ธนาคารแห่งประเทศไทย

คู่มือ Check List ตรวจสอบเทคนิคเชิงลึก (เล่ม1)

สนับสนุนการตรวจสอบตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

Version 1.0

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ
สายกำกับสถาบันการเงิน
ธันวาคม 2558

สารบัญ

Executive Summary

ที่มาและเหตุผลความจำเป็น

ระบบเทคโนโลยีสารสนเทศ (IT) นับเป็นโครงสร้างพื้นฐานสำคัญที่ใช้รองรับกลยุทธ์และกระบวนการดำเนินธุรกิจด้านต่างๆ (Business Process) ของธนาคารพาณิชย์ (ธพ.) จุดอ่อนหรือช่องโหว่ของระบบ IT อาจมีผลต่อความปลอดภัย ความถูกต้องและความต่อเนื่องในการให้บริการทางการเงินแก่ลูกค้าประชาชน อีกทั้งอาจส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือของ ธพ. แต่ละแห่งหรือระบบสถาบันการเงินโดยรวม ดังนั้น ธปท. จึงได้จัดให้มีโครงการจัดทำแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยง (IT Best Practices) ด้าน Operational/ IT Risk Management ของ ธพ. ที่เชื่อมโยงกับธุรกิจหลัก โดยมุ่งเน้นธุรกรรมที่มีผลกระทบต่อประชาชนในวงกว้าง เพื่อให้ ธพ. สามารถนำไปใช้เป็นแนวทางในการควบคุมความเสี่ยงตนเอง (Self Control System) และพัฒนาโครงสร้างพื้นฐานระบบ IT พร้อมรองรับกลยุทธ์การขยายธุรกิจในอนาคต ตลอดจนใช้ในการพัฒนาการกำกับดูแลสถาบันการเงินของ ธปท. ให้ทันกับวิวัฒนาการและความเสี่ยงที่เปลี่ยนแปลงที่เกิดขึ้น โดยในปี 2556 และ 2557 ได้จัดทำ IT Best Practices Phase 1 และ Phase 2 ที่ครอบคลุมธุรกิจด้านเงินฝาก ถอน และโอนเงินรวมถึงการให้บริการการเงินและการชำระเงินทางอิเล็กทรอนิกส์เสร็จไปแล้ว

ในปี 2558 ทางฝตส. ได้จัดทำโครงการตรวจสอบระบบปฏิบัติการทางเทคนิคเชิงลึกสำหรับเครื่องคอมพิวเตอร์แม่ข่าย โดยเน้นเรื่องการกำหนดสิทธิ์ของผู้ใช้งาน การรักษาความปลอดภัยบนระบบปฏิบัติการ และการเก็บหลักฐานหรือเหตุการณ์ในการเข้าถึงเครื่องคอมพิวเตอร์ (Audit Log) โดยระบบปฏิบัติการที่จะทำการตรวจสอบ ได้แก่ AIX AS/400 และMicrosoft Window Server ซึ่ง ธพ. ส่วนใหญ่ใช้เป็นระบบปฏิบัติการหลักสำหรับเครื่องคอมพิวเตอร์แม่ข่าย เพื่อให้ผู้ตรวจสอบ ธปท. สามารถนำไปใช้เป็นแนวทางการตรวจสอบระบบปฏิบัติทางเทคนิคที่มีความซับซ้อน และมีประสิทธิภาพมากขึ้น อีกทั้งยังเป็นการลดความเสี่ยงของการรักษาความปลอดภัยที่อาจจะมีแนวโน้มเกิดขึ้น ในกรณีไม่ได้มีการตั้งค่าการรักษาความปลอดภัยของเครื่อง Server อย่างเหมาะสม หรือการให้สิทธิ์การเข้าถึงระบบปฏิบัติการที่ไม่ถูกต้อง รวมทั้งเป็นการเพิ่มประสิทธิภาพในการตรวจสอบและวิเคราะห์ปัญหาในกรณีที่เกิดเหตุการณ์ผิดปกติ (IT Incidents)

สรุปการตรวจสอบระบบปฏิบัติการทางเทคนิคเชิงลึก

1. การกำหนดขอบเขตการจัดทำแนวปฏิบัติที่ดี

ครอบคลุมกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ ดังต่อไปนี้

1. การควบคุมการเข้าถึงระบบปฏิบัติการ ในการบริหารจัดการบัญชีและสิทธิ์ของผู้ใช้งาน
2. การควบคุมการตั้งค่าความปลอดภัยของระบบปฏิบัติการ เป็นการกำหนดระดับการรักษาความปลอดภัย (Hardening) ของระบบ
3. การกำหนด Audit Log สำหรับการบันทึกเหตุการณ์ให้สามารถใช้ติดตาม ตรวจสอบการเข้าใช้งานระบบของผู้ใช้งาน

2. การเตรียมความพร้อมผู้ตรวจสอบ ธปท .

เตรียมความพร้อมผู้ตรวจสอบ ธปท. ให้เข้าใจแนวทางการตั้งค่า Parameters ของระบบปฏิบัติการ AIX AS/400 และ Window Server

3. การรวบรวมข้อมูล เพื่อจัดทำแนวปฏิบัติที่ดี

ศึกษาการตั้งค่า Parameters ที่เกี่ยวข้องกับการกำหนดสิทธิ์ผู้ใช้งานบนระบบปฏิบัติการและด้านรักษาความปลอดภัยและการกำหนด Audit log เช่น การตั้งค่ารหัสผ่านของระบบ การกำหนดหน้าที่ที่จำเป็นของกลุ่มผู้ใช้งาน และการเก็บ log บนระบบ เป็นต้น

ระบบปฏิบัติการ AS400

เป็นระบบที่พัฒนาโดย IBM เพื่อที่ใช้รองรับการใช้งานข้อมูลที่มีความสำคัญ (Sensitive Data) โดยระบบนี้สามารถทำให้การเก็บข้อมูลและการประมวลผลข้อมูลสามารถทำได้โดยผู้ใช้หลายคนพร้อมกัน (Multitasking) เช่นข้อมูลของการทำธุรกรรมทางการเงินและระบบที่พัฒนานั้นใช้สำหรับการเก็บข้อมูลที่มีปริมาณมากๆ ข้อดีของระบบ AS/400 เป็นระบบที่วางโครงสร้างสถาปัตยกรรมแบบเป็นลำดับชั้น (Layered Machine Architecture) สามารถปรับเปลี่ยนตัวอุปกรณ์ Hardware โดยไม่ต้องมีการหยุดการประมวลผลของงาน ระบบนี้สามารถรองรับการประมวลผลโดยเทคโนโลยีการแบ่งพาร์ติชั่นแบบโลจิคัล (logical partition-LPAR) โดยสามารถติดตั้ง Software ประมวลผลหลายตัวพร้อมกัน

Platform AS/400	รายละเอียดการตรวจสอบ	ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Logical Access	**ส่วนที่ 1 การควบคุมสิทธิและหน้าที่ในการเข้าถึงระบบ Core Banking ทาง Logical**				
วัตถุประสงค์	• เพื่อให้มีการควบคุมการเข้าถึงระบบ Core Banking (AS/400) ที่มีประสิทธิภาพ โดยจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาต (Authorized Person) และหน้าที่ที่กำหนดให้ (Authorized Function) เท่านั้น เพื่อให้มีการจัดการ User Profile ที่เข้มงวดและรัดกุม ทั้งการสร้าง แก้ไข และลบรายชื่อผู้ใช้งานในระบบ ซึ่งสอดคล้องกับลักษณะงานของผู้ใช้งานและนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ				
ความเสี่ยง	• การใช้สิทธิเกินหน้าที่ที่ได้อนุญาตจะเป็นการเปิดโอกาสให้ผู้ไม่ประสงค์ดีสร้างความเสียหายต่อระบบ Core Banking การกำหนดรหัสผ่านที่ง่ายต่อการคาดเดา เช่น default password ตัวเลขเรียงกัน มีความเสี่ยงที่ผู้ไม่ประสงค์ดีจะคาดเดารหัสผ่านของผู้ใช้งานอื่นได้ง่าย ซึ่งเอื้อต่อการสวมสิทธิ์ของผู้ใช้งานอื่นและสามารถเข้าถึงระบบ Core Banking ได้โดยง่าย				
Best Practice	• ระยะเวลาในการระงับรหัสผู้ใช้งานที่ไม่ได้เข้าใช้ระบบมาระยะหนึ่ง • มีการจำกัดสิทธิ์ในการเข้าถึงและการใช้งานโปรแกรมอรรถประโยชน์ (System Utility), Command Line และชุดคำสั่งที่สำคัญ (Command) ที่สำคัญของระบบปฏิบัติการไว้เฉพาะบุคคลที่มีอำนาจหน้าที่เหมาะสมเท่านั้น				

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
	• การกำหนดสิทธิ์ในการเข้าใช้ทรัพยากรสำคัญของระบบงานตามอำนาจหน้าที่อย่างเหมาะสม เช่น การเข้าถึง File, Folder, Library ที่สำคัญ โดยคำนึงถึงสิทธิ์ในการ Read, Write, Execute, Append และ Delete เป็นต้น • มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น รหัสผ่านควรประกอบไปด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ					
Access Control ข้อ 2.4.6.2 (2)	1.1	มีการแสดงข้อมูลเมื่อ log in เช่น วัน/เวลาที่เข้าระบบล่าสุด **Parameter: QDSPSGNINF**	1			ป้องกันผู้ไม่หวังดีลักลอบเข้าใช้งาน
Application Security ข้อ 2.4.6.3 (7)	1.2	ระยะเวลาที่ระบบยินยอมให้ Job inactive หลังจากนั้นจะ take action **Parameter:** QINACTITV	60			
	1.3	Action ที่จะทำหลังหมดเวลา **Parameter:** QINACTMSGQ	*DSCJOB			
	1.4	ระยะเวลาที่ระบบจะ End Job หากข้อ 1.3 เลือก action เป็น Disconnect Job **Parameter:** QDSCJOBITV	120			
Logical Access Control ข้อ 2.3.1 (7)	1.5	ให้ผู้ใช้งานสามารถเข้าระบบได้จากอุปกรณ์เดียว **Parameter: QLMTDEVSSN**	1			
Logical Access Control ข้อ 2.3.1 (1)	1.6	ผู้ใช้งานสิทธิสูง (*ALLOBJ หรือ *SERVICE) สามารถเข้าระบบได้จากที่ใดบ้าง	1			

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
		Parameter: QLMTSECOFR				
Network Access Control ข้อ 2.2.1(10)	1.7	การควบคุมการเชื่อมต่อแบบ Remote sign on **Parameter: QRMTSIGN**	*REJECT			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องทางในการเข้าสู่ระบบได้
Logical Access Control ข้อ 2.3.1 (6)	1.8	สิทธิในการเข้าใช้งาน Object ใหม่ที่ถูกสร้างขึ้น **Parameter: QCRTAUT**	*EXCLUDE (ไม่มีการเปลี่ยนแปลงสิทธิ์ของผู้ใช้ในกรณีที่มีการสร้าง Object ใหม่เกิดขึ้น)			
Logical Access Control ข้อ 2.3.1 (12.1.1)	1.9	รหัสผ่านควรเปลี่ยนทุกกี่วัน **Parameter: QPWDEXPITV**	60			**เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)**
Logical Access Control ข้อ 2.3.1 (12.2)	1.10	รหัสผ่านควรมีความยาวไม่น้อยกว่า xx ตัวอักษร **Parameter: QPWDMINLEN**	8			
	1.11	การกำหนดความซับซ้อนของรหัสผ่าน **Parameter: QPWDLVL**	3			
Logical Access Control ข้อ 2.3.1 (12.3)	1.12	ในรหัสผ่านห้ามตั้งตัวเลขติดกัน **Parameter: QPWDLMTAJC**	1			
	1.13	การใช้ตัวอักษรซ้ำกันในรหัสผ่าน **Parameter: QPWDLMTREP**	2			

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
	1.14	รหัสผ่านใหม่ที่ตั้งมีตัวอักษรเดิมของรหัสผ่านเดิมอยู่ในตำแหน่งเดียวกัน **Parameter: QPWDPOSDIF**	1			**เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)**
Logical Access Control ข้อ 2.3.1 (12.3)	1.15	ในรหัสผ่านต้องมีตัวเลขอยู่ด้วย **Parameter: QPWDRQDDGT**	1			
Logical Access Control ข้อ 2.3.1 (12.4)	1.16	รหัสผ่านถูกล๊อกเมื่อมีการใส่ผิด XX ครั้งติดกัน **Parameter: QMAXSIGN**	3			**มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของระบบรักษาความปลอดภัยในการเข้าสู่ระบบเพื่อเข้าถึงข้อมูลในเครื่องได้**
	1.17	Action เมื่อมีการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนด **Parameter: QMAXSGNACN**	3			
Logical Access Control ข้อ 2.3.1 (12.5)	1.18	รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ xx ครั้งที่ผ่านมา **Parameter: QPWDRQDDIF**	12			**เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)**

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Access Control ข้อ 2.4.6.2 (5)	1.19	การตั้งค่าให้มีการเปลี่ยน Password ในการ sign-on ครั้งแรก Parameter: PWDEXP	*YES			ช่วยยกระดับการรักษาความปลอดภัยระบบให้ดีขึ้น
	ส่วนที่ 2 การควบคุมการตั้งค่าความปลอดภัยของระบบ AS/400					
วัตถุประสงค์	เป็นการกำหนดระดับการรักษาความปลอดภัย (Hardening) ของระบบ Core Banking AS/400 เพื่อป้องกันระบบจากการข้าถึงโดยไม่ได้รับอนุญาต					
ความเสี่ยง	• การกำหนดระดับการรักษาความปลอดภัยที่ต่ำหรืออ่อนจะเอื้อต่อผู้ไม่ประสงค์ดีในการบุกรุกเข้าถึงระบบ Core Banking ได้โดยง่าย					
Best Practice	• มีการลบ ระงับ หรือยกเลิก Services Application หรือ Network Protocol ที่ไม่มีความจำเป็นในการใช้งาน (Hardening)					
System Security Management ข้อ 6	2.1	ระดับการรักษาความปลอดภัยของระบบ AS/400 **Parameter: QSECURITY**	40			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของระบบรักษาความปลอดภัยในการเข้าสู่ระบบเพื่อเข้าถึงข้อมูลในเครื่องได้
Logical Access Control ข้อ 2.3.1 (9)	2.2	การตั้งค่าอุปกรณ์ที่มาเชื่อมต่อโดยตรงกับ OS/400โดยอัตโนมัติ **Parameter: QAUTOCFG**	0			ความเสี่ยงจากการเข้าใช้งานจากอุปกรณ์ที่ไม่ได้รับอนุญาต
	2.3	จำนวน Virtual Device ที่ระบบสร้างให้สำหรับ remote user **Parameter: QAUTOVRT**	0			
Logical Access Control ข้อ 2.3.1 (3.1)	2.4	อนุญาตให้มีการเก็บ Password ที่ถูกถอดรหัสไว้แล้วบนระบบ **Parameter: QRETSVRSEC**	0			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของระบบรักษาความปลอดภัยในการเข้าสู่ระบบเพื่อเข้าถึงข้อมูลในเครื่องได้

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Input Validation ข้อ 1	2.5	การตั้งค่าในกรณีถ้ามีการใส่ข้อมูล (Input) ผิดพลาดบนระบบ (Error) **Parameter:** QDEVRCYACN	*DSCMSG			
Application Security ข้อ 2.4.6.3 (7)	2.6	การตั้งค่าของงานที่ไม่ได้ถูก run (Inactive Job) และผ่าน Time-out ของระบบไปแล้ว **Parameter:** QINACTMSGQ	*DSCJOB			ความเสี่ยงจากผู้ไม่ประสงค์ดีแอบใช้เครื่องที่ log-on ค้างไว้
Logical Access Control ข้อ 2.3.1 (4)	2.7	การตั้งค่าไม่ให้มีการปรับเปลี่ยนสิทธิ์ของผู้ใช้เนื่องจากลงโปรแกรมใหม่ Parameter : QUSEADPAUT	*NO			
Logical Access Control ข้อ 2.3.1 (6)	2.8	การตั้งค่าไม่ให้ผู้ใช้ที่ไม่มีสิทธิ์เข้าไปแก้ไข QSYS.Lib ซึ่งเป็น Library ของระบบ Parameter : QPWFSERVER	*EXCLUDE			
	ส่วนที่ 3 การกำหนด Audit Log					
วัตถุประสงค์	เพื่อกำหนดระดับการเก็บข้อมูล Log การเข้าใช้งานระบบ Core Banking AS/400 ที่เพียงพอต่อการสอบทานเหตุการณ์ย้อนหลัง โดยข้อมูล Log ของระบบ AS/400 นั้นเมื่อถูกบันทึกในระบบแล้วต้องมั่นใจได้ว่าจะไม่สามารถแก้ไขหรือเปลี่ยนแปลงได้					
ความเสี่ยง	1.การไม่บันทึกการเข้าถึงระบบสารสนเทศ ทำให้ไม่สามารถตรวจสอบความผิดปกติย้อนหลังได้ และไม่สามารถหาข้อมูลที่สำคัญที่จะช่วยเป็นแนวทางการแก้ไขปัญหา (Detection) รวมทั้งวิธีการแก้ไขที่จะเกิดขึ้น (Prevention) ในอนาคตได้					
Best Practice	**System Security Management** จัดให้มีการจัดเก็บบันทึกเหตุการณ์ดังต่อไปนี้อย่างมั่นคงปลอดภัย 1. บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log) 2. บันทึกการเข้าถึงระบบงาน (Access Log) โดยบัญชีผู้ใช้ทุกประเภท					

Platform AS/400	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
	3. บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม ● การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล) Update/ Insert/ Delete) ในตารางที่สำคัญ ● การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ ● การเข้าถึง Object ที่สำคัญของระบบ ● การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน โดยบันทึกดังกล่าวต้องถูกจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน					
System Security Management ข้อ 12	3.1	มีการเปิดใช้ audit log **Parameter: QAUDCTL**	*AUDLVL *OBJAUD *NOQTEMP			มีความเสี่ยงที่จะไม่สามารถหาข้อมูลที่สำคัญรวมถึงหาแนวทางการแก้ไขปัญหา (Detection) และวิธีการแก้ไขที่จะเกิดขึ้น (Prevention) ในอนาคตได้รวมถึง จะทำให้ไม่สามารถตรวจสอบความผิดปกติย้อนหลังได้
	3.2	บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ **Parameter: QAUDLVL**	*AUTFAIL *DELETE *OBJMGT *PGMFAIL *SAVRST *SECURITY *SERVICE *SYSMGT *CREATE			
	3.3	Action ที่ระบบจะทำเมื่อไม่สามารถเขียน Audit log ได้ **Parameter: QAUDENDACN**	*NOTIFY			
	3.4	ตั้งค่าให้มีการ Audit เมื่อมี Object ใหม่	*ALL			

Platform AS/400	รายละเอียดการตรวจสอบ	ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
	Parameter: QCRTOBJAUD				

Appendix

User Profile

Special User Classes	Special User Classes				
Authority	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	ALL	10 or 20	10 or 20	10 or 20	10 or 20
*SECADM	ALL	ALL			
*JOBCTL	ALL	10 or 20	10 or 20	ALL	
*SPLCTL	ALL				
*SAVSYS	ALL	10 or 20	10 or 20	ALL	10 or 20
*SERVICE	ALL				
*AUDIT	ALL				
*IOSYSCFG	ALL				

Configuration

Parameters	Description
*ALL	คำสั่งให้สิทธิ์ผู้ใช้สามารถใช้และเข้าถึงโปรแกรมและ Object บนระบบ
*ALLOBJ	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้ทุก Object บนระบบ
*AUDIT	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการตรวจสอบบนระบบ
*AUTFAIL	ตรวจสอบว่ามีการเข้าสู่ระบบที่ผิดพลาดหรือล้มเหลว

*AUDLVL	การตั้งค่าเกี่ยวข้องกับการตรวจสอบการใช้คำสั่งบนระบบ
*CREATE	คำสั่งการสร้าง Object
*DELETE	คำสั่งการลบ Object
*DSCJOB	คำสั่งการยกเลิกการเชื่อมต่อกับงานที่ทำอยู่
*DSCMSG	คำสั่งการยกเลิกการเชื่อมต่อกับงานที่ทำอยู่และแสดงข้อความในระบบที่ผิดพลาด
*ENDJOB	คำสั่งการปิดงานที่ทำอยู่
*EXCLUDE	คำสั่งการระงับการเข้าถึงโปรแกรมและ Object บนระบบ
*JOBCTL	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการ Run Batch และการพิมพ์ผลของการ Run Batch
*IOSYSCFG	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการปรับเปลี่ยนข้อมูลที่ป้อนเข้าและออกจากระบบ
*NOTIFY	คำสั่งที่แจ้งเตือนสิ่งที่ผิดปกติต่างๆ (Error Message)
*OBJAUD	การตั้งค่าเกี่ยวข้องกับการตรวจสอบการใช้ Object บนระบบ
*OBJMGT	การแจ้งเตือนเมื่อมีการย้าย Object รวมถึงการเปลี่ยนชื่อ Object ต่างๆ
*PGMFAIL	การแจ้งเตือนเมื่อมีโปรแกรมทำงานผิดพลาด
*PGMR	Programmer Profile
*SAVSYS	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการ Save และ Restore Object บนระบบ
*SAVRST	การแจ้งเตือนเมื่อมีการ Save และ Restore Object และโปรแกรมบนระบบ
*SECADM	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการให้สิทธิ์ผู้ใช้ระบบได้ และ Security Admin Profile
*SECOFR	Security Officer Profile
*SECURITY	การแจ้งเตือนเมื่อมีการตั้งค่ารักษาความปลอดภัย
*SERVICE	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการปรับค่าการใช้ที่เกี่ยวข้องกับ Software
*SPLCTL	อนุญาตให้สิทธิ์ผู้ใช้สามารถใช้คำสั่งที่เกี่ยวข้องกับการจัดลำดับการ Run Batch
*SYSMGT	การแจ้งเตือนเมื่อมีการจัดการค่า Parameter บนระบบ
*SYSOPR	System Operator Profile
*USER	User Profile

Security Level

Parameters	Description
10	ผู้ใช้ไม่จำเป็นต้องลงชื่อเข้าใช้บนระบบและไม่มีการรักษาความปลอดภัย
20	ผู้ใช้จำเป็นต้องลงชื่อเข้าใช้บนระบบโดยสามารถเข้าได้ทุก Object บนระบบ
30	ผู้ใช้จำเป็นต้องลงชื่อเข้าใช้บนระบบโดยจำเป็นต้องมีการควบคุมด้านความปลอดภัย
40	ผู้ใช้จำเป็นต้องลงชื่อเข้าใช้บนระบบโดยจำเป็นต้องมีการควบคุมด้านความปลอดภัยและการตรวจสอบความถูกต้องของชื่อผู้ใช้และรหัสผ่านทุกครั้ง
50	ผู้ใช้จำเป็นต้องลงชื่อเข้าใช้บนระบบโดยจำเป็นต้องมีการควบคุมด้านความปลอดภัยสูงสุดและการตรวจสอบความถูกต้องของชื่อผู้ใช้และรหัสผ่านสูงสุดทุกครั้ง

Software Support Lifecycle

Product Name	Version	General Availability	End of Support
OS/400	5.1.x	25 May-2001	30 Sep 2005
OS/400	5.2.x	30 Aug 2002	30 Apr 2007
i5/OS	5.3.x	11 Jun 2004	30 Apr 2009
i5/OS	5.4.x	14 Feb 2006	30 Sep 2013
IBM i	6.1.x	21 Mar 2008	30 Sep 2015
IBM i	7.1.x	23 Apr 2010	
IBM i	7.2.x	02 May 2014	

ระบบปฏิบัติการ AIX

AIX (Advanced Interactive eXecutive) คือ Operating Systems ที่ Run บน Hardware ของเครื่อง IBM pSeries (RS/6000 ในอดีต) ซึ่งมีพื้นฐานมาจากระบบปฏิบัติการ UNIX ทั้งนี้ ระบบปฏิบัติการ AIX สามารถ run ได้บน Hardware หลากหลาย platform ทั้ง pSeries , System/370 Mainframe หรือแม้กระทั่ง iSeries แต่โดยมากมัก Run บน Platform pSeries ที่ใช้ CPU chip “POWER” ของ IBM ซึ่งระบบปฏิบัติการ AIX ได้เริ่มพัฒนาขึ้นในปี 1986 และเริ่มมีขายเป็น Commercial ตั้งแต่ปี 1990 เป็นต้นมา

Platform AIX	รายละเอียดการตรวจสอบ	ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
	ส่วนที่ 1 การควบคุมสิทธิและหน้าที่ในการเข้าถึงระบบ Core Banking ทาง Logical				
วัตถุประสงค์	• เพื่อให้มีการควบคุมการเข้าถึงระบบ (AIX) ที่มีประสิทธิภาพ โดยจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาต (Authorized Person) และหน้าที่ที่กำหนดให้ (Authorized Function) เท่านั้น • เพื่อให้มีการจัดการ User Profile ที่เข้มงวดและรัดกุม ทั้งการสร้าง แก้ไข และลบรายชื่อผู้ใช้งานในระบบ ซึ่งสอดคล้องกับลักษณะงานของผู้ใช้งานและนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ				
ความเสี่ยง	• การใช้สิทธิเกินหน้าที่ที่ได้อนุญาตจะเป็นการเปิดโอกาสให้ผู้ไม่ประสงค์ดีสร้างความเสียหายต่อระบบ Core Banking • การกำหนดรหัสผ่านที่ง่ายต่อการคาดเดา เช่น default รหัสผ่าน ตัวเลขเรียงกัน มีความเสี่ยงที่ผู้ไม่ประสงค์ดีจะคาดเดารหัสผ่านของผู้ใช้งานอื่นได้ง่าย ซึ่งเอื้อต่อการสวมสิทธิ์ของผู้ใช้งานอื่นและสามารถเข้าถึงระบบ Core Banking ได้โดยง่าย				
Best Practice	• ระยะเวลาในการระงับรหัสผู้ใช้งานที่ไม่ได้เข้าใช้ระบบมาระยะหนึ่ง • มีการจำกัดสิทธิ์ในการเข้าถึงและการใช้งานโปรแกรมอรรถประโยชน์ (System Utility), Command Line และชุดคำสั่งที่สำคัญ (Command) ที่สำคัญของระบบปฏิบัติการไว้เฉพาะบุคคลที่มีอำนาจหน้าที่เหมาะสมเท่านั้น • การกำหนดสิทธิ์ในการเข้าใช้ทรัพยากรสำคัญของระบบงานตามอำนาจหน้าที่อย่างเหมาะสม เช่น การเข้าถึง File, Folder, Library ที่สำคัญ โดยคำนึงถึงสิทธิ์ในการ Read, Write, Execute, Append และ Delete เป็นต้น				

Platform AIX		รายละเอียดการตรวจสอบ	ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
		• Best Practice มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น • รหัสผ่านควรประกอบไปด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ				
Logical Access Control ข้อ 2.3.1 (3.2)	1.1	ไม่ให้มีการ login ด้วย User deamon bin sys adm nobody uucp lpd โดยไม่ใช้สิทธิ์ su หรือ root **คำสั่งที่ใช้เช็ค: lsuser -a login rlogin <u>ชื่อ user account</u>**	Output ที่ควรจะได้ <u>ชื่อ user account</u> login=false rlogin=false			กรณีที่ไม่ได้มีการจำกัดเข้าถึงของแต่ละผู้ใช้ มีความเสี่ยงที่ผู้ใช้งานอาจนำไปใช้ผิดวัตถุประสงค์ และสามารถเข้าถึงเปลี่ยนแปลงข้อมูลในเครื่องได้
Application Security ข้อ 2.4.6.3 (7)	1.2	เมื่อใส่ รหัสผ่าน ผิดในเวลา XX วินาที จะทำการตัดการเชื่อมต่อ **Configuration file path: /etc/security/login.cfg** **Parameter: logininterval**	300 or less			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของระบบรักษาความปลอดภัยในการเข้าสู่ระบบเพื่อเข้าถึงข้อมูลในเครื่องได้
	1.3	เมื่อใส่ รหัสผ่าน ผิดจำนวน XX ครั้ง ในเวลาตามข้อ 1.2 จะทำการตัดการเชื่อมต่อ **Configuration file path: /etc/security/login.cfg**	10 or less			

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
		Parameter: logindisable				
	1.4	Unlock อัตโนมัติ ในเวลา XX นาทีหลังจากถูก lock **Configuration file path: /etc/security/login.cfg** **Parameter: loginreenable**	360 or greater			
	1.5	ระยะเวลา XX วินาที ในการใส่ รหัสผ่าน **Configuration file path: /etc/security/login.cfg** **Parameter: logintimeout**	30 or less			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack)
Logical Access Control ข้อ 2.3.1 (12.4)	1.6	Lock account เมื่อใส่ รหัสผ่าน ผิด XX ครั้ง **Configuration file path: /etc/security/user** **Parameter: loginretries**	3			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack)
Logical Access Control ข้อ 2.3.1 (3.1)	1.7	ไม่อนุญาตให้ user root login แบบ remote **Configuration file path: /etc/security/user** **Parameter: rlogin**	rlogin=false			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องทางในการเข้าสู่ระบบได้

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Logical Access Control ข้อ 2.3.1 (11)	1.8	รหัสผ่านควรเปลี่ยนทุกกี่สัปดาห์ **Configuration file path: /etc/security/user** **Parameter: maxage** = xx	xx = 12			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack)
Logical Access Control ข้อ 2.3.1 (12.2)	1.9	รหัสผ่านควรมีความยาวไม่น้อยกว่า xx ตัวอักษร **Configuration file path:/etc/security/user** **Parameter: minlen = xx**	xx = 8			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)
Logical Access Control ข้อ 2.3.1 (12.3)	1.10	รหัสผ่านควรมีตัวอักษรไม่น้อยกว่า **Configuration file path: /etc/security/user** **Parameter: minalpha=xx**	xx = 2			
Logical Access Control ข้อ 2.3.1 (12.3)	1.11	รหัสผ่านควรมีอักขระพิเศษไม่น้อยกว่า **Configuration file path:/etc/security/user** **Parameter: minspecialchar=xx**	xx = 2			
System Security Management ข้อ.3.2 (16)	1.12	ปิดไม่ให้ผู้ใช้ Remote เข้าถึงระบบได้เนื่องจากมีการส่ง Usernames และ รหัสผ่าน เป็น Clear text ซึ่งไม่ปลอดภัย **Configuration file path:**/etc/inetd.conf.	ต้องไม่มีค่าดังต่อไปนี้ใน Config File: **Parameter: /usr/bin/rcp**			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถดักจับ (sniffer) Username Password ได้

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
		Parameter: chmod ugo= /usr/bin/rcp **chmod ugo= /usr/bin/rlogin** **chmod ugo= /usr/bin/rsh**	**/usr/bin/rlogin** **/usr/bin/rsh**			
Logical Access Control ข้อ 2.3.1 (12.3)	1.14	การใช้ตัวอักษรซ้ำกันในรหัสผ่าน **Configuration file path: /etc/security/user** **Parameter: maxrepeats = xx**	xx = 2			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้หรือเข้าสู่ระบบงาน (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)
Logical Access Control ข้อ 2.3.1 (3.2)	1.15	การจำกัดการเข้าถึง User root ผ่านกลุ่มของ Super User (SU) **Configuration file path:/etc/security/user** ● กรณีเป็น **Super User** **Parameter: su=true sugroups=system root** ● กรณีเป็น User ทั่วไป **Parameter: su=false Usergroups=User Group Name**	ตรวจสอบจาก Policy ของธนาคาร			กรณีที่ไม่ได้มีการจำกัดเข้าถึง User root มีความเสี่ยงที่ผู้ใช้งานอาจนำไปใช้ผิดวัตถุประสงค์ และสามารถเข้าถึงเปลี่ยนแปลงข้อมูลในเครื่องได้
Logical Access	1.16	ในรหัสผ่านต้องมีตัวเลขอยู่ด้วย	xx = 1			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้หรือเข้าสู่ระบบงาน

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Control ข้อ 2.3.1 (12.3)		**Configuration file path:/etc/security/user** **Parameter: mindigit = XX**				(Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)
Logical Access Control ข้อ 2.3.1 (12.4)	1.17	รหัสผ่านถูกล๊อกเมื่อมีการใส่ผิด XX ครั้งติดกัน กรณีที่การ Login โดยใช้ Secure Shell(SSH) **Configuration file path:** /etc/ssh/sshd_config **Parameter: MaxAuthTries xx**	xx = 3			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้หรือเข้าสู่ระบบงาน (Brute Force Attack)
Logical Access Control ข้อ 2.3.1 (12.5)	1.18	รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ xx ครั้งที่ผ่านมา **Configuration file path: /etc/security/user** **Parameter: histsize=XX**	xx = 12			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้หรือเข้าสู่ระบบงาน (Brute Force Attack)
Access Control ข้อ 2.4.6.2 (5)	1.19	การตั้งค่าต้องให้มีการเปลี่ยน รหัสผ่าน หลังจากหมดอายุ **Configuration file path: /etc/security/user** **Parameter : maxexpired=xx**	xx = 1			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องหรือเข้าสู่ระบบงานได้ (Brute Force Attack)
Application Security ข้อ	1.20	การตั้งค่า Timeout เมื่อมีการไม่ใช้งาน กรณีที่การ Login โดยใช้ SSH (Seconds)	xx = 300 , yy = 0			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องทางในการเข้าสู่ระบบได้

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
2.4.6.3 (7)		**Configuration file path:** /etc/ssh/sshd_config **Parameter: ClientAliveCountMax XX ClientAliveInterval YY**				
	ส่วนที่ 2 การควบคุมการตั้งค่าความปลอดภัยของระบบ AIX					
วัตถุประสงค์	เป็นการกำหนดระดับการรักษาความปลอดภัย (Hardening) ของระบบ Core Banking AIX เพื่อป้องกันระบบจากการข้าถึงโดยไม่ได้รับอนุญาต					
ความเสี่ยง	• การกำหนดระดับการรักษาความปลอดภัยที่ต่ำหรืออ่อนจะเอื้อต่อผู้ไม่ประสงค์ดีในการบุกรุกเข้าถึงระบบ Core Banking ได้โดยง่าย					
Best Practice	• มีการลบ ระงับ หรือยกเลิก Services Application หรือ Network Protocol ที่ไม่มีความจำเป็นในการใช้งาน (Hardening)					
Application Security ข้อ 2.4.6.3 (4)	2.1	ปิดการตั้งค่าไม่ให้เครื่อง Server มีการตอบกลับในกรณีที่ส่ง Broadcast มาและป้องกันการโจมตีจากการส่ง Packet จำนวนมาก (Smurf Attack) **Configuration file path:** /etc/tunables/nextboot **Parameter: bcastping = xx**	xx = 0			มีความเสี่ยงที่จะทำให้เกิดการหยุดชะงักต่อเครื่อง Server จากการใช้ทรัพยากรของระบบเครือข่าย (Dos Atttack)
Application Security ข้อ 2.4.6.3 (4)	2.2	ปิดการตั้งค่าไม่ให้เครื่อง Server มีการตอบกลับจากการส่งข้อมูลจากระบบเครือข่าย (IP Source Route Attack)	xx = 0			มีความเสี่ยงที่จะนำข้อมูลบนระบบเครือข่ายมาใช้โจมตีได้ (Bypass Security Restrictions)

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
		Configuration file path: /etc/tunables/nextboot **Parameter: icmpaddressmask = xx** **udp_pmtu_discover = xx** **ipsrcrouterecv = xx** **nonlocsrcroute = xx**				
Application Security ข้อ 2.4.6.3 (4)	2.3	ปิดการใช้คำสั่ง Core Dumps **Configuration file path:** /etc/security/limits **Parameter: core = xx core_hard = xx** **fullcore = yy**	xx = 0 yy = 0			เนื่องจากมีโอกาสที่สามารถโดนโจมตีจากผู้ที่ไม่หวังดีเพื่อที่จะเอารหัสผ่านหรือข้อมูลที่สำคัญออกมา
Logical Access Control ข้อ 2.3.1 (9)	2.4	ปิดการไม่ให้มีการ Login โดยไม่ใช้รหัสผ่าน **Configuration file path:** /etc/ssh/sshd_config **Parameter: PermitEmpty**รหัสผ่าน **xx**	xx = no			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของระบบรักษาความปลอดภัยในการเข้าสู่ระบบเพื่อเข้าถึงข้อมูลในเครื่องได้
Logical Access	2.5	การตั้งค่าอนุญาตและปฏิเสธการเข้าใช้ของผู้ใช้ และกลุ่มของผู้ใช้งาน				กรณีที่ไม่ได้มีการจำกัดเข้าถึงของแต่ละกลุ่มผู้ใช้ มีความเสี่ยงที่ผู้ใช้งานอาจนำไปใช้ผิดวัตถุประสงค์ และ

Platform AIX	รายละเอียดการตรวจสอบ	ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
Control ข้อ 2.3.1 (3.2)	**Configuration file path:** /etc/ssh/sshd_config **Parameter: AllowUsers <userlist>** **AllowGroups <grouplist>** **DenyUsers <userlist>** **DenyGroups <grouplist>**				สามารถเข้าถึงเปลี่ยนแปลงข้อมูลในเครื่องได้
	ส่วนที่ 3 การกำหนด Audit Log				
วัตถุประสงค์	เพื่อกำหนดระดับการเก็บข้อมูล Log การเข้าใช้งานระบบ Core Banking AIX ที่เพียงพอต่อการสอบทานเหตุการณ์ย้อนหลัง โดยข้อมูล Log ของระบบ AIX นั้นเมื่อถูกบันทึกในระบบแล้วต้องมั่นใจได้ว่าจะไม่สามารถแก้ไขหรือเปลี่ยนแปลงได้				
ความเสี่ยง	1.การไม่บันทึกการเข้าถึงระบบสารสนเทศ ทำให้ไม่สามารถตรวจสอบความผิดปกติย้อนหลังได้ และไม่สามารถหาข้อมูลที่สำคัญที่จะช่วยเป็นแนวทางการแก้ไขปัญหา (Detection) รวมทั้งวิธีการแก้ไขที่จะเกิดขึ้น (Prevention) ในอนาคตได้				
Best Practice	System Security Management จัดให้มีการจัดเก็บบันทึกเหตุการณ์ดังต่อไปนี้อย่างมั่นคงปลอดภัย 1. บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log) 2. บันทึกการเข้าถึงระบบงาน (Access Log) โดยบัญชีผู้ใช้ทุกประเภท 3. บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม ● การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล) Update/ Insert/ Delete) ในตารางที่สำคัญ ● การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ ● การเข้าถึง Object ที่สำคัญของระบบ ● การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน โดยบันทึกดังกล่าวต้องถูกจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน				

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
System Security Management ข้อ.3.2 (12)	3.1	มีการเปิดใช้ audit log **Path: /etc/security/audit** **Parameter: Binmode, Streammode**	Binmode= on หรือ Streammode=on			
System Security Management ข้อ.3.2 (12)	3.2	บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ **Path: /etc/security/audit** **Parameter: general, objects**	Classes: general=USER_SU, รหัสผ่าน_Change ,FILE_Unlink,FILE_Link,FILE_Rename, FS_Chdir,FS_Chroot, PORT_Locked, PORT_Change,FS_Mkdir, FS_Rmdir objects= S_ENVIRON_WRITE, S_GROUP_WRITE, S_LIMITS_WRITE,S_LOGIN_WRITE, S_PASSWD_READ, S_PASSWD_WRITE,S			มีความเสี่ยงที่จะไม่สามารถหาข้อมูลที่สำคัญรวมถึงหาแนวทางการแก้ไขปัญหา (Detection) และวิธีการแก้ไขที่จะเกิดขึ้น (Prevention) ในอนาคตได้รวมถึง จะทำให้ไม่สามารถตรวจสอบความผิดปกติย้อนหลังได้

Platform AIX	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิดขึ้น
			_USER_WRITE, AUD_CONFIG_WR			

Appendix

Configuration

Parameters	Description
u(User)	คำสั่งเรียกให้การปรับเปลี่ยนของหน้าที่ของผู้ใช้
g(Group)	คำสั่งเรียกให้การปรับเปลี่ยนของหน้าที่ของกลุ่มผู้ใช้
o(Other)	คำสั่งเรียกให้การปรับเปลี่ยนของหน้าที่ของผู้ใช้อื่นๆ
adm	บัญชีผู้ใช้พื้นฐาน (Local User) บนระบบซึ่งสามารถทำหน้าที่ Monitor Status หรือ Service สำคัญ
bcastping	คำสั่งให้เครื่อง Server ส่งการตอบกลับในกรณีที่เครื่อง Client หรือ Server อื่นๆมีการตรวจเช็คระบบทั้งเครือข่าย(Broadcast) เพื่อทดสอบว่า เครื่องต้นทางและปลายทางเครื่องใดสามารถสื่อสารกันผ่านระบบเครือข่ายได้ (Ping)
bin	บัญชีผู้ใช้พื้นฐานซึ่งทำหน้าที่ช่วยแยก Directory ซึ่งทำหน้าที่บรรจุ Files ของผู้ใช้แต่ละคน
binmode	เปิดการตรวจสอบ Files ชั่วคราวที่ถูกเรียกดูหรือประมวลผลไปแล้ว (Temporary Files)
chmod	คำสั่งใช้เปลี่ยน Mode ของ Services หรือ Command Line ต่างๆที่ถูกเขียนไว้
Core	แกนหลักของ CPU บนตัวเครื่อง Server
Core_hard	แกนหลักอุปกรณ์ Hardware บนตัวเครื่อง Server

deamon	บัญชีผู้ใช้พื้นฐานซึ่งทำหน้าที่ช่วยให้ Process ต่างๆบน O/S ใช้ข้อมูลที่เกี่ยวข้องกับ Process นั้นๆได้ถูกต้อง
default	คำสั่งการปรับเปลี่ยนค่าเริ่มต้นของ Command line
Fullcore	การนำเอาข้อมูลทั้งหมดในหน่วยความจำ (RAM) ณ ขณะหนึ่งออกมาครับ
icmpaddressmask	คำสั่งให้เครื่อง Server ส่งการตอบกลับในกรณีที่เครื่อง Client หรือเครื่อง Server อื่นๆมีการตรวจเช็คในกลุ่มของ IP (Subnet Mark) ของเครื่อง Server เพื่อทดสอบว่าเครื่องต้นทางและปลายทางเครื่องใดสามารถสื่อสารกันผ่านระบบเครือข่ายได้
ipsrcrouterecv	คำสั่งให้เครื่อง Server ส่งการตอบกลับในกรณีที่เครื่องต้นทางที่มีการตรวจเช็คว่าเครื่องใดสามารถสื่อสารกันผ่านระบบเครือข่ายได้
lpd	บัญชีผู้ใช้พื้นฐานให้เครื่อง Server นั้นทำหน้าที่เป็น Printer Server
nobody	บัญชีผู้ใช้พื้นฐานซึ่งทำหน้าที่อนุญาตให้ผู้ใช้อื่น Remote เพื่อที่จะ Print งานบน Printer Server ในระดับเครือข่าย (Network File System)
nonlocsrcroute	คำสั่งให้เครื่อง Server ส่งการตอบกลับในกรณีที่เครื่อง Client หรือ Server อื่นๆมีการตรวจเช็กนอกกลุ่มของ IP เครื่อง Server เพื่อทดสอบว่า เครื่องต้นทางและปลายทางเครื่องใดสามารถสื่อสารกันผ่านระบบเครือข่ายได้
sys	บัญชีผู้ใช้พื้นฐานซึ่งทำหน้าที่อนุญาตให้ติดตั้งโปรแกรมประยุกต์ แบบ client/server ที่ยินยอมให้เครื่อง client ในการเข้าถึงและประมวลผลข้อมูลที่เก็บบนเครื่อง server ถ้าอยู่บนคอมพิวเตอร์เครื่องเดียวกัน
Streamode	เปิดการตรวจสอบ Files ชั่วคราวที่กำลังถูกประมวลผลอยู่
udp_pmtu_discover	คำสั่งให้เครื่อง Server ส่งการตอบกลับในกรณีที่เครื่องต้นทางมีการแยกส่ง Packet (Packet Fragmentation)
uucp	บัญชีผู้ใช้พื้นฐานซึ่งทำหน้าที่อนุญาตให้ผู้ใช้อื่นสามารถทำการคัดลอกข้อมูลในระดับเครือข่าย

Configuration Directory

Directory	Description

../etc/inetd.conf.	Folders ใช้ปรับเปลี่ยนค่าการจัดการ Service ของตัวระบบ
../etc/security/audit	Folders ใช้ปรับเปลี่ยนค่าการตรวจสอบ ของตัวระบบ
../etc/security/limits	Folders สำหรับจัดการให้ผู้ใช้บางคนสามารถใช้คำสั่งเฉพาะหรือเข้าถึงตัวความจำของ CPU ของตัวเครื่อง
../etc/security/login.cfg	Folders สำหรับจัดการและตั้งค่า Login ของตัวระบบ
../etc/ssh/sshd_config	Folders สำหรับจัดการและตั้งค่า Secure Shell ของตัวระบบ
../etc/tunables/nextboot	Folders สำหรับความปลอดภัยในระดับเครือข่ายของตัวระบบ

Software Support Lifecycle

Product Name	General Availability	End of Support
AIX 7	September 10, 2010	Not Announced
AIX 6	November 9, 2007	Not Announced
AIX V5.3	August 13, 2004	April 30, 2012
AIX V5.2	October 18, 2002	April 30, 2009
AIX V5.1	May 4, 2001	April 1, 2006

ระบบปฏิบัติการ Window

Windows Server เป็นระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่พัฒนาโดยบริษัทไมโครซอฟท์ ซึ่งสามารถทำให้การเก็บข้อมูลและการประมวลผลข้อมูลสามารถทำได้โดยผู้ใช้หลายคนพร้อมกัน (Multitasking) ให้บริการ Services หลากหลายขึ้นกับ Application ที่ติดตั้งบนระบบปฏิบัติการ เช่น ระบบฐานข้อมูล เว็บเซิฟเวอร์ เป็นต้น มีความเสถียร และความสามารถในการจัดการสิทธิ์ เช่น Active Directory, Group policy เป็นต้น

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
Logical Access	ส่วนที่ 1 การควบคุมการเข้าถึงระบบปฏิบัติการ Windows					
วัตถุประสงค์ ความเสี่ยง Best Practice						
Logical Access Control ข้อ 2.3.1 (11)	1.1	ปิดการใช้งาน Build-in Guest account **Parameter: Guest Account status**	Disabled			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องโหว่ในการเข้าถึงเครื่องได้ โดยการสุ่มเดา User/Password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks) (Brute Force Attack)
Logical Access	1.2	สิทธิในการทำตัวเสมือนเป็นส่วนหนึ่งของระบบปฏิบัติการ	Not defined			มีความเสี่ยงที่ผู้ไม่หวังดีจะใช้เป็นช่องทางเข้าสู่ระบบ

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
Control ข้อ 2.3.1 (4)		**Parameter**: Act as part of the operating system				ปฏิบัติการของเครื่อง Server ได้โดยไม่ผ่านระบบรักษาความปลอดภัย หรือผ่านในระดับต่ำ
	1.8	ห้าม Log on เข้ามาในลักษณะ Service **Parameter: Deny log on as a service**	Not defined			
Logical Access Control ข้อ 2.3.1 (12.4)	1.11	Locked Account เมื่อมีการใส่รหัสผ่านผิด XX ครั้งติดกัน **Parameter: Account lockout threshold**	3			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องโหว่ในการเข้าถึงเครื่องได้ โดยการสุ่มเดา User/Password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks) (Brute Force Attack)
	1.13	ระยะเวลาก่อนที่ windows จะทำการ reset จำนวนครั้งที่ใส่รหัสผ่านผิดเป็น 0 **Parameter: Reset account lockout counter after**	99999			
	1.14	ระยะเวลาที่ lock account ผู้ใช้ที่เดารหัสผิด **Parameter: Account lockout duration**	0			มีความเสี่ยงที่ทำให้ผู้ไม่หวังดีใช้เป็นช่องโหว่ในการเข้าถึงเครื่องได้ โดยการสุ่มเดา User/Password จากการรวบรวมคำศัพท์
Logical Access Control ข้อ 2.3.1 (12.1.1)	1.12	รหัสผ่านควรเปลี่ยนทุก XX วัน	60			

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
		Parameter: Maximum password age				ต่างๆ (Dictionary Attacks) (Brute Force Attack)
Logical Access Control ข้อ 2.3.1 (12.2)	1.15	รหัสผ่านควรมีความยาวไม่น้อยกว่า xx ตัวอักษร **Parameter: Minimum password length**	8			
Logical Access Control ข้อ 2.3.1 (12.3)	1.9	การกำหนดความซับซ้อนของรหัสผ่าน **Parameter: Password must meet complexity requirement**	Enable			
Logical Access Control ข้อ 2.3.1 (12.5)	1.16	รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ xx ครั้งที่ผ่านมา **Parameter: Enforce password history**	12			
System Security Management 2.3.2 (16)	1.10	เก็บรหัสผ่านแบบที่สามารถถอดรหัสกลับได้ (Plain Text) **Parameter: Store password using reversible encryption**	Disable			
	ส่วนที่ 2 การควบคุมการตั้งค่าความปลอดภัยของ Windows (Security Option)					
วัตถุประสงค์						
ความเสี่ยง						

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
Best Practice						
Logical Access Control ข้อ 2.3.1(9)	2.1	ห้ามใช้ Local account Logon ผ่าน Network services โดยไม่ใช้รหัสผ่าน **Parameter: Limit local account use of blank passwords to console logon only**	Enabled			ง่ายต่อการเกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องโดยการใช้ Local Account ได้ (Brute Force Attack)
Logical Access Control ข้อ 2.3.1(4)	2.2	ห้ามติดตั้ง Driver Printer บนเครื่อง Server **Parameter: Prevent users from installing printer drivers**	Enabled			เกิดช่องโหว่ที่เครื่อง Server จะติดโปรแกรมไวรัสหรือโปรแกรมที่ผู้ไม่หวังดีใช้ในการเข้าถึงเครื่อง
Logical Access Control ข้อ 2.3.1 (12.1.1)	2.3	Machine account Password ต้องเปลี่ยนทุก XX วัน **Parameter: Maximum machine account password age**	60			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack) และเป็นการสุ่มเดา password จากการรวบรวมคำศัพท์ต่างๆ (Dictionary Attacks)
Logical Access Control ข้อ 2.3.1 (12.1.3)	2.4	ให้ Machine account เปลี่ยน Password อย่างสม่ำเสมอ **Parameter: Disable machine account password changes**	Disabled			
Application Security ข้อ 2.4.6.3(7)	2.5	ตัดการเชื่อมต่อเมื่อหมดระยะเวลาที่ตั้งไว้ **Parameter: Disconnect clients when logon hours expire**	Enabled			เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องได้ (Brute Force Attack)

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
	2.6	Force logoff when logon hours expire	Enabled			
	ส่วนที่ 3 การกำหนด Audit Log					
วัตถุประสงค์						
ความเสี่ยง						
Best Practice						
System Security Management ข้อ 2.3.2 (12)	3.1	บันทึกการเข้าถึง/ออกระบบงาน **Parameter: Audit account logon event**	Success, Failure			มีความเสี่ยงที่จะไม่สามารถตรวจสอบความผิดปกติย้อนหลัง และหาข้อมูลที่สำคัญช่วยในการแก้ไขปัญหาและรวมถึงหาแนวทางการแก้ไขปัญหา (Detection) และป้องกันปัญหาที่จะเกิดขึ้น (Prevention) ในอนาคตได้
	3.2	บันทึกเมื่อ User account/service ใช้งาน sensitive privilege **Parameter: Audit privilege use**	Success, Failure			
	3.3	บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ **Parameter: Audit account management**	Success, Failure			
	3.4	บันทึกการเข้าใช้งาน Object ของ Active directory **Parameter: Audit directory service access**	Success, Failure			
	3.5	บันทึกการเข้าใช้งานจากเครื่องคอมพิวเตอร์	Success, Failure			

Platform Windows	รายละเอียดการตรวจสอบ		ค่า Parameter ที่ Recommend	ค่า Baseline ของธนาคาร	ค่า Parameter ของธนาคาร	ความเสี่ยงที่จะเกิด
		Parameter: Audit logon event				
	3.6	บันทึกเหตุการณ์ที่ User เข้าใช้ Object **Parameter: Audit object access**	Success, Failure			
	3.7	บันทึกการเปลี่ยนแปลงสิทธิ์ของผู้ใช้, การเปลี่ยนแปลง Policies **Parameter: Audit policy change**	Success			
	3.8	บันทึกการเปลี่ยนแปลงของระบบ เช่น restart, shutdown **Parameter: Audit system event**	Success			
	3.9	บันทึกรายละเอียดการเปลี่ยนแปลงของ Process **Parameter: Audit process tracking**	Success			

Appendix

Software Support Lifecycle

Product Name	Version	General Availability	End of Support
Windows Server 2003	Cluster Edition	09/06/2006	07/14/2015
	R2 Data Center Edition	03/05/2006	07/14/2015

	R2 Data Center Edition Service Pack 2	03/13/2007	24 months after service pack release
	R2 Standard Edition, R2 Enterprise Edition	03/05/2006	07/14/2015
	Service Pack 1	03/30/2005	04/14/2009
	Service Pack 2 for Itanium	03/13/2007	24 months after service pack release
Windows Server 2008	ทุก Edition	05/06/2008	01/14/2020
Windows Server 2012	Data Center Edition	10/30/2012	01/10/2023
	R2 Data Center	11/25/2012	01/10/2023
	Standard Edition	10/30/2012	01/10/2023

Appendix: รายการขอเอกสารจากสง.สำหรับการตรวจสอบเทคนิคเชิงลึก

ระบบปฏิบัติการ	รายละเอียดรายการขอเอกสาร
AS400	File Configuration ของระบบปฏิบัติการ ในส่วนของ Security Parameter ที่เกี่ยวข้องกับการตั้งค่า Password Policy, Audit Log Setting และ Service/Network Setting
AIX	Print Screen หน้าจอจากระบบปฏิบัติการหรือส่ง File Configurationในส่วนของ Security Parameter ที่เกี่ยวข้องกับการตั้งค่า Password Policy, Account Policy และ Audit Policy ใน Path ดังนี้ **/etc/security/login.cfg** **/etc/security/user** **/etc/ssh/sshd_config** **/etc/tunables/nextboot** **/etc/security/audit/config**
Window Server	Print Screen หน้าจอจากระบบปฏิบัติการในส่วนของ Security Parameter ที่เกี่ยวข้องกับการตั้งค่า Password Policy, Account Lockout Policy, Security options, User Rights Assignment และ Audit Policy