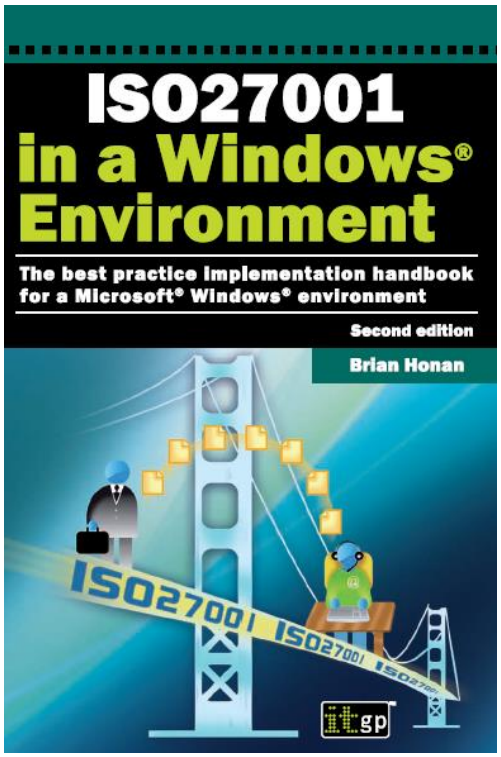
บทวิจารณ์หนังสือ

นิตยา วงศ์ภินันท์วัฒนา
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

doi: 10.14456/jisb.2018.18



Title: ISO27001 in a Windows Environment: The best practice implementation handbook for a Microsoft Windows environment (Second edition)
Author: Brian Honan
Edition: 2010
Publisher: IT Governance Publishing
Number of pages: 312

หนังสือ ISO27001 in a Windows Environment เป็นสิ่งที่ต้องกำหนดเพื่อให้ระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัยตามมาตรฐานของ ISO27001 ประกอบด้วยการกำหนดนโยบายความมั่นคงปลอดภัยของสารสนเทศ การกำหนดหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ ความมั่นคงปลอดภัยสำหรับทรัพยากรมนุษย์ การบริหารจัดการทรัพย์สิน การควบคุมการเข้าถึง การเข้ารหัสข้อมูล สภาพแวดล้อมความมั่นคงปลอดภัยทางกายภาพ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล การจัดหา การพัฒนา และการบำรุงรักษาระบบ ความสัมพันธ์กับผู้ให้บริการภายนอก การบริหารจัดการอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความต่อเนื่องของธุรกิจด้านความมั่นคงปลอดภัยสารสนเทศ และความสอดคล้อง นอกจากนี้ยังกล่าวถึงการกำหนดค่าการทำงานของ Windows Server เพื่อให้มีการรักษาความมั่นคงปลอดภัย โดยสรุปดังนี้

1. ระบบปฏิบัติการติดตั้ง service pack ที่เป็นปัจจุบัน
   คำสั่ง
   control panel -> system ดูที่ชื่อระบบปฏิบัติการว่าติดตั้ง service pack ใด (สามารถไปดูรุ่นของ service pack ที่เป็นปัจจุบันได้จาก web ของ Microsoft)
2. กำหนด account policies
   คำสั่ง
   start -> administrative tools -> domain security setting -> account policies
   2.1 minimum password length เป็นการกำหนดขนาดของรหัสผ่าน ขนาดของรหัสผ่านจะส่งผลต่อการแกะรหัสผ่าน กล่าวคือถ้ารหัสผ่านมีขนาดสั้นจะใช้เวลาในการแกะรหัสผ่านน้อย
   2.2 maximum password age เป็นการกำหนดวันที่รหัสผ่านจะหมดอายุใช้งาน เพื่อให้ผู้ใช้เปลี่ยนรหัสผ่านใหม่

2.3 minimum password age เป็นการกำหนดจำนวนวันที่ต้องใช้รหัสผ่านที่เปลี่ยนใหม่ เพื่อป้องกันไม่ให้ผู้ใช้เปลี่ยนไปใช้รหัสผ่านเดิมเร็วเกินไป

2.4 password complexity เป็นการกำหนดให้รหัสผ่านที่กำหนดต้องมีความซับซ้อน

2.5 password history เป็นการกำหนดประวัติของรหัสผ่านเพื่อไม่ใช้ผู้ใช้เปลี่ยนไปใช้รหัสผ่านเดิมเร็วเกินไป

2.6 store passwords using reversible encryption เป็นการเข้ารหัสรหัสผ่านที่เก็บอยู่ในระบบปฏิบัติการ

3. กำหนด audit policies

คำสั่ง

start -> administrative tools -> domain security setting -> local policies -> audit policy

3.1 audit account logon events เป็นการติดตามการเข้าถึง server เนื่องจากการ logon ที่ล้มเหลวแสดงว่ามีการโจมตีด้วยการเดารหัสผ่านอยู่

3.2 audit account management เป็นการติดตามการจัดการบัญชีผู้ใช้จะทำให้ทราบถึง การสร้าง เปลี่ยนแปลง หรือลบบัญชีผู้ใช้ ซึ่งจะทำให้ทราบเกี่ยวกับบัญชีผู้ใช้ปลอมหรือค้นหาสาเหตุของการที่บัญชีผู้ใช้ถูก lock

3.3 audit directory service access เพื่อจัดเก็บข้อมูลการเข้าถึงทรัพยากรใน active directory

3.4 audit logon events เพื่อมั่นใจว่ามีการติดตามการเข้าถึง server ของ local account

3.5 audit object access เป็นการติดตามการเข้าถึงทรัพยากรต่างๆ ในระบบ เช่น เครื่องพิมพ์ แฟ้มข้อมูล เป็นต้น แต่การกำหนดค่าดังกล่าวจะทำให้มีรายการการใช้งานทรัพยากรของระบบจำนวนมากเช่นกัน

3.6 audit policy change เพื่อให้จัดเก็บรายการเกี่ยวกับการเปลี่ยนแปลง user rights, account policies, group policies และอื่นๆ

3.7 audit privilege use เพื่อจัดเก็บข้อมูลการใช้สิทธิพิเศษในการปฏิบัติงาน เช่น การสำรองข้อมูล เป็นต้น นอกจากนี้ยังรวมถึงการทำกิจกรรมปลอมในระบบ

3.8 audit process tracking มักไม่ใช้งานเนื่องจากจะจัดเก็บรายการจำนวนมาก ไม่ว่าจะเป็นการเปิด ปิด และรายการเปลี่ยนแปลงต่างๆ

3.9 audit system events เพื่อจัดเก็บข้อมูลการเปิด ปิด server และระบบอื่นๆ

4. account lockout policy

คำสั่ง

start -> administrative tools -> domain security setting -> account logout policy

4.1 account lockout duration จะกำหนดช่วงเวลาไม่ให้บัญชีผู้ใช้สามารถใช้งานได้ โดยผู้บริหารจะสามารถปรับค่านี้ได้ นอกจากนี้ผู้โจมตีสามารถใช้หน้าที่งานนี้เพื่อโจมตีแบบ DoS (denial of service) ด้วยการ lock บัญชีผู้ใช้ทุกคน

4.2 account lockout threshold กำหนดจำนวนครั้งที่ผู้ใช้สามารถป้อนบัญชีผู้ใช้ผิดก่อนที่ระบบจะ lock out

4.3 reset account lockout counter after จะกำหนดร่วมกับ account lockout threshold โดย counter ของจำนวนครั้งที่ป้อนบัญชีผู้ใช้ผิดจะถูกเปลี่ยนให้เป็นศูนย์หลังจากระยะเวลาที่กำหนดในค่านี้

4.4 lockout after กำหนดจำนวนครั้งที่ผู้ใช้ถึงระบบและล้มเหลว ต่อจากนั้นผู้ใช้จะไม่สามารถเข้าถึงระบบได้

4.5 forcibly disconnect remote user from server when logon hours expire เป็นการกำหนดว่าผู้ที่เชื่อมต่อเข้ามาในระบบเครือข่ายคอมพิวเตอร์จะถูกปิดการติดต่อ

หมายเหตุ 4.4 และ 4.5 เป็นคำสั่งสำหรับ windows server 2008

5. event log settings

คำสั่ง

start -> administrative tools -> domain security setting -> event log

5.1 application log settings เป็นการจัดเก็บลงบันทึกการใช้งานโปรแกรมประยุกต์ ประกอบด้วย

- maximum application log size การกำหนดขนาดของลงบันทึกเพื่อใช้ในการจัดเก็บข้อมูล
- prevent local guests group from accessing application log กำหนดว่าไม่ให้ guest accounts เปิดข้อมูลในลงบันทึกนี้ได้
- retain application log กำหนดจำนวนวันจัดเก็บข้อมูลในลงบันทึกซึ่งจะต้องสอดคล้องกับ overwrite by days
- retention method for application log ประกอบด้วย
  + overwrite events as needed
  + overwrite by days
  + do not overwrite (clear logs manually)

5.2 security log settings เป็นการจัดเก็บลงบันทึกเกี่ยวกับการพยายามเข้าสู่ระบบด้วยรหัสที่ถูกต้องและไม่ถูกต้อง (logon attempt) รายละเอียดการกำหนดขนาดและวิธีการเก็บลงบันทึกเช่นเดียวกับ 5.1

5.3 system log settings เป็นการจัดเก็บลงบันทึกเกี่ยวกับการพยายามเข้าองค์ประกอบของระบบปฏิบัติการ เช่น ความล้มเหลวในการเปิดใช้งาน driver เป็นต้น รายละเอียดการกำหนดขนาดและวิธีการเก็บลงบันทึกเช่นเดียวกับ 5.1

6. การกำหนดการจัดเก็บลงบันทึกที่ web server และการ disable guest account

คำสั่ง

start -> administrative tools -> internet information services (IIS) manager -> web sites -> default web site คลิกขวาที่ default web site -> เลือก properties

6.1 เลือก tab web site -> enable logging

6.2 เลือก tab directory security -> ที่ authentication and access control กดปุ่ม edit ยกเลิก anonymous access

7. การ set up อื่นๆ ที่ควรให้ความสนใจ

7.1 การเปลี่ยนชื่อหรือกำหนดไม่ให้ใช้งานได้ (disable) บัญชี administrator account และ guest account

7.2 การกำหนดสิทธิในการ backup และ restore

7.3 ให้พิมพ์งานจาก print server เท่านั้น

7.4 ให้ server เลิกการสร้าง 8.3 file names ด้วยการทำให้ client ต้องใช้ชื่อเต็มเท่านั้น

7.5 ถ้าต้องการใช้บริการของ telnet ในการโอนข้อมูลให้ทำผ่าน secure shell (SSH) แทน