษาความลับของข้อมูล

2.3 การบริหารความเสี่ยงเกี่ยวกับเรื่องกฎหมายและชื่อเสียง (Legal and Reputational Risk Management)

เพื่อปกป้องธนาคารต่อความเสี่ยงทางธุรกิจ เช่น ความเสี่ยงทางด้านกฎหมายและชื่อเสียง การให้บริการ E – Banking ต้องดำเนินไปด้วยความถูกต้องและตรงเวลา สอดคล้องกับความคาดหวังของลูกค้าที่มีอยู่สูงต่อความรวดเร็วและสม่ำเสมอของบริการ และช่วงเวลาที่มีการทำรายการจำนวนมาก ธนาคารต้องมีความสามารถที่จะให้บริการ E – Banking แก่ผู้ใช้บริการทุกคน และสามารถรักษาการให้บริการเช่นนั้นได้ในทุกสถานการณ์ เครื่องมือที่มีประสิทธิภาพในการทำงานมีความสำคัญมากในการช่วยลดความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงที่สถาบันการเงินอาจถูกฟ้องร้องได้ และความเสี่ยงต่อการเสื่อมเสียชื่อเสียงให้น้อยลง ความเสี่ยงที่กล่าวอาจสืบเนื่องจากเหตุการณ์ที่คาดไม่ถึง

เช่น การคุกคามจากภายในและภายนอก ซึ่งอาจจะกระทบกับการจัดให้มีระบบการให้บริการ E – Banking ในการที่จะทำให้ลูกค้าได้รับสิ่งที่คาดหวังไว้ ธนาคารควรมีการจัดทำแผนรองรับปริมาณธุรกรรม แผนการดำเนินธุรกิจอย่างต่อเนื่อง และแผนสำรองฉุกเฉินที่มีประสิทธิผล ธนาคารควรพัฒนาแผนงานเพื่อรองรับเหตุการณ์ต่างๆ (incident response plan) ซึ่งรวมกลยุทธ์ทางด้านการสื่อสาร ทั้งนี้เพื่อให้มั่นใจว่าสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง สามารถควบคุมความเสี่ยงต่อชื่อเสียงของสถาบันการเงิน และจำกัดความเสียหายอันเนื่องมาจากเกิดการขัดข้องในการให้บริการ E – Banking ทำให้ไม่สามารถทำงานได้ตามปกติ

ในเรื่องของการบริหารความเสี่ยงเกี่ยวกับเรื่องกฎหมายและชื่อเสียง จะแยกเป็น 4 หลักการที่สถาบันการเงินพึงปฏิบัติ โดยมีรายละเอียดดังนี้

<u>หลักการข้อที่ 11</u> สถาบันการเงินควรเปิดเผยข้อมูลอย่างเพียงพอบน Website ของตนเอง เพื่อให้ลูกค้าทราบว่าเป็นWebsite ของสถาบันการเงินที่แท้จริงและมีสถานภาพทางกฎหมายที่ถูกต้อง ก่อนที่ลูกค้าจะดำเนินการทำธุรกรรมกับสถาบันการเงิน

(1) ควรมีการให้ข้อมูลที่ชัดเจนและเข้าใจได้ง่ายเกี่ยวกับความเสี่ยง ประโยชน์ของการใช้บริการ สิทธิ พันธะผูกพัน และความรับผิดชอบระหว่างลูกค้ากับสถาบันการเงิน ก่อนที่ลูกค้าจะสมัครใช้บริการ

(2) ควรแสดงข้อมูลขั้นต่ำของสถาบันการเงินบน Website ดังนี้

- ชื่อของสถาบันการเงิน สถานที่ตั้งของสำนักงานใหญ่ (รวมสำนักงานท้องถิ่นด้วย ถ้ามี)
- ชื่อหน่วยงานของสถาบันการเงินที่รับผิดชอบดูแลการให้บริการ E-Banking
- วิธีที่ลูกค้าจะสามารถติดต่อกับศูนย์บริการลูกค้า หากเกิดปัญหาเกี่ยวกับบริการ
- ขั้นตอนในการร้องเรียน รวมทั้งเวลาที่คาดว่าจะใช้ในสรุปข้อร้องเรียนนั้น
- นโยบายรักษาความปลอดภัยของสถาบันการเงินและคำแนะนำในการรักษาความปลอดภัยที่ลูกค้าพึงปฏิบัติ
- ข้อมูลอื่นตามสมควร หรือตามที่กฎหมายกำหนด

<u>หลักการข้อที่ 12</u> สถาบันการเงินควรดำเนินมาตรการที่เหมาะสม เพื่อให้ลูกค้ามั่นใจว่าได้ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Customer privacy) ที่กำหนดภายใต้กรอบของกฎหมายที่เกี่ยวข้อง

(1) ควรกำหนดนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายของประเทศที่สถาบันการเงินให้บริการ E-Banking

(2) ควรเลือกใช้เทคนิคการเข้ารหัสหรือการควบคุมการรักษาความปลอดภัย (security controls) ซึ่งเป็นที่ยอมรับโดยทั่วไป และสามารถสนับสนุนการคุ้มครองข้อมูลส่วนบุคคล

(3) ควรกำหนดให้หน่วยงานภายนอกที่ให้บริการ E-Banking ดำเนินนโยบายเกี่ยวกับในการรักษาความลับและคุ้มครองข้อมูลส่วนบุคคลสอดคล้องไปในทิศทางเดียวกันกับนโยบายของสถาบันการเงิน

(4) ควรแจ้งให้ลูกค้าทราบถึงข้อมูลขั้นต่ำเกี่ยวกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า ดังนี้

(4.1) นโยบายการคุ้มครองข้อมูลส่วนบุคคลบน Website โดยใช้ภาษาที่กระชับ ชัดเจน และเข้าใจง่าย

(4.2) คำแนะนำในการสร้างและเก็บรักษา User ID และรหัสผ่านของลูกค้า อย่างปลอดภัย เช่น

- ควรมีความยาวอย่างน้อย 6 หลัก
- ไม่ควรมีอักขระเดียวกันซ้ำมากกว่า 2 ครั้ง
- ไม่ควรนำ user-id เบอร์โทรศัพท์ วันเกิด หรือข้อมูลส่วนบุคคลของอื่นมาใช้
- ไม่ควรจดไว้ หรือบอกให้ผู้อื่นรู้

(4.3) คำแนะนำให้ลูกค้าปรับรุ่นของ Browsers และ Application Software ให้ทันกับการเปลี่ยนแปลงทางเทคโนโลยี

(4.4) ความรู้เกี่ยวกับการรักษาความปลอดภัยทั่วไปในการใช้เครื่องคอมพิวเตอร์และการเชื่อมโยงเข้าเครือข่าย

(5) ควรแจ้งให้ลูกค้าทราบว่าสถาบันการเงินจะไม่เปิดเผยข้อมูลนอกเหนือจากที่ได้รับอนุญาตจากลูกค้า

<u>หลักการข้อที่ 13</u> สถาบันการเงินควรจัดทำแผนสำรองฉุกเฉินและขั้นตอนการดำเนินงานที่สามารถรองรับการทำธุรกรรมได้อย่างมีประสิทธิภาพและต่อเนื่อง เพื่อให้เกิดเสถียรภาพในการให้บริการ

(1) ควรประเมินความสามารถในการให้บริการด้าน E-Banking ในปัจจุบันและอนาคต และจัดเตรียมช่องทางเพื่อให้สามารถรองรับการให้บริการได้อย่างต่อเนื่อง

(2) ควรทดสอบความสามารถของระบบในการรองรับปริมาณธุรกรรมเป็นประจำ

(3) ควรจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องและแผนสำรองฉุกเฉินสำหรับระบบงาน E-Banking และให้มีการทดสอบแผนอย่างสม่ำเสมอ

(4) ควรกำหนดแผนฉุกเฉิน ให้ครอบคลุมด้าน E-Banking เพิ่มเติมจากแผนฉุกเฉินที่มีอยู่แล้ว โดยประกอบด้วยเรื่องต่อไปนี้เป็นอย่างน้อย

- แนวทางแก้ไขรองรับเหตุฉุกเฉินต่างๆที่อาจเกิดขึ้น
- ขั้นตอนการปฏิบัติงานรองรับสถานการณ์ฉุกเฉิน
- รายชื่อเจ้าหน้าที่ที่รับผิดชอบ และผู้เกี่ยวข้องทั้งหมด รวมทั้งช่องทางการติดต่อสื่อสารกับบุคคลเหล่านั้น

(5) ในกรณีที่สถาบันการเงินใช้บริการจากหน่วยงานภายนอก จะต้องจัดให้มีช่องทางสำรองเพื่อรองรับหากผู้ให้บริการเดิมไม่สามารถให้บริการได้

<u>หลักการข้อที่ 14</u> สถาบันการเงินควรจัดให้มีแผนรองรับเหตุการณ์ที่ไม่คาดคิด (incident response plan) ซึ่งอาจส่งผลให้ความสามารถของระบบงานและการให้บริการ E-Banking เสื่อมถอยลง

(1) ควรจัดทำแผนรองรับเหตุการณ์ที่ไม่คาดคิดให้ครอบคลุมความเสี่ยงต่างๆที่อาจเกิดขึ้น โดยวิเคราะห์ผลกระทบต่อสถาบันการเงิน และจัดทำแผนให้ครอบคลุมถึงการดำเนินการในส่วนที่ว่าจ้างหน่วยงานภายนอก (outsource)

(2) ควรพัฒนาเครื่องมือช่วยในการระบุเหตุการณ์ที่ไม่คาดคิดได้อย่างทันเหตุการณ์ และสามารถประเมินความรุนแรงและควบคุมความเสี่ยงต่อชื่อเสียงจากการหยุดชะงัก/ขัดข้องของการให้บริการ

(3) ควรมีขั้นตอนในการขออนุญาตจากธปท. หากระบบรักษาความปลอดภัยได้รับความเสียหายรุนแรง หรือเกิดเหตุการณ์ที่ทำให้ระบบงานขัดข้อง หยุดทำการนานกว่า 1 วันทำการ ทั้งนี้เพื่อเป็นการถือปฏิบัติตามหนังสือที่ สนส.26/2551ลงวันที่ 3 สิงหาคม 2551 เรื่อง การอนุญาตให้ธนาคารพาณิชย์ให้บริการการเงินทางอิเล็กทรอนิกส์

(4) ควรจัดตั้งหน่วยงานซึ่งมีอำนาจหน้าที่ในการที่จะเข้าไปดำเนินการแก้ไขปัญหาที่เกิดจากเหตุการณ์ที่ไม่คาดคิด และควรได้รับการฝึกอบรมอย่างเพียงพอเพื่อที่จะสามารถวิเคราะห์ระบบตรวจจับและโต้ตอบกับเหตุการณ์ต่างๆ รวมทั้งสามารถประเมินความมีนัยสำคัญของผลลัพธ์ที่ตามมาได้

(5) ควรมีการมอบหมายบุคลากรที่ต้องรับผิดชอบอย่างชัดเจนสำหรับการดำเนินการภายในและการดำเนินการโดยหน่วยงานภายนอก เพื่อให้สามารถดำเนินการต่อเหตุการณ์

ต่างๆ ได้อย่างทันท่วงทีและมีความเหมาะสม นอกจากนั้นควรมีการกำหนดขั้นตอนการสื่อสารภายในและการรายงานขึ้นตรงต่อระดับบนและแจ้งให้คณะกรรมการทราบตามความเหมาะสม

(6) ควรจัดให้มีกระบวนการแจ้งให้บุคคลภายนอก เช่น ลูกค้า องค์กรที่เกี่ยวข้องและสื่อต่างๆ ทราบถึงสาเหตุที่ขัดข้องและแนวทางในการแก้ไขและฟื้นฟูธุรกิจได้อย่างทันท่วงที

(7) ควรจัดเตรียมแผนกลยุทธ์ในการแจ้งข่าวสารที่ฉับพลันต่อบุคคลภายนอกและสื่อต่างๆ ในช่วงสถานการณ์

(8) ควรจัดให้มีกระบวนการในการรวบรวมและเก็บรักษาหลักฐานที่จำเป็นต้องใช้ในการดำเนินคดีตามกฎหมาย

ส่วนที่ 3 การตรวจสอบด้าน E-Banking

1. วัตถุประสงค์และขอบเขตของการตรวจสอบ

คู่มือการตรวจสอบด้าน E-Banking ฉบับนี้ จัดทำขึ้นเพื่อใช้สำหรับปฏิบัติงานตรวจสอบการให้บริการ Internet Banking ของสถาบันการเงินเท่านั้น อย่างไรก็ดีแนวทางการตรวจสอบที่จะกล่าวถึงในบทนี้สามารถนำไปประยุกต์ใช้กับบริการทางการเงินผ่านเครือข่ายอิเล็กทรอนิกส์ชนิดอื่นได้ด้วยเช่นกัน โดยรายละเอียดการตรวจสอบบางประเด็น อาจจะต้องพิจารณาปรับเปลี่ยนหรือเพิ่มเติมให้เหมาะสมกับลักษณะของเครือข่ายอิเล็กทรอนิกส์ชนิดนั้นๆ

การตรวจสอบด้าน Internet Banking มีวัตถุประสงค์เพื่อประเมินความเสี่ยงของสถาบันการเงินในการประกอบธุรกิจ Internet Banking ที่อาจมีผลกระทบต่อฐานะและความสามารถในการดำเนินงานของสถาบันการเงิน รวมทั้งให้ข้อเสนอแนะในการแก้ไขปัญหาหรือลดความเสี่ยงในการประกอบธุรกิจ Internet Banking ก่อนที่จะเกิดความเสียหายแก่สถาบันการเงินเป็นสำคัญ

2. การประเมินความเสี่ยงทางด้าน E-Banking

ผู้ตรวจสอบจะสามารถพิจารณาความเสี่ยงทางด้าน E-Banking และสามารถประเมินภาพรวมของความเสี่ยงทางด้าน E-Banking ได้นั้น ผู้ตรวจสอบจะต้องแยกแยะการพิจารณาความเสี่ยงเชิงปริมาณและความเสี่ยงเชิงคุณภาพของการจัดการด้านความเสี่ยงของสถาบันการเงินออกจากกันให้ได้ก่อน แล้วจึงนำผลรวมทั้ง 2 มิตินี้ มารวมกันเป็นภาพรวมของความเสี่ยงของสถาบันการเงินโดยภาพรวมอีกครั้งหนึ่ง

2.1 การพิจารณาความเสี่ยงเชิงปริมาณ[4]

การพิจารณาความเสี่ยงเชิงปริมาณก็คือการพิจารณาในลักษณะที่ว่าสถาบันการเงินมีการให้ บริการทางการเงินโดยอาศัยเครือข่ายอิเล็กทรอนิกส์ต่อลูกค้าจำนวนมากหรือไม่ และมีชนิดของการให้บริการหรือระดับความยุ่งยากของขั้นตอนการให้บริการมากหรือไม่ เพราะยิ่งสถาบันการเงินมีลูกค้ามาก มีประเภทของการให้บริการมาก และแต่ละประเภทของบริการยังมีขั้นตอนการดำเนินงานที่ปลีกย่อยลงไปมากเท่าใด สถาบันการเงินก็ยิ่งจะมีความเสี่ยงเกิดขึ้นมากเท่านั้น ทั้งนี้ปัจจัยในการพิจารณาขึ้นอยู่กับเรื่องดังต่อไปนี้

2.1.1 ความสามารถในการให้บริการ (Capacity)

[4] “Information Technology School” , OCC, IS & E-banking Training, March 27-Apr 3-2001 at BOT

2.1.2 ความสลับซับซ้อนของการให้บริการ (Complexity)

2.1.3 ความสลับซับซ้อนของปัญหาทางด้านกฎหมาย (Litigation)

2.1.4 ระดับของการให้บริการ (Services Levels)

2.2. การพิจารณาความเสี่ยงเชิงคุณภาพ[5]

การพิจารณาความเสี่ยงเชิงคุณภาพ ก็คือ การพิจารณาในลักษณะที่ว่าสถาบันการเงินมีการดำเนินการในลักษณะใดบ้าง เพื่อให้ตนเองสามารถที่จะควบคุมหรือ ลดระดับของความเสี่ยงจากการให้บริการทางการเงินโดยอาศัยเครือข่ายอิเล็กทรอนิกส์ให้เหลือในระดับที่สถาบันการเงินสามารถยอมรับความเสี่ยงนั้นๆ ในการดำเนินงานประจำวันได้ (ความเสี่ยงนั้นจะต้องไม่มีผลกระทบที่รุนแรงจนกระทบกับฐานะและการหารายได้ของสถาบันการเงิน) โดยปัจจัยที่ใช้ในการพิจารณาเพื่อประเมินความเสี่ยงเชิงคุณภาพมี ดังนี้

2.2.1 เป้าหมายในการดำเนินธุรกิจของสถาบันการเงิน (Goals)

2.2.2 ผลกระทบในการดำเนินธุรกิจของสถาบันการเงิน (Effect on Business)

2.2.3 ผลการเปลี่ยนแปลงของสถาบันการเงินและความสามารถในการควบคุมการเปลี่ยนแปลง (Pace of Change)

2.2.4 ประเภทของการให้บริการมีความสลับซับซ้อนหรือไม่และสถาบันการเงินได้มีการเตรียมการรองรับอยู่ในระดับใด (Services)

2.2.5 นโยบายของสถาบันการเงินในการดำเนินงานด้านอิเล็กทรอนิกส์ว่ามีความเป็นไปได้เพียงใด (Services Levels)

2.2.6 ขั้นตอนในการดำเนินธุรกรรมของสถาบันการเงินว่ามีประสิทธิภาพหรือไม่ (Processes)

2.2.7 ประสิทธิภาพของบุคลากรของสถาบันการเงิน (Human Resources)

2.2.8 ประสิทธิภาพของเครื่องมือในการวัดผลการดำเนินงานของสถาบันการเงินว่ามีประสิทธิภาพหรือไม่ (Feedback Devices)

3. ขั้นตอนการตรวจสอบ

การตรวจสอบจะมีขั้นตอน ดังนี้

(1) ขั้นเตรียมการก่อนออกตรวจสอบ

[5] “Information Technology School” , OCC, IS & E-banking Training, March 27-Apr 3-2001 at BOT

(2) ขั้นปฏิบัติงานตรวจสอบ

(2.1) การตรวจสอบเพื่อประเมินความเสี่ยงเชิงปริมาณ

(2.2) การตรวจสอบเพื่อประเมินความเสี่ยงเชิงคุณภาพ

(2.3) การตรวจสอบเพื่อประเมินการปฏิบัติตามกฎหมาย

(3) ขั้นตอนการสรุปผลและจัดทำรายงาน

อนึ่ง ในการตรวจสอบสถาบันการเงินทางด้าน E-Banking นั้น ผู้ตรวจสอบจะประเมินความเสี่ยงเชิงปริมาณและเชิงคุณภาพ ตามแนวทาง 5 เรื่อง ดังนี้

1. ด้านนโยบายและการจัดการ

ปัจจัยหลักที่ใช้ในการพิจารณาคือ ความเพียงพอและความเหมาะสมของนโยบายและขั้นตอนการปฏิบัติงาน รวมถึงการกำกับดูแลของคณะกรรมการและฝ่ายบริหาร

2. ด้านการควบคุมภายในและการรักษาความปลอดภัย

ปัจจัยหลักที่ใช้ในการพิจารณาคือ ประสิทธิภาพและความเพียงพอของการสร้างสภาพแวดล้อมสำหรับการควบคุมภายในและการรักษาความปลอดภัยที่ดี

3. ด้านการตรวจสอบและสอบทาน

ปัจจัยหลักที่ใช้ในการพิจารณาคือ ความเป็นอิสระของการตรวจสอบและความครอบคลุมของขอบเขตการตรวจสอบและสอบทาน

4. ด้านการติดตามในระบบสารสนเทศและสื่อสาร

ปัจจัยหลักที่ใช้ในการพิจารณาคือ ความเพียงพอและความน่าเชื่อถือของระบบข้อมูลและการสื่อสารที่เกี่ยวโยงกับการดำเนินงานด้าน Internet Banking

5. ด้านการบริหารจัดการทางเทคโนโลยีโดยองค์กรภายนอก

ปัจจัยหลักที่ใช้ในการพิจารณาคือ ความมีประสิทธิภาพของการกำกับดูแล และบริหารจัดการ การดำเนินงานในส่วนที่ว่าจ้างองค์กรภายนอก

ซึ่งในแต่ละเรื่องจะเกี่ยวโยงสัมพันธ์กับความเสี่ยง 2 ประเภทหลักที่สำคัญ คือ ความเสี่ยงด้านกลยุทธ์ และความเสี่ยงด้านปฏิบัติการ กล่าวโดยสรุป คือ

ความเสี่ยงเชิงกลยุทธ์ จะว่าด้วยเรื่องที่เกี่ยวข้องกับนโยบาย การจัดการ บทบาทคณะกรรมการและฝ่ายบริหาร การพัฒนาบุคลากร และการบริหารงานทั่วไปด้าน Internet Banking และการบริหารเรื่องเฉพาะด้าน เช่น นโยบายด้านระบบรักษาความปลอดภัย นโยบายการว่าจ้างองค์กรภายนอก ดำเนินการทางด้านเทคโนโลยี เป็นต้น

ความเสี่ยงจากการดำเนินงาน จะว่าด้วยเรื่องขั้นตอนและวิธีการดำเนินงานทั้งที่เป็นกระบวนการทำงานประจำ (Daily Operation) และงานในลักษณะโครงการ เช่น การพัฒนาระบบงาน เป็นต้น และยังหมายรวมถึงกระบวนการด้านรักษาความปลอดภัย กระบวนการตรวจสอบ กระบวนการติดตามในระบบสารสนเทศและสื่อสาร และกระบวนการดำเนินการในส่วนที่ว่าจ้างองค์กรภายนอก และหากผู้ตรวจสอบพบว่ามีประเด็นที่อาจส่งผลกระทบต่อความเสี่ยงด้านอื่น ได้แก่ ความเสี่ยงด้านเครดิต ความเสี่ยงด้านตลาด และความเสี่ยงด้านสภาพคล่อง ให้ดำเนินการรวบรวมประเด็นหรือข้อสังเกตที่พบส่งให้ทีมตรวจสอบที่รับผิดชอบตรวจสอบความเสี่ยงด้านนั้นๆทราบ เพื่อดำเนินการต่อไป

3.1 ขั้นเตรียมการก่อนออกตรวจสอบ

วัตถุประสงค์

กระบวนการเตรียมการก่อนออกตรวจสอบมีวัตถุประสงค์หลักดังต่อไปนี้

- เพื่อลดเวลาที่ใช้ในการตรวจสอบสถาบันการเงินและลดภาระที่มีต่อผู้บริหารและเจ้าหน้าที่ของสถาบันการเงิน
- เพื่อให้เข้าใจสถาบันการเงินที่จะออกตรวจสอบในเบื้องต้น ในเรื่องโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบรักษาความปลอดภัย และบริการด้าน Internet Banking
- เพื่อประเมินระดับความเสี่ยงและพิจารณานโยบาย ขั้นตอน ระบบการติดตามที่เกี่ยวข้องกับการดำเนินงานด้าน Internet Banking
- เพื่อให้ทราบถึงความเปลี่ยนแปลงต่างๆที่เกิดขึ้นทางด้านการให้บริการ Internet Banking ของสถาบันการเงิน จากช่วงเวลาที่เข้าตรวจสอบครั้งล่าสุด
- เพื่อกำหนดขอบเขตการตรวจสอบโดยมุ่งเน้นประเด็นไปที่การดำเนินธุรกรรมหรือการให้บริการที่ส่อว่าจะทำให้สถาบันการเงินมีความเสี่ยงเพิ่มขึ้น

ขั้นตอนหลัก

- รวบรวมข้อมูล
- วิเคราะห์และประเมินข้อมูลที่ได้รับ
- สรุปประเด็นและกำหนดขอบเขตการตรวจสอบ
- จัดสรรกำลังคน ระยะเวลาที่ใช้ในการตรวจสอบ และจัดทำแผนการตรวจสอบ
- ขออนุมัติออกตรวจสอบ
- เตรียมการเพื่อออกตรวจสอบ

รายละเอียดขั้นตอนการเตรียมการก่อนออกตรวจสอบ

(1) รวบรวมข้อมูล

รวบรวมข้อมูลทั้งจากภายในและภายนอก เพื่อใช้ในการประเมินลักษณะการดำเนินงาน การให้บริการ ทางด้าน Electronic Banking เบื้องต้น และควรติดต่อกับส่วนงานอื่น เช่น ฝ่ายกำกับที่ดูแลสถาบันการเงินนั้น สายนโยบายสถาบันการเงิน สายระบบชำระเงิน เพื่อทราบประเด็นที่ต้องติดตามและการสั่งการของทางการต่อสถาบันการเงิน นอกจากนี้ ควรติดตามข่าวสารและความเคลื่อนไหวต่างๆ ในแวดวงที่เกี่ยวข้องจากแหล่งข้อมูลต่างๆ

(2) วิเคราะห์และประเมินข้อมูลที่ได้รับ

นำข้อมูลที่รวบรวมมาวิเคราะห์และประเมินความเสี่ยงในเบื้องต้น โดยพิจารณาตามแนวทางการตรวจสอบ 5 ด้าน ตามที่กล่าวมาแล้วข้างต้น เพื่อกำหนดขอบเขตการตรวจสอบ และอาจซักถามประเด็น ข้อสงสัยกับองค์กรภายนอกที่เกี่ยวข้อง เช่น ผู้ประเมินระบบอิสระ เพื่อให้เกิดความเข้าใจมากขึ้น

<u>ด้านนโยบายและการจัดการ</u>

1. สอบทานเอกสารจากฝ่ายงานกำกับสถาบันการเงินนั้นและเอกสารต่างๆที่ใช้ในการติดตามประเด็นต่างๆ (Follow-up activities) ที่เกี่ยวข้อง เพื่อให้ทราบถึงประเด็นทางด้าน Electronic Banking ของสถาบันการเงินนั้น

2. มีการเปลี่ยนแปลงสินค้า บริการ หรือการดำเนินงานที่เป็นนัยสำคัญเกิดขึ้นหลังจากการตรวจสอบครั้งก่อนหรือไม่ และสถาบันการเงินวางแผนที่จะดำเนินการเปลี่ยนแปลงใดๆ ในอนาคตอันใกล้ หรือไม่

3. สอบทานเอกสารต่างๆและหารือในเบื้องต้นกับผู้บริหารของสถาบันการเงิน เพื่อกำหนดเรื่องต่อไปนี้

3.1 ผู้บริหารกำกับดูแลการดำเนินงานด้าน Internet Banking รวมทั้งดูแลการบริหารจัดการของบริษัทผู้ให้บริการภายนอก อย่างไร

3.2 การเปลี่ยนแปลงที่เป็นนัยสำคัญของนโยบาย วิธีปฏิบัติ บุคลากร หรือระบบควบคุม

3.3 ปัจจัยภายในและภายนอกอื่นๆ ที่อาจส่งผลกระทบต่อ Internet Banking

4. สอบทานแผนดำเนินธุรกิจและแผนกลยุทธ์ของสถาบันการเงิน พิจารณาดูว่าแผนทางด้าน Internet Banking มีความชัดเจน และสัมพันธ์กับทิศทางการดำเนินงานทางด้านดังกล่าวในปัจจุบันหรือไม่

5. พิจารณาดูว่าแผนสำรองฉุกเฉินของสถาบันการเงินครอบคลุมด้าน Internet Banking ด้วยหรือไม่

6. ทำความเข้าใจธุรกิจด้าน Internet Banking และการเปิดเผยข้อมูลของสถาบันการเงิน โดยการสอบทาน WebSite ของสถาบันการเงิน เพื่อ

6.1. กำหนดประเภทของธุรกรรม Internet Banking ของสถาบันการเงินในปัจจุบันและที่วางแผนว่าจะดำเนินการ โดยพิจารณาในเรื่องต่อไปนี้

6.1.1 ระดับของการให้บริการทาง Internet Banking (รูปแบบให้ข้อมูลข่าวสาร [Information-only] สื่อสาร [Communication] และการทำธุรกรรมทางการเงิน [Transaction])

6.1.2 มีการให้บริการผ่านเครือข่ายอื่น นอกเหนือจากเครือข่าย Internet เช่น Direct dial-up PC Banking เครือข่ายโทรศัพท์ (Telephone banking) เป็นต้น หรือไม่

6.1.3 มีการให้บริการอื่นๆ เช่น เป็นผู้ให้บริการทาง Internet (Internet service provider), Web site hosting, Trust services, Account aggregation, Electronic bill presentment หรือไม่

6.2 ตรวจสอบเนื้อหาใน Website มีความถูกต้องและเป็นปัจจุบันหรือไม่

6.3 ตรวจสอบ Website ของสถาบันการเงิน พิจารณาว่าปฏิบัติภายใต้ตามกฎระเบียบ ข้อบังคับตามที่ธปท. กำหนดหรือไม่

7. ประเมินการให้ความสำคัญต่อธุรกิจด้าน Internet Banking

7.1 พิจารณาถึงความสำคัญของบริการ Internet Banking โดยพิจารณาเรื่องต่อไปนี้

7.1.1 สัดส่วนและจำนวนของลูกค้า (เช่นสินเชื่อ เงินฝาก เป็นต้น) ที่ใช้บริการ Internet Banking เป็นประจำ

7.1.2 ปริมาณสินเชื่อและเงินฝาก รวมทั้งการใช้บริการประเภทอื่นผ่านทาง Internet

7.1.3 จำนวนและปริมาณธุรกรรมรายเดือนจากบริการ Internet Banking

7.2 สอบทานบันทึกการประชุมของคณะกรรมการต่างๆ เพื่อประเมินว่าผู้บริหารตระหนักถึงความรับผิดชอบ การบริหารจัดการรายวัน และประเด็นทางด้าน Internet Banking หรือไม่

<u>ด้านการควบคุมภายในและการรักษาความปลอดภัย</u>

1. สอบทานเอกสารต่างๆและหารือในเบื้องต้นกับผู้บริหารของสถาบันการเงิน เพื่อให้ทราบถึงวิธีการรักษาความปลอดภัยของระบบงาน Internet Banking

2. พิจารณาลักษณะ การดำเนินงานพัฒนาและดูแลการทำธุรกรรม Internet Banking โดยพิจารณาเรื่องต่อไปนี้

2.1 ตำแหน่ง/สถานที่ของ Web Site

2.2 บุคคล/หน่วยงานที่รับผิดชอบในการดูแล Website ของสถาบันการเงิน

2.3 บุคคล/หน่วยงานที่รับผิดชอบในการพัฒนาระบบงาน Internet Banking ของสถาบันการเงิน

2.4 ตำแหน่ง/สถานที่ตั้งของระบบงาน Internet Banking

2.5 บุคคล/หน่วยงานที่รับผิดชอบในการดูแลระบบงาน Internet Banking ของสถาบันการเงิน

2.6 บุคคล/หน่วยงานที่รับผิดชอบในการให้บริการลูกค้า เช่น Call Center

2.7 การประมวลผลการชำระรายการ (Bill Payment Processing) หรือบริการเสริมอื่นๆ (Other ancillary services) กระทำโดยองค์กรอื่น (บุคคลที่สาม)

<u>ด้านการตรวจสอบและสอบทาน</u>

1. สอบทานรายงานตรวจสอบดังต่อไปนี้ เพื่อรวบรวมประเด็นปัญหาทางด้าน Internet Banking ที่พบ และเพื่อใช้ดำเนินการติดตามว่าสถาบันการเงินได้ดำเนินการแก้ไขแล้วหรือไม่ อย่างไร

1.1 รายงานการตรวจสอบและกระดาษทำการของการตรวจสอบครั้งก่อน เพื่อติดตามประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบครั้งก่อน

1.2 รายงานจากผู้ตรวจสอบภายในและภายนอก หรือรายงานการตรวจสอบของผู้ให้บริการแก่สถาบันการเงิน และรายงานตรวจสอบอื่นๆที่เกี่ยวข้อง

2. ขอรายงานการสอบทาน ประเมิน และทดสอบระบบของผู้ตรวจสอบภายในและ/หรือภายนอก บริษัทที่ปรึกษา หรือผู้เชี่ยวชาญทางด้านเทคโนโลยี ที่ได้รับการว่าจ้างจากสถาบันการเงินให้กระทำการดังกล่าว และจดประเด็นข้อบกพร่องที่เป็นนัยสำคัญไว้

ด้านการติดตามในระบบสารสนเทศและสื่อสาร

1. สถาบันการเงินบริหารจัดการ Website ของระบบงาน Internet Banking และระบบประมวลผลข้อมูลหลักภายในเองหรือไม่ ถ้าใช่ ให้สอบทาน system & network topology และพิจารณาดูว่ามีการเชื่อมต่อโดยตรงและ Online ระหว่างระบบประมวลผลหลักของสถาบันการเงินกับ Internet Web Site หรือไม่

2. ถ้าสถาบันการเงินบริหารจัดการระบบงาน Internet Banking หรือระบบประมวลผลข้อมูลหลักของสถาบันการเงินเอง ให้สอบทานทางเดินของการประมวลผลธุรกรรมระหว่างระบบงาน Internet Banking กับระบบประมวลผลหลักของสถาบันการเงิน ระบุจุดควบคุมหลัก (Key Control Points) และระบุว่าการแลกเปลี่ยนข้อมูลเป็นแบบ Real-time, batch หรือ กระทำในรูปแบบผสม (Hybrid processing mode)

ด้านการบริหารจัดการทางเทคโนโลยีโดยองค์กรภายนอก

พิจารณาดูว่ามีการว่าจ้างบริษัทผู้ให้บริการภายนอกหรือไม่ และให้บริการประเภทใด ผู้ตรวจสอบควรรวบรวมรายชื่อรวมทั้งรายละเอียดอื่นๆตามสมควรของส่วนงาน/องค์กร ที่รับผิดชอบในการพัฒนาการดำเนินงาน และ/หรือทำหน้าที่สนับสนุนระบบงานด้าน Internet Banking

(3) สรุปประเด็นและกำหนดขอบเขตการตรวจสอบ

(3.1) สรุปภาพรวมของการดำเนินงานทางด้าน Internet Banking โครงสร้างระบบงาน ระบบเครือข่าย และระบบรักษาความปลอดภัย

(3.2) ทำความเข้าใจลักษณะและระดับธุรกรรมและการให้บริการ Internet Banking

(3.3) ระบุธุรกรรมหรือการให้บริการที่มีแนวโน้มความเสี่ยงสูง

(3.4) ระบุประเด็นสำคัญที่ต้องติดตาม โดยเรียงลำดับความสำคัญของประเด็นที่พบตามระดับความเสี่ยงจากสูงไปหาต่ำ โดยอาศัยผลการวิเคราะห์ข้อมูลและวิจารณญาณของทีมผู้ตรวจสอบ

(3.5) ศึกษาปัจจัยภายนอกที่สำคัญที่อาจก่อให้เกิดความเสี่ยงใดๆ แก่สถาบันการเงิน เช่น การเปลี่ยนแปลงทางเทคโนโลยี

(3.6) เข้าร่วมประชุมหารือกับฝ่ายตรวจสอบ ฝ่ายกำกับสถาบันการเงินและตรวจสอบสถาบันเฉพาะกิจ และฝ่ายวิเคราะห์และติดตามฐานะ

(3.7) กำหนดขอบเขตการตรวจสอบ โดย

- สรุปผลการประเมินความเสี่ยง
- กำหนดขอบเขตธุรกรรมที่จะทำการทดสอบรายการ (ในกรณีที่จำเป็น)

- พิจารณาให้สอดคล้องกับนโยบายจากผู้บริหารระดับสูง (กรณีมีคำสั่งตรวจเฉพาะเรื่อง)

(3.8) จัดทำบันทึกแสดงขอบเขตการตรวจสอบ โดยมีหัวข้อขั้นต่ำ ดังนี้

- วัตถุประสงค์ของการตรวจสอบ
- ประเด็นที่จะตรวจสอบ
- ขอบเขตธุรกรรมที่จะทำการทดสอบรายการ (ในกรณีที่จำเป็น)
- จำนวนผู้ตรวจสอบ
- ระยะเวลาการตรวจสอบ

(4) จัดสรรกำลังคน ระยะเวลาที่ใช้ในการตรวจสอบ และจัดทำแผนการตรวจสอบ

(4.1) กำหนดแผนตรวจสอบจากผลที่ประเมินได้

(4.2) ประมาณอัตรากำลังคนและเวลาที่จะใช้ในการตรวจสอบในแต่ละเรื่อง

(4.3) จัดทำแผนการตรวจสอบ

หมายเหตุ : เนื่องจากการดำเนินงานในระยะแรก มีข้อจำกัดในเรื่องอัตรากำลังของผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ และ E-Banking และการกำหนดแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศและ E-Banking จะขึ้นอยู่กับการกำหนดแผนตรวจสอบโดยรวมของสายกำกับสถาบันการเงิน ธปท. ดังนั้น การจัดสรรกำลังคนและการกำหนดระยะเวลาในการตรวจสอบจึงไม่สามารถทำได้โดยอิสระ

(5) ขออนุมัติออกตรวจสอบ

เสนอบันทึกขออนุมัติออกตรวจสอบสถาบันการเงิน พร้อมแนบแผนการตรวจสอบ ให้ผู้บริหารพิจารณาอนุมัติการออกตรวจสอบ

(6) เตรียมการเพื่อออกตรวจสอบ

(6.1) จัดเตรียมรายการขอเอกสาร (ตามภาคผนวก 5) และนัดสัมภาษณ์ เพื่อให้สถาบันการเงินเตรียมไว้ให้ในวันแรกของการออกตรวจสอบ โดยอาจส่งทางโทรสารหรือพนักงานเดินเอกสารก็ได้

(6.2) จัดเตรียมหนังสือถึงผู้บริหารสถาบันการเงินเพื่อแจ้งการเข้าตรวจสอบและส่งให้สถาบันการเงินลงนามรับทราบก่อนเข้าตรวจสอบ (ในกรณีที่เป็นการตรวจสอบร่วมกับทางฝ่ายตรวจสอบ1 หรือฝ่ายตรวจสอบ 2 EIC จะเป็นผู้เตรียม)

(6.3) ส่งบันทึกแสดงขอบเขตการตรวจสอบให้ผู้ตรวจสอบที่จะออกตรวจรับทราบ

(6.4) ชี้แจงให้ทีมผู้ตรวจสอบเข้าใจขอบเขต แผนงาน และการจัดสรรกำลังคนในการตรวจสอบ

(6.5) ยืนยันการนัดหมายกับผู้บริหารของสถาบันการเงิน เพื่อพบปะหารือในวันแรกของการตรวจสอบ

(6.6) เตรียมเอกสาร กระดาษทำการ อุปกรณ์ และเครื่องเขียนต่างๆ ที่ใช้ในการตรวจสอบ

3.2 ขั้นปฏิบัติงานตรวจสอบ

3.2.1 การตรวจสอบเพื่อประเมินความเสี่ยงเชิงปริมาณ

วัตถุประสงค์

- เพื่อประเมินระดับความเสี่ยงโดยพิจารณาจากขนาด ปริมาณ และโครงสร้างความซับซ้อนของธุรกรรมและลักษณะการให้บริการด้าน Internet Banking

- เพื่อประเมินจุดอ่อนในโครงสร้างของระบบงาน และความรัดกุมของสภาพแวดล้อมของระบบรักษาความปลอดภัย

- เพื่อประเมินระดับความเสี่ยงจากทิศทางของแนวนโยบายของระดับ และแผนดำเนินธุรกิจต่างๆ ทางด้าน Internet Banking

วิธีการ

<u>ด้านนโยบายและการจัดการ</u>

1. แจกแจงประเภท ปริมาณ และความซับซ้อนของผลิตภัณฑ์และบริการทาง Internet Banking โดยรวม รวมทั้งบริการที่เป็น Retail Wholesale และ Fiduciary

2. หารือกับผู้บริหารของสถาบันการเงิน จดประเด็นการเปลี่ยนแปลงในประเภท ปริมาณ หรือ ความซับซ้อนของผลิตภัณฑ์หรือบริการที่คาดว่าจะเกิดขึ้นในอีก 2 ปีข้างหน้า

3. ประเมินกลยุทธ์ทางการตลาดด้าน Internet Banking เพื่อกำหนดดูว่ามีแผนที่จะขยายเข้าไปสู่ตลาดใหม่ สินค้าใหม่ หรือเทคโนโลยีใหม่ๆ หรือไม่

4. ขอภาพรวมของทางเดินรายการทางการเงินและบริการด้านการชำระเงิน รวมทั้งกระบวนการชำระรายการจากผู้บริหาร พร้อมทั้งพิจารณาในเรื่องดังต่อไปนี้

4.1 ผู้บริหารเข้าใจทางเดินรายการและกระบวนการชำระรายการหรือไม่

4.2 มีการกำหนดหน้าที่และความรับผิดชอบในการชำระรายการของสถาบันการเงินไว้ชัดเจนหรือไม่

4.3 สถาบันการเงินรับทราบถึงความเสี่ยงด้านเครดิตที่อาจเกิดขึ้นจากช่วงเวลาในการชำระบัญชี (Settlement) ของคู่ค้าแต่ละคนแตกต่างกันหรือไม่

4.4 นโยบายของบริษัทผู้ให้บริการครอบคลุมถึงเรื่องเงินทุนที่เรียกเก็บไม่ได้ การชำระรายการ การสำรองข้อมูล แผนฉุกเฉิน บริการสำหรับลูกค้า และการกู้ระบบหรือไม่

4.5 มีการรายงานกิจกรรมที่ได้รับยกเว้นต่างๆ (Exception reporting) เพียงพอหรือไม่

ด้านการควบคุมภายในและการรักษาความปลอดภัย

1. ขอรายละเอียด หรือแผนผังของ Configuration ของระบบงาน Internet Banking และกำลังความสามารถของระบบ พิจารณา Hardware Software และการเชื่อมต่อของระบบงาน Internet Banking รวมทั้งจุดเข้าถึงระบบงานจากระยะไกล (Remote Access Points) การประเมินเรื่องต่อไปนี้ จะช่วยให้ผู้ตรวจสอบกำหนดระดับความเสี่ยงได้

1.1 ระบบงาน Internet Banking เชื่อมต่อกับ Host system หรือโครงสร้างเครือข่ายของสถาบันการเงินอย่างไร

1.2 ข้อมูลและรายการต่างๆเคลื่อนไหวผ่านเครือข่ายอย่างไร

1.3 ประเภทของช่องทางการสื่อสาร และกำลังความสามารถของการเข้าถึงจากระยะไกล (ใช้ direct modem dial in หรือผ่าน Internet หรือสามารถเข้าถึงได้ด้วยทั้ง 2 วิธี)

2. สอบทานโครงสร้างรูปแบบของระบบงานและเครือข่าย (system and network architecture) เพื่อแจกแจงจุดเข้าถึง (access point) และส่วนที่อาจจะเป็นจุดอ่อนของระบบได้

3. สอบทานการให้บริการทางการเงินและการชำระเงิน และพิจารณาว่ามีการควบคุมในระบบงานเพียงพอหรือไม่เพื่อยืนยันการแสดงตัวตนของผู้ใช้ ความถูกต้องของข้อมูล การรักษาความลับของข้อมูล และรายการทางการเงิน

ด้านการตรวจสอบและสอบทาน

มีการตรวจสอบระบบงาน Internet Banking อย่างต่อเนื่อง เป็นประจำ โดยผู้ตรวจสอบภายใน หรือผู้ประเมินอิสระหรือไม่

ด้านการติดตามในระบบสารสนเทศและสื่อสาร

1. มีระบบที่คอยติดตามการให้บริการและการรักษาความปลอดภัยของเครือข่ายที่ให้บริการ Internet Banking หรือไม่

2. พิจารณาดูว่ามีรายงานของระบบข้อมูลเพื่อการบริหาร (MIS report) หรือไม่ รายงานดังกล่าวมีความเพียงพอต่อการบริหารจัดการธุรกรรม Internet Banking และธุรกรรมด้านบริการการชำระเงินหรือไม่

ด้านการบริหารจัดการทางเทคโนโลยีโดยองค์กรภายนอก

มีการประเมินหรือตรวจสอบความเสี่ยงของบริษัทผู้ให้บริการภายนอกหรือไม่

3.2.2 การตรวจสอบเพื่อประเมินความเสี่ยงเชิงคุณภาพ

ลักษณะการตรวจสอบเพื่อประเมินความเสี่ยงเชิงคุณภาพแบ่งเป็น 2 ระดับ คือ การตรวจสอบหลัก (Core Analysis) และการตรวจสอบเพิ่มเติม (Expanded Analysis)

(1) การตรวจสอบหลัก

วัตถุประสงค์

- เพื่อประเมินประเด็นที่มีนัยสำคัญ และพิจารณาดูว่ามีความจำเป็นต้องทำการตรวจสอบเพิ่มเติมหรือไม่ ซึ่งในการตัดสินใจว่าจะทำการตรวจสอบเพิ่มเติมต่อหรือไม่นั้นขึ้นกับวิจารณญาณของผู้ตรวจสอบ

- เพื่อนำผลที่ได้จากการประเมิน มาใช้พิจารณาความเพียงพอของการกำหนด วัด ติดตาม และควบคุมความเสี่ยง

วิธีการ

<u>ด้านนโยบายและการจัดการ</u>

<u>นโยบายและขั้นตอนการดำเนินงาน</u>

1. พิจารณาดูว่านโยบายด้านการรักษาความปลอดภัยระบบ Internet Banking ครอบคลุมเรื่องต่อไปนี้ หรือไม่

1.1 มีการแบ่งแยกความรับผิดชอบของการรักษาความปลอดภัยระบบอย่างชัดเจน

1.1.1 สอบทานหน้าที่ของผู้บริหารระบบ/ผู้ดูแลระบบ (System Administrator) และพิจารณาดูว่าบุคคลนั้นมีความรู้เกี่ยวกับเรื่องนโยบายการรักษาความปลอดภัยและการควบคุมภายในของระบบงานหรือไม่ อย่างไร

1.1.2 พิจารณาดูว่า ผู้บริหารระบบ/ผู้ดูแลระบบ (System Administrator) มีอำนาจในการควบคุมและบังคับใช้นโยบายหรือไม่

1.2 การควบคุมระบบเครือข่ายและการเข้าถึง

2. มีการกำหนดนโยบายเกี่ยวกับ Firewall ให้ครอบคลุมเรื่องต่อไปนี้ หรือไม่

2.1 ความรับผิดชอบในการจัดการดูแลและติดตาม Firewall

2.2 กฎที่ใช้ในการเข้าถึงระบบงานที่กำหนดไว้อย่างชัดเจน (well-defined access rules)

2.3 กฎที่ใช้ในการเข้าถึงระบบงาน (Access rule) ระบุถึงประเภทของ traffic ที่จะได้รับอนุญาตให้ผ่านเข้าไปในระบบได้ และประเภทที่จะถูกห้ามไม่ให้ผ่านเข้าไป

3. นโยบายด้านรักษาความปลอดภัยครอบคลุมถึงเรื่องการเข้ารหัส อย่างเพียงพอหรือไม่ โดยมีการระบุเรื่องต่อไปนี้หรือไม่

3.1 หน่วยงาน และ/หรือบุคลากรที่รับผิดชอบในการควบคุมกระบวนการเข้ารหัส

3.2 วิธีการเข้ารหัส

3.3 เทคนิคการจัดประเภทของข้อมูล (Data classification techniques)

3.4 การเข้ารหัสเพื่อป้องกันข้อมูล ข้อความ รหัสของลูกค้าที่ส่งผ่านเครือข่ายสื่อสารภายในและเครือข่ายสาธารณะ

4. ถ้ามีการใช้เทคนิคการเข้ารหัสด้วยกุญแจสาธารณะ (public key cryptographic system) พิจารณาดูว่า Private key อยู่ภายใต้การควบคุมของสถาบันการเงิน และ มีการกำหนดนโยบายและการควบคุมในเรื่องการบริหารจัดการ private key หรือไม่ ดูว่านโยบายและขั้นตอนการปฏิบัติงานระบุเรื่องต่อไปนี้หรือไม่

4.1 การบริหารจัดการกุญแจโดยสถาบันการเงินหรือบุคคลที่สาม (third party)

4.2 การรักษาความปลอดภัยของ secret หรือ private key storage

4.3 บุคคลที่ได้รับอนุญาตให้เข้าถึงกุญแจได้ และมีการควบคุมอย่างไร

4.4 ถ้ามี private key escrow arrangement พิจารณาดูว่ามีการควบคุมเรื่องดังกล่าวอย่างไร

4.5 ขั้นตอนและวิธีปฏิบัติงานสำหรับการยกเลิกหรือออกเพื่อทดแทน (reissuance) กุญแจที่สูญหาย ใช้ร่วมกัน (compromised) หรือหมดอายุ

4.6 การเก็บกุญแจไว้บน server หรือเครื่องคอมพิวเตอร์ที่ไม่ได้เชื่อมต่อกับระบบเครือข่ายภายนอก

5. นโยบายครอบคลุมเรื่องการใช้ software เพื่อตรวจจับ virus หรือไม่ พร้อมทั้งจดบันทึกว่าใช้ผลิตภัณฑ์ไหนบ้าง

6. มีการสอบทานและปรับปรุงให้นโยบายด้านรักษาความปลอดภัยทันสมัยอยู่เสมอเป็นประจำหรือไม่ และผ่านการอนุมัติจากคณะกรรมการ และผู้บริหารระดับสูงของสถาบันการเงินหรือไม่

7. มีการกำหนดนโยบายเกี่ยวกับ hyper links ที่ให้ผู้ใช้สามารถแยกแยะความแตกต่างในเรื่องดังต่อไปนี้อย่างชัดเจนหรือไม่

7.1 สินค้าและบริการที่เป็นของสถาบันการเงินและที่มิใช่ของสถาบันการเงิน

7.2 เมื่อออกจาก Web Site ของสถาบันการเงิน

8. สอบทานขั้นตอนการปฏิบัติงานในการดูแล Website ของสถาบันการเงิน โดยพิจารณาเรื่องต่อไปนี้

8.1 การ update หรือเปลี่ยนแปลงแก้ไขข้อมูลบน WebSite สามารถดำเนินการได้โดยพนักงานที่ได้รับมอบหมายอำนาจให้ทำได้เท่านั้น

8.2 มีการทำ dual verification ทุกครั้งที่มีการ update หรือเปลี่ยนแปลงแก้ไขข้อมูล

8.3 มีการตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลบน Website และจุดเชื่อมต่อไปที่ Websiteอื่น

8.4 ผู้บริหารจัดให้มีขั้นตอนการปฏิบัติงานเพื่อตรวจสอบ (verify) ความถูกต้องของเนื้อหาและองค์ประกอบของ Software ที่ใช้ในการวางแผนทางการเงิน การคำนวณ หรือโปรแกรม Interactive อื่นๆ ที่จัดหาให้แก่ลูกค้าผ่าน Internet Website หรือบริการ Internet Banking อื่นๆ

8.5 ในการเชื่อมต่อไปที่ Website อื่นๆ ควรจัดให้มี Disclaimer ที่แจ้งว่าลูกค้ากำลังออกจาก Website ของสถาบันการเงิน และควรจัดให้มีการเปิดเผยข้อมูล (Disclosure) อย่างเหมาะสม เช่น แจ้งให้ผู้ใช้ทราบถึงพันธะข้อผูกพันที่สถาบันการเงินมีต่อธุรกรรมหรือข้อมูลบน Website อื่น

9. ประเมินการบริหารกระบวนการทำงาน (Process Management) ที่ใช้ในการกำหนดประเภทของ Web Site ที่เหมาะสม (แจ้งข้อมูลข่าวสาร (Information) สื่อสาร (Communication) ทำธุรกรรมทางการเงิน (Transaction) ที่ใช้ในการดำเนินธุรกิจการธนาคารผ่าน Internet

10. สอบทานนโยบายและขั้นตอนการดำเนินงานเพื่อพิจารณาว่านโยบายและขั้นตอนการดำเนินงานที่กำหนด (ขั้นต่ำ) ครอบคลุมเรื่องดังต่อไปนี้หรือไม่

10.1 ขั้นตอนการดำเนินงานและการควบคุมสำหรับการเปิดบัญชีลูกค้าใหม่ผ่านสื่ออิเล็กทรอนิกส์

10.2 ขั้นตอนการปฏิบัติงานในการสร้างบัญชีใหม่บนระบบงาน Internet Banking

10.3 การควบคุมการเข้าถึงระบบ Internet Banking เช่นการใช้รหัสผ่าน (Password) รหัสลับ PINs และเลขที่บัญชี (account number)

10.4 Appropriate authorizations for electronic debits initiated against other accounts.

10.5 วงเงินของการทำธุรกรรมต่างๆ บน Internet Banking

10.6 การประมวลผลสำหรับการชำระรายการ (Bill payment) การกระทบยอดรายการ รวมทั้งการประมวลผลรายการที่มีเงินทุนไม่เพียงพอ

11. นโยบายและขั้นตอนการดำเนินงานในการรักษาความปลอดภัยของข้อมูลระบุถึงการเข้าถึงและการป้องกันข้อมูลลับของลูกค้าที่เก็บไว้และ/หรือสามารถเรียกดูได้จากการใช้บริการทาง Internet Banking หรือไม่

12. นโยบายของสถาบันการเงินกำหนดถึงเรื่องการรายงานธุรกรรมที่น่าสงสัย (Formal suspicious activity) จากความพยายามบุกรุกเข้าระบบคอมพิวเตอร์อันจะส่งผลกระทบต่อระบบงาน Internet Banking หรือไม่

13. พิจารณาดูว่าการพัฒนาและการให้บริการทางอิเล็กทรอนิกส์กระทำโดยบุคลากรที่มีประสบการณ์ และมีการแบ่งแยกหน้าที่ความรับผิดชอบกันอย่างชัดเจน อีกทั้งสถาบันการเงินจัดให้มีพนักงานเพียงพอกับปริมาณงานหรือไม่

14. มีการปรับปรุงนโยบายของสถาบันการเงินในเรื่องของการแบ่งแยกหน้าที่เข้ากับกำลังความสามารถในการเข้าถึงระบบผ่านทางสื่ออิเล็กทรอนิกส์ และเป็นไปตามหลักการควบคุมภายในที่ดีหรือไม่

15. มีนโยบายการทดสอบระบบงานแต่ละระบบหรือไม่

15.1 Volume Stress Testing -ทดสอบความสามารถของระบบในการรองรับปริมาณธุรกรรม

15.2 Screen Testing (Review content) -ทดสอบความถูกต้องครบถ้วนของเนื้อหาที่ปรากฏอยู่บนหน้า Web Page และทดสอบความถูกต้องของการเชื่อมโยง

15.3 Pilot Program -ประเมินความเป็นไปได้ของการนำระบบงานไปใช้

16. สอบทานนโยบายและขั้นตอนการดำเนินงาน เพื่อพิจารณาดูว่าได้มีการปรับปรุงนโยบายและขั้นตอนการดำเนินงานให้เหมาะสมกับลักษณะเฉพาะและความเสี่ยงที่อาจเกิดจากรูปแบบการให้บริการผ่านทางสื่ออิเล็กทรอนิกส์หรือไม่ และนโยบายครอบคลุมถึงรูปแบบการให้บริการทางอิเล็กทรอนิกส์หรือไม่

17. มีการรายงานลักษณะ ปริมาณ และ แนวโน้มของธุรกรรมในแต่ละระบบงานหรือไม่ อย่างไร รวมทั้งมีการเปรียบเทียบสิ่งที่เกิดขึ้นจริงกับประมาณการที่ทำไว้หรือไม่

18. เครื่องมือวัดตามที่กล่าวรวมอยู่ในแผนกลยุทธ์ แผนดำเนินงาน งบประมาณ และการวิเคราะห์อื่นๆ หรือไม่ (เครื่องมือวัดควรรวมอยู่ในนโยบายและขั้นตอนการดำเนินงาน เช่นการบริหารกองทุน สภาพคล่อง และความเสี่ยงทางด้านอัตราดอกเบี้ย เป็นต้น)

19. การกำหนดและปรับปรุง (Update) นโยบายและขั้นตอนการดำเนินงานสำหรับการทำธุรกรรมกับลูกค้า ครอบคลุมเรื่องดังต่อไปนี้หรือไม่

19.1 โอนเงิน (ลูกค้าสามารถทำผ่าน Bahtnet หรือระบบชำระเงินอื่นๆ หรือไม่ และมีนโยบายและการป้องกันที่เหมาะสมหรือไม่)

19.2 วงเงิน เช่น วงเงินรายวัน (Day limit)

19.3 Minimum Credit Standard for participants

19.4 แนวทางการชำระรายการ

19.5 วงเงินสภาพคล่องรายวัน (Daylight overdrafts) - กำหนดประมาณการของปริมาณธุรกรรมในแต่ละบริการ และสถาบันการเงินจัดให้มี กำลังความสามารถ (Capacity) เหมาะสมเพียงพอที่จะรองรับปริมาณธุรกรรมที่ประมาณการไว้หรือไม่

20. มีการกำหนดนโยบายและขั้นตอนการดำเนินงานเพื่อควบคุมการทำธุรกรรมเงินตราต่างประเทศที่เหมาะสมหรือไม่

21. สำหรับระบบที่สามารถเข้าถึง Credit Lines ได้ สถาบันการเงินจัดให้มีการควบคุมการขยาย Credit อย่างเหมาะสมหรือไม่

22. มีการจัดทำและปรับปรุงแนวทางในการจัดเก็บสำหรับเอกสารต้นฉบับเพื่อรองรับธุรกรรมทางสื่ออิเล็กทรอนิกส์ เช่น ใบสมัครขอเปิดบัญชี (Account application) ธุรกรรมทางบัญชี (Account transactions) และการเก็บข้อมูลอื่นๆ (Other records) เป็นต้น หรือไม่ และพิจารณาว่าแนวทางดังกล่าวครอบคลุมถึง E-Mail ไฟล์ข้อมูล และการเก็บข้อมูลรูปแบบอื่นๆ หรือไม่

23. ประเมินความเพียงพอของกระบวนการวัดหรือประเมินความเสี่ยงของระบบรักษาความปลอดภัย โดยพิจารณาดูว่ามีการดำเนินการต่อไปนี้ หรือไม่:

23.1 ระบุอุปสรรคและจุดอ่อนของ Internet Banking

23.2 ระบุ application และข้อมูลที่สำคัญๆ

23.3 กำหนดมาตรฐานของการควบคุมระบบรักษาความปลอดภัย (Security Control)

23.4 พิจารณาทักษะความเชี่ยวชาญของบุคลากรในองค์กรและความจำเป็นที่จะต้องจ้างผู้เชี่ยวชาญภายนอก

24. ประเมินความเพียงพอของกระบวนการสร้างหรือส่งเสริมความน่าเชื่อถือและความถูกต้องของระบบเครือข่ายและการควบคุมการเข้าถึงหรือการเรียกใช้ข้อมูล

<u>แผนสำรองฉุกเฉิน</u>

1. มีกระบวนการทำงานที่เพียงพอในการพัฒนาและสอบทานการวิเคราะห์ผลกระทบต่อธุรกิจของสถาบันการเงินหรือไม่ โดยพิจารณาว่า

1.1 Internet Banking ถือเป็นธุรกิจที่ผู้บริหารระดับสูงให้ความสำคัญหรือไม่

1.1.1 มีการกำหนดกลยุทธ์ทางการตลาดเพื่อขยายฐานลูกค้าหรือไม่

1.1.2 ปริมาณการทำธุรกรรมผ่าน Internet อยู่ในระดับใด

1.2 ผู้บริหารได้สอบทานผลกระทบต่อชื่อเสียงของสถาบันการเงินหากไม่สามารถจัดหาสินค้าและบริการทาง Internet Banking ได้ หรือไม่

2. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอในการพัฒนาและทดสอบแผนสำรองฉุกเฉินและแผนฟื้นฟูสำหรับงานด้าน Internet Banking

2.1 แผนดังกล่าวเพียงพอสำหรับการฟื้นฟู (Recovery) หรือไม่

2.2 มีการทดสอบแผนอย่างต่อเนื่องเป็นประจำหรือไม่

3. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอสำหรับการฟื้นฟูระบบงาน Internet Banking พิจารณาว่าครอบคลุมเรื่องต่อไปนี้หรือไม่

3.1 มีการทดสอบและ update แผนฉุกเฉินและแผนฟื้นฟูเป็นประจำ

3.2 กำหนดเจ้าหน้าที่บุคลากรรับผิดชอบในการจัดทำและบริหารแผนฟื้นฟูระบบ

3.3 สามารถระบุจุดที่ทำให้ระบบงานล้มเหลวได้อย่างชัดเจน

3.4 กำหนดกลยุทธ์ในการกู้กลับคืน Hardware และ Software จุดเชื่อมต่อเพื่อการสื่อสารและข้อมูล

3.5 มีสัญญา/ข้อตกลง Backup อย่างเพียงพอสำหรับบริษัทผู้ให้บริการภายนอก หรือผู้จัดหา (Supplier) และมีการทดสอบการจัดการกับ Back-up ครบถ้วนหรือไม่

3.6 ผู้บริหารระดับสูงและคณะกรรมการได้ตระหนักถึงสถานการณ์อันเป็นผลมาจากความรุนแรงของความเสียหายและ/หรือผลขาดทุนที่เกิดจากระบบงาน Internet Banking ของสถาบันการเงินเองหรือสถาบันการเงินอื่นล้มเหลวหรือขัดข้อง พร้อมทั้งได้จัดให้มีกระบวนการหรือมาตรการใดๆเพื่อโต้ตอบหรือรองรับสถานการณ์เหล่านั้นหรือไม่

3.7 Outreach strategies เพียงพอที่จะแจ้งมาตรการแก้ไขต่อสื่อและลูกค้าได้หรือไม่ ประชาสัมพันธ์ให้ทราบถึงเหตุการณ์ที่เกิดขึ้น และสถาบันการเงินจะดำเนินการอย่างไรเพื่อแก้ไขสถานการณ์ที่เกิดขึ้นนั้น

3.8 ในกระบวนการโต้ตอบ (Response processes) มีการพิจารณาถึงผลกระทบจากภาระผูกพันตามกฎหมายด้วย หรือไม่

3.9 ขั้นตอนการปฏิบัติงานเพื่อให้ผู้บริหารและองค์กรภายนอก เช่น หน่วยงานทางการ ทราบถึงการล่วงละเมิดระบบรักษาความปลอดภัยหรือไม่

4. สถาบันการเงินมีกระบวนการสอบทานผลการทดสอบแผนสำรองฉุกเฉินที่เพียงพอ ซึ่งผู้บริหารเข้ามามีส่วนร่วมต่อไปนี้ หรือไม่

4.1 กำหนดและส่งเสริมให้มีการทดสอบระบบงานและการฟื้นระบบเป็นประจำทุกปี

4.2 ล่วงรู้ถึงผลการทดสอบที่เป็นเชิงลบได้ทันเวลา

4.3 แจ้งผลการทดสอบต่อคณะกรรมการและผู้บริหารระดับสูงให้ทราบ

5. ขั้นตอนการฟื้นฟูธุรกิจสามารถชี้ถึงกรณีต่างๆที่อาจส่งผลกระทบต่อความสามารถในการให้บริการของระบบงาน Internet Banking เช่น ระบบงานล้าสมัย ภัยธรรมชาติ หรือปัจจัยที่อาจทำให้ระบบงานหยุดชะงัก และระยะเวลาของการฟื้นฟูระบบที่กำหนดไว้สอดคล้องกับระดับความสำคัญของธุรกรรม Internet Banking หรือไม่

6. มีระบบสำรอง (Backup) หรือขั้นตอนการปฏิบัติงานสำหรับผู้ใช้เพื่อให้สามารถปฏิบัติงานตามปกติต่อไปได้ในช่วงเวลาที่ระบบหยุดชะงัก

6.1 คู่มือการทำงานครอบคลุมถึงระบบสำรองหรือขั้นตอนการปฏิบัติงานหรือไม่

6.2 ผู้บริหารกำหนดขั้นตอนการดำเนินงานสำหรับการแจ้งปัญหาแก่ผู้ใช้หรือไม่

7. ผู้บริหารกำหนดแผนสำรองฉุกเฉินและทีมงานเพื่อจัดการปัญหาต่างๆ ที่อาจเกิดขึ้น และคณะกรรมการอนุมัติการกระจายอำนาจหน้าที่ความรับผิดชอบให้ทีมงานดังกล่าวโดยเขียนไว้เป็นลายลักษณ์อักษรหรือไม่

<u>บทบาทของคณะกรรมการและผู้บริหาร</u>

1. คณะกรรมการสถาบันการเงินหรือคณะกรรมการอื่นที่เกี่ยวข้อง อนุมัติระบบงานทางอิเล็กทรอนิกส์ต่างๆ ตามแผนกลยุทธ์ที่จัดทำขึ้นเป็นลายลักษณ์อักษรและผลการวิเคราะห์ความเสี่ยงหรือไม่ และการวิเคราะห์ควรครอบคลุมถึงเรื่องดังต่อไปนี้

1.1 บทบาทหน้าที่หรือขอบเขตของช่องทางการให้บริการทางอิเล็กทรอนิกส์ภายใต้แผนกลยุทธ์และแผนดำเนินงาน

1.2 ความเสี่ยงที่เกี่ยวข้องกับระบบงานทางอิเล็กทรอนิกส์ต่างๆ

2. ผู้บริหารทำการศึกษาความเป็นไปได้ของแต่ละระบบงานที่จะใช้งานในประเด็นต่อไปนี้ หรือไม่

2.1 การศึกษาความเป็นไปได้ดังกล่าวครอบคลุมทุกสถานการณ์ รวมถึงสถานการณ์ที่เลวร้ายที่สุดด้วย

2.2 ผู้บริหารระดับสูงและคณะกรรมการสอบทานผลจากการศึกษา

3. ผู้บริหารได้มีการสอบทาน Defined trade area ของสถาบันการเงินคือการกำหนดแนวทางสำหรับการเปิดบัญชี นโยบายหรือขั้นตอนการปฏิบัติงานอื่นๆที่เกี่ยวข้องใหม่หรือปรับจากแนวทาง นโยบาย หรือขั้นตอนการปฏิบัติงานที่ใช้กับการให้บริการรูปแบบเดิม ให้มีความเหมาะสมกับรูปแบบการให้บริการใหม่นี้หรือไม่

4. พิจารณาดูว่าคณะกรรมการสถาบันการเงินหรือคณะกรรมการอื่นที่เกี่ยวข้อง อนุมัติการดำเนินการใหม่ๆหรือการเปลี่ยนแปลงที่มีนัยสำคัญทางด้านการให้บริการ Internet Banking ตามแผนธุรกิจที่จัดทำขึ้นเป็นลายลักษณ์อักษรและผลการประเมินความเสี่ยง โดยพิจารณาตามหัวข้อต่อไปนี้

4.1 บริการรูปแบบใหม่เป็นการให้บริการระดับไหน ให้ข้อมูลข่าวสาร ให้บริการเดิมกับกลุ่มลูกค้าเดิม หรือเพื่อจับกลุ่มลูกค้าใหม่

4.2 มีการให้สิ่งจูงใจทางการเงินเพื่อดึงดูดความสนใจของลูกค้าผ่านบริการ Internet Banking หรือไม่

4.3 มีผลกระทบของบริการ Internet Banking ต่อฐานลูกค้า ที่อาจจะเกิดขึ้น หรือไม่

4.4 มีผลการสอบทานผลกระทบทางการเงินของบริการใหม่ที่คาดว่าจะเกิดขึ้น หรือไม่

4.5 มีการควบคุมภายในสำหรับบริการใหม่หรือไม่

4.6 มีการรายงานต่อผู้บริหารเพียงพอหรือไม่ และมีการสอบทานการรายงานดังกล่าวอย่างต่อเนื่องหรือไม่

4.7 บทบาทของพนักงานฝ่ายตรวจสอบ ฝ่ายการปฏิบัติตามกฎหมาย และฝ่ายกฎหมาย

4.8 เป็นธุรกรรมที่สามารถกระทำได้ตามกฎหมาย พรบ. ข้อบังคับ ธปท. หรือไม่

4.9 มีเรื่องอื่นๆ เช่น การบริหารจัดการระบบงานโดยบริษัทภายนอก (Outsourcing) หรือไม่

5. ผู้บริหารตระหนักถึงความจำเป็นที่จะต้องมีแผนรองรับและทีมงานโต้ตอบเหตุการณ์ต่างๆ (Incident Response Team) ในการจัดการกับสถานการณ์ที่มีการขัดข้อง (disruption) ใน Website การคุกคาม Website (mailcious tampering) หรือปัญหาอื่นๆ หรือไม่

6. ผู้บริหารจัดให้มีการควบคุมการเข้าถึง (Physical Access) อุปกรณ์คอมพิวเตอร์ Hardware และ Software อุปกรณ์สื่อสาร และสายสื่อสาร อย่างเหมาะสมหรือไม่

7. ผู้บริหารตระหนักถึงกฎหมายอื่นๆที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ หรือไม่

8. ผู้บริหารกำหนดแนวทางและวิธีปฏิบัติงานที่เหมาะสมเพื่อตรวจสอบการปฏิบัติงานตามกฎหมายต่างๆที่เกี่ยวข้องหรือไม่

9. ผู้บริหารปฏิบัติตามและ/หรือดำเนินการแก้ไขตามข้อสังเกตหรือประเด็นของผู้ตรวจสอบหรือไม่

10. ผู้บริหารจัดทำและสอบทานรายงานกิจกรรมที่ได้รับการยกเว้นต่างๆ (Exception reports) เป็นประจำหรือไม่

11. สำหรับ Stored Value Program พิจารณาว่าผู้บริหารได้กำหนดเงินทุนรองรับ หรือ Insured deposits หรือไม่

12. ผู้บริหารประเมินความเพียงพอของการทำประกันภัยของบริษัทผู้ให้บริการรายหลักๆของสถาบันการเงินหรือไม่ โดยพิจารณาจากการทำประกันภัยในเรื่องต่อไปนี้

12.1 Blanket bond

12.2 Excess Liability

12.3 Errors and Omissions

12.4 Electronic Fund Transfer

12.5 ประกันภัยประเภทอื่นที่ครอบคลุมความเสี่ยงของการให้บริการ Internet Banking

13. สำหรับระบบงานที่เชื่อมโยงกับระบบปฏิบัติการ (Operating System) หรือฐานข้อมูล ผู้บริหารได้รับผลการสอบทาน Interactive components และกระบวนการ เพื่อยืนยันถึงความสอดคล้องกัน และความปลอดภัยหรือไม่ (ขอ Topology Map มาดู)

14. ผู้บริหารตรวจสอบความถูกต้องและรายละเอียดของโปรแกรมช่วยในการวางแผนทางการเงิน (Financial planning software) การคำนวณและโปรแกรมโต้ตอบ (interactive) ระหว่างสถาบันการเงินและกลุ่มลูกค้า กับระบบงาน Internet Banking หรือไม่

15. มีการติดต่อ/เชื่อมต่อทางตรงและทางอ้อมระหว่างระบบปฏิบัติงานภายในของสถาบันการเงิน และ host ที่ให้บริการทางอิเล็กทรอนิกส์แก่ภายนอก เช่น Web Site หรือไม่

16. หารือกับผู้บริหารของสถาบันการเงิน และสอบทานแผนงานด้านเทคโนโลยี เพื่อประเมินกลยุทธ์ระยะสั้นและระยะยาวเกี่ยวกับสินค้าและการให้บริการ Internet Banking และพิจารณาเรื่องต่อไปนี้ เพื่อประเมินกระบวนการวางแผนของสถาบันการเงิน

16.1 การให้บริการ Internet Banking สอดคล้องกับพันธกิจ (mission) เป้าหมายกลยุทธ์ และแผนดำเนินงานโดยรวมของสถาบันการเงินหรือไม่

16.2 ระดับของการติดตามของคณะกรรมการและผู้บริหารเป็นอย่างไร

16.3 ผู้บริหารมีความเข้าใจมาตรฐานอุตสาหกรรมเพื่อให้มั่นใจว่าระบบงานของสถาบันการเงินสามารถทำงานร่วมกับ /เข้ากับระบบงานภายนอกได้

16.4 การวิเคราะห์ cost and benefit ของธุรกรรม Internet Banking ครอบคลุมค่าใช้จ่ายในการstart-up การดำเนินงาน การปรับรุ่นโปรแกรมระบบงาน (upgrade) การสนับสนุนลูกค้า และค่าบำรุงรักษาหรือไม่

16.5 ผู้บริหารประเมินความเสี่ยงต่อระบบรักษาความปลอดภัย ภัยคุกคาม (threat) และจุดอ่อนของระบบหรือไม่

16.6 มีการพัฒนาความรู้ความเชี่ยวชาญภายในองค์กรและการฝึกอบรมเชิงเทคนิค

16.7 ความใส่ใจของผู้บริหารต่อการติดตามและทดสอบระบบรักษาความปลอดภัยและการติดตามผลการดำเนินงาน

16.8 ความรู้ของผู้บริหารและการปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับของทางการ รวมทั้งการตีความ การทำความเข้าใจในกฎหมายที่เกี่ยวข้องกับเทคโนโลยีด้าน Internet Banking และ E-Commerce เป็นอย่างไร

17. พิจารณาว่าผู้บริหารมีกระบวนการทำงานที่เพียงพอเพื่อทำการประเมิน Product mix และปัจจัยความสำเร็จด้านการตลาดของ Internet Banking เป็นประจำหรือไม่ และการประเมินดังกล่าวรวมอยู่ในกระบวนการจัดทำแผนกลยุทธ์ด้วยหรือไม่

<u>การดำเนินงานด้านบุคลากร</u>

1. หารือกับผู้บริหาร เพื่อประเมินระดับความรู้เชิงเทคนิคของผู้บริหาร รวมทั้งความรู้เกี่ยวกับขนาดและขอบเขตของการทำธุรกรรมและการดำเนินงานด้าน Internet banking

2. ประเมินเทคโนโลยีที่เกี่ยวข้องกับโปรแกรมการฝึกอบรมและการตระหนักในเรื่องการรักษาความปลอดภัยของระบบงาน

3. ประเมินประสิทธิภาพของผู้บริหารโดย ประเมินว่าผู้บริหารได้ตระหนักในเรื่องการรักษาความปลอดภัยระบบเพียงใด

4. ประเมินความรับผิดชอบของพนักงานสถาบันการเงินและผู้ใช้ระบบงาน Internet Banking ในการ ตระหนักถึงความรับผิดชอบต่อการรักษาความปลอดภัยและการถือปฏิบัติตามนโยบายของสถาบันการเงิน

5. คณะกรรมการจัดให้มีทรัพยากรอย่างเพียงพอเพื่อรองรับธุรกรรม Internet Banking หรือไม่ โดยพิจารณาเรื่องต่อไปนี้

5.1 มีบุคลากรปฏิบัติงานกับระบบงานเพียงพอหรือไม่

5.2 มีผู้เชี่ยวชาญทางด้านเทคโนโลยีเพียงพอ และเหมาะสมกับระดับความซับซ้อนของระบบงาน Internet Banking หรือไม่ ผู้บริหารพึ่งพาความรู้ความเชี่ยวชาญเชิงเทคนิค (Technical expertise) จากบริษัทผู้ให้บริการภายนอกทั้งหมดหรือเป็นบางเรื่อง

5.3 การฝึกอบรมและพัฒนาบุคลากร

5.3.1 ผู้บริหารจัดหาโอกาสการฝึกอบรมเชิงเทคนิคให้กับพนักงานในระยะเวลาที่เหมาะสมหรือไม่

5.3.2 ผู้บริหารจัดให้มีการฝึกอบรมพนักงานทุกคนที่ได้รับผลกระทบจากระบบงานอิเล็กทรอนิกส์ เช่นพนักงานที่ให้บริการทางระบบงานดังกล่าว พนักงานในส่วนระบบฐานข้อมูล ฝ่ายตรวจสอบ ฝ่ายตรวจสอบการปฏิบัติตามกฎหมายและ ฝ่ายกฎหมาย หรือไม่ (หมายเหตุสถาบันการเงินควรจัดให้มีการฝึกอบรมพนักงานอย่างต่อเนื่อง)

6. มีการจัดทำคู่มือการปฏิบัติงานหรือวิธีปฏิบัติเกี่ยวกับ Internet Banking ของแต่ละฝ่ายงานหรือส่วนงานที่เกี่ยวข้องหรือไม่

<u>ด้านการควบคุมภายในและการรักษาความปลอดภัย</u>

<u>ระบบรักษาความปลอดภัย</u>

1. ถ้าระบบงาน Internet Banking ของสถาบันการเงินเป็น Turnkey คือ ซื้อ Software Package สำเร็จรูปซึ่งผลิตโดยบริษัทผู้แทนจำหน่าย Software หรืออยู่ในความดูแลของบริษัทผู้ให้บริการ ผู้ตรวจสอบควรสอบทานเอกสารที่เกี่ยวข้องกับการฝึกอบรมและระบบรักษาความปลอดภัยที่จัดหาโดยบริษัทผู้แทนจำหน่าย Software หรือบริษัทผู้ให้บริการนั้นๆ รวมทั้งพิจารณาดูว่าพนักงานของสถาบันการเงินได้ปฏิบัติตามขั้นตอนการดำเนินงานและการรักษาความปลอดภัยที่กำหนดไว้สำหรับแต่ละระบบงานอย่างถูกต้องเหมาะสมหรือไม่ โดยพิจารณาเรื่องต่อไปนี้

1.1 พนักงานมีความคุ้นเคยกับการควบคุมหลักของบริษัทผู้ผลิตหรือไม่

1.2 Workstations ที่เชื่อมต่อกับระบบงานของบริษัทผู้ให้บริการเพื่อการปฏิบัติงาน (Administrative procedures) หรือเพื่อการโอนข้อมูล และข้อมูลถูกเก็บรักษาไว้ในที่ที่ปลอดภัยโดยมีการเข้ารหัส มีการใช้เทคนิคการควบคุมการเข้าถึงต่างๆ ขั้นตอนการตรวจสอบรายการโดยบุคคล 2 ฝ่าย (Dual verification procedures) หรืออื่นๆ เป็นต้น

2. สถาบันการเงินมีโปรแกรมการรักษาความปลอดภัยทางด้าน Internet Banking อย่างเพียงพอ โดยครอบคลุมเรื่องดังต่อไปนี้หรือไม่

2.1 การเข้าถึง การป้องกัน การเปิดเผยข้อมูลที่เป็นความลับของลูกค้า

2.2 วิธีกำหนดการให้สิทธิบุคคลทำรายการทางบัญชีหรือส่งคำสั่งหรือข้อมูล

2.3 ประเภทของข้อมูลที่สามารถ share ให้กับบุคคลที่สามได้

2.4 ขีดความสามารถของผู้ให้บริการ (บุคคลที่สาม) ในการเข้าถึงหรือติดตามการส่งข้อมูลทางอิเล็กทรอนิกส์ระหว่างสถาบันการเงินกับลูกค้า

3. มีการปรับปรุง นโยบายและขั้นตอนการดำเนินงานที่ดูแลการเข้าถึงการเปิดเผยข้อมูลความลับของลูกค้าให้เหมาะกับกำลังความสามารถของสื่ออิเล็กทรอนิกส์ ในประเด็นต่อไปนี้หรือไม่

3.1 นโยบายระบุประเภทของข้อมูลที่สามารถใช้ร่วมกับบุคคลที่สาม เช่น บริการที่ไม่ใช่เงินฝาก discount brokerage services เป็นต้น

3.2 สัญญาหรือข้อตกลงกับบุคคลที่สามครอบคลุมแนวทางเพื่อการรักษาความลับของข้อมูลที่เป็นความลับ หรือไม่

4. มีการกำหนดแนวทางควบคุมบริษัทผู้ให้บริการ (เช่น บริษัทผู้จัดหาระบบงานทางอิเล็กทรอนิกส์ บริษัทประมวลผลข้อมูล เป็นต้น) ในการเข้าถึงหรือติดตามการส่งข้อมูลระหว่างสถาบันการเงินกับลูกค้าหรือไม่ และมีการรวมแนวทางดังกล่าวเข้าไปเป็นส่วนหนึ่งของสัญญาหรือข้อตกลงการสนับสนุน /ให้บริการ (Service Arrangement) หรือไม่

5. ผู้บริหารระดับสูงกำหนดระดับ/อำนาจในการเข้าถึงข้อมูลหรือระบบงานให้กับพนักงาน เจ้าหน้าที่ของบริษัทผู้แทนจำหน่ายระบบ ลูกค้า และผู้ใช้ระบบงานกลุ่มอื่นๆ หรือไม่ และมีการบังคับใช้และสอบทานระดับ/อำนาจในการเข้าถึงดังกล่าวเป็นประจำหรือไม่

6. พิจารณาถึงวิธีการที่สถาบันการเงินใช้กำหนดหลักเกณฑ์/ข้อกำหนดเกี่ยวกับบุคคลที่จะสามารถขอทำธุรกรรมทางบัญชี หรือส่งคำสั่งหรือข้อมูลที่เกี่ยวข้องได้

7. มีการจัดหาโครงการสำหรับการให้บริการลูกค้า การสนับสนุนและการศึกษา พิจารณาดูว่ามีกิจกรรมสนับสนุนหรือควบคุมดังต่อไปนี้หรือไม่

7.1 มีการจัดทำเอกสารหรือคู่มือประกอบเกี่ยวกับการรักษาความปลอดภัยของระบบงาน การควบคุมและพันธะผูกพันต่างๆ ให้กับลูกค้าหรือไม่

7.2 มีโปรแกรมที่ค้นหา/ระบุ ถึงปัญหาที่เกิดซ้ำซากในระยะเวลาอันควรหรือไม่

8. พิจารณาดูว่าสถาบันการเงินกำหนดให้ลูกค้าจัดส่งใบมอบอำนาจสำหรับผู้รับเงินแต่ละราย สำหรับกรณีเช่น การชำระค่าสินค้าและบริการ การโอนเงิน เป็นต้น

8.1 พิจารณาดูว่าสถาบันการเงินจะมีการตรวจสอบความถูกต้องตามกฎหมายของผู้รับเงินแต่ละรายอย่างไร

8.2 สถาบันการเงินมีแนวทางที่สมเหตุสมผลสำหรับการเพิ่มหรือลดจำนวนผู้รับเงินหรือไม่

9. ดูว่ามีเครื่องมือป้องกันและตรวจจับธุรกรรม/รายการที่ซ้ำซ้อนภายในแต่ละระบบงานหรือไม่

10. มีการเปิดเผยข้อมูลทางด้านการรักษาความปลอดภัยระบบ การควบคุมระบบ และพันธะผูกพันต่างๆ ให้แก่ลูกค้าอย่างเพียงพอเหมาะสมหรือไม่

11. มีขั้นตอนการกระทบรายการที่ทำเป็นประจำรวมอยู่ในกระบวนการทำรายการ (Full scope of transactional capabilities) หรือไม่

12. ขั้นตอนดังกล่าวมีความเหมาะสมสอดคล้องกับบัญชีแยกประเภทและบัญชีย่อยต่างๆ หรือไม่

<u>การจัดการเกี่ยวกับรหัส</u>

1. ประเมินความเพียงพอของกระบวนการปฏิบัติงานเกี่ยวกับรหัสที่พนักงานและลูกค้าใช้เข้าถึงระบบงาน Internet Banking หรือ Workstation ที่ใช้เชื่อมต่อกับระบบของบริษัทผู้ให้บริการในระยะไกล โดยพิจารณาเรื่องต่อไปนี้

1.1 ขั้นตอนการดำเนินงานเพื่อจำกัดให้เฉพาะพนักงานที่ได้รับอนุญาตเท่านั้น เข้าถึงระบบงาน Internet Banking และข้อมูลได้ รวมถึงกระบวนการออกหรือกำหนดรหัสผ่านให้ลูกค้า

1.2 หลักเกณฑ์ต่างๆเกี่ยวกับรหัส เช่น ความยาวของรหัส หลีกเลี่ยงการใช้รหัสที่สามารถคาดเดาได้ง่าย หรือใช้ default password เช่นเลขที่บัตรประชาชน เลขที่บัญชี การใช้ตัวอักษร เป็นต้น

1.3 ขั้นตอนการดำเนินงานในการตั้งค่ารหัสใหม่ ในกรณีที่ลูกค้าลืมรหัส พิจารณาดูว่ามีขั้นตอนการดำเนินงานที่สามารถป้องกันการเข้าถึง User ID หรือเลขรหัสโดยไม่ได้รับอนุญาตอย่างเพียงพอ

1.4 มีการ Logoff อัตโนมัติออกจากระบบ หากไม่มีการใช้งานระบบในช่วงเวลาหนึ่ง

1.5 จำนวนครั้งของการพยายามเข้าถึงระบบงานอย่างล้มเหลว ก่อนที่ระบบงานจะปฏิเสธสิทธิการเข้าถึงดังกล่าว

1.6 รหัสมีวันหมดอายุโดยอัตโนมัติหรือไม่

1.7 ขั้นตอนการกำหนดรหัสใหม่

1.8 ขั้นตอนสำหรับกรณีที่ลูกค้าลืม Password

1.9 การเก็บไฟล์รหัสและข้อมูลต่างๆ อย่างปลอดภัย เช่น มีการเข้ารหัสไฟล์ หรือไม่ และอยู่ในความดูแลของสถาบันการเงินหรือบริษัทผู้แทนจำหน่าย (Vendor)

2. ประเมินความเพียงพอของกระบวนการทำงานที่รหัสจะนำมาใช้ในการแสดงตนของผู้ใช้งาน โดยพิจารณาว่า กระบวนการทำงานครอบคุลมเรื่องต่อไปนี้หรือไม่

2.1 การควบคุมระบบงาน ซึ่งหมายรวมถึงการใช้รหัสผ่านกับเทคนิคการแสดงตนอื่นๆ

2.2 รหัสที่ใช้ในการ log-in ถูกใช้เพื่อควบคุมการเข้าถึงหรือการเรียกใช้ระบบงานและแสดงตนของผู้ใช้

2.3 รหัสที่ใช้ในการ log-in ถูกใช้เพื่อการเข้าถึงหรือการเรียกใช้ระบบเครือข่ายเปิด (Internet) หรือไม่ ถ้าใช่ พิจารณาว่าสถาบันการเงินมีเทคนิคการควบคุมอื่นเพื่อใช้ในการแสดงตนหรือไม่

Firewalls

1. พิจารณาว่าสถาบันการเงินมีกระบวนการทำงานที่ดีที่สามารถยืนยันได้ว่ามีการควบคุมอย่างเพียงพอบนช่องทางที่เชื่อมต่อระหว่าง Website กับระบบเครือข่ายภายในหรือการระบบคอมพิวเตอร์ของสถาบันการเงิน หรือไม่

2. สถาบันการเงิน หรือผู้ให้บริการแก่สถาบันการเงินจัดให้มี Firewall เพื่อป้องกัน Website ของสถาบันการเงินหรือไม่ โดยพิจารณาเรื่อง

2.1 การกำหนดค่า Firewall: ขอดู Firewall Configuration

2.2 การจัดการดูแลเกี่ยวกับ Firewall และการใช้งาน

2.2.1 รายชื่อผู้รับผิดชอบ Firewall: ที่ OS และ Applications ทุกตัวที่มีอยู่บน Firewall

2.2.2 ขั้นตอนการเปลี่ยน USER ID และ Password ของ ADMINS ที่ดูแล Firewall : ความถี่ของการเปลี่ยนแปลง รูปแบบของการเปลี่ยนแปลง (บังคับเปลี่ยนโดยอัตโนมัติหรือไม่) มีการใช้ทะเบียนคุมการเปลี่ยนรหัสหรือไม่

2.2.3 มีการป้องกันไวรัสที่อุปกรณ์ Firewall หรือไม่

3. พิจารณาว่ามีการบริหารกระบวนการทำงานที่สามารถยืนยันได้ว่า Firewalls สามารถป้องกันการเข้าถึงหรือการเรียกใช้ระบบเครือข่ายภายในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือไม่

4. ถ้าสถาบันการเงินซื้อ Firewall จากบริษัทภายนอก พิจารณาว่าสถาบันการเงินมีกระบวนการทำงานที่เพียงพอสำหรับการกำหนดความรับผิดชอบของบริษัทผู้ให้บริการอย่างชัดเจนถูกต้องหรือไม่

5. พิจารณาความเพียงพอของการปฏิบัติงานด้านการติดตั้งและการกำหนดค่า Firewall :

5.1 ขั้นตอนการปฏิบัติงานสำหรับการควบคุมการเปลี่ยนแปลง Software มีความเหมาะสมหรือไม่

5.2 บริษัทผู้ให้บริการ ให้บริการซ่อมแซม และปรับรุ่น (upgrade) ในเวลาอันควร และผู้บริหารใช้งานได้ทันเวลาหรือไม่

5.3 มีการทดสอบ การกำหนดค่า Firewall ที่มีการเปลี่ยนแปลง ก่อนใช้งาน หรือไม่

5.4 มีการใช้การควบคุมของระบบปฏิบัติการ (Operating System control features) หรือไม่

5.5 การกำหนดค่า Default ของโปรแกรมระบบปฏิบัติการมีความเพียงพอเหมาะสมหรือไม่

6. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอสำหรับ

6.1 ทดสอบการเจาะระบบ (Penetration testing) และการรับรอง (Certification) หรือไม่

6.2 สอบทานคุณสมบัติของบริษัท/บุคลากรที่ทำการรับรอง (Certification) หรือไม่

7. สถาบันการเงินมีกระบวนการทำงานที่ใช้ประเมินความเพียงพอของการควบคุมทางกายภาพ (physical controls) เพื่อจำกัดการเข้าถึง firewall server และอุปกรณ์อื่นๆอย่างมีประสิทธิภาพหรือไม่

8. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอในการกำหนดและแยกแยะการเข้าถึงจากระยะไกลที่ไม่ได้ผ่าน Firewall และวิธีที่ผู้บริหารใช้ติดตามและควบคุมการเข้าถึงนั้น หรือไม่

9. พิจารณาความเพียงพอของกระบวนการทำงานเพื่อจำกัดการเข้าถึงเอกสารเกี่ยวกับการกำหนดค่า Firewall

10. มีการวิเคราะห์ Pattern ของ log บนเครื่อง Firewall เพื่อติดตามการเข้าสู่ระบบธนาคารหรือไม่ รวมทั้งพิจารณาความถี่ของการวิเคราะห์ การรายงานต่อผู้บริหารหรือบุคคลที่เกี่ยวข้อง และผู้รับผิดชอบในการจัดทำรายงาน

<u>การรักษาความปลอดภัยทางกายภาพ (Physical Security)</u>

1. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอในการแจกแจงระบบรักษาความปลอดภัยทางกายภาพสำหรับ Hardware Software และอุปกรณ์การสื่อสารที่เกี่ยวข้องกับระบบงาน Internet Banking ซึ่งรวมถึง

1.1 การจัดตั้ง Network Server ในสถานที่ปลอดภัยหรือไม่

1.2 มีการป้องกันการเข้าถึงหรือการเข้าใช้อุปกรณ์ต่างๆโดยไม่ได้รับอนุญาตอย่างไร

1.3 มีการรักษาความปลอดภัยในอุปกรณ์ของบริษัทผู้ให้บริการอย่างไร

1.4 มีการควบคุมทางกายภาพที่เหมาะสมสำหรับศูนย์ข้อมูลหรือสถานที่จัดเก็บอุปกรณ์และเอกสารอย่างไร

2. มีการแบ่งแยกหน้าที่ระหว่างบุคคลที่พัฒนาระบบกับบุคคลที่ปฏิบัติการกับระบบงาน หรือไม่

2.1 ใครเป็นผู้ดูแล OS บน Server ต่างๆ

2.2 ใครเป็น SUPER ADMIN และ ADMIN ของแต่ละ Applications บน Server ต่างๆ (ควรจะแยกบุคคลที่ดูแล OS และ Applications บน Server แต่ละ Server)

3. การจัดการกับรหัสของ SUPER ADMIN และ ADMINS ของแต่ละ Server เป็นอย่างไร

<u>การตรวจสอบความถูกต้องของรายการ (Transaction Verification)</u>

สถาบันการเงินมีกระบวนการทำงานที่เหมาะสมในการตรวจสอบความถูกต้องของรายการเพื่อหลีกเลี่ยงข้ออ้างในการปฏิเสธการทำรายการของลูกค้า

<u>การเข้ารหัสและการรักษาความลับของข้อมูล (Encryption and Confidentiality)</u>

1. ถ้ามีการใช้ E-mail สื่อสารกับลูกค้า พิจารณาว่ามีการเข้ารหัสการสื่อสารนั้นๆ หรือไม่ มีคำเตือนที่แจ้งลูกค้าและพนักงานทราบว่าไม่ควรส่งข้อมูลที่เป็นความลับผ่านทาง E-mail หรือไม่

2. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอในการคัดเลือกวิธีการเข้ารหัสที่เหมาะสมกับสภาวะแวดล้อม และโครงสร้างการเข้ารหัสที่เลือกอยู่บนพื้นฐานของ public key private key หรือ hybrid encryption system หรือไม่

2.1 ประเภทของ algorithm ที่ใช้และวัตถุประสงค์ของการใช้

2.2 สถาบันการเงินใช้ proprietary หรือ unknown algorithm

2.3 ความยาวของกุญแจที่ใช้เข้ารหัส

2.4 การเข้ารหัสถูกใช้ในการรักษาความปลอดภัยของรหัสในระหว่างการส่งข้อมูลหรือการเก็บข้อมูลหรือไม่

2.5 การเข้ารหัสถูกใช้เพื่อป้องกันข้อมูลชนิดพิเศษ (Sensitive data) ที่จัดเก็บไว้หรือไม่

3. ถ้าสถาบันการเงินทำธุรกรรมทางการเงินระหว่างประเทศ พิจารณาว่าสถาบันการเงินตระหนักถึงนโยบาย กฎหมายระหว่างประเทศและข้อจำกัดที่ใช้ควบคุมการค้า การเงินระหว่างประเทศ และการใช้เทคโนโลยีการเข้ารหัสอื่นๆ หรือไม่

4. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอทางด้านการเก็บและใช้ข้อมูลส่วนบุคคลที่จำเป็นต่อการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า หรือไม่

<u>การป้องกันไวรัสทางคอมพิวเตอร์</u>

1. สถาบันการเงินมีมาตรการที่เพียงพอในการป้องกันComputer Virus บนระบบงาน Internet Banking และระบบงานที่เชื่อมต่อกับภายนอกต่างๆ หรือไม่

2. สถาบันการเงินมีกระบวนการทำงานอย่างเพียงพอเพื่อตรวจจับและป้องกัน Virus ในระบบงาน Internet Banking โดยพิจารณาในเรื่องต่อไปนี้

2.1 ผู้ใช้ตระหนักถึงอันตรายจากไวรัส หรือไม่

2.2 การประเมินความเสี่ยงและรายงานตรวจสอบครั้งล่าสุดพบประเด็น ข้อบกพร่องในการควบคุม Virus หรือไม่

2.3 ความถี่ในการปรับปรุงรุ่นของโปรแกรม Anti-virus และคำนิยาม และมีการติดตั้ง Versions หรือ Release ล่าสุดหรือไม่

3. สถาบันการเงินมีกระบวนการทำงานที่เพียงพอในการตรวจจับและป้องกัน Virusหรือไม่ โดยพิจารณาว่า

3.1 การแจกจ่าย Software ที่ใช้ตรวจจับ Virus ทำโดยการ Download จาก Server ของสถาบันการเงินหรือไม่

3.2 กระบวนการแจกจ่าย Software ของสถาบันการเงินมีการตรวจจับและป้องกัน Virus หรือไม่

<u>ลายมือชื่ออิเล็กทรอนิกส์</u>

1. ผู้บริหารกำหนดให้ใช้ลายมือชื่ออิเล็กทรอนิกส์ในการแสดงตนของสถาบันการเงิน ผู้ใช้ และในการทำรายการธุรกรรมหรือไม่

2. บริษัทผู้ให้บริการภายนอกเป็นผู้บริหารหรือผู้ให้การรับรองลายเซ็นต์อิเล็กทรอนิกส์หรือไม่

3. ถ้าสถาบันการเงินทำหน้าที่เป็น Certificate Authority ให้พิจารณาประเด็นต่อไปนี้

3.1 ระบบลายมือชื่ออิเล็กทรอนิกส์เป็นระบบเปิดหรือระบบปิด

3.2 สถาบันการเงินจัดทำนโยบายและขั้นตอนปฏิบัติงานสำหรับการออก ต่ออายุ และยกเลิกใบรับรอง หรือไม่

3.3 วิธีการที่สถาบันการเงินสร้าง (establish) และตรวจสอบความน่าเชื่อของสมาชิก

3.4 ระบบรายงานการปฏิบัติงานมีความเพียงพอที่จะช่วยในการค้นหา (Directory Lookup) และการตรวจสอบ (เช่น ประทับเวลา)

3.5 สิ่งที่ Certificate Authorityจัดให้มีหรือขอบเขตหน้าที่ของ Certificate Authority เพื่อทำให้เกิดความปลอดภัยที่เพียงพอหรือไม่ โดยให้พิจารณาว่า

3.5.1 การควบคุมเพื่อป้องกัน servers ที่ใช้เก็บข้อมูลและรายชื่อ (directories)

3.5.2 แผนฉุกเฉินสามารถรองรับความต้องการของลูกค้าในระหว่างที่ระบบงานล้มเหลวหรือเสียหาย

3.5.3 สถาบันการเงินกำหนดความหมายเชิงกฎหมายในการนำเสนอหน้าที่หลักปฏิบัติของ Certificate Authority

3.5.4 Certificate Authority ปฏิบัติตามมาตรฐานที่กำหนดโดย NIST, IETF หรือไม่

3.5.5 มีกระบวนการตรวจสอบหรือไม่

3.5.6 มีข้อจำกัดในการออกใบรับรองในเรื่องต่อไปนี้ หรือไม่

- จำนวนรายการ
- ประเภทของรายการ
- วันหมดอายุ

3.5.7 CA กำหนดระดับชั้นของใบรับรองตามความพิเศษของข้อความหรือรายการ

3.5.8 สถาบันการเงินทำการวิเคราะห์ cost/benefit ของการเป็น CA เป็นประจำหรือไม่

<u>เครื่องมือทางชีวภาพที่ใช้ในการแสดงตัวตน (Biometric device)</u>

1. สถาบันการเงินใช้ Biometric devices เพื่อการแสดงตนของผู้ใช้ระบบงาน หรือไม่

2. มีการประเมินความเสี่ยงหรือวิเคราะห์ Cost/benefit ของการใช้ Biometric devices เพื่อวัตถุประสงค์ของการแสดงตนหรือไม่

3. มีการจัดทำนโยบายและ biometric tolerance ที่ยอมรับได้ สำหรับการแสดงตนของรายการที่จะถูกประมวลผลหรือไม่

4. ผู้บริหารได้สอบทานรายงานการวัดผลการดำเนินงานเชิงสถิติของเครื่องมือ biometric devices ที่ใช้เพื่อการแสดงตน หรือไม่

<u>การปรับรุ่นและแจกจ่ายโปรแกรมระบบงาน (Software Distribution)</u>

1. มีการควบคุมการเปลี่ยนแปลงโปรแกรมหรือไม่ และมีการป้องกันการเปลี่ยนแปลงโปรแกรม Software ที่ไม่ได้รับอนุญาตอย่างเพียงพอหรือไม่ (บนเครื่อง Server)

1.1 มีขั้นตอนอนุมัติการเปลี่ยนแปลงโปรแกรมหรือไม่ และขั้นตอนดังกล่าวจัดได้ว่าเป็นส่วนสำคัญในกระบวนการพัฒนาหรือไม่

1.2 มีขั้นตอนการปฏิบัติงานสำหรับการปรับปรุงแก้ไข Software ฉุกเฉินและชั่วคราว และการออก software ใหม่

1.3 ขั้นตอนการเปลี่ยนแปลงโปรแกรม มีเอกสารที่เกี่ยวข้องที่จะใช้สำหรับติดตามตรวจสอบและเอกสารดังกล่าวเพียงพอสำหรับการสนับสนุนการเปลี่ยนแปลงดังกล่าวหรือไม่

2. ประเมินการควบคุมการปรับเปลี่ยนรุ่น (version control) และขั้นตอนการแจกจ่าย software ทางด้าน Internet banking ในเรื่องต่อไปนี้

2.1 ความเพียงพอของวิธีการแจกจ่าย Software (download ให้โดยอัตโนมัติหรือผู้ใช้เป็นคน download หรือจัดส่ง software แบบ manual)

2.2 มีการควบคุมอย่างเพียงพอเพื่อป้องกันการติด virus ระหว่างการแจกจ่าย software และเพื่อให้มั่นใจในความถูกต้องของ Software หรือไม่

2.3 มีการทดสอบ software ก่อนแจกจ่ายหรือไม่

3. ถ้าสถาบันการเงินเป็นผู้ดำเนินการพัฒนาระบบงาน Internet Banking ด้วยตนเอง (in-house) พิจารณาดูว่าสถาบันการเงินมีการ ปรับรุ่น (upgrade) Software ที่ใช้กับ Internet Banking เป็นประจำหรือไม่ เพื่อให้เข้ากับ การปรับรุ่น Softwareของบริษัทผู้แทนจำหน่าย และสามารถชี้ให้เห็นถึงจุดอ่อนด้านความปลอดภัยด้วยหรือไม่

4. โปรแกรม Anitvirus บน Server ได้รับการปรับรุ่นให้เป็นปัจจุบันหรือไม่ ใครเป็นผู้ดำเนินการ update และวิธีดำเนินการปรับรุ่น (manual หรือไม่)

<u>ด้านการตรวจสอบและสอบทาน</u>

1. แผนการตรวจสอบ (Audit Program) โดยผู้ตรวจสอบภายในและภายนอก ครอบคลุมถึงธุรกรรมและระบบงาน Internet Banking โดยครอบคลุมถึงเรื่องความเสี่ยงทาง

การเงิน ความเสี่ยงจากการดำเนินงาน และความเสี่ยงต่อชื่อเสียงของสถาบันการเงินหรือไม่ และขอบเขตการตรวจสอบภายในและภายนอกรวมถึงระบบงาน Internet Banking หรือไม่

2. แผนการตรวจสอบ ครอบคลุมถึงการสอบทานระบบควบคุมและการกระทบยอดรายการธุรกรรมที่เกิดขึ้นผ่านระบบงาน Internet Banking และมีขั้นตอนการแก้ปัญหาเหตุการณ์ข้อยกเว้นต่างๆ (Exception resolution procedures) หรือไม่

3. พิจารณาระดับของการสอบทานผลการตรวจสอบ (Audit review) ผลการดำเนินงานของบริษัทผู้ให้บริการเทียบกับเงื่อนไขในสัญญา และสอบทานผลการตรวจสอบ (Audit Result)

4. มีการปรับปรุงแผนการตรวจสอบภายในและภายนอก (Audit Program) ให้ครอบคลุมธุรกรรมทางอิเล็กทรอนิกส์และระบบงานทางอิเล็กทรอนิกส์ หรือไม่

4.1 ฝ่ายตรวจสอบมีพนักงานเพียงพอที่จะดูแลธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งขอบเขตและความถี่ในการตรวจสอบเพียงพอหรือไม่ (แผนการตรวจสอบควรครอบคลุมและสามารถปกป้องสินทรัพย์ทางการเงินและข้อมูล รวมทั้งความน่าเชื่อถือของระบบ)

4.2 สอบทานประเด็นที่เป็นนัยสำคัญจากรายงานตรวจสอบครั้งล่าสุด เพื่อประเมินขีดความสามารถของผู้บริหารในการแก้ไขข้อบกพร่อง

5. มีการจัดทำร่องรอยการทำรายการเพื่อการตรวจสอบ (Audit Trail) สำหรับทุกระบบงานหรือไม่

6. มีการกำหนดให้มีร่องรอยการทำรายการเพื่อการตรวจสอบ (Audit Trail) และขั้นตอนการตรวจสอบครอบคลุมทางเดินธุรกรรม (ตั้งแต่เริ่มต้นจนจบ) ที่เกิดขึ้นภายในระบบงานหรือไม่

7. มีแผนการสอบทานระบบงานแต่ละระบบอย่างต่อเนื่องหรือไม่ และครอบคลุมด้านต่อไปนี้หรือไม่

7.1 เนื้อหาหรือองค์ประกอบของระบบงาน (Content)

7.2 ความเหมาะสมอย่างต่อเนื่อง (Continued appropriateness)

7.3 ความถูกต้องครบถ้วน (Accuracy and integrity)

7.4 การควบคุมและการรักษาความปลอดภัย (Security and controls)

7.5 การปรับรุ่นระบบและความล้าสมัย (System updates and obsolescence)

7.6 กำลังความสามารถของระบบ (System capacity)

7.7 ทิศทางกลยุทธ์ (Strategic direction)

8. การประเมินความเสี่ยงหรือการตรวจสอบเป็นไปตามหลักปฏิบัติเพื่อการบริหาร (key management practices) ที่กำหนดไว้หรือไม่ สอบทานรายงานที่เกี่ยวข้อง

9. การตรวจสอบภายในรวมอยู่ในขั้นตอนการวางแผนและการนำระบบงาน Internet Banking ไปใช้หรือไม่

10. ขอรายงานการตรวจสอบภายในและภายนอกที่ประเมินกระบวนการดูแลบริษัทผู้ให้บริการภายนอก หรือการรักษาสัมพันธภาพกับบริษัทผู้เชี่ยวชาญด้าน IS และเทคโนโลยี

11.ขอรายงานผู้บริหารหรือสัมภาษณ์ผู้บริหารเพื่อพิจารณาว่ามีการประเมินการควบคุมบริษัทผู้ให้บริการหรือไม่

11.1 การควบคุมรายงานด้านระบบรักษาความปลอดภัย: ผู้บริหารเข้าใจและประเมินระบบรักษาความปลอดภัยของการควบคุมการเข้าถึง/เรียกใช้ระบบงาน การแสดงตนของผู้ใช้ และการรักษาความเป็นส่วนตัวของข้อมูลหรือไม่

11.2 การติดตามระบบรักษาความปลอดภัยของบริษัทผู้ให้บริการในการตรวจจับการบุกรุกแบบ Real-time และทดสอบการเจาะระบบของ Offsite หรือ in-house network หรือไม่

11.3 ระดับของบริการ (Service level) และความสามารถของบริษัทผู้แทนจำหน่ายระบบงาน (Vendor ability) เป็นไปตามมาตรฐานที่ตกลงกันไว้หรือไม่

11.4 มีการทดสอบโดยบริษัทผู้ให้บริการก่อนแจกจ่าย Product หรือไม่

11.5 มีกระบวนการตรวจจับ virus หรือไม่

11.6 มีแผนฉุกเฉินและแผนฟื้นฟู หรือไม่

12. ถ้าสถาบันการเงินว่าจ้างบริษัทผู้เชี่ยวชาญภายนอกให้ประมวลผลรายการ Internet Banking ให้พิจารณาชื่อเสียงของบริษัทดังกล่าว และสถาบันการเงินได้รับและสอบทานรายงานการตรวจสอบบริษัทดังกล่าวโดยหน่วยงานทางการหรือไม่

13. ฝ่ายตรวจสอบสอบทานความสอดคล้องระหว่างมาตรฐานการรักษาความปลอดภัยและนโยบายคุ้มครองข้อมูลส่วนบุคคลกับการปฏิบัติงานจริงของสถาบันการเงินหรือไม่

<u>ด้านการติดตามในระบบสารสนเทศและการสื่อสาร</u>

<u>การติดตามระบบรักษาความปลอดภัยระบบ (Monitoring)</u>

1. หารือกับผู้บริหารถึงเทคนิคที่ใช้ในการติดตามการรักษาความปลอดภัยของระบบงาน Internet Banking และสอบทานรายงานต่างๆ เช่น

1.1 ผลและขอบเขตการทดสอบการเจาะระบบ (Penetration Testing)

1.2 ข้อมูลเกี่ยวกับการละเมิดระบบรักษาความปลอดภัย

1.3 รายงานการตรวจจับการบุกรุกแบบ Real-time

1.4 รายงานการล่วงละเมิดระบบรักษาความปลอดภัย (Security breach) หรือการบุกรุกระบบ

2. มีการใช้ Software วิเคราะห์ระบบรักษาความปลอดภัยหรือไม่ และให้ทำการจดบันทึก ขีดความสามารถของ Software ดังกล่าวไว้ด้วย

3. ผู้บริหารดำเนินการเองหรือจ้างบริษัทผู้ให้บริการภายนอกมาทดสอบโดยการเจาะระบบ (penetration testing) ทั้งนี้ผู้ตรวจสอบควรจะประเมินดูว่า

3.1 บุคคลที่ทำการทดสอบเจาะระบบเป็นบุคคลที่มีคุณสมบัติและอยู่ในสถานภาพที่เหมาะสมหรือไม่

3.2 มีการทำสัญญากับเจ้าหน้าที่ที่ทำการทดสอบเจาะระบบ อย่างเหมาะสมหรือไม่

3.3 ทำการทดสอบการเจาะระบบอย่างน้อยปีละครั้ง หรือตามความถี่ที่เป็นที่ยอมรับโดยขึ้นกับการประเมินความเสี่ยงและความทนทานต่อความเสี่ยง (risk tolerance) ของผู้บริหารหรือไม่

3.4 มีการควบคุมการทดสอบข้อมูลและเอกสารการทดสอบอย่างเคร่งครัดหรือไม่

3.5 ผู้บริหารดำเนินการสอบทานผลการทดสอบระบบหรือไม่

4. พิจารณาวิธีที่ผู้บริหารติดตามและตรวจจับการบุกรุกระบบเครือข่ายภายในและเครือข่ายภายนอก

4.1 ใช้ Software เพื่อติดตามเพื่อ Network traffic แบบ real-time หรือไม่

4.2 การติดตาม Network traffic อยู่ในความรับผิดชอบของเจ้าหน้าที่ที่มีคุณสมบัติเหมาะสมหรือไม่

4.3 มีการเก็บรักษาและสอบทาน Activity log เป็นประจำหรือไม่

4.4 ด้วยเทคนิคการตรวจจับการบุกรุกที่ใช้อยู่ในปัจจุบันมีความสามารถที่จะแจ้งผู้ดูแลระบบเครือข่าย (Network Administrators) หรือเจ้าหน้าที่รักษาความปลอดภัยระบบเมื่อเกิดเหตุการณ์ผิดปกติได้ทันทีหรือไม่

4.5 ในส่วนของนโยบายด้านรักษาความปลอดภัยระบบ ได้มีการกำหนดเหตุการณ์ผิดปกติที่ควรจะรายงาน (Reportable events) หรือไม่

4.6 ได้มีการสอบทานเหตุการณ์ต่างๆ ที่เกิดขึ้น และรายงานผลตามสายการบังคับบัญชาอย่างถูกต้องเหมาะสมหรือไม่

4.7 มีกระบวนการทำงานที่สร้างความมั่นใจในความเหมาะสมของระดับการบริหาร จัดการ และสิทธิอำนาจของผู้ใช้ภายนอกองค์กรหรือไม่

4.8 มีการลงโปรแกรม Sniffer หรือ Network analyser อยู่บนเครื่อง PC ที่เป็น Clients หรือไม่ (เพราะการกระทำดังกล่าวอาจทำให้เกิดการรั่วไหลของข้อมูลหรือจุดอ่อนของระบบได้)

4.9 สำหรับเครื่องยี่ห้อ SUN ที่ใช้ OS Solaris นั้น ธนาคารดำเนินการลบทิ้ง Software Component หรือ Utilities ที่ไม่ได้ใช้ออก หรือปรับ Permission ให้เหมาะสมหรือไม่

5. มีการสอบทานรายงานหรือสอบถามผู้บริหารเพื่อพิจารณาว่าสถาบันการเงินเคยประสบเหตุการณ์ดังต่อไปนี้หรือไม่ หากเคย ควรตรวจสอบดูว่ามีเอกสารประกอบเพียงพอหรือไม่ ในเรื่องต่อไปนี้

5.1 การเปลี่ยนแปลง home page ของสถาบันการเงิน

5.2 การเข้าถึงโดยไม่ได้รับอนุญาตจากแหล่งภายนอกและภายในสถาบันการเงิน

5.3 ความสูญเสียหรือความเสียหายทางการเงินที่เป็นผลจากการบุกรุกโดยไม่ได้รับอนุญาต

6. ผู้บริหารได้จัดให้มีขั้นตอนการปฏิบัติงานเพื่อโต้ตอบเหตุการณ์ต่างๆ (incidents) และจัดการกับการบุกรุกที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพหรือไม่

6.1 มีการกำหนดนโยบายด้านการรักษาความปลอดภัยครอบคลุมการเข้าถึงหรือการเรียกใช้ระบบงานจากระยะไกลหรือไม่

6.2 พนักงานได้ตระหนักถึงความสำคัญของนโยบายและการปฏิบัติตามนโยบายหรือไม่ มีการติดตามการปฏิบัติตามนโยบายของพนักงานหรือไม่

6.3 มีการจัดเก็บรักษาทะเบียนบันทึกทางคอมพิวเตอร์เพื่อติดตามการเข้าถึงหรือการเรียกใช้ระบบงานจากระยะไกลหรือไม่

7. มีการจัดเก็บรายงานกิจกรรมที่น่าสงสัย (Suspicious activity report) ที่เกี่ยวข้องกับบริการ Internet Banking อย่างเหมาะสมหรือไม่

8. การติดตามในส่วนการเชื่อมเครือข่ายต่อระหว่างธนาคารและบริษัทผู้ให้บริการทางอินเทอร์เน็ต (Internet Service Provider : ISP) ทำอย่างไร

การติดตามผลการดำเนินงานของระบบ (Performance Monitoring)

1. ประเมินว่าผู้บริหารได้ติดตามผลการดำเนินงานของระบบในประเด็นต่อไปนี้หรือไม่

- ปริมาณของการทำธุรกรรม
- ความเร็วในการโต้ตอบกับลูกค้า
- ความมีประสิทธิภาพและสามารถให้บริการได้อย่างต่อเนื่องไม่หยุดชะงัก
- การจัดทำบันทึกแสดงพฤติกรรมการใช้บริการของลูกค้า
- รายงานเกี่ยวกับข้อร้องเรียนของลูกค้า

โดยพิจารณาเรื่องต่อไปนี้ประกอบการประเมิน

1.1 พิจารณาวิธีที่ผู้บริหารใช้คาดการณ์ความจำเป็นของระบบในอนาคต (future system need) เพื่อให้มั่นใจว่าระบบเครือข่ายสามารถตอบสนองความต้องการของลูกค้าได้ตลอดเวลา

1.2 มีการรายงานสรุปเกี่ยวกับการใช้ WebSite ปริมาณธุรกรรม System problem log และรายงานรายการที่ได้รับการยกเว้น (transaction exception reports) ให้ผู้บริหารทราบในระยะเวลาที่เหมาะสมพอเพียง เพื่อให้ผู้บริหารทราบถึงแนวโน้มการใช้งานระบบ ลูกค้า และปัญหาการดำเนินงาน การแก้ไขปัญหา หรือไม่

1.3 มีการจัดทำรายงานเกี่ยวกับ Website Address ในรายงานสถานะ (Report of Condition) ให้กับผู้บริหารอย่างถูกต้องหรือไม่

2. มีขั้นตอนการดำเนินงานที่เหมาะสมในการดูแลการเชื่อมโยงกับ Website อื่นๆ ทั้ง Website ภายในและภายนอก (Intranets or other Private Network) (ผู้บริหารควรติดตาม Site เชื่อมโยงเหล่านี้เป็นประจำเพื่อตรวจสอบความเหมาะสมและความถูกต้องของ site addresses)

3. พิจารณาดูว่าสถาบันการเงินรับประกัน (Guaranty or similar pledge) ระบบการชำระเงินหรือการส่งมอบหรือไม่

4. มีการสอบทานการรับประกันดังกล่าวโดยที่ปรึกษาทางกฎหมายของสถาบันการเงิน หรือไม่

5. มีนโยบายและขั้นตอนการดำเนินงานที่เหมาะสมในการติดตามการใช้ e-mail ทั้งภายในและภายนอก หรือไม่ และพิจารณาดูว่านโยบายและขั้นตอนดังกล่าวครอบคลุมเรื่องต่อไปนี้หรือไม่

5.1 การส่ง E-mail ระหว่างกลุ่มผู้ใช้ เช่นลูกค้า พนักงาน

5.2 กำหนดเนื้อหาที่ได้อนุมัติให้ส่งได้ เพื่อลดความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือไม่เหมาะสม

6. กระบวนการรักษาความถูกต้องของข้อมูลใน Website เป็นอย่างไร

<u>การติดตามการให้บริการแก่ลูกค้า (Customer Support)</u>

1. ประเมินบทบาทและคุณภาพของการให้บริการลูกค้าและบริการสนับสนุนอื่นๆทางด้าน Internet Banking มีขั้นตอนการดำเนินงานเพื่อติดตามและระบุปัญหาของลูกค้าที่เกี่ยวข้องกับการใช้บริการทาง Internet Banking เช่นการ log-in เข้าระบบทำได้ยาก ความพร้อมของระบบสำหรับใช้งาน ระยะเวลาในการประมวลผลรายการ และความถูกต้องของข้อมูลลูกค้า

2. สอบทานโครงสร้างองค์กรและความรับผิดชอบของหน่วยงานสนับสนุนการให้บริการแก่ลูกค้า (Customer Support)

3. พิจารณาดูว่าบริการสนับสนุนแก่ลูกค้า (Customer Support Service) กระทำโดยบริษัทภายนอกหรือไม่ ถ้าใช่ จดบันทึกความรับผิดชอบของบริษัทผู้ให้บริการและพิจารณาวิธีที่ผู้บริหารติดตามปัญหา ความต้องการ และข้อร้องทุกข์ของลูกค้า

4. มีการกำหนดระดับการให้บริการลูกค้าหรือไม่ ถ้ามี ประเมินว่าผู้บริหารมีการตรวจสอบการปฏิบัติตามระดับการให้บริการตามที่กำหนดหรือไม่

5. พิจารณาวิธีที่ผู้บริหารประเมินความเพียงพอของบริการลูกค้า

6. จากการสอบทาน Problem logs และรายงานบริการลูกค้า และการหารือกับผู้บริหาร พิจารณาว่ามีจุดบกพร่องในกระบวนการทำงานนั้นหรือไม่

7. ในการประมาณการเติบโตและการวางแผนทรัพยากรด้าน Internet Banking มีการพิจารณารวมด้านบริการลูกค้าด้วยหรือไม่

8. มีรายงานติดตามรูปแบบพฤติกรรมลูกค้า เช่นรายงานสรุปการเข้าใช้บริการผ่านทาง Internet หรือไม่

<u>ด้านการบริหารจัดการทางด้านเทคโนโลยีโดยองค์กรภายนอก</u>

<u>การบริหารจัดการบริษัทผู้แทนจำหน่ายระบบงาน (Vendor Management)</u>

1. มีสัญญาที่เป็นลายลักษณ์อักษรและมีการลงนามกับบริษัทผู้แทนจำหน่าย (Vendor) บริษัทผู้ให้บริการ บริษัทที่ปรึกษา หรือคู่สัญญาอื่นๆ ที่เกี่ยวข้องในการพัฒนาและบำรุงรักษาบริการ Internet Banking ทุกรายหรือไม่

1.1 เงื่อนไขในสัญญาครอบคลุมเพียงพอหรือไม่

1.1.1 รายละเอียดของงานและบริการที่จัดหาโดยบริษัทผู้ให้บริการ

1.1.2 รายละเอียดของค่าใช้จ่ายและค่าธรรมเนียมอื่นๆ

1.1.3 การสื่อสารแบบ online และเสถียรภาพของระบบงาน (availability) ความปลอดภัยในการส่งข้อมูล (transmission security) และการแสดงตนในการทำรายการ (transaction authentication)

1.1.4 สิทธิและความรับผิดชอบของฝ่ายตรวจสอบ

1.1.5 แผนสำรองฉุกเฉินสำหรับการฟื้นฟูระบบการให้บริการและสำรองข้อมูล และมาตรการป้องกันต่างๆ

1.1.6 ภาระผูกพัน (liability) สำหรับข้อมูลและการรักษาความลับของข้อมูล และกรณี ผู้ให้บริการประมวลผลรายการล้มเหลว ล่าช้า หรือผิดพลาด และรายการอื่นที่มีผลขาดทุนเกิดขึ้น (เงินขาด)

1.1.7 การปรับรุ่น (upgrade) hardware software และการเปลี่ยนแปลงราคา

1.1.8 สัญญาระบุถึงการที่สถาบันการเงินสามารถได้รับข้อมูลฐานะทางการเงิน รายงานตรวจสอบ และการตรวจสอบระบบรักษาความปลอดภัยของบริษัทผู้ให้บริการ

1.1.9 การฝึกอบรมและการแก้ไขปัญหา

1.1.10 บทลงโทษ (ในกรณีที่ไม่สามารถดำเนินการได้ตามสัญญา) และการยกเลิกเงื่อนไขสัญญา

1.1.11 ข้อห้ามในเรื่องการโอนสิทธิของสัญญา (Prohibition of contract assignment)

1.2 ที่ปรึกษาทางกฎหมายสอบทานสัญญาเพื่อยืนยันว่าสามารถใช้บังคับได้และสามารถป้องกันความเสี่ยงได้

2. ผู้บริหารและพนักงานทำ due diligence เพื่อสอบทานบริษัทผู้ให้บริการ และ ประเมินความเพียงพอของผลการสอบทานนั้นหรือไม่ ผู้บริหารได้รับการยืนยันว่าผู้ให้บริการทำ due diligence บริษัทที่ให้การสนับสนุนหรือไม่

3. ประเมินการทำ Due Diligence เพื่อคัดเลือกบริษัทผู้ให้บริการพิจารณาว่าการประเมินประกอบด้วยเรื่องต่อไปนี้หรือไม่

3.1 แผนกลยุทธ์และแผนธุรกิจสอดคล้องกับการบริหารจัดการระบบงานโดยบริษัทภายนอก

3.2 ผู้บริหารระดับสูงและคณะกรรมการบริหารธนาคารมีส่วนร่วมในการตัดสินใจคัดเลือกบริษัทผู้ให้บริการและว่าจ้างบริษัทผู้เชี่ยวชาญภายนอก หรือไม่

3.3 รวบรวมและวิเคราะห์ข้อมูลของบริษัทผู้ให้บริการภายนอกก่อนทำสัญญา

3.4 ผู้บริหารพิจารณาเรื่องดังต่อไปนี้ประกอบการตัดสินใจหรือไม่

3.4.1 ชื่อเสียงของบริษัทผู้ให้บริการ

3.4.2 ฐานะทางการเงิน

3.4.3 ต้นทุนในการพัฒนา บำรุงรักษา และสนับสนุน

3.4.4 กระบวนการควบคุมภายในและการฟื้นฟูระบบ (Recovery)

3.4.5 ข้อตกลงของระดับการให้บริการ (Service Level Agreement)

3.4.6 ความรับผิดชอบของบริษัทผู้ให้บริการและผู้บริหารของสถาบันการเงิน

4. ประเมินความเพียงพอของแผนงานหรือโปรแกรมการติดตามดูแลบริษัทผู้แทนจำหน่าย พิจารณาขอบเขตหน้าที่ความรับผิดชอบในการจัดการดูแล ติดต่อกับบริษัทผู้แทนจำหน่าย (Vendor Management)

4.1 ติดตามผลการดำเนินงาน ดูว่าสามารถปฏิบัติได้ตามสัญญาและแจ้งข้อบกพร่องต่างๆที่พบให้กับบริษัทผู้ให้บริการและผู้บริหารของสถาบันการเงิน หรือไม่

4.2 สอบทานฐานะทางการเงินของบริษัทผู้ให้บริการเป็นประจำ และ พิจารณาดูว่ามีการเตรียมพร้อมในการรองรับต่อเหตุการณ์ต่างๆ หรือไม่

4.3 สอบทานมาตรฐาน นโยบาย ขั้นตอนการดำเนินงานของบริษัทผู้ให้บริการที่เกี่ยวข้องกับการควบคุมภายใน การรักษาความปลอดภัย การพัฒนาและบำรุงรักษาระบบงาน แผนฉุกเฉิน พิจารณาดูว่าเป็นไปตามแนวทางขั้นต่ำของสถาบันการเงินหรือไม่

4.4 สอบทานรายงานการติดตามที่จัดทำโดยบริษัทผู้ให้บริการซึ่งเกี่ยวข้องกับปริมาณธุรกรรม เวลาการโต้ตอบ (Response times) เสถียรภาพของระบบงาน ช่วงเวลาที่ระบบไม่สามารถดำเนินงานได้ รายงานกิจกรรมที่ได้รับการยกเว้น และ รายงานกำลังความสามารถ

ของระบบ พร้อมทั้งแจ้งประเด็นที่พบให้กับผู้บริหารของสถาบันการเงินและบริษัทผู้แทนจำหน่าย ทราบ

4.5 สอบทานรายงานผู้ตรวจสอบภายนอก และรายงานการตรวจสอบอื่นๆ (ถ้ามี) ที่เกี่ยวข้องกับบริษัทผู้ให้บริการ และติดตามประเด็นต่างๆในรายงานการตรวจสอบ

4.6 สอบถามกลุ่มผู้ใช้ระบบงาน

4.7 บริษัทผู้แทนจำหน่ายหรือให้บริการจัดให้มีโปรแกรมการฝึกอบรม และเอกสารประกอบการใช้งานอย่างเพียงพอหรือไม่

4.8 ติดตามในเรื่องค่าใช้จ่าย ค่าบริการ ค่าธรรมเนียมเพิ่มเติมอื่นๆที่เกี่ยวข้อง ค่าบำรุงรักษา ค่าสนับสนุนอื่นๆ

4.9 เงื่อนไขเกี่ยวกับการทำสัญญาต่อ (Subcontracting) ครอบคลุมเรื่องบทบาทและหน้าที่ความรับผิดชอบขององค์กรที่รับดำเนินการต่อ (Subcontractor) หรือไม่

5. พิจารณาดูว่าสถาบันการเงินแจ้งหน่วยงานทางการที่กำกับดูแลสถาบันการเงินให้ทราบถึงการว่าจ้างองค์กรภายนอกมาบริหารจัดการระบบงานทางด้าน Internet Banking หรือไม่

6. สัญญาหรือข้อตกลงในเรื่องการบริหารจัดการระบบงานโดยองค์กรภายนอก หรือ สัญญาย่อยต่างๆ รวมอยู่ในการสอบทานการคุ้มครองลูกค้าและการสอบทานการปฏิบัติตามกฎหมายหรือไม่

7. พิจารณาว่าสถาบันการเงินทบทวนสัญญาของบริษัทผู้ให้บริการเพื่อให้มั่นใจว่าขอบเขตความรับผิดชอบของแต่ละบุคคลถูกกำหนดไว้ในสัญญาอย่างเหมาะสมและชัดเจน

8. สถาบันการเงินได้รับและสอบทานรายงานการตรวจสอบภายในและภายนอกที่ประเมินกระบวนการบริหารจัดการกับบริษัทผู้ให้บริการภายนอก หรือความสัมพันธ์กับเฉพาะบริษัทผู้ให้บริการระบบข้อมูลและเทคโนโลยี หรือไม่

9. ผู้บริหารแต่งตั้งบุคลากรเพื่อรับผิดชอบต่อการบริหารจัดการบริษัทผู้ให้บริการภายนอกหรือไม่ ทั้งนี้ควรจดบันทึกความรับผิดชอบของผู้บริหารและพิจารณาว่าผู้บริหารรับผิดชอบในการติดตามการทำงานและบริการด้วยหรือไม่

10. ถ้าสถาบันการเงินเป็นผู้จัดหา Software product สำหรับงาน Internet Banking เอง ให้พิจารณาว่าผู้บริหารมีกระบวนการทำงานที่เพียงพอในการกำหนดตัวบุคคลที่รับผิดชอบในการดูแลเก็บรักษา Source code ของโปรแกรมหรือไม่

11. ถ้าบริษัทผู้แทนจำหน่ายเป็นผู้ดูแลระบบงาน Internet Banking ซึ่งพัฒนาโดยสถาบันการเงินเอง (In-house) ให้พิจารณาดูว่ามีการควบคุมการเข้าถึงระบบของบริษัทผู้แทนจำหน่าย (รวมการเข้าถึงจากระยะไกล) ที่เพียงพอหรือไม่ โดยพิจารณาในเรื่องต่อไปนี้

11.1 สถาบันการเงินติดตามการเข้าถึงระบบของบริษัทผู้แทนจำหน่ายโดยใช้ Activity logs หรือมาตรการอื่นๆ หรือไม่

11.2 ขั้นตอนการแจกจ่าย Software ของบริษัทผู้แทนจำหน่ายมีความครอบคลุมทั่วถึงอย่างเพียงพอหรือไม่ และมีเอกสารประกอบการใช้งานเพียงพอหรือไม่

12. ถ้าบริษัทผู้ให้บริการภายนอกสามารถ dial-in เข้ามาในระบบของสถาบันการเงิน เพื่อ ประเมินและบำรุงรักษาสภาพระบบงาน ให้พิจารณาว่าสถาบันการเงินมีกระบวนการทำงานที่เพียงพอ เพื่อยืนยันว่าการทำงานของบริษัทผู้ให้บริการอยู่ภายใต้การควบคุมที่ดี (sound control) และ fidelity insurance ครอบคลุมถึงพนักงานและเจ้าหน้าที่ของบริษัทผู้ให้บริการหรือไม่

13. ถ้าสถาบันการเงินใช้ Software Package สำหรับระบบงาน Internet Banking (Turnkey) ผู้ตรวจสอบควรพิจารณาดูว่าSoftware ที่ใช้อยู่ภายใต้ Software Escrow Agreement หรือไม่ และมีขั้นตอนการปฏิบัติงานเพื่อยืนยันว่าความปลอดภัยในการเก็บรักษาโปรแกรมและเอกสารประกอบอื่นๆ และไฟล์ถูกจัดเก็บอยู่ในสถานะที่เป็นปัจจุบันอยู่เสมอหรือไม่

<u>การบริหารจัดการบริษัทผู้ให้บริการทางอินเตอร์เน็ต (Internet Service Provider-ISP)</u>

1. สถาบันการเงินพึ่งพา ISP เพื่อให้การสนับสนุนการเข้าถึงบริการ Internet Banking หรือไม่ ถ้าใช่พิจารณาว่าผู้บริหารติดตามบริษัทผู้ให้บริการในเรื่องต่อไปนี้หรือไม่

1.1 ผลการดำเนินงานเป็นไปตามข้อตกลงของระดับการให้บริการหรือไม่

1.2 กำหนดให้ ISP ติดตามการเชื่อมต่อ Internet ของสถาบันการเงินและรายงานให้ทราบเมื่อการเชื่อมต่อล้มเหลวหรือศักยภาพลดลง

1.3 พิจารณาว่ามีการวางแผนฉุกเฉินและความสามารถของ ISP ในการฟื้นระบบ หรือไม่

1.4 พิจารณาว่า ISP มีพนักงานเพียงพอเพื่อรองรับการให้บริการหรือไม่

1.5 พิจารณาว่าสถาบันการเงินใช้ชนิดของการเข้าถึงบริการที่แตกต่างกันออกไป ซึ่งอาจทำให้การสนับสนุนการให้บริการต่ำกว่ามาตรฐานหรือระดับที่ยอมรับได้หรือไม่

1.6 ในการติดตั้งอุปกรณ์ป้องกันระบบงาน เช่น filtering หรือ firewall นั้น ISP ออกแบบอุปกรณ์ดังกล่าวให้กับสถาบันการเงินโดยเฉพาะ หรือใช้อุปกรณ์ที่ได้ออกแบบไว้อยู่แล้ว

1.7 พิจารณาว่า ISP มีการควบคุมที่ดีต่อการเปลี่ยนแปลง Internet address ของสถาบันการเงินหรือไม่

1.8 พิจารณาว่ามีการประเมินความมั่นคงของฐานะการเงินของ ISP หรือไม่

1.9 การสอบทานมาตรฐานของระบบรักษาความปลอดภัยและวิธีปฏิบัติของ ISP

2. สถาบันการเงินมีช่องทางการสื่อสารข้อมูลอื่น เพื่อทดแทนกรณีที่ ISP หลักไม่สามารถจัดการหรือรองรับ Internet Traffic อันสืบเนื่องมาจากเกิดการขัดข้องทางเทคนิคหรือขีดกำลังความสามารถไม่เพียงพอ หรือไม่

3. บริษัทผู้ให้บริการรับผิดชอบในการ hosting และดูแล Web Site ของสถาบันการเงินในเรื่องต่อไปนี้หรือไม่

3.1 การควบคุมเพื่อป้องกัน Web Site ของสถาบันการเงินจากการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต และ การคุกคามหรือประสงค์ร้ายต่างๆ (malicious attacks)

3.2 ขั้นตอนการดำเนินงานเพื่อแจ้งให้สถาบันการเงินทราบถึงเหตุการณ์นั้นๆ

3.3 การสำรองข้อมูล WebSite เป็นประจำ

(2) การตรวจสอบเพิ่มเติม

ในกรณีที่ผู้ตรวจสอบพบว่าจุดอ่อนของผู้บริหารส่งผลกระทบที่เป็นนัยสำคัญต่อInternet Banking และมีข้อบกพร่องในผลการดำเนินงานซึ่งส่งผลกระทบที่เป็นนัยสำคัญต่อฐานะความมั่นคงของสถาบันการเงินให้ผู้ตรวจสอบดำเนินการตามแนวทางการตรวจสอบเพิ่มเติมดังนี้

วัตถุประสงค์

- เพื่อประเมินความรุนแรงของประเด็นนัยสำคัญและข้อบกพร่องต่างๆ
- ผลที่ได้จากการประเมิน นำมาใช้พิจารณาความเพียงพอของการกำหนดวัด ติดตาม และควบคุมความเสี่ยง

วิธีการ

<u>ด้านนโยบายและการจัดการ</u>

1. ตรวจสอบดูว่านโยบายที่กำหนดไว้ได้ครอบคลุมถึงเรื่องธุรกรรม Internet Banking อย่างสมบูรณ์เพียงพอหรือไม่ และประเมินแผนงานของผู้บริหารในการที่จะรวมธุรกรรม Internet Banking เข้าไปอยู่ในนโยบายและขั้นตอนการดำเนินงาน

2. พิจารณาผลกระทบของการขาดโปรแกรมช่วยติดตามและบริหารความเสี่ยงที่เกิดจากธุรกรรม Internet Banking ที่มีประสิทธิภาพ โดยพิจารณาจากความสำคัญของบริการและ Risk Profile ของสถาบันการเงิน พร้อมทั้งประเมินแผนงานของผู้บริหารในการแก้ไขจุดอ่อน และความสมเหตุสมผลของแผน

<u>ด้านการควบคุมภายในและการรักษาความปลอดภัย</u>

1. ตรวจสอบการควบคุมภายในทางด้าน Internet Bankingว่ามีความเพียงพอหรือไม่ และสาเหตุที่ยังไม่เพียงพอ โดยพิจารณาเรื่องต่อไปนี้

1.1 การทดสอบระบบ Internet Banking ก่อนใช้งาน ได้แก่ การทดสอบเพื่อยืนยันความน่าเชื่อถือของระบบและความสามารถของระบบ; Pilot Program เพื่อประเมินผลกระทบหรือความเป็นไปได้ทางตลาด; และการประเมินด้านการรักษาความปลอดภัย

1.2 สิทธิและอำนาจในการเข้าถึงระบบของพนักงาน พิจารณาดูว่า Access is necessary in all cases และมีการ log และสอบทานการเปลี่ยนแปลงอำนาจในการเข้าถึงต่างๆที่เกิดขึ้นหรือไม่

1.3 การรักษาความปลอดภัย เช่น Firewall และระบบการตรวจจับผู้บุกรุก

1.4 ความเพียงพอของแผนและขั้นตอนในการฟื้นฟูธุรกิจทางด้าน Internet Banking ในกรณีที่ระบบการทำงานหยุดชะงัก

2. สอบทานรายงานสรุปเกี่ยวกับปัญหาจากการดำเนินงานและจากลูกค้าทางด้านการให้บริการ Internet Banking โดยให้ตรวจสอบดูจากลักษณะและปริมาณการเกิดปัญหาที่เกิดขึ้น โดยชี้ให้เห็นถึงปัญหาที่เกิดซ้ำๆกันหรือบ่อยครั้ง ความเอาใจใส่ ตระหนักถึงความรุนแรงของปัญหาและการติดตามแก้ไขปัญหาของผู้บริหาร

3. ประเมินแผนหรือแนวทางของผู้บริหารในการแก้ไขความเสี่ยงที่เกิดขึ้นจากการมีระบบควบคุมภายในที่ไม่เหมาะสม

4. ตรวจสอบเพื่อยืนยันว่ามีเครื่องมือตรวจจับและป้องกันการทำรายการซ้ำซ้อนเกิดขึ้นในแต่ละระบบงานและแก้ไขรายการพิเศษต่างๆ

5. สุ่มตรวจสอบรายการที่ทำผ่านระบบงาน Internet Banking ตั้งแต่ Customer application ที่ลูกค้าใช้ทำรายการ online กับสถาบันการเงิน การใส่ข้อมูลการทำรายการของลูกค้า ส่งข้อมูลการทำรายการไปที่บัญชีลูกค้า ทำรายการ (Settlement) ตลอดจนการปฏิบัติขั้นสุดท้าย

ด้านการตรวจสอบและการสอบทาน

1. ขอบเขตการตรวจสอบครอบคลุมถึงการดำเนินงานด้าน Internet Banking หรือไม่

2. ประเด็นที่พบจากการตรวจสอบข้อไหนที่ผู้บริหารยังไม่ได้ดำเนินการแก้ไข หากมี ให้ประเมินผลกระทบ (ระดับความรุนแรง) ต่อการปฏิบัติงานด้าน Internet Banking

ด้านระบบสารสนเทศและการสื่อสาร

ตรวจสอบหาสาเหตุของข้อผิดพลาด ในกรณีที่ระบบสารสนเทศและการสื่อสารประมวลผลข้อมูลในรายงานไม่ถูกต้องและมีผลให้สถาบันการเงินไม่ได้ถือปฏิบัติตามนโยบายที่กำหนด กฎหมาย และคำสั่งของทางการ

ด้านการบริหารจัดการทางด้านเทคโนโลยีโดยองค์กรภายนอก

1. ประเมินคุณภาพของบริการและความน่าเชื่อถือของการควบคุมความเสี่ยงที่จัดหาโดยบริษัทผู้แทนจำหน่าย พิจารณาดูว่าเงื่อนไขในสัญญาที่ขาดหายไปทำให้สถาบันการเงินเกิดความเสี่ยงหรือไม่ อย่างไร โดยพิจารณาเทียบกับความสำคัญของบริการและภาระผูกพัน (liability) ที่อาจเกิดขึ้น

2. พิจารณาประสิทธิภาพในการแก้ไขปัญหาที่เกิดขึ้นกับบริษัทผู้แทนจำหน่าย มีการใช้มาตรการอื่น เช่นการสื่อสารที่เพิ่มขึ้น การลงโทษ หรือการยกเลิกสัญญา หรือไม่

3. สอบทานรายงานติดตามระดับการให้บริการของบริษัทผู้แทนจำหน่าย โดยตรวจสอบดูว่ามีประเด็นหรือปัญหาอะไรบ้างที่เกิดขึ้นจากการทำงานของบริษัทผู้แทนจำหน่าย ที่อาจส่งผลกระทบต่อความสามารถในการบริหารความเสี่ยงจากการดำเนินงาน (Operational Risks) ของสถาบันการเงิน และปรึกษากับผู้เชี่ยวชาญทางด้าน IT เพื่อพิจารณาดูว่าการติดต่อกับบริษัทผู้แทนจำหน่ายมีความเหมาะสมเพียงพอต่อการที่สถาบันการเงินจะได้รับข้อมูลเกี่ยวกับการดำเนินงานของบริษัทผู้แทนจำหน่ายต่อๆไปหรือไม่

3.2.3 การตรวจสอบเพื่อประเมินการปฏิบัติตามกฎหมาย

วัตถุประสงค์

- เพื่อให้ทราบว่าการดำเนินงานที่เกี่ยวข้องกับการให้บริการ Internet Banking และตัวธุรกรรมหรือบริการ Internet Banking ของสถาบันการเงิน เป็นไปตามกฎหมาย และระเบียบหรือข้อบังคับที่เกี่ยวข้อง

- เพื่อประเมินความเพียงพอของระบบที่ใช้ในการติดตามการปฏิบัติตามกฎหมายของสถาบันการเงิน

วิธีการ

1. การให้บริการทางการเงิน Internet Banking อยู่ภายใต้กรอบของพระราชบัญญัติการธนาคารพาณิชย์ พ.ศ. 2505 และที่แก้ไขเพิ่มเติม และกฎหมายว่าด้วยการประกอบธรกิจเงินทุน ธุรกิจหลักทรัพย์ และธุรกิจบัตรเครดิตฟองซิเอร์ พศ.2522 หรือไม่

2. สอบทานประเด็นจากการตรวจสอบครั้งก่อน จากรายงานการตรวจสอบของผู้ตรวจสอบภายในและภายนอก พิจารณาดูว่าผู้บริหารดำเนินการแก้ไขประเด็นเหล่านั้นแล้วหรือยัง

3. มีรายงานที่สามารถตรวจพบธุรกรรมที่เข้าข่ายเป็นการฟอกเงินหรือไม่

4. มีข้อความประกาศเตือนผู้ใช้ระบบ หากเกิดกรณีมีการบุกรุก หรือการคุกคามระบบโดยไม่ได้รับอนุญาตในขณะนั้นหรือไม่

5. มีรายงานกิจกรรมที่น่าสงสัย (Suspicious activity report) หรือไม่

6. สถาบันการเงินจัดให้มีการเปิดเผยนโยบายความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าในการใช้บริการทาง Internet Banking หรือไม่

3.3 ขั้นการสรุปผลและจัดทำรายงาน

วัตถุประสงค์

สอบทานผลกระทบต่อฐานะโดยรวมของสถาบันการเงินที่อาจเกิดจากจุดอ่อน ข้อบกพร่อง และประเด็นที่พบจากการตรวจสอบหลัก (Core Analysis) และการตรวจสอบเพิ่มเติม (Expanded Analysis)

วิธีการสรุปผลการตรวจสอบและความเห็นของผู้ตรวจสอบ

1. รวบรวมประเด็นข้อสังเกตที่พบจากการตรวจสอบ โดยจำแนกตามหัวข้อสรุปตามแนวทางการตรวจสอบ ดังนี้

1.1 นโยบายและการจัดการ

1.2 การควบคุมภายในและการรักษาความปลอดภัย

1.3 การตรวจสอบและสอบทาน

1.4 การติดตามในระบบสารสนเทศและสื่อสาร

1.5 การบริหารจัดการทางเทคโนโลยีโดยองค์กรภายนอก

1.6 การปฏิบัติไม่ชอบด้วยกฎหมาย

2. ปรึกษาหารือกันในทีมที่ออกตรวจสอบ(สำหรับในกรณีที่ออกตรวจสอบพร้อมกัน ให้รวมถึงผู้ตรวจสอบด้าน IS และผู้ตรวจสอบทั่วไปด้วย) เพื่อพิจารณาผลกระทบ และระดับความรุนแรงของประเด็นจุดอ่อน หรือข้อบกพร่องที่พบจากการตรวจสอบ

3. สรุปประเด็นข้อสังเกตกับผู้บริหารของสถาบันการเงิน พร้อมทั้งชี้แจงให้ผู้บริหารเล็งเห็นถึงความจำเป็นของการดำเนินการแก้ไข ปรับปรุงต่อไป

4. เรียบเรียงข้อสรุปผลการตรวจสอบก่อนนำเข้าพิจารณาในที่ประชุมคณะกลั่นกรอง IS

5. นำเข้าพิจารณาในที่ประชุมคณะกลั่นกรอง IS

6. ส่งมอบรายงานสรุปผลการตรวจสอบด้าน IS และ E-Banking ให้แก่ฝ่ายตรวจสอบ 1 หรือ ฝ่ายตรวจสอบ 2 เพื่อดำเนินการต่อไป

ภาคผนวก 1 : คำนิยามของ E-Banking

สำหรับคำนิยามของ "E-Banking" นั้นมีการให้ความหมายไว้โดยองค์กรต่าง ๆ มากมาย โดยขอนำคำนิยามของธนาคารกลางและองค์กรกำกับสถาบันการเงินต่างประเทศที่เกี่ยวข้อง และคำนิยามที่หน่วยงานภายใน ธปท. ให้ไว้มาเป็นตัวอย่าง ดังนี้

คำนิยาม E-Banking ของธนาคารกลางและองค์กรกำกับสถาบันการเงินต่างประเทศ

1. Deutsche Bundesbank , Germany

การดำเนินธุรกรรมของธนาคารผ่านเครือข่ายอิเล็กทรอนิกส์ แต่จะไม่ครอบคลุมถึง E-Money[6] ดังนั้น E-Banking หมายถึง รูปแบบในการดำเนินธุรกรรมมากกว่าจะหมายถึงบริการหรือผลิตภัณฑ์ของธนาคาร โดยประเภทของ E-Banking สามารถแบ่งได้เป็น

- PC Banking
- Online Banking
- Internet Banking
- Telephone Banking
- Mobile Banking

2. Office of the Comptroller of the Currency; OCC

การนำเสนอบริการและผลิตภัณฑ์ทางการเงินผ่านช่องทางหรือเครือข่ายอิเล็กทรอนิกส์ เช่น โทรศัพท์ คอมพิวเตอร์ (ซึ่งรวมถึง Palmtop) และเพจเจอร์ เป็นต้น

3. Basel Committee; BIS

การนำเสนอบริการหรือผลิตภัณฑ์ทางการเงินในลักษณะรายย่อยหรือมีมูลค่าไม่สูง ผ่านเครือข่ายอิเล็กทรอนิกส์ ซึ่งรวมถึงธุรกรรมการฝากเงิน การให้สินเชื่อ การบริหารเงิน การให้คำปรึกษาทางการเงิน และการชำระเงินทางอิเล็กทรอนิกส์ เช่น การชำระค่าสาธารณูปโภคและ Electronic money (E-money)

---

[6] E-money (Electronic money) หมายถึง การให้บริการหรือการออกผลิตภัณฑ์อื่นที่อยู่ในรูป Non-banking financial (เช่นธุรกิจประกันภัย) แม้ว่าบริการหรือผลิตภัณฑ์เหล่านี้ถูกนำเสนอผ่านเครือข่ายอิเล็กทรอนิกส์ก็ตาม

4. The Federal Reserve Board; FRB

ให้คำจำกัดความในขอบเขตค่อนข้างกว้าง ซึ่งรวมถึงบริการที่มีอยู่ในปัจจุบันที่ใช้เครือข่ายอิเล็กทรอนิกส์เป็นหลัก เช่นบริการธนาคารทางโทรศัพท์ เครดิตการ์ด บริการผ่านเอทีเอ็ม นอกจากนี้ยังรวมถึงบัตรสะสมมูลค่า เดบิตการ์ด การชำระเงินผ่านเครือข่ายอินเตอร์เน็ต และบริการ PC Banking

5. Bangko Sentral ng Pilipinas, Philippines (2000)

ระบบที่ช่วยให้ลูกค้าสามารถเข้าใช้บริการหรือเข้าถึงผลิตภัณฑ์ของธนาคาร โดยใช้เครือข่ายคอมพิวเตอร์ (โดยผ่านระบบอินเตอร์เน็ต หรือ Direct Modem) หรือติดต่อผ่านเครือข่ายโทรศัพท์ทั่วไปหรือโทรศัพท์มือถือ

6. Bank Negara Malaysia

การทำธุรกรรมทางการเงินผ่านเครือข่ายอิเล็กทรอนิกส์

7. Hong Kong Monetary Authority (HKMA)

การให้บริการการธนาคารโดยผ่านเครือข่ายอินเตอร์เน็ต และ/หรือเครือข่ายการสื่อสารแบบไร้สาย เช่น m-banking

8. Central Bank of Lebanon

ธุรกรรมทางการธนาคารที่ดำเนินการผ่านเครื่องมือทางอิเล็กทรอนิกส์ เช่น Internet โทรศัพท์ คอมพิวเตอร์ และATM เป็นต้น ทั้งนี้ขอบเขตของ E-Banking ให้ครอบคลุมถึงทุกธนาคาร สถาบันการเงิน ผู้ออกเครดิตการ์ด และสถาบันอื่นที่เกี่ยวข้องกับการโอนเงิน

คำนิยาม E-Banking ของหน่วยงานภายใน ธปท.

1. สายระบบการชำระเงิน

บริการที่ธนาคารจัดให้ลูกค้าสามารถทำธุรกรรมทางการเงิน สอบถามข้อมูลด้านการเงินของตนเอง และข้อมูลอื่น ๆ โดยที่ไม่ต้องไปติดต่อ ณ สำนักงานธนาคาร สื่อที่ใช้ติดต่ออาจอยู่ในรูปบริการธนาคารทางโทรศัพท์ (Telebanking) หรือคอมพิวเตอร์ส่วนบุคคลเชื่อมโยงกับเครือข่ายอิเล็กทรอนิกส์ของธนาคาร โดยลูกค้าจะได้รับรหัสประจำตัวผู้ใช้บริการซึ่งระบบคอมพิวเตอร์ของธนาคารจะตรวจสอบความถูกต้องก่อนจะให้ผ่านเข้าไปทำรายการ

2. สายนโยบายสถาบันการเงิน ทีมนโยบายระบบชำระเงิน (ชื่อเดิมก่อนการปรับโครงสร้างองค์กร)

การดำเนินธุรกรรมการธนาคารของสถาบันการเงิน ซึ่งรวมถึงการนำเสนอบริการหรือผลิตภัณฑ์ของสถาบันการเงินผ่านเครือข่ายอิเล็กทรอนิกส์ ใด ๆ เช่น บริการธนาคารผ่านเครือข่าย Internet, ATM, Online Banking, Telephone Banking, Mobile Banking เป็นต้น ทั้งนี้ ธุรกรรมการธนาคารหมายถึงการประกอบธุรกิจตาม พรบ.ธุรกิจสถาบันการเงินที่บังคับใช้ในปัจจุบัน

ภาคผนวก 2 : การให้บริการธนาคารผ่านเครือข่าย Internet ในประเทศ และต่างประเทศ

การให้บริการธนาคารผ่านเครือข่าย Internet ในประเทศไทย

1. **บริการสอบถามข้อมูลที่เป็นข้อมูลส่วนบุคคล**

- สอบถามข้อมูล บัญชี บัตรเครดิต สินเชื่อส่วนบุคคล เช็ค
- บริการสมัครขอใช้บริการต่าง ๆ ของธนาคาร เช่น ส่งคำขออนุมัติสินเชื่อ, สมัครบัตรเครดิต, เปิดบัญชีเงินฝาก เป็นต้น

2. **บริการโอนเงิน ซึ่งแบ่งเป็น**

- บริการ โอนเงินระหว่างบัญชีต่าง ๆ ของลูกค้า
- บริการ โอนเงินเข้าบัญชีบุคคลอื่น-ภายในสถาบันเดียวกัน
- บริการ โอนเงินเข้าบัญชีบุคคลอื่น-ต่างสถาบัน

3. **บริการรับ-จ่ายชำระค่าสินค้าและบริการ**

- บริการรับชำระค่าสินค้าหรือบริการ เช่น ชำระภาษีมูลค่าเพิ่มแก่กรมสรรพกร, ชำระค่าลงทะเบียนของมหาวิทยาลัย, ค่าโทรศัพท์มือถือ, ค่าเพจเจอร์, ค่าประกันภัย, ค่าสินค้าของบริษัทขายตรง, การจองตั๋วเครื่องบิน (บริการ ไทยทัศน์ของธนาคารกรุงไทย) และอื่น ๆ
- บริการชำระค่าสาธารณูปโภค เช่น ค่าไฟฟ้า, ค่าน้ำประปา
- บริการชำระค่าใช้จ่ายบัตรเครดิต

4. **บริการทางด้านการค้าการเงิน**

- บริการด้าน Cash Management เช่น บริการนำเงินเดือนเข้าบัญชีพนักงาน
- บริการด้าน Treasury Management เช่น การซื้อ-ขายเงินตราต่างประเทศ, การซื้อ-ขายตราสารหนี้
- บริการด้าน Trade Finance เป็นบริการทางด้าน Import- Export เช่น การส่งคำขอเปิดL/C, การขอแก้ไข L/C
- บริการด้านการลงทุน (Securities Trading) เช่น ซื้อ-ขายหุ้น, ซื้อ-ขายกองทุน, ให้คำปรึกษาทางด้านการลงทุน

5. บริการทางด้าน E-Commerce

- บริการ E-Money เช่น กระเป๋าสตางค์อิเล็กทรอนิกส์ (E-Purse) เพื่อใช้ชำระค่าสินค้าหรือบริการที่มีมูลค่าต่ำ, Virtual card เป็นบัตรเครดิตที่ไม่มีบัตรพลาสติกสำหรับใช้ในการซื้อสินค้าทางอินเตอร์เน็ตซึ่งลูกค้าสามารถกำหนดวงเงินเองได้ทำให้มีความปลอดภัยมากขึ้น

- บริการ Payment Gateway / e-Payment เป็นบริการที่ทำหน้าที่เป็นตัวกลางรับชำระเงินระหว่างองค์กรที่เป็นคู่ค้าระหว่างกันด้วยการตัดบัญชีเงินฝากออมทรัพย์หรือกระแสรายวัน รวมถึงรองรับการชำระเงินสำหรับองค์กรที่ทำธุรกิจ E-Commerce แบบค้าปลีกบนอินเตอร์เน็ตด้วยบัตรเครดิตหรือด้วยการตัดบัญชีเงินฝากออมทรัพย์หรือกระแสรายวัน

- บริการให้การรับรองความถูกต้อง CA (Certification Authority) เป็นองค์กรกลางที่คอยให้คำรับรองว่าใครเป็นใครในโลกยุคอิเล็กทรอนิกส์ โดยออกใบรับรองดิจิทัล

- บริการเชื่อมโยงไป web sites สถาบันอื่น

6. บริการอื่น ๆ

- บริการ E-mail เพื่อเป็นช่องทางหนึ่งในการให้ลูกค้าสามารถติดต่อกับธนาคาร

- บริการเปลี่ยนรหัสต่าง ๆ เช่น รหัส ATM รหัสของระบบ Telephone banking

- บริการดาวน์โหลดข้อมูลธุรกรรมทางการเงิน เช่น ใบแสดงรายการบัญชี (Statement) ธุรกรรมที่ทำทางอินเตอร์เน็ต ข้อมูลทางธุรกิจทั่วไป เป็นต้น

พัฒนาการในการให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตในต่างประเทศ

ที่มาของอินเตอร์เน็ต

เครือข่ายอินเตอร์เน็ตเริ่มเกิดขึ้นหลังสงครามโลกครั้งที่ 2 ในประมาณปี ค.ศ. 1960 โดยเกิดจากแนวความคิดของประเทศสหรัฐอเมริกาที่จะเตรียมการให้มีเครือข่ายระบบการสื่อสาร และแลกเปลี่ยนฐานข้อมูลความรู้ที่สามารถเชื่อมโยงกันได้ แต่เป็นอิสระจากกัน และสามารถจะอยู่รอดได้เองแม้ว่าจะเกิดสงครามขึ้นก็ตาม จนต่อมาประมาณ ปี ค.ศ. 1982 ก็ได้มีการพัฒนาโปรโตคอล TCP/IP ซึ่งเป็นโปรโตคอลที่ใช้อยู่ในปัจจุบันนี้ การใช้ อินเตอร์เน็ตในสมัยสมัยแรกๆ เป็นการติดต่อกันในลักษณะที่เป็นการส่งข้อความติดต่อกันเป็นหลัก (Text-based communication) จนกระทั่งปี ค.ศ. 1991 จึงได้มีการพัฒนาการให้ข้อมูลในลักษณะที่เป็น WWW (World Wide Web) ซึ่งเราคุ้นเคยกันในปัจจุบันนี้และต่อมาจนถึงปี ค.ศ. 1994 จึงได้เกิดธนาคารแห่งแรกที่ให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตขึ้น

การให้บริการอินเตอร์เน็ตในต่างประเทศ

การให้บริการทางการเงินบนเครือข่ายอินเตร์เน็ตของสถาบันการเงินในต่างประเทศนั้นเริ่มขึ้นในปี ค.ศ. 1994[7] ประเทศญี่ปุ่นเปิดให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตประมาณปลายปี ค.ศ. 1998 ในขณะที่ประเทศสิงคโปร์ก็เริ่มให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตในเวลาที่ไล่เลี่ยกัน ส่วนประเทศฟิลิปปินส์ก็เริ่มให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตในปี ค.ศ. 1999

ตารางสรุปภาพรวมประเภทของบริการทางการเงินผ่านเครือข่าย Internet ในต่างประเทศ

Countries	Balance Inquiry/ Online Statement	Funds Transfer	Bills Payment	Security Trading	Online Shopping	Loan Application	Online Insurance	Online Leasing	Online Traveling
Australia	/	/	/	/	/	/	/	/	/
Japan	/	/	/	**N/A**	**N/A**	/	**N/A**	**N/A**	**N/A**
Korea	/	/	/	**N/A**	**N/A**	/	**N/A**	**N/A**	**N/A**
Singapore	/	/	/	/	/	/	/	**N/A**	**N/A**
UK	/	/	/	/	/	/	/	**N/A**	**N/A**
USA	/	/	/	/	/	/	/	/	**N/A**

1. Balance Inquiry/Online Statement เป็นบริการสอบถามยอดเงินคงเหลือในบัญชีและการขอรายการเคลื่อนไหวทางบัญชีประจำงวด

2. Fund Transfer เป็นบริการโอนเงินจากบัญชีไปมาระหว่างบัญชีทั้งของตนเองหรือโอนไปให้บุคคลที่สาม

3. Bills Payment เป็นบริการชำระเงินค่าสินค้าและบริการตามเอกสารเรียกเก็บเงิน

4. Security Trading เป็นบริการซื้อขายหุ้น/หลักทรัพย์

5. Online Shopping เป็นบริการเชื่อมโยงไป Web site ของร้านค้าและบริการรับชำระเงินค่าสินค้า

6. Loan Application เป็นบริการสมัครขอใช้บริการสินเชื่อ

7. Online Insurance เป็นบริการเชื่อมโยงไป Web site ของบริษัทขายประกันและบริการรับชำระเงินค่าประกัน

[7] "First Cyber Bank began in 1994", FRS-Internet Technology Paper, 5th SEACEN Course on IT RISK Management Supervision, Manila, The Philippines

8. Online Traveling เป็นบริการเชื่อมโยงไป Web site ของบริษัททัวร์และบริการรับชำระเงินในธุรกิจการท่องเที่ยว

9. Online Leasing เป็นบริการเชื่อมโยงไป Web site ของบริษัทเช่าซื้อและบริการรับชำระเงินในธุรกิจเช่าซื้อ

สรุปการให้บริการ Internet Banking และ Virtual Banking รายประเทศได้ดังต่อไปนี้

ประเทศออสเตรเลีย

จากการศึกษาสถาบันการเงินที่ศึกษาจำนวน 9 ธนาคาร พบว่าเป็นการให้บริการทางการเงินผ่าน Mobile Phone เพียง 1 ธนาคารเท่านั้น และยังไม่มีการจัดตั้ง Virtual Bank

การให้บริการทางการเงินบนเครือข่าย Internet ของสถาบันการเงินในประเทศออสเตรเลียมีขอบเขตการให้บริการที่กว้างขวางมากที่สุด โดยมีการให้บริการทางการเงินที่ครอบคลุมทุกๆด้าน ทั้ง 9 ข้อข้างต้น

ประเทศญี่ปุ่น

การให้บริการทางการเงินบนเครือข่าย Internet ของสถาบันการเงินในประเทศญี่ปุ่นเริ่มต้นในช่วงปลายปี 1998 โดยมีธนาคาร Sumitomo, Sanwa, Asahi เป็นผู้นำในการให้บริการทางการเงินบนเครือข่าย Internet มีขอบเขตการให้บริการในช่วงแรกที่ไม่ครอบคลุมทุกด้าน

แต่ต่อมาได้มีการขยายขอบเขตของการให้บริการทางการเงินได้มากขึ้นและกว้างขวางขึ้น ซึ่งจะเห็นได้จากตัวอย่างคือการจัดตั้ง Sony Bank (Internet-Only Bank หรือที่เรียกอีกชื่อว่า Virtual Bank) ขึ้นมาใหม่โดยเน้นการให้บริการที่เรียกว่า Private Banking Service ซึ่งเป็นความร่วมมือของ J.P. Morgan จากประเทศสหรัฐอเมริกาในการวางแผนการให้บริการทางการเงินแก่ลูกค้าที่กว้างขวางขึ้นกว่าเดิม แต่อย่างไรก็ตาม Web Site ของธนาคารในประเทศญี่ปุ่นมักจะแสดงรายละเอียดของการให้บริการเป็นภาษาญี่ปุ่นเท่านั้น ทำให้ไม่สามารถรวบรวมข้อมูลต่างๆ มากนักเท่าที่พบมีการให้บริการทางการเงินเพียง 4 ประเภทคือ

1. Balance Inquiry/Online Statement
2. Fund Transfer
3. Bills Payment
4. Loan Application

ประเทศเกาหลี

จากการเดินทางไปศึกษาและดูงานที่ Financial Supervisory Services (FSS-เป็นหน่วยงานที่ทำหน้าที่กำกับและตรวจสอบธนาคารพาณิชย์ บริษัทเงินทุนและบริษัทหลักทรัพย์ บริษัท

ประกันภัย) และธนาคารพาณิชย์จำนวน 4 แห่ง (ซึ่งเป็นผู้นำในการให้บริการทางด้าน E-Banking) คือ Shinhan Bank, Chohung Bank, Koram Bank และ Korea Exchange Bank ได้รับข้อมูลดังสรุปได้ดังต่อไปนี้:

ธนาคารพาณิชย์ของประเทศเกาหลีจำนวน18 แห่งจาก 22 แห่ง ได้เปิดให้บริการ Internet Banking ในขณะที่มีสาขาธนาคารพาณิชย์ต่างประเทศเพียง 1 แห่งเท่านั้นคือ Citibank นอกจากนี้การให้บริการทางการเงินในประเทศเกาหลีผ่านเครือข่าย Internet จะต้องใช้ Digital Signature ประกอบด้วย เพราะฉะนั้นสถาบันการเงินทุกแห่งจะต้องใช้เทคโนโลยี PKI และใช้ Certificate Authorities ในการพิสูจน์และตรวจสอบความถูกต้องของตัวบุคคลทุกคนที่เข้ามาทำรายการทางการเงินบนเครือข่ายอินเตอร์เน็ตโดยมีการประเภทของการให้บริการถึง 6 ประเภทคือ

1. Balance Inquiry/Online Statement
2. Fund Transfer
3. Bills Payment
4. Online Shopping
5. Loan Application
6. Online Insurance

ประเทศสหรัฐอเมริกา

จากการศึกษาสถาบันการเงินจำนวน 11 ธนาคาร ที่มีการให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตพบว่า สัดส่วนการให้บริการทางการเงินบน Wap Phone ประมาณ 1/ 3 ทั้งนี้ธนาคารในประเทศสหรัฐอเมริกามีประเภทของการให้บริการทางการเงินที่กว้างขวางมากเป็นอันดับสองรองจากประเทศออสเตรเลียเท่านั้นโดยมีการประเภทของการให้บริการถึง 8 ประเภทคือ

1. Balance Inquiry/Online Statement
2. Fund Transfer
3. Bills Payment
4. Security Trading
5. Online Shopping
6. Loan Application
7. Online Insurance
8. Online Leasing

ประเทศอังกฤษ

จากการศึกษาสถาบันการเงินจำนวน 2 ธนาคาร คือ ธนาคาร First Direct และธนาคาร Barclays พบว่า ธนาคาร First Direct (Internet-Only Bank หรือที่เรียกอีกชื่อว่า (Virtual Bank) เป็นธนาคารเดียวที่ให้บริการทางการเงินผ่าน Mobile Phone การให้บริการทางการเงินบนเครือข่าย Internet ของสถาบันการเงินในประเทศอังกฤษมีขอบเขตการให้บริการที่กว้างขวางถึง 7 ประเภท คือ

1. Balance Inquiry/Online Statement
2. Fund Transfer
3. Bills Payment
4. Security Trading
5. Online Shopping
6. Loan Application
7. Online Insurance

ประเทศสิงคโปร์

จากการศึกษาสถาบันการเงินจำนวน 5 ธนาคาร พบว่าเป็นการให้บริการทางการเงินผ่าน Mobile Phone ถึง 2 ธนาคารคือธนาคาร DBS และธนาคาร Overseas Union Bank แต่ยังไม่มีการจัดตั้ง Virtual Bank

การให้บริการทางการเงินบนเครือข่าย Internet ของสถาบันการเงินในประเทศสิงคโปร์ มีขอบเขตการให้บริการที่กว้างขวางถึง 7 ประเภทเช่นเดียวกันกับที่สถาบันการเงินในประเทศอังกฤษ

จากการติดตามการดำเนินงานด้าน Internet Banking[8] สิ้นสุดเดือนพฤษภาคม 2544 ผ่าน Web-site ของธนาคารต่างๆรวมทั้งสิ้น 39 แห่ง จาก 6 ประเทศ คือ ประเทศออสเตรเลีย ประเทศญี่ปุ่นประเทศสาธารณรัฐเกาหลี ประเทศสิงคโปร์ ประเทศอังกฤษ และประเทศสหรัฐอเมริกา ได้ข้อสรุปดังต่อไปนี้ คือ

1. ธนาคารที่ให้บริการ Internet Banking จะเสนอบริการทางการเงินเพิ่มเติมพิเศษจากการให้บริการธุรกรรมของธนาคารตามปกติ เช่น การยกเว้นค่าธรรมเนียมในการเปิดบัญชีประเภทกระแสรายวัน การยกเว้น /หรือจ่ายทดแทนค่าบริการในการเบิกเงินจากตู้ ATM หรือการให้บริการเสริมด้านการรับประกันความเสียหายเป็นต้น

[8] การศึกษาเรื่องรูปแบบและการให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตของธนาคารต่างประเทศได้อาศัยข้อมูลที่ค้นได้จากอินเตอร์เน็ต ซึ่งข้อมูลที่ได้อาจจะไม่สมบรูณ์ครบถ้วนทุกด้านหรือทุกประเด็น

2. ธนาคารที่มีลักษณะเป็น Internet-Only Bank หรือที่เรียกอีกอย่างหนึ่งว่า Virtual Bank นั้นมีจำนวนที่น้อยมาก เมื่อเปรียบเทียบกับธนาคารที่จัดตั้งเพื่อเสนอบริการทางการเงินแบบปกติแล้วขยายขอบเขตของการให้บริการมาจนครอบคลุมการให้บริการ Internet Banking ด้วย

3. ธนาคารของประเทศ ออสเตรเลีย มีประเภทของการให้บริการทางการเงินบนเครือข่ายอินเตอร์เน็ตสูงสุด ธนาคารของประเทศสหรัฐอเมริกา มีประเภทของการให้บริการมากรองลงมาเป็นอันดับสอง ในขณะที่ธนาคารของประเทศสิงคโปร์และอังกฤษมีประเภทของการให้บริการมากรองลงมาเป็นอันดับสาม เท่ากัน อย่างไรก็ตามธนาคารของประเทศเกาหลีมีการเสนอบริการเสริมให้แก่ลูกค้าหลายประเภท

ลักษณะที่ทำการของ Internet Bank

สามารถแบ่งได้เป็น 2 ประเภท

1. ถ้าเป็นธนาคารหรือสถาบันการเงินที่ให้บริการทางการเงินโดยไม่มีตัวอาคารสถานที่สำหรับบริการลูกค้าตามปกติ ก็เรียกว่า Internet-Only Bank หรือ Virtual Bank

2. ถ้าเป็นธนาคารหรือสถาบันการเงินที่มีตัวอาคารสถานที่สำหรับบริการลูกค้าตามปกติ ก็เรียกว่า Internet Bank ซึ่งเป็นรูปแบบที่ธนาคารส่วนใหญ่ทำกัน

ภาคผนวก 3 : การบริหารความเสี่ยงตามแนวทางของ OCC และ FDIC

การบริหารความเสี่ยงตามแนวทางของ OCC[9]

1. กระบวนการบริหารความเสี่ยงทางด้านเทคโนโลยี

กระบวนการบริหารความเสี่ยงทางด้านเทคโนโลยีมีส่วนประกอบที่สำคัญ 3ประการ คือ:

(1) การวางแผนใช้เทคโนโลยี (The planning process for the use of technology)

(2) การดำเนินการติดตั้งและใช้เทคโนโลยี (Implementation of the technology)

(3) การวัดและติดตามความเสี่ยง (The Means to measures and monitor risk)

วัตถุประสงค์ของการประเมินความเสี่ยง ก็คือการพิจารณาว่าธนาคารได้ดำเนินธุรกรรมด้านอินเตอร์เน็ตแบ้งก์กิ้ง (Internet Banking) ในลักษณะที่ปลอดภัยและเหมาะสม (การบริหารความเสี่ยงด้วยวิธีนี้สามารถประยุกต์ใช้กับการใช้เทคโนโลยีใหม่ๆได้ทั้งหมด) ธนาคารควรจะใช้ขั้นตอนการวิเคราะห์ที่จริงจังและเข้มงวดในการแยกแยะ, วัด, และควบคุมความเสี่ยง ซึ่งผู้ตรวจสอบจะต้องพิจารณาว่าระดับของความเสี่ยง (ของระบบงาน Internet Banking) สัมพันธ์กับระดับความเสี่ยงของธนาคารโดยรวมซึ่งธนาคารสามารถแบกรับได้ และอยู่ในความสามารถของธนาคารที่จะจัดการหรือ ควบคุม

1.1 การวางแผนใช้เทคโนโลยี (The planning process for the use of technology)

เป็นความรับผิดชอบของคณะกรรมการบริหารและผู้บริหารระดับสูง โดยที่ผู้บริหารดังกล่าวจะต้องใช้ความรู้และความเชี่ยวชาญในการจัดการใช้เทคโนโลยีทางด้าน Internet Banking และความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี ทั้งนี้คณะกรรมการบริหารควรที่จะทบทวน อนุมัติ และเฝ้าติดตามโครงการต่างๆ ที่ใช้เทคโนโลยีด้าน Internet Banking ซึ่งจะมีผลกระทบกับระดับความเสี่ยงของธนาคารพาณิชย์

คณะกรรมการบริหารควรที่จะพิจารณาว่าเทคโนโลยีและผลิตภัณฑ์ทางการเงินเป็นสิ่งที่อยู่ในเป้าหมายของแผนกลยุทธ์ของธนาคาร และตรงตามความต้องการของตลาด ในขณะที่ผู้บริหารระดับสูงควรที่จะมีความชำนาญในการที่จะประเมินเทคโนโลยีที่ใช้และความเสี่ยงที่เกิดขึ้น

[9] "Internet Banking", Comptroller's Handbook, October 1999

การประเมินเทคโนโลยีด้าน Internet Banking และผลิตภัณฑ์ทางการเงินแบบเป็นอิสระเป็นช่วงๆ โดยผู้ตรวจสอบภายในและบริษัทที่ปรึกษาสามารถที่จะช่วยให้คณะกรรมการบริหารและผู้บริหารระดับสูงสามารถบรรลุวัตถุประสงค์ทางด้านความรับผิดชอบได้

1.2 การดำเนินการติดตั้งและใช้เทคโนโลยี (Implementation the technology)

เป็นความรับผิดชอบของฝ่ายจัดการที่จะต้องใช้ความชำนาญในการที่จะประเมินเทคโนโลยีและผลิตภัณฑ์ทางการเงินทางด้าน Internet Banking, การเลือกใช้ส่วนผสมของเทคโนโลยีและผลิตภัณฑ์ทางการเงินที่เหมาะสม, และคอยควบคุมให้มีการติดตั้งและใช้เทคโนโลยีอย่างเหมาะสม แต่ถ้าธนาคารไม่มีความชำนาญที่จะช่วยในการดำเนินงานได้โดยตนเองตามลำพัง ธนาคารก็สมควรที่จะติดต่อขอความช่วยเหลือจากบรรดาผู้จัดจำหน่ายอุปกรณ์ด้านเทคโนโลยีที่มีความเชี่ยวชาญหรือติดต่อกับหุ้นส่วนทางด้านเทคโนโลยีอื่นๆ ที่มีความชำนาญด้านนี้

1.3 วิธีการในการวัดและติดตามเฝ้าดูความเสี่ยง (Measures and monitoring risk)

เป็นความรับผิดชอบของฝ่ายจัดการ ซึ่งควรที่จะมีความชำนาญที่จะสามารถที่จะแยกแยะอย่างมีประสิทธิภาพ, การวัด, การเฝ้าติดตาม และควบคุมความเสี่ยงที่สัมพันธ์กับ Internet Banking

คณะกรรมการบริหารควรที่จะได้รับรายงานเป็นประจำเกี่ยวกับการใช้เทคโนโลยี, ความเสี่ยงที่เกิดขึ้น, และวิธีการซึ่งใช้ในการจัดการความเสี่ยง ซึ่งการเฝ้าติดตามระบบการปฏิบัติงานเป็นสิ่งที่สำคัญที่สุด

ทั้งนี้ธนาคารควรที่จะคำนึงถึงการรับประกันคุณภาพ และ ขั้นตอนการตรวจสอบว่าเป็นส่วนหนึ่งของขั้นตอนในการออกแบบ และธนาคารควรที่จะทบทวนระบบงานของตนเองเป็นระยะๆ เพื่อประกอบการตัดสินใจว่าธนาคารสามารถปฏิบัติงานได้ตามมาตรฐานการปฏิบัติงานที่กำหนดเอาไว้แล้ว

2. การควบคุมภายใน

การควบคุมภายในของธนาคารทางด้านระบบ Internet Banking ควรที่จะจัดให้เหมาะสมกับระดับของความเสี่ยงของสถาบันการเงินนั้นๆ ซึ่งฝ่ายจัดการก็มีหน้าที่ที่จะต้องรับผิดชอบในการพัฒนาและติดตั้งระบบการควบคุมภายในที่ดีทางด้าน Internet Banking และผลิตภัณฑ์ทางการเงิน

ระบบการตรวจสอบระบบการควบคุมต่างๆ จะสามารถทำให้เกิดความมั่นใจว่าระบบการควบคุมอย่างเหมาะสมและสามารถทำงานได้อย่างมีประสิทธิภาพ ตัวอย่างเช่นวัตถุประสงค์ของ

การควบคุมเทคโนโลยีและผลิตภัณฑ์ทางการเงินทางด้าน Internet Banking ของแต่ละธนาคารจะประกอบด้วย

(1) ความต่อเนื่องของการวางแผนทางด้านเทคโนโลยี และเป้าหมายของแผนกลยุทธ์(รวมไปถึงความมีประสิทธิภาพและความประหยัดของการดำเนินการและการปฏิบัติที่สอดคล้องกับนโยบายของบริษัทและความจำเป็นทางด้านกฎหมายต่างๆ)

(2) ความมีอยู่ของข้อมูลเพื่อการใช้งานได้ (Data availability)

(3) ความสมบูรณ์ถูกต้องของข้อมูล (Data integrity) ซึ่งรวมไปถึงการจัดเตรียมให้มีการเก็บรักษาของสินทรัพย์, การอนุมัติรายการอย่างเหมาะสม, และความเชื่อถือได้ของขั้นตอนการประมวลผลและผลลัพธ์จากการประมวลผล

(4) ความลับของข้อมูลและการป้องกันความเป็นส่วนตัว

(5) ความเชื่อถือได้ของระบบข้อมูลสำหรับการจัดการ

เมื่อวัตถุประสงค์ของการควบคุมได้จัดตั้งขึ้นมาแล้ว ฝ่ายจัดการก็มีความรับผิดชอบในการติดตั้งการควบคุมภายในที่จำเป็นเพื่อควบคุมให้วัตถุประสงค์ของสถาบันการเงินสามารถบรรลุได้

ฝ่ายจัดการยังคงมีความรับผิดชอบในการประเมินความเหมาะสมของระบบการควบคุมต่างๆ ซึ่งอาศัยแนวความคิดเรื่องต้นทุน-กำไรเป็นหลัก ดังนั้นฝ่ายจัดการจะต้องวิเคราะห์ลงไปถึงความมีประสิทธิภาพของการควบคุมและมูลค่าของตัวเงินที่ไหลผ่านในแต่ละขั้นตอน รวมทั้งต้นทุนต่างๆในการควบคุม

ผู้ตรวจสอบจำเป็นที่จะต้องเข้าใจสภาพแวดล้อมในการดำเนินงานของธนาคารเพื่อที่จะสามารถประเมินความเหมาะสมของการประสมกันอย่างเหมาะสมของระบบการควบคุมภายในที่เพียงพอ ซึ่ง ISACA[10] ได้กำหนดไว้ว่าระบบการควบคุมภายในขั้นต้นควรที่จะประกอบด้วยระบบการควบคุมภายในทางด้านบัญชี ซึ่งมีไว้ใช้สำหรับการปกป้องทรัพย์สินต่างๆ และความเชื่อถือได้ของระบบการบันทึกข้อมูลทางการเงิน ซึ่งรวมไปถึงการบันทึกรายการทางธุรกิจและงบทดลอง

(1) ระบบการควบคุมการปฏิบัติงาน ซึ่งมีไว้ใช้ให้เกิดความมั่นใจว่าจะสามารถบรรลุวัตถุประสงค์ของธุรกิจได้ ซึ่งรวมไปถึงแผนการปฏิบัติงานและงบประมาณเพื่อใช้เปรียบเทียบว่าสิ่งที่เกิดขึ้นจริงกับแผนการปฏิบัติงานที่วางไว้

(2) ระบบการควบคุมการบริหาร/การจัดการ ซึ่งมีไว้ให้เกิดความมั่นใจในความมีประสิทธิผลและการเป็นไปตามนโยบายและระเบียบขั้นตอนการปฏิบัติงานซึ่งประกอบไปด้วยการ

[10] Information Systems Audit and Control Association (ISACA)

ตรวจสอบทั้งภายในและภายนอกตามช่วงระยะเวลา

ISACA ได้แบ่งแยกการควบคุมภายในออกเป็นอีก 3 ประเภทใหญ่ ซึ่งระบบการควบคุมดังกล่าวก็ปรากฏอยู่ในระบบการควบคุมขั้นพื้นฐานที่ได้กล่าวถึงมาแล้วข้างต้น (เป็นการจัดระบบการควบคุมภายใน ในอีกรูปแบบหนึ่ง)

(1) ระบบการควบคุมเชิงป้องกัน (Preventive Controls) การป้องกันไม่ให้บางสิ่งเกิดขึ้น (เป็นข้อผิดพลาดหรือการปฏิบัติที่ผิดกฎหมาย) โดยมีตัวอย่างคือระบบการเข้าถึงทางตรรกภาพ (Logical Access) ของระบบ Software ซึ่งป้องกันไม่ให้ผู้ที่ไม่มี ID และ Password เข้าสู่ระบบเครือข่ายได้

(2) ระบบการควบคุมเชิงตรวจจับ (Detective Controls) สำแดง หรือชี้ให้เห็นการกระทำที่เกิดขึ้น เช่นระบบ Software ที่ตรวจจับการบุกรุกเข้าสู่ระบบซึ่งจะส่งสัญญาณภัยเตือนเมื่อมีเหตุการณ์ดังกล่าวเกิดขึ้น

(3) ระบบการควบคุมเชิงการแก้ไข (Corrective Controls) แก้ไขสถานการณ์เมื่อมีการตรวจพบสถานการณ์ เช่นระบบการสำรอง/ สำเนา Software ซึ่งจะสามารถใช้ได้เมื่อแฟ้มข้อมูลหรือระบบฐานข้อมูลเสียหาย

ธนาคารต่างๆ หรือผู้ที่ให้บริการผลิตภัณฑ์ทางการเงินบนเครือข่าย Internet ในระดับ Transaction-Based ควรที่จะมีระบบการควบคุมที่สูงพอที่จะช่วยให้สามารถบริหารความเสี่ยงจากการทำรายการของธนาคาร ซึ่งตัวอย่างของระบบการควบคุมต่างๆ จะประกอบด้วย

(1) การเฝ้าติดตามกิจกรรมในการทำรายการเพื่อดูความไม่ปกติในชนิดของการทำรายการ, ปริมาณของการทำรายการ, มูลค่าของการทำรายการ, และช่วงเวลาของการทำรายการ

(2) การเฝ้าติดตามและบันทึกรายการที่กระทำโดยละเมิดระเบียบปฏิบัติงานหรือความพยายามที่จะทำเพื่อที่จะสำแดงกิจกรรมที่ต้องสงสัยซึ่งประกอบด้วย การร้องขอ (ข้อมูล)ที่ไม่ถูกต้อง, การทำรายการในเวลาที่ผิดปกติ, หรือรูปแบบการทำรายการที่ไม่ปกติ

(3) การใช้กับดักหรือเทคนิคในการติดตามเพื่อสำแดงให้เห็นว่าแหล่งที่มาของคำขอ (ทำรายการ) มาจากลูกค้าจริง

การตรวจสอบระบบการรายงานตามปกติและการตรวจการทำรายการที่ไม่ปกติจะช่วยให้สามารถ ติดตามและเข้าใจในเรื่องต่อไปนี้คือ

(1) การบุกรุกหรือพยายามที่จะบุกรุกโดยผู้ที่ไม่ได้รับอนุญาต

(2) ความผิดพลาดต่างๆของการบันทึกข้อมูลการทำรายการของลูกค้า

(3) ลูกค้ามีพฤติกรรมในการทำธุรกรรมและการใช้บริการอย่างไร ในช่วงเวลาต่างๆ

การบริหารความเสี่ยงตามแนวทางของ FDIC [11]

ความเสี่ยงที่เกิดขึ้นจากขั้นตอนการบริหารงานด้าน IT (Management Processes)	
ข้อแนะนำในการบริหารงานที่ดี	**ผลกระทบที่อาจเกิดขึ้น ถ้าไม่สามารถปฏิบัติได้**
1. ผู้บริหารควรพัฒนาแผนสำรอง/แผนฉุกเฉินเพื่อรองรับสถานการณ์ต่างๆที่เกิดขึ้นไว้อย่างเพียงพอ	1. สถาบันการเงินอาจต้องรับผิดชอบต่อผลสูญเสียของลูกค้าที่เกิดจากระบบถูก Interrupt หรือเกิดการผิดพลาด
2. มีการป้องกันระบบภายในและข้อมูลของลูกค้าที่เป็นความลับจาก Internal และ External Attacks อย่างเพียงพอ	2.1 บุคคลที่ไม่ได้รับอนุญาตอาจเข้าถึงระบบและเปลี่ยนแปลงข้อมูลลูกค้าและข้อมูลที่เป็นความลับอื่นๆ ของสถาบันการเงิน 2.2 การตรวจจับ การรายงาน การบุกรุกต่างๆ ต่อระบบอาจไม่สามารถกระทำได้ทันเวลา ซึ่งจะทำให้ความเสียหายหรือสูญเสียข้อมูลที่สำคัญๆของสถาบันการเงิน
3. ควรทำการวิเคราะห์และประเมินระบบงาน (Due Diligent) อย่างครอบคลุมเพียงพอก่อนใช้งาน	3. การขาดการควบคุมภายในที่ครอบคลุมเพียงพอทำให้สถาบันการเงินไม่สามารถควบคุมความเสี่ยงทางด้านระบบความปลอดภัยและต่อการทุจริต
4. สัญญาทางด้านการ Outsource เทคโนโลยีบริการ หรือระบบงานของ E-Banking ควรจะมีความซับซ้อน ละเอียดครอบคลุมทุกด้าน และผ่านการสอบทานจากบุคคลากรทางด้านกฎหมายก่อน อีกทั้งควรมีการสอบทานและจัดการอย่างต่อเนื่องเป็นประจำ	4. การไม่ปฏิบัติตามมาตรฐานอาจส่งผลให้เกิดความเสี่ยงด้านเครดิต ตลาด สภาพคล่อง กฎหมาย การดำเนินงาน และชื่อเสียงของสถาบันการเงิน

[11] ข้อมูลจาก FDIC บทความชื่อ Electronic Banking, Draft : July, 2000

ความเสี่ยงที่เกิดขึ้นจากขั้นตอนการดำเนินงานด้าน IT (Operational)	
ข้อแนะนำในการบริหารงานที่ดี	**ผลกระทบที่อาจเกิดขึ้น ถ้าไม่สามารถปฏิบัติได้**
1. คณะกรรมการสถาบันการเงินและผู้บริหารสอบทานนโยบายและขั้นตอนการปฏิบัติงานและทำการเปลี่ยนแปลงแก้ไขนโยบายและขั้นตอนการปฏิบัติงานให้สอดคล้องเหมาะสมกับประเภทของการให้บริการด้าน E-Banking	1.1 นโยบายและขั้นตอนการปฏิบัติงานอาจไม่ครอบคลุมถึงผลกระทบต่อธุรกรรม, การดำเนินงานหรือความปลอดภัยของสถาบันการเงิน 1.2 การควบคุมอาจไม่สามารถป้องกันข้อมูลความลับที่อยู่ในรูปสื่ออิเล็กทรอนิกส์ได้อย่างเพียงพอ
2. คณะกรรมการสถาบันการเงินจัดทำมาตรฐานและขั้นตอนการปฏิบัติงานสำหรับการปฏิบัติงาน E-Banking ทั่วไป และการดำเนินงานกับระบบ (System Operation)	2. ธนาคารอาจประสบผลขาดทุนได้ ถ้าระบบล้าสมัยหรือระบบงานมีความจำเป็นที่จะต้องทำการ Update อยู่เรื่อยๆ มากกว่าที่คาดคิดไว้ ทำให้ลูกค้าอาจจะได้รับข้อมูลที่ผิดพลาดซึ่งทำให้สถาบันการเงินมีความเสี่ยงทางด้านกฎหมายและความเสี่ยงต่อการเสียชื่อเสียงของสถาบันการเงิน
3. การตรวจสอบโดยผู้ตรวจสอบภายในและภายนอกควรครอบคลุมถึงการดำเนินงานด้าน E-Banking ไว้ด้วย	3. ไม่สามารถพบจุดอ่อนในด้านความปลอดภัย การดำเนินงาน การปฏิบัติตามกฎหมาย หรือการควบคุมในระบบงาน E-Banking
4. ควรมีการระบุ ประมวลผล และรายงานข้อมูลที่เกี่ยวข้องไว้ในระบบสารสนเทศและการสื่อสารของสถาบันการเงิน	4. การรายงานอาจไม่น่าเชื่อถือ ไม่ได้ถือปฏิบัติตามกฎหมายหรือการควบคุมในระบบงาน E-Banking และนโยบายภายในอาจมีความบกพร่องได้
5. ผู้บริหารตระหนักถึงเรื่องการจัดการทางด้าน Outsourcing	5.1 บริการ E-Banking อาจหยุดชะงักได้ถ้าผู้ให้บริการ (Vendor, หรือ Third Party providers) มีปัญหาทางการเงิน 5.2 ผู้ให้บริการไม่สามารถปฏิบัติตามเงื่อนไขในสัญญา ทำให้เกิดผลขาดทุนหรือลูกค้าสูญเสียความเชื่อมั่นในตัวสถาบันการเงิน นำไปสู่การการแห่ถอนเงินฝากหรือปิดบัญชีได้

ความเสี่ยงที่เกิดขึ้นจากขั้นตอนการดำเนินงานด้าน IT (Operational)	
ข้อแนะนำในการบริหารงานที่ดี	**ผลกระทบที่อาจเกิดขึ้น ถ้าไม่สามารถปฏิบัติได้**
6. ผู้บริหารจัดให้มีการฝึกอบรมอย่างเพียงพอแก่พนักงานเกี่ยวกับการควบคุมและความเสี่ยงที่เกิดขึ้นจากระบบส่งมอบและชำระเงิน (Delivery and Payment System)	6. พนักงานอาจละเลยการควบคุมที่เพียงพอต่อความถูกต้องของข้อมูล ความปลอดภัยของข้อมูล และแผนสำรอง/แผนฟื้นฟู (Business Resumption Plan)
7. คณะกรรมการสถาบันการเงินหรือคณะกรรมการที่เกี่ยวข้องอนุมัติบริการที่เสนอผ่าน E-Banking โดยยึดตามแผนธุรกิจที่จัดทำไว้เป็นลายลักษณ์อักษร ซึ่งครอบคลุมถึง Cost/Benefit ความเสี่ยง และวิเคราะห์ผลกระทบทางการเงินที่เกี่ยวข้องกับธุรกรรมนั้นๆ	7. การวางแผนไม่เพียงพออาจทำให้การเสนอบริการส่งผลกระทบอย่างไม่คาดคิดต่อสภาพคล่อง ความไวต่อความเสี่ยงทางตลาด หรือคุณภาพของสินเชื่อ การลงทุนในระบบงาน E-Banking อาจส่งผลกระทบอย่างไม่คาดคิดต่อรายได้และเงินกองทุนของสถาบันการเงิน

ภาคผนวก 4 : ความรู้ทางด้านเทคโนโลยี

1. Digital Certificates : A Secure Method for Digital Transfers[12]

ปัจจุบันองค์กรต่างๆ ได้ปรับปรุงแผนกลยุทธ์ทางธุรกิจของตนเอง โดยมุ่งไปสู่การบริการที่ทันสมัย รวดเร็วเพื่อเพิ่มรายได้และการลดค่าใช้จ่ายด้านการให้บริการใหม่ๆ ทางด้าน e-commerce ซึ่งทำให้ธุรกิจสามารถเข้าถึงกลุ่มลูกค้าได้เพิ่มขึ้น อย่างไรก็ดี ในขณะที่การให้บริการทางด้าน e-commerce จะมีประโยชน์และน่าสนใจมาก แต่ก็ก่อให้เกิดความเสี่ยงด้วย เพราะว่าการให้บริการทางด้าน e-commerce สามารถมีช่องทางในการทุจริตทางการเงิน และการขัดข้องของระบบงานอันเนื่องมาจากการโจมตีจากผู้ที่ไม่ประสงค์ดี ได้ ดังเช่นข่าวการโจมตีระบบ Cash Management System ของธนาคารซิตี้แบงค์ในปี 1995 การเข้าไปโจมตีระบบงานของกระทรวงกลาโหมสหรัฐอเมริกา และการเข้าไปขโมยโค้ดโปรแกรมของบริษัทไมโครซอฟท์ เป็นต้น

ตัวอย่างของความเสียหายทางการเงินที่เกิดจากการทุจริตดังนี้คือ

- การขโมยโปรแกรม หมายเลขบัตรเครดิต และข้อมูลลับของหน่วยงานต่างๆ เฉพาะที่เกิดในสหรัฐอเมริกาเอง มีความเสียหายประมาณ 10 ล้าน ดอลล่าร์สหรัฐอเมริกาต่อปี
- มากกว่าครึ่งหนึ่งขององค์กรต่างๆ ต้องเคยสูญเสียข้อมูลทางด้านการเงินในช่วงระยะ2 ปีที่ผ่านมานี้
- การทุจริตที่มีสาเหตุมาจากบัตรเครดิตมีความเสียหายประมาณ 5 พันล้าน ดอลล่าร์สหรัฐอเมริกาต่อปี

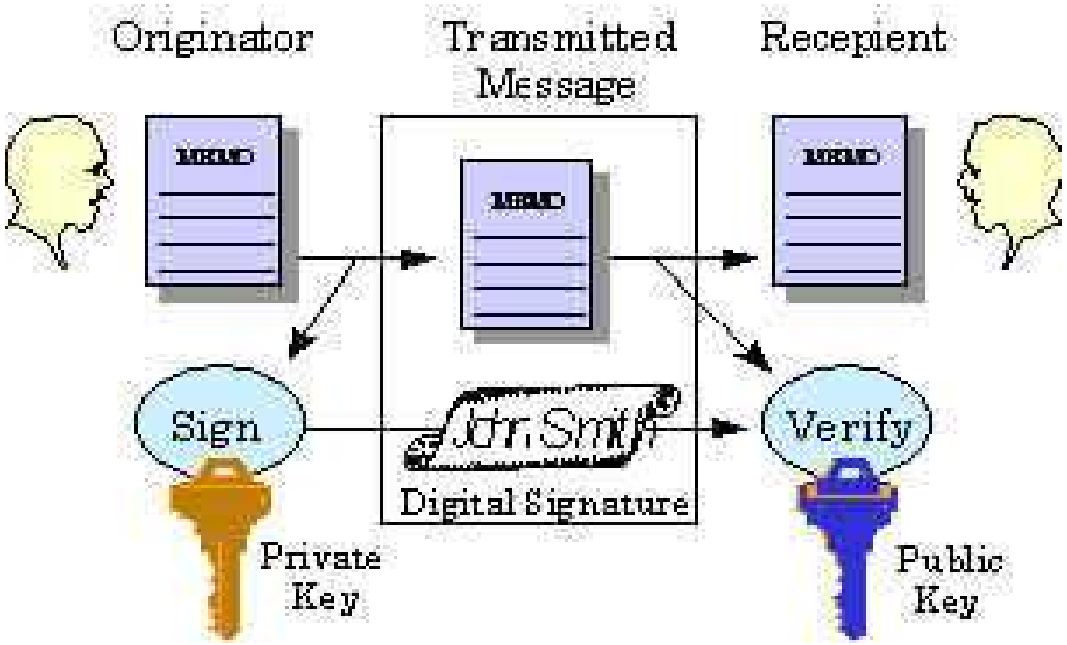
ดังนั้นเพื่อช่วยเสริมสร้างความปลอดภัยของบริการทางด้าน e-commerce จึงได้มีการนำdigital authentication เข้ามาช่วยในการป้องกันความลับของข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ต ทั้งนี้ เทคนิคดังกล่าวจะประกอบไปด้วยการเข้ารหัสข้อมูล และการใช้ลายมือชื่ออิเล็กทรอนิกส์ ร่วมกัน ซึ่งช่วยให้ภาคธุรกิจสามารถพิสูจน์ความถูกต้องของตัวตนของผู้ที่เข้ามาทำรายการได้ นอกจากนี้ยังช่วยในการพิสูจน์ความถูกต้องของข้อมูลที่ส่งไปได้ และยังช่วยยืนยันการติดต่อการสื่อสารระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลจนทำให้ไม่มีใครสามารถปฏิเสธความรับผิดชอบในการทำรายการได้

ลายมือชื่ออิเล็กทรอนิกส์เป็นกลุ่มข้อมูลอิเล็กทรอนิกส์ที่ใช้ยืนยันตัวบุคคลได้เช่นเดียวกันกับการลงลายมือชื่อของบุคคลบนกระดาษ ทั้งนี้บุคคลที่ 3 (Certificate Authority, CA) จะทำหน้าที่ในการออกใบอนุญาตให้บุคคลต่างๆ ไว้ เพื่อใช้ในการยืนยันตัวตนเมื่อจะเข้าไปทำธุรกรรม

[12] Digital Certificates: A Secure Method for Digital Transfers, Stephen N. Williams, http://www.sans.org/infosecFAQ/encryption/digicert.htm

อิเล็กทรอนิกส์ วิธีการปฏิบัติ CA จะใช้ public key และข้อมูลส่วนบุคคลในการสร้างลายมือชื่ออิเล็กทรอนิกส์ แล้วจึงทำการเข้ารหัสลายมือชื่ออิเล็กทรอนิกส์ นั้น เพื่อให้เจ้าของลายมือชื่ออิเล็กทรอนิกส์สามารถยืนยันตนเองได้ อนึ่งเนื่องจากว่าลายมือชื่ออิเล็กทรอนิกส์นี้ไม่สามารถปลอมแปลงได้ และมีความเป็นเอกลักษณ์เฉพาะตัวเช่นเดียวกันกับลักษณะเฉพาะของลายนิ้วมือของบุคคล ดังนั้นผู้ที่ทำรายการอิเล็กทรอนิกส์จึงไม่สามารถปฏิเสธความรับผิดชอบในการทำรายการได้เลย

ในการติดต่อสื่อสารกัน ผู้ส่งจะใช้ private key ในการลงลายมือชื่ออิเล็กทรอนิกส์ ในขณะที่ผู้รับข้อมูลจะใช้ public key ของผู้ส่งมาใช้ในการพิสูจน์ความถูกต้องของตัวตนของผู้ส่งว่าใช่บุคคลเดียวกันหรือไม่ เพื่อป้องกันการการโต้แย้งและการปฏิเสธความรับผิดชอบ รายละเอียดดังปรากฏอยู่ในแผนภูมิข้างท้ายนี้



ประโยชน์ของลายมือชื่ออิเล็กทรอนิกส์ ในการทำธุรกรรมทางอิเล็กทรอนิกส์มีอยู่ 2 ประการคือ

(1) การยืนยันตัวตนของผู้ถือ ที่อาจเป็นบุคคล web site หรือตัว router

(2) การปกป้องข้อมูลไม่ให้ถูกเปลี่ยนแปลง หรือถูกขโมยไป

ลายมือชื่ออิเล็กทรอนิกส์ สร้างขึ้นมาจากเทคโนโลยี Public Key Infrastructure (PKI) ซึ่งเป็นเทคโนโลยีเดียวกันกับเทคโนโลยีที่ใช้ในฐานยิงอาวุธนิวเคลียร์ PKI ได้ถูกใช้เป็นระบบความปลอดภัยพื้นฐานบนอินเตอร์เน็ต เนื่องจากว่าเป็นระบบที่สามารถออกกุญแจที่ไม่มีความเหมือนกัน

หรือซ้ำกันเลย และผู้รับกับผู้ส่งก็ใช้กุญแจคนละชนิดกันในการส่งและรับข้อมูลระหว่างกัน ทำให้ข้อมูลไม่สามารถถูกเปลี่ยนแปลงแก้ไขได้และทั้งผู้รับและผู้ส่งต่างไม่สามารถปฏิเสธความรับผิดชอบได้

PKI มีคุณลักษณะในการทำงานต่างๆ ในการป้องกันความลับของข้อมูลดังต่อไปนี้คือ

- Authenticate identity : สามารถยืนยันตัวตน และสามารถระบุได้ว่าผู้ที่ทำรายการเป็นบุคคล องค์กร ผู้ดูแล web site หรือผู้ใดที่มีหน้าที่เกี่ยวข้อง

- Verify integrity : สามารถยืนยันว่าเอกสารมิได้ถูกเปลี่ยนแปลงหรือแก้ไขระหว่างทาง

- Ensure privacy : สามารถป้องกันไม่ให้ผู้อื่นเห็นข้อมูลได้ หรือดักจับข้อมูลระหว่างทางได้

- Authorize access : ทำหน้าที่แทน user id และ password ของผู้เข้าทำรายการทางอิเล็กทรอนิกส์ได้

- Authorize transactions: สามารถควบคุมระดับของการทำธุรกรรมได้

- Support for non-repudiation: สามารถป้องกันการปฏิเสธความรับผิดชอบในการทำธุรกรรมบน web ได้

ในการใช้ลายมือชื่ออิเล็กทรอนิกส์ นั้น จะต้องมีการเผยแพร่กุญแจสาธารณะ(public key) ของเจ้าของลายมือชื่ออิเล็กทรอนิกส์ ออกไป เพื่อให้ผู้รับสามารถนำไปใช้ในการพิสูจน์ความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ ดังกล่าวได้ แต่การกระทำดังกล่าวจะไม่มีผลกระทบกับความปลอดภัยแต่ประการใดเพราะตัวลายมือชื่ออิเล็กทรอนิกส์ สามารถรักษาความปลอดภัยของตัวเองได้อยู่แล้ว ประกอบกับที่กุญแจส่วนตัว (private key)ซึ่งเป็นส่วนประกอบของลายมือชื่ออิเล็กทรอนิกส์ ก็เป็นความลับที่ไม่มีใครสามารถทราบได้นอกจากเจ้าของ จึงทำให้การเผยแพร่ข้อมูล public key ไม่มีผลกระทบใดๆ ทั้งนี้วิธีการเผยแพร่ public key มีวิธีการดังต่อไปนี้คือ

- Certificate accompanying signature ผู้ลงลายมือชื่ออิเล็กทรอนิกส์ จะส่งชุดสำรองของข้อมูลมาพร้อมกับลายมือชื่ออิเล็กทรอนิกส์ ด้วยวิธีนี้ผู้ใดที่ต้องการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ ก็จะมีข้อมูลในมือ

- Directory service เป็นการเผยแพร่ข้อมูลผ่านทาง Web ซึ่งจะต้องมีการจัดการที่ดีจึงจะทำให้ผู้รับข้อมูลสามารถไปค้นหาข้อมูลของผู้ส่งข้อมูลได้

เจ้าของลายมือชื่ออิเล็กทรอนิกส์จะเป็นผู้เก็บรักษา private key เพื่อใช้ในการทำงานกับเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย หรือ เวบไซต์ ซึ่งจะมีกุญแจสาธารณะ (public

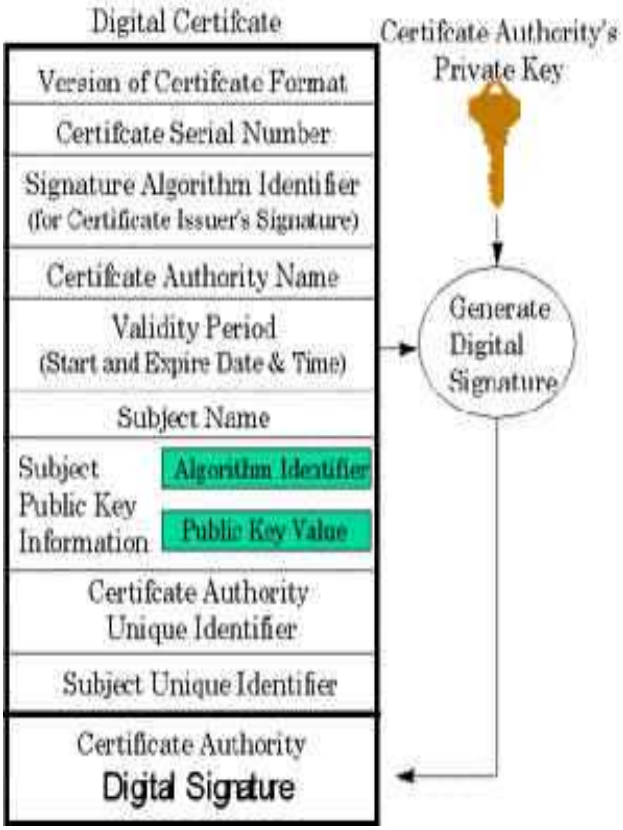
key) ของผู้ใช้งาน แล้วจึงจะมีการจับคู่กัน กุญแจตัวหนึ่งเรียกว่า private key ส่วนกุญแจอีกตัวเรียกว่า public key ตัว public key จะถูกเข้ารหัสไว้แล้ว ส่วนตัว private key จะเป็นกุญแจที่ใช้ในการถอดรหัส

ทั้งนี้ public key จะถูกเผยแพร่ออกไปอย่างทั่วถึงเพื่อให้ผู้ที่ต้องการติดต่อสื่อสารกับเราสามารถติดต่อสื่อสารได้ ส่วน private key จะแสดงถึงลายมือชื่ออิเล็กทรอนิกส์ที่ถูกสร้างขึ้นมาสำหรับผู้ใช้แต่ละคนเท่านั้น private key จึงเป็นความลับที่ผู้เป็นเจ้าของจะต้องเก็บรักษาไว้ให้ดี และจะต้องไม่เปิดเผยหรือเผยแพร่ไปที่ใด เมื่อเราเริ่มติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่น ผ่านเครือข่ายการสื่อสาร เครื่องคอมพิวเตอร์ที่เราติดต่อด้วยก็จะไปดึงเอาข้อมูลของกุญแจสาธารณะ (public key) ที่เรามีอยู่มาใช้เพื่อการยืนยันตัวตนของเรา เมื่อได้ทำการพิสูจน์ความถูกต้องแล้วเครื่องคอมพิวเตอร์ดังกล่าวก็จะทำการเข้ารหัสข้อมูลโดยผ่าน Secured Socket Layer (SSL) อนึ่งก่อนที่จะทำการเข้ารหัสข้อมูล คอมพิวเตอร์จะทำการย่อและย่อยข้อมูลด้วยเทคนิคที่เรียกว่า Secure Hash ก่อนเพื่อให้เกิดความปลอดภัยสูงสุดในการรักษาความลับของข้อมูล ซึ่งผู้รับจะต้องใช้ private key ที่มีอยู่เฉพาะตนเท่านั้นจึงจะสามารถเปิดอ่านข้อมูลได้

Secure Hash เป็นกระบวนการในการลดขนาดของข้อมูลลงให้เล็กที่สุด โดยใช้ขบวนการทางคณิตศาสตร์เข้าช่วยในการสร้างข้อมูลแบบนี้ขึ้น โดยที่มีหลักฐานทางในการดำเนินการทางคณิตศาสตร์ ที่สามารถใช้ยืนยันได้ว่า วิธีการดักล่าวสามารถป้องกันการลอกเลียนข้อมูลได้อย่างแน่นอน เพราะไม่สามารถที่จะสร้างข้อมูลที่มีลักษณะเหมือนกันขึ้นมาเลียนแบบได้เลย

ข้อมูลลายมือชื่ออิเล็กทรอนิกส์ ก็เป็นส่วนประกอบของแผนการรักษาความปลอดภัยของข้อมูลที่ดีนอกเหนือจากการเข้ารหัสข้อมูล ดังนั้นทุกองค์กรควรที่จะให้ความสำคัญกับการออกแบบระบบสร้างโครงสร้างในการรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสข้อมูลด้วย ทั้งนี้เพื่อให้ระบบดังกล่าวสามารถรักษาความปลอดภัยของข้อมูลที่ส่งไปมาได้ และยังสามารถใช้ป้องกันการปฏิเสธความรับผิดชอบในการส่งข้อมูลได้ด้วย นอกจากนี้การเข้ารหัสข้อมูลเพื่อไม่ให้ผู้อื่นแอบดูและเข้าไปแก้ไขได้ก็ได้มีการนำไปใช้โดยทั่วไป ตัวอย่างเช่นการเข้ารหัสข้อมูลในการโอนเงินที่มีมูลค่าสูงในระดับหลายล้านดอลล่าร์สหรัฐอเมริกา การชำระเงินทางอิเล็กทรอนิกส์ การส่งหมายเลขบัตรเครดิตเพื่อการชำระเงิน รวมถึงการใช้บริการ pay-TV , video-on-demand, และการสื่อสารด้วย mobile phone ต่างก็ใช้วิธีการเข้ารหัสข้อมูลทั้งสิ้น

รูปภาพข้างล่างเป็นการแสดงถึงข้อมูลอิเล็กทรอนิกส์ที่ใช้ สำหรับระบบ SET (Secure Electronic Transactions) ซึ่งพัฒนาขึ้นในปี 1995 โดย VISA , MasterCard, VeriSign และอื่นๆ เพื่อสนับสนุนการใช้บัตรเครดิตในการชำระเงินบนเครือข่ายอินเตอร์เน็ต

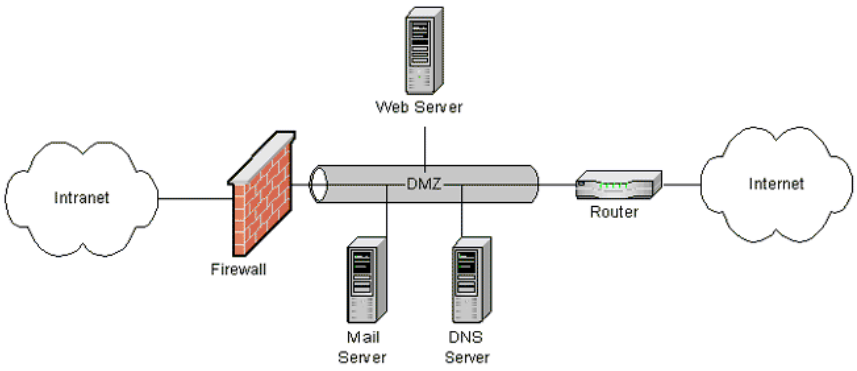


ขั้นตอนการชำระเงินจะเกิดขึ้น เมื่อผู้ซื้อได้สั่งซื้อสินค้าแล้ว ก็จะมีการส่งคำสั่งซื้อไปยังผู้ขาย และผู้ขายก็จะติดต่อไปที่สถาบันการเงินซึ่งจะทำหน้าที่เป็นคนกลางในการทำรายการเช็คสอบเครดิตของผู้ซื้อ แล้วก็จะทำการยืนยันการชำระเงินให้ผู้ขายอีกครั้งหนึ่ง

2. Network Security by Design[13]

การออกแบบระบบเครือข่ายการสื่อสารด้วยคอมพิวเตอร์ที่ปลอดภัยนั้น มีความยุ่งยากมาก ทั้งนี้การรักษาความปลอดภัยในการสื่อสาร ไม่สามารถจัดทำได้โดยวิธีการง่ายๆ โดยการจัดหา Firewall มาติดตั้งไว้ข้างหน้าระบบเครือข่ายการสื่อสารด้วยคอมพิวเตอร์เท่านั้น แต่จะต้องมีการออกแบบและติดตั้งเขตรักษาความปลอดภัย (Demilitarized Zone, DMZ) เพื่อเป็นบริเวณที่จะจัดไว้ให้ระบบการติดต่อสื่อสารจากภายนอกสามารถเข้ามาสู่ server ต่างๆ ก่อนที่จะเข้าสู่ระบบการสื่อสารภายในไว้ด้วย (รายละเอียดดังปรากฏในภาพข้างท้ายนี้)

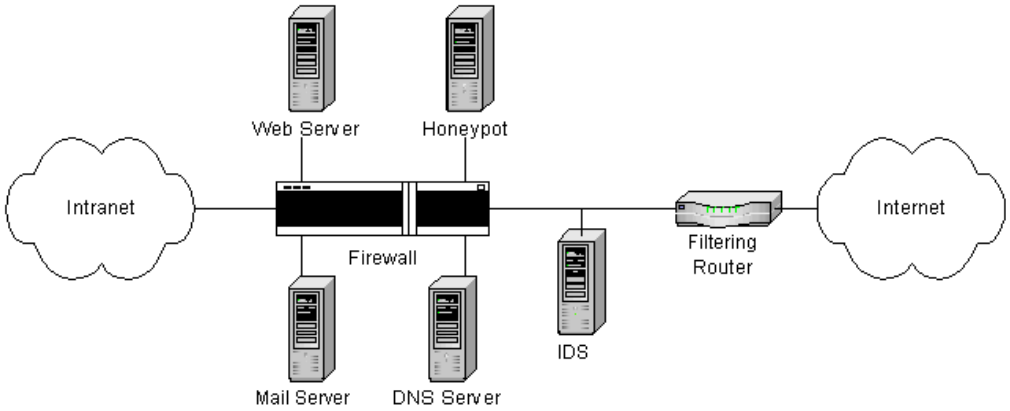
[13] Network Security by Design, Chris Stanley, http://www.sans.org/infosecFAQ/securitybasics/netsec_design.htm



ปัญหาจากความไม่ปลอดภัยที่มาจากเครือข่ายการสื่อสารภายนอกองค์กร

การแก้ปัญหาจะทำได้โดยการวาง DMZ ไว้ที่ด้านหลังอุปกรณ์ router แต่อยู่ข้างหน้า firewall และเครือข่ายการสื่อสารภายใน แม้นว่าการออกแบบการรักษาความปลอดภัยแบบนี้จะสามารถทำได้สะดวกและง่ายแต่ก็ก่อให้เกิดปัญหาในการรักษาความปลอดภัยของ server ต่างๆ ใน DMZ (รายละเอียดดังปรากฏในภาพข้างต้น)

ดังนั้นเพื่อแก้ไขจุดอ่อนในการออกแบบระบบการรักษาความปลอดภัย จะมีการวาง DMZ ไว้ที่ด้านหลังอุปกรณ์ router แต่อยู่ข้างหน้า firewall รวมทั้งมีการติดตั้งอุปกรณ์เพื่อตรวจจับการบุกรุก (intrusion detection system) และ มีการเสริมสร้างความสามารถของ firewall ให้ส่งผ่านข้อมูลที่ถูกต้องไปสู่ server ของระบบงานที่ถูกต้อง แต่จะส่งข้อมูลที่ไม่ได้รับการอนุญาตอย่างถูกต้องไปที่เก็บหรือไม่อนุญาตให้ผ่านที่ honeypot server (รายละเอียดดังปรากฏในภาพข้างท้ายนี้) แต่ในบางกรณีก็จะมีการวางตำแหน่งของ DMZ ไว้ที่ด้านหลังของ firewall ตัวที่3 ซึ่งจะอยู่ก่อนระบบเครือข่ายการติดต่อสื่อสารภายใน (Intranet)



ปัญหาของการเชื่อมโยงระบบการสื่อสารขององค์กรอื่นเข้ามาสู่ระบบงานของเรา

การเชื่อมโยงสายการติดต่อสื่อสารไปยังคู่ค้าทางธุรกิจ จำเป็นที่จะต้องได้รับความสนใจอย่างมากเพราะเป็นจุดอ่อนที่สำคัญในเรื่องการรักษาความปลอดภัย ทั้งนี้เพราะระบบการสื่อสารแบบ LANและ WAN ที่องค์กรเชื่อมโยง ติดต่อสื่อสารเฉพาะภายในองค์กรเท่านั้นที่มีระดับของความปลอดภัยสูงสุด แต่ถ้ามีความจำเป็นต้องเชื่อมโยงเครือข่ายไปนอกองค์กรก็ควรที่จะเลือกใช้เครือข่าย ATM และ gateway-to-gateway VPN รวมทั้งการจัดทำข้อตกลงกับผู้ให้บริการด้านการสื่อสารเพื่อเสริมสร้างความปลอดภัยให้มากยิ่งขึ้น

ปัญหาที่เกิดจากการติดต่อสื่อสารเพื่อเข้าสู่ระบบงานจากระยะไกล

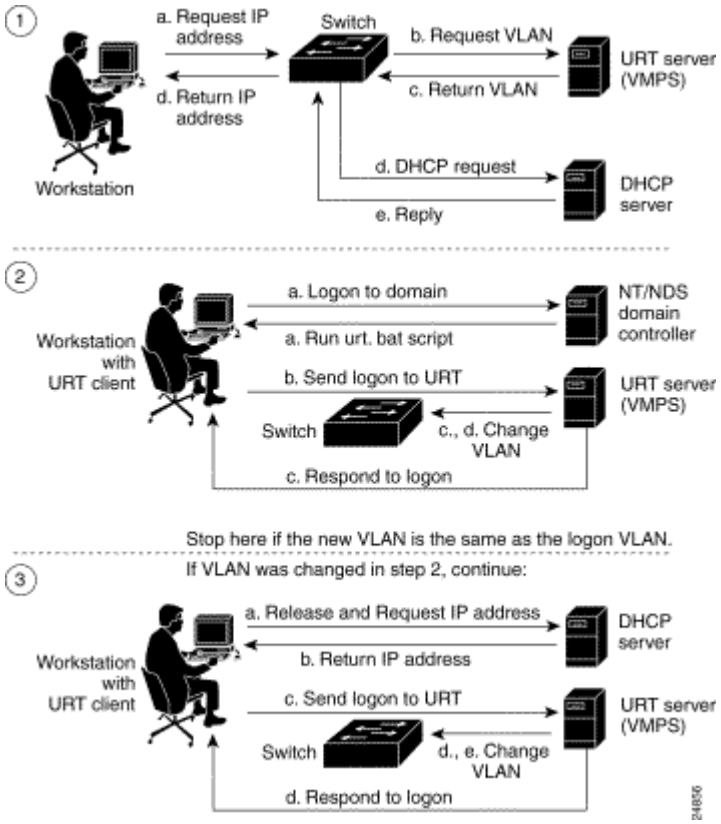
การสื่อสารจากระยะไกลเพื่อเข้ามาใช้ข้อมูลในองค์กรทั้งที่มีอยู่ในระบบ Intranet และ Internet จะต้องมีการกำหนดระดับของการพิสูจน์ตัวตนไว้ตามระดับความสำคัญของข้อมูลเช่น ถ้าเข้ามาดู mail ก็ใช้ระบบ SSL ของ Browser เป็นตัวควบคุม แต่ถ้าเข้ามาใช้งานได้มากกว่านั้นก็จะต้องใช้ token อุปกรณ์เสริมในการพิสูจน์ตัวตนเช่น smart card หรือเครื่องมือที่จะให้รหัสผ่านที่เปลี่ยนแปลงไปทุกครั้ง เป็นต้น

ปัญหาการติดต่อสื่อสารที่เกิดขึ้นภายในองค์กร

การออกแบบระบบการสื่อสารภายในขององค์กรที่ไม่มีประสิทธิภาพ จะก่อให้เกิดช่องทางในการทุจริตได้ ทั้งนี้หน่วยงาน FBI ได้ให้ข้อมูลมาว่า 70%-80% ของเหตุการณ์ที่เกี่ยวข้องกับการโจมตีระบบการสื่อสารด้วยคอมพิวเตอร์ภายในองค์กร มักจะเกิดหรือมีสาเหตุมาจากการดำเนินการภายในองค์กรเอง โดยมีสาเหตุมาจากลูกจ้างที่มีความไม่พอใจต่อองค์กรด้วยเหตุผลต่างๆกันไป หรือเกิดจากสายลับที่อยู่ภายในองค์กร แต่อย่างไรก็ตามตั้งแต่ปี 2000 เป็นต้นมา สัดส่วนของการโจมตีระบบคอมพิวเตอร์ที่มีที่มาจากภายนอกองค์กรได้เพิ่มขึ้นอย่างมากจนเห็นได้ชัดเจนเป็น 20-30 %

ดังนั้นหน่วยงานหลายแห่งจึงได้วางมาตรการป้องกันโดยการควบคุมการตอบรับการเรียกเข้ามาหรือการหนุนสายโทรศัพท์ผ่านออกไปจะต้องทำเฉพาะกับ modem ที่องค์กรได้กำหนดไว้เท่านั้น นอกจากนี้จะมีการใช้โปรแกรมป้องกันไวรัส ที่สามารถ update ข้อมูลเกี่ยวกับไวรัส ได้โดยอัตโนมัติและมีการใช้ PC ในการติดตั้ง firewall

แต่ในสภาพแวดล้อมในการทำงานทั่วไป องค์กรก็มิได้ให้ความสนใจเกี่ยวกับควบคุมการเข้าถึงอุปกรณ์(Physical Access) และก็มิได้ดำเนินการในเชิงป้องกันที่เพียงพอ และเพื่อให้แน่ใจได้ว่าการเชื่อมต่ออุปกรณ์เข้าไปในระบบจะไม่เป็นการเชื่อมต่อเข้าสู่ระบบการสื่อสารได้เองโดยอัตโนมัตินั้นมีการใช้วิธีการแบบเก่าแก่ในการแก้ไขปัญหาคือการระบุรหัส IP ให้อุปกรณ์ที่เชื่อมต่อกับ Hub Port ไว้ กับ Ethernet-card mac address ก็จะสามารถช่วยแก้ปัญหาได้แต่การดำเนินการดังกล่าวก่อให้เกิดค่าใช้จ่าย overhead ที่ค่อนข้างสูง แต่อย่างไรก็ตามเนื่องจาก operating system ในปัจจุบันยอมให้มีการทำเปลี่ยนแปลงแก้ไข mac address ได้ง่าย มาตรการเดิมที่เคยใช้ได้ดีก็มีผลน้อยลงไปมาก บางองค์กรใช้ DHCP system ซึ่งจะมีขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน 2 ขั้นตอน โดยในขั้นแรก เมื่อผู้ใช้งานเปิดระบบเข้าไป คอมพิวเตอร์รับค่า IP ตอนเปิดระบบมาตรวจสอบความถูกต้องก่อนที่จะกำหนดค่า IP ใหม่มาให้ ซึ่งจะทำให้ผู้ใช้งานสามารถขยายขอบเขตและหน้าที่ในการทำงานได้มากขึ้น นอกจากนี้ยังมีการใช้ระบบ network switching ซึ่งจะทำให้ DHCP สามารถใช้งานจาก dynamic VLAN ซึ่งจะช่วยให้ผู้ใช้งานสามารถติดต่อเข้าสู่ระบบงานย่อยได้เสมอว่าจะอยู่ที่ไหนก็ตาม
(รายละเอียดดังปรากฏอยู่ในภาพข้างท้ายนี้)



3. Trust Model in PGP and X.509 Standard PKI[14]

คำนำ

ในชีวิตจริงเราสามารถยืนยันตัวบุคคลได้โดยการใช้บัตรประจำตัวประชาชนหนังสือเดินทาง หรือ ใบขับขี่ ที่ออกให้โดยหน่วยงานที่เชื่อถือได้ แต่ในโลกของการสื่อสารด้วยสื่ออิเล็กทรอนิกส์ เราจะต้องใช้ลายมือชื่ออิเล็กทรอนิกส์ ซึ่งอาศัยการเทคนิคในการเข้ารหัส public key จากโครงสร้างและแนวทางในการกำหนด public key ที่ปลอดภัยและมีประสิทธิภาพจาก Public Key Infrastructure

PKI และ Cryptography

การเข้ารหัส (encryption) ก็คือการเปลี่ยนแปลงรูปแบบของข้อความตามปกติให้เป็นข้อความที่อ่านไม่ได้ใจความ แต่สามารถเปลี่ยนแปลงให้กลับไปเป็นข้อความที่อ่านได้ชัดเจนเหมือนเดิม (decryption) ได้ซึ่งสามารถแบ่งวิธีการดังกล่าวออกได้เป็น 2 วิธีใหญ่ๆ คือ

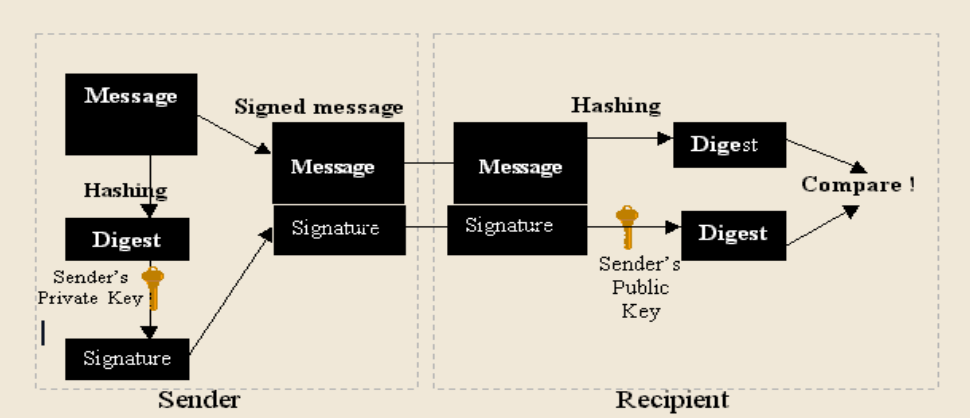
[14] Trust Model in PGP and X.509 Standard PKI, Eyas Al-Hajery, http://www.sans.org/infosecFAQ/encryption/trust_model.htm

(1) Private Key (Symmetric) Crytography คือ การใช้กุญแจดอกเดียวกัน ทั้งที่ใช้ในการเข้ารหัสและการถอดรหัส ซึ่งทั้งผู้รับและผู้ส่งจะใช้กุญแจดอกเดียวกันทั้งสำหรับรับและส่งข้อมูลระหว่างกัน

(2) Public Key(Asymmetric) Crytography คือการใช้กุญแจ 2 ดอกที่แตกต่างกันสำหรับการเข้าและการถอดรหัส โดยผู้ส่งจะต้องกุญแจดอกหนึ่งในการเข้ารหัส และให้ผู้รับใช้กุญแจอีกดอกหนึ่งในการถอดรหัสเสมอ ทั้งนี้กุญแจทั้งหมดจะถูกสร้างขึ้นมาจากการคำนวณทางคณิตศาสตร์ โดยมีการสร้างกุญแจส่วนตัว (private key) ให้เจ้าของเก็บรักษาไว้เป็นความลับ ส่วนกุญแจอีกดอกหนึ่งเรียกว่ากุญแจสาธารณะ (public key) ที่ต้องประกาศให้รู้ทั่วไป ซึ่งในขั้นตอนการติดต่อสื่อสารกันสามารถสรุปได้ดังนี้คือ ถ้านาย ก ต้องการส่งข้อมูลลับให้นาย ข โดยที่นาย ก ต้องใช้กุญแจสาธารณะของนาย ข ในการเข้ารหัส ซึ่งนาย ข จะต้องใช้กุญแจส่วนตัวของตนเองเท่านั้น ในการถอดรหัสเพื่ออ่านข้อมูลได้ แต่ก็มีข้อเสียของการใช้กุญแจสาธารณะจะทำให้ความเร็วในการติดต่อสื่อสารลดลง ดังนั้นในทางปฏิบัติเราจะใช้ระบบกุญแจดอกเดียวและกุญแจ 2 ดอกร่วมกัน โดยจะส่งข้อมูลโดยเข้ารหัสลับแบบกุญแจดอกเดียว แต่จะใช้ระบบการเข้ารหัสแบบกุญแจ 2 ดอก ในการจัดส่งกุญแจถอดรหัสข้อมูลไปให้อีกขั้นหนึ่ง

Digital Signature ลายมือชื่ออิเล็กทรอนิกส์

จะอาศัยแนวทางในเรื่องกุญแจสาธารณะในการเข้ารหัสข้อมูล ซึ่งข้อมูลจะถูกย่อยโดยวิธีการ hashing algorithm ที่จะได้ข้อความย่อที่ไม่เหมือนเดิม และไม่สามารถทำการย้อนกลับจากข้อความย่อไปสู่ข้อความต้นฉบับได้เลย และข้อมูลย่อยจะต้องเปลี่ยนแปลงไปตามข้อความต้นฉบับที่เปลี่ยนไปเสมอทั้งนี้เพื่อเป็นการยืนยันความถูกต้องของข้อมูล ดังนั้นลายมือชื่ออิเล็กทรอนิกส์ก็จะใช้ประโยชน์จากทั้งเทคนิคการเข้ารหัสแบบกุญแจดอกเดียว และhashing algorithm โดยที่ข้อมูลที่ผ่านการย่อยแล้วจะถูกเข้ารหัสโดยกุญแจส่วนตัวของผู้ส่ง แล้วผู้รับข้อมูลก็จะใช้กุญแจสาธารณะของผู้ส่งในการถอดรหัส เพื่อคำนวณผลที่ได้กับข้อมูลที่ส่งมา ถ้าผลที่ได้ถูกต้องตรงกัน ก็เป็นการยืนยันว่าข้อมูลถูกต้องเชื่อถือได้ (รายละเอียดดังปรากฏอยู่ในภาพข้างล่างนี้)



Digital Certificate

เมื่อนาย ก ต้องการส่งข้อมูลให้นาย ข นาย ก จะต้องใช้กุญแจสาธารณะของนาย ข ในการเข้ารหัส กุญแจที่ใช้ต้องเป็นของนาย ข เท่านั้น แต่ก็เป็นไปได้ที่คนอื่นจะแอบอ้างเป็นนาย ข ได้ ซึ่งเราเรียกวิธีการนี้ว่าการโจมตีโดยคนกลาง man-in-the-middle-attack ซึ่งผู้แอบอ้างจะใช้กุญแจที่แอบอ้างว่าเป็นของนาย ข ที่ถูกต้อง ดังนั้นเมื่อผู้ส่งเข้าใจผิดไปนำกุญแจดังกล่าวไปเข้ารหัสข้อมูล ข้อมูลดังกล่าวก็จะ ถูกถอดรหัสได้โดยคนอื่นที่แอบอ้างเป็นนาย ข ได้ ดังนั้นในระบบการสื่อสารที่มีเครือข่ายขนาดใหญ่เช่นอินเตอร์เน็ต ซึ่งมีผู้ใช้จำนวนมาก จึงมีความจำเป็นที่จะต้องมีหน่วยงานกลาง (บุคคลที่ 3) เพื่อให้ทำการยืนยันกุญแจสาธารณะของคนอื่นๆในระบบ ทั้งนี้ข้อมูลลายมือชื่ออิเล็กทรอนิกส์เป็นข้อมูลส่วนตัวของบุคคลหรือองค์กร ที่ผ่านการรับรองจากหน่วยงานกลางที่ทำการตรวจสอบข้อมูล ก่อนที่จะออกใบอนุญาตให้ ซึ่งจะประกอบไปด้วยข้อมูลกุญแจสาธารณะของผู้ถือ serial number ข้อมูลส่วนตัวและอื่นๆ ภายใต้มาตรฐาน X.509

4. Virtual Private Network (VPN)[15]

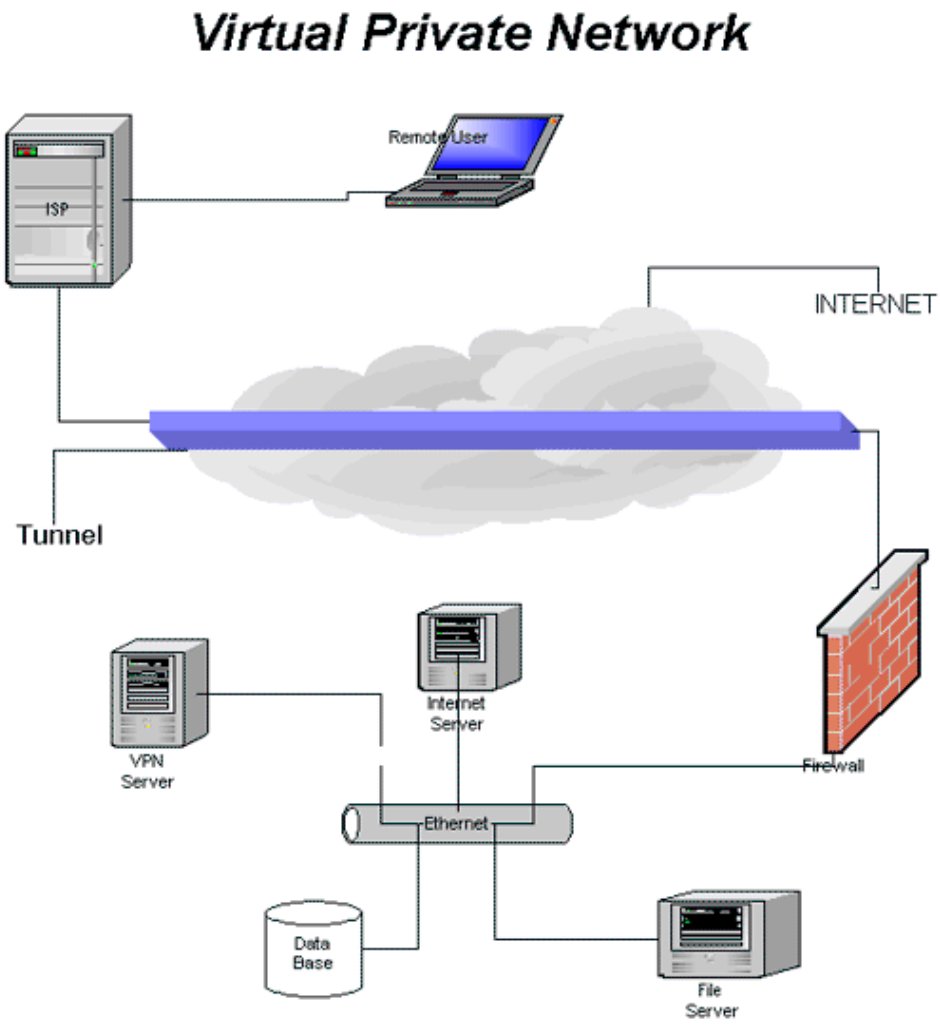
บทความชุดนี้ มีวัตถุประสงค์ที่จะแสดงให้เห็นถึงคุณลักษณะของ VPN ในส่วนที่เกี่ยวข้องกับการรักษาความปลอดภัยของอินเตอร์เน็ต ซึ่งประกอบไปด้วยลักษณะดังต่อไปนี้คือ

(1) Authentication : ความสามารถในการยืนยันตัวตน ของผู้ติดต่อเชื่อมต่อระบบทั้งสองฝั่ง

(2) Integrity : ความสามารถในการยืนยันความสมบูรณ์ ถูกต้อง ครบถ้วนของข้อมูลที่ส่ง

(3) Confidentiality : ความสามารถที่จะช่วยยืนยันและให้ความมั่นใจ ได้ว่าข้อมูลที่ส่งไปมิได้ถูกอ่านหรือเห็นโดยบุคคลอื่นที่มิใช่ผู้รับที่แท้จริง

[15] Virtual Private Network (VPN) Security, Gregory J.Ciolek, http:// www.sans.org/infosecFAQ/encrytion/VPN_sec.htm



VPN เป็นเครือข่ายการสื่อสารด้วยคอมพิวเตอร์แบบหนึ่ง ซึ่งอาศัยทั้งเครือข่ายคอมพิวเตอร์ส่วนตัว (private network) และเครือข่ายอินเตอร์เน็ต ซึ่งเป็นเครือข่ายการสื่อสารแบบสาธารณะ (public network) แต่ได้เพิ่มเติมระบบการรักษาความปลอดภัยเข้าไป จนเครือข่ายคอมพิวเตอร์ที่เกิดขึ้นจากเครือข่ายทั้ง 2 ระบบ มีความปลอดภัยได้เสมือนหนึ่งว่าเป็นเครือข่ายคอมพิวเตอร์ส่วนตัว (private network) โดยมีหลักการในการทำงานโดยย่อดังต่อไปนี้คือ

เครือข่าย VPN จะสร้างช่องทางติดต่อสื่อสารที่ปลอดภัย ซึ่งมีลักษณะเหมือนเป็นการสร้างท่อติดต่อโดยเฉพาะผ่านช่องทางบนเครือข่ายอินเตอร์เน็ต (Tunneling) จากนั้นก็จะย่อยข้อมูลเป็นหน่วยย่อยๆ (packet) พร้อมทั้งกำหนดค่า IP และทำการเข้ารหัสข้อมูล หลังจากนั้นจึงส่ง packet เหล่านั้นผ่านไปบนเครือข่ายอินเตอร์เน็ต เมื่อ packet เหล่านั้นไปถึงปลายทางก็จะถูกถอดรหัสพร้อมทำการตรวจสอบค่า IP เพื่อดำเนินการกับข้อมูลชุดนั้นๆ ต่อไป ทั้งนี้เครือข่าย VPN จะมีระเบียบวิธีในการ

ปฏิบัติงาน (protocol) ที่ใช้อยู่โดยทั่วไปอยู่ 3 แบบด้วยกันคือ Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP) และ Point to Point Tunneling Protocol (PPTP)

Internet Protocol Security (IPSec)

IPSec เป็นส่วนหนึ่งของกลุ่ม IP โปรโตคอล โดยประกอบไปด้วย 2 โปรโตคอล คือ AH(Authentication header) และ ESP (Encapsulated Security Payload) เมื่อมีการใช้ IPSec ทั้ง AH และ ESP จะให้บริการทั้ง 3 ด้านคือ authentication, integrity และ confidentiality

AH header จะอยู่ถัดจาก IP header ประกอบไปด้วยข้อมูลที่ถูกเข้ารหัสและการทำ Secure Hash โดย AH จะปกป้องที่อยู่ต้นทางและปลายทางของ IP header

ESP header จะทำการเข้ารหัสข้อมูลที่ดูแลความเป็นส่วนตัวและความน่าเชื่อถือ ESP นี้จะทำงานร่วมกับระบบกุญแจเดี่ยว (symmetric encryption algorithm) เช่น DES, 3DES และ Blowfish ดังนั้นการติดต่อสื่อสาร โดยใช้ IPSec โปรโตคอล จึงมีความจำเป็นที่จะต้องใช้วิธีเข้ารหัสและตัวกุญแจที่เหมือนกันทั้งสองด้าน ทั้งนี้ IPSec ยังสามารถใช้ร่วมกับ key management เพื่อสนับสนุนการใช้ digital certificates และยังสนับสนุนการใช้ Internet Key Exchange (IKE) ซึ่งเป็นวิธีที่ใช้แลกเปลี่ยน Key บนเครือข่ายอินเตอร์เน็ตได้ด้วย

Point to Point Tunneling Protocol (PPTP)

PPTP ได้ถูกพัฒนาโดยบริษัท Microsoft, Ascend, 3Com, US Robotics และ ECI Telematics ดังนั้นบริษัทไมโครซอฟท์ จึงให้การสนับสนุน PPTP ซึ่งได้ใช้ Extensible Authentication Protocol (EAP) ของ Microsoft ในการยืนยันตัวตนของผู้ติดต่อเชื่อมต่อระบบทั้งสองฝั่ง นอกจากนี้ PPTP ยังสนับสนุนการใช้ Challenge-Handshake Authentication Protocol (MS-CHAP), CHAP, Shiva Password Authentication Protocol (SPAP) และ Password Authentication Protocol (PAP) ซึ่งโปรโตคอลทั้งหมดเหล่านี้ จะทำงานโดยอาศัยความแข็งแกร่งของระบบพื้นฐานของการกำหนดรหัสผ่านรายการ (password) ดังนั้นการกำหนดนโยบายเกี่ยวกับการใช้ password ที่ดีเท่านั้นที่จะนำไปสู่ความสำเร็จในการรักษาความปลอดภัย และการยืนยันตัวตน (authentication) ทั้งนี้นโยบายการกำหนดรหัสผ่านรายการ (password) ที่ดี ควรจะประกอบไปด้วยคุณลักษณะดังต่อไปนี้คือ

- มีความยาวระหว่าง 6 – 8 ตัวอักษร
- ต้องมีตัวอักษรตัวเล็ก อักษรตัวใหญ่ ตัวเลข อย่างละ 1 หน่วย
- ต้องไม่มีตัวอักษรที่เหมือนกันในตำแหน่งที่อยู่ติดกันเลย
- ต้องไม่มีการใช้ รหัสผ่านรายการ password ชุดเดิมอีก
- ต้องไม่มีส่วนที่เป็น user name
- ต้องเปลี่ยนทุก 60 วัน

- รหัสผ่านรายการต้องยากต่อการคาดเดาและไม่สามารถใช้โปรแกรมตรวจเช็คได้

นอกจากนี้ ระบบจะต้องหยุดให้บริการต่อลูกค้าที่ใส่รหัสผ่านรายการผิดพลาดติดต่อกันถึง 3 ครั้ง และจะต้องมีการตรวจสอบการเปลี่ยน password ของ user เป็นระยะๆ PPTP ทำการเข้ารหัส PPP frame ในส่วนของข้อมูล IP ที่ใช้ส่งไปบนเครือข่ายอินเตอร์เน็ตโดยการใช้ Generic Routing Encapsulation (GRE)

การเข้ารหัสของ PPTP ได้ใช้ Microsoft Point-to-Point Encryption (MPPE) โดย MPPE ได้จัดการการเชื่อมโยงที่เข้ารหัส และใน Window 2000 ต้องใช้ EAP หรือ MS-CHAP ที่จะเข้ารหัส PPTP ในขณะที่ MPPE ใช้การเข้ารหัส RSA RC4 ที่ใช้จำนวน bit เป็น 40 bit, 56 bit และ 128 bit

Layer Two Tunneling Protocol (L2TP)

L2TP เป็นการใช้ PPTP ร่วมกับ Layer 2 Forwarding (L2F) ที่ถูกพัฒนาโดย Cisco system ซึ่งในการสร้างท่อเชื่อมต่อกันได้ใช้เทคนิคการเข้ารหัสหลายชั้นเช่น L2TP, UDP, IPSec, IP และ Data Link L2TP จะทำการยืนยันตัวตนของผู้ติดต่อเข้าสู่ระบบ (authenticate) ทั้งผู้ใช้งานและเครื่องคอมพิวเตอร์ที่ใช้ โดยจะทำการ authenticate เครื่องคอมพิวเตอร์ที่ใช้งานผ่าน IPSec ESP และจะทำการยืนยันตัวตนของผู้ใช้งาน ผ่าน PPTP โดยใช้ MS-CHAP, CHAP, SPAP และ PAP ทั้งนี้ การเข้ารหัสที่ใช้ L2TP บน IPSec จะใช้ เทคนิคการเข้ารหัสแบบ DES และ 3DES

Firewalls

Firewall เป็นอุปกรณ์ที่ใช้ร่วมกับ VPN เพื่อเสริมสร้างให้เกิดความน่าเชื่อถือมากขึ้น ซึ่งการวางตำแหน่งของ firewall ร่วมกับเครื่อง VPN มีอยู่ 3 วิธีดังนี้คือ

(1) วาง firewall ระหว่างอินเตอร์เน็ตกับเครื่อง VPN ที่ต่อเชื่อมยังการสื่อสารภายใน

(2) วาง firewall ระหว่างเครื่อง VPN กับระบบการสื่อสารภายใน

(3) วาง VPN แบบคู่ขนานไปกับ firewall

วิธีที่ง่ายที่สุดคือวาง VPN แบบคู่ขนานไปกับ firewall เพราะว่าไม่จำเป็นต้องกำหนดค่าภายใน (configure) ของเครื่อง firewall แต่ข้อเสียก็คือเป็นการเปิดช่องทางการติดต่อสื่อสารมากขึ้นเป็น 2 ช่องทาง

การวาง VPN อยู่ไว้ที่ด้านหลังของ firewall นั้นเราจำเป็นที่จะต้องเปลี่ยนแปลงค่า (configure) ของ firewall เพราะว่า firewall บางประเภทก็มีข้อจำกัดจนไม่สามารถแยกช่องทางสื่อสารของ VPN ได้

การวางเครื่อง VPN ไว้ด้านหน้า firewall เป็นวิธีที่ปลอดภัยที่สุด เพราะว่าเครื่อง VPN จะสามารถแยกแยะได้ว่าถ้าเป็นข้อมูลที่ส่งเข้ามาเป็นของ VPN นั้น เครื่องก็จะทำการ authenticate และถอดรหัสข้อมูล จากนั้นจะส่งข้อมูลดังกล่าวไปยัง firewall เพื่อไปยังจุดหมายปลายทางต่อไป แต่ถ้าไม่ใช่ข้อมูลของ VPN เครื่องก็จะส่งข้อมูลผ่านตรงไปที่ firewall ทันทีเลย

อนึ่งการวางเครื่อง VPN ไว้บนเครื่องเดียวกันกับ firewall เป็นสิ่งที่ไม่ควรทำเพราะจะทำให้ประสิทธิภาพของการทำงานต่ำลงทั้งคู่

Authentication Re-enforcement's

การเสริมสร้างประสิทธิภาพในการการยืนยันตัวตนของผู้ใช้งาน (authenticate) บน VPN สามารถกระทำได้โดยการเลือกใช้อุปกรณ์เสริมดังเช่น smart card และ token card ทั้งนี้การเลือกใช้อุปกรณ์แต่ละแบบก็จะมีผลกระทบกับงบประมาณในการลงทุนด้วย

Smart Card

Smart card เป็นอุปกรณ์ที่มีขนาดเท่าบัตรเครดิต มีหน่วยความจำและประมวลผลอยู่ฝังอยู่ภายใน ที่บรรจุข้อมูลผู้ถือบัตรพร้อมทั้งกุญแจที่ถูกเข้ารหัสไว้แล้ว ซึ่งจำเป็นต้องใช้ร่วมกับรหัสผ่าน (Password) ในการใช้งาน

Token card

Token card มีลักษณะคล้ายกับ smart card แต่จะมีจอ LCD และ keypad เพื่อให้ผู้ใช้งานป้อน PIN หลังจากนั้น Token card ก็จะแสดงรหัสผ่านเพื่อให้ผู้ใช้งาน นำไปใช้เพื่อติดต่อเข้าสู่ระบบเครือข่ายการสื่อสารต่อไป

Remote Authentication Dial-In User Service (Radius Servers)

เครื่อง Radius จะเก็บข้อมูล authenticate ไว้ที่ฐานข้อมูล และเก็บข้อมูลผู้ใช้งาน VPN ที่อาจมีค่าที่เป็นตัวแปร ค่า IP การ callback ข้อมูล account รวมอยู่ด้วย

ภาคผนวก 5 : รายการขอข้อมูลและเอกสาร ที่ใช้ในการตรวจสอบสถาบันการเงิน

เอกสารที่จะยื่นให้สถาบันการเงิน
พร้อมกับหนังสือแจ้งการตรวจสอบ

การตรวจสอบด้าน E-Banking

ธนาคาร ..... จำกัด (มหาชน)

วันที่ตรวจสอบ .....

รายการขอข้อมูลและเอกสารที่ใช้ในการตรวจสอบสถาบันการเงิน สำหรับผู้ตรวจสอบ ธนาคารแห่งประเทศไทย ตามรายการดังต่อไปนี้

1. ขอให้จัดพนักงานมาบรรยายสรุปโดยย่อในช่วง 2 วันทำการแรกที่เข้าทำการตรวจสอบในหัวข้อต่อไปนี้

1.1 ทิศทางและแนวนโยบายทางด้าน E-Banking

1.2 ลักษณะการให้บริการทางด้าน E-Banking

1.3 IT Configuration ระบบ Network และการปฏิบัติงานภายในศูนย์คอมพิวเตอร์

1.4 มาตรการรักษาความปลอดภัย

1.5 การตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ

2. รายการขอสำเนา/ไฟล์ข้อมูลหรือเอกสารยืมมาเพื่อตรวจสอบ ดังนี้

2.1 นโยบายและการจัดการ

2.1.1 Organization Chart ล่าสุดของฝ่ายและส่วนงานที่เกี่ยวข้องทางด้าน E-Banking รวมถึงฝ่ายตรวจสอบคอมพิวเตอร์

2.1.2 สำเนาของนโยบายทั่วๆไปทางด้าน E-Banking

2.1.3 สำเนาของนโยบายและขั้นตอนการดำเนินงานเฉพาะด้านที่เกี่ยวข้องกับการปฏิบัติงาน E-Banking เช่น การออกผลิตภัณฑ์และบริการใหม่ ช่องทางเสนอบริการใหม่

2.1.4 สำเนานโยบายทางด้านการรักษาความปลอดภัยระบบ

2.1.5 แฟ้มบันทึกการประชุมคณะกรรมการ และคณะทำงานต่างๆที่เกี่ยวข้องกับ E-Banking

2.1.6 สำเนาผลประเมินความเสี่ยงและสอบทานการทำธุรกรรม E-Banking

2.1.7 สำเนาของแผนกลยุทธ์ และผลการศึกษาความเป็นไปได้ การวิเคราะห์ต้นทุนและประโยชน์ที่จะได้รับ (cost/benefit analysis), แผนทดสอบระบบและผลการทดสอบ, แผนใช้งานจริง และผลจากการนำระบบไปใช้งานจริง (deployment plans and reviews)

2.1.8 รายงานที่ใช้วัดและวิเคราะห์ผลการดำเนินงานจริงเทียบกับเป้าหมายที่คาดคะเนไว้ ได้แก่ผลการดำเนินงานในธุรกิจหลัก เช่น อัตราการเติบโตของเงินฝาก และในด้านเทคโนโลยี เช่น ขีดความสามารถในการประมวลผลรายการและสนับสนุนการทำธุรกรรมต่างๆ

2.1.9 สำเนาของนโยบายด้านการทำประกันภัยสำหรับการทำธุรกรรม E-Banking

2.1.10 สำเนาของแผนสำรอง/ฉุกเฉินทางด้าน E-Banking

2.1.11 ข้อมูลเกี่ยวกับคดีความอันสืบเนื่องมาจากการทำธุรกรรมที่กำลังอยู่ระหว่างการดำเนินการและ/หรือดำเนินการเรียบร้อยแล้ว

2.1.12 สำเนาของรายงานการเข้ารับฝึกอบรมและ/หรือพัฒนาทางด้าน E-Banking เช่น ตารางเวลา (schedule) พร้อมวันที่ ผู้เข้าร่วมการอบรมและหัวข้อการอบรม

2.2 การปฏิบัติการ

2.2.1 รายชื่อ ตำแหน่ง หมายเลขโทรศัพท์ติดต่อ ของ Contact persons ทางด้าน E-Banking และผังโครงสร้างส่วนงาน E-Banking รวมทั้ง Job Description ของแต่ละตำแหน่งงาน

2.2.2 สำเนาของรายละเอียด Electronic Banking Platforms ที่ใช้ และ System Topology Maps ซึ่งครอบคลุมถึง server, routers, firewalls และองค์ประกอบอื่นๆของระบบงาน

2.2.3 สำเนาขั้นตอนการปฏิบัติงานทางด้านการรักษาความปลอดภัยระบบ

2.2.4 สำเนารายงานที่ใช้ติดตามการทำงานของระบบ E-Banking เช่น ปริมาณธุรกรรม แนวโน้ม ภัยคุกคามต่างๆที่เกิดแก่ระบบงาน

2.2.5 รายชื่อของผู้ใช้ระบบที่ได้รับอนุญาตและระดับการเข้าถึงระบบ ได้แก่ เจ้าหน้าที่พนักงาน ผู้แทนจำหน่ายระบบงาน, ลูกค้า และกลุ่มผู้ใช้อื่น

2.2.6 สำเนาของรายการกิจกรรมที่ต้องให้ความสนใจเป็นพิเศษ (Exceptional reports), ผลสอบทาน logs และรายชื่อพนักงานผู้สอบทานรายงานและเวลา

2.2.7 รายงานการติดตามรูปแบบพฤติกรรมของลูกค้าในการเข้าใช้บริการผ่านเครือข่าย Internet

2.2.8 ระเบียบและ/หลักเกณฑ์ของธนาคารในการพิจารณาคัดเลือกโปรแกรมระบบงาน และ/หรืออุปกรณ์ทางคอมพิวเตอร์ที่เกี่ยวข้องกับระบบงาน E-Banking ของบริษัทตัวแทนจำหน่ายต่างๆ

2.2.9 แฟ้มแสดงรายละเอียดการจัดซื้อโปรแกรมระบบงาน และ/หรือการจัดจ้างบริษัทผู้ให้บริการภายนอก (ประกอบด้วย สัญญาหรือข้อตกลงในการจัดซื้อ/จัดจ้าง บันทึกการประชุมคณะทำงาน เอกสารการทำ due diligence review บริษัทผู้ให้บริการ คู่สัญญา บริษัทผู้แทนจำหน่ายระบบงาน และเอกสารประกอบอื่นๆในขั้นตอนของกระบวนการจัดซื้อ/จัดจ้าง)

2.2.10 สัญญาบำรุงรักษาเครื่องอุปกรณ์คอมพิวเตอร์ต่างๆ เช่น Server, Firewall ของระบบงาน E-Banking

2.3 การตรวจสอบ

2.3.1 สำเนาเอกสารการตรวจสอบโดยผู้ตรวจสอบภายใน ได้แก่ แผนการตรวจสอบ (Audit schedule) ขอบเขตการตรวจสอบ รายงานการตรวจสอบ และประวัติของผู้ตรวจสอบ

2.3.2 สำเนาเอกสารการตรวจสอบโดยผู้ตรวจสอบภายนอก ได้แก่ สัญญาการว่าจ้าง แผนการตรวจสอบ (Audit schedule) ขอบเขตการตรวจสอบ รายงานการตรวจสอบ

2.3.3 สำเนารายงานผลการตรวจสอบ ประเมิน และสอบทานระบบรักษาความปลอดภัยโดยองค์กรภายนอกและ/หรือภายใน

2.3.4 แฟ้มบันทึกการประชุมคณะกรรมการตรวจสอบคอมพิวเตอร์