# Payment Card Industry (PCI)
## มาตรฐานความปลอดภัยของข้อมูล

---

## ความต้องการ และ กระบวนการประเมินความปลอดภัย

เวอร์ชั่น 3.0

พฤศจิกายน 2556

# เอกสารการเปลี่ยนแปลง

| วันที่ | เวอร์ชั่น | รายละเอียด | หน้า |
|---|---|---|---|
| ตุลาคม 2551 | 1.2 | เพื่อแนะนำ PCI DSS v1.2 ในรูปแบบ ความต้องการ PCI DSS และกระบวนการประเมินความปลอดภัย ขจัดการซ้ำซ้อนของเอกสาร และการเปลี่ยนแปลงทั้งในด้านทั่วๆไปและการเปลี่ยนแปลงเฉพาะจากกระบวนการตรวจสอบความปลอดภัย PCI DSS V1.1 โปรดดูสรุปความเปลี่ยนแปลงมาตรฐานความปลอดภัยของข้อมูล PCI จาก PCI DSS เวอร์ชั่น 1.1 ไปยัง 1.2 สำหรับข้อมูลที่สมบูรณ์ | |
| กรกฎาคม 2552 | 1.2.1 | เพิ่มประโยคส่วนที่ถูกลบไปอย่างไม่ถูกต้องในระหว่าง PCI DSS v1.1 และ v.1.2 | 5 |
| | | แก้ไขคำจาก then เป็น than ในกระบวนการการทดสอบ 6.3.7.a และ 6.3.7.b | 32 |
| | | ลบอักษรที่เป็นสีเทาสำหรับคำว่า “in place” และ “not in place” ในตารางกระบวนการทดสอบ 6.5.b | 33 |
| | | สำหรับเอกสารการควบคุมแบบทดแทน – ทำให้ตัวอย่างสมบูรณ์ แก้ไขคำในส่วนต้นของหน้าที่กล่าวไว้ว่า “ใช้เอกสารนี้เพื่อกำหนดการควบคุมแบบทดแทนสำหรับความต้องการใดๆที่ระบุไว้ว่า ‘มีการใช้งาน (in place)’ ในส่วนการควบคุมแบบทดแทน” | 64 |
| ตุลาคม 2553 | 2.0 | อัพเดทและดำเนินการเปลี่ยนแปลงจาก v1.2.1 โปรดดู PCI DSS – สรุปการเปลี่ยนแปลง จาก PCI DSS v1.2.1 ไปยัง 2.0 | |
| พฤศจิกายน 2556 | 3.0 | อัพเดทจาก v2.0 โปรดดู สรุปการเปลี่ยนแปลง จาก PCI DSS เวอร์ชั่น 2.0 ไปยัง 3.0 | |

# สารบัญ

# บทนำและภาพรวมของ มาตรฐานความปลอดภัยของข้อมูล PCI

มาตรฐานความปลอดภัยของข้อมูลของ The Payment Card Industry (PCI DSS) ถูกพัฒนาขึ้นมาเพื่อสร้างความมั่นใจและเพิ่มระดับความปลอดภัยให้กับข้อมูลผู้ถือบัตร และอำนวยความสะดวกการใช้งานอย่างกว้างขวาง ของมาตรฐานความปลอดภัยของข้อมูลที่สอดคล้องกับมาตรฐานระดับโลก PCI DSS ได้ให้ข้อมูลทางเทคนิคเบื้องต้น และความต้องการในการปฏิบัติการที่ออกแบบมาเพื่อปกป้องข้อมูลผู้ถือบัตร PCI DSS ประยุกต์สิ่งที่เรียกว่าเป็นกระบวนการการชำระเงินผ่านบัตรที่เกี่ยวข้องทั้งหมดไว้ — รวมไปถึงผู้ค้า ผู้ดำเนินการ ผู้ให้บริการแก่ผู้รับบัตร ผู้ออกบัตร และ ผู้ให้บริการ พร้อมทั้งหน่วยงาน (entity) อื่นๆที่ จัดเก็บ ดำเนินการ ส่งข้อมูล ข้อมูล ผู้ถือบัตร (CHD) และ/หรือ ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง (SAD) ด้านล่างคือ ภาพรวมความต้องการของ PCI DSS ขั้นสูง 12 ข้อ

PCI มาตรฐานความปลอดภัยของข้อมูล – ภาพรวมความต้องการขั้นสูง (High Level)

| | |
|---|---|
| สร้าง และ ปรับปรุง เครือข่ายที่ปลอดภัย และระบบต่างๆ | 1.ติดตั้งและปรับปรุงการตั้งค่า firewall เพื่อปกป้องข้อมูลผู้ถือบัตร<br>2.ไม่ใช้ค่าตั้งต้นของ การสนับสนุนจากผู้ขายสำหรับรหัสผ่านของระบบ และส่วนความปลอดภัยอื่นๆ |
| ปกป้องข้อมูลผู้ถือบัตร | 3.ปกป้องข้อมูลผู้ถือบัตรที่บันทึกไว้<br>4.เข้ารหัสการส่งข้อมูลผู้ถือบัตรในเครือข่ายสาธารณะ |
| บำรุงรักษาโปรแกรมจัดการช่องโหว่ | 5.ปกป้องระบบทั้งหมดจาก malware และ อัพเดทโปรแกรม anti-virus เป็นประจำ<br>6.พัฒนาและบำรุงรักษาระบบและแอปพลิเคชั่นรักษาความปลอดภัย |
| ดำเนินการประเมินการควบคุมการเข้าถึงอย่างเคร่งครัด | 7.จำกัดการเข้าถึงข้อมูลผู้ถือบัตรด้วยความต้องการทางธุรกิจที่ทราบ<br>8.ตรวจสอบ และ รับรองความถูกต้องของการเข้าถึงส่วนประกอบระบบ<br>9.จำกัดการเข้าถึงทางกายภาพไปยังข้อมูลผู้ถือบัตร |
| สังเกต และ ทดสอบเครือข่ายเป็นประจำ | 10.ติดตามและสังเกตการเข้าถึงทั้งหมดไปยังแหล่งข้อมูลเครือข่ายและข้อมูลผู้ถือบัตร<br>11.ทดสอบระบบความปลอดภัย และกระบวนการอยู่เป็นประจำ |
| ปรับปรุง นโยบายความปลอดภัยของข้อมูล | 12.บำรุงรักษานโยบายซึ่งกล่าวถึงความปลอดภัยของข้อมูลของบุคลากรทั้งหมด |

เอกสาร ความต้องการของ มาตรฐานความปลอดภัยของข้อมูล PCI และขั้นตอนการประเมินนี้ ได้รวบรวมความต้องการทั้ง 12 ของ PCI DSS และ กระบวนการทดสอบที่เกี่ยวข้องไว้เป็นเครื่องมือประเมินความปลอดภัย มันถูกออกแบบมาสำหรับใช้งานในระหว่างช่วงการประเมินการปฏิบัติตาม PCI DSS ในส่วนกระบวนการตรวจสอบความถูกต้อง ของหน่วยงาน (entity) ส่วนต่อไปนี้จะให้ข้อมูลเกี่ยวกับการแนะแนวทางอย่างละเอียด และขั้นตอนการปฏิบัติที่ดีที่สุดเพื่อช่วยให้การเตรียมหน่วยงาน (entity) ของ การนำ และรายงานผลของการ PCI DSS ความต้องการของ PCI DSS และกระบวนการทดสอบเริ่มต้นที่หน้า 15

PCI DSS ประกอบด้วยความต้องการขั้นต่ำในการปกป้องข้อมูลผู้ถือบัตรและอาจยกระดับได้ด้วยการควบคุมและกระบวนการเพิ่มเติมเพื่อบรรเทาความเสี่ยง พร้อมกันกับ กฎหมาย และแนวทางปฏิบัติของ ท้องถิ่น ประเทศ และภาคส่วน อีกทั้งการออกกฎหมาย และความต้องการในการกำกับดูแลอาจต้องการการปกป้องเฉพาะข้อมูลที่สามารถระบุตัวตนบุคคลได้ หรือส่วนประกอบของข้อมูลอื่นๆ (เช่น ชื่อผู้ถือบัตร) PCI DSS ไม่อาจทดแทนกฎหมายท้องถิ่น หรือประเทศ แนวปฏิบัติของรัฐบาล หรือความต้องการทางกฎหมายอื่นๆได้

## แหล่งข้อมูล PCI DSS

สภามาตรฐานความปลอดภัยของ PCI (PCI SSC) เว็บไซต์ (www.pcisecuritystandards.org) ได้แหล่งข้อมูลเพิ่มเติมไว้เพื่ออำนวยความสะดวกให้แก่องค์กรที่ใช้การกระเมินและการตรวจสอบความถูกต้อง PCI DSS ดังนี้:

- ห้องสมุดเอกสาร ได้แก่:
  - *PCI DSS* – สรุปการเปลี่ยนแปลงจาก *PCI DSS* เวอร์ชั่น *2.0* ไปยัง *3.0*
  - *PCI DSS* คู่มืออ้างอิงด่วน
  - อภิธานศัพท์ ตัวย่อ และ คำย่อของ *PCI DSS* และ *PA-DSS*
  - ข้อมูลเสริม และคำแนะนำ
  - อันดับความสำคัญของวิธีการสำหรับ *PCI DSS*
  - รายงานการปฏิบัติตาม *(ROC)* แบบฟอร์มการรายงาน และคำแนะนำขั้นตอนการรายงาน
  - แบบสอบถามการประเมินด้วยตนเอง *(SAQs)* และขั้นตอนและคำแนะนำ *SAQ*
  - การรับรองมาตรฐาน *(AOCs)*
- คำถามที่พบบ่อย (FAQs)
- PCI สำหรับเว็บไซต์เชิงพาณิชย์ขนาดเล็ก
- คอร์สการฝึก และการสัมมนาให้ข้อมูลผ่านเว็บ
- รายการ ผู้ประเมินความปลอดภัยที่ผ่านการรับรอง (QSAs) แสกนผู้ขาที่ได้รับการอนุมัติ (ASVs)
- รายการ PTS อุปกรณ์ที่ได้รับอนุญาต และแอปพลิเคชั่นการชำระเงินที่ได้รับการอนุมัติ PA-DSS

***หมายเหตุ**: ข้อมูลส่วนประกอบเสริม PCI DSS และ การพิจารณาการระบุตัวตนเพิ่มเติม และ การแนะนำเพื่อให้ตรงตามความต้องการ PCI DSS — ไม่ได้แทนที่ สับเปลี่ยนได้ หรือ ขยายต่อ PCI DSS หรือความต้องการใดๆ*

โปรดดู *www.pcisecuritystandards.org* สำหรับข้อมูลเกี่ยวกับสิ่งนี้และทรัพยากรอื่นๆ

# ข้อมูลการบังคับใช้ของ **PCI DSS**

PCI DSS ใช้กับกระบวนการที่เกี่ยวข้องกับการชำระเงินผ่านบัตรทั้งหมดของหน่วยงาน (entity) — รวมไปถึงผู้ค้า ผู้ดำเนินการ สถาบันทางการเงิน และผู้ให้บริการ รวมทั้งหน่วยงาน (entity) อื่นๆ ซึ่ง จัดเก็บ ดำเนินการ และส่งข้อมูลผู้ถือบัตรและ/หรือ ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง

ข้อมูลผู้ถือบัตรและข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยงมีดังนี้:

| ข้อมูลบัญชี | |
|---|---|
| ข้อมูลผู้ถือบัตรประกอบไปด้วย: | ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง ประกอบไปด้วย: |
| ▪ หมายเลขบัญชีหลัก (PAN)<br>▪ ชื่อผู้ถือบัตร<br>▪ วันหมดอายุ<br>▪ หมายเลขบริการ | ▪ ข้อมูลการติดตามทั้งหมด<br>(ข้อมูลแถบแม่เหล็ก หรือค่าในชิป)<br>▪ CAV2/CVC2/CVV2/CID<br>▪ PINs/PIN block |

**หมายเลขบัญชีหลัก คือส่วนประกอบหลักที่บ่งชี้ข้อมูลผู้ถือบัตร** หากชื่อผู้ถือบัตร หมายเลขบริการ และ/หรือ วันหมดอายุ ซึ่งถูกจัดเก็บ ดำเนินการ หรือ ส่งข้อมูลด้วย PAN หรือถูกนำเสนอในข้อมูลแวดล้อมของผู้ถือบัตร ข้อมูลเหล่านั้นควรถูกปกป้องตามความต้องการของ PCI DSS

ความต้องการของ PCI DSS นำไปใช้กับองค์กรและสิ่งแวดล้อมซึ่งข้อมูลบัญชีได้ถูกจัดเก็บไว้ (ข้อมูลผู้ถือบัตร และ/หรือ ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง) ซึ่งถูกดำเนินการหรือมีการส่งข้อมูล ความต้องการของ PCI DSS บางส่วนอาจสามารถนำไปใช้ได้กับองค์กรซึ่งใช้การชำระเงินด้วยกระบวนการนอกการควบคุม หรือการจัดการ CDE[1] ของพวกเขา นอกจากนั้นแล้ว องค์กรซึ่งใช้กระบวนการที่นอกเหนือจาก CDE หรือกระบวนการการชำระเงินโดยบุคคลที่3 ต้องรับผิดชอบในการยืนยันว่าข้อมูลบัญชีนั้นๆจะได้รับการปกป้องโดยบุคคลที่3 ทุกการใช้งานตามความต้องการของ PCI DSS

ตารางที่แสดงอยู่ในหน้านี้แสดงให้เห็นส่วนประกอบของข้อมูลผู้ถือบัตรและ ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง ไม่ว่าการจัดเก็บแต่ละส่วนของข้อมูลจะได้รับการยินยอมหรือปฏิเสธ และไม่ว่าส่วนประกอบข้อมูลแต่ละส่วนจะถูกปกป้องไว้หรือไม่ก็ตาม ตารางนี้อาจจะไม่ได้แสดงผลทั้งหมดออกมา แต่นำเสนอออกมาเพื่อให้เห็นความแตกต่างของความต้องการซึ่งจะนำไปใช้ในแต่องค์ประกอบข้อมูล

[1] เพื่อความสอดคล้องกันกับโปรแกรมการชำระเงินของแต่ละแบรนด์

| | | องค์ประกอบข้อมูล | อนุญาตให้เข้าถึงส่วนเก็บข้อมูล | Render ข้อมูลที่จัดเก็บไว้ให้ไม่สามารถอ่านได้ตามความต้องการ 3.4 |
|---|---|---|---|---|
| ข้อมูลบัญชี | ข้อมูลผู้ถือบัตร | หมายเลขบัญชีหลัก (PAN) | ใช่ | ใช่ |
| | | ชื่อผู้ถือบัตร | ใช่ | ไม่ใช่ |
| | | หมายเลขบริการ | ใช่ | ไม่ใช่ |
| | | วันหมดอายุ | ใช่ | ไม่ใช่ |
| | ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง[2] | ข้อมูลการติดตามทั้งหมด[3] (full tack data) | ไม่ใช่ | ไม่สามารถเก็บข้อมูลได้ ตามความต้องการ 3.2 |
| | | CAV2/CVC2/CVV2/CID[4] | ไม่ใช่ | ไม่สามารถเก็บข้อมูลได้ ตามความต้องการ 3.2 |
| | | PIN/PIN block[5] | ไม่ใช่ | ไม่สามารถเก็บข้อมูลได้ ตามความต้องการ 3.2 |

ความต้องการ PCI DSS 3.3 และ 3.4 ใช้งานสำหรับ PAN เท่านั้น หาก PAN ถูกจัดเก็บไว้กับองค์ประกอบข้อมูลอื่นๆของข้อมูลผู้ถือบัตร เฉพาะ PAN ที่จะต้อง render ให้ไม่สามารถอ่านได้ตามความต้องการ PCI DSS 3.4

ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยง ไม่ควรจะถูกจัดเก็บไว้หลังได้รับการอนุญาต แม้ว่าจะถูกเข้ารหัสไว้ก็ตาม รวมไปถึงขณะที่ไม่มี PAN อยู่ในสิ่งแวดล้อม องค์กรควรติดต่อ ผู้ให้บริการแก่ผู้รับบัตร ของพวกเขา หรือแบรนด์การชำระเงินโดยตรงเพื่อความเข้าใจว่า SAD นั้นได้รับอนุญาตให้สามารถถูกจัดเก็บลงไปตามสิทธิการเข้าถึงหรือไม่ นานเท่าไร และมีการใช้งานที่เกี่ยวข้องและความต้องการการปกป้องหรือไม่

2 ข้อมูลการรับรองความถูกต้องที่สุ่มเสี่ยงไม่ควรจะถูกจัดเก็บไว้หลังได้รับการอนุญาตแล้ว (แม้ว่าจะถูกเข้ารหัสไว้ก็ตาม)

3 ข้อมูลการติดตามทั้งหมด (full tack data) จากแถบแม่เหล็ก ค่าบนชิพ หรือที่อื่นๆ

4 ค่าตัวเลข 3 หรือ 4 ตัวที่พิมพ์ไว้ที่ด้านหน้าหรือหลังบัตรที่ชำระเงิน

5 หมายเลขบัตรประชาชนที่ระบุโดยผู้ถือบัตรระหว่างการแสดงบัตรเพื่อทำธุรกรรม และ/หรือ PIN block ที่เข้ารหัสไว้ ระหว่างข้อความการทำธุรกรรม

# ความสัมพันธ์ระหว่าง PCI DSS และ PA-DSS

**การบังคับใช้ของ *PCI DSS* สำหรับแอพพลิเคชั่น *PA-DSS***

การใช้มาตรฐานความปลอดภัยของข้อมูลในแอปพลิเคชั่นการชำระเงิน (PA-DSS) ซึ่งเป็นของตัวแอปพลิเคชั่นเอง ไม่สามารถทำให้หน่วยงาน (entity) ได้รับการยินยอมจาก PCI DSS ได้ เนื่องจากแอปพลิเคชั่นนั้นต้องดำเนินการตามสิ่งแวดล้อม PCI DSS และตามแนวปฏิบัติของ PA-DSS ที่ให้ไว้โดยผู้ขายแอปพลิเคชั่นการชำระเงิน

แอปพลิเคชั่นทั้งหมดที่จัดเก็บ ดำเนินการ ส่ง ข้อมูลผู้ถือบัตร อยู่ในขอบข่ายการประเมิน PCI DSS ของหน่วยงาน รวมทั้งแอปพลิเคชั่นที่ได้รับการตรวจสอบไปสำหรับ PA-DSS แล้วการประเมิน PCI DSS ควรตรวจความถูกต้องว่า แอปพลิเคชั่นการชำระเงินที่ตรวจสอบแล้วโดย PA-DSS ได้มีการตั้งค่าอย่างเหมาะสมหรือไม่ และดำเนินการอย่างปลอดภัยตามความต้องการ PCI DSS หรือไม่ หากแอปพลิเคชั่นการชำระเงินมีการปรับแต่งที่นอกเหนือจากที่กล่าวมา ต้องมีการทบทวนเชิงลึก ในการประเมิน PCI DSS ก่อน เพราะตัวแอปพลิเคชั่นอาจไม่ใช่เวอร์ชั่นเดียวกันกับที่ PA-DSS ได้ทำการตรวจสอบไว้

ความต้องการ PA-DSS สืบเนื่องมาจาก ความต้องการ PCI DSS และกระบวนการประเมินความปลอดภัย (กำหนดไว้ในเอกสารนี้) PA-DSS ได้ให้รายละเอียดความต้องการซึ่งแอปพลิเคชั่นการชำระเงินจะต้องมีเพื่ออำนวยความสะดวกต่อการปฏิบัติตาม PCI DSS ของลูกค้า

เมื่อดำเนินการตามสิ่งแวดล้อมของ PCI DSS แล้ว การรักษาความปลอดภัยแอปพลิเคชั่นการชำระเงิน จะลดการเจาะเข้าระบบความปลอดภัยที่อาจเกิดขึ้นให้น้อยที่สุด ซึ่งเจาะเข้ามาที่ PAN และ ข้อมูลการติดตามทั้งหมด (full track data) การตรวจสอบความถูกต้องของโค้ดบัตร และค่าต่างๆ (CAV2, CID, CVC2, CVV2) และ PINs กับ PIN block พร้อมทั้งความเสียหายจากการปลอมแปลงอันเป็นผลจากการเจาะเข้าระบบนี้

เพื่อที่จะกำหนดว่า PA-DSS จะนำไปใช้กับแอปพลิเคชั่นที่ชี้แจงไว้หรือไม่ โปรดดู คำแนะนำโปรแกรม PA-DSS ซึ่งสามารถพบได้ที่ www.pcisecuritystandards.org

**การบังคับใช้ของ PCI DSS เพื่อผู้ขายแอปพลิเคชั่นการชำระเงิน**

PCI DSS อาจใช้กับผู้ขายแอปพลิเคชั่นชำระเงิน หากผู้ขายทำการ จัดเก็บ ดำเนินการ ส่งเปลี่ยน ข้อมูลผู้ถือบัตร หรือสามารถเข้าถึงข้อมูลผู้ถือบัตรของลูกค้าได้ (เช่น ในฐานะผู้ให้บริการ)

## ขอบเขตความต้องการ PCI DSS

ความต้องการทางความปลอดภัยของ PCI DSS ใช้กับส่วนประกอบของระบบทั้งหมดที่มีอยู่ใน หรือ เชื่อมโยงไปถึง สิ่งแวดล้อมข้อมูลผู้ถือบัตร สิ่งแวดล้อมข้อมูลผู้ถือบัตร หรือ CDE ประกอบไปด้วย ผู้คน กระบวนการ เทคโนโลยี ซึ่งจัดเก็บ ดำเนินการ ส่ง ข้อมูลผู้ถือบัตร หรือ ข้อมูลการตรวจสอบความถูกต้องที่ สุ่มเสี่ยง "ส่วนประกอบระบบ" ได้แก่ อุปกรณ์เครือข่าย เซิฟเวอร์ อุปกรณ์คอมพิวเตอร์ และ แอปพลิเคชั่น ตัวอย่างของส่วนประกอบระบบมีดังนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้):

- ระบบซึ่งให้ความปลอดภัยต่อบริการ (เช่น เซิฟเวอร์รับรองความถูกต้อง) ส่วนอำนวยความสะดวก (เช่น firewall ภายใน) หรือระบบซึ่งอาจกระทบไปถึงความปลอดภัย CDE (เช่น name resolution หรือ web redirection server)
- ส่วนประกอบจำลองเช่น เครื่องจำลอง สวิตช์จำลอง/เราเตอร์ อุปกรณ์จำลอง แอปพลิเคชั่นจำลอง/เดสทอป และ hypervisor
- ส่วนประกอบเครือข่าย ได้แก่ firewalls สวิตช์ เราเตอร์ จุดเชื่อมต่อไวร์เลส อุปกรณ์เครือข่าย และอุปกรณ์ความปลอดภัยอื่นๆ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้)
- ชนิดของเซิฟเวอร์ ได้แก่ web แอปพลิเคชั่น ฐานข้อมูล การรับรองความถูกต้อง เมล์ proxy Network Time Protocol (NTP) และ Domain Name System (DNS) (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้)
- แอปพลิเคชั่น รวมไปถึงการซื้อทั้งหมด และแอปพลิเคชั่น custom รวมไปถึง แอปพลิเคชั่นภายนอกและภายใน (เช่น อินเทอร์เน็ต)
- ส่วนประกอบอื่นใดก็ตามที่อยู่ใน หรือเชื่อมต่อไปยัง CDE

ขั้นแรกของการประเมิน PCI DSS คือการกำหนดขอบข่ายการตรวจสอบอย่างแม่นยำ อย่างน้อยปีละครั้ง และก่อนการประเมินประจำปี หน่วยงาน (entity) ที่ถูกประเมินจะต้องยืนยันความแม่นยำของขอบข่าย PCI DSS ของพวกเขา ด้วยการระบุตำแหน่งและกระบวนการทั้งหมดของข้อมูลผู้ถือบัตร และทำให้แน่ใจว่า สิ่งเหล่านั้นรวมอยู่ในขอบเขตของ PCI DSS แล้ว และเพื่อยืนยันความแม่นยำและความเหมาะสมของขอบเขต PCI DSS กรุณาดำเนินการตามขั้นตอนดังนี้:

- ระบุตัวตน หน่วยงาน (entity) ที่รับการประเมิน และจัดทำเอกสารการมีอยู่ของข้อมูลผู้ถือบัตรในสิ่งแวดล้อมของพวกเขา เพื่อตรวจสอบความถูกต้องว่าไม่มีข้อมูลผู้ถือบัตรปรากฏอยู่นอก CDE ที่กำหนดไว้ปัจจุบัน
- เมื่อตำแหน่งทั้งหมดของข้อมูลผู้ถือบัตรได้รับการระบุตำแหน่ง และบันทึกลงเอกสารแล้ว ให้หน่วยงาน (Entity) ใช้ผลที่ได้เพื่อตรวจสอบความถูกต้องว่า ขอบเขตของ PCI DSS เหมาะสม หรือไม่ (ตัวอย่าง เช่น ผลลัพธ์อาจเป็น แผนภาพ หรือ inventory ของตำแหน่งข้อมูลผู้ถือบัตร)
- หน่วยงาน (entity) พิจารณาข้อมูลผู้ถือบัตรใดๆที่พบว่าอยู่ในขอบเขตการประเมินของ PCI DSS และเป็นส่วนหนึ่งของ CDE หรือไม่ หากหน่วยงาน (entity) ระบุพบข้อมูลซึ่งยังไม่ได้รวมอยู่ใน CDE ปัจจุบัน ข้อมูลนั้นควรได้รับการลบออกไปอย่างปลอดภัย หรือย้ายไปอยู่ใน CDE ที่กำหนดปัจจุบัน หรือ CDE ที่กำหนดใหม่เพื่อให้ข้อมูลนี้รวมอยู่ภายในด้วย
- หน่วยงาน (entity) จัดเก็บเอกสารซึ่งแสดงถึงวิธีการที่ขอบเขต PCI DSS ถูกพิจารณา การจัดทำเอกสารจะถูกจัดเก็บไว้สำหรับการพิจารณาของผู้ประเมิน และ/หรือ สำหรับอ้างอิงในระหว่างกระบวนการยืนยันขอบเขต PCI DSS ประจำปีถัดไป

สำหรับการประเมิน PCI DSS แต่ละครั้ง ผู้ประเมินจะต้องตรวจสอบความถูกต้องว่า ขอบเขตของการประเมินนั้นได้ถูกกำหนดไว้ และจัดทำเป็นลายลักษณ์อักษรไว้อย่างแม่นยำ

## ส่วนเครือข่าย

การแบ่งส่วนเครือข่าย หรือการแยก (Segmenting) สิ่งแวดล้อมข้อมูลผู้ถือบัตรออกจากส่วนที่เหลือของเครือข่ายของหน่วยงานไม่ใช่ความต้องการของ PCI DSS อย่างไรก็ตามถือเป็นขั้นตอนที่ได้รับการแนะนำอย่างมากว่าอาจช่วยลด:

- ขอบข่ายการประเมิน PCI DSS
- ค่าใช้จ่ายการประเมิน PCI DSS
- ค่าใช้จ่ายและความลำบากของ การดำเนินการ และการบำรุงรักษาการควบคุม PCI DSS
- ความเสี่ยงขององค์กร (ลดลงด้วยการรวมข้อมูลผู้ถือบัตรให้มีความกระจัดกระจายน้อยลง อยู่ในตำแหน่งที่สามารถควบคุมได้มากขึ้น)

หากไม่มีส่วนเครือข่ายที่เหมาะสม (บางครั้งเรียกว่า flat network หรือ เครือข่ายแบน) เครือข่ายทั้งหมดจะอยู่ในการประเมิน PCI DSS การแยกส่วนเครือข่ายจะสามารถบรรลุจุดประสงค์ได้ผ่านวิธีการทางกายภาพ หรือทางตรรกะวิทยา เช่น network firewall ภายใน ที่ได้รับการตั้งค่าไว้อย่างดี เราเตอร์ที่มีรายการการควบคุมการเข้าถึงอย่างเข้มงวด หรือ เทคโนโลยีอื่นๆซึ่งจำกัดการเข้าถึงเฉพาะส่วนในเครือข่าย หากพิจารณานอกขอบเขต PCI DSS ส่วนประกอบของระบบจะต้องถูกแยก (segmented) จาก CDE อย่างเหมาะสม เพื่อที่ว่า แม้ส่วนประกอบระบบที่อยู่นอกขอบเขตจะถูกการเจาะเข้าระบบ แต่ก็ไม่ได้ส่งผลกระทบต่อความปลอดภัยของ CDE

สิ่งสำคัญที่จำเป็นต้องมีเพื่อลดขอบเขตของสิ่งแวดล้อมข้อมูลผู้ถือบัตร คือความต้องการทางธุรกิจที่สามารถเข้าใจได้อย่างชัดเจน และกระบวนการที่เกี่ยวข้องกับจัดเก็บ ดำเนินการ ส่งถ่าย ข้อมูลผู้ถือบัตร การจำกัดให้ข้อมูลผู้ถือบัตรอยู่ในสถานที่ที่น้อยลงเท่าที่ทำได้ ด้วยการตัดข้อมูลที่ไม่จำเป็นออก และรวบรวมข้อมูลที่จำเป็นไว้ ซึ่งอาจต้องใช้การ Re-engineering สำหรับการทำธุรกิจที่หวังผลเป็นระยะยาว

การทำเอกสารการเดินทางของข้อมูลผู้ถือบัตร จากแผนภาพการเดินทางของข้อมูลช่วยให้สามารถเข้าใจได้อย่างสมบูรณ์เกี่ยวกับการเดินทางของข้อมูลผู้ถือบัตรทั้งหมด และเพื่อให้มั่นใจว่าส่วนใดๆก็ตามของเครือข่ายนั้นได้ผลดีในการแยกสิ่งแวดล้อมข้อมูลผู้ถือบัตร

หากการแบ่งส่วนเครือข่ายนั้นได้ถูกนำไปใช้เพื่อการลดการประเมินขอบเขต PCI DSS ผู้ประเมินจะต้องตรวจสอบว่า การแบ่งส่วนนั้นเพียงพอที่จะลดการประเมินขอบเขตลงหรือไม่ ระดับสูง (high level) การแบ่งส่วนเครือข่ายที่เพียงพอจะแยกระบบต่างๆซึ่ง จัดเก็บ ดำเนินการ หรือส่งถ่าย ข้อมูลผู้ถือบัตร จากส่วนที่ไม่ได้กระทำการดังกล่าว อย่างไรก็ตาม ความเพียงพอของการดำเนินการเฉพาะของการแบ่งส่วนเครือข่ายอาจแปรผันได้ง่ายมาก และขึ้นอยู่กับจำนวนของตัวแปร เช่น การตั้งค่าเครือข่ายที่กำหนดไว้ให้ การใช้เทคโนโลยีต่างๆ และการดำเนินการควบคุมอื่นๆ

ภาคผนวก *D:* การแบ่งส่วนและการสุ่มตัวอย่าง ส่วนอำนวยความสะดวกทางธุรกิจ/ส่วนประกอบระบบ จะให้ข้อมูลที่มากขึ้นเกี่ยวกับผลลัพธ์การแบ่งส่วนเครือข่าย และการสุ่มตัวอย่างบนการประเมินขอบเขต PCI DSS

**ไวร์เลส**

หากมีการใช้เทคโนโลยีไร้สายเพื่อจัดเก็บ ดำเนินการ ส่งเปลี่ยน ข้อมูลผู้ถือบัตร (เช่น การทำธุรกรรมแบบ point-of-sale หรือ line-busting) หรือหาก wireless local area network (WLAN) เป็นส่วนประกอบหนึ่งด้วย หรือมีการเชื่อมต่อไปยังสิ่งแวดล้อมข้อมูลผู้ถือบัตร ความต้องการ PCI DSS และกระบวนการทดสอบสำหรับสิ่งแวดล้อมแบบไร้สายจะต้องถูกนำไปใช้ด้วย (เช่น ความต้องการ 1.2.3 และ 2.1.1 และ 4.1.1) ก่อนเทคโนโลยีไร้สายจะถูกนำไปใช้ หน่วยงาน (entity) ควรมีการประเมินผลความเสี่ยงต่อเทคโนโลยีนี้อย่างระมัดระวัง พิจารณาให้ปล่อยสัญญาณไวร์เลสเพียงเพื่อการส่งเปลี่ยนข้อมูลที่ไม่สุ่มเสี่ยงเท่านั้น

**การใช้งานผู้ให้บริการบุคคลที่3/บุคคลภายนอก**

สำหรับผู้ให้บริการจะต้องได้รับการประเมินประจำปีแบบในสถานที่ จะต้องมีการตรวจสอบภาคปฏิบัติตามบนส่วนประกอบทั้งหมดของระบบในสิ่งแวดล้อมข้อมูลผู้ถือบัตร

ผู้ให้บริการหรือผู้ค้าอาจใช้งานผู้ให้บริการบุคคลที่3 เพื่อ จัดเก็บ ดำเนินการ ส่งเปลี่ยน ข้อมูลผู้ถือบัตรด้วยตัวของผู้ให้บริการเอง หรือเพื่อจัดการส่วนประกอบ เช่น เราเตอร์ Firewall ฐานข้อมูล ความปลอดภัยทางกายภาพ และ/หรือ เซิฟเวอร์ หากใช่อาจมีการเกิดผลกระทบต่อสิ่งแวดล้อมของข้อมูลผู้ถือบัตรได้

บุคคลอื่นๆ ควรมีการระบุอย่างชัดเจนถึง บริการและส่วนประกอบระบบ ซึ่งอยู่ภายใน 1.ขอบเขตการประเมิน PCI DSS ของผู้ให้บริการ 2.ความต้องการเฉพาะของ PCI DSS ที่อยู่ภายใต้ผู้ให้บริการ และ 3.ความต้องการใดๆซึ่งเป็นความรับผิดชอบลูกค้าของผู้ให้บริการ ได้รวมไว้ในการพิจารณา PCI DSS ของพวกเขา ตัวอย่าง เช่น ผู้ให้บริการการจัดการ hosting ควรระบุให้ชัดเจนว่า IP address ใดบ้างของพวกเขาที่ได้รับการตรวจสอบในกระบวนการตรวจสอบหาช่องโหว่ประจำไตรมาส และ IP address ใดเป็นความรับผิดชอบของลูกค้าที่ต้องได้รับการตรวจสอบในกระบวนการตรวจสอบหาช่องโหว่ประจำไตรมาสด้วยตัวของพวกเขาเอง

มีสองตัวเลือกสำหรับผู้ให้บริการบุคคลที่3 เพื่อตรวจสอบการปฏิบัติตาม:

1) หากพวกเขาสามารถผ่านการประเมิน PCI DSS ด้วยตนเอง และให้หลักฐานกับลูกค้าเพื่อให้ทราบถึงการปฏิบัติตาม; หรือ
2) หากพวกเขาไม่ผ่านการประเมิน PCI DSS ด้วยตนเอง พวกเขาจะต้องให้มีการตรวจสอบบริการของพวกเขาในระหว่างกระบวนการประเมิน PCI DSS ของลูกค้าแต่ละครั้ง

หากบุคคลที่3 ผ่านการประเมิน PCI DSS ด้วยตนเอง พวกเขาควรให้หลักฐานที่เพียงพอแก่ลูกค้า เพื่อยืนยันว่าขอบเขตการประเมิน PCI DSS ของผู้ให้บริการครอบคลุมการบังคับใช้บริการสำหรับลูกค้า และความต้องการ PCI DSS ที่เกี่ยวข้องได้รับการตรวจสอบและพิจารณาแล้วว่าเหมาะสม หลักฐานเฉพาะซึ่งผู้ให้บริการชี้แจงแก่ลูกค้าจะขึ้นอยู่กับ ข้อตกลง/สัญญาระหว่าง 2 บุคคล ตัวอย่าง เช่น การใช้ AOC และ/หรือ ส่วนต่างๆที่เกี่ยวข้องกับ ROC (ได้รับการตรวจทานเพื่อปกป้องข้อมูลที่เป็นความลับใดๆก็ตาม) จะช่วยให้ผู้ให้บริการสามารถให้ข้อมูลทั้งหมด หรือบางส่วนได้

นอกจากนั้น ผู้ค้าและผู้ให้บริการจะต้องจัดการและเฝ้าสังเกต การปฏิบัติตาม PCI DSS ของผู้ให้บริการบุคคลที่3 ผู้ที่มีสิทธิการเข้าถึงข้อมูลผู้ถือบัตรที่ร่วมให้บริการด้วย ดูความต้องการ *12.8* ในเอกสารนี้สำหรับรายละเอียด

## วิธีการที่ดีที่สุดในการนำ PCI DSS ไปใช้ในกระบวนการ Business-as-Usual

เพื่อความมั่นใจว่าการควบคุมความปลอดภัยเป็นไปอย่างต่อเนื่องสำหรับการดำเนินการอย่างเหมาะสม ควรมีการปฏิบัติตาม PCI DSS ในกิจกรรม business-as-usual (BAU) ในรูปแบบส่วนหนึ่งของแผนการความปลอดภัยโดยรวมของหน่วยงาน (entity) สิ่งนี้จะทำให้หน่วยงานสามารถเฝ้าสังเกตประสิทธิผลของการควบคุมความปลอดภัยของพวกเขาบนพื้นฐานการดำเนินการอย่างต่อเนื่องได้ และสามารถบำรุงรักษาสิ่งแวดล้อมการปฏิบัติตาม PCI DSS ในการประเมิน PCI DSS ได้ ตัวอย่างวิธีการที่ PCI DSS จะเข้ากันกับกิจกรรม BAU มีดังนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้):

1. การเฝ้าสังเกตการควบคุมความปลอดภัย — เช่น firewall ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก (IDS/IPS) เฝ้าระวังความสมบูรณ์ของไฟล์ (file-integrity monitoring หรือ FIM) โปรแกรมป้องกันไวรัส การควบคุมการเข้าถึง และอื่นๆ — เพื่อให้มั่นใจว่าสิ่งเหล่านี้ทำงานได้อย่างมีประสิทธิภาพ และตรงตามจุดประสงค์
2. ทำให้มั่นใจว่าความล้มเหลวทั้งหมดในการควบคุมความปลอดภัย ถูกตรวจพบ และตอบสนองอย่างทันท่วงที กระบวนการเพื่อตอบสนองต่อความล้มเหลวในการควบคุมความปลอดภัยควรมีดังนี้:
   - กู้คืนการควบคุมความปลอดภัย
   - ตรวจหาสาเหตุความล้มเหลว
   - ตรวจหา และชี้แจงประเด็นความปลอดภัยซึ่งเกิดขึ้นในช่วงความล้มเหลวของการควบคุมความปลอดภัย
   - ดำเนินการปรับปรุงข้อมูล (เช่น กระบวนการ หรือ การควบคุมทางเทคนิค) เพื่อป้องกันการเกิดความล้มเหลวซ้ำจากสาเหตุเดิม
   - นำการเฝ้าสังเกตกลับมาทำงานเพื่อควบคุมความปลอดภัย อาจพร้อมกับการเพิ่มการเฝ้าระวังในช่วงระยะเวลาหนึ่ง เพื่อตรวจสอบว่าการควบคุมเป็นไปอย่างมีประสิทธิภาพ
3. พิจารณาการเปลี่ยนแปลงของสิ่งแวดล้อม (ตัวอย่าง เช่น การเพิ่มเติมระบบใหม่ๆ การเปลี่ยนแปลงในระบบ หรือ การตั้งค่าเครือข่าย) ไปจนถึงความสมบูรณ์ของการเปลี่ยนแปลง และดำเนินการตามขั้นตอนดังนี้:
   - กำหนดผลกระทบที่อาจเกิดขึ้นกับขอบเขต PCI DSS (ตัวอย่าง เช่น กฎ firewall ใหม่ ซึ่งอนุญาตให้มีการเชื่อมต่อระหว่างระบบใน CDE และระบบอื่นๆ ซึ่งอาจนำมาซึ่งระบบเพิ่มเติมหรือ เครือข่ายในขอบเขตสำหรับ PCI DSS)
   - แยกแยะความต้องการ PCI DSS ที่สามารถนำไปประยุกต์ใช้กับระบบ และเครือข่ายที่ได้รับผลจากการเปลี่ยนแปลงได้ (ตัวอย่างเช่น หากระบบใหม่อยู่ในขอบเขตสำหรับ PCI DSS จะต้องได้รับการตั้งค่าตามมาตรฐานการตั้งค่าระบบ รวมไปถึง FIM AV แพทช์ การทำประวัติการตรวจสอบ และอื่นๆ และจะต้องถูกเพิ่มเข้าไปในการแสกนหาช่องโหว่ประจำไตรมาส)
   - อัพเดทขอบเขต PCI DSS และ การดำเนินการควบคุมความปลอดภัยอย่างเหมาะสม
4. การเปลี่ยนแปลงของโครงสร้างองค์กร (ตัวอย่างเช่น การรวมองค์กร หรือการเข้าซื้อกิจการ) ควรให้มีการตรวจสอบอย่างเป็นทางการถึงผลกระทบต่อขอบเขตและความต้องการ PCI DSS
5. ควรมีการดำเนินการตรวจสอบและการติดต่อสื่อสารตามช่วงเวลาเพื่อยืนยันว่าความต้องการ PCI DSS ยังใช้งานได้อย่างต่อเนื่อง และบุคลากรยังคงปฏิบัติตามกระบวนการความปลอดภัย การตรวจสอบตามช่วงเวลาควรครอบคลุมสถานที่และตำแหน่งทั้งหมด รวมไปถึงร้านค้าปลีก ศูนย์ข้อมูล และอื่นๆ และรวมทั้งการตรวจสอบส่วนประกอบระบบ (หรือตัวอย่างส่วนประกอบของระบบ) เพื่อยืนยันความถูกต้องว่าความต้องการ PCI DSS ยังอยู่ในการดำเนินการอย่างต่อเนื่อง — ตัวอย่างเช่น มาตรฐานการตั้งค่าได้ถูกนำไปใช้ แพทช์ และ AV ได้รับการอัพเดท ประวัติการตรวจสอบกำลังได้รับการตรวจสอบ และอื่นๆ ความถี่ในการตรวจสอบตามช่วงเวลาควรได้รับการกำหนดโดยหน่วยงาน (entity) อย่างเหมาะสมสำหรับ ขนาดและความซับซ้อนของสิ่งแวดล้อมของพวกเขา

   การตรวจสอบเหล่านี้สามารถนำไปใช้ได้กับการตรวจสอบว่าหลักฐานที่เหมาะสมได้รับการปรับปรุงหรือไม่ — ตัวอย่างเช่น ประวัติการตรวจสอบ รายงานการแสกนหาช่องโหว่ การตรวจสอบ firewall และอื่นๆ — เพื่อช่วยในการจัดเตรียมของหน่วยงาน (entity) สำหรับการประเมินการปฏิบัติตามครั้งถัดไป

6. ตรวจสอบ hardware และเทคโนโลยี software อย่างน้อยปีละครั้งเพื่อยืนยันว่าสิ่งเหล่านี้จะยังคงได้รับการสนับสนุนจากผู้ขาย และสามารถบรรลุความต้องการด้านความปลอดภัยของหน่วยงาน (entity) รวมไปถึง PCI DSS ได้ หากพบว่าเทคโนโลยีนั้นๆไม่ได้รับการสนับสนุนจากผู้ขายอีกต่อไปแล้ว หรือไม่สามารถบรรลุความต้องการด้านความปลอดภัยของหน่วยงาน (entity) ได้ หน่วยงาน (entity) ควรเตรียมแผนการฟื้นฟูไว้ และรวมไปถึงการเปลี่ยนเทคโนโลยี หากจำเป็น

นอกเหนือจากวิธีการที่กล่าวมา องค์กรอาจพิจารณาการจำแนกหน้าที่การดำเนินการสำหรับฟังก์ชั่นความปลอดภัยเพื่อที่ว่าความปลอดภัย และ/หรือ ฟังก์ชั่นการตรวจสอบได้แยกไว้จากฟังก์ชั่นการดำเนินการ ในสิ่งแวดล้อมซึ่งหนึ่งส่วนทำหน้าที่หลายหน้าที่ (ตัวอย่างเช่น การดูแลจัดการ (administration) และ การดำเนินการด้านความปลอดภัย) หน้าที่อาจได้รับการมอบหมายในแบบที่ไม่มีส่วนหนึ่งส่วนใดที่ไม่มีการควบคุมแบบ end-to-end สำหรับ กระบวนการ ที่ไม่มี independent checkpoint ตัวอย่างเช่น ความรับผิดชอบต่อการตั้งค่า และ ความรับผิดชอบต่อการอนุมัติความเปลี่ยนแปลงอาจถูกมอบหมายให้ส่วนที่แยกจากกัน

**หมายเหตุ**: กระบวนการที่ดีที่สุดสำหรับการดำเนินการ PCI DSS เข้าสู่ กระบวนการ business-as-usual เหล่านี้ ได้ถูกระบุไว้เพื่อเป็นข้อแนะนำ และการแนวทางเท่านั้น สิ่งเหล่านี้ไม่ได้แทนที่ หรือขยายต่อความต้องการ PCI DSS ใดๆ

# สำหรับผู้ประเมิน: การสุ่มตัวอย่าง อาคารทางธุรกิจ /ส่วนประกอบของระบบ

การสุ่มตัวอย่างเป็นทางเลือกหนึ่งสำหรับผู้ประเมินเพื่ออำนวยความสะดวกกระบวนการประเมินซึ่งอาจมี อาคารทางธุรกิจ และ/หรือส่วนประกอบของระบบเป็นจำนวนมาก

การสุ่มตัวอย่าง อาคารทางธุรกิจ/ส่วนประกอบระบบ เพื่อเป็นรูปแบบหนึ่งของการตรวจสอบการปฏิบัติตาม PCI DSS ของหน่วยงาน (entity) เป็นสิ่งที่ผู้ประเมินยอมรับได้ แต่จะไม่เป็นที่ยอมรับหาก หน่วยงานใช้ความต้องการ PCI DSS สำหรับตัวอย่างสิ่งแวดล้อมเพียงตัวอย่างเดียวของพวกเขาเท่านั้น (ตัวอย่าง เช่น ความต้องการสำหรับการตรวจสอบหาช่องโหว่ประจำไตรมาสซึ่งใช้กับส่วนประกอบระบบทั้งหมด) เช่นเดียวกัน เป็นที่ยอมรับไม่ได้ หากผู้ประเมินตรวจสอบตัวอย่างเพียงตัวอย่างเดียวสำหรับการปฏิบัติตามความต้องการ PCI DSS

หากพิจารณาขอบเขตโดยรวมและความซับซ้อนของสิ่งแวดล้อมที่ได้รับการประเมิน ผู้ประเมินอาจเลือกตัวอย่าง อาคารทางธุรกิจ/ส่วนประกอบระบบ อย่างเอกเทศน์เพื่อประเมินการปฏิบัติตามความต้องการ PCI DSS ของหน่วยงาน ตัวอย่างเหล่านี้จะต้องถูกระบุก่อนเพื่อ อาคารทางธุรกิจ และหลังจากนั้น เพื่อส่วนประกอบของระบบ จากการเลือก อาคารทางธุรกิจ แต่ละครั้ง ตัวอย่างจะต้องเป็นตัวแทนของ รูปแบบและสถานที่ตั้งทั้งหมดของ อาคารทางธุรกิจ รวมทั้งรูปแบบทั้งหมดของส่วนประกอบระบบภายใน อาคารทางธุรกิจ ที่เลือก ตัวอย่างจะต้องใหญ่เพียงพอเพื่อสร้างความเชื่อใจให้กับผู้ประเมินซึ่งควบคุมการตามที่ได้คาดหวังไว้

ตัวอย่างของ อาคารทางธุรกิจ ได้แก่ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้): Office ขององค์กร ร้านค้า แฟรนไชส์ อาคารดำเนินการ ศูนย์ข้อมูล และ อาคารรูปแบบอื่นๆในสถานที่ที่แตกต่างกันออกไป การสุ่มตัวอย่างควรรวมส่วนประกอบที่อยู่ภายในแต่ละ อาคารทางธุรกิจ ที่เลือกด้วย ตัวอย่างเช่น แต่ละ อาคารทางธุรกิจ ที่เลือก จะต้องมี ระบบปฏิบัติการ ฟังก์ชั่น และแอปพลิเคชั่นซึ่งนำมาประยุกต์ใช้ในพื้นที่ อยู่ภายใต้การตรวจสอบด้วย

เพื่อเป็นตัวอย่าง ผู้ประเมินอาจกำหนดตัวอย่างที่ อาคารทางธุรกิจ ใดที่หนึ่งที่มี Sun servers ที่เปิดใช้งาน Apache, Windows servers ที่เปิดใช้งาน Oracle, ระบบเมนเฟรมเซิฟเวอร์ ที่เปิดใช้งาน legacy card processing applications, เซิฟเวอร์โอนถ่ายข้อมูล ที่เปิดใช้งาน HP-UX, และ Linux Servers ที่เปิดใช้งาน MySQL หากแอปพลิเคชั่นทั้งหมดเปิดใช้งานบนระบบปฏิบัติการเพียงเวอร์ชั่นเดียว (ตัวอย่างเช่น Windows 7 หรือ Solaris 10) ตัวอย่างควรจะมีแอปพลิเคชั่นต่างๆอยู่ด้วย (ตัวอย่างเช่น เซิฟเวอร์ฐานข้อมูล เว็บเซิฟเวอร์ เซิฟเวอร์โอนถ่ายข้อมูล)

เมื่อเลือกตัวอย่างสำหรับ อาคารทางธุรกิจ/ส่วนประกอบระบบอย่างเป็นเอกเทศน์ ผู้ประเมินควรพิจารณาดังต่อไปนี้:

- หากมีการวัดมาตรฐาน ให้รวมความปลอดภัย PCI DSS กระบวนการดำเนินการ และควบคุมเอาไว้ด้วยกัน ซึ่งทำให้มั่นใจถึงความมั่นคง และซึ่งแต่ละ อาคารทางธุรกิจ/ส่วนประกอบระบบจะต้องดำเนินการตาม ตัวอย่างสามารถมีขนาดเล็กกว่าได้หากไม่มีการใช้ กระบวนการ/การควบคุม มาตรฐาน ตัวอย่างจะต้องใหญ่เพียงพอที่จะสร้างความเชื่อใจให้กับผู้ประเมินได้ว่า อาคารทางธุรกิจ/ส่วนประกอบระบบ ทั้งหมดได้รับการตั้งค่าตามกระบวนการมาตรฐาน ผู้ประเมินต้องตรวจสอบว่า การรวมการควบคุมที่ผ่านมาตรฐานนั้น เป็นไปอย่างที่คาดหมาย และสามารถดำเนินการได้อย่างมีประสิทธิภาพหรือไม่

- หากมีการใช้งานมาตรฐานความปลอดภัย และ/หรือ กระบวนการดำเนินการ มากกว่าหนึ่ง (ตัวอย่างเช่น ใช้งานสำหรับ อาคารทางธุรกิจ/ส่วนประกอบระบบ ที่แตกต่างกัน) ตัวอย่างจะต้องใหญ่เพียงพอที่จะรวม อาคารทางธุรกิจ/ส่วนประกอบระบบ ที่ปลอดภัยเอาไว้ ในแต่ละกระบวนการ

- หากไม่มีการใช้กระบวนการ/การควบคุม PCI DSS มาตรฐาน และในแต่ละ อาคารทางธุรกิจ/ส่วนประกอบระบบ อยู่ในการจัดการโดยกระบวนการที่ไม่ตรงตามมาตรฐาน ตัวอย่างจะต้องใหญ่พียงพอเพื่อสร้างความเชื่อใจให้กับผู้ประเมินว่าแต่ละ อาคารทางธุรกิจ/ส่วนประกอบระบบ นั้นเป็นไปตามความต้องการ PCI DSS อย่างเหมาะสม

- ตัวอย่างของส่วนประกอบระบบจะต้องรวมทุกๆรูปแบบ และการผสมผสานที่นำไปใช้งานไว้ ตัวอย่างเช่น ตำแหน่งที่แอปพลิเคชั่นนั้นได้รับการสุ่มตัวอย่าง ตัวอย่างจะต้องรวบรวมเวอร์ชั่นทั้งหมด และแพลตฟอร์มสำหรับแอปพลิเคชั่นแต่ละประเภทไว้

สำหรับแต่ละส่วนซึ่งมีการสุ่มตัวอย่างเกิดขึ้น ผู้ประเมินจะต้อง:

- จัดทำเอกสารจุดประสงค์เบื้องหลังเทคนิคการสุ่มตัวอย่างและขนาดของตัวอย่าง
- จัดทำเอกสารและตรวจสอบความถูกต้องของกระบวนการและการควบคุม PCI DSS มาตรฐานที่ใช้เพื่อกำหนดขนาดของตัวอย่าง และ
- อธิบายเหตุผลที่ทำให้ตัวอย่างเหมาะสมและเป็นตัวแทนของทั้งหมดทั้งมวลได้

โปรดดู: ภาคผนวก D: การแยกส่วน (Segmentation) และ การสุ่มตัวอย่าง (Sampling) ของ อาคารทางธุรกิจ/ส่วนประกอบระบบ.

ผู้ประเมินจะต้องตรวจสอบความถูกต้องของจุดประสงค์การสุ่มตัวอย่างใหม่ในการประเมินทุกครั้ง หากจะมีการใช้การสุ่มตัวอย่าง จะต้องมีการเลือกตัวอย่าง อาคารทางธุรกิจ และส่วนประกอบระบบ ที่แตกต่างกันไปในการประเมินแต่ละครั้ง

## การควบคุมแบบทดแทน

ในวาระประจำปี การควบคุมแบบทดแทนใดๆก็ตามจะต้องได้รับการบันทึกเป็นเอกสาร ตรวจสอบ และยินยืนความถูกต้องโดยผู้ประเมิน และระบุลงในรายงานในการการส่งการปฏิบัติตาม ตาม ภาคผนวก *B:* การควบคุมแบบทดแทน และ ภาคผนวก *C:* เอกสารควบคุมการชดเชย

สำหรับการควบคุมแบบทดแทนทุกๆครั้ง เอกสารการควบคุมแบบทดแทน *(ภาคผนวก C)* **ต้อง** เสร็จสมบูรณ์ นอกจากนั้นแล้ว ผลการควบคุมแบบทดแทนจะต้องถูกจัดทำเป็นเอกสารใน ROC ตรงกันกับ ส่วนความต้องการ PCI DSS

โปรดดูที่ ภาคผนวก B และ C ดังกล่าวเพื่อรายละเอียดเกี่ยวกับ “การควบคุมแบบทดแทน”

# คำแนะนำ และ เนื้อหา สำหรับรายงานการปฏิบัติตาม

คำแนะนำ และ เนื้อหา สำหรับรายงานการปฏิบัติตาม (ROC) ได้ถูกระบุไว้แล้วในแบบแผนการรายงาน *PCI DSS ROC*

แบบแผนการรายงาน PCI DSS ROC จะต้องถูกนำมาใช้เป็นแบบเพื่อการจัดทำรายงานการปฏิบัติตาม หน่วยงานผู้ถูกประเมินควรทำตามความต้องการของแบรนด์การชำระเงินแต่ละแบรนด์ตามลำดับ เพื่อให้มั่นใจว่าแบรนด์การชำระเงินแต่ละแบรนด์ได้รับรู้ถึงสถานะการปฏิบัติตามของหน่วยงาน โปรดติดต่อกับแบรนด์การชำระเงินแต่ละแบรนด์ หรือผู้ให้บริการแก่ผู้รับบัตร เพื่อกำหนดความต้องการและขั้นตอนการรายงาน

## กระบวนการประเมิน PCI DSS

1. ยืนยันขอบเขตการประเมิน PCI DSS
2. ดำเนินการประเมินสิ่งแวดล้อม PCI DSS และดำเนินการตามขั้นตอนการทดสอบสำหรับแต่ละความต้องการ
3. หากจำเป็น ดำเนินการฟื้นฟูสำหรับส่วนที่ไม่สามารถใช้งานได้
4. ทำรายงานที่สามารถนำไปประยุกต์ใช้ได้สำหรับการประเมินให้สมบูรณ์ (เช่น Self-*Assessment Questionnaire* (SAQ) หรือ รายงานการปฏิบัติตาม (ROC) รวมไปถึงการจัดทำเอกสารการควบคุมแบบทดแทน ตามแนวทางและคำแนะนำ PCI ที่สามารถนำไปประยุกต์ใช้ได้
5. ทำการรับรองการปฏิบัติตามสำหรับผู้ให้บริการ หรือ ผู้ค้า ที่เหมาะสมให้สมบูรณ์ทั้งหมด การรับรองการปฏิบัติตามมีให้ใช้งานบนเว็บไซต์ PCI SSC
6. ส่ง SAQ หรือ ROC และการประเมินการปฏิบัติตาม พร้อม ด้วยเอกสารอื่นๆที่ต้องการ — เช่น รายงานผลการแสกน ASV— ให้กับ ผู้ให้บริการแก่ผู้รับบัตร (สำหรับผู้ค้า) หรือให้กับแบรนด์ชำระเงิน หรือ ผู้ร้องขอรายอื่นๆ (สำหรับผู้ให้บริการ)

# รายละเอียดความต้องการ และ กระบวนการประเมินความปลอดภัย PCI DSS

ข้อมูลต่อไปนี้จะชี้แจงชื่อหัวข้อสำหรับความต้องการและกระบวนการประเมินความปลอดภัย PCI DSS:

- **ความต้องการ** PCI DSS – หัวข้อนี้กำหนดสำหรับความต้องการมาตรฐานความปลอดภัยของข้อมูล; การปฏิบัติตาม PCI DSS จะถูกตรวจสอบความถูกต้องจากความต้องการเหล่านี้
- **กระบวนการทดสอบ** – หัวข้อนี้จะแสดงกระบวนการที่ผู้ประเมินจะต้องดำเนินการเพื่อตรวจสอบความถูกต้องว่าตรงตามความต้องการ PCI DSS และ"ใช้งานได้" หรือไม่
- **คำแนะนำ** – หัวข้อนี้ให้แสดงถึงเจตนา หรือจุดประสงค์ด้านความปลอดภัยเบื้องหลังความต้องการ PCI DSS แต่ละข้อ หัวข้อนี้เป็นเพียงแนวทางเท่านั้น และมีไว้เพื่อช่วยให้เข้าใจจุดประสงค์ของความต้องการแต่ละข้อมากขึ้น แนวทางในหัวข้อนี้ไม่ได้แทนที่ หรือขยายต่อ ความต้องการ PCI DSS และกระบวนการทดสอบ

**หมายเหตุ**: ความต้องการ PCI DSS จะไม่ถูกพิจารณาว่าใช้งานได้หากยังไม่ได้ปฏิบัติตามการควบคุมหรือยังอยู่ในแผนการในอนาคต หลังจาก ช่องโหว่ หรือ สิ่งที่ยังไม่สามารถใช้งานได้ได้รับการชี้แจงโดยหน่วยงานแล้ว ผู้ประเมินจึงจะทำการประเมินอีกครั้งเพื่อตรวจสอบความถูกต้องว่าการฟื้นฟูนั้นสมบูรณ์และตรงตามความต้องการแล้วหรือไม่

โปรดดูที่แหล่งข้อมูลต่อไปนี้ (สามารถใช้งานได้บนเว็บไซต์ PCI SSC) เพื่อจัดทำเอกสารการประเมิน PCI DSS:

- สำหรับคำแนะนำในการทำให้รายงานการปฏิบัติตาม (ROC) สำเร็จลุล่วง โปรดดู แบบแผนการรายงาน PCI DSS ROC
- สำหรับคำแนะนำในการทำให้ self-assessment questionnaires (SAQ) สำเร็จ โปรดดูที่ คำแนะนำ และ แนวทาง PCI DSS SAQ
- สำหรับคำแนะนำในการส่งรายงานการตรวจสอบความถูกต้องการปฏิบัติตาม PCI DSS โปรดดูที่การรับรองการปฏิบัติตาม PCI DSS

# สร้างและบำรุงรักษา เครือข่ายและระบบที่ปลอดภัย

**ความต้องการที่** 1: **ติดตั้งและบำรุงรักษาการตั้งค่า firewall เพื่อปกป้องข้อมูลข้อมูลผู้ถือบัตร**

Firewalls คืออุปกรณ์ที่ควบคุมการอนุญาตการส่งข้อมูล ระหว่างเครือข่ายของหน่วยงาน (ภายใน) และเครือข่ายที่ไม่สามารถเชื่อถือได้ (ภายนอก) พร้อมกับการส่งข้อมูล เข้าและออกจาก พื้นที่สุ่มเสี่ยงภายในเครือข่ายภายในของหน่วยงาน (entity) สิ่งแวดล้อมข้อมูลผู้ถือบัตรเป็นตัวอย่างหนึ่งของพื้นที่ที่สุ่มเสี่ยงภายใต้เครือข่ายภายในของหน่วยงาน

Firewall ตรวจสอบการส่งข้อมูลทั้งหมด และยับยั้งการส่งข้อมูลที่ไม่ได้ผ่านการแยกแยะด้านความปลอดภัยอย่างเฉพาะเจาะจง

ระบบทั้งหมดจะต้องได้รับการปกป้องจากการเข้าถึงที่ไม่ได้รับการอนุญาตซึ่งมาจากเครือข่ายที่ไม่ได้รับการไว้วางใจ ไม่ว่าจะเข้าสู่ระบบผ่านอินเทอร์เน็ตในฐานะ E-commerce การเข้าถึงอินเทอร์เน็ตผ่าน browser บน desktop ของลูกจ้าง การเข้าถึงอีเมล์ของลูกจ้าง การเชื่อมต่อเฉพาะเช่น การเชื่อมต่อแบบ business-to-business ผ่านทาง wireless network หรือผ่านแหล่งอื่นๆก็ตาม เส้นทางที่ดูเหมือนว่าไม่มีนัยสำคัญที่เชื่อม ไปยัง หรือ มาจาก เครือข่ายที่ไม่ได้รับการไว้วางใจ มักจะสร้างเส้นทางที่ไร้การป้องกันเข้าไปสู่ส่วนสำคัญของระบบได้ ดังนั้น Firewall จึงเป็นกุญแจสำคัญในการปกป้องกลไกของเครือข่ายคอมพิวเตอร์ใดๆก็ตาม

ส่วนประกอบระบบอื่นๆ อาจผ่าน Firewall ได้ตราบใดที่สิ่งเหล่านั้นสามารถผ่านความต้องการขั้นพื้นฐานของ firewall ตามที่กำหนดไว้ในความต้องการที่ 1 ได้ ในขณะที่การที่ส่วนประกอบระบบอื่นๆถูกนำไปใช้ในสิ่งแวดล้อมข้อมูลผู้ถือบัตรเพื่อผ่าน firewall นั้น อุปกรณ์เหล่านี้จะต้องรวมอยู่ในขอบเขตและการประเมินความต้องการที่ 1

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.1 จัดตั้ง firewall และดำเนินการตามมาตรฐานการตั้งค่าเราเตอร์ดังนี้: | 1.1 ตรวจสอบมาตรฐานการตั้งค่า เราเตอร์ และ firewall และเอกสารอื่นๆ ดังที่ระบุไว้ด้านล่าง และตรวจสอบว่าสมบูรณ์ตามมาตรฐาน และดำเนินการตามข้อมูลดังนี้: | Firewall และ เราเตอร์ คือส่วนประกอบสำคัญของสถาปัตยกรรมซึ่งควบคุม การเข้า และ ออกจาก เครือข่าย อุปกรณ์เหล่านี้คือ software หรือ hardware ซึ่งป้องกันการเข้าถึงที่ไม่พึงประสงค์ และจัดการการให้สิทธิในการ การเข้าถึง และการออกจาก เครือข่าย<br>มาตรฐานการตั้งค่าและกระบวนการ จะช่วยให้มั่นใจว่าการป้องกันชั้นหน้าสุดขององค์กรนั้นเข้มแข็งเพียงพอในการปกป้องข้อมูลองค์กร |
| 1.1.1 กระบวนการอย่างเป็นทางการในการอนุมัติและทดสอบการเชื่อมต่อเครือข่ายทั้งหมด และการเปลี่ยนแปลงการตั้งค่าของ firewall และ เราเตอร์ | 1.1.1.a ตรวจสอบกระบวนการในเอกสารเพื่อตรวจให้แน่ใจว่าได้มีกระบวนการอย่างเป็นทางการสำหรับการทดสอบและการอนุมัติทั้งหมดดังต่อไปนี้:<br>• การเชื่อมต่อเครือข่าย และ<br>• การเปลี่ยนแปลง การตั้งค่าของ firewall และ เราเตอร์ | กระบวนการที่จัดทำในเอกสารซึ่งได้รับการดำเนินการเพื่อการอนุมัติ และการทดสอบเครือข่ายทั้งหมด และการเปลี่ยนแปลงของ firewall และ เราเตอร์ จะช่วยป้องกันปัญหาความปลอดภัยที่อาจเกิดขึ้นโดยการตั้งค่าที่ผิดพลาดของ เครือข่าย เราเตอร์ หรือ firewall<br>หากไม่มีการอนุมัติอย่างเป็นทางการ และการทดสอบการเปลี่ยนแปลง บันทึกการเปลี่ยนแปลงจะไม่เป็นปัจจุบัน ซึ่งอาจนำไปสู่ความไม่สอดคล้องกันระหว่างเอกสารเครือข่าย และ การตั้งค่าจริง |
| | 1.1.1.b สำหรับตัวอย่างการเชื่อมต่อเครือข่าย ทำการสัมภาษณ์บุคลากรผู้รับผิดชอบ และตรวจสอบบันทึกเพื่อตรวจให้แน่ใจว่าการเชื่อมต่อเครือข่ายเหล่านั้นได้รับการอนุมัติและการทดสอบแล้ว | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| | 1.1.1.c ระบุตัวอย่างการเปลี่ยนแปลงจริงกับการตั้งค่า firewall และ เราเตอร์ เปรียบเทียบกับประวัติการเปลี่ยนแปลง และทำการสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจให้แน่ใจว่าการเปลี่ยนแปลงนั้นๆได้รับการอนุมัติและการทดสอบแล้ว | |
| 1.1.2 แผนภาพเครือข่าย ปัจจุบัน ซึ่งระบุการเชื่อมต่อทั้งหมดระหว่างสิ่งแวดล้อมข้อมูลผู้ถือบัตร และ เครือข่ายอื่นๆ รวมไปถึงการเชื่อมต่อแบบไร้สาย | 1.1.2.a ตรวจสอบแผนภาพ และสังเกตการตั้งค่าเครือข่ายเพื่อตรวจสอบความถูกต้องของแผนภาพเครือข่ายปัจจุบัน และตรวจสอบว่าได้มีการบันทึกการเชื่อมต่อทั้งหมดของข้อมูลผู้ถือบัตร รวมไปถึงเครือข่ายไร้สายใดๆแล้วหรือไม่ | แผนภาพเครือข่ายอธิบายวิธีการที่เครือข่ายถูกตั้งค่า และระบุสถานที่ของอุปกรณ์เครือข่ายทั้งหมด<br>หากไม่มีแผนภาพปัจจุบัน อุปกรณ์อาจถูกมองข้ามและถูกทิ้งไว้ให้ปราศจากการควบคุมความปลอดภัยที่ดำเนินการตาม PCI DSS และทำให้มีช่องโหว่ |
| | 1.1.2.b ทำการสัมภาษณ์บุคลากรที่รับผิดชอบเพื่อตรวจสอบความถูกต้องว่าแผนภาพนั้นเป็นปัจจุบัน | |
| 1.1.3 แผนภาพปัจจุบันซึ่งแสดงให้เห็นการเดินทางของข้อมูลผู้ถือบัตร ในระบบและเครือข่าย | 1.1.3 ตรวจสอบแผนภาพการเดินทางของข้อมูล และทำการสัมภาษณ์บุคลากรเพื่อตรวจความถูกต้องของแผนภาพ:<br>• แสดงให้เห็นการเดินทางของข้อมูลผู้ถือบัตรทั้งหมดภายในระบบและเครือข่าย<br>• ให้แน่ใจว่าเป็นปัจจุบัน และอัพเดทเท่าที่จำเป็นสำหรับการเปลี่ยนแปลงของสิ่งแวดล้อม | แผนภาพการเดินทางของข้อมูลผู้ถือบัตรต้องระบุตำแหน่งข้อมูลผู้ถือบัตรทั้งหมดซึ่ง จัดเก็บ ดำเนินการ หรือ ส่งถ่ายภายในเครือข่าย<br>เครือข่าย และ แผนภาพการเดินทางของข้อมูลผู้ถือบัตร ช่วยให้องค์กรเข้าใจ และ ติดตามขอบเขตสิ่งแวดล้อมของสิ่งเหล่านั้นด้วยการแสดงให้เห็นเส้นทางการเดินทางของข้อมูลผู้ถือบัตรในเครือข่ายระหว่างแต่ละระบบ และอุปกรณ์ |
| 1.1.4 ความต้องการสำหรับ firewall สำหรับการเชื่อมต่ออินเทอร์เน็ตแต่ละครั้ง และระหว่าง demilitarized zone (DMZ) และ ในบริเวณเครือข่ายภายใน | 1.1.4.a ตรวจสอบมาตรฐานการตั้งค่า firewall และตรวจให้แน่ใจว่าพวกเขารวบรวมความต้องการเพื่อ firewall ในแต่ละการเชื่อมต่ออินเทอร์เน็ตและ ระหว่าง DMZ ใดๆ และพื้นที่เครือข่ายภายใน | การใช้ Firewall ในแต่ละการเชื่อมต่ออินเทอร์เน็ตที่ เข้า (และออกจาก) เครือข่าย และ ระหว่าง DMZ ใดๆก็ตาม และเครือข่ายภายใน อนุญาตให้องค์กรสามารถเฝ้าสังเกตและเข้าถึงการควบคุม และลดโอกาสความเป็นไปได้ของผู้ประสงค์ร้ายที่จะได้รับการเข้าถึงเครือข่ายภายในผ่านการเชื่อมต่อที่ไร้การป้องกันได้ |
| | 1.1.4.b ตรวจให้แน่ใจว่าแผนภาพเครือข่ายปัจจุบันนั้นสอดคล้องกันกับมาตรฐานการตั้งค่า firewall | |
| | 1.1.4.c สังเกตการตั้งค่าเครือข่ายเพื่อให้แน่ใจว่า firewall ใช้งานได้ในการเชื่อมต่ออินเทอร์เน็ตแต่ละครั้ง และระหว่าง demilitarized zone (DMZ) ใดๆ และในบริเวณเครือข่ายภายใน ตามเอกสารมาตรฐานการตั้งค่า และแผนภาพเครือข่าย | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.1.5 อธิบายถึงกลุ่ม บทบาท และความรับผิดชอบ สำหรับ การจัดการส่วนประกอบเครือข่าย | 1.1.5.a ตรวจให้แน่ใจว่า มาตรฐานการตั้งค่า firewall และ เราเตอร์ รวมไปถึงรายละเอียดของ กลุ่ม บทบาท และ ความรับผิดชอบในการจัดการส่วนประกอบเครือข่าย | นี่เป็นรายละเอียดบทบาทของการมอบหมายความรับผิดชอบเพื่อให้มั่นใจว่าบุคลากรได้ตระหนักว่าใครเป็นผู้รับผิดชอบความปลอดภัยของส่วนประกอบเครือข่ายทั้งหมด และการมอบหมายการจัดการส่วนประกอบเครือข่ายนั้นตระหนักถึงความรับผิดชอบของพวกเขา หากบทบาท และความรับผิดชอบไม่ได้รับการมอบหมายอย่างเป็นทางการ อุปกรณ์อาจถูกทิ้งไว้โดยไร้การจัดการ |
| | 1.1.5.b ทำการสัมภาษณ์บุคลากรที่รับผิดชอบต่อการจัดการส่วนประกอบเครือข่ายเพื่อยืนยันบทบาท และความรับผิดชอบซึ่งได้รับการมอบหมายตามเอกสาร | |
| 1.1.6 การจัดทำเอกสารและ การแสดงสิทธิทางธุรกิจ (business justification) สำหรับ service, protocol และ port ที่ได้รับอนุญาตทั้งหมด รวมไปถึง การทำเอกสาร feature ที่ดำเนินการสำหรับ protocol ที่พิจารณาว่าไม่ปลอดภัย<br><br>ตัวอย่างของ service, protocol หรือ port ที่ไม่ปลอดภัย รวมไปถึง FTP, Telnet, POP3, IMAP และ SNMP v1 และ v2<br>(เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) | 1.1.6.a ตรวจให้แน่ใจว่า มาตรฐานการตั้งค่า firewall และ เราเตอร์ ได้รวมเอกสารรายการ services protocols และ port ทั้งหมด รวมทั้งการแสดงสิทธิทางธุรกิจ (business justification) สำหรับแต่ละสิ่งไว้ — ตัวอย่าง เช่น hypertext transfer protocol (HTTP) และ Secure Sockets Layer (SSL), Secure Shell (SSH) และ Virtual Private Network (VPN) protocols | การเจาะเข้าระบบมักเกิดขึ้นเนื่องจาก service และ port ที่ไม่ปกติ หรือไม่ปลอดภัย เนื่องจากรู้กันว่าสิ่งนี้มักเป็นช่องโหว่ และองค์กรจำนวนมากมักไม่จัดการช่องโหว่สำหรับ service, protocol และ port ที่พวกเขาไม่ได้ใช้ (แม้ว่าช่องโหว่จะยังถูกพบอยู่ในปัจจุบัน) ด้วยการกำหนดอย่างชัดเจนและการจัดทำเอกสารservice, protocol และ port ซึ่งจำเป็นสำหรับธุรกิจ องค์กรจะสามารถมั่นใจได้ว่า service, protocol, และ port อื่นๆนั้นได้รับการปิดใช้งาน หรือถอดถอนออกไปแล้ว<br><br>หาก service, protocol, หรือ port ที่ไม่ปลอดภัยนั้นจำเป็นต่อธุรกิจ ความเสี่ยงจากการใช้ protocol เหล่านี้ควรเป็นที่เข้าใจอย่างแน่ชัด และได้รับการยอมรับจากองค์กร การใช้ protocol นี้ ควรได้รับการแสดงการตัดสินใจ และ feature ความปลอดภัยซึ่งอนุญาตให้ protocol เหล่านี้ถูกใช้งานจะต้องได้รับการจัดทำเป็นเอกสาร และดำเนินการ หาก service, protocol หรือ port ที่ไม่ปลอดภัยเหล่านี้ไม่จำเป็นสำหรับธุรกิจ ควรถูกปิดการใช้งาน หรือถอดถอนออกไป |
| | 1.1.6.b ระบุ service, protocol และ port ที่ได้รับอนุญาต ซึ่งไม่ปลอดภัย; และตรวจให้แน่ใจว่า feature ความปลอดภัย ได้ถูกจัดทำเป็นเอกสารสำหรับแต่ละ service | |
| | 1.1.6.c 9 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ ให้แน่ใจว่าเอกสาร feature ความปลอดภัยนั้นดำเนินการถูกต้องสำหรับแต่ละ service, protocol และ port ที่ไม่ปลอดภัย | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.1.7 ความต้องการในการตรวจสอบกฎของ firewall และ เราเตอร์ จะต้องทำอย่างน้อย 6 เดือนต่อครั้ง | 1.1.7.a ตรวจให้แน่ใจว่า มาตรฐานการตั้งค่า firewall และ เราเตอร์ มีการร้องขอการตรวจสอบกฎ firewall และ เราเตอร์ 6 เดือนต่อครั้ง<br><br>1.1.7.b ตรวจสอบการจัดทำเอกสารที่เกี่ยวข้องกับการตรวจสอบกฎ และทำการสัมภาษณ์บุคลากรที่รับผิดชอบ ตรวจให้แน่ใจว่ากฎ (rule sets) ได้รับการตรวจทาน อย่างน้อย 6 เดือนต่อครั้ง | การตรวจสอบนี้สร้างโอกาสให้องค์กรสามารถจัดการกับข้อมูลที่ไม่จำเป็น ล้าสมัย หรือ กฎที่ไม่ถูกต้องได้ทุกๆ 6 เดือน และเพื่อให้มั่นใจว่ากฎ (rule sets) ทั้งหมด อนุญาตให้เฉพาะ service ที่ได้รับอนุญาต และ port ซึ่งตรงกับเอกสาร business justifications<br><br>องค์กรที่มีการเปลี่ยนแปลงระดับสูงต่อกฎ (rule sets) ของ firewall และ เราเตอร์ ควรต้องพิจารณาให้มีการตรวจสอบถี่ขึ้น เพื่อให้มั่นใจได้ว่า the rule sets เหล่านั้นตรงต่อความต้องการของธุรกิจอย่างต่อเนื่อง |
| 1.2 สร้างการตั้งค่า firewall และ เราเตอร์ ซึ่งจำกัดการเชื่อมต่อระหว่างเครือข่ายที่ไม่ได้รับความไว้วางใจ กับ ส่วนประกอบระบบใดๆก็ตามในสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br><br>หมายเหตุ: “เครือข่ายที่ไม่ได้รับความไว้วางใจ” คือ เครือข่ายใดก็ตามซึ่งอยู่ภายนอกความเป็นเจ้าของภายใต้การตรวจสอบของ หน่วยงาน (*entity*) และ/หรือ ไม่อยู่ในการควบคุมหรือการจัดการของหน่วยงาน | 1.2 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ และดำเนินการตามต่อไปนี้เพื่อตรวจให้แน่ใจว่าการเชื่อมต่อนั้นได้มีการจำกัดไว้ระหว่างเครือข่ายที่ไม่ได้รับการไว้วางใจ และ ส่วนประกอบระบบในสิ่งแวดล้อมข้อมูลผู้ถือบัตร: | เป็นสิ่งจำเป็นที่จะต้องติดตั้งการปกป้องเครือข่ายระหว่างเครือข่ายภายใน ที่ได้รับการไว้วางใจ และเครือข่ายที่ไม่ได้รับการไว้วางใจซึ่งเป็นเครือข่ายภายนอก และ/หรืออยู่นอกเหนือการควบคุมหรือจัดการของ หน่วยงาน ความล้มเหลวในการปฏิบัติตาม measure นี้อย่างถูกต้อง ส่งผลให้หน่วยงานมีช่องโหว่สำหรับการเข้าถึงที่ไม่ได้รับอนุญาตจากบุคคล หรือ software ที่ประสงค์ร้าย<br><br>การจะให้ firewall ทำงานได้อย่างมีประสิทธิภาพ ควรจะต้องมีการตั้งค่าอย่างเหมาะสมเพื่อควบคุม และ/หรือ จำกัดการเชื่อมต่อ เข้าสู่ หรือ ออกจากเครือข่ายของหน่วยงาน |
| 1.2.1 จำกัดการเชื่อมต่อ เข้าสู่ และ ออกจากเครือข่ายไว้เฉพาะส่วนที่จำเป็นสำหรับสิ่งแวดล้อมข้อมูลผู้ถือบัตร และปฏิเสธการส่งข้อมูลอื่นๆทั้งหมดอย่างเฉพาะเจาะจง | 1.2.1.a ตรวจสอบ มาตรฐานการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่าสิ่งเหล่านั้นได้ระบุ การเชื่อมต่อ เข้าสู่ และ ออกจาก เครือข่ายที่จำเป็นสำหรับสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br><br>1.2.1.b ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่าการเชื่อมต่อ เข้าสู่ และออกจากเครือข่าย ได้มีการจำกัดไว้เท่าที่จำเป็นสำหรับสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br><br>1.2.1.c ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า การเชื่อมต่อ เข้าสู่ และ ออกจากระบบอื่นๆทั้งหมดได้รับการปฏิเสธอย่างเฉพาะเจาะจง ตัวอย่างเช่น จากการใช้งานอย่างชัดเจน “ปฏิเสธทั้งหมด” หรือ การปฏิเสธอย่างชัดเจนหลังจากสถานะการอนุญาต | ความต้องการนี้ มีจุดประสงค์เพื่อป้องกันผู้ประสงค์ร้ายจากการเข้าถึงเครือข่ายของ หน่วยงาน (entity) จาก IP addresses ที่ไม่ได้รับอนุญาต หรือ โดยใช้ service, protocol, หรือ ports ที่อยู่ในสถานะไม่ได้รับอนุญาต (ตัวอย่าง เช่น เพื่อส่งข้อมูลที่พวกเขาได้จากคุณจากภายในเครือข่ายของคุณ ออกไปยังเซิฟเวอร์ที่ไม่ได้รับความไว้วางใจ)<br><br>การดำเนินการให้กฎปฏิเสธการเชื่อมต่อ เข้าสู่ และ ออกจากเครือข่ายทั้งหมดซึ่งไม่ได้ระบุเป็นการเฉพาะไว้เป็นสิ่งจำเป็นเพื่อป้องกัน ช่องโหว่ที่เกิดจากความไม่ตั้งใจซึ่งอาจอนุญาตให้ การเชื่อมต่อที่ไม่ต้องการ และอาจมีอันตราย เข้าสู่ หรือ ออกจาก เครือข่ายได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.2.2 สร้างความปลอดภัย และ Sync ไฟล์การตั้งค่าเราเตอร์ | 1.2.2.a ตรวจสอบไฟล์การตั้งค่าเราเตอร์เพื่อตรวจให้แน่ใจว่าสิ่งเหล่านี้ปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาต<br><br>1.2.2.b ตรวจสอบการตั้งค่าเราเตอร์เพื่อให้แน่ใจว่าได้ Sync แล้ว — ตัวอย่าง เช่น run (หรือ active) การตั้งค่าที่ตรงกับการตั้งค่าเริ่มต้น (ใช้เมื่อเครื่อง boot) | ระหว่าง run (หรือ active) ไฟล์การตั้งค่าเราเตอร์ รวมไปถึง current การตั้งค่าความปลอดภัย ไฟล์ start- up (ซึ่งถูกนำไปใช้เมื่อเราเตอร์ถูกรีสตาร์ท หรือ boot) จะต้องอัพเดทด้วยการตั้งค่าเดียวกันเพื่อให้แน่ใจว่าการตั้งค่าเหล่านี้ได้ถูกนำไปใช้เมื่อ start –up ด้วย<br><br>เพราะว่ามัน run เป็นบางครั้งนั้น ไฟล์การตั้งค่าเมื่อ start-up นั้นมักถูกลืม และไม่ได้อัพเดท เมื่อเราเตอร์รีสตาร์ท และโหลดการตั้งค่า start-up ซึ่งไม่ได้อัพเดทให้เป็นแบบเดียวกันกับการ run อาจทำให้นั่นเป็นจุดอ่อนซึ่งอาจอนุญาตให้ผู้ประสงค์ร้ายเข้าสู่เครือข่ายได้ |
| 1.2.3 ติดตั้งขอบเขตกั้น firewalls ระหว่างการเชื่อมต่อเครือข่ายไร้สายทั้งหมด และสิ่งแวดล้อมข้อมูลผู้ถือบัตร และตั้งค่า firewalls เหล่านั้นให้ปฏิเสธ หรือ หากการเชื่อมเชื่อมต่อนั้นมีเหตุจำเป็นต่อธุรกิจ ให้อนุญาตเฉพาะการเชื่อมต่อที่ได้รับอนุญาตระหว่างสิ่งแวดล้อมไร้สาย และสิ่งแวดล้อมข้อมูลผู้ถือบัตร | 1.2.3.a ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่ามีขอบเขตกั้น firewalls ติดตั้งไว้ระหว่างเครือข่ายไร้สายและสิ่งแวดล้อมข้อมูลผู้ถือบัตรทั้งหมด<br><br>1.2.3.b ตรวจให้แน่ใจว่า firewalls ปฏิเสธ หรือหากการเชื่อมต่อนั้นมีเหตุจำเป็นต่อธุรกิจ ให้อนุญาตเฉพาะการเชื่อมต่อที่ได้รับอนุญาตระหว่างสิ่งแวดล้อมไร้สาย และสิ่งแวดล้อมข้อมูลผู้ถือบัตร | การดำเนินการที่รู้จัก (หรือ ไม่รู้จัก) และ การแสวงหาผลประโยชน์ของเทคโนโลยีไร้สายภายในเครือข่าย มักเป็นเส้นทางหลักๆสำหรับผู้ประสงค์ร้ายในการได้มาซึ่งการเข้าถึงเครือข่ายและข้อมูลผู้ถือบัตร หากอุปกรณ์ไร้สาย หรือ เครือข่ายได้รับการติดตั้งโดยปราศจากความรู้ของ หน่วยงาน (entity)ผู้ประสงค์ร้ายสามารถเข้าออกเครือข่ายอย่างไร้ร่องรอย และอย่างง่ายดายได้ หาก firewalls ไม่ได้ทำการจำกัดการเข้าถึงเครือข่ายไร้สายลงใน CDEผู้ประสงค์ร้ายผู้ได้รับการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตจะสามารถเชื่อมต่อไปยัง CDE ได้อย่างง่ายดาย และเจาะเข้าระบบข้อมูลบัญชีได้<br><br>Firewalls จะต้องได้รับการติดตั้งระหว่างเครือข่ายไร้สายทั้งหมดและ CDE โดยไม่คำนึงว่าจุดประสงค์ของสิ่งแวดล้อมจะเชื่อมต่อไปยังเครือข่ายไร้สายใด นี่อาจรวมไปถึง เครือข่าย corporate ร้านค้าปลีก เครือข่ายผู้มาเยือน สิ่งแวดล้อมwarehouse และอื่นๆ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) |

| ความต้องการ **PCI DSS** | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.3 ยับยั้งการเข้าถึงอย่างสาธารณะระหว่าง อินเทอร์เน็ต และส่วนประกอบระบบใดๆ ในสิ่งแวดล้อมข้อมูลผู้ถือบัตร | 1.3 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ — รวมไปถึง choke router ไปยัง อินเทอร์เน็ต, DMZ เราเตอร์ และ firewall, ส่วนผู้ถือบัตร DMZ, ค่าเราเตอร์, และ ส่วนเครือข่ายผู้ถือบัตรภายใน (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) — และ ดำเนินการตามต่อไปนี้เพื่อกำหนดให้ไม่มีการเข้าถึงโดยตรงระหว่าง อินเทอร์เน็ต กับ ส่วนประกอบระบบในส่วนเครือข่ายข้อมูลผู้ถือบัตรภายใน: | จุดประสงค์ของ Firewall คือการจัดการ และควบคุมการเชื่อมต่อ ทั้งหมด ระหว่างระบบสาธารณะ และระบบภายใน โดยเฉพาะส่วน ที่ จัดเก็บ ดำเนินการ ส่งถ่าย ข้อมูลผู้ถือบัตร หากการเข้าถึงโดยตรง ได้รับการอนุญาต ระหว่างระบบสาธารณะ และ CDE การป้องกัน ของ firewall จะถูก bypassed และส่วนประกอบระบบ ที่จัดเก็บ ข้อมูลผู้ถือบัตรอาจถูกเปิดเผยให้สามารถเจาะเข้ามาได้ |
| 1.3.1 ดำเนินการให้ DMZ จำกัดการเชื่อมต่อ เข้าสู่ เครือข่ายเพื่อให้เฉพาะส่วนประกอบระบบที่ได้รับการ อนุญาตเข้าถึง service, protocol, และ port อย่าง สาธารณะ | 1.3.1 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า DMZ ได้มีการ ดำเนินการเจอจำกัดการเชื่อมต่อ เข้าสู่ เครือข่ายไว้ให้เฉพาะส่วนประกอบระบบที่ได้รับ การอนุญาตเข้าถึง service, protocol, และ port อย่างสาธารณะเท่านั้น | DMZ คือส่วนหนึ่งของเครือข่ายที่จัดการการเชื่อมต่อระหว่าง อินเทอร์เน็ต (หรือ เครือข่ายที่ไม่ได้รับความไว้วางใจอื่นๆ) และ service ซึ่งองค์กรต้องการให้สามารถใช้ได้อย่างสาธารณะ (เช่น web server)<br><br>การใช้งานนี้มีจุดประสงค์เพื่อป้องกันผู้ประสงค์ร้ายจากการ เข้าถึงเครือข่ายภายในขององค์กรจากอินเทอร์เน็ต หรือ ผ่านการ ใช้ service, protocol, หรือ port ในสภาวะที่ไม่ได้รับอนุญาต |
| 1.3.2 จำกัดการเชื่อมต่ออินเทอร์เน็ต เข้าสู่ เครือข่าย สำหรับ IP addresses ภายใน DMZ | 1.3.2 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า การเชื่อมต่อ อินเทอร์เน็ต เข้าสู่ เครือข่าย ได้จำกัดไว้สำหรับ IP addresses ภายใน DMZ | |
| 1.3.3 ไม่อนุญาตให้การเชื่อมต่อ เข้าสู่ หรือ ออก จาก เครือข่ายโดยตรง ระหว่าง อินเทอร์เน็ตและ สิ่งแวดล้อมข้อมูลผู้ถือบัตร | 1.3.3 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า การเชื่อมต่อ โดยตรง เข้าสู่ หรือ ออกจาก เครือข่าย ไม่ได้รับอนุญาตระหว่างอินเทอร์เน็ต และ สิ่งแวดล้อมข้อมูลผู้ถือบัตร | การตรวจสอบการเชื่อมต่อ เข้าสู่ และ ออกจาก เครือข่ายทั้งหมดทำให้ สามารถ ตรวจสอบ และ จำกัดการส่งข้อมูลได้ โดยมีพื้นฐานมาจาก แหล่งที่มา และ/หรือ address ปลายทาง รวมไปถึงการตรวจสอบ และ ปิดกั้นเนื้อหาที่ไม่ต้องการ แล้วจึงป้องกันการเข้าถึงที่ไม่ผ่านการ กลั่นกรองระหว่าง สิ่งแวดล้อมที่เชื่อถือได้ กับ เชื่อถือไม่ได้ สิ่งนี้จะ ช่วยในการป้องกัน ตัวอย่างเช่น ผู้ประสงค์ร้ายที่ต้องการส่ง ข้อมูลที่ได้รับจากภายในเครือข่ายของคุณ ออกไปยังเซิฟเวอร์ ภายนอกที่ไม่ได้รับการไว้วางใจในเครือข่ายที่ไม่ได้รับการไว้วางใจ เช่นกัน |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.3.4 ดำเนินการประเมิน การต่อต้านการปลอมแปลง (anti-spoofing) เพื่อตรวจจับและ ปิดกั้น forged source IP addresses จากการเข้าสู่เครือข่าย (ตัวอย่างเช่น ปิดกั้นการส่งข้อมูลที่มีที่มาจากอินเทอร์เน็ตใน address ที่มีแหล่งที่มาจากภายใน) | 1.3.4 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า การประเมินการต่อต้านการปลอมแปลง ได้รับการดำเนินการแล้ว ตัวอย่างเช่น address ภายใน ไม่สามารถผ่านอินเทอร์เน็ตเข้ามาใน DMZ ได้ | โดยปรกติ packet ที่มี IP address ของคอมพิวเตอร์ซึ่งส่งมาจากคอมพิวเตอร์เครื่องอื่นในเครือข่ายจะรู้สถานที่ที่ packet ถูกส่งมา ผู้ประสงค์ร้ายมักจะพยายามปลอมแปลง (หรือ เลียนแบบ) IP address ที่ส่งไป เพื่อที่ระบบเป้าหมายจะได้เชื่อว่า packet นั้นมาจากแหล่งที่มาที่เชื่อถือได้<br>การกลั่นกรอง packets ที่เข้ามายังเครือข่าย ช่วยให้มั่นใจว่า packet นั้นๆ ไม่ได้ถูกปลอมแปลงให้เหมือนมาจากเครือข่ายภายในองค์กรเอง |
| 1.3.5 ไม่อนุญาตให้มีการส่งข้อมูล ออกจากเครือข่าย โดยไม่ได้รับอนุญาต จากสิ่งแวดล้อมข้อมูลผู้ถือบัตรไปยังอินเทอร์เน็ต | 1.3.5 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า การส่งข้อมูล ออกจาก เครือข่าย จากสิ่งแวดล้อมข้อมูลผู้ถือบัตร ไปยังอินเทอร์เน็ตนั้นได้รับการอนุญาตอย่างชัดเจน | การส่งข้อมูล ออกจาก เครือข่ายทั้งหมด จากสิ่งแวดล้อมข้อมูลผู้ถือบัตรควรได้รับการประเมินผล เพื่อให้มั่นใจว่าเป็นไปตามค่าที่จัดตั้งไว้และกฎการอนุญาต การเชื่อมต่อควรจะได้รับการตรวจสอบ เพื่อจำกัดให้เฉพาะการส่งข้อมูลที่ได้รับอนุญาตเท่านั้น (ตัวอย่างเช่น โดยการจำกัด address/port แหล่งที่มา/ปลายทาง และ/หรือ การปิดกั้น เนื้อหา) |
| 1.3.6 ดำเนินการตรวจสอบแบบ stateful หรือที่รู้จักกันในชื่อ dynamic packet filtering (ซึ่งก็คือ เฉพาะการเชื่อมต่อที่ได้รับการ “จัดตั้งขึ้นมา” ที่ได้รับอนุญาตให้เข้าสู่เครือข่ายได้) | 1.3.6 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า firewall ได้ทำการตรวจสอบแบบ stateful แล้วหรือไม่ (dynamic packet filtering) (เฉพาะการเชื่อมต่อที่ได้รับการ “จัดตั้งขึ้นมา” ที่ได้รับอนุญาตให้เข้าสู่เครือข่ายได้ และเฉพาะการเชื่อมต่อที่เกี่ยวข้องกับการจัดตั้งครั้งก่อนเท่านั้น) | firewall ซึ่งดำเนินการตรวจสอบ stateful packet เพื่อรักษาสถานะ (state หรือ status) สำหรับแต่ละการเชื่อมต่อผ่าน ด้วยการที่ firewall รักษา “state” ไว้ firewall จะรู้อย่างชัดเจนถึงการตอบสนองกับการเชื่อมต่อก่อนหน้านั้น การตอบสนองที่ได้รับอนุญาต (เนื่องจากมันรักษาสถานะของแต่ละการเชื่อมต่อ) หรือเป็นการส่งข้อมูล malicious ที่พยายามหลอกให้ firewall อนุญาตการเชื่อมต่อ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.3.7 จัดวางส่วนประกอบระบบซึ่งจัดเก็บข้อมูลผู้ถือบัตร (เช่น ฐานข้อมูล) ในบริเวณเครือข่ายภายใน แยกจากกันกับ DMZ และเครือข่ายที่ไม่ได้รับความไว้วางใจอื่นๆ | 1.3.7 ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า ส่วนประกอบระบบที่จัดเก็บข้อมูลผู้ถือบัตรอยู่ภายในบริเวณเครือข่ายภายใน แยกจากกันกับ DMZ และเครือข่ายที่ไม่ได้รับความไว้วางใจอื่นๆ | หากข้อมูลผู้ถือบัตร ถูกบรรจุไว้ภายใน DMZ มันจะง่ายกว่าสำหรับผู้โจมตีจากภายนอกที่จะเข้าถึงข้อมูลส่วนนี้ เนื่องจากมี layer จำนวนน้อยกว่าที่จะต้องทำการเจาะ ส่วนประกอบระบบรักษาความปลอดภัยซึ่ง จัดเก็บข้อมูลผู้ถือบัตรในบริเวณเครือข่ายภายในซึ่งแยกจากกันกับ DMZ และเครือข่ายที่ไม่ได้รับความไว้วางใจอื่นๆ โดย firewall สามารถป้องกันการส่งข้อมูลจากเครือข่ายที่ไม่ได้รับอนุญาตจากการเข้าถึงส่วนประกอบระบบได้<br><br>**หมายเหตุ**: ความต้องการนี้ไม่ได้มีจุดประสงค์เพื่อใช้กับ แหล่งจัดเก็บข้อมูลชั่วคราวของข้อมูลผู้ถือบัตร หรือ ข้อมูลใน volatile memory |
| 1.3.8 ไม่ทำการเปิดเผย IP addressesส่วนตัว และข้อมูล routing ให้กับผู้ที่ไม่ได้รับอนุญาต<br><br>**หมายเหตุ**: วิธีการปิดบัง *IP addressing* อาจระบุไว้ : (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้)<br>• การแปลที่อยู่ของเครือข่าย Network Address Translation (NAT)<br>• จัดวางเซิฟเวอร์ที่บรรจุข้อมูลผู้ถือบัตรไว้ภายใต้ proxy server/firewall<br>• ลบ หรือ กลั่นกรองเส้นทางโฆษณา สำหรับเครือข่ายส่วนตัวซึ่งมีที่อยู่ที่ลงทะเบียนไว้<br>• การใช้ที่อยู่ *RFC1918* ภายใน แทนที่ลงทะเบียนไว้ | 1.3.8.a ตรวจสอบการตั้งค่า firewall และ เราเตอร์ เพื่อตรวจให้แน่ใจว่า กระบวนการใช้งานได้ดี เพื่อป้องกันการแสดง IP address ส่วนตัว และข้อมูล routing ของเครือข่ายภายในจากอินเทอร์เน็ต<br><br>1.3.8.b ทำการสัมภาษณ์บุคลากรและตรวจสอบเอกสารเพื่อให้แน่ใจว่าการแสดงผล IP address ส่วนตัวใดๆก็ตามไปยัง หน่วยงาน (entity) ภายนอกนั้น ได้รับการอนุญาตแล้ว | การจำกัดการแสดงผล IP address ภายใน หรือส่วนตัวนั้นสำคัญเป็นอย่างมากเพื่อการป้องกันไม่ให้ hacker “รู้” IP address ของเครือข่ายภายใน และใช้ข้อมูลนั้นในการเข้าถึงเครือข่ายได้<br><br>กระบวนการต่างๆที่ใช้เพื่อความต้องการเหล่านี้อาจต่างกันออกไปขึ้นอยู่กับเทคโนโลยีเครือข่ายที่ใช้ ตัวอย่าง เช่น การควบคุมที่ต้องใช้เพื่อให้บรรลุความต้องการอาจต่างออกไปสำหรับ IPv4 network กับ IPv6 network |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 1.4 ติดตั้ง software firewall ส่วนตัวบน อุปกรเคลื่อนที่ใดๆก็ตาม และ/หรือ อุปกรณ์ของลูกจ้าง ซึ่งมีการเชื่อมต่ออินเทอร์เน็ตนอกระบบ (ตัวอย่าง เช่น แลปท็อปที่ใช้โดยลูกจ้าง) และสิ่งที่ใช้เพื่อเข้าถึงเครือข่าย การตั้งค่า Firewall มีดังนี้:<br>• กำหนดการตั้งค่าเฉพาะสำหรับ software firewall ส่วนตัว<br>• Software firewall ส่วนตัวมีการดำเนินการอย่างต่อเนื่อง<br>• Software firewall ส่วนตัว ไม่สามารถถูกเปลี่ยนแปลงได้โดย ผู้ใช้อุปกรณ์เคลื่อนที่ และ/หรือ อุปกรณ์ของลูกจ้าง | 1.4.a ตรวจสอบ นโยบาย และมาตรฐานการตั้งค่าเพื่อให้แน่ใจว่า:<br>• Software firewall ส่วนตัว นั้นจำเป็นสำหรับการใช้อุปกรณ์เคลื่อนที่ทั้งหมดในการเชื่อมต่ออินเทอร์เน็ต (ตัวอย่าง เช่น แลปท็อปที่ใช้โดยลูกจ้าง) เมื่ออยู่นอกเครือข่าย และอุปกรณ์ที่ใช้เพื่อเข้าถึงเครือข่าย<br>• กำหนดการตั้งค่าเฉพาะสำหรับ software firewall ส่วนตัว<br>• Software firewall ส่วนตัวมีการดำเนินการอย่างต่อเนื่อง<br>• Software firewall ส่วนตัว ไม่สามารถถูกเปลี่ยนแปลงได้โดย ผู้ใช้อุปกรณ์เคลื่อนที่ และ/หรือ อุปกรณ์ของลูกจ้าง<br><br>1.4.b ตรวจสอบตัวอย่างของอุปกรณ์เคลื่อนที่ และ/หรือ อุปกรณ์ของลูกจ้าง เพื่อตรวจให้แน่ใจว่า:<br>• Software firewall ส่วนตัว ได้รับการติดตั้งและตั้งค่าตามการตั้งค่าเฉพาะขององค์กร<br>• Software firewall ส่วนตัวมีการดำเนินการอย่างต่อเนื่อง<br>• Software firewall ส่วนตัว ไม่สามารถถูกเปลี่ยนแปลงได้โดย ผู้ใช้อุปกรณ์เคลื่อนที่ และ/หรือ อุปกรณ์ของลูกจ้าง | อุปกรณ์คอมพิวเตอร์พกพาซึ่งได้รับอนุญาตให้เชื่อมต่ออินเทอร์เน็ตจากภายนอก firewall ขององค์กร มีความเสี่ยงต่ออันตรายจากอินเทอร์เน็ตมากกว่า การใช้ firewall ส่วนตัว ช่วยปกป้องอุปกรณ์เหล่านั้นจากการโจมตีที่มีพื้นฐานมาจากอินเทอร์เน็ต ซึ่งอาจใช้อุปกรณ์เหล่านั้นในการเข้าถึงระบบและข้อมูลขององค์กรเมื่ออุปกรณ์นั้นๆกลับมาเชื่อมต่อที่เครือข่ายภายใน<br><br>การตั้งค่า firewall อย่างเฉพาะเจาะจงนั้นควรได้รับการพิจารณาจากองค์กร<br><br>หมายเหตุ: จุดประสงค์ของความต้องการนี้ ใช้เพื่ออุปกรณ์ของลูกจ้าง และอุปกรณ์คอมพิวเตอร์ขององค์กร ระบบที่ไม่สามารถจัดการได้โดยนโยบายองค์กร จะส่งผลเกิดความอ่อนแอและเปิดโอกาสให้ผู้ประสงค์ร้ายใช้ประโยชน์ได้ การเปิดโอกาสให้ระบบที่ไม่ได้รับความไว้วางใจเชื่อมต่อเข้ามาสู่เครือข่ายองค์กรอาจส่งผลให้การโจมตีและ ผู้ใช้งานที่ประสงค์ร้าย ได้รับอนุญาตให้กระทำการใดๆได้ |
| 1.5 ให้มั่นใจว่านโยบายความปลอดภัยและกระบวนการดำเนินการสำหรับจัดการ firewall ได้รับการจัดทำเป็นเอกสาร ได้ใช้งาน และเป็นที่รู้จักสำหรับผู้ที่เกี่ยวข้องทั้งหมด | 1.5 ตรวจสอบเอกสาร และทำการสัมภาษณ์บุคลากรเพื่อตรวจให้แน่ใจว่านโยบายความปลอดภัย และ กระบวนการดำเนินการเพื่อจัดการ firewall ได้มีการ:<br>• จัดทำเป็นเอกสาร<br>• ใช้งาน และ<br>• เป็นที่รู้จักของบุคคลที่มีผลกระทบทั้งหมด | บุคลากรจะต้องตระหนักนโยบายความปลอดภัยและกระบวนการดำเนินการเพื่อให้มั่นใจว่า firewall และ router ได้รับการจัดการอย่างต่อเนื่องเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตมาสู่เครือข่าย |

# ความต้องการที่ 2: ไม่ใช้การตั้งค่าแบบตั้งต้นจากผู้ขายสำหรับรหัสผ่าน และค่าความปลอดภัยอื่น ๆ

ผู้ประสงค์ร้าย (ภายนอก และ ภายในหน่วยงาน) มักใช้รหัสผ่านตั้งตนจากผู้ขาย และการตั้งค่าแบบตั้งต้นจากผู้ขายเพื่อการเจาะเข้าระบบ รหัสผ่านและการตั้งค่าเหล่านี้ เป็นที่รู้กันดีในกลุ่มสังคม hacker และถือว่าสามารถรู้ได้อย่างดายจากข้อมูลสาธารณะ

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 2.1 เปลี่ยนรหัสผ่านจากค่าตั้งต้นอยู่เสมอ และลบหรือปิดการใช้งานบัญชีตั้งต้น **ก่อน** ติดตั้งระบบเข้าสู่เครือข่าย<br><br>กระบวนการนี้นำไปใช้กับ รหัสผ่านตั้งต้น ทั้งหมด รวมไปถึงส่วนที่ใช้โดย ระบบปฏิบัติการ ซอฟแวร์ซึ่งให้บริการความปลอดภัย แอปพลิเคชั่น บัญชีระบบ ส่วน *point-of-sale (*POS*)* Simple Network Management Protocol (SNMP) community strings และ อื่นๆ(เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) | 2.1.a เลือกตัวอย่างหนึ่งของส่วนประกอบระบบ และพยายามล็อคอินเข้าสู่อุปกรณ์และแอปพลิเคชั่นโดยใช้ username และ รหัสผ่านตั้งต้นจากผู้ขาย (ด้วยการช่วยเหลือของผู้ดูแลระบบ) เพื่อตรวจให้แน่ใจว่า รหัสผ่านตั้งต้นทั้งหมด (รวมทั้งบนระบบปฏิบัติการ ซอฟแวร์ซึ่งให้บริการความปลอดภัย แอปพลิเคชั่น บัญชีระบบ ส่วน *point-of-sale (*POS*)* Simple Network Management Protocol (SNMP) community strings) ได้รับการเปลี่ยนแล้ว (ใช้คู่มือจากผู้ขาย และแหล่งข้อมูลบนอินเทอร์เน็ตเพื่อค้นหาชื่อบัญชี/รหัสผ่าน ที่เป็นส่วนสนับสนุนจากผู้ขาย) | ผู้ประสงค์ร้าย (ภายใน และ ภายนอกต่อองค์กร ) มักใช้การตั้งค่าแบบตั้งตนจากผู้ขาย ชื่อบัญชี และรหัสผ่านเพื่อการเจาะเข้า software ระบบปฏิบัติการ แอปพลิเคชั่น และระบบ ซึ่งได้รับการติดตั้ง เนื่องจากการตั้งค่าแบบตั้งต้นเหล่านี้มักได้รับการเผยแพร่ และเป็นที่รู้จักกันในกลุ่มสังคม hacker การเปลี่ยนการตั้งค่าแบบตั้งต้นเหล่านี้จะทำให้ระบบมีความเสี่ยงจากการถูกโจมตีน้อยลง<br><br>ถึงแม้ว่าบัญชีตั้งต้นจะไม่ได้มีไว้เพื่อจุดประสงค์ในการใช้งาน แต่การเปลี่ยนรหัสผ่านตั้งต้นให้เป็นรหัสผ่านที่ปลอดภัยและปิดการใช้งานบัญชีนั้นๆ ก็จะป้องกันผู้ประสงค์ร้ายจากการเปิดการใช้งานบัญชีเหล่านั้นขึ้นมาใหม่เพื่อเข้าถึงข้อมูลและระบบด้วยบัญชีเหล่านั้นได้ด้วยรหัสผ่านตั้งต้น |
| | 2.1.b สำหรับตัวอย่างของส่วนประกอบระบบ ตรวจให้แน่ใจว่า บัญชีตั้งต้นที่ไม่จำเป็นต่อการใช้งานได้ถูกลบ หรือ ปิดการใช้งานไปแล้ว (รวมไปถึงส่วนที่ใช้โดย ระบบปฏิบัติการ ซอฟแวร์ซึ่งให้บริการความปลอดภัย แอปพลิเคชั่น ระบบ ส่วน *point-of-sale (*POS*)* Simple Network Management Protocol (SNMP) community strings และ อื่นๆ) | |
| | 2.1.c สัมภาษณ์บุคลากร และตรวจสอบเอกสารการสนับสนุนเพื่อตรวจให้แน่ใจว่า:<br>• ค่าตั้งต้นจากผู้ขายได้รับการเปลี่ยนแล้ว ก่อนที่ระบบจะถูกติดตั้งลงบนเครือข่าย (รวมไปถึง รหัสผ่านตั้งต้นของระบบปฏิบัติการซอฟแวร์ซึ่งให้บริการความปลอดภัย แอปพลิเคชั่น บัญชีระบบ ส่วน *point-of-sale (*POS*)* Simple Network Management Protocol (SNMP) community strings และ อื่นๆ)<br>• บัญชีตั้งต้นที่ไม่จำเป็นได้รับการลบ หรือ ปิดการใช้งานก่อนที่ระบบจะถูกติดตั้งลงบนเครือข่าย (รวมไปถึงส่วนที่ใช้โดย ระบบปฏิบัติการ ซอฟแวร์ซึ่งให้บริการความปลอดภัย แอปพลิเคชั่น ระบบ ส่วน *point-of-sale (*POS*)* Simple Network Management Protocol (SNMP) community strings และ อื่นๆ) | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 2.1.1 สำหรับสิ่งแวดล้อมไร้สายซึ่งเชื่อมต่อไปยังสิ่งแวดล้อมข้อมูลผู้ถือบัตร หรือ ส่งเปลี่ยนข้อมูลผู้ถือบัตร ให้เปลี่ยนการตั้งค่าแบบตั้งต้นจากผู้ขายทั้งหมดในระหว่างการติดตั้ง รวมไปถึงการเข้ารหัส wireless ตั้งต้น รหัสผ่าน และ SNMP community string (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) | 2.1.1.a สัมภาษณ์บุคลากรที่รับผิดชอบ และตรวจสอบเอกสารการสนับสนุนเพื่อตรวจให้แน่ใจว่า:<br>• การเข้ารหัสได้รับการเปลี่ยนแปลงจากค่าตั้งต้นเมื่อติดตั้ง<br>• คีย์การเข้ารหัส ได้รับการเปลี่ยนแปลงเมื่อผู้ใดก็ตามที่มีความรู้ในคีย์เหล่านี้ออกจากองค์กร หรือ เปลี่ยนตำแหน่ง | หากเครือข่ายไร้สายไม่ได้ดำเนินการตามการตั้งค่าความปลอดภัยที่เพียงพอ (รวมไปถึงการเปลี่ยนแปลงการตั้งค่าแบบตั้งต้น) wireless sniffer สามารถ ดักฟัง การส่งข้อมูล จับข้อมูล และรหัสผ่านอย่างง่ายดาย และเข้าสู่ระบบและทำการโจมตีได้อย่างไม่ยากเย็น<br>อีกทั้ง Protocol แลกเปลี่ยนคีย์ สำหรับเวอร์ชั่นที่เก่ากว่าของการเข้ารหัส 802.11x (นโยบายการเข้ารหัสเทียบเท่าเทคโนโลยีมีสาย Wired Equivalent Privacy หรือ WEP) ถูกทำลาย และความสามารถการ render เข้ารหัสได้นั้นไม่มีประโยชน์ Firmware สำหรับอุปกรณ์ควรได้รับการอัพเดท เพื่อให้สนับสนุน protocol ที่ปลอดภัยมากขึ้น |
| | 2.1.1.b สัมภาษณ์บุคลากร และตรวจสอบนโยบายและกระบวนการต่างๆเพื่อให้แน่ใจว่า:<br>• SNMP community string ตั้งต้น จะต้องถูกเปลี่ยนตั้งแต่การติดตั้ง<br>• รหัสผ่าน/รหัสผ่าน Passphrases ตั้งต้น ใน access point จะต้องถูกเปลี่ยนแปลงเมื่อติดตั้ง | |
| | 2.1.1.c ตรวจสอบเอกสารจากผู้ขายและล็อคอินอุปกรณ์ไร้สาย (ด้วยความช่วยเหลือจากผู้ดูแลระบบ) เพื่อให้มั่นใจว่า:<br>• ต้องไม่ใช้งาน SNMP community string ตั้งต้น<br>• ต้องไม่ใช้งาน รหัสผ่าน/passphrase ตั้งต้น ใน access point | |
| | 2.1.1.d ตรวจสอบเอกสารจากผู้ขาย และสังเกตการณ์ตั้งค่า wireless เพื่อตรวจสอบให้แน่ใจว่า firmware ในอุปกรณ์ไร้สาย ได้รับการอัพเดทเพื่อให้เข้ารหัสได้ปลอดภัยมากขึ้นเพื่อ:<br>• การรับรองความปลอดภัย บนเครือข่ายไร้สาย<br>• การส่งผ่านข้อมูล บนเครือข่ายไร้สาย | |
| | 2.1.1.e ตรวจสอบเอกสารของผู้ขาย และสังเกตการตั้งค่า wireless เพื่อให้แน่ใจว่าค่าตั้งต้นที่เกี่ยวข้องกับความปลอดภัยอื่นๆจากผู้ขายได้รับการเปลี่ยนแปลงแล้วหากทำได้ | |

| ความต้องการ **PCI DSS** | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 2.2 พัฒนามาตรฐานการตั้งค่าสำหรับส่วนประกอบระบบทั้งหมด ทำให้มั่นใจว่ามาตรฐานเหล่านี้ได้แสดงให้เห็นจุดอ่อนที่รู้ทั้งหมด และตรงกับมาตรฐานการป้องกันระบบในระดับอุตสาหกรรม<br><br>แหล่งข้อมูลมาตรฐานการป้องกันระบบในระดับอุตสาหกรรมนั้นรวมไปถึง: (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้)<br><br>• ศูนย์กลางความปลอดภัยอินเทอร์เน็ต หรือ Center for Internet Security (CIS)<br>• การรับรองมาตรฐานขององค์กรระดับสากล หรือ International Organization for Standardization (ISO)<br>• สถาบันความปลอดภัยเครือข่ายผู้ตรวจสอบผู้ดูแลระบบ หรือ SysAdmin Audit Network Security (SANS) Institute<br>• สถาบันมาตรฐานเทคโนโลยีแห่งชาติ หรือ National Institute of Standards Technology (NIST) | 2.2.a ตรวจสอบมาตรฐานการตั้งค่าระบบขององค์กรสำหรับส่วนประกอบระบบทุกประเภท และตรวจสอบว่ามาตรฐานการตั้งค่าระบบตรงกับกับมาตรฐานการป้องกันระบบในระดับอุตสาหกรรม<br><br>2.2.b ตรวจสอบนโยบายและสัมภาษณ์บุคลากรเพื่อตรวจให้แน่ใจว่ามาตรฐานการตั้งค่าระบบได้รับการอัพเดทที่ได้ตรวจสอบและระบุแล้วซึ่งจุดอ่อนใหม่ๆที่เกิดขึ้นอย่างที่อยู่ในความต้องการที่ 6.1<br><br>2.2.c ตรวจสอบนโยบาย และสัมภาษณ์บุคลากรเพื่อตรวจให้แน่ใจว่ามาตรฐานการตั้งค่าระบบได้รับการใช้งานและใช้งานได้ผลดีเมื่อระบบใหม่ถูกตั้งค่า ก่อนที่ระบบจะติดตั้งลงบนเครือข่าย<br><br>2.2.d ตรวจให้แน่ใจว่ามาตรฐานการตั้งค่าระบบมีกระบวนการดังต่อไปนี้สำหรับส่วนประกอบระบบทุกประเภท:<br><br>• เปลี่ยนค่าตั้งต้นที่เป็นส่วนสนับสนุนจากผู้ขาย และลบบัญชีตั้งต้นที่ไม่จำเป็นออก<br>• ดำเนินการเฉพาะฟังก์ชั่นหลัก ในแต่ละเซิฟเวอร์เพื่อป้องกันไม่ให้ฟังก์ชั่นที่ต้องการระดับความปลอดภัยคนละระดับอยู่ในเซิฟเวอร์เดียวกัน<br>• เปิดใช้งานเฉพาะ service, protocol, daemon และ อื่นๆ ที่จำเป็น ซึ่งฟังก์ชั่นของระบบต้องการใช้งานเท่านั้น<br>• ดำเนินการ features ความปลอดภัยเพิ่มเติมสำหรับ service, protocol หรือ daemon ที่ต้องการซึ่งได้รับการพิจารณาว่าไม่ปลอดภัย<br>• ตั้งค่าความปลอดภัยระบบ เพื่อป้องกัน การใช้งานในทางที่ผิด<br>• ลบฟังก์ชั่นที่ไม่จำเป็นทั้งหมด เช่น script, driver, feature, subsystem ไฟล์ระบบ และ เว็บเซิฟเวอร์ที่ไม่จำเป็น | ระบบปฏิบัติการ ฐานข้อมูล แอปพลิเคชั่นสำหรับองค์กร จำนวนมากมีจุดอ่อนที่รับทราบแล้ว และมีการตั้งค่าที่มีไว้เพื่อแก้ไขจุดบกพร่องนั้นๆเช่นกัน เพื่อช่วยผู้ที่ไม่เชี่ยวชาญในด้านความปลอดภัย องค์กรความปลอดภัยจำนวนมากได้จัดตั้ง แนวทางการเสริมการป้องกันระบบ และข้อแนะนำ ซึ่งแนะนำวิธีการกำจัดจุดบกพร่องเหล้านั้น<br><br>ตัวอย่างแหล่งข้อมูลที่เป็นแนวทางมาตรฐานการตั้งค่าได้แก่: www.nist.gov, www.sans.org, และ www.cisecurity.org, www.iso.org, และจากผู้ขายต่างๆ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้)<br><br>มาตรฐานการตั้งค่าระบบจะต้องมีการอัพเดทเสมอเพื่อให้ทราบถึงจุดบกพร่องใหม่ๆและแก้ไขปรับปรุงระบบที่ติดตั้งบนเครือข่ายแล้วเช่นกัน |

| ความต้องการ **PCI DSS** | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 2.2.1 ดำเนินการเฉพาะฟังก์ชั่นหลัก ในแต่ละเซิฟเวอร์เพื่อป้องกันไม่ให้ฟังก์ชั่นที่ต้องการระดับความปลอดภัยคนละระดับอยู่ในเซิฟเวอร์เดียวกัน (ตัวอย่าง เช่น เว็บเซิฟเวอร์ เซิฟเวอร์ ฐานข้อมูล และ DNS ควรดำเนินการบนเซิฟเวอร์ที่แยกจากกัน)<br><br>หมายเหตุ: หากส่วนใดมีการใช้เทคโนโลยีการจำลองให้ดำเนินการเฉพาะฟังก์ชั่นหลักหนึ่งเดียว สำหรับแต่ละส่วนประกอบระบบจำลอง | 2.2.1.a เลือกตัวอย่างส่วนประกอบระบบ และตรวจสอบการตั้งค่าระบบเพื่อตรวจให้แน่ใจว่ามีการดำเนินการเพียงฟังก์ชั่นหลักหนึ่งเดียวในแต่ละเซิฟเวอร์หรือไม่<br><br>2.2.1.b หากส่วนใดมีการใช้เทคโนโลยีการจำลอง ตรวจสอบการตั้งค่าระบบเพื่อให้แน่ใจว่ามีการดำเนินการเฉพาะฟังก์ชั่นหลักหนึ่งเดียว สำหรับแต่ละส่วนประกอบระบบ หรือ อุปกรณ์จำลอง | หากฟังก์ชั่นต่างๆในเซิฟเวอร์ต้องการระดับความปลอดภัยคนละระดับ ตั้งอยู่ในเซิฟเวอร์เดียวกัน ระดับความปลอดภัยของฟังก์ชั่นที่ต้องการความปลอดภัยสูงกว่าจะถูกลดระดับให้ใช้งานความปลอดภัยที่ต่ำกว่า อีกทั้งฟังก์ชั่นของเซิฟเวอร์ที่ต้องการความปลอดภัยต่ำกว่า อาจสร้างจุดอ่อนให้กับฟังก์ชั่นอื่นๆในเซิฟเวอร์เดียวกันได้ หากพิจารณาจากความต้องการความปลอดภัยของฟังก์ชั่นเซิฟเวอร์แต่ละตัวในฐานะส่วนหนึ่งของมาตรฐานการตั้งค่าระบบ และกระบวนการที่เกี่ยวข้อง องค์กรสามารถทำให้แน่ใจได้ว่าฟังก์ชั่นที่ต้องการระดับความปลอดภัยคนละระดับอยู่ในเซิฟเวอร์ที่แยกจากกัน |
| 2.2.2 เปิดใช้งานเฉพาะ service, protocol daemons และอื่นๆ ที่จำเป็นที่ฟังก์ชั่นของระบบต้องใช้งาน | 2.2.2.a เลือกตัวอย่างหนึ่งของส่วนประกอบระบบ และตรวจสอบว่ามีการเปิดใช้งาน system, service, daemon และ protocol เพื่อให้แน่ใจว่าเฉพาะ service หรือ protocol ที่จำเป็นเท่านั้นที่ได้เปิดใช้งาน<br><br>2.2.2.b ตรวจสอบและระบุ service daemon หรือ protocol ใดๆก็ตามที่ไม่ปลอดภัย และสัมภาษณ์บุคลากรเพื่อให้แน่ใจว่าสิ่งเหล้านั้นได้รับการแสดงผลตามเอกสารมาตรฐานการตั้งค่า | ดังที่กล่าวไว้ใน ความต้องการที่ 1.1.6 มี protocol จำนวนมากซึ่งธุรกิจอาจต้องการใช้ (หรือ เปิดใช้งานโดยค่าตั้งต้น) ซึ่งมักถูกใช้โดยผู้ประสงค์ร้ายเพื่อเจาะเข้าระบบ รวมไปถึงความต้องการนี้ในฐานะส่วนของมาตรฐานการตั้งค่าองค์กร และกระบวนกรอื่นๆเพื่อให้มั่นใจว่าเฉพาะ service และ protocol ที่จำเป็นเท่านั้นที่ได้รับการเปิดใช้งาน |
| 2.2.3 ดำเนินการ feature ความปลอดภัยเพิ่มเติมสำหรับ service, protocol หรือ daemon ที่ต้องการ ซึ่งได้รับการพิจารณาว่าไม่ปลอดภัย — ตัวอย่างเช่น ใช้เทคโนโลยีที่ปลอดภัย อย่าง SSH, S-FTP, SSL, หรือ IPSec VPN เพื่อปกป้อง service ที่ไม่ปลอดภัย อย่าง NetBIOS, file-sharing, Telnet, FTP, และอื่นๆ | 2.2.3 ตรวจสอบการตั้งค่าเพื่อให้แน่ใจว่า feature ความปลอดภัยได้รับการจัดทำเป็นเอกสาร และปฏิบัติตาม สำหรับ service, daemon, หรือ protocol ที่ไม่ปลอดภัยทั้งหมด | การเปิดใช้งาน feature ความปลอดภัย ก่อนการเปิดเซิฟเวอร์ใหม่ ป้องกันไม่ให้เซิฟเวอร์ถูกติดตั้งลงไปในสิ่งแวดล้อมที่มีการตั้งค่าที่ไม่ปลอดภัย<br><br>ให้มั่นใจว่า service protocol และ daemon ที่ไม่ปลอดภัยนั้นได้รับความปลอดภัยที่เพียงพอด้วยฟังก์ชั่นความปลอดภัยที่เหมาะสม ทำให้ยากสำหรับผู้ประสงค์ร้ายยิ่งขึ้นในการใช้ประโยชน์จากจุดที่มักถูกใช้เจาะเข้าเครือข่าย |
| 2.2.4 ตั้งค่าความปลอดภัยของระบบเพื่อป้องกันการใช้งานในทางที่ผิด | 2.2.4.a สัมภาษณ์ผู้ดูแลระบบ และ/หรือผู้จัดการเพื่อให้แน่ใจว่าพวกเขามีความรู้พื้นฐานในการตั้งค่าความปลอดภัยขั้นต้นสำหรับส่วนประกอบระบบ<br><br>2.2.4.b ตรวจสอบมาตรฐานการตั้งค่าระบบเพื่อให้แน่ใจว่าการตั้งค่าความปลอดภัยขึ้นต้นได้ถูกนำไปใช้ | มาตรฐานการตั้งค่าระบบ และกระบวนการอื่นๆควรแสดงให้เห็นถึงการตั้งค่าความปลอดภัยเฉพาะและค่าซึ่งรู้กันว่าเป็นการดำเนินการด้านความปลอดภัยสำหรับแต่ละประเภทระบบที่ใช้ |

(มีต่อหน้าถัดไป)

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| | 2.2.4.c เลือกตัวอย่างหนึ่งของส่วนประกอบระบบ และตรวจสอบค่าความปลอดภัยขั้นต้นเพื่อให้แน่ใจว่าสิ่งเหล่านั้นได้มีการตั้งค่าไว้อย่างเหมาะสม และเป็นไปตามมาตรฐานการตั้งค่า | ในการตั้งค่าระบบอย่างปลอดภัย บุคลากรที่รับผิดชอบการตั้งค่าและ/หรือ ผู้ดูแลระบบ จะต้องมีความรู้ในค่าความปลอดภัยเฉพาะและการตั้งค่าซึ่งใช้งานกับระบบ |
| 2.2.5 ลบฟังก์ชั่นที่ไม่จำเป็นทั้งหมด เช่น script, driver, feature, subsystem, file system และเว็บเซิฟเวอร์ที่ไม่จำเป็นทั้งหมด | 2.2.5.a เลือกตัวอย่างหนึ่งของส่วนประกอบระบบ และตรวจสอบการตั้งค่าเพื่อตรวจให้แน่ใจว่าฟังก์ชั่นที่ไม่จำเป็นทั้งหมดได้ถูกลบออกแล้ว (ตัวอย่าง เช่น script, driver, feature, subsystem, file system และอื่นๆ)<br>2.2.5.b. ตรวจสอบการจัดทำเอกสารและค่าความปลอดภัยเพื่อให้แน่ใจว่าฟังก์ชั่นที่เปิดใช้งานได้รับการจัดทำเป็นเอกสารและสนับสนุนการตั้งค่าความปลอดภัย<br>2.2.5.c. ตรวจสอบการจัดทำเอกสารและค่าความปลอดภัยเพื่อให้แน่ใจว่าเฉพาะฟังก์ชั่นที่บันทึกไว้เท่านั้นที่ปรากฏอยู่ในตัวอย่างส่วนประกอบระบบ | ฟังก์ชั่นที่ไม่จำเป็นสามารถทำให้เกิดโอกาสเพิ่มเติมสำหรับผู้ประสงค์ร้ายในการเข้าถึงระบบได้ ด้วยการลบฟังก์ชั่นที่ไม่จำเป็น องค์กรสามารถมุ่งไปที่การสร้างความปลอดภัยไปที่ฟังก์ชั่นที่จำเป็นต่อการใช้งาน และลดความเสี่ยงจากการที่ฟังก์ชั่นที่ไม่รู้จักจะถูกนำไปใช้ประโยชน์ได้<br>อีกทั้ง นี่คือมาตรฐานการเสริมการป้องกันเซิฟเวอร์ และกระบวนการชี้การปฏิบัติตามความปลอดภัยเฉพาะพร้อมทั้งฟังก์ชั่นที่ไม่จำเป็น<br>(ตัวอย่าง เช่น โดยการ ลบ/ปิดการใช้งาน FTP หรือเว็บเซิฟเวอร์หากเซิฟเวอร์นั้นๆไม่ได้มีการใช้งาน) |
| 2.3 เข้ารหัสการเข้าถึงของผู้ดูแลระบบแบบ non-console ด้วย การอ่านรหัสลับ (cryptography) ที่เข้มงวด ใช้เทคโนโลยี อย่างเช่น SSH, VPN, or SSL/TLS สำหรับการจัดการในลักษณะ web-based และการเข้าถึงระดับผู้ดูแลระบบแบบ non-console | 2.3 เลือก ตัวอย่างหนึ่งของส่วนประกอบระบบ และเพื่อให้แน่ใจว่า การเข้าถึงของผู้ดูแลระบบแบบ non- console ได้รับการเข้ารหัสด้วยกระบวนการต่อไปนี้:<br>2.3.a สังเกตการเข้าสู่ระบบของผู้ดูแลระบบไปยังแต่ละระบบ และตรวจสอบ การตั้งค่าระบบเพื่อให้แน่ใจว่าวิธีการเข้ารหัสที่ปลอดภัยถูกนำมาใช้ก่อนมีการขอรหัสผ่านผู้ดูแลระบบ<br>2.3.b ตรวจสอบ services และไฟล์ค่าตัวแปรบนระบบเพื่อพิจารณาว่า Telnet และคำสั่งการล็อคอินระยะไกลที่ไม่ปลอดภัยอื่นๆไม่สามารถใช้ได้ด้วยการเข้าถึงแบบ non-console<br>2.3.c สังเกตการเข้าสู่ระบบของผู้ดูแลระบบไปยังแต่ละระบบเพื่อให้แน่ใจว่า การเข้าถึงของผู้ดูแลไปยังหน้าจอการใช้งานการจัดการในลักษณะ web-based ได้รับการเข้ารหัสด้วย strong cryptography<br>2.3.d ตรวจสอบเอกสารของผู้ขาย และสัมภาษณ์บุคลากร เพื่อให้แน่ใจว่า ได้มีการใช้ strong cryptography ในเทคโนโลยีที่ใช้อยู่ และดำเนินการตามวิธีการที่ดีที่สุด และ/หรือ ตามคำแนะนำจากผู้ขาย | หากการจัดการระบบแบบ non-console (รวมถึง การควบคุมระยะไกล) ไม่ใช้การรับรองและเข้ารหัสการสื่อสาร สิทธิการดูแลระบบที่สุ่มเสี่ยง หรือ ข้อมูลระดับปฏิบัติการ (เช่น ID ผู้ดูแลระบบ และรหัสผ่าน) สามารถถูกเปิดเผยต่อผู้ดักฟังได้ ผู้ประสงค์ร้ายสามารถใช้ข้อมูลเหล่านี้เข้าถึงเครือข่าย เข้าเป็นผู้ดูแลระบบ และขโมยข้อมูลได้<br>Clear-text protocols (เช่น HTTP, telnet, และอื่นๆ) ไม่ได้เข้ารหัสการส่งข้อมูล หรือ รายละเอียดการ logon ซึ่งทำให้ง่ายต่อการดักจับ เพื่อสกัดกั้นข้อมูลเหล่านี้<br>ควรพิจารณา “การอ่านรหัสลับ หรือ cryptography” industry-recognized protocols พร้อมทั้ง ความรัดกุมของ key ที่เหมาะสมและการจัดการkey ควรจะมีประสิทธิภาพเพียงพอสำหรับเทคโนโลยีที่ใช้ (โปรดดู "strong cryptography (การอ่านรหัสลับที่เข้มงวด)" ในอภิธานศัพท์ ตัวย่อ และ คำย่อของ *PCI DSS* และ *PA-DSS*) |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 2.4 บำรุงรักษารายการอุปกรณ์ส่วนประกอบระบบซึ่งอยู่ภายใต้ PCI DSS | 2.4.a ตรวจสอบรายการอุปกรณ์ระบบเพื่อให้แน่ใจว่ารายการส่วนประกอบ hardware และsoftware ได้รับการบำรุงดูแล และรวมไปถึง รายละเอียดฟังก์ชั่น/การใช้งานของแต่ละส่วน<br><br>2.4.b สัมภาษณ์บุคลากร เพื่อให้แน่ใจว่าเอกสารรายการอุปกรณ์ได้รับการอัพเดทให้เป็นปัจจุบัน | การบำรุงรักษารายการปัจจุบันของส่วนประกอบระบบทั้งหมดจะทำให้องค์กรสามารถระบุขอบเขตของสิ่งแวดล้อมสำหรับการปฏิบัติตามการควบคุม PCI DSS ได้อย่างแม่นยำ และมีประสิทธิภาพ หากปราศจากรายการอุปกรณ์ ส่วนประกอบระบบบางส่วนอาจถูกลืม และอาจไม่ได้รับการตั้งค่าตามมาตรฐานองค์กรด้วยความไม่ตั้งใจได้ |
| 2.5 ทำให้มั่นใจว่านโยบายความปลอดภัย และกระบวนการดำเนินการสำหรับจัดการค่าตั้งต้นผู้ขาย และค่าความปลอดภัยอื่นๆได้รับการจัดทำเป็นเอกสาร ได้ใช้งาน และเป็นที่รู้จักสำหรับผู้ที่เกี่ยวข้องทั้งหมด | 2.5 ตรวจสอบการจัดทำเอกสารและสัมภาษณ์บุคลากร เพื่อให้แน่ใจว่านโยบายความปลอดภัยและกระบวนการดำเนินการสำหรับจัดการค่าตั้งต้นจากผู้ขาย และค่าความปลอดภัยอื่นๆนั้น:<br>• ได้รับการจัดทำเป็นเอกสาร<br>• ได้ใช้งาน และ<br>• เป็นที่รู้จักสำหรับผู้ที่เกี่ยวข้องทั้งหมด | บุคลากรต้องตระหนักและปฏิบัติตามนโยบายความปลอดภัยและกระบวนการดำเนินการประจำวัน เพื่อให้มั่นใจว่าค่าตั้งต้นจากผู้ขายและค่าความปลอดภัยอื่นๆได้รับการจัดการอย่างต่อเนื่องเพื่อป้องกันการตั้งค่าที่ไม่ปลอดภัย |
| 2.6 ผู้ให้บริการ Shared hosting จะต้องปกป้องแต่ละสิ่งแวดล้อม และข้อมูลผู้ถือบัตรของบุคคลที่ทำการให้บริการ host ผู้ให้บริการเหล่านี้จะต้องบรรลุความต้องการเฉพาะที่ระบุไว้ใน *ภาคผนวก A: ความต้องการ PCI DSS เพิ่มเติม สำหรับผู้ให้บริการ Shared Hosting* | 2.6 ดำเนินการตามกระบวนการทดสอบ A.1.1 ถึง A.1.4 ที่อธิบายไว้ใน *ภาคผนวก A: ความต้องการ PCI DSS เพิ่มเติมสำหรับผู้ให้บริการ Shared hosting* สำหรับการประเมิน PCI DSS ของ ผู้ให้บริการ Shard hosting เพื่อความแน่ใจว่าผู้ให้บริการได้ปกป้องข้อมูลและสิ่งแวดล้อมของลูกค้าของพวกเขา (ผู้ค้า และผู้ให้บริการ) | จุดประสงค์ของกระบวนการเหล่านี้มีไว้สำหรับ ผู้ให้บริการ hosting ซึ่งทำการ host สิ่งแวดล้อมแบบแบ่งปันกับ client จำนวนมากบนเซิฟเวอร์เดียวกัน เมื่อข้อมูลทั้งหมดอยู่บนเซิฟเวอร์เดียวกัน และอยู่ภายใต้การควบคุมของสิ่งแวดล้อมเดียว บ่อยครั้งที่การตั้งค่าของ server แชร์ เหล่านี้มักไม่สามารถจัดการได้โดย client แต่ละคน ซึ่งเป็นสาเหตุให้ client สามารถเพิ่มฟังก์ชั่นที่ไม่ปลอดภัย และscript ซึ่งอาจกระทบต่อความปลอดภัยของสิ่งแวดล้อมของ client คนอื่นๆทั้งหมดได้; ดังนั้น จึงเป็นการง่ายต่อผู้ประสงค์ร้ายที่จะเจาะเข้าสู่ข้อมูล client หนึ่งคน และได้รับการเข้าถึงข้อมูล client อื่นๆทั้งหมด โปรดดู *ภาคผนวก A* สำหรับรายละเอียดความต้องการ |

# ปกป้องข้อมูลผู้ถือบัตร

**ความต้องการที่ *3:* ปกป้องข้อมูลผู้ถือบัตรที่จัดเก็บไว้**

วิธีการปกป้องข้อมูล เช่นการเข้ารหัส, การตัดคำ (truncation), การบดบัง (masking), และ การเข้ารหัสทางเดียว (hashing) คือส่วนประกอบสำคัญของการป้องกันข้อมูลผู้ถือบัตร หากผู้บุกรุกหลอกการควบคุมความปลอดภัยอื่นๆ และได้รับสิทธิการเข้าถึงข้อมูลที่เข้ารหัส แต่ไม่มี คีย์การอ่านรหัสลับ (cryptographic keys) ที่เหมาะสม จะไม่สามารถอ่านข้อมูลและไม่สามารถนำไปใช้ประโยชน์ได้ ควรมีการพิจารณาถึงวิธีการอื่นๆในการปกป้องข้อมูลที่จัดเก็บไว้อย่างมีประสิทธิภาพ เพราะจะช่วยลดโอกาสในการเกิดความเสี่ยงได้ ตัวอย่าง เช่น วิธีการลดความเสี่ยงให้เหลือน้อยที่สุดโดยการไม่จัดเก็บข้อมูลผู้ถือบัตรหากไม่จำเป็นจริงๆ ตัดทอน (truncating) ข้อมูลผู้ถือบัตรหากไม่จำเป็นต้องใช้งาน PAN ทั้งหมด และไม่ส่ง PANs ที่ไม่ได้รับการป้องกันไปยังผู้ใช้ปลายทางด้วยเทคโนโลยีการส่งข้อความ เช่น email และ instant messaging (ระบบส่งข้อความทันที)

โปรดดู อภิธานศัพท์ ตัวย่อ และ คำย่อ ของ *PCI DSS* และ *PA-DSS* สำหรับความหมายของ “strong cryptography (การอ่านรหัสลับที่เข้มงวด)” และ อภิธานศัพท์อื่นๆของ PCI DSS

| ความต้องการ PCI DSS | กระบวนการทดสอบ | แนวทาง |
|---|---|---|
| 3.1 ลดการจัดเก็บข้อมูลผู้ถือบัตรไว้ให้น้อยที่สุด โดยปฏิบัติตามนโยบาย ขั้นตอน และกระบวนการการจัดเก็บและการจัดการข้อมูล ซึ่งรวมไปถึง การจัดเก็บข้อมูลผู้ถือบัตร (CHD) ดังนี้เป็นอย่างน้อย:<br>• จำกัดจำนวนการจัดเก็บข้อมูลและระยะเวลาการเก็บตามกฎหมาย ระเบียบ และความต้องการทางธุรกิจ<br>• ดำเนินการลบข้อมูลอย่างปลอดภัย เมื่อไม่ได้ใช้งานแล้ว<br>• กำหนดการจัดเก็บเฉพาะสำหรับข้อมูลผู้ถือบัตรแต่ละส่วน<br>• ตรวจหา และลบข้อมูลผู้ถือบัตรซึ่งเกินการจัดเก็บที่กำหนดไว้ทุกๆไตรมาส | 3.1.a ตรวจสอบนโยบาย ขั้นตอน และกระบวนการการจัดเก็บและการจัดการข้อมูล เพื่อให้มั่นใจมีสิ่งดังต่อไปนี้เป็นอย่างน้อย:<br>• กฎหมาย ระเบียบ และความต้องการทางธุรกิจสำหรับการจัดเก็บข้อมูลดังนี้<br>• มีความต้องการเฉพาะสำหรับข้อมูลผู้ถือบัตร (ตัวอย่างเช่น จะต้องจัดเก็บข้อมูลผู้ถือบัตรอย่างน้อยเป็นเวลา X สำหรับเหตุผล Y ทางธุรกิจ)<br>• ดำเนินการลบข้อมูลอย่างปลอดภัยเมื่อไม่ได้ใช้งานแล้ว ตามกฎหมาย ระเบียบ และความต้องการทางธุรกิจ<br>• ครอบคลุมการจัดเก็บข้อมูลผู้ถือบัตรทั้งหมด<br>• ตรวจหา และลบข้อมูลผู้ถือบัตรซึ่งเกินการจัดเก็บที่กำหนดไว้ทุกๆไตรมาส<br><br>3.1.b สัมภาษณ์บุคลากรเพื่อให้แน่ใจว่า:<br>• สถานที่จัดเก็บข้อมูลผู้ถือบัตรทั้งหมดได้รวมอยู่ในกระบวนการจัดเก็บและจัดการข้อมูลแล้ว<br>• มีการดำเนินการลบข้อมูลอย่างปลอดภัยเมื่อไม่ได้ใช้งานแล้วไม่ว่าด้วยกระบวนการอัตโนมัติหรือด้วยตนเอง<br>• กระบวนการอัตโนมัติหรือด้วยตนเองที่ใช้จะต้องใช้สำหรับข้อมูลผู้ถือบัตรทุกๆที่ที่จัดเก็บไว้ | นโยบายการจัดเก็บข้อมูลอย่างเป็นทางการระบุว่าข้อมูลส่วนใดจะถูกจัดเก็บไว้ และที่ใดที่นำไปจัดเก็บ เพื่อที่จะได้สามารถทำลายหรือ ลบอย่างปลอดภัย เมื่อสิ้นสุดความต้องการในการใช้งาน<br><br>ส่วนของข้อมูลผู้ถือบัตรที่จะต้องจัดเก็บไว้หลังการอนุญาตคือ หมายเลขบัญชีหลัก หรือ PAN (rendered unreadable) วันหมดอายุ ชื่อผู้ถือบัตร และหมายเลขบริการ<br><br>การเข้าใจว่าข้อมูลผู้ถือบัตรถูกจัดเก็บไว้ที่ใดเป็นสิ่งจำเป็น เพื่อที่มันจะสามารถถูกจัดเก็บ หรือจัดการได้เมื่อไม่มีความต้องการใช้งาน เพื่อกำหนดความต้องการในการจัดเก็บที่เหมาะสม หน่วยงาน (entity) จะต้องเข้าใจความต้องการในธุรกิจของตนเองก่อน พร้อมทั้งกฎหมาย ระเบียบ ข้อควรปฏิบัติ ซึ่งใช้กับอุตสาหกรรม และ/หรือ ใช้กับประเภทข้อมูลที่จัดเก็บ<br><br>(มีต่อหน้าถัดไป) |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 3.1.c **ตัวอย่างส่วนประกอบระบบซึ่งจัดเก็บข้อมูลผู้ถือบัตร**:<br>• ตรวจสอบไฟล์และบันทึกระบบ เพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บไว้ไม่เกินความต้องการที่กำหนดไว้ของนโยบายการจัดเก็บข้อมูล<br>• สังเกตกลไกการลบข้อมูล เพื่อให้แน่ใจว่ามีการลบอย่างปลอดภัย | การระบุ และลบข้อมูลที่จัดเก็บไว้ซึ่งเกินระยะเวลาเฉพาะในการจัดเก็บข้อมูลไว้ ช่วยป้องกันการจัดเก็บข้อมูลที่ไม่จำเป็นซึ่งไม่ได้นำมาใช้งานแล้ว กระบวนการนี้อาจทำโดยอัตโนมัติ ด้วยตนเอง หรือ ทั้งสองแบบก็ได้ ตัวอย่างเช่น กระบวนการที่โปรแกรมไว้ในการระบุตำแหน่ง และลบข้อมูล (อัตโนมัติ หรือ ด้วยตนเอง) และ/หรือ การตรวจทานพื้นที่จัดเก็บข้อมูลด้วยตนเองก็สามารถดำเนินการได้<br><br>การปฏิบัติตามวิธีการลบข้อมูลอย่างปลอดภัย ทำให้มั่นใจว่า ข้อมูลนั้นจะไม่สามารถถูกนำกลับมาได้เมื่อไม่ได้ใช้งานแล้ว<br><br>จำไว้ว่า หากไม่มีการใช้งาน ก็ไม่มีความจำเป็นต้องเก็บไว้! |
| 3.2 ไม่จัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยงหลังการตรวจการอนุญาต (แม้ว่าจะเข้ารหัสไว้ก็ตาม) หากได้รับข้อมูลการอนุญาตที่สุ่มเสี่ยงให้ทำการ render ข้อมูลทั้งหมดให้ ไม่สามารถกู้กลับคืนได้หลังกระบวนการตรวจการอนุญาต<br><br>เป็นเรื่องที่ได้รับอนุญาตสำหรับ ผู้ออกบัตรและ องค์กรซึ่งสนับสนุนบริการการออกบัตร เพื่อจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยงหาก:<br><br>• ไม่มีการอ้างเหตุผลทางธุรกิจ และ<br>• ข้อมูลถูกจัดเก็บไว้อย่างปลอดภัย<br><br>ข้อมูลการอนุญาตที่สุ่มเสี่ยง ได้แก่ข้อมูลที่อ้างอิงไว้ใน ความต้องการ 3.2.1 ถึง 3.2.3: | 3.2.a สำหรับผู้ออกบัตร และ/หรือองค์กร ซึ่งสนับสนุนบริการการออกบัตร และจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยง ตรวจสอบนโยบาย และสัมภาษณ์บุคลากรเพื่อตรวจให้แน่ใจว่ามีการอ้างเหตุผลทางธุรกิจเป็นลายลักษณ์อักษรหรือไม่ในการจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยง. | ข้อมูลการอนุญาตที่สุ่มเสี่ยง ประกอบไปด้วย ข้อมูลการติดตามทั้งหมด รหัส หรือ ค่าตัวเลขที่ใช้ตรวจสอบบัตร และ ข้อมูล PIN การจัดเก็บ ข้อมูลการอนุญาตที่สุ่มเสี่ยงหลังการตรวจการอนุญาตนั้นเป็นสิ่งต้องห้าม! ข้อมูลเหล่านี้มีค่ามากสำหรับ ผู้ประสงค์ร้าย เพราะจะทำให้พวกเขาสามารถสร้างการชำระเงินจากบัตรปลอม และปลอมแปลงการทำธุรกรรมได้ |
| | 3.2.b สำหรับผู้ออกบัตร และ/หรือองค์กร ซึ่งสนับสนุนบริการการออกบัตร และจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยง ตรวจสอบการจัดเก็บข้อมูล และการตั้งค่าระบบเพื่อตรวจให้แน่ใจว่าข้อมูลการอนุญาตที่สุ่มเสี่ยงได้รับความปลอดภัย<br><br>3.2.c สำหรับ entity อื่นๆทั้งหมด หากได้รับข้อมูลการอนุญาตที่สุ่มเสี่ยง ต้องตรวจสอบนโยบายและกระบวนการ ตรวจสอบการตั้งค่าระบบ เพื่อตรวจให้แน่ใจว่าข้อมูลไม่ได้มีการเก็บไว้หลังการอนุญาต | หน่วยงานผู้ซึ่งออกบัตรที่ใช้ชำระเงิน หรือ ดำเนินการ หรือสนับสนุน การออกบัตร มักสร้าง และ ควบคุมข้อมูลการอนุญาตที่สุ่มเสี่ยง ในฐานะส่วนหนึ่งของการออกบัตร มีการอนุญาตสำหรับองค์กร ซึ่งดำเนินการ อำนวยความสะดวก หรือ สนับสนุน บริการการออกบัตรให้ข้อมูลการอนุญาตที่สุ่มเสี่ยง เฉพาะเมื่อพวกเขามีความต้องการทางธุรกิจในการจัดเก็บข้อมูลเหล่านี้ตามกฎหมายเท่านั้น<br><br>ควรจำว่า ความต้องการ PCI DSS ทั้งหมด ใช้กับผู้ออกบัตรและผู้ได้รับการยกเว้น มีเพียงผู้ออกบัตรและผู้ดำเนินการในการออกบัตรซึ่งอาจจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยงไว้หากมีเหตุผลตามกฎหมาย เหตุผลทางกฎหมายคือสิ่งหนึ่งซึ่งจำเป็นสำหรับประสิทธิภาพการทำงานโดยผู้ออกบัตร และไม่ใช่สิ่งที่อำนวยความสะดวก ข้อมูลใดๆก็ตามจะต้องถูกจัดเก็บไว้อย่างปลอดภัย และเป็นไปตามความต้องการ PCI DSS และแบรนด์ชำระเงินแต่ละแบรนด์ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 3.2.d สำหรับหน่วยงานอื่นๆทั้งหมด หากได้รับข้อมูลการอนุญาตที่สุ่มเสี่ยง ให้ตรวจสอบกระบวนการ และตรวจสอบขั้นตอนการลบข้อมูลอย่างปลอดภัยเพื่อให้แน่ใจว่าข้อมูลเหล่านั้นจะไม่สามารถกู้กลับมาได้ | หน่วยงานที่ไม่ได้ทำการออกบัตรนั้น จะไม่ได้รับอนุญาตให้ทำการจัดเก็บข้อมูลการอนุญาตที่สุ่มเสี่ยงหลังจากการตรวจการอนุญาตแล้ว |
| 3.2.1 ไม่เก็บข้อมูลทั้งหมดของการติดตามใดๆ (จากแถบแม่เหล็กหลังบัตร หรือข้อมูลรูปแบบเดียวกันที่อยู่ในชิปหรือที่อื่นๆ) ข้อมูลเหล่านี้ เรียกในชื่ออื่นๆว่า ข้อมูลการติดตามทั้งหมด (full track), track, track 1, track 2, และข้อมูลแถบแม่เหล็ก<br><br>หมายเหตุ: โดยธุรกิจปกติแล้ว องค์ประกอบข้อมูลดังต่อไปนี้จากแถบแม่เหล็กอาจจะต้องถูกจัดเก็บไว้:<br>• ชื่อผู้ถือบัตร<br>• หมายเลขบัญชีหลัก *(PAN)*<br>• วันหมดอายุ<br>• หมายเลขบริการ<br>เพื่อลดความเสี่ยง เก็บข้อมูลเหล่านี้เท่าที่จำเป็นต่อธุรกิจ | 3.2.1 สำหรับตัวอย่างของส่วนประกอบระบบ ตรวจสอบแหล่งที่มาของข้อมูล รวมไปถึงสิ่งต่อไปนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) และตรวจสอบให้แน่ใจว่า ข้อมูลทั้งหมดของ การติดตามใดๆจากแถวแม่เหล็กหลังบัตร หรือข้อมูลที่เทียบเท่าบนชิป ไม่ได้ถูกจัดเก็บไว้หลังตรวจการอนุญาต:<br>• ข้อมูลการทำธุรกรรมที่เข้ามา<br>• ประวัติทั้งหมด (ตัวอย่าง เช่น การซื้อขาย ประวัติ debugging และ error)<br>• ไฟล์ประวัติ<br>• ไฟล์ติดตาม<br>• แบบแผนของฐานข้อมูลหลายๆแบบ<br>• เนื้อหาในฐานข้อมูล | หากมีการบันทึก ข้อมูลการติดตามทั้งหมด (full track data) ไว้ ผู้ประสงค์ร้าย ผู้ที่ได้รับข้อมูลไป สามารถใช้มันเพื่อสำเนาบัตรในการชำระเงิน และปลอมแปลงการทำธุรกรรม |
| 3.2.2 ไม่เก็บโค้ด หรือ ค่าการตรวจสอบบัตร (ตัวเลข 3 ตัว หรือ 4 ตัวที่พิมพ์เอาไว้ด้านหน้า หรือหลังบัตรชำระเงิน) ที่ใช้เพื่อธุรกรรมที่มีการตรวจสอบบัตรโดยไม่ต้องแสดงบัตร | 3.2.2 สำหรับตัวอย่างของส่วนประกอบของระบบ ตรวจสอบแหล่งที่มาข้อมูล ได้แก่สิ่งต่อไปนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) และตรวจสอบให้แน่ใจว่า ตัวเลข 3 ตัว หรือ 4 ตัวที่พิมพ์เอาไว้ด้านหน้า หรือหลังบัตรชำระเงิน หรือ ส่วนลายเซ็น (CVV2, CVC2, CID, CAV2 data) ไม่ได้มีการจัดเก็บไว้หลังการตรวจสอบการอนุญาต:<br>• ข้อมูลการทำธุรกรรมที่เข้ามา<br>• ประวัติทั้งหมด<br>(ตัวอย่าง เช่น การซื้อขาย ประวัติ debugging และ error)<br>• ไฟล์ประวัติ<br>• ไฟล์ติดตาม<br>• แบบแผนของฐานข้อมูลหลายๆแบบ<br>• เนื้อหาใน ฐานข้อมูล | จุดประสงค์ของโค้ดตรวจสอบบัตร คือเพื่อปกป้องการใช้ "ธุรกรรมที่มีการตรวจสอบบัตรโดยไม่ต้องแสดงบัตร"— อินเทอร์เน็ต หรือ การสั่งซื้อทางไปรษณีย์ /การสั่งซื้อทางโทรศัพท์ (MO/TO) — ซึ่งไม่ต้องมีการแสดงตนของผู้ซื้อและบัตร<br><br>หากข้อมูลเหล่านี้ถูกขโมยไป ผู้ประสงค์ร้าย สามารถจัดการปลอมแปลงธุรกรรม ทางอินเทอร์เน็ต และ MO/TO ได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.2.3 ไม่จัดเก็บข้อมูลการระบุตัวตนส่วนบุคคล (PIN) หรือ PIN block ที่เข้ารหัส | 3.2.3 สำหรับตัวอย่างของส่วนประกอบระบบ ให้ทำการตรวจสอบ ตรวจสอบแหล่งที่มาข้อมูล ได้แก่สิ่งต่อไปนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) และให้แน่ใจว่า PINs และ PIN block ที่เข้ารหัสไม่ได้ถูกเก็บไว้หลังตรวจการอนุญาต:<br>• ข้อมูลการทำธุรกรรมที่เข้ามา<br>• ประวัติทั้งหมด (ตัวอย่าง เช่น การซื้อขาย ประวัติ debugging และ error)<br>• ไฟล์ประวัติ<br>• ไฟล์ติดตาม<br>• แบบแผนของฐานข้อมูลหลายๆแบบ<br>• เนื้อหาในฐานข้อมูล | ค่าเหล่านี้ควรจะทราบเฉพาะกับผู้ถือบัตร หรือ ธนาคารเท่านั้น หากข้อมูลเหล่านี้ถูกขโมยไป ผู้ประสงค์ร้าย สามารถดำเนินการปลอมแปลงธุรกรรมที่มีพื้นฐานจาก การทำธุรกรรมแบบที่มีพื้นฐานจาก PIN หรือ PIN-based debit (ตัวอย่างเช่น การถอนเงินผ่าน ATM) |
| 3.3 ทำการบดบัง (mask) PAN เมื่อมีการแสดงผล (ตัวเลข 6 ตัวแรก และ 4 ตัวสุดท้ายคือตัวเลขสูงสุดที่สามารถแสดงผลได้) ให้เฉพาะบุคลากรที่มีความต้องการทางธุรกิจตามกฎหมายเท่านั้นที่สามารถมองเห็น PAN ทั้งหมดได้<br><br>หมายเหตุ: ความต้องการนี้ไม่ได้ทดแทนความต้องการที่เข้มงวดกว่านี้ที่ใช้งาน เพื่อการแสดงผลข้อมูลผู้ถือบัตร — ตัวอย่าง เช่น กฎหมาย หรือ ความต้องการของแบรนด์การชำระเงินสำหรับใบเสร็จ *point-of-sale (POS)* | 3.3.a ตรวจสอบนโยบายและกระบวนการที่บันทึกไว้สำหรับการบดบัง (mask) การแสดงผลของ PANs เพื่อให้แน่ใจว่า:<br>• รายชื่อผู้มีหน้าที่ที่ต้องการสิทธิการเข้าถึงการแสดงผล PAN ทั้งหมด ได้ถูกจัดทำเป็นเอกสารเอาไว้ พร้อมกันกับความต้องการทางธุรกิจตามกฎหมายสำหรับแต่ละหน้าที่ซึ่งมีสิทธิการเข้าถึงเหล่านั้น<br>• PAN จะต้องถูก mask เมื่อแสดงผล เพื่อให้บุคลากรที่มีความต้องการทางธุรกิจตามกฎหมายเท่านั้นที่จะมองเห็น PAN ทั้งหมดได้<br>• ผู้มีบทบาทอื่นๆซึ่งไม่มีสิทธิเฉพาะในการอนุญาตให้เห็น PAN ทั้งหมด จะเห็นเพียง PAN ที่บดบังไว้ | การแสดงผลของ PAN บนสิ่งต่างๆ เช่นหน้าจอคอมพิวเตอร์ ใบเสร็จการชำระเงิน แฟกซ์ รายงานในรูปแบบกระดาษ อาจทำให้ข้อมูลนั้นตกเป็นของผู้ที่ไม่ได้รับอนุญาต และนำไปใช้ปลอมแปลงได้ ทำให้มั่นใจว่า PAN แสดงผลเฉพาะผู้ที่มีความต้องการทางธุรกิจตามกฎหมายเท่านั้น เพื่อลดความเสี่ยงให้น้อยที่สุดที่ผู้ไม่ได้รับอนุญาตจะเข้าถึงข้อมูลได้<br><br>ความต้องการนี้คล้ายคลึงกับการปกป้องมิให้ PAN ถูก แสดงผล บนหน้าจอ ใบเสร็จ เอกสารตีพิมพ์ และอื่นๆ ไม่ควรสับสนกับ ความต้องการ 3.4 สำหรับการปกป้อง PAN เมื่อถูก จัดเก็บ ในไฟล์และฐานข้อมูล และอื่นๆ |
| | 3.3.b ตรวจสอบการตั้งค่าระบบเพื่อให้แน่ใจว่า PAN ทั้งหมด แสดงผลต่อ ผู้ใช้/ผู้ทำหน้าที่ ที่มีความต้องการทางธุรกิจตามเอกสาร และ PAN ถูกบดบัง (mask) สำหรับการร้องขออื่นๆ | |
| | 3.3.c ตรวจสอบการแสดงผลของ PAN (ตัวอย่าง เช่น บนหน้าจอ บนใบเสร็จ) เพื่อให้มั่นใจว่า PAN ได้รับการบดบัง เมื่อแสดงข้อมูลผู้ถือบัตร และเฉพาะผู้ที่มีความต้องการทางธุรกิจตามกฎหมายเท่านั้นที่สามารถมองเห็น PAN ทั้งหมดได้ | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.4 Render PAN ให้ไม่สามารถอ่านอ่านได้ ไม่ว่าที่ไหนก็ตามที่จัดเก็บไว้ (รวมไปถึง สื่อที่สามารถเคลื่อนที่ได้ ส่วน backup และ ส่วนประวัติ) โดยใช้วิธีการต่อไปนี้:<br>• การเข้ารหัสทางเดียว (hashing) ที่มีพื้นฐานบน การอ่านรหัสลับที่เข้มงวด (strong cryptography) (hash จะต้องใช้กำ PAN ทั้งหมด)<br>• การตัดคำ (Truncation) (การทำ hashing ไม่สามารถทดแทน PAN ส่วนที่ตัดคำแล้วได้)<br>• Index tokens และ pads (pads จะต้องถูกจัดเก็บไว้อย่างปลอดภัย)<br>• การอ่านรหัสลับที่เข้มงวด พร้อมกระบวน และ ขั้นตอนการจัดการคีย์ที่เกี่ยวข้อง<br><br>หมายเหตุ: มันอาจเป็นความพยายามที่เล็กๆน้อยๆของผู้ประสงค์ร้ายในการพยายามกู้คืนข้อมูล *PAN* ดั้งเดิม หากพวกเขาสามารถเข้าถึง ทั้งเวอร์ชั่นที่ ตัดทอน และ เข้ารหัสทางเดียว ดังนั้นจึงควรมีการควบคุมเพิ่มเติมสำหรับสิ่งแวดล้อมของหน่วยงานที่ *PAN* ทั้ง 2 เวอร์ชั่นถูกจัดเก็บไว้เพื่อให้มั่นใจได้ว่า *PAN* ดั้งเดิม จะไม่สามารถถูกกู้คืนกลับมาได้ | 3.4.a ตรวจสอบ การจัดทำเป็นเอกสารเกี่ยวกับระบบที่ใช้ปกป้อง PAN รวมไปถึง ผู้ขาย ประเภทของระบบ/กระบวนการ และ อัลกอริทึ่มการเข้ารหัส (หากทำได้) เพื่อให้มั่นใจว่า PAN ได้รับการ render ให้ไม่สามารถอ่านได้ด้วยวิธีการดังนี้:<br>• การเข้ารหัสทางเดียว ที่มีพื้นฐานบน การอ่านรหัสลับที่เข้มงวด<br>• การตัดคำ<br>• ใช้ Index tokens และ pads (pads จะต้องถูกจัดเก็บไว้อย่างปลอดภัย)<br>• การอ่านรหัสลับที่เข้มงวด พร้อมกระบวน และ ขั้นตอนการจัดการคีย์ที่เกี่ยวข้อง<br><br>3.4.b ตรวจสอบตารางหรือไฟล์ต่างๆจากตัวอย่างที่เก็บข้อมูลเพื่อให้มั่นใจว่า PAN ถูก render ให้ไม่สามารถอ่านได้ (ซึ่งก็คือ ไม่ได้อยู่ในรูปแบบตัวหนังสือธรรมดา)<br><br>3.4.c ตรวจสอบตัวอย่างของสื่อข้อมูลที่สามารถเคลื่อนที่ได้ (ตัวอย่าง เช่น เทป Back up) เพื่อยืนยันว่า PAN ถูก render ให้ไม่สามารถอ่านได้แล้ว<br><br>3.4.d ตรวจสอบตัวอย่างของ ประวัติการตรวจสอบเพื่อยืนยันว่า PAN ถูก render ให้ไม่สามารถอ่านได้ หรือถูกลบออกจากประวัติแล้ว | PAN ที่จัดเก็บไว้ในส่วนเก็บข้อมูลหลัก (ฐานข้อมูล หรือ ฐานข้อมูลรายแฟ้ม (flat files) เช่น ไฟล์ตัวหนังสือ แผ่นตารางทำการ (spreadsheets)) รวมไปถึงส่วนเก็บข้อมูลอื่นๆ (backup ประวัติการตรวจสอบ ยกเว้นประวัติการตรวจหาข้อผิดพลาด (troubleshooting logs)) จะต้องถูกปกป้อง<br><br>การเข้ารหัสทางเดียว (One-way hash) ที่มีพื้นฐานบน การอ่านรหัสลับที่เข้มงวด (strong cryptography) สามารถใช้เพื่อ render ข้อมูลผู้ถือบัตรให้ไม่สามสามารถอ่านได้ ฟังก์ชั่นนี้เหมาะสมกับการที่ไม่ต้องการนำข้อมูลตัวเลขดั้งเดิมกลับมาใช้อีก (การเข้ารหัสทางเดียว ไม่สามารถย้อนกระบวนการได้) เป็นสิ่งที่แนะนำ แต่ยังไม่ถึงกับเป็นความต้องการสำหรับการเพิ่มค่าที่สุ่มลงไปในข้อมูลผู้ถือบัตรก่อนเข้ารหัสเพื่อลดความเป็นไปได้สำหรับผู้โจมตีในการเปรียบเทียบข้อมูล (และสืบค้น PAN จาก) ตารางการคำนวณค่าก่อนการเข้ารหัส<br><br>จุดประสงค์ของการตัดคำคือ เฉพาะส่วน (ตัวเลขไม่เกิน 6 ตัวแรก และ 4 ตัวท้าย) ของ PAN ที่จะถูกเก็บไว้<br><br>Index token เป็น อุปกรณ์การอ่านรหัส ซึ่งแทนที่ PAN โดยพื้นฐานของการใช้ค่าที่คาดเดาไม่ได้ และ one-time pad เป็นระบบซึ่งสุ่มสร้างกุญแจ (key) ส่วนตัวเพื่อเข้ารหัสข้อความซึ่งจะทำการถอดรหัสเมื่อใช้งาน one-time pad ตรงกับ กุญแจ (key)<br><br>จุดประสงค์ของ การอ่านรหัสลับที่เข้มงวด (Strong cryptography) (อย่างที่ได้ระบุไว้ในอภิธานศัพท์ ตัวย่อ และ คำย่อของ *PCI DSS* และ *PA-DSS*) ซึ่งก็คือ การเข้ารหัสที่มีพื้นฐานมาจาก การทดสอบระดับอุตสาหกรรม และอัลกอริทึ่มที่ได้รับการยอมรับ (ไม่ใช่อัลกิรอทึ่มที่เป็นเจ้าของ หรือ "สร้างขึ้นมาเอง") พร้อมคีย์การอ่านรหัสที่เข้มงวด<br><br>ด้วยการนำ PAN เวอร์ชั่นที่เข้ารหัสทางเดียว และ ตัดคำมาใช้คู่กัน ผู้ประสงค์ร้ายอาจได้รับข้อมูลPAN ดั้งเดิมได้โดยง่าย การควบคุมซึ่งปกป้องข้อมูลที่สัมพันธ์กันเหล่านี้จะช่วยให้มั่นใจได้ว่า PAN ดั้งเดิมไม่สามารถอ่านได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.4.1 หากมีการใช้งานการเข้ารหัส disk (ที่ไม่ใช่การเข้ารหัสฐานข้อมูลระดับ file- หรือ column-) การเข้าถึงผ่านระบบ (logical access) จะต้องมีการกระทำอย่างแยกแยะและอย่างเป็นเอกเทศน์จากการตรวจการอนุญาตจากระบบปฏิบัติการ และกลไกการเข้าถึง (ตัวอย่าง เช่น โดยไม่ใช้ฐานข้อมูลผู้ใช้ภายใน หรือ ข้อมูลการล็อคอินเครือข่ายทั่วไป) การถอดรหัสจะต้องไม่ทำร่วมกับบัญชีผู้ใช้ | 3.4.1.a หากมีการใช้งานการเข้ารหัส disk ให้ตรวจสอบการตั้งค่า และสังเกตกระบวนการตรวจสอบการอนุญาต เพื่อให้มั่นใจว่า การเข้าถึงผ่านระบบ ไปยังระบบไฟล์เข้ารหัสได้มีการดำเนินการตามกลไกซึ่งแยกออกจากกลไกการตรวจการอนุญาตจากระบบปฏิบัติการ (ตัวอย่าง เช่น โดยไม่ใช้ฐานข้อมูลผู้ใช้ภายใน หรือข้อมูลการล็อคอินเครือข่ายทั่วไป)<br><br>3.4.1.b สังเกตกระบวนการ และสัมภาษณ์บุคลากรเพื่อให้มั่นใจว่า คีย์การอ่านรหัสลับ ถูกเก็บไว้อย่างปลอดภัย (ตัวอย่างเช่น เก็บเอาไว้ในสื่อที่สามารถเคลื่อนที่ได้ซึ่งได้รับการปกป้องเทียบเท่าการควบคุมที่เข้มงวด)<br><br>3.4.1.c ตรวจสอบการตั้งค่า และสังเกตกระบวนการ เพื่อให้มั่นใจว่า ข้อมูลผู้ถือบัตรบนสื่อที่สามารถเคลื่อนที่ได้นั้นได้รับการเข้ารหัสทุกครั้งที่เก็บข้อมูล<br><br>หมายเหตุ: หากการเข้ารหัส *disk* ไม่ได้ถูกนำมาใช้ ข้อมูลที่เก็บอยู่ในสื่อนั้นควรจะต้อง *render* ให้ไม่สามารถอ่านได้ด้วยวิธีการบางอย่าง | จุดประสงค์ของความต้องการนี้มีเพื่อแสดงให้เห็นการยอมรับได้ของการเข้ารหัสในระดับ disk ในการ render ข้อมูลผู้ถือบัตรให้ไม่สามารถอ่านได้ การเข้ารหัสในระดับ disk ทั้งหมดของ disk /partition บนคอมพิวเตอร์ และถอดรหัสอัตโนมัติเมื่อผู้ใช้ที่ได้รับอนุญาตร้องขอวิธีการเข้ารหัส disk จะสกัดกั้นกระบวนการ อ่าน/เขียน ของระบบปฏิบัติการ และ บรรจุการแปลงการอ่านรหัสที่เหมาะสมโดยปราศจากการกระทำพิเศษใดๆจากผู้ใช้นอกจากการกรอก password หรือ pass phrase เมื่อระบบเริ่มต้น (startup) หรือเมื่อเริ่มต้นใช้งาน ขึ้นอยู่กับลักษณะเฉพาะของการเข้ารหัสในระดับ disk ในการยินยอมความต้องการนี้ จะไม่สามารถ:<br><br>1)ใช้งานการให้อนุญาตบัญชีผู้ใช้เดียวกันกับระบบปฏิบัติการ หรือ<br>2)ใช้คีย์การเข้ารหัสซึ่งเกี่ยวพันกับ หรือ ได้รับมาจากฐานข้อมูลผู้ใช้ภายใน หรือ ข้อมูลการล็อคอินเครือข่ายทั่วไป<br><br>การเข้ารหัส disk อย่างสมบูรณ์ ช่วยในการปกป้องข้อมูลจากการสูญเสียทางกายภาพของ disk และนอกจากนั้น อาจเหมาะกับสื่อเคลื่อนที่ได้ซึ่งจัดเก็บข้อมูลผู้ถือบัตร |
| 3.5 เอกสาร และกระบวนการการปฏิบัติตามเพื่อปกป้อง คีย์ที่ใช้ในการรักษาความปลอดภัยข้อมูลผู้ถือบัตรต่อการเปิดเผยและการนำไปใช้ในทางที่ผิด:<br><br>หมายเหตุ: ความต้องการนี้ใช้กับคีย์ที่ใช้ในการเข้ารหัสข้อมูลผู้ถือบัตรที่จัดเก็บไว้ และใช้กับกุญแจการเข้ารหัสที่ใช้เพื่อปกป้องข้อมูลคีย์การเข้ารหัส กุญแจการเข้ารหัสนั้นจะต้องเข้มงวดเทียบเท่ากับคีย์การเข้ารหัสที่มันปกป้อง | 3.5 ตรวจสอบนโยบายการจัดการคีย์ และกระบวนการ เพื่อให้มั่นใจว่ากระบวนการนั้นถูกทำขึ้นเฉพาะเจาะจงสำหรับการปกป้องคีย์ที่ใช้ในการเข้ารหัสข้อมูลผู้ถือบัตรต่อการเปิดเผยและนำไปใช้ในทางที่ผิดอย่างน้อยดังนี้:<br><br>● การเข้าถึง คีย์ ถูกจำกัดไว้เฉพาะผู้ควบคุมที่จำเป็นจำนวนหนึ่งเท่านั้น<br>● กุญแจการเข้ารหัสเข้มงวดเทียบเท่ากับคีย์การเข้ารหัสข้อมูลที่มันปกป้อง<br>● กุญแจการเข้ารหัสถูกเก็บไว้แยกจากคีย์การเข้ารหัส<br>● คีย์ ถูกเก็บไว้อย่างปลอดภัยในตำแหน่งและ และรูปแบบที่น้อยที่สุดเท่าที่ทำได้ | คีย์การอ่านรหัสจะต้องได้รับการปกป้องอย่างเข้มงวด เพราะว่าผู้ที่ได้รับการเข้าถึงจะสามารถถอดรหัสข้อมูลได้ หากมีการใช้กุญแจการเข้ารหัส มันจะต้องเข้มงวดเทียบเท่ากับข้อมูลคีย์การเข้ารหัส เพื่อให้มั่นใจว่ามีการปกป้องที่เหมาะสมให้กับคีย์การเข้ารหัส เช่นเดียวกันกับกุญแจที่ใช้กับคีย์นั้น<br><br>ความต้องการในการปกป้องคีย์จากการถูกเปิดเผย และนำไปใช้ในทางที่ผิด ใช้กับทั้ง คีย์การเข้ารหัสข้อมูล และ กุญแจคีย์เข้ารหัส เพราะกุญแจหนึ่งอัน อาจทำให้เข้าถึงข้อมูลการเข้ารหัสมากมายได้ กุญแจการเข้ารหัสจึงต้องการการปกป้องที่เข้มงวด |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| **3.5.1** จำกัดการเข้าถึงคีย์การเข้ารหัสไว้ให้เฉพาะผู้ดูแลที่จำเป็นเพียงจำนวนหนึ่งเท่านั้น | **3.5.1** ตรวจสอบการเข้าถึงของผู้ใช้เพื่อให้มั่นใจว่าการเข้าถึงคีย์นั้นถูกจำกัดไว้ให้เฉพาะผู้ดูแลที่จำเป็นเพียงจำนวนหนึ่งเท่านั้น | ควรจะมีเพียงผู้ดูแลจำนวนน้อยเท่านั้นที่สามารถเข้าถึงคีย์การเข้ารหัส (ลดความเป็นไปได้สำหรับการ render ข้อมูลผู้ถือบัตรให้สามารถอ่านได้โดยบุคคลที่ไม่ได้รับอนุญาต) ปกติแล้วมักให้สิทธิเฉพาะผู้ที่มีหน้าที่ความรับผิดชอบเท่านั้น |
| **3.5.2** ไม่ว่าเมื่อใดก็ตาม จัดเก็บความลับ และคีย์ส่วนตัวที่ใช้ในการ เข้า/ถอดรหัส ข้อมูลผู้ถือบัตรไว้ในรูปแบบ 1 ข้อ (หรือมากกว่า) ดังต่อไปนี้:<br>●เข้ารหัสด้วยกุญแจคีย์การเข้ารหัสซึ่งเข้มงวดเทียบเท่ากับ คีย์การเข้ารหัสข้อมูล และที่เก็บไว้แยกจากกันกับคีย์การเข้ารหัสข้อมูล<br>●ภายในอุปกรณ์การเข้ารหัสที่ปลอดภัย (เช่น host security module(HSM) หรืออุปกรณ์ point-of-interactionที่ได้รับการอนุญาตจาก PTS)<br>●อย่างน้อย 2 ส่วนประกอบของคีย์เต็มรูปแบบ (full-length key)หรือคีย์แชร์ (key shares) ที่จะต้องได้รับมาตรฐานระดับอุตสาหกรรม<br>หมายเหตุ:ไม่ได้เป็นการแนะนำในการจัดเก็บคีย์สาธารณะไว้ในรูปแบบเหล่านี้ | **3.5.2.a** ตรวจสอบเอกสารกระบวนการเพื่อให้มั่นใจว่าคีย์การเข้ารหัสที่ใช้ในการ เข้า/ถอดรหัส ข้อมูลผู้ถือบัตร จะต้องปรากฏอยู่ใน 1 รูปแบบ (หรือมากกว่า) ต่อไปนี้เท่านั้นไม่ว่าเมื่อใดก็ตาม<br>●ได้รับการเข้ารหัสด้วยกุญแจคีย์การซึ่งเข้มงวดเทียบเท่ากับ คีย์การเข้ารหัสข้อมูล และที่เก็บไว้แยกจากกันกับคีย์การเข้ารหัสข้อมูล<br>●ภายในอุปกรณ์การเข้ารหัสที่ปลอดภัย (เช่น host security module(HSM)หรืออุปกรณ์ point-of-interactionที่ได้รับการอนุญาตจาก PTS)<br>●ในรูปแบบของส่วนประกอบคีย์ หรือ คีย์แชร์ (key shares) ด้วยกระบวนการระดับอุตสาหกรรม<br><br>**3.5.2.b** ตรวจสอบการตั้งค่าระบบ และ ตำแหน่งในการจัดเก็บคีย์เพื่อให้แน่ใจว่าคีย์การเข้ารหัสถูกใช้สำหรับเข้า/ถอดรหัสข้อมูลผู้ถือปรากฏอยู่ใน 1 รูปแบบ (หรือมากกว่า) ต่อไปนี้เท่านั้นไม่ว่าเมื่อใดก็ตาม<br>●เข้ารหัสด้วยกุญแจคีย์การเข้ารหัส<br>●ภายในอุปกรณ์การเข้ารหัสที่ปลอดภัย (เช่น host security module(HSM)หรืออุปกรณ์ point-of-interactionที่ได้รับการอนุญาตจาก PTS)<br>●ในรูปแบบของส่วนประกอบคีย์ หรือ คีย์แชร์ (key shares) ด้วยกระบวนการระดับอุตสาหกรรม<br><br>3.5.2.cเมื่อใดก็ตามที่กุญแจการเข้ารหัสถูกใช้งานตรวจสอบการตั้งค่าระบบและตำแหน่งที่คีย์ถูกเก็บไว้ เพื่อให้มั่นใจว่า:<br>●กุญแจการเข้ารหัสเข้มงวดเทียบเท่ากับคีย์การเข้ารหัสข้อมูลเหล่านั้น<br>●กุญแจการเข้ารหัสถูกเก็บแยกไว้จากคีย์การเข้ารหัสข้อมูล | คีย์การเข้ารหัสจะต้องถูกเก็บไว้อย่างปลอดภัย เพื่อป้องกันผู้ไม่ได้รับอนุญาต หรือ การเข้าถึงที่ไม่มีความจำเป็น ซึ่งอาจทำให้ข้อมูลผู้ถือบัตรถูกเปิดเผย<br><br>ไม่ได้มีจุดประสงค์ให้กุญแจการเข้ารหัสถูกเข้ารหัสอย่างไรก็ตาม กุญแจเหล่านั้นจะต้องได้รับการป้องกันจากการเปิดเผย และ นำไปใช้ในทางที่ผิด ดังที่ได้กล่าวไว้ในความต้องการ3.5.หากมีการใช้งานกุญแจการเข้ารหัสจัดเก็บกุญแจการเข้ารหัสในสถานที่แยกจากคีย์การเข้ารหัสข้อมูล ทั้งทางกายภาพ และ/หรือการเข้าถึงผ่านระบบเพื่อลดความเสี่ยงสำหรับการเข้าถึงที่ไม่ได้รับอนุญาต |

| ความต้องการ **PCI DSS** | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.5.3 จัดเก็บคีย์เข้ารหัสไว้ในน้อยสถานที่เท่าที่จะเป็นไปได้ | 3.5.3 ตรวจสอบสถานที่จัดเก็บคีย์ และสังเกตกระบวนการเพื่อให้แน่ใจว่าจัดเก็บคีย์เข้ารหัสไว้ในน้อยสถานที่เท่าที่จะเป็นไปได้ | การจัดเก็บคีย์เข้ารหัสไว้ในสถานที่จำนวนน้อยๆจะช่วยให้องค์กรสามารถติดตามและเฝ้าคีย์ทั้งหมดเอาไว้ได้ เป็นการลดความเสี่ยงในการถูกเปิดเผยแก่ผู้ไม่ได้รับอนุญาต |
| 3.6 จัดทำเอกสาร และ ดำเนินการตามกระบวนการทั้งหมดในการจัดการคีย์ และกระบวนการสำหรับคีย์เข้ารหัสที่ใช้ในการเข้ารหัสข้อมูลผู้ถือบัตร รวมไปถึงขั้นตอนดังนี้:<br><br>หมายเหตุ: มาตรฐานอุตสาหกรรมจำนวนมากสำหรับคีย์ ได้มีเปิดให้ใช้งานจากหลากหลายแหล่งข้อมูล ได้แก่ *NIST* ซึ่งสามารถพบได้ที่ *http://csrc.nist.gov* | 3.6.a กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ: หากผู้ให้บริหารแบ่งปันคีย์ กับลูกค้าของพวกเขา สำหรับการส่งข้อมูล หรือ จัดเก็บข้อมูลผู้ถือบัตร ตรวจสอบการจัดทำเอกสารว่าผู้ให้บริการนั้นๆได้ให้คำแนะนำเรื่องความปลอดภัยในการส่งข้อมูล จัดเก็บ และ อัพเดทกุญแจ ของลูกค้าตามความต้องการ 3.6.1 - 3.6.8 ด้านล่างหรือไม่<br><br>3.6.b ตรวจสอบกระบวนการจัดการคีย์ และกระบวนการสำหรับคีย์ เข้ารหัสที่ใช้ในการเข้ารหัสข้อมูลผู้ถือบัตร และดำเนินการตามขั้นตอนดังนี้: | วิธีการที่จัดการคีย์เข้ารหัสเป็นส่วนสำคัญในการสร้างความปลอดภัยอย่างต่อเนื่อง กระบวนการจัดการคีย์ที่ดี ไม่ว่าจะเป็นวิธีการอัตโนมัติ หรือวิธีการที่ทำด้วยมือในส่วนหนึ่งของผลิตภัณฑ์การเข้ารหัส ต้องมีพื้นฐานจากมาตรฐานอุตสาหกรรม และบรรลุความต้องการ 3.6.1 - 3.6.8<br><br>ให้คำแนะนำกับลูกค้าเกี่ยวกับความปลอดภัยในการส่งข้อมูล จัดเก็บ และ อัพเดทคีย์ ซึ่งจะช่วยป้องกันไม่ให้ คีย์ มีการจัดการที่ผิดพลาด หรือ ถูกเปิดเผยต่อผู้ไม่ได้รับอนุญาต<br><br>ความต้องการนี้ใช้กับคีย์ที่ใช้ในการเข้ารหัสข้อมูลผู้ถือบัตร และคีย์อื่นใดก็ตามที่ใช้เข้ารหัส |
| 3.6.1 การสร้างคีย์เข้ารหัสที่เข้มงวด | 3.6.1.a ตรวจสอบว่ากระบวนการจัดการคีย์ได้มีการกำหนดวิธีการสร้างคีย์ที่เข้มงวดไว้<br><br>3.6.1.b สังเกตวิธีการสร้างคีย์เพื่อตรวจสอบว่าได้สร้างคีย์ที่ปลอดภัยแล้ว | การเข้ารหัสจะต้องสร้างคีย์ที่เข้มงวด ตามที่กำหนดไว้ใน PCI DSS และ อภิธานศัพท์ ตัวย่อ และ คำย่อของ PCI DSS และ PA-DSS ภายใต้ "การเข้ารหัสที่เข้มงวด (strong cryptography)" การใช้คีย์ที่เข้มงวดจะช่วยเพิ่มความปลอดภัยให้กับการเข้ารหัสข้อมูลผู้ถือบัตรเป็นอย่างมาก |
| 3.6.2 การแจกจ่ายคีย์เข้ารหัสอย่างปลอดภัย | 3.6.2.a ตรวจสอบว่า กระบวนการจัดการคีย์ได้มีการกำหนดวิธีการแจกจ่ายคีย์ที่ปลอดภัยไว้<br><br>3.6.2.b สังเกตวิธีการแจกจ่ายคีย์ เพื่อตรวจสอบว่าได้แจกจ่ายคีย์อย่างปลอดภัย | จะต้องมีการแจกจ่ายคีย์อย่างปลอดภัย หมายความว่า จะต้องแจกจ่ายคีย์ให้เฉพาะผู้ดูตามความต้องการ 3.5.1 และต้องไม่แจกจ่ายคีย์ในที่ที่ไม่ปลอดภัย |
| 3.6.3 การจัดเก็บคีย์เข้ารหัสอย่างปลอดภัย | 3.6.3.a ตรวจสอบว่ากระบวนการจัดการคีย์ได้มีการกำหนดวิธีการจัดเก็บคีย์ที่ปลอดภัยแล้ว<br><br>3.6.3.b สังเกตวิธีการที่ใช้จัดเก็บคีย์เพื่อตรวจสอบว่าได้จัดเก็บอย่างปลอดภัย | จะต้องมีการจัดเก็บคีย์อย่างปลอดภัย เช่น โดยการเข้ารหัสไว้ด้วยกุญแจคีย์การเข้ารหัส หากเก็บคีย์ไว้โดยไม่มีการป้องกันจากทำให้ผู้โจมตีที่เหมาะสม อาจทำให้เกิดการถอดรหัสข้อมูล และข้อมูลถูกเปิดเผยได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.6.4 เปลี่ยนคีย์เข้ารหัส สำหรับคีย์ที่หมดช่วงเวลาการเข้ารหัส (เช่น หลังจากระยะเวลาที่กำหนดไว้ผ่านไป และ/หรือ หลังจากได้สร้าง รหัส ตามจำนวนที่กำหนด ) ที่กำหนดโดยผู้ขายแอปพลิเคชั่น หรือ เจ้าของคีย์ และ มีพื้นฐานบนวิธีการที่ดีที่สุดของอุตสาหกรรม และ คำแนะนำ (เช่น สิ่งพิมพ์พิเศษของ NIST 800-57 (NIST Special Publication)) | 3.6.4.a ตรวจสอบว่า กระบวนการจัดการคีย์ได้มี ช่วงเวลาการเข้ารหัส สำหรับคีย์แต่ละประเภท และ กำหนดกระบวนการเปลี่ยนคีย์เมื่อช่วงเวลาการเข้ารหัสสิ้นสุดไว้<br><br>3.6.4.b สัมภาษณ์บุคลากรเพื่อตรวจสอบว่าคีย์ได้รับการเปลี่ยนเมื่อสิ้นสุดช่วงเวลาการเข้ารหัส | ช่วงเวลาการเข้ารหัส คือช่วงระยะเวลาระหว่างที่คีย์เข้ารหัสนั้นๆ จะสามารถใช้เพื่อจุดประสงค์ที่กำหนดไว้ได้ สิ่งที่ต้องพิจารณาสำหรับการกำหนดช่วงเวลาการเข้ารหัส มีดังนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) ความแข็งแรงของอัลกอริทึ่มพื้นฐาน ขนาดหรือความยาวของคีย์ ความเสี่ยงของการเจาะเข้าคีย์ และความอ่อนไหวของข้อมูลที่เข้ารหัสไว้<br><br>การเปลี่ยนคีย์ตามระยะเวลาเมื่อหมดช่วงเวลาการเข้ารหัสนั้นมีความจำเป็นเพื่อลดความเสี่ยงในการที่บุคคลจะได้รับคีย์และใช้มันเพื่อถอดรหัสข้อมูลได้ |
| 3.6.5 การปลดระวาง หรือ แทนที่คีย์ตามที่เห็นว่าจำเป็น (เช่น การเก็บ ทำลาย และ/หรือ การเพิกถอน) เมื่อความสมบูรณ์ของคีย์อ่อนแอลง (เช่น การลาออกของลูกจ้างที่รู้ข้อมูลเกี่ยวกับส่วนประกอบของคีย์ที่สามารถอ่านได้ (clear-text) หรือ คีย์ตกอยู่ในความสงสัยว่าถูกเจาะข้อมูล<br><br>หมายเหตุ: หากมีความจำเป็นต้องเก็บคีย์ที่ปลดระวาง หรือ ถูกแทนที่ไว้ คีย์เหล่านี้จะต้องถูกเก็บรักษาไว้อย่างปลอดภัย (เช่น โดยการใช้กุญแจการเข้ารหัส) คีย์เข้ารหัสที่เก็บไว้ ควรจะต้องใช้เฉพาะเพื่อจุดประสงค์ในการ ถอดรหัส/ตรวจสอบความถูกต้องเท่านั้น | 3.6.5.a ตรวจสอบว่ากระบวนการจัดการคีย์มีกระบวนการเฉพาะดังต่อไปนี้:<br>• การปลดระวาง หรือ การแทนที่คีย์ เมื่อเมื่อความสมบูรณ์ของคีย์อ่อนแอลง<br>• การเปลี่ยนคีย์เมื่อมีผู้รู้จักหรือต้องสงสัยจากการเจาะระบบ<br>• คีย์ใดๆก็ตามที่เก็บไว้หลังปลดระวาง หรือ แทนที่จะต้องไม่ถูกใช้ในกระบวนการเข้ารหัส<br><br>3.6.5.b สัมภาษณ์บุคลากรเพื่อตรวจสอบว่าได้มีการดำเนินการตามเงื่อนไขดังนี้:<br>• ปลดระวาง หรือ แทนที่คีย์ตามที่เห็นว่าจำเป็น เมื่อความสมบูรณ์ของคีย์อ่อนแอลง รวมไปถึงเมื่อมีการลาออกของบุคคลที่รู้ข้อมูลเกี่ยวกับคีย์<br>• เปลี่ยนคีย์เมื่อเป็นที่รู้จักหรือต้องสงสัยว่าถูกเจาะข้อมูล<br>• คีย์ใดๆที่จัดเก็บไว้หลังการ ปลดระวาง หรือ แทนที่จะต้องไม่ถูกใช้ในกระบวนการเข้ารหัส | คีย์ซึ่งไม่ได้ใช้ ไม่ต้องการแล้ว มีผู้รู้จักหรือต้องสงสัยว่าถูกเจาะข้อมูล ควรต้องมีการเพิกถอนการใช้ และ/หรือ ทำลาย เพื่อให้มั่นใจว่าไม่สามารถใช้งานได้อีก หากมีความจำเป็นต้องเก็บไว้ (เช่น เพื่อสนับสนุน ข้อมูลที่จัดเก็บ เข้ารหัสไว้) ควรได้รับการป้องกันที่เข้มงวด<br><br>ควรมีกระบวนการอำนวยความสะดวกการเปลี่ยนคีย์ที่หมดระยะเวลา หรือ มีผู้รู้จัก หรือ ต้องสงสัยว่าถูกเจาะข้อมูล |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 3.6.6 หากมีการดำเนินการจัดการคีย์เข้ารหัสที่สามารถอ่านได้ (clear text) ด้วยมือ การดำเนินการเหล่านี้จะต้องถูกจัดการด้วย การแบ่งเป็นส่วนย่อยๆ (split knowledge) และการควบคุมคู่ (dual control)<br><br>หมายเหตุ: ตัวอย่างของการดำเนินการจัดการคีย์ด้วยมือมีดังนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้): การสร้างคีย์ (*key generation*) การส่งข้อมูล (*transmission*) การโหลด (*loading*) การจัดเก็บ (*storage*) และ การทำลาย (*destruction*) | 3.6.6.a ตรวจสอบว่ากระบวนการจัดการคีย์ที่สามารถอ่านได้ (clear text) ด้วยมือ ได้มีการใช้กระบวนการต่อไปนี้:<br>• การแบ่งคีย์เป็นส่วนย่อยๆ เช่น ส่วนประกอบของคีย์อยู่ภายใต้การควบคุมของอย่างน้อย 2 คน ที่มีความรู้เฉพาะส่วนประกอบที่ตนมี และ<br>• การควบคุมคู่ เช่น ต้องใช้อย่างน้อย 2 คน ในการดำเนินใดๆในการจัดการคีย์ และไม่มีบุคคลใดบุคคลหนึ่งที่สามารถเข้าถึงส่วนการอนุญาตได้ (เช่น รหัสผ่าน หรือ คีย์) ของอีกคนหนึ่ง<br><br>3.6.6 b สัมภาษณ์บุคลากรและ/หรือ สังเกตกระบวนการเพื่อตรวจสอบว่า คีย์ที่สามารถอ่านได้ถูกจัดการด้วยวิธีการ:<br>• การแบ่งเป็นส่วนย่อยๆ (Split knowledge) และ<br>• การควบคุมคู่ (Dual control) | การแบ่งเป็นส่วนย่อยๆ และ การควบคุมคู่ นั้นใช้เพื่อไม่ให้มีการที่บุคคลเดียวสามารถเข้าถึงคีย์ทั้งหมดได้ การควบคุมนี้เหมาะสำหรับนำไปใช้ในการดำเนินการจัดการคีย์ด้วยมือ หรือ ที่ที่ไม่มีการดำเนินการจัดการคีย์โดยผลิตภัณฑ์การเข้ารหัส<br><br>การแบ่งเป็นส่วนย่อยๆ (Split knowledge) คือวิธีการที่ใช้คน 2 คนหรือมากกว่าซึ่งแยกจากกันในการเก็บส่วนประกอบคีย์ ซึ่งแต่ละคนมีความรู้เฉพาะส่วนที่ตนมีเท่านั้น และส่วนประกอบแต่ละส่วนไม่ได้บ่งชี้ถึงคีย์เข้ารหัสดั้งเดิม<br><br>การควบคุมคู่ (Dual control) คือวิธีการที่ต้องใช้ 2 คน หรือมากกว่า ในการดำเนินการใดๆ และไม่มีบุคคลใดบุคคลหนึ่งที่สามารถเข้าถึง หรือ ใช้ ส่วนการอนุญาตของอีกคนได้ |
| 3.6.7 ป้องกันการแทนที่โดยสิ่งที่ไม่ได้รับอนุญาตในส่วนคีย์เข้ารหัส | 3.6.7.a ตรวจสอบว่ากระบวนการจัดการคีย์มีการป้องกันการแทนที่โดยสิ่งที่ไม่ได้รับอนุญาตในส่วนคีย์เข้ารหัส<br><br>3.6.7.b สัมภาษณ์บุคลากรและ/หรือ สังเกตกระบวนการเพื่อตรวจสอบว่า มีการป้องกันการแทนที่โดยสิ่งที่ไม่ได้รับอนุญาตในส่วนคีย์เข้ารหัส | กระบวนการ ไม่ควรอนุญาตให้มีการแทนที่โดยสิ่งที่ไม่ได้รับอนุญาตในส่วนคีย์เข้ารหัส หรือกระบวนการที่ไม่ได้คาดการณ์ไว้ |
| 3.6.8 ผู้ดูแลคีย์เข้ารหัสต้องมีการรับทราบอย่างเป็นทางการถึง พวกเขาเข้าใจ และการยอมรับหน้าที่ความรับผิดชอบในการดูแลคีย์ | 3.6.8.a ตรวจสอบว่ากระบวนการจัดการคีย์ได้ให้ผู้ดูแลรับทราบ (ทางเอกสารหรือทางอิเล็กทรอนิกส์) ว่าพวกเขาเข้าใจ และ ยอมรับหน้าที่ความรับผิดชอบในการดูแลคีย์<br><br>3.6.8.b สังเกตเอกสาร หรือ หลักฐานอื่นที่แสดงให้เห็นว่าผู้ดูแลคีย์รับทราบ (ทางเอกสาร หรือทางอิเล็กทรอนิกส์) ว่าพวกเขาเข้าใจ และ ยอมรับหน้าที่ความรับผิดชอบในการดูแลคีย์ | กระบวนการนี้จะช่วยให้มั่นใจว่าแต่ละส่วนซึ่งมีบทบาทในการดูแลคีย์ ยอมรับบทบาทการดูแลคีย์ และ เข้าใจถึงหน้าที่ความรับผิดชอบ |
| 3.7 ทำให้มั่นใจว่านโยบายความปลอดภัย และขั้นตอนการดำเนินการสำหรับ จัดเก็บข้อมูลผู้ถือบัตร ได้ทำเป็นเอกสาร ใช้งาน และเป็นที่รู้จักสำหรับผู้ที่มีผลกระทบทั้งหมด | 3.7 ตรวจสอบเอกสาร สัมภาษณ์บุคลากรเพื่อตรวจสอบว่า นโยบายความปลอดภัย ปลอดภัย และ ขั้นตอนการดำเนินการสำหรับ จัดเก็บข้อมูลผู้ถือบัตร ได้:<br>• จัดทำเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักสำหรับผู้ที่มีผลกระทบทั้งหมด | บุคลากรจะต้องตระหนักถึง และ ดำเนินการตามนโยบายความปลอดภัย และเอกสารกระบวนการดำเนินการในการจัดการการจัดเก็บข้อมูลผู้ถือบัตรอย่างปลอดภัยอย่างต่อเนื่อง |

# ความต้องการที่ 4: เข้ารหัสการส่งข้อมูลผู้ถือบัตรในที่เปิดโล่ง และ เครือข่ายสาธารณะ

ข้อมูลที่สุ่มเสี่ยงจะต้องถูกเข้ารหัสไว้ในระหว่างการส่งข้อมูลผ่านเครือข่ายที่ง่ายต่อการเข้าถึงโดยผู้ประสงค์ร้าย การตั้งค่าเครือข่ายไร้สายที่ไม่ถูกต้อง และ ช่องโหว่ใน Legacy encryption (ช่องโหว่ของการเข้ารหัส) และ protocol การรับรองความถูกต้อง ยังคงเป็นเป้าของผู้ประสงค์ร้าย ผู้ซึ่งใช้ประโยชน์จากช่องโหว่เหล่านี้ในการใช้สิทธิการเข้าถึงสิ่งแวดล้อมข้อมูลผู้ถือบัตร

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 4.1 ใช้การเข้ารหัสที่เข้มงวด และ protocol ความปลอดภัย (เช่น SSL/TLS, IPSEC, SSH, และ อื่นๆ) เพื่อปกป้องข้อมูลผู้ถือบัตรที่สุ่มเสี่ยง ข้อมูลผู้ถือบัตรระหว่างการส่งข้อมูลในที่เปิดโล่ง และ เครือข่ายสาธารณะ ดังต่อไปนี้:<br>• เฉพาะคีย์ที่เชื่อถือได้ และ ได้รับใบรับรองเท่านั้นที่ยอมรับได้<br>• Protocol ที่ใช้ต้องสนับสนุนเฉพาะเวอร์ชั่น หรือการตั้งค่าที่ปลอดภัย<br>• ความเข้มงวดในการเข้ารหัสเหมาะสมเพียงพอสำหรับวิธีการเข้ารหัสที่ใช้อยู่<br>ตัวอย่างของที่เปิดโล่ง และเครือข่ายสาธารณะ มีดังนี้ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้):<br>• อินเทอร์เน็ต<br>• เทคโนโลยีไร้สาย รวมทั้ง *802.11* และ *Bluetooth*<br>• เทคโนโลยี *Cellular* ตัวอย่างเช่น *GSM* และ *CDMA*<br>• *General Packet Radio Service (GPRS)*<br>• การสื่อสารผ่านดาวเทียม | 4.1.a ระบุตำแหน่งทั้งหมดที่ข้อมูลผู้ถือบัตรถูกส่ง หรือ ได้รับผ่านทางที่เปิดโล่งเครือข่ายสาธารณะ ตรวจสอบเอกสารมาตรฐาน และ เปรียบเทียบกับการตั้งค่าระบบเพื่อตรวจสอบการใช้งาน Protocol ความปลอดภัย และการเข้ารหัสที่เข้มงวดสำหรับทุกสถานที่<br>4.1.b ตรวจทานเอกสารนโยบายและกระบวนการ เพื่อตรวจสอบกระบวนดังนี้:<br>• เพื่อ การยอมรับเฉพาะคีย์ที่ไว้ใจได้ และ/หรือ ที่มีใบรับรอง<br>• เพื่อ Protocol ที่ใช้งานสนับสนุนเฉพาะเวอร์ชั่น หรือการตั้งค่าที่ปลอดภัย (ไม่สนับสนุนเวอร์ชั่น หรือ การตั้งค่าที่ไม่ปลอดภัย)<br>• เพื่อการดำเนินการให้เหมาะสมตามการเข้ารหัสที่เข้มงวดสำหรับแต่ละวิธีการที่ใช้<br>4.1.c เลือกและสังเกตตัวอย่างของการส่งข้อมูล เข้าและออกในขณะดำเนินการเพื่อตรวจสอบว่า ข้อมูลผู้ถือบัตรทั้งหมดมีการเข้ารหัสที่เข้มงวดไว้ระหว่างการส่ง<br>4.1.d ตรวจสอบคีย์ และ ใบอนุญาต เพื่อตรวจสอบว่าเฉพาะคีย์ที่ไว้ใจได้ และ/หรือ ใบอนุญาต ที่ได้รับการยอมรับ<br>4.1.e ตรวจสอบการตั้งค่าระบบ เพื่อตรวจสอบว่า Protocol ได้ดำเนินการตามการตั้งค่าที่ปลอดภัยและไม่สนับสนุนเวอร์ชั่น หรือ การตั้งค่าที่ไม่ปลอดภัย<br>4.1.f ตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่าการเข้ารหัสที่เข้มงวดได้ถูกนำมาใช้สำหรับแต่ละวิธีการที่ใช้งาน (โปรดดู คำแนะนำจากผู้ขาย/วิธีการที่ดีที่สุด) | ข้อมูลที่สุ่มเสี่ยงจะต้องถูกเข้ารหัสไว้ระหว่างส่งข้อมูลผ่านเครือข่ายสาธารณะ เพราะเป็นการง่าย และเป็นธรรมดาสำหรับผู้ประสงค์ร้ายที่จะขัดขวาง และ/หรือ เปลี่ยนทิศทางข้อมูลระหว่างการส่ง<br>การส่งข้อมูลข้อมูลผู้ถือบัตรอย่างปลอดภัย ต้องการการใช้คีย์ที่ไว้ใจได้/ใบอนุญาต Protocol ที่ปลอดภัยสำหรับการขนส่ง และการเข้ารหัสที่เข้มงวดอย่างเหมาะสมเพื่อเข้ารหัสข้อมูลผู้ถือบัตร การร้องขอการเชื่อมต่อจากระบบ ซึ่งไม่สนับสนุนการเข้ารหัสที่เข้มงวดที่ต้องการ อาจทำให้เกิดการเชื่อมต่อที่ไม่ปลอดภัย ซึ่งไม่ควรได้รับการยอมรับ<br>จำไว้ว่า Protocol การดำเนินการ (เช่น SSL v2.0, SSH v1.0 และ TLS 1.0) มีช่องโหว่ที่เป็นที่รู้จักซึ่งผู้โจมตีสามารถใช้ได้เพื่อเข้าถึงการควบคุมระบบที่มีผลกระทบ ไม่ว่าใช้ Protocol ความปลอดภัยตัวไหนอยู่ก็ตาม ต้องทำให้มั่นใจว่า Protocol ตั้งค่าไว้เพื่อใช้กับเวอร์ชั่นและการตั้งค่าที่ปลอดภัย เพื่อป้องกันการเชื่อมต่อที่ไม่ปลอดภัย เช่น TLS v1.1 หรือสูงกว่า ใบรับรองที่ได้รับผู้ให้ที่เป็นที่รู้จักต่อสาธารณะ และต้องมีการพิจารณาการสนับสนุนเฉพาะการเข้ารหัสที่เข้มงวด<br>ตรวจสอบว่าใบอนุญาตสามารไว้ใจได้ (เช่น ไม่หยดอายุ และอนุญาตจากแหล่งที่เชื่อถือได้) ช่วยในความสมบูรณ์ของการเชื่อมต่อที่ปลอดภัย |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 4.1.g ตรวจสอบการตั้งค่าระบบ สำหรับการใช้งาน SSL/TLS เพื่อตรวจสอบว่า SSL/TLS ได้เปิดใช้งานเมื่อใดก็ตามที่มีการส่ง หรือได้รับ ข้อมูลผู้ถือบัตร<br>เช่น สำหรับการดำเนินการที่มีพื้นฐานจาก browser:<br>• “HTTPS” ปรากฏบน URL และ<br>• ข้อมูลผู้ถือบัตรถูกร้องขอเฉพาะเมื่อ “HTTPS” ปรากฏบน URL | โดยทั่วไป URL ของหน้าเว็บควรเริ่มต้นด้วย "HTTPS" และ/หรือการที่ browser แสดง ไอคอนกุญแจล็อค ผู้ค้าที่มีใบอนุญาต SSL จำนวนมากมักแสดงตราสัญลักษณ์การตรวจสอบที่สามารถเห็นได้ง่าย — บางครั้งอาจเรียกว่า “ตราประทับความปลอดภัย (security seal)” "ตราประทับเว็บไซต์ที่ปลอดภัย (secure site seal)" หรือ “ตราประทับความไว้ใจได้ (secure trust seal)” —ซึ่งสามารถคลิกเข้าไปที่ตราเพื่อแสดงข้อมูลเกี่ยวกับเว็บไซต์ได้ |
| 4.1.1 ทำให้มั่นใจว่าการส่งข้อมูลผ่านเครือข่ายไร้สายของข้อมูลผู้ถือบัตร หรือ เชื่อมโยงไปถึงสิ่งแวดล้อมข้อมูลผู้ถือบัตร ได้ใช้วิธีการแบบอุตสาหกรรม (เช่น IEEE 802.11i) ในการดำเนินการเข้ารหัสอย่างเข้มงวดสำหรับการรับรอง และการส่งข้อมูล<br>หมายเหตุ: ห้ามใช้ WEP ในการควบคุมความปลอดภัย | 4.1.1 ระบุการส่งข้อมูลแบบไร้สายทั้งหมดของ ข้อมูลผู้ถือบัตร หรือเชื่อมโยงไปถึงสิ่งแวดล้อมข้อมูลผู้ถือบัตร ตรวจสอบเอกสารมาตรฐานและเปรียบเทียบกับการตั้งค่าระบบ เพื่อตรวจสอบเงื่อนไขดังนี้:<br>• มีการใช้งานวิธีการที่ดีที่สุดของอุตสาหกรรม (เช่น IEEE 802.11i) เพื่อการเข้ารหัสที่เข้มงวดสำหรับการรับรอง และการส่งข้อมูล<br>• ไม่มีการใช้การเข้ารหัสที่อ่อนแอ (เช่น WEP, SSL เวอร์ชั่น 2.0 หรือเก่ากว่า) เพื่อควบคุมความปลอดภัยสำหรับการรับรอง และการส่งข้อมูล | ผู้ใช้ที่ประสงค์ร้าย ใช้อุปกรณ์ฟรีที่มีให้ใช้ทั่วไปเพื่อ ดักจับ การเชื่อมต่อไร้สาย การใช้การเข้ารหัสที่เข้มงวดช่วยจำกัดการเปิดเผยข้อมูลที่สุ่มเสี่ยงบนเครือข่ายไร้สายได้<br>การเข้ารหัสที่เข้มงวดสำหรับการรับรอง และการส่งข้อมูลผู้ถือบัตรนั้นจำเป็น เพื่อป้องกันผู้ประสงค์ร้ายจากการได้รับสิทธิการเข้าถึงเครือข่ายไร้สาย หรือ ใช้งานเครือข่ายไร้สายเพื่อเข้าถึงเครือข่ายภายใน หรือ ข้อมูลอื่นๆ |
| 4.2 ห้ามส่ง PAN ที่มีมีการป้องกันด้วยวิธีการ ส่งข้อความไปยังลูกค้า (end-user) (เช่น e-mail, ส่งข้อความทันที (instant message), chat, และอื่นๆ). | 4.2.a หากมีการใช้การ ส่งข้อความไปยังลูกค้า (end-user)ในการส่งข้อมูลผู้ถือบัตร, สังเกตกระบวนการการส่ง PAN และ ตรวจสอบตัวอย่างการส่งข้อมูลออก เพื่อตรวจสอบว่า PAN ได้รับการ render ให้ไม่สามารถอ่านได้ หรือ ปกป้องไว้ด้วยการเข้ารหัสที่เข้มงวดเมื่อใดก็ตามที่ทำการส่งไปด้วยเทคโนโลยีการส่งข้อความ (messaging technology) | E-mail, การส่งข้อความทันที (instant messaging), และ แชท (chat) สามารถถูกดักข้อมูลได้ง่ายโดยการดักข้อมูล (packet-sniffing) ระหว่างการส่งข้อมูลผ่านเครือข่าย ภายใน และ ภายนอก อย่าใช้ อุปกรณ์ส่งข้อความเหล่านี้ในการส่ง PAN เว้นแต่ว่าได้รับการตั้งค่าให้เข้ารหัสอย่างเข้มงวดแล้ว |
| | 4.2.b ตรวจทานเอกสารนโยบายเพื่อตรวจสอบว่ามีนโยบายที่ครอบคลุมให้ไม่สามารถส่ง PAN ด้วยเทคโนโลยีการส่งข้อความ (messaging technology) ไปยังลูกค้า (end-user) ได้ | |
| 4.3 ทำให้มั่นใจว่าทำให้มั่นใจว่านโยบายความปลอดภัย และขั้นตอนการดำเนินการสำหรับ การเข้ารหัสการส่งข้อมูล ของ ข้อมูลผู้ถือบัตร ได้รับการจัดทำเป็นเอกสาร ใช้งาน และเป็นที่รู้จักกับผู้ที่มีผลกระทบ | 4.3 ตรวจสอบเอกสาร สัมภาษณ์บุคลากรเพื่อตรวจสอบว่า นโยบายความปลอดภัย และขั้นตอนการดำเนินการ for เข้ารหัสการส่งข้อมูล of ข้อมูลผู้ถือบัตร are:<br>• จัดทำเป็นเอกสารแล้ว<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักกับผู้ที่มีผลกระทบ | บุคลากรจะต้องตระหนัก นโยบายความปลอดภัย และ ขั้นตอนการดำเนินการดังต่อไปนี้ เพื่อจัดการความปลอดภัยในการส่งข้อมูลผู้ถือบัตรอย่างต่อเนื่อง |

# ปรับปรุงโปรแกรมจัดการช่องโหว่

**ความต้องการที่ 5: ปกป้องระบบทั้งหมดจาก malware และ อัพเดท software หรือ program ป้องกันไวรัสอยู่เป็นประจำ**

Software ประสงค์ร้าย หรือมักเรียกว่า “malware” — ได้แก่ ไวรัส worm และ Trojan — เข้ามาสู่เครือข่ายระหว่างธุรกิจมากมาย – กิจกรรมที่ได้รับอนุญาต รวมทั้ง e-mail ลูกจ้าง และการใช้งาน อินเทอร์เน็ต คอมพิวเตอร์เคลื่อนที่ และอุปกรณ์เก็บข้อมูล ทำให้เกิดการใช้ประโยชน์จากช่องโหว่ของระบบ Software ป้องกันไวรัส จะต้องถูกใช้งานบนระบบทั้งหมดที่มักได้รับผลกระทบจาก malware เพื่อปกป้องระบบจาก การโจมตีของ software ที่ประสงค์ร้ายทั้งปัจจุบัน และที่อาจวิวัฒนาการในอนาคต นอกจากนั้น การจัดการมัลแวร์ (anti-malware) ควรได้รับการพิจารณาเป็นส่วนสนับสนุนให้กับ Software ป้องกันไวรัส; อย่างไรก็ตาม ทางเลือกเพิ่มเติมเหล่านี้ไม่ได้แทนที่ความต้องการในการใช้งาน software ป้องกันไวรัส

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 5.1 ใช้งาน software ป้องกันไวรัสบนระบบทั้งหมดที่มักได้รับผลกระทบจาก malware (โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ส่วนบุคคลและเซิร์ฟเวอร์) | 5.1 สำหรับตัวอย่างของส่วนประกอบระบบ รวมทั้ง ระบบปฏิบัติการทุกรูปแบบ ที่มักได้รับผลกระทบจาก software ที่ประสงค์ร้าย ตรวจสอบว่า software ป้องกันไวรัสถูกนำไปใช้ | ผู้โจมตีจะมีการโจมตีอย่างหนาแน่นโดยการใช้ประโยชน์จากข้อมูลที่ถูกเผยแพร่ หรือมักเรียกว่า "zero day" (การโจมตีโดยใช้ประโยชน์จากช่องโหว่ที่รู้จากครั้งก่อน) กับระบบที่ปลอดภัย หากไม่มีการป้องกันไวรัสซึ่งอัพเดทเป็นประจำ Software ประสงค์ร้ายรูปแบบที่ใหม่เหล่านี้จะสามารถโจมตี ปิดการใช้งานเครือข่าย หรือ นำไปสู่การเจาะข้อมูลได้ |
| 5.1.1 ทำให้มั่นใจว่าโปรแกรมป้องกันไวรัส สามารถตรวจหา ลบ และ ป้องกัน software ประสงค์ร้ายทั้งหมดที่รู้จักได้ | 5.1.1 ตรวจทานเอกสารของผู้ขาย และตรวจสอบการตั้งค่าการป้องกันไวรัส เพื่อตรวจสอบว่าโปรแกรมป้องกันไวรัสนั้น;<br>• ตรวจพบ Software ที่ประสงค์ร้ายที่รู้จักทั้งหมด<br>• ลบ Software ที่ประสงค์ร้ายที่รู้จักทั้งหมด และ<br>• ป้องกัน Software ที่ประสงค์ร้ายที่รู้จักทั้งหมด<br>ตัวอย่างประเภทของ Software ที่ประสงค์ร้าย ได้แก่ ไวรัส Trojan, worm, spyware adware, และ rootkit | เป็นสิ่งสำคัญในการป้องกันระบบจาก Software ที่ประสงค์ร้าย **ทุก** ประเภท และ รูปแบบ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 5.1.2 สำหรับระบบที่ไม่ถูกพิจารณาว่ามักได้รับผลกระทบโดย Software ที่ประสงค์ร้าย ดำเนินการประเมินเป็นระยะๆ เพื่อตรวจสอบ และ ประเมินการวิวัฒนาการการโจมตีของ malware เพื่อยืนยันว่าระบบยังคงไม่ต้องการ software ป้องกันไวรัสอยู่หรือไม่ | 5.1.2 สัมภาษณ์บุคลากรเพื่อตรวจสอบว่า วิวัฒนาการการโจมตีของ malware ได้รับการเฝ้าระวัง และประเมิน สำหรับระบบที่ปัจจุบันพิจารณาว่ามักไม่ได้รับผลกระทบจาก Software ที่ประสงค์ร้าย เพื่อยืนยันว่าระบบยังคงไม่ต้องการ software ป้องกันไวรัสอยู่หรือไม่ | โดยทั่วไปแล้ว Mainframes, คอมพิวเตอร์ระดับกลาง (เช่น AS/400) และระบบที่คล้ายกัน อาจไม่ได้ตกเป็นเป้าหมาย หรือ ได้รับผลกระทบจาก malware เท่าไรนัก อย่างไรก็ตามแนวโน้มอุตสาหกรรมของ Software ที่ประสงค์ร้ายสามารถเปลี่ยนไปได้อย่างรวดเร็ว จึงเป็นสิ่งสำคัญสำหรับองค์กรที่จะตระหนักถึง Malware ใหม่ๆ ซึ่งอาจส่งผลกระทบต่อระบบได้ — เช่น โดยการเฝ้าระวัง ประกาศด้านความปลอดภัยจากผู้ขาย และกลุ่มข่าวสารการป้องกันไวรัส เพื่อกำหนดว่าระบบของตนอยู่ภายใต้อันตรายจาก malware ใหม่ๆ และ malware ที่วิวัฒนาการหรือไม่<br><br>แนวโน้มของ Software ที่ประสงค์ร้ายควรจะรวมอยู่ในการระบุช่องโหว่ใหม่ๆ และวิธีการจัดการกับแนวโน้มใหม่นี้ควรมีการรวมเข้าด้วยกันกับมาตรฐานการตั้งค่าขององค์กร และกลไกการป้องกันเท่าที่จำเป็น |
| 5.2 ทำให้มั่นใจว่ากลไกการป้องกันไวรัสทั้งหมดได้รับการบำรุงรักษาดังนี้:<br>• เป็นปัจจุบัน<br>• แสกนเป็นระยะๆ<br>• สร้างประวัติการตรวจสอบ ซึ่งเก็บรักษาไว้ตามความต้องการ PCI DSS 10.7 | 5.2.a ตรวจสอบนโยบาย และ กระบวนการ เพื่อตรวจสอบว่า software ป้องกันไวรัส และฐานข้อมูลไวรัส(definition) นั้นได้รับการดูแลให้เป็นปัจจุบัน | วิธีการป้องกันไวรัสที่ดีที่สุดก็ยังมีขีดจำกัดในประสิทธิภาพหากหากไม่ได้รับการบำรุงรักษา และทำให้เป็นปัจจุบันด้วยการอัพเดทความปลอดภัย ไฟล์ signature หรือการป้องกัน malware<br><br>ประวัติการตรวจสอบทำให้สามารถเฝ้าระวังกิจกรรมของ ไวรัส และ Malware และกระบวนการตอบโต้ malware ดังนั้นจึงมีความจำเป็นที่ วิธีการป้องกัน malware จะต้องตั้งค่าเพื่อให้สร้างประวัติการตรวจสอบ และประวัติเหล่านั้นจะถูกจัดการตามความต้องการที่ 10 |
| | 5.2.b ตรวจสอบ การตั้งค่าการป้องกันไวรัส รวมไปถึงการติดตั้งหลัก (master installation) เพื่อตรวจสอบว่ากลไกการป้องกันไวรัสนั้น:<br>• ตั้งค่าไว้เพื่อดำเนินการอัพเดทอัตโนมัติ และ<br>• ตั้งค่าไว้เพื่อดำเนินการแสกนเป็นระยะๆ | |
| | 5.2.c ตรวจสอบตัวอย่างส่วนประกอบระบบ อันได้ระบบปฏิบัติการทุกรูปแบบที่มักได้รับผลกระทบโดย Software ที่ประสงค์ร้าย เพื่อตรวจสอบว่า:<br>• Software ป้องกันไวรัส และ ฐานข้อมูลไวรัสเป็นปัจจุบัน<br>• มีการแสกนเป็นระยะๆ | |
| | 5.2.d ตรวจสอบ การตั้งค่าการป้องกันไวรัส รวมไปถึงการติดตั้งหลัก (master installation) ของ Software และตัวอย่างส่วนประกอบระบบ เพื่อตรวจสอบว่า:<br>• Software ป้องกันไวรัส ได้เปิดใช้งานการสร้างประวัติ และ<br>• ประวัติถูกจัดเก็บไว้ตามความต้องการ PCI DSS 10.7 | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 5.3 ทำให้มั่นใจว่ากลไกการป้องกันไวรัสดำเนินการอยู่อย่างต่อเนื่อง และไม่สามารถปิดการใช้งานได้ หรือเปลี่ยนแปลงโดยผู้ใช้ เว้นแต่ว่าได้รับการอนุญาตเฉพาะ โดยการจัดการแบบเป็นกรณีไป (case-by-case) ในช่วงเวลาที่จำกัด<br><br>หมายเหตุ: การป้องกันไวรัสอาจมีการปิดการใช้งานชั่วคราว เฉพาะเมื่อมีความต้องการทางเทคนิคตามกฎหมายที่ได้รับการอนุญาตโดยการจัดการแบบเป็นกรณีไปเท่านั้น หากมีความต้องการปิดการใช้งานการป้องกันไวรัสเพื่อเหตุผลเฉพาะ จะต้องได้รับการอนุญาตอย่างเป็นทางการ จะต้องมีกระบวนการความปลอดภัยเพิ่มเติมในระหว่างการปิดใช้งานป้องกันไวรัสเช่นกัน | 5.3.a ตรวจสอบ การตั้งค่าการป้องกันไวรัส รวมไปถึงการติดตั้งหลัก (master installation) ของ software และตัวอย่างของส่วนประกอบระบบ เพื่อตรวจสอบว่า software ป้องกันไวรัสดำเนินการอยู่อย่างต่อเนื่อง<br><br>5.3.b ตรวจสอบ การตั้งค่าการป้องกันรวมไปถึงการติดตั้งหลัก (master installation) ของ software และตัวอย่างของส่วนประกอบระบบ เพื่อตรวจสอบว่า software ป้องกันไวรัสไม่สามารถปิดการใช้ไม่สามารถปิดการใช้งานได้ หรือเปลี่ยนแปลงโดยผู้ใช้ได้<br><br>5.3.c สัมภาษณ์บุคลากรผู้รับผิดชอบ และ สังเกตกระบวนการ เพื่อตรวจสอบว่า software ป้องกันไวรัสไม่สามารถปิดการใช้งานได้ หรือ เปลี่ยนแปลงโดยผู้ใช้ได้ เว้นแต่ว่า ได้รับการอนุญาตเฉพาะโดยการจัดการแบบเป็นกรณีไปในช่วงเวลาที่จำกัด | โปรแกรมป้องกันไวรัสที่ดำเนินการอย่างต่อเนื่อง และไม่สามารถเปลี่ยนแปลงได้ จะช่วยให้การป้องกันที่มั่นคงต่อ malware<br><br>การใช้การควบคุมที่มีพื้นฐานมาจากนโยบาย กับระบบทั้งหมด เพื่อให้มั่นใจได้ว่า การป้องกัน Malware ไม่สามารถเปลี่ยนแปลงได้ หรือ ปิดการใช้งานได้ จะช่วยป้องกันไม่ให้ระบบมีจุดอ่อนจากการใช้งาน Software ที่ประสงค์ร้าย.<br><br>อาจมีความจำเป็นต้องใช้กระบวนการความปลอดภัยเพิ่มเติมอื่นๆ เป็นครั้งคราว ในเวลาที่ การป้องกันไวรัส ไม่ได้เปิดใช้งาน — เช่น การปิดการเชื่อมต่อระบบที่ไม่มีการป้องกันจากอินเทอร์เน็ต ในระหว่างปิดการใช้งานป้องกันไวรัส และทำการแสกนละเอียด (full scan) หลังเปิดการใช้งานอีกครั้งแล้ว |
| 5.4 ทำให้มั่นใจว่า นโยบายความปลอดภัย และขั้นตอนการดำเนินการ สำหรับปกป้องระบบจาก malware ได้รับการจัดทำเป็นเอกสาร มีการใช้งาน และเป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 5.4 ตรวจสอบ การจัดทำเป็นเอกสาร และสัมภาษณ์บุคลากรเพื่อตรวจสอบว่า นโยบายความปลอดภัยและขั้นตอนการดำเนินการสำหรับการป้องกันระบบจาก malware นั้น:<br>• ได้รับการจัดทำเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรจะต้องตระหนักถึง และดำเนินการตามนโยบายความปลอดภัย และขั้นตอนการดำเนินการเพื่อให้มั่นใจว่าระบบได้รับการป้องกันจาก malware อย่างต่อเนื่อง |

# ความต้องการที่ 6: พัฒนาและปรับปรุงระบบและแอปพลิเคชั่นรักษาความปลอดภัย

บุคคลที่ไม่มีศีลธรรมใช้ช่องโหว่ของความปลอดภัยเพื่อเสาะหาสิทธิการเข้าถึง ช่องโหว่เหล่านี้จะถูกปรับปรุงโดยผู้ขาย – ให้เห็น Patch ความปลอดภัย ซึ่งจะต้องมีการติดตั้งโดยหน่วยงาน ซึ่งจัดการระบบ ระบบทั้งหมดจะต้องมี Patch ที่เหมาะสมทั้งหมดของ software เพื่อป้องกันการถูกใช้ประโยชน์ในทางที่ผิด และการเจาะข้อมูลผู้ถือบัตรโดยผู้ประสงค์ร้าย และ Software ที่ประสงค์ร้าย

หมายเหตุ: ***Patch*** ที่เหมาะสม คือ ***Patch*** ที่ได้รับการประเมิน และทดสอบเพียงพอที่จะตัดสินว่า ***Patch*** นั้นไม่ได้สร้างความขัดแย้งให้กับการตั้งค่าความปลอดภัยปัจจุบัน สำหรับแอปพลิเคชั่นที่พัฒนาขึ้นเองภายในองค์กร จะสามารถหลีกเลี่ยงช่องโหว่ส่วนมากได้โดยการใช้งานกระบวนการพัฒนาระบบมาตรฐาน และ เทคนิคการ coding ที่ปลอดภัย

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.1 สร้างกระบวนการเพื่อตรวจสอบช่องโหว่ของความปลอดภัยโดยใช้แหล่งข้อมูลภายนอกที่มีชื่อเสียง และจัดอันดับความเสี่ยง (เช่น “สูง” “ปานกลาง” หรือ “ต่ำ”) ให้กับช่องโหว่ที่ค้นพบใหม่<br><br>หมายเหตุ: การจัดอันกับความเสี่ยงควรจะมีพื้นฐานมาจากวิธีการที่ดีที่สุดของอุตสาหกรรม และ การพิจารณาถึงผลกระทบที่อาจเกิด เช่น การแยกประเภทการจัดอันดับ อาจมีการพิจารณา คะแนน *CVSS base score* และ/หรือ การแยกแยะโดยผู้ขาย และ/หรือ ประเภทของระบบที่กระทบ วิธีการที่ใช้ในการประเมินช่องโหว่ และ การจัดอันกับความเสี่ยง อาจต่างออกไป ขึ้นอยู่กับวิ่งแวดล้อมขององค์กร และแผนการประเมินผลความเสี่ยง การจัดอันดับความเสี่ยง อย่างน้อยที่สุด ควรจะระบุช่องโหว่ทั้งหมดที่ถือว่า “มีความเสี่ยงสูง” ได้ นอกจากนั้น ช่องโหว่อาจถูกพิจารณาว่า “ร้ายแรง” หากช่องโหว่เหล่านั้นมีความเสี่ยงที่ใกล้ชิดกับสิ่งแวดล้อม และส่งผลกระทบต่อระบบหลัก และ/หรือ อาจทำให้เกิดความเสี่ยงในการเจาะข้อมูลหากไม่ได้รับการจัดการ ตัวอย่างของระบบหลัก อาจรวมไปถึง ระบบความปลอดภัย อุปกรณ์ที่เปิดเผยต่อสาธารณะ และ ระบบฐานข้อมูล และ ระบบอื่นๆซึ่งจัดเก็บ ดำเนินการ และส่งข้อมูลผู้ถือบัตร | 6.1.a ตรวจสอบนโยบายและกระบวนการเพื่อตรวจสอบว่า กระบวนการได้กำหนดไว้ดังเงื่อนไขต่อไปนี้:<br>• เพื่อระบุช่องโหว่ใหม่ๆ<br>• เพื่อจัดอันดับความเสี่ยงของช่องโหว่ซึ่งรวมไปถึงช่องโหว่ที่ “มีความเสี่ยงสูง” และ “ร้ายแรง”<br>• เพื่อใช้งาน แหล่งข้อมูลภายนอกที่มีชื่อเสียงสำหรับข้อมูลช่องโหว่ความปลอดภัย<br><br>6.1.b สัมภาษณ์บุคลากรที่รับผิดชอบ และสังเกตกระบวนการ เพื่อตรวจสอบว่า:<br>• ช่องโหว่ใหม่ได้รับการระบุ<br>• การจัดอันดับความเสี่ยงได้มีการระบุช่องโหว่ที่ “มีความเสี่ยงสูง” และ “ร้ายแรง”<br>• กระบวนการเพื่อระบุช่องโหว่ใหม่ ได้ใช้งาน แหล่งข้อมูลภายนอกที่มีชื่อเสียงสำหรับข้อมูลช่องโหว่ความปลอดภัย | จุดประสงค์ของความต้องการนี้คือการให้องค์กรได้อัพเดทช่องโหว่ใหม่ซึ่งอาจส่งผลกระทบต่อสิ่งแวดล้อมของพวกเขาได้<br><br>แหล่งข้อมูลสำหรับช่องโหว่ควรจะเชื่อถือได้ และ ได้ระบุเว็บไซต์ผู้ขาย กลุ่มข่าวสารอุตสาหกรรม รายการจดหมาย(mailing list) หรือRSS feeds ไว้<br><br>เมื่อองค์กรได้ทำการระบุช่องโหว่ซึ่งอาจกระทบต่อสิ่งแวดล้อม ความเสี่ยงที่ช่องโหว่มีจะต้องถูกประเมิน และจัดอันดับ องค์กรจะต้องมีวิธีการประเมินช่องโหว่อย่างต่อเนื่อง และจัดอันดับช่องโหว่เหล่านั้น สิ่งนี้ไม่ได้ถูกดำเนินการโดย การแสกน ASV หรือการแสกนช่องโหว่ภายใน นอกจากนั้นยังต้องการกระบวนการเพื่อการเฝ้าตรวจตราแหล่งข้อมูลช่องโหว่ของอุตสาหกรรมอย่างต่อเนื่อง<br><br>การแยกแยะความเสี่ยง (เช่น “สูง” “ปานกลาง” หรือ “ต่ำ”) ช่วยให้องค์กรสามารถระบุได้ถึงลำดับความสำคัญ และจัดการกับความเสี่ยงที่สูงที่สุดก่อน และลดความเป็นไปได้ที่ความเสี่ยงที่สูงที่สุดจะถูกนำไปใช้ในทางที่ผิด |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.2 ทำให้มั่นใจว่าส่วนประกอบระบบ และ Software ทั้งหมดได้รับการปกป้องจากช่องโหว่ที่ไม่รู้จัก โดยการติดตั้ง Patch ความปลอดภัยจากการสนับสนุนของผู้ขายอย่างเหมาะสม ติดตั้ง Patch ความปลอดภัยที่สำคัญภายใน 1 เดือน หลังจาก Patch ออก<br><br>หมายเหตุ: Patch ความปลอดภัยที่สำคัญควรได้รับการระบุตามการจัดอันดับความเสี่ยงที่ระบุในความต้องการ 6.1 | 6.2.a ตรวจสอบนโยบายและกระบวนการที่เกี่ยวข้องกับการติดตั้ง Patch ความปลอดภัยเพื่อตรวจสอบว่ากระบวนการได้กำหนดไว้เพื่อ:<br>• การติดตั้ง Patch ความปลอดภัยจากการสนับสนุนของผู้ขายภายใน 1 เดือนหลังจาก Patch ออก<br>• การติดตั้ง Patch ความปลอดภัยจากการสนับสนุนของผู้ขายภายในกรอบเวลาที่เหมาะสม (เช่น ภายใน 3 เดือน)<br><br>6.2.b ตัวอย่างสำหรับส่วนประกอบระบบและ Software ที่เกี่ยวข้อง เปรียบเทียบรายการ Patch ความปลอดภัยที่ติดตั้งไว้บนแต่ละระบบกับรายการ Patch ล่าสุดจากผู้ขายเพื่อตรวจสอบดังต่อไปนี้:<br>• Patch ความปลอดภัยจากการสนับสนุนของผู้ขายได้รับการติดตั้งภายใน 1 เดือนหลังจาก Patch ออก<br>• Patch ความปลอดภัยจากการสนับสนุนของผู้ขายได้รับการติดตั้งภายในกรอบเวลาที่เหมาะสม (เช่น ภายใน 3 เดือน) | มีการโจมตีอย่างเข้มข้นโดยใช้งานข้อมูลที่ถูกเผยแพร่ ที่มักเรียกกันว่า "zero day" (การโจมตีที่ใช้ช่องโหว่ที่ไม่รู้จักจากครั้งก่อน) ต่อระบบที่มีความปลอดภัย หาก patch ล่าสุดไม่ได้รับการติดตั้งบนระบบสำคัญเร็วที่สุดเท่าที่ทำได้ ผู้ประสงค์ร้ายสามารถใช้สิ่งเหล่านี้ในการโจมตี ปิดระบบ หรือ เข้าถึงข้อมูลที่สุ่มเสี่ยงได้<br><br>จัดอันดับความสำคัญ patch สำหรับโครงสร้างปัจจัยที่สำคัญเพื่อให้มั่นใจว่าระบบและอุปกรณ์ที่มีความสำคัญสูง ได้รับการป้องกันจากช่องโหว่โดยเร็วที่สุดหลังจาก Patch ออก พิจารณาจัดอันดับความสำคัญการติดตั้ง patch เช่นว่า patch ความปลอดภัยสำหรับระบบที่สำคัญ หรือ ที่มีความเสี่ยง ควรได้รับการติดตั้งภายใน 30 วัน และระบบที่มีความเสี่ยงต่ำ ควรมีการติดตั้งภายใน 2-3 เดือน<br><br>ความต้องการนี้ ใช้กับ patch ของ software ทั้งหมดที่มีการติดตั้ง |
| 6.3 พัฒนาความปลอดภัยของแอปพลิเคชั่น software ภายใน และ ภายนอก (รวมไปถึง การเข้าถึงแอปพลิเคชั่นการจัดการที่มีพื้นฐานบนเว็บ) อย่างปลอดภัยดังนี้:<br>• ให้เป็นไปตาม PCI DSS (เช่น การอนุญาตความปลอดภัย และการบันทึกประวัติ)<br>• ให้มีพื้นฐานบนมาตรฐานอุตสาหกรรม และ/หรือ วิธีการที่ดีที่สุด<br>• ใช้มาตรการความปลอดภัยผ่านวัฏจักรการพัฒนา Software (การพัฒนา software life cycle)<br><br>หมายเหตุ: สิ่งเหล่านี้ใช้กับ *software* ทั้งหมดที่พัฒนาภายในรวมไปถึง ที่สั่งทำ หรือ ปรับแต่งเอง ที่พัฒนาโดยบุคคลที่ 3 | 6.3.a ตรวจสอบเอกสารกระบวนการพัฒนา software เพื่อตรวจสอบว่ากระบวนการได้มีพื้นฐานบนมาตรฐานอุตสาหกรรม และ/หรือวิธีการที่ดีที่สุดหรือไม่<br><br>6.3.b ตรวจสอบเอกสารกระบวนการพัฒนา software เพื่อตรวจสอบว่าความปลอดภัยของข้อมูลได้มีอยู่ในวัฏจักร (life cycle)<br><br>6.3.c ตรวจสอบเอกสารกระบวนการพัฒนา software เพื่อตรวจสอบว่า software แอปพลิเคชั่น ได้รับการพัฒนาตาม PCI DSS<br><br>6.3.d สัมภาษณ์ผู้พัฒนา **software** เพื่อตรวจสอบว่าได้มีการดำเนินการตามเอกสารกระบวนการพัฒนา software | หากไม่มีการใช้ความปลอดภัยระหว่างการกำหนดความต้องการ ดีไซน์ การวิเคราะห์ และ กระบวนการทดสอบ ของการพัฒนา software ช่องโหว่ความปลอดภัยสามารถถูกเปิดเผยต่อผู้ประสงค์ร้ายโดยไม่ตั้งใจในขั้นตอนการพัฒนาได้<br><br>การเข้าใจแอปพลิเคชั่นสามารถจัดการข้อมูลที่สุ่มเสี่ยงได้อย่างไร — รวมไปถึง เมื่อจัดเก็บ ส่งข้อมูล และ เมื่ออยู่ในหน่วยความจำ (memory) — จะช่วยให้สามารถระบุได้ว่าส่วนไหนที่ข้อมูลจะต้องได้รับการป้องกัน |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.3.1 ลบบัญชี ID และรหัสผ่านแอปพลิเคชั่น ในขั้นตอนการพัฒนา ทดสอบ ก่อนที่แอปพลิเคชั่นจะถูกนำไปใช้ หรือ ออกสู่ตลาดผู้บริโภค | 6.3.1 ตรวจสอบเอกสารกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบเพื่อตรวจสอบว่า กระบวนการ pre- production (เตรียมการก่อนการจัดทำเป็นผลิตภัณฑ์) และ/หรือ บัญชีปรับแต่งที่ใช้ใน แอปพลิเคชั่น (custom application account), ID และ/หรือ รหัสผ่าน ได้ถูกลบออกไปก่อนเข้าสู่กระบวนการผลิต หรือ ออกสู่ตลาดผู้บริโภค | ลบบัญชี ID และรหัสผ่านแอปพลิเคชั่น ในขั้นตอนการพัฒนา ทดสอบ ออกจากโค้ดของก่อนที่แอปพลิเคชั่นจะถูกนำไปใช้ หรือ ออกสู่ตลาดผู้บริโภค เนื่องจากสิ่งเหล่านี้อาจให้ข้อมูลเกี่ยวกับการทำงานของแอปพลิเคชั่น การมีข้อมูลเหล่านี้ อาจช่วยในการเจาะเข้าแอปพลิเคชั่น และข้อมูลผู้ถือบัตรที่เกี่ยวข้อง |
| 6.3.2 ทบทวนโค้ดปรับแต่งก่อนการปล่อยสู่ตลาดเพื่อระบุช่องโหว่จากโค้ดที่อาจเกิดขึ้น (ด้วยวิธีการด้วยมือ หรือ อัตโนมัติ) เพื่อให้ตรงตามเงื่อนไขต่อไปนี้:<br>• มีการทบทวนการเปลี่ยนแปลงโค้ดโดยผู้ที่ไม่ใช่ผู้เขียน นอกเหนือไปจากการรับข้อมูลจากผู้เขียนโค้ด และโดยผู้มีความรู้ด้านเทคนิคการตรวจทานโค้ด และวิธีการเขียนโค้ดอย่างปลอดภัย<br>• ทบทวนว่าโค้ดได้ถูกพัฒนาตามคำแนะนำในการเขียนโค้ดอย่างปลอดภัย<br>• ทำการแก้ไขให้ถูกต้องอย่างเหมาะสม ก่อนการปล่อย<br>• มีการพิจารณาผลการตรวจทานโค้ด และยอมรับจากการจัดการก่อนการปล่อย<br>*(มีต่อหน้าถัดไป)* | 6.3.2.a ตรวจสอบเอกสารกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าการเปลี่ยนแปลงของโค้ดปรับแต่งทั้งหมดได้รับการตรวจทาน (ด้วยกระบวนการด้วยมือ หรือ อัตโนมัติ) ดังนี้:<br>• มีการตรวจทานการเปลี่ยนแปลงของโค้ด โดยผู้ที่ไม่ใช่ผู้เขียน นอกเหนือไปจากการรับข้อมูลจากผู้เขียนโค้ด และโดยผู้มีความรู้ด้านเทคนิคการตรวจทานโค้ด และวิธีการเขียนโค้ดอย่างปลอดภัย<br>• ทบทวนว่าโค้ดได้ถูกพัฒนาตามคำแนะนำในการเขียนโค้ดอย่างปลอดภัย (โปรดดู ความต้องการ PCI DSS 6.5)<br>• ทำการแก้ไขให้ถูกต้องอย่างเหมาะสม ก่อนการปล่อย<br>• มีการพิจารณาผลการตรวจทานโค้ด และยอมรับจากการจัดการก่อนการปล่อย | ช่องโหว่ความปลอดภัยในโค้ดปรับแต่ง มักถูกนำไปใช้โดยผู้ประสงค์ร้าย เพื่อได้รับสิทธิการเข้าถึงเครือข่าย และเจาะข้อมูลผู้ถือบัตร<br>ผู้มีความรู้ด้านเทคนิคการตรวจทานโค้ด และมีประสบการณ์ในเทคนิคการตรวจทานโค้ด ควรจะต้องเข้ามาเกี่ยวข้องในกระบวนการตรวจทาน การตรวจทานโค้ดควรจะดำเนินการโดยผู้ที่ไม่ใช่ผู้เขียนเองเพื่อการตรวจทานที่เป็นไปตามตรงตามจุดประสงค์ และเป็นเอกเทศน์ เครื่องมือหรือกระบวนการอัตโนมัติ อาจถูกนำมาใช้แทนการตรวจสอบด้วยมือ แต่จำไว้ว่ามันอาจยาก หรือ แทบจะเป็นไปไม่ได้ที่จะสร้างเครื่องมือที่ระบุปัญหาการเขียนโค้ดได้<br>การแก้ไขโค้ดก่อนออกสู่ตลาด ช่วยป้องกันโค้ดจากการถูกเปิดเผยไปยังสิ่งแวดล้อมที่เสียงต่อการถูกนำไปใช้ การเขียนโค้ดที่ผิดพลาดยิ่งเป็นเรื่องยาก และสิ้นเปลืองในการจัดการในภายหลัง<br>รวมการตรวจทานอย่างเป็นทางการ และการเห็นชอบจากการจัดการ ก่อนการปล่อยสู่ตลาด เพื่อทำให้มั่นใจว่าโค้ดได้รับการอนุมัติ และได้รับการพัฒนาตามนโยบาย และกระบวนการ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| หมายเหตุ: ความต้องการในการตรวจทานโค้ดนี้ ใช้งานกับโค้ดปรับแต่งทั้งหมด (*custom code*) *(*ทั้งที่อยู่ภายในและทั้งที่มองเห็นจากสาธารณะ*)* ในส่วนหนึ่งของวัฏจักรการพัฒนาแอปพลิเคชั่น การตรวจทานโค้ดสามารถทำได้โดยผู้มีความรู้ที่เป็นบุคลากรภายใน หรือ ภายนอก ส่วนเว็บแอปพลิเคชั่นที่มองเห็นจากสาธารณะเป็นส่วนที่ต้องมีการควบคุมเพิ่มเติมเพื่อคอยเฝ้าระวังจากการจู่โจม และช่องโหว่อย่างต่อเนื่องตามความต้องการ *PCI DSS 6.6* | 6.3.2.b เลือกตัวอย่างของการปรับแต่งแอปพลิเคชั่นล่าสุด และตรวจสอบว่าโค้ดปรับแต่งนั้นได้รับการตรวจทานตามความต้องการ 6.3.2.a ด้านบน | |
| 6.4 ติดตามกระบวนการและขั้นตอนควบคุมการเปลี่ยนแปลงทั้งหมด สำหรับการเปลี่ยนแปลงต่อส่วนประกอบระบบ ให้เป็นไปตามดังต่อไปนี้: | 6.4 ตรวจสอบนโยบายและกระบวนการเพื่อตรวจสอบว่าเป็นไปตามดังต่อไปนี้:<br>• สิ่งแวดล้อมการพัฒนา/ทดสอบ แยกจากสิ่งแวดล้อมผลิตภัณฑ์ด้วยการการควบคุมการเข้าถึงที่บังคับใช้แยกจากกัน<br>• แยกภาระหน้าที่ของบุคลากรในสิ่งแวดล้อมการพัฒนา/ทดสอบ กับ ผลิตภัณฑ์ออกจากกัน<br>• ข้อมูลผลิตภัณฑ์ (live PAN) จะต้องไม่ถูกนำไปใช้ในการทดสอบหรือ พัฒนา<br>• ลบข้อมูลการทดสอบ และบัญชี ก่อนออกสู่ตลาด<br>• จัดทำเอกสารการเปลี่ยนกระบวนการควบคุม ที่เกี่ยวข้องตามแพทช์ความปลอดภัย | หากไม่มีเอกสารและการดำเนินการควบคุมการเปลี่ยนแปลงที่เหมาะสมแล้ว ความสามารถด้านความปลอดภัยอาจไม่สามารถทำงานได้ปกติทั้งด้วยความไม่ตั้งใจ และตั้งใจ ความผิดปรกติในกระบวนการประมวลผลอาจเกิดขึ้น หรือ โค้ดที่มุ่งร้ายอาจเกิดขึ้นได้ |
| 6.4.1 แยกสิ่งแวดล้อมการพัฒนา/ทดสอบออกจากสิ่งแวดล้อมผลิตภัณฑ์ และบังคับใช้การควบคุมการเข้าถึงที่แยกจากกัน | 6.4.1.a ตรวจสอบเอกสารเครือข่าย และการตั้งค่าอุปกรณ์เครือข่าย เพื่อตรวจสอบว่าการพัฒนา/ทดสอบ ได้แยกจากสิ่งแวดล้อมผลิตภัณฑ์หรือไม่<br><br>6.4.1.b ตรวจสอบการตั้งค่าการควบคุมการเข้าถึง เพื่อตรวจสอบว่า ใช้งานได้ เพื่อบังคับใช้ให้สิ่งแวดล้อมการพัฒนา/ทดสอบ แยกจากผลิตภัณฑ์ | เนื่องจากการเปลี่ยนแปลงอย่างต่อเนื่องในช่วงการพัฒนาและทดสอบ สิ่งเหล่านั้นอาจมีความปลอดภัยน้อยกว่าสิ่งแวดล้อมผลิตภัณฑ์ หากไม่มีการแยกจากกันแล้ว อาจเป็นไปได้ที่จะเกิดการเจาะข้อมูลผู้ถือบัตรเนื่องจากการตั้งค่าความปลอดภัยที่เข้มงวดน้อยกว่าซึ่งอาจทำให้เกิดช่องโหว่นี้ได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.4.2 แยกหน้าที่ระหว่างการพัฒนา/ทดสอย กับสิ่งแวดล้อมผลิตภัณฑ์ | 6.4.2 สังเกตกระบวนการและสัมภาษณ์บุคลากรที่ได้รับมอบหมายในสิ่งแวดล้อมการพัฒนา/ทดสอบ และบุคลากรที่ได้รับมอบหมายในสิ่งแวดล้อมผลิตภัณฑ์ เพื่อตรวจสอบว่า ได้มีการแบ่งหน้าที่ระหว่าง ทั้ง2สิ่งแวดล้อมหรือไม่ | ลดจำนวนบุคลากรที่มีสิทธิการเข้าถึงสิ่งแวดล้อมผลิตภัณฑ์และข้อมูลผู้ถือบัตรเพื่อลดความเสี่ยงและช่วยทำให้มั่นใจว่าการเข้าถึงนั้นจำกัดไว้เฉพาะผู้ที่มีความต้องการทางธุรกิจในการรับรู้เท่านั้น<br>จุดประสงค์ของความต้องการนี้คือเพื่อแบ่งฟังก์ชั่นการพัฒนาและทดสอบ ออกจากฟังก์ชั่นผลิตภัณฑ์ เช่น ผู้พัฒนาอาจใช้บัญชีระดับผู้ดูแลพร้อมสิทธิระดับสูงในสิ่งแวดล้อมการพัฒนา และ มีบัญชีผู้ใช้ที่มีสิทธิการเข้าถึงระดับปรกติในสิ่งแวดล้อมผลิตภัณฑ์. |
| 6.4.3 ข้อมูลผลิตภัณฑ์ (live PAN) จะต้องไม่ถูกนำไปใช้ในการทดสอบ หรือ พัฒนา | 6.4.3.a สังเกตกระบวนการทดสอบและสัมภาษณ์บุคลากรเพื่อตรวจสอบว่าไม่มีข้อมูลผลิตภัณฑ์ (live PAN)ที่ถูกในไปใช้ในการทดสอบหรือพัฒนา<br>6.4.3.b ตรวจสอบตัวอย่างข้อมูลการทดสอย เพื่อตรวจสอบว่าไม่มีข้อมูลผลิตภัณฑ์ (live PAN) ถูกนำไปใช้ในการทดสอบ หรือ พัฒนา | การควบคุมความปลอดภัยมักจะไม่ได้เข้มงวดในสิ่งแวดล้อมการทดสอบและพัฒนา การใช้ข้อมูลผลิตภัณฑ์ (Production data) อาจทำให้ผู้ประสงค์ร้ายฉวยโอกาสเข้าถึงโดยไม่ได้รับอนุญาตเพื่อเข้าถึงข้อมูลผลิตภัณฑ์ได้(ข้อมูลผู้ถือบัตร) |
| 6.4.4 ลบข้อมูลและบัญชีการทดสอบ ก่อนเปิดให้ใช้งานระบบของผลิตภัณฑ์ | 6.4.4.a สังเกตกระบวนการทดสอบและสัมภาษณ์บุคลากรเพื่อตรวจสอบว่าได้ลบข้อมูลและบัญชีการทดสอบก่อนระบบจะเปิดให้ใช้งานแล้วหรือไม่<br>6.4.4.b ตรวจสอบตัวอย่างข้อมูลและบัญชีจากระบบผลิตภัณฑ์ซึ่งเพิ่งได้รับการติดตั้ง หรือ อัพเดท เพื่อตรวจสอบว่าได้มีการลบข้อมูลและบัญชีการทดสอบก่อนเปิดให้ใช้งานระบบหรือไม่ | ข้อมูลและบัญชีการทดสอบควรจะถูกลบจาก production code ก่อนแอปพลิเคชั่นเปิดให้ใช้งาน เนื่องจากข้อมูลเหล่านี้อาจแสดงถึงการทำงานของแอปพลิเคชั่น หรือ ระบบ หากมีข้อมูลเหล่านี้อาจทำให้สามารถเจาะเข้าระบบและข้อมูลผู้ถือบัตรที่เกี่ยวข้องได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.4.5 เปลี่ยนกระบวนการควรคุมเพื่อดำเนินการตามแพทช์ความปลิดภัยและการปรับแต่งsoftware ให้เป็นไปตามดังต่อไปนี้: | 6.4.5.a ตรวจสอบเอกสารการเปลี่ยนแปลงกระบวนการควบคุมที่เกี่ยวข้อง เพื่อดำเนินการตามแพทช์ความปลอดภัยและการปรับแต่งsoftware และตรวจสอบว่ากระบวนการเป็นไปตามดังต่อไปนี้:<br>• การจัดทำเป็นเอกสารของผลกระทบ<br>• จัดทำเอกสารการอนุญาตการเปลี่ยนแปลงโดยบุคคลที่มีอำนาจ<br>• ทดสอบการทำงาน เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่ได้ส่งผลกระทบต่อความปลอดภัยของระบบ<br>• จัดทำแผนการแก้ไข | หากไม่มีการจัดการที่เหมะสม ผลกระทบจากการอัพเดท software และ patch ความปลอดภัยอาจถูกเปิดเผย และ ทำให้เกิดผมที่ไม่คาดคิดตามมา |
| | 6.4.5.b สำหรับตัวอย่างส่วนประกอบระบบ สัมภาษณ์บุคลากรที่รับผิดชอบเพื่อพิจารณาการเปลี่ยนแปลง/แพทช์ความปลอดภัยล่าสุด ติดตามการเปลี่ยนแปลงเหล่านั้นตามเอกสารการควบคุมการเปลี่ยนแปลงที่เกี่ยวข้อง สำหรับการตรวจสอบแต่ละการเปลี่ยนแปลง ดำเนินการดังนี้: | |
| 6.4.5.1 การจัดทำเอกสารผลกระทบ | 6.4.5.1 ตรวจสอบว่าเอกสารผลกระทบได้รวมอยู่ในการควบคุมการเปลี่ยนแปลงหรือไม่ในแต่ละการเปลี่ยนแปลง | ผลกระทบจากการเปลี่ยนแปลงควรได้รับการบันทึกเป็นเอกสารเพื่อที่ว่าผู้ที่ได้รับผลกระทบทั้งหมดจะสามารถวางแผนสำหรับการเปลี่ยนแปลง |
| 6.4.5.2 จัดทำเอกสารการอนุญาตการเปลี่ยนแปลงโดยบุคคลที่มีอำนาจ | 6.4.5.2 ตรวจสอบว่าได้มีการจัดทำเอกสารการอนุญาตการเปลี่ยนแปลงโดยบุคคลที่มีอำนาจหรือไม่ในแต่ละการเปลี่ยนแปลง | การอนุญาตจากบุคคลที่มีอำนาจแสดงให้เห็นว่าการเปลี่ยนแปลงนั้นเป็นไปตามกฎหมาย และได้รับการยินยอมจากองค์กร |
| 6.4.5.3 ทดสอบการทำงาน เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่ได้ส่งผลกระทบต่อความปลอดภัยของระบบ | 6.4.5.3.a สำหรับแต่ละการเปลี่ยนแปลง ตรวจสอบว่าได้มีการดำเนินการทดสอบการทำงานหรือไม่ เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่ได้ส่งผลกระทบต่อความปลอดภัยของระบบ | ทั้งหมดทั้งมวลแล้ว จะต้องมีการดำเนินการทดสอบ เพื่อตรวจสอบว่าความปลอดภัยของระบบไม่ได้ถูกลดลงจากการเปลี่ยนแปลง การทดสอบควรระบุได้ว่าการควบคุมความปลอดภัยทั้งหมดที่มียังใช้งานได้ดี หรือได้รับการแทนที่ด้วยการควรคุมที่เทียบเท่า หรือเข้มงวดขึ้นหลังการเปลี่ยนแปลงไปยังสิ่งแวดล้อม |
| | 6.4.5.3.b สำหรับการเปลี่ยนแปลงโค้ดปรับแต่ง (custom code) ตรวจสอบว่าการอัพเดททั้งหมดได้ถูกทดสอบตามความต้องการ PCI DSS 6.5 ก่อนเปิดให้ใช้งาน | |
| 6.4.5.4 แผนการแก้ไข | 6.4.5.4 ตรวจสอบว่าแผนการแก้ไขได้ถูกเตรียมไว้หรับแต่ละตัวอย่างการเปลี่ยนแปลง | ในแต่ละการเปลี่ยนแปลง ควรมีเอกสารแผนการแก้ไขไว้หากเกิดการผอดพลาด หรือ ผลกระทบต่อแอปพลิเคชั่นหรือระบบ เพื่อให้ระบบสามารถกู้คืนกลับไปยังสถานะก่อนหน้าได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.5 จัดการกับช่องโหว่การเขียนโค้ดในกระบวนการพัฒนา software ดังต่อไปนี้:<br>• ฝึกฝนผู้พัฒนาในเทคนิคการเขียนโค้ดอย่างปลอดภัย รวมไปถึงการหลีกเลี่ยงช่องโหว่ทั่วไป และให้เข้าใจว่ามีการจัดการกับข้อมูลที่สุ่มเสี่ยงอย่างไรในหน่วยความจำ (memory)<br>• พัฒนา แอปพลิเคชั่นบนพื้นฐานคำแนะนำการเขียนโค้ดอย่างปลอดภัย<br>หมายเหตุ: รายการช่องโหว่ใน *6.5.1 - 6.5.10* คือวิธีที่ดีที่สุดในอุตสาหกรรมในเวลาที่ *PCI DSS* เวอร์ชั่นนี้ได้ถูกเผยแพร่ อย่างไรก็ตาม วิธีการที่ดีที่สุดสำหรับจัดการช่องโหว่จะถูกอัพโหลดไว้ *(เช่น คำแนะนำจาก OWASP, SANS CWE Top 25, CERT Secure Coding,* และอื่นๆ*)* จะต้องใช้วิธีการที่ดีที่สุดในเวลาปัจจุบันสำหรับความต้องการเหล่านี้ | 6.5.a ตรวจสอบนโยบายและกระบวนการการพัฒนา software เพื่อตรวจสอบว่าการฝึกฝนเป็นสิ่งที่ต้องทำสำหรับผู้พัฒนาโดยให้มีพื้นฐานบนวิธีการที่ดีที่สุดของอุตสาหกรรมและคำแนะนำ<br>6.5.b สัมภาษณ์ตัวอย่างผู้พัฒนา เพื่อตรวจสอบว่าพวกเขามีความรู้ในการเขียนโค้ดอย่างปลอดภัยหรือไม่<br>6.5.c ตรวจสอบประวัติการฝึกฝน เพื่อตรวจสอบว่าผู้พัฒนา software ได้รับการฝึกฝนเทคนิคการเขียนโค้ดอย่างปลอดภัย รวมไปถึงการหลีกเลี่ยงช่องโหว่ทั่วไปแล้วหรือไม่ และเข้าใจว่ามีการจัดการกับข้อมูลที่สุ่มเสี่ยงอย่างไรในหน่วยความจำ (memory)<br>6.5.d. ตรวจสอบว่ากระบวนการป้องกันแอปพลิเคชั่นได้มีการดำเนินการเพื่อป้องกันช่องโหว่ดังนี้: | Layer แอปพลิเคชั่นนั้นมีความเสี่ยงสูง และอาจตกเป็นเป้าของทั้งภัยจากภายนอกและภายใน<br>ความต้องการ 6.5.1 - 6.5.10 คือการควบคุมอย่างน้อยที่ควรมี และองค์กรควรรวบรวมวิธีการการเขียนโค้อย่างปลอดภัยไว้ ตามความเหมาะสมสำหรับเทคโนโลยีของสิ่งแวดล้อมของพวกเขา<br>ผู้พัฒนาแอปพลิเคชั่นควรได้รับการฝึกฝนอย่างเหมาะสมเพื่อสามารถระบุ และจัดการปัญหาที่เกี่ยวข้องกับช่องโหว่การเขียนโค้กทั่วไป (และอื่นๆ) ได้ การมีทีมงานที่มีความรู้ในคำแนะนำการเขียนโค้ดอย่างปลอดภัยจะช่วยลดช่องโหว่ความปลอดภัยที่เกิดจากวิธีการเขียนโค้ดที่ไม่รัดกุมเพียงพอ การฝึกฝนของผู้พัฒนาอาจจัดขึ้นโดยภายในองค์กร หรือ โดยบุคคลที่3ก็ได้ และควรเหมาะสมสำหรับเทคโนโลยีที่ใช้<br>การเปลี่ยนแปลงวิธีการเขียนโค้ดอย่างปลอดภัยที่ได้รับการยอมรับจากอุตสาหกรรม วิธีการเขียนโค้ดระดับองค์กร และการฝึกฝนผู้พัฒนาควรเป็นปัจจุบัน และทันต่อภัยอันตรายใหม่ๆ — เช่น memory scraping attack (การโจมตีผ่านหน่วยความจำ)<br>ช่องโหว่ที่ระบุไว้ใน 6.5.1 - 6.5.10 ได้กำหนดพื้นฐานอย่างน้อยที่สุดเอาไว้ ขึ้นอยู่กับแต่ละองค์กรที่จะติดตามแนวโน้มช่องโหว่ปัจจุบัน และรวบรวมมาตรการไว้สำหรับวิธีการเขียนโค้ดของพวกเขาเอง |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| หมายเหตุ: *ความต้องการ 6.5.1 - 6.5.6 ด้านล่างใช้กับแอปพลิเคชั่นทั้งหมด (ภายนอก หรือ ภายใน)* | | |
| 6.5.1 การแทรกโค้ด (Injection flaws) โดยเฉพาะกับ SQL อีกทั้งพิจารณาการแทรกโค้ดคำสั่งระบบปฏิบัติการ (OS Command), การแทรกโค้ด LDAP และ XPath รวมทั้ง การแทรกโค้ดอื่นๆ | 6.5.1 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และ สัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่า การแทรกโค้ด (Injection flaws) ได้รับการจัดการด้วยเทคนิคการเขียนโค้ดต่อไปนี้:<br>• ตรวจความถูกต้องของการป้อนค่า (input) เพื่อตรวจสอบว่าข้อมูลผู้ใช้ไม่สามารถเปลี่ยนแปลงความหมายของคำสั่ง (command และ query) ได้<br>• ใช้งานคำสั่งที่กำหนดค่าแล้ว (parameterized queries) | การแทรกโค้ด (Injection flaws) โดยเฉพาะกับ SQL เป็นวิธีที่มักถูกใช้ในการเจาะแอปพลิเคชั่น การแทรกโค้ดเกิดในขณะที่ข้อมูลของผู้ใช้ถูกส่งไปยังตัวแปลคำสั่ง ในฐานะส่วนหนึ่งของคำสั่ง (command และ query) ข้อมูลที่ไม่เป็นมิตรจากผู้โจมตีจะหลอกตัวแปลคำสั่งให้ดำเนินการตามคำสั่งที่ไม่ได้ตั้งใจ หรือ เปลี่ยนข้อมูล และอนุญาตให้ผู้โจมตีจู่โจมส่วนประกอบภายในเครือข่ายผ่านแอปพลิเคชั่นได้ เพื่อที่จะเริ่มการดจมตี เช่น การป้อนข้อมูลเกินขอบเขต (buffer overflow) หรือเพื่อเปิดเผย ข้อมูลที่เป็นความลับ และส่วนการทำงานของ server<br>ข้อมูลจะต้องได้รับการตรวจความถูกต้องก่อนส่งไปยังแอปพลิเคชั่น — เช่น โดยการตรวจสอบอักษร alphabet ทั้งหมด และการผสมผสานระหว่าง อักษร และ อักษรตัวเลข และอื่นๆ |
| 6.5.2 Buffer overflows | 6.5.2 ตรวจสอบ นโยบายและกระบวนการการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าการป้อนข้อมูลเกินขอบเขต (buffer overflow) ได้รับการจัดการด้วยเทคนิคการเขียนโค้ดดังนี้:<br>• ตรวจสอบความถูกต้องของขอบเขตที่พักข้อมูล (buffer)<br>• ตัดทอนเงื่อนไขการป้อนข้อมูล | การป้อนข้อมูลเกินขอบเขต (Buffer overflow) เกิดขึ้นเมื่อแอปพลิเคชั่นไม่มีการตรวจสอบขอบเขตที่เหมาะสมบนพื้นที่พักข้อมูล (buffer) ซึ่งทำให้ข้อมูลถูกผลักออกไปจากหน่วยความจำของ buffer และเข้าไปยังพื้นที่หน่วยความจำการปฏิบัติการ เมื่อสิ่งนี้เกิดขึ้นผู้โจมตีจะสามารถสอดแทรกโค้ดที่ประสงค์ร้ายเข้าไปยัง buffer และผลักให้ข้อมูลนั้นเข้าไปยังหน่วยความจำส่วนปฏิบัติการได้ ด้วยการทำให้หน่วยความจำเกินขอบเขต โค้ดที่ประสงค์ร้ายจะได้รับการดำเนินการ และมักจะเปิดให้ผู้โจมตีควบคุมจากระยะไกลเพื่อเข้าถึงแอปพลิเคชั่น และ/หรือแทรกเข้าระบบได้ |
| 6.5.3 พื้นที่เก็บข้อมูลเข้ารหัสที่ไม่ปลอดภัย | 6.5.3 ตรวจสอบ นโยบายและกระบวนการการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าพื้นที่เก็บข้อมูลเข้ารหัสที่ไม่ปลอดภัยได้รับการจัดการด้วยเทคนิคการเขียนโค้ดดังนี้:<br>• ป้องกันการเข้ารหัสที่บกพร่อง<br>• ใช้อัลกอริทึ่มการเข้ารหัสและคีย์ที่เข้มงวด | แอปพลิเคชั่นที่ไม่ใช้การเข้ารหัสที่เข้มงวดอย่างเหมาะสมจะมีความเสี่ยงในการจัดเก็บข้อมูล และการถูกเปิดเผยข้อมูลสิทธิการรับรอง และ/หรือข้อมูลผู้ถือบัตร หากผู้โจมตีสามารถใช้ประโยชน์จากกระบวนการเข้ารหัสที่อ่อนแอได้ พวกเขาจะสามารถได้รับการเข้าถึงที่อ่านได้ (clear-text) ไปยังข้อมูลที่เข้ารหัส |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.5.4 การสื่อสารที่ไม่ปลอดภัย | 6.5.4 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าการสื่อสารที่ไม่ปลอดภัยได้รับการจัดการด้วยเทคนิคการเขียนโค้ดซึ่งมีการรับรองที่ถูกต้อง และเข้ารหัสการสื่อสารที่สุ่มเสี่ยงทั้งหมด | แอปพลิเคชั่นที่ไม่มีการเข้ารหัสการเดินทางบนเครือข่ายโดยใช้การเข้ารหัสที่เข้มงวดนั้น เสี่ยงที่จะมีการเจาะข้อมูล และเปิดเผยข้อมูลผู้ถือบัตร หากผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่ของกระบวนการเข้ารหัสได้ พวกเขาอาจสามารถเข้าถึงการควบคุมแอปพลิเคชั่น หรือแม้แต่ได้สิทธิการเข้าถึงข้อมูลที่อ่านได้ (clear-text) ไปยังข้อมูลที่เข้ารหัส |
| 6.5.5 การจัดการ error ที่ไม่ถูกต้อง | 6.5.5 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าการจัดการที่ไม่ถูกต้องได้รับการจัดการด้วยเทคนิคการเขียนโค้ดซึ่งไม่ทำให้เกิดการรั่วไหลของข้อมูลจากข้อความ error (error message) (เช่น ให้ข้อมูลทั่วไปแทนที่จะให้ข้อมูลรายละเอียดการ error ที่เฉพาะเจาะจง) | แอปพลิเคชั่นอาจทำให้ข้อมูลการตั้งค่า หรือ การทำงานภายในรั่วไหลได้โดยไม่ได้ตั้งใจ หรือเปิดเผยข้อมูลสิทธิพิเศษได้จากการจัดการ Error ที่ไม่ถูกต้อง ผู้โจมตีสามารถใช้จุดอ่อนนี้เพื่อขโมยข้อมูลที่สุ่มเสี่ยงหรือเจาะระบบด้วยเช่นกัน หากผู้ประสงค์ร้ายสามารถสร้าง error ซึ่งแอปพลิเคชั่นไม่สามารถจัดการได้อย่างถูกต้องแล้ว พวกเขาสามารถเจาะเอาข้อมูลระบบอย่างละเอียดไปได้ และสร้างการปฏิเสธการให้บริการได้ (DoS) ทำให้ระบบความปลอดภัยล้มเหลว หรือทำให้เซิฟเวอร์ crash เช่น ข้อความ "รหัสผ่านที่ป้อนไม่ถูกต้อง" บอกกับผู้โจมตีว่า user ID นั้นถูกต้องแล้ว และพวกเขาจะมุ่งประเด็นไปยังรหัสผ่านเพียงอย่างเดียว ให้ใช้ข้อความทั่วๆไปเช่น "ไม่สามารตรวจสอบข้อมูลได้ " แทน |
| 6.5.6 ช่องโหว่ที่ “มีความเสี่ยงสูง” ทั้งหมดได้รับการระบุโดย กระบวนการระบุช่องโหว่ (ที่ได้กำหนดไว้ในความต้องการ PCI DSS 6.1) | 6.5.6 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าเทคนิคการเขียนโค้ดได้จัดการกับช่องโหว่ที่ “มีความเสี่ยงสูง” ซึ่งอาจทำให้กระทบแอปพลิเคชั่น ดังที่ได้ระบุไว้ในความต้องการ PCI DSS 6.1 แล้ว | ช่องโหว่ที่ได้รับการระบุ จากกระบวนการจัดอันดับความเสี่ยงของช่องโหว่ (ระบุไว้ในความต้องการ 6.1) ส่วนที่ “มีความเสี่ยงสูง” และ ที่กระทบต่อแอปพลิเคชั่น ควรจะได้รับการระบุ และจัดการระหว่างการพัฒนาแอปพลิเคชั่น |
| หมายเหตุ: *ความต้องการ 6.5.7 - 6.5.10 ด้านล่าง ใช้งานกับ web application และ หน้าจอการใช้งานแอปพลิเคชั่น(interface) (ภายใน หรือ ภายนอก):* | | เว็บแอปพลิเคชั่น (Web application) ทั้งภายในและภายนอก (เห็นได้จากสาธารณะ) มีความเสี่ยง และการเกิดการเจาะข้อมูลในแบบที่แตกต่างกันออกไปตามพื้นฐานวิศวกรรม เช่นกันกับส่วนอื่นๆที่เกี่ยวข้อง |
| 6.5.7 การฝังโค้ดบนหน้าเว็บ(Cross-site scripting หรือ XSS) | 6.5.7 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่าการฝังโค้ดบนหน้าเว็บ(Cross-site scripting หรือ XSS) ได้รับการจัดการด้วยเทคนิคการเขียนโค้ดซึ่ง<br>• ตรวจสอบความถูกต้องของค่าทั้งหมดก่อนการรวม<br>• ใช้งานการ เข้ารหัสการส่งออกที่สุ่มเสี่ยง (context-sensitive escaping) | การฝังโค้ดบนหน้าเว็บ (XSS flaws) เกิดขึ้นเมื่อแอปพลิเคชั่นนำข้อมูลที่ผู้ใช้ป้อน ส่งไปยัง web browser โดยไม่มีการตรวจสอบความถูกต้องหรือเปลี่ยนเป็นรหัส (encode) ก่อน XSS ทำให้ผู้โจมตีจัดการกับ script บนหน้าเว็บของผู้ถูกโจมตีได้ ซึ่งทำให้สามารถยึดหน้าเว็บ หรือทำให้เสื่อมเสียได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.5.8 การควบคุมการเข้าถึงที่ไม่ถูกต้อง (เช่น การอ้างถึง object โดยตรงที่ไม่ปลอดภัย การล้มเหลวในการจำกัดการเข้าถึง URL, การสำรวจเส้นทาง directory ,และการล้มเหลวในการจำกัดการเข้าถึงของผู้ใช้ต่อฟังก์ชั่นการทำงาน) | 6.5.8 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่า การควบคุมการเข้าถึงที่ไม่ถูกต้อง — เช่น การอ้างถึง object โดยตรงที่ไม่ปลอดภัย การล้มเหลวในการจำกัดการเข้าถึง URL, การสำรวจเส้นทาง directory — ได้รับการจัดการด้วยเทคนิคซึ่ง:<br>• รับรองความถูกต้องของผู้ใช้<br>• จัดการกับการป้อนข้อมูล (input)<br>• ไม่เปิดเผยการอ้างถึง object ภายในต่อผู้ใช้<br>• จัดการให้หน้าจอการใช้งาน ไม่มีสิทธิการเจ้าถึงฟังก์ชั่นที่ไม่ได้รับอนุญาต | การอ้างถึง object โดยตรงเกิดขึ้นเมื่อผู้พัฒนาเปิดเผย การอ้างอิงถึง object ภายใน เช่นไฟล์, directory, บันทึกฐานข้อมูล, หรือ คีย์ ที่อยู่ในรูปของ URL หรือค่าตัวแปร ผู้โจมตีสามารถใช้การอ้างอิงเหล่านั้นในการเข้าถึง object ต่างๆที่ไม่ได้รับอนุญาตได้<br>บังคับใช้กระบวนการควบคุมการเข้าถึงอย่างต่อเนื่องใน Layer การนำเสนอและส่วนธุรกิจ สำหรับ URL ทั้งหมด บ่อยครั้ง ทางเดียวที่จะสามารถป้องกันฟังก์ชั่นการทำงานที่สุ่มเสี่ยงของแอปพลิเคชั่นได้คือการป้องกันการแสดง ลิงค์ หรือ URL ต่อผู้ใช้ที่ไม่ได้รับอนุญาต ผู้โจมตีสามารถใช้จุดอ่อนนี้ในการเข้าถึง และดำเนินการโดยไม่ได้รับอนุญาต จากการเข้าถึง URL เหล่านั้นโดยตรง<br>ผู้โจมตีอาจสามารถแยกแยะ และไปตามโครงสร้าง directory ของเว็บไซต์ (การสำรวจเส้นทาง directory) จนได้รับสิทธิการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หรือสามารถเข้าไปยังส่วนลึกในส่วนการทำงานของเว็บไซต์ได้<br>หากหน้าจอการใช้งานได้รับสิทธิการเข้าถึงฟังก์ชั่นการทำงานที่ไม่ได้รับอนุญาตได้ การเข้าถึงนี้อาจทำให้ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสิทธิพิเศษส่วนตัว หรือ ข้อมูลผู้ถือบัตรได้ เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่ควรได้รับการอนุญาตให้เข้าถึง object โดยตรงซึ่งอ้างถึงแหล่งข้อมูลที่สุ่มเสี่ยงได้ การจำกัดการเข้าถึงแหล่งข้อมูลจะช่วยป้องกันข้อมูลผู้ถือบัตรจากการถูกเปิดเผยต่อแหล่งที่ไม่ได้รับอนุญาต |
| 6.5.9 ซีเซิร์ฟ (Cross-site request forgery หรือ CSRF) | 6.5.9 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่า cross-site request forgery (CSRF) ได้รับการจัดการด้วยเทคนิคการเขียนโค้ดซึ่งทำให้มั่นใจได้ว่าแอปพลิเคชั่นนั้นจะไม่วางใจข้อมูลการเข้าใช้ และ token ที่ป้อนเข้ามาจากผู้ใช้ผ่าน browser โดยอัตโนมัติ | การโจมตีแบบซีเซิร์ฟ (CSRF) จะบังคับการ logged-on บน browser ของผู้ถูกโจมตี และส่งข้อมูลการร้องขอก่อนการรับรองความถูกต้อง (pre-authenticated) ไปยังช่องโหว่ของเว็บแอปพลิเคชั่น ซึ่งจะทำให้ผู้โจมตีสามารถดำเนินการเปลี่ยนแปลงสถานะการทำงานใดๆก็ตามที่เป้าหมายมีสิทธิได้ (เช่น การอัพเดทรายละเอียดบัญชีผู้ใช้ ทำการซื้อ หรือแม้แต่รับรองความถูกต้องไปยังแอปพลิเคชั่น) |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.5.10 การจัดการ การรับรองและเซสชั่น (session) ที่เสียหาย<br><br>หมายเหตุ: ความต้องการ *6.5.10* คือวิธีการที่ดีที่สุดจนถึง 30 มิถุนายน 2556 หลังจากเป็นส่วนหนึ่งของความต้องการ | 6.5.10 ตรวจสอบ นโยบายและกระบวนการพัฒนา software และสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่า การจัดการ การรับรองและเซสชั่น (session) ที่เสียหายได้รับการจัดการด้วยเทคนิคการเขียนโค้ดซึ่ง:<br><br>● ถือว่า session token (เช่น คุกกี้) นั้น “ปลอดภัย”<br><br>● ไม่เปิดเผย session ID บน URL<br><br>● ใช้มาตรการการหมดเวลา (time-out) ที่เหมาะสม และเวียน (rotation) session ID หลังการล็อคอินสำเร็จ | การจัดการการรับรองและเซสชั่น (session) ที่ปลอดภัย ช่วยป้องกันผู้ไม่ได้รับอนุญาต จากการเจาะข้อมูล ข้อมูลบัญชีประจำตัวตาม กฎหมาย, คีย์, หรือ session token ซึ่งสามารถทำให้ผู้บุกรุกสันนิษฐานตัวตนของผู้ใช้ที่ได้รับอนุญาตได้ |
| 6.6 สำหรับส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะ จัดการภัยอันตรายใหม่ๆ และช่องโหว่อย่างสม่ำเสมอ และทำให้มั่นใจว่าแอปพลิเคชั่นเหล่านี้ได้รับการป้องกันจากการโจมตีที่รู้จักด้วยกระบวนการต่อไปนี้:<br><br>● ตรวจทาน ส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะ ด้วยมือ หรือ เครื่องมือหรือวิธีการประเมินความปลอดภัยของช่องโหว่แอปพลิเคชั่นอัตโนมัติ อย่างน้อยๆปีละครั้ง และหลังจากการเปลี่ยนแปลงใดๆ<br><br>หมายเหตุ: การประเมินนี้ไม่เหมือนกับการแสกนช่องโหว่ที่ดำเนินการในความต้องการ *11.2*<br><br>● ติดตั้ง กระบวนการแก้ปัญหาทางเทคนิคอัตโนมัติซึ่งสามารถตรวจหา และป้องกันการโจมตีที่มีพื้นฐานบนเว็บ (web-based) (เช่น firewall ของเว็บแอปพลิเคชั่น) ไว้เบื้องหน้าส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะ เพื่อตรวจสอบการเดินทางของข้อมูลทั้งหมดอย่างต่อเนื่อง | 6.6 สำหรับส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะ ทำให้มั่นใจว่าได้มีการใช้วิธีการอย่างใดอย่างหนึ่งดังต่อไปนี้:<br><br>● ตรวจสอบเอกสารกระบวนการ สัมภาษณ์บุคลากร และตรวจสอบประวัติการประเมินความปลอดภัยของแอปพลิเคชั่น เพื่อตรวจสอบว่า ส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะได้รับการตรวจทาน — ด้วยมือ หรือ เครื่องมือหรือวิธีการประเมินความปลอดภัยของช่องโหว่แอปพลิเคชั่นอัตโนมัติ — ดังต่อไปนี้:<br>- ดำเนินการอย่างน้อยปีละครั้ง<br>- ดำเนินการหลังจากการเปลี่ยนแปลงใดๆ<br>- ดำเนินการโดยผู้เชี่ยวชาญด้านความปลอดภัยแอปพลิเคชั่น<br>- อย่างน้อย ต้องมีการประเมินช่องโหว่ตามความต้องการ 6.5<br>- ช่องโหว่ทั้งหมดได้รับการแก้ไข<br>- แอปพลิเคชั่นได้รับการประเมินใหม่อีกครั้งหลังการแก้ไข<br>● ตรวจสอบการตั้งค่าระบบและสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่ากระบวนการแก้ไขทางเทคนิคอัตโนมัติ ตรวจพบและป้องกันการโจมตีที่มีพื้นฐานบนเว็บ (web-based) (เช่น firewall ของเว็บแอปพลิเคชั่น) ได้มีการใช้งานดังต่อไปนี้:<br>- ตั้งอยู่เบื้องหน้าส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะเพื่อตรวจจับและป้องกันการโจมตีที่มีพื้นฐานบนเว็บ<br>- ดำเนินการอย่างต่อเนื่อง และ เป็นปัจจุบันเท่าที่จำเป็น<br>- สร้างประวัติการตรวจสอบ<br>- ตั้งค่าให้ปิดกั้นการโจมตีที่มีพื้นฐานบนเว็บ หรือสร้างการแจ้งเตือน | ส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะ คือเป้าหมายหลักของผู้โจมตี และการเขียนโค้ดที่ไม่ดีพอจะทำให้ผู้โจมตีมีหนทางที่จะได้รับสิทธิการเข้าถึงข้อมูลที่สุ่มเสี่ยงและระบบได้ ความต้องการสำหรับการตรวจทานแอปพลิเคชั่น ก่อนการติดตั้ง firewall ของเว็บแอปพลิเคชั่น มีจุดประสงค์เพื่อลดความเป็นไปได้จากการเจา ส่วนเว็บแอปพลิเคชั่นที่เปิดเผยต่อสาธารณะจากโค้ดหรือวิธีการจัดการแอปพลิเคชั่นที่ไม่ดีพอ<br><br>● ตรวจทานด้วยมือ หรือ ด้วยเครื่องมือประเมินความปลอดภัยช่องโหว่อัตโนมัติ และ/หรือ ทดสอบช่องโหว่แอปพลิเคชั่น<br><br>● Firewall ของเว็บแอปพลิเคชั่น กรอง และ ปิดกั้นการส่งข้อมูลที่ไม่จำเป็นบน layer ของแอปพลิเคชั่นร่วมกับfirewall เครือข่าย การตั้งค่า firewall เว็บแอปพลิเคชั่นที่เหมาะสมจะช่วยป้องกันการโจมตี application-layer หากแอปพลิเคชั่นนั้นได้รับการ coding หรือ การตั้งค่าอย่างเหมาะสม<br><br>หมายเหตุ: “องค์กรที่มีความเชี่ยวชาญในด้านความปลอดภัยแอปพลิเคชั่น” อาจเป็นองค์กรบุคคลที่3 หรือ องค์กรภายในก็ได้ ตราบใดที่ผู้ตรวจทานมีความสามารถเชี่ยวชาญในด้านนี้ และสามารถแสดงให้เห็นได้ว่าเป็นอิสระจากทีมผู้พัฒนา |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 6.7 ทำให้มั่นใจว่า นโยบายความปลอดภัยและขั้นตอนการดำเนินการ สำหรับการพัฒนา และบำรุงรักษาความปลอดภัยของระบบและแอปพลิเคชั่น ได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และเป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 6.7 ตรวจสอบเอกสารและสัมภาษณ์บุคลากรเพื่อตรวจสอบว่า นโยบายความปลอดภัยและขั้นตอนการดำเนินการสำหรับการพัฒนาและบำรุงรักษาความปลอดภัยระบบและแอปพลิเคชั่นนั้น:<br>• ได้รับการบันทึกเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรจะต้องตระหนักถึง และ ดำเนินการตามนโยบายความปลอดภัยและขั้นตอนการดำเนินการเพื่อให้มั่นใจว่าระบบและแอปพลิเคชั่น ได้รับการพัฒนาอย่างปลอดภัย และได้รับการปกป้องจากช่องโหว่อย่างต่อเนื่อง |

# ดำเนินการประเมินการควบคุมการเข้าถึงอย่างเคร่งครัด

## ความต้องการที่ 7: จำกัดการเข้าถึงข้อมูลผู้ถือบัตรเฉพาะความต้องการทางธุรกิจที่ร้องขอ

เพื่อให้มั่นใจว่าข้อมูลที่สุ่มเสี่ยงเข้าถึงได้เฉพาะโดยบุคลากรที่ได้รับอนุญาต ระบบและกระบวนการจะต้องมีการใช้งานในการจำกัดการเข้าถึงโดยยึดพื้นฐานจากความต้องการที่ร้องขอและตามความรับผิดชอบของหน้าที่ "ความต้องการที่ร้องขอ (Need to know)" คือ เมื่อมีการให้สิทธิการเข้าถึงข้อมูลและสิทธิพิเศษจำนวนน้อยที่สุดเพื่อการทำงาน

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 7.1 จำกัดการเข้าถึงส่วนประกอบระบบและข้อมูลผู้ถือบัตรไว้เฉพาะสำหรับผู้ที่มีความต้องการตามหน้าที่ในการเข้าถึง | 7.1 ตรวจสอบเอกสารนโยบายสำหรับการควบคุมการเข้าถึง และตรวจสอบว่านโยบายได้มี 7.1.1 - 7.1.4 ดังนี้:<br>• กำหนดความต้องการในการเข้าถึง และสิทธิพิเศษ สำหรับแต่ละหน้าที่<br>• จำกัดการเข้าถึง ID ผู้ใช้สิทธิพิเศษให้มีน้อยที่สุดเท่าที่จำเป็นต่อการทำงาน<br>• จัดตั้งการเข้าถึงบนพื้นฐานการจำแนกประเภทและการดำเนินงานของบุคลากร<br>• จัดทำเอกสารการอนุมัติ (อิเล็กทรอนิกส์ หรือสิ่งพิมพ์) โดยบุคคลผู้ที่อำนาจสำหรับการเข้าถึงทั้งหมด รวมไปถึงจัดทำรายชื่อสิทธิพิเศษเฉพาะที่ได้รับอนุญาต | ยิ่งมีผู้มีสิทธิการเข้าถึงข้อมูลผู้ถือบัตรมากเท่าไร ยิ่งมีความเสี่ยงมากขึ้นในการที่ข้อมูลจะถูกนำไปใช้ในทางที่ผิด การจำกัดการเข้าถึงสำหรับเฉพาะผู้ที่มีความต้องการทางธุรกิจตามกฎหมาย ช่วยองค์กรในการป้องกันการที่ข้อมูลผู้ถือบัตรจะตกอยู่ในมือผู้ไม่พึงประสงค์ จากความไม่มีประสบการณ์ หรือ การปองร้าย |
| 7.1.1 กำหนดความต้องการการเข้าถึงสำหรับแต่ละหน้าที่ ดังนี้:<br>• ส่วนประกอบระบบและแหล่งข้อมูลซึ่งแต่ละบทบาทต้องการเพื่อเข้าถึงฟังก์ชั่นการทำงาน<br>• ระดับของสิทธิพิเศษที่ต้องการ (เช่น ผู้ใช้ ผู้ดูแล และอื่นๆ) สำหรับการเข้าถึงแหล่งข้อมูล | 7.1.1 เลือกตัวอย่างหน้าที่และตรวจสอบการเข้าถึงเพื่อตรวจสอบว่าแต่ละบทบาทหน้าที่ได้รับการกำหนดและมี:<br>• ส่วนประกอบระบบและแหล่งข้อมูลซึ่งแต่ละหน้าที่ต้องการเข้าถึงเพื่อฟังก์ชั่นการทำงาน<br>• การระบุตัวตนของสิทธิพิเศษที่จำเป็นสำหรับแต่ละหน้าที่เพื่อการทำงาน | เพื่อจำกัดการเข้าถึงข้อมูลผู้ถือบัตรให้เฉพาะผู้ที่ที่มีความต้องการเท่านั้นเป็นสิ่งจำเป็น เพื่อกำหนดความต้องการการเข้าถึงสำหรับแต่ละหน้าที่ (เช่น ผู้ดูแลระบบ เจ้าหน้าที่รับโทรศัพท์ เจ้าหน้าที่คลัง) กำหนด ระบบ/อุปกรณ์/ข้อมูล ที่แต่ละหน้าที่ต้องการเข้าถึง และ กำหนดระดับสิทธิพิเศษเพื่อการดำเนินงานอย่างมีประสิทธิภาพ เมื่อบทบาทหน้าที่และลักษณะความต้องการการเข้าถึงได้รับการกำหนด บุคคลที่ทำหน้าที่นั้นก็จะได้รับสิทธิการเข้าถึงตามที่กำหนดไว้ |
| 7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | 7.1.2.a สัมภาษณ์บุคลากรที่รับผิดชอบการจัดตั้งสิทธิการเข้าถึงเพื่อตรวจสอบว่า การเข้าถึง User ID สิทธิพิเศษ:<br>• มอบหมายให้เฉพาะผู้มีบทบาทที่ต้องการสิทธิการเข้าถึงเท่านั้น<br>• จำกัดสิทธิพิเศษให้น้อยที่สุดเท่าที่จำเป็นต่อหน้าที่ | เป็นสิ่งสำคัญในการมอบ ID สิทธิพิเศษตามแต่ละหน้าที่ของบุคคลเฉพาะที่ต้องการเพื่อการทำงาน ("สิทธิพิเศษที่น้อยที่สุด") เช่น ผู้ดูแลฐานข้อมูล หรือ ผู้ดูแล backup ไม่ควรได้รับการมอบสิทธิเดียวกันกับผู้ดูแลระบบทั้งหมด<br>*(มีต่อหน้าถัดไป)* |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 7.1.2.b เลือกตัวอย่าง user ID ที่มีสิทธิการเข้าถึงพิเศษ และ สัมภาษณ์บุคลากรผู้รับผิดชอบการจัดการ เพื่อตรวจสอบว่าสิทธิพิเศษที่มอบให้นั้น:<br>• จำเป็นสำหรับหน้าที่ของบุคคลนั้นๆ<br>• จำกัดสิทธิให้น้อยที่สุดเท่าที่จำเป็นต่อหน้าที่ | การให้สิทธิน้อยที่สุด ช่วยป้องกันไม่ให้ผู้ใช้ที่รู้เท่าไม่ถึงการณ์เกี่ยวกับแอปพลิเคชั่น เปลี่ยนแปลงการตั้งค่าแอปพลิเคชั่นอย่างไม่ตั้งใจ หรืออย่างไม่ถูกต้อง การบังคับใช้การให้สิทธิที่น้อยที่สุดยังช่วยลดขอบเขตความเสียหายที่อาจเกิดขึ้นเมื่อผู้ไม่ได้รับอนุญาตสามารถเข้าถึง User ID นั้นๆได้ |
| 7.1.3 จัดตั้งสิทธิการเข้าถึงบนพื้นฐานประเภท และลักษณะการดำเนินงานของแต่ละหน้าที่ | 7.1.3 เลือกตัวอย่าง user ID ที่มีสิทธิการเข้าถึงพิเศษ และ สัมภาษณ์บุคลากรผู้รับผิดชอบการจัดการ เพื่อตรวจสอบว่า สิทธิพิเศษได้มอบให้บนพื้นฐานของประเภทและลักษณะการดำเนินงานหรือไม่ | เมื่อความต้องการถูกกำหนดสำหรับแต่ละบทบาทหน้าที่ (ตามความต้องการ PCI DSS 7.1.1) จะเป็นเรื่องง่ายในการให้การเข้าถึงของแต่ละบุคคลตามประเภทงาน และลักษณะการดำเนินงานโดยใช้บทบาทหน้าที่ที่ได้กำหนดไว้แล้ว |
| 7.1.4 ร้องขอเอกสารการอนุมัติ จากบุคคลที่มีอำนาจต่อความต้องการสิทธิพิเศษ | 7.1.4 เลือกตัวอย่างของ user ID และเปรียบเทียบกับเอกสารการอนุมัติเพื่อตรวจสอบว่า:<br>• มีเอกสารการอนุมัติสำหรับสิทธิพิเศษที่จัดตั้ง<br>• การอนุมัติ มาจากผู้มีอำนาจ<br>• สิทธิพิเศษเฉพาะ ตรงกับบทบาทหน้าที่ | เอกสารการอนุมัติ (เช่น รูปแบบสิ่งพิมพ์ หรือ อิเล็กทรอนิกส์) ทำให้มั่นใจว่า ผู้ที่มีการเข้าถึงและสิทธิพิเศษเป็นที่รู้จักและได้รับการอนุญาตโดยการจัดการ และการเข้าถึงของพวกเขาจำเป็นสำหรับการดำเนินงาน |
| 7.2 จัดตั้งระบบการควบคุมการเข้าถึงสำหรับส่วนประกอบระบบซึ่งจำกัดการเข้าถึงบนพื้นฐานความต้องการที่ร้องขอของผู้ใช้แต่ละคนและ ตั้งค่า “ปฏิเสธทั้งหมด” เว้นแต่ได้รับการอนุญาตเฉพาะระบบควรคุมการเข้าถึงนี้จะต้อง: | 7.2 ตรวจสอบการตั้งค่าระบบและเอกสารของผู้ขาย เพื่อตรวจสอบว่าระบบควบคุมการเข้าถึงดำเนินการตามดังต่อไปนี้: | หากไม่มีกลไกการจำกัดการเข้าถึงบนพื้นฐานความต้องการที่ร้องขอของผู้ใช้ ผู้ใช้อาจได้รับการเข้าถึงข้อมูลผู้ถือบัตรด้วยความไม่รู้ ระบบควบคุมการเข้าถึงช่วยดำเนินการกระบวนการจำกัดการเข้าถึงและให้สิทธิพิเศษอย่างอัตโนมัติ นอกจากนั้นค่าตั้งต้น “ปฏิเสธทั้งหมด” ยังช่วยยืนยันว่าจะไม่มีผู้ใดได้สิทธิ จนกว่าและเว้นแต่ จะมีการจัดตั้งกฎเฉพาะให้สามารถได้รับสิทธิการเข้าถึงได้<br>หมายเหตุ: ระบบควบคุมการเข้าถึงบางระบบ มีการตั้งค่าตั้งต้นเป็น “ยอมรับทั้งหมด” ซึ่งก็คือการให้สิทธิ เว้นแต่/จนกว่า จะมีการตั้งกฎเฉพาะเพื่อปฏิเสธ |
| 7.2.1 ครอบคลุมส่วนประกอบระบบทั้งหมด | 7.2.1 ยืนยันว่าระบบควบคุมการเข้าถึงใช้งานบนส่วนประกอบระบบทั้งหมด | |
| 7.2.2 มอบสิทธิให้บุคคลบนพื้นฐาน ประเภทงาน และลักษณะการดำเนินงาน. | 7.2.2 ยืนยันว่าระบบควบคุมการเข้าถึงได้รับการตั้งค่าให้มอบสิทธิพิเศษบนพื้นฐาน ประเภทงาน และลักษณะการดำเนินงาน. | |
| 7.2.3 ค่าตั้งต้นคือ “ปฏิเสธทั้งหมด” | 7.2.3 ยืนยันว่าระบบควบคุมการเข้าถึงมีค่าตั้งต้นเป็น “ปฏิเสธทั้งหมด” | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 7.3 ทำให้มั่นใจว่า นโยบายความปลอดภัยและขั้นตอนการดำเนินการสำหรับการจำกัดการเข้าถึงข้อมูลผู้ถือบัตรได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และเป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 7.3 ตรวจสอบเอกสาร และ สัมภาษณ์บุคลากรเพื่อตรวจสอบว่า นโยบายความปลอดภัยและขั้นตอนการดำเนินการสำหรับจำกัดการเข้าถึงข้อมูลผู้ถือบัตรนั้น:<br>● มีการบันทึกเป็นเอกสาร<br>● มีการใช้งาน และ<br>● เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรจะต้องตระหนัก และดำเนินการตามนโยบายความปลอดภัยและขั้นตอนการดำเนินการ เพื่อทำให้มั่นใจว่าการเข้าถึงทั้งหมดได้รับการควบคุม และอยู่บนบนพื้นฐานความต้องการที่ร้องขอ (need- to-know) และ สิทธิพิเศษที่น้อยที่สุด (least privilege) อย่างต่อเนื่อง |

# ขั้นตอนความต้องการที่ 8: ระบุและตรวจสอบการอนุญาตการเข้าถึงส่วนประกอบระบบ

มอบหมาย ID ที่มีเอกลักษณ์ ให้กับผู้ที่มีสิทธิเข้าถึง เพื่อให้แน่ใจว่าแต่ละคนจะรับผิดชอบในส่วนการกระทำของแต่ละคน เมื่อมีการรับผิดชอบแล้ว การกระทำที่เกี่ยวข้องกับข้อมูลที่สำคัญ และระบบ ถูกดำเนินการโดยผู้ใด สามารถติดตาม รับรู้ได้ถึง ผู้ที่ได้รับอนุญาตและกระบวนการ

ประสิทธิภาพของรหัสผ่าน เป็นสิ่งสำคัญสิ่งหนึ่งที่ต้องพิจารณา โดยการออกแบบ และปฏิบัติของระบบตรวจสอบการอนุญาต — โดยเฉพาะ ความถี่ที่รหัสผ่านถูกป้อน อาจแสดงถึงว่าเป็นการกระทำของผู้โจมตี และ วิธีการทางความปลอดภัย เพื่อป้องกันรหัสผ่านผู้ใช้ เมื่อเข้าระบบ ระหว่างการส่งข้อมูล และ เมื่อทำการจัดเก็บข้อมูล

หมายเหตุ: ความต้องการเหล่านี้สามารถนำไปใช้ได้กับบัญชีทุกบัญชี รวมไปถึง *point-of-sale accounts* พร้อมทั้งความสามารถการดูแลจัดการระบบ และ บัญชีทั้งหมดที่ใช้สำหรับดู หรือ เข้าถึงข้อมูลผู้ถือบัตร หรือ เพื่อเข้าถึงระบบที่มีข้อมูลผู้ถือบัตร นี่รวมไปถึงบัญชีที่ใช้โดยผู้ขาย และบุคคลที่ 3 อื่นๆ *(ตัวอย่าง เช่น เพื่อสนับสนุน หรือบำรุงรักษา)*

อย่างไรก็ตาม ความต้องการ *8.1.1, 8.2, 8.5, 8.2.3 - 8.2.5,* และ *8.1.6 - 8.1.8* นั้นไม่ได้มีจุดประสงค์เพื่อใช้กับบัญชีภายในแอปพลิเคชั่นการชำระเงิน *point-of- sale* ซึ่งมีการเข้าถึงบัตรเพียงหนึ่งใบต่อหนึ่งครั้ง เพื่ออำนวยความสะดวกการทำธุรกรรมเพียงครั้งเดียว (เช่น บัญชีแคชเชียร์)

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.1 กำหนดและดำเนินการนโยบายและกระบวนการเพื่อให้การจัดการการการระบุตัวตนผู้ใช้ที่เหมาะสมสำหรับผู้ใช้ที่ไม่ใช้ลูกค้า (non-consumer) และ ผู้ดูแลระบบ ในส่วนประกอบระบบทั้งหมดดังต่อไปนี้: | 8.1.a ตรวจทาน กระบวนการและยืนยันว่าสิ่งเหล่านั้นได้กำหนดกระบวนการสำหรับแต่ละข้อด้านล่างตั้งแต่ 8.1.1 - 8.1.8 | ด้วยการทำให้มั่นใจว่าแต่ละ user แตกต่างกัน — แทนการใช้ user ID เดียวกันกับลูกจ้างหลายคน — องค์กร สามารถจัดการความรับผิดชอบของแต่ละบุคคลสำหรับ การกระทำและการประเมินผลลัพธ์สำหรับแต่ละบุคคล สิ่งนี้จะช่วยเพิ่มความเร็วในการจัดการปัญหาและตรวจสอบได้หากมีการใช้งานในทางที่ผิดเกิดขึ้น |
| | 8.1.b ตรวจสอบว่ามีการดำเนินการตามประบวนการสำหรับการจัดการการระบุตัวตนโดยการดำเนินการดังนี้: | |
| 8.1.1 มอบหมาย ID ผู้ใช้ที่แตกต่างกัน ก่อนให้สิทธิในการเข้าถึงส่วนประกอบระบบ หรือ ข้อมูลผู้ถือบัตร | 8.1.1 สัมภาษณ์บุคลากรผู้ดูแลระบบเพื่อยืนยันว่าผู้ใช้ทั้งหมด ได้รับ ID ที่แตกต่างกัน สำหรับการเข้าถึงส่วนประกอบระบบ หรือ ข้อมูลผู้ถือบัตร | |
| 8.1.2 ควบคุม การเพิ่ม, การลบ, และการเปลี่ยนแปลง user ID, ข้อมูลส่วนตัว, และ สิ่งที่ระบุตัวตนอื่นๆ | 8.1.2 สำหรับตัวอย่างของ user ID ที่มีสิทธิพิเศษ และ user ID ทั่วไป ตรวจสอบการอนุมัติที่เกี่ยวข้อง และสังเกตกรตั้งค่าระบบ เพื่อตรวจสอบว่าแต่ละ ID ดำเนินการตามเท่าที่สิทธิพิเศษที่บันทึกไว้ในเอกสารมอบให้ | เพื่อให้มั่นใจว่าบัญชีผู้ใช้ที่ได้รับสิทธิการเข้าถึงทั้งหมดนั้นถูกต้อง และรู้จักผู้ใช้ กระบวนการที่เข้มงวดจะต้องจัดการการเปลี่ยนแปลงทั้งหมดที่ไปยัง user ID และข้อมูลการอนุญาตส่วนตัวอื่นๆ รวมไปถึง การเพิ่ม และเปลี่ยนแปลง หรือลบบัญชีที่มีอยู่ |
| 8.1.3 เพิกถอนการเข้าถึงทันทีสำหรับ user ที่สิ้นสุด | 8.1.3.a เลือกตัวอย่างของ user ที่สิ้นสุดใน 6 เดือนที่ผ่านมา และตรวจทานรายการการเข้าถึงของ user ปัจจุบัน — สำหรับการเข้าถึงทั้ง ภายใน และจากทางไกล — เพื่อตรวจสอบว่า ID เหล่านั้นได้ถูกปิดการใช้งาน หรือลบออกจากรายการการเข้าถึงแล้ว | หากลูกจ้างลาออกจากองค์กร และยังสามารถเข้าถึงเครือข่ายจากบัญชีของพวกเขาได้ การเข้าถึงที่ไม่จำเป็น หรือในทางที่ไม่พึงประสงค์สู่ข้อมูลผู้ถือบัตรอาจเกิดขึ้นได้ — ไม่ว่าจะเป็นจากอดีตลูกจ้าง หรือ ผู้ประสงค์ร้ายซึ่งใช้ประโยชน์จากบัญชีเก่า และ/หรือ บัญชีที่ไม่ได้ใช้ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ข้อมูลส่วนตัวผู้ใช้และวิธีการรับรองอื่นๆทั้งหมดจะต้องถูกเพิกถอนทันที (เร็วที่สุดเท่าที่ทำได้) ที่ลูกจ้างออกจากองค์กร |
| | 8.1.3.b ตรวจว่าวิธีการรับรองทางกายภาพทั้งหมด — เช่น smart cards, tokens, และอื่นๆ — ได้รับการส่งคืน หรือ ปิดการใช้งานแล้ว | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.1.4 ลบ/ปิดการใช้งาน ผู้ใช้ที่ไม่มีการใช้งานอย่างน้อยทุกๆ 90 วัน | 8.1.4 สังเกตบัญชีผู้ใช้เพื่อตรวจสอบว่าบัญชีผู้ใช้ที่ไม่มีการใช้งานเกิน 90 วัน ได้รับการปิดการใช้งาน หรือ ลบออก | บัญชีที่ไม่มีการใช้งานบ่อยครั้งมักเป็นเป้าหมายการโจมตีเนื่องจากจะไม่มีการเปลี่ยนแปลงใดๆ (เช่น รหัสผ่าน) จะถูกสังเกตได้ ซึ่งก็คือบัญชีเหล่านี้จะง่ายต่อการนำไปใช้เข้าถึงข้อมูลผู้ถือบัตร |
| 8.1.5 จัดการ ID ที่ใช้โดยผู้ขายเพื่อเข้าถึง สนับสนุน หรือ ปรับปรุงส่วนประกอบระบบผ่านการเข้าถึงระยะไกลดังนี้:<br>• เปิดการใช้งานเฉพาะระหว่างช่วงที่ต้องการใช้ และปิดเมื่อไม่ได้ใช้<br>• เฝ้าติดตามเมื่อมีการใช้งาน | 8.1.5.a สัมภาษณ์บุคลากรและสังเกตกระบวนการจัดการ ID ที่ใช้โดยผู้ขายเพื่อเข้าถึง สนับสนุน หรือ ปรับปรุงส่วนประกอบ เพื่อตรวจสอบว่าบัญชีที่ใช้โดยผู้ขายเพื่อการเข้าถึงระบบไกลนั้น:<br>• ปิดการใช้งานเมื่อไม่ได้ใช้<br>• เปิดการใช้งานเฉพาะระหว่างช่วงที่ผู้ขายต้องการใช้ และปิดเมื่อไม่ได้ใช้ | การอนุญาตให้ผู้ขายสามารถเข้าถึงเครือข่ายของคุณได้ 24 ชั่วโมง ในกรณีที่พวกเขาต้องการสนับสนุนระบบ จะเพิ่มโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต จากทั้งผู้ขายเอง หรือจากผู้ประสงค์ร้ายที่ค้นหาและใช้งานช่องทางที่ เปิดตลอดเวลา นี้เข้าสู่เครือข่ายของคุณ การเปิดการใช้งานเฉพาะช่วงเวลาที่ต้องการ และปิดทันทีที่ไม่ได้ใช้งาน จะช่วยป้องกันการนำการเชื่อมต่อนี้ไปใช้ในทางที่ผิดได้<br>การเฝ้าติดตามการเข้าถึงของผู้ขาย ช่วยให้มั่นใจว่าผู้ขายเข้าถึงเฉพาะระบบที่จำเป็น และเฉพาะกรอบเวลาที่อนุมัติเท่านั้น |
| | 8.1.5.b สัมภาษณ์บุคลากรและสังเกตกระบวนการ เพื่อตรวจสอบว่าได้มีการเฝ้าติดตามบัญชีการเข้าถึงระยะไกลของผู้ขายระหว่างใช้งานหรือไม่ | |
| 8.1.6 จำกัดจำนวนความพยายามการเข้าถึงซ้ำด้วยการล็อค user ID หลังจากความพยายามไม่เกิน 6 ครั้ง | 8.1.6.a สำหรับตัวอย่างของส่วนประกอบระบบ ตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่าตัวแปรการรับรองได้ตั้งค่าไว้ให้มีการล็อค user ID หลังจากความพยายาม log-on ไม่เกิน 6 ครั้ง | หากไม่มีกลไกการล็อคบัญชี ผู้โจมตีสามารถพยายามอย่างต่อเนื่องในการคาดเดารหัสผ่านด้วยมือ หรือ ด้วยเครื่องมืออัตโนมัติได้ (เช่น การเจาะรหัสผ่าน (password cracking)) จนกว่าพวกเขาจะเจาะสำเร็จ และได้สิทธิการเข้าถึงบัญชีนั้นๆ |
| | 8.1.6.b **กระบวนทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจทานกระบวนการภายใน และเอกสารของ ลูกค้า/ผู้ใช้ และสังเกตกระบวนการเพื่อตรวจสอบว่า user ที่ไม่ใช่ลูกค้า (non- consumer) ได้ถูกหลังความพยายาม log-on ไม่เกิน 6 ครั้ง | |
| 8.1.7 ตั้งระยะเวลาการล็อคอย่างน้อย 30 นาที หรือจนกว่าผู้ดูแลระบบจะเปิดการใช้งาน | 8.1.7 สำหรับตัวอย่างของส่วนประกอบระบบ ตรวจสอบการตั้งค่าระบบ เพื่อตรวจสอบว่าค่ารหัสผ่านได้ถูกตั้งไว้ให้มีการล็อค บัญชี และล็อคอยู่อย่างน้อย 30 นาที หรือ จนกว่าผู้ดูแลระบบจะรีเซทบัญชีนั้น | หากมีการล็อคบัญชีจากการพยายามเข้าระบบของบุคคลที่พยายามคาดเดารหัสผ่าน ควบคุมระยะเวลาการเปิดให้ใช้งานใหม่ของบัญชี เพื่อหยุดผู้ประสงค์ร้ายจากการพยายามคาดเดาอย่างต่อเนื่อง (พวกเขาจะต้องรออย่างน้อย 30 นาที จนกว่าบัญชีจะสามารถใช้งานได้อีกครั้ง) นอกจากนั้น หากต้องมีการร้องขอการเปิดให้ใช้งาน ผู้ดูแลระบบ หรือ help desk สามารถตรวจสอบความเป็นเจ้าของบัญชีได้เพื่อการเปิดให้ใช้งานอีกครั้ง |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.1.8 หาก session ไม่มีการเคลื่อนไหวมากกว่า 15 นาที ให้มีการรับรองใหม่ เพื่อเปิดการใช้งานอีกครั้ง | 8.1.8 สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่า ระบบ/session การหมดเวลาจากการไม่มีความเคลื่อนไหว (idle time out feature) ได้ถูกตั้งไว้ที่ 15 นาที หรือน้อยกว่า | เมื่อผู้ใช้เดินออกไปจากอุปกรณ์ที่มีสิทธิการเข้าถึงส่วนประกอบระบบที่สำคัญ หรือข้อมูลผู้ถือบัตร อุปกรณ์นั้นอาจถูกใช้งานโดยผู้อื่น อาจส่งผลให้เกิดการนำไปใช้ในทางที่ผิด<br>การเปิดใช้งานใหม่อีกครั้ง สามารถใช้งานกับระดับระบบได้ เพื่อป้องกัน Session ทั้งหมดที่ทำงานอยู่บนอุปกรณ์ หรือ ในระดับแอปพลิเคชั่น |
| 8.2 นอกจากการมอบ ID ที่แตกต่างกันแล้ว ทำให้มั่นใจว่า มีการจัดการการรับรอง user ที่เหมาะสม สำหรับ user ที่ไม่ใช่ลูกค้า และ การดูแลระบบ บนส่วนประกอบระบบทั้งหมด ด้วยการใช้งานวิธีการอย่างน้อย 1 วิธีดังต่อไปนี้เพื่อเรียกการรับรองความถูกต้องจากผู้ใช้:<br>• สิ่งที่คุณรู้ เช่น รหัสผ่าน หรือ passphrase<br>• สิ่งที่คุณมี เช่น อุปกรณ์ token หรือ smartcard<br>• สิ่งที่เป็น เช่น ข้อมูลทางชีวภาพ (biometric) | 8.2 เพื่อตรวจสอบว่า user ได้มีการรับรองด้วย ID ที่แตกต่าง และ การรับรองเพิ่มเติม (เช่น password/phrase) ในการเข้าถึงสิ่งแวดล้อมข้อมูลผู้ถือบัตร ดำเนินการดังต่อไปนี้:<br>• ตรวจสอบเอกสารที่ให้รายละเอียดวิธีการรับรองที่ใช้งาน<br>• สำหรับการรับรองและส่วนประกอบระบบแต่ละประเภท สังเกตการรับรองเพื่อตรวจสอบความถูกต้องของการรับรองว่าทำงานได้อย่างต่อเนื่องด้วยเอกสารวิธีการรับรอง | วิธีการรับรองเหล่านี้ เมื่อใช้ควบคู่กับ ID ที่แตกต่างกัน จะช่วยป้องกัน users ID จากการเจาะข้อมูล เนื่องจาก ผู้ที่พยายามเจาะเข้ามาจะต้องทราบถึงทั้ง ID ที่มีเอกลักษณ์ และ รหัสผ่าน (หรือการรับรองแบบอื่นๆที่ใช้) จำไว้ว่า ใบรับรองดิจิทัล เป็นทางเลือกหนึ่งที่สามารถใช้ได้ สำหรับ “สิ่งที่คุณมี” ตราบใดก็ตามที่มันแตกต่างออกไปสำหรับผู้ใช้แต่ละคน<br>เนื่องจากหนึ่งในขั้นตอนแรกที่ผู้ประสงค์ร้ายจะเจาะเข้ามา คือการใช้ประโยชน์จากรหัสผ่านที่อ่อนแอ หรือไม่มีรหัสผ่าน จึงเป็นสิ่งสำคัญในการต้องมีกระบวนการจัดการการรับรองที่เหมาะสม |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.2.1 การใช้งานการเข้ารหัสที่เข้มงวด render ข้อมูลการรับรองส่วนตัวทั้งหมด (เช่น passwords/phrases) ให้ไม่สามารถอ่านได้ระหว่างส่งข้อมูลระหว่างการส่ง และ จัดเก็บข้อมูลบนส่วนประกอบระบบทั้งหมด | 8.2.1.a ตรวจสอบเอกสารของผู้ขาย และการตั้งค่าระบบเพื่อตรวจสอบว่ารหัสผ่านได้รับการป้องกันด้วยการเข้ารหัสที่เข้มงวด ระหว่างการส่ง และ จัดเก็บข้อมูล | อุปกรณ์เครือข่ายจำนวนมาก และ แอปพลิเคชั่น ส่งข้อมูลโดยไม่เข้ารหัสและส่งรหัสผ่านที่สามารถอ่านได้ ผ่านเครือข่าย และ/หรือ จัดเก็บรหัสผ่านโดยไม่มีการเข้ารหัส ผู้ประสงค์ร้ายสามารถดักข้อมูลเหล่านั้นได้อย่างง่ายดายระหว่างการส่งข้อมูล โดยใช้ “sniffer (การดักข้อมูล)” หรือ เข้าถึงไฟล์รหัสผ่านโดยตรงในสถานที่ที่จัดเก็บไว้ และใช้ข้อมูลเหล่านั้นเพื่อเข้าถึงอย่างไม่ได้รับอนุญาต |
| | 8.2.1.b สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบไฟล์รหัสผ่าน เพื่อดูว่ารหัสผ่านมีการทำให้ไม่สามารถอ่านได้ระหว่างการจัดเก็บ | |
| | 8.2.1.c สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบการส่งข้อมูลเพื่อดูว่ารหัสผ่านถูกทำให้ไม่สามารถอ่านได้ระหว่างการส่งข้อมูล | |
| | 8.2.1.d **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: สังเกตไฟล์รหัสผ่านเพื่อตรวจสอบว่ารหัสผ่านลูกค้าถูกทำให้ไม่สามารถอ่านได้ระหว่างการจัดเก็บ | |
| | 8.2.1.e **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: สังเกตการส่งข้อมูลเพื่อตรวจสอบว่า รหัสผ่านลูกค้าถูกทำให้ไม่สามารถอ่านได้ระหว่างการส่งข้อมูล | |
| 8.2.2 ตรวจสอบตัวตนของผู้ใช้ ก่อนการเปลี่ยนแปลงข้อมูลส่วนตัวใดๆก็ตาม — เช่น รีเซทรหัสผ่าน จัดหา token ใหม่ หรือ สร้างคีย์ใหม่ | 8.2.2 ตรวจสอบกระบวนการรับรอง สำหรับการเปลี่ยนแปลงข้อมูลส่วนตัว และสังเกตบุคลากรด้านความปลอดภัยเพื่อตรวจสอบว่า หากมีผู้ใช้ร้องขอการรีเซทข้อมูลการรับรองส่วนตัวผ่านทางโทรศัพท์ e-mail เว็บ หรือ อื่นๆที่ไม่มีการแสดงตัวตนจริงๆ (non-face-to-face) จะต้องมีการตรวจสอบผู้ใช้ก่อนเปลี่ยนแปลงข้อมูลเหล่านั้น | ผู้ประสงค์ร้ายจำนวนมาก ใช้ "social engineering ” — เช่น การโทรไปยังศูนย์ช่วยเหลือ (help desk) และแสดงตนเป็นผู้ใช้งานที่ถูกต้อง — เพื่อขอเปลี่ยนรหัสผ่าน เพื่อที่พวกเขาจะได้ใช้ user ID ได้ พิจารณาใช้ “คำถามลับ” ซึ่งเฉพาะบุคคลที่ถูกต้องสามารถตอบได้ เพื่อช่วยให้ผู้ดูแลระบบ สามารถระบุตัวตนผู้ใช้ก่อนการดำเนินการได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.2.3 Passwords/phrases จะต้องเป็นไปตามต่อไปนี้:<br>• ต้องมีความยาวอย่างน้อย7ตัวอักษร<br>• มีทั้งตัวเลข และ ตัวอักษร<br>หรืออีกทางหนึ่ง passwords/phrases จะต้องซับซ้อนและ เข้มงวดเทียบเท่ากับข้อกำหนดด้านบน | 8.2.3a สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่าค่ารหัสผ่านของผู้ใช้ ได้รับการร้องขอให้อย่างน้อย เข้มงวด/ซับซ้อน ดังนี้:<br>• ต้องมีความยาวอย่างน้อย7ตัวอักษร<br>• มีทั้งตัวเลข และ ตัวอักษร | passwords/phrase ที่เข้มงวดคือด่านป้องกันชั้นแรกที่จะป้องกันการเข้าสู่เครือข่าย เนื่องจากผู้ประสงค์ร้ายมักพยายามค้นหาบัญชีที่มีรหัสผ่านที่อ่อนแอ หรือ ไม่มีรหัสผ่าน หากรหัสผ่านสั้น หรือง่ายต่อการคาดเดา จะเป็นเรื่องง่ายสำหรับพวกเขาในการเจาะเข้าระบบโดยบัญชีเหล่านั้น<br>ความต้องการนี้ชี้เฉพาะว่ารหัสผ่านต้องมีความยาวอย่างน้อย7ตัวอักษร และมีทั้งตัวเลข และ ตัวอักษร สำหรับแต่ละกรณีที่ไม่สามารถทำตามเงื่อนไขนี้ได้ ด้วยข้อจำกัดทางเทคนิค หน่วยงานสามารถใช้ “ความเข้มงวดที่เท่าเทียมกัน” ได้ NIST SP 800-63-1 กำหนดให้ “entropy” เป็นมาตรวัดความยากของการคาดเดา หรือ กำหนดรหัสผ่าน หรือ คีย์ เอกสารนี้และอื่นๆที่มีการกล่าวถึง “password entropy” สามารถศึกษาเพิ่มเติมได้เพื่อข้อมูลที่เพิ่มเติมสำหรับการใช้ entropy ที่เหมาะสม และสำหรับการเข้าถึงความแปรปรวนของรหัสผ่านที่มีความเข้มงวดเทียบเท่าสำหรับ passwords/phrases ในรูปแบบที่แตกต่างกัน |
| | 8.2.3.b **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจกระบวนการภายใน และเอกสารของ ลูกค้า/ผู้ใช้ เพื่อตรวจสอบว่า รหัสผ่านของบัญชีที่ไม่ใช่ของลูกค้ามีเงื่อนไขดังต่อไปนี้:<br>• ต้องมีความยาวอย่างน้อย7ตัวอักษร<br>• มีทั้งตัวเลข และ ตัวอักษร | |
| 8.2.4 เปลี่ยน passwords/passphrase ของผู้ใช้อย่างน้อยทุกๆ 90 วัน | 8.2.4.a สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่าค่ารหัสผ่านของผู้ใช้ถูกร้องขอให้มีการเปลี่ยนใหม่อย่างน้อยทุกๆ 90 วัน | Passwords/phrases ซึ่งมีอยู่เป็นเวลานาน โดยไม่มีการเปลี่ยน ทำให้ผู้ประสงค์ร้ายที่มีเวลามาก สามารถเจาะ password/phrase ได้ |
| | 8.2.4.b **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจทานกระบวนการภายในและเอกสารของ ลูกค้า/ผู้ใช้ เพื่อตรวจว่า:<br>• รหัสผ่านของบัญชีที่ไม่ใช่ของลูกค้า มีการร้องขอให้เปลี่ยนใหม่เป็นช่วงๆ; และ<br>• บัญชีที่ไม่ใช่ของลูกค้าได้รับคำแนะนำว่าเมื่อไร และในสถานการณ์ใด ที่ควรเปลี่ยนรหัสผ่าน | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.2.5 ไม่อนุญาตให้ผู้ใดระบุ password/phrase ใหม่ ซึ่งเหมือนกับรหัส 4 ชุดล่าสุดที่เคยใช้มา | 8.2.5.a สำหรับตัวอย่างส่วนประกอบระบบ ขอรับและตรวจสอบการตั้งค่าระบบเพื่อตรวจสอบว่าไม่มีการอนุญาตให้ใช้รหัสเหมือนกับรหัส 4 ชุดล่าสุดที่เคยใช้มา<br><br>8.2.5.b **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจทานกระบวนการภายใน และเอกสารของ ลูกค้า/ผู้ใช้ เพื่อตรวจสอบว่ารหัสผ่านใหม่ของบัญชีที่ไม่ใช่ของลูกค้าไม่สามารถใช้รหัสเหมือนกับรหัส 4 ชุดล่าสุดที่เคยใช้มาได้ | หากประวัติรหัสผ่านไม่ได้มีการเก็บรักษาไว้ ประสิทธิภาพในการเปลี่ยนรหัสผ่านจะลดลง เนื่องจากจะสามารถใช้รหัสผ่านเดิมได้ซ้ำแล้วซ้ำเล่า ต้องขอให้รหัสผ่านเดิมไม่สามารถนำมาใช้ในเป็นระยะเวลาหนึ่ง เพื่อลดความเสี่ยงที่รหัสจะถูกคาดเดา หรือ ลองผิดลองถูกจนเข้าใช้งานได้ในอนาคต |
| 8.2.6 ตั้ง passwords/phrases สำหรับการเข้าใช้งานครั้งแรก ก่อนการรีเซทให้แตกต่างออกไปสำหรับแต่ละ user และทำการเปลี่ยนทันทีที่เข้าใช้งานครั้งแรก | 8.2.6 ตรวจสอบกระบวนการของรหัสผ่าน และสังเกตบุคลากรด้านความปลอดภัยเพื่อตรวจสอบรหัสผ่านสำหรับ user ใหม่ การรีเซทรหัสผ่าน ได้รับการตั้งค่าให้มีค่าที่แตกต่างกันออกไปสำหรับแต่ละ user และมีการเปลี่ยนทันทีที่เข้าใช้งานครั้งแรก | หากมีการใช้งานรหัสผ่านเดิมกับผู้ใช้งานใหม่ทุกคน ผู้ใช้งานภายในอดีตลูกจ้าง หรือ ผู้ประสงค์ร้ายอาจรับรู้ หรือ สามารถค้นพบรหัสผ่านได้อย่างง่ายดาย และใช้มันเพื่อเข้าสู่บัญชี |
| 8.3 ใช้งานการรับรอง 2 ปัจจัย (two-factor authentication) สำหรับการเข้าถึงจากทางไกลโดยบุคลากร (รวมถึง ผู้ใช้ และ ผู้ดูแลระบบ) และ บุคคลที่ 3 ทั้งหมด (รวมถึง การเข้าถึงของผู้ขาย เพื่อสนับสนุน หรือ การบำรุงรักษา)<br><br>หมายเหตุ: การรับรอง 2 ปัจจัย (*Two-factor authentication*) ต้องให้มีการใช้งาน 2 จาก 3 วิธีการรับรอง (โปรดดู ความต้องการ *8.2* สำหรับรายละเอียดวิธีการรับรอง) เพื่อการรับรอง การใช้ปัจจัยเดียวซ้ำ 2 ครั้ง (เช่น ใช้รหัสผ่าน 2 รหัส) ไม่นับเป็น *Two-factor* ตัวอย่าง เช่น การพิสูจน์ตัวตนแบบ *RADIUS* พร้อมด้วย *token;* การรับรองแบบ *TACACS* พร้อมด้วย *token;* และเทคโนโลยีอื่นๆซึ่งช่วยในการรับรองตัวตนแบบ 2 ปัจจัย | 8.3.a ตรวจสอบการตั้งค่าระบบสำหรับการเข้าถึงเซิฟเวอร์และระบบทางไกลเพื่อตรวจสอบว่าได้มีการร้องขอการรับรอง 2 ปัจจัยสำหรับ:<br>• การเข้าถึงทางไกลจากบุคลากรทั้งหมด<br>• การเข้าถึงทางไกลจากบุคคลที่ 3/ผู้ขายทั้งหมด (รวมไปถึง การเข้าถึงแอปพลิเคชั่น และ ส่วนประกอบระบบเพื่อการสนับสนุน หรือจุดประสงค์การบำรุงรักษา)<br><br>8.3.b สังเกตตัวอย่างของบุคลากร (เช่น ผู้ใช้ และผู้ดูแล) ในการเชื่อมต่อจากทางไกลมายังเครือข่าย และตรวจสอบว่ามีการใช้วิธีการรับรอง 2 จาก 3 วิธีการ | การรับรอง 2 ปัจจัย ต้องการการรับรองตัวตน 2 ประเภทสำหรับการเข้าถึงที่มีความเสี่ยงสูง เช่นจากเครือข่ายภายนอก<br><br>ความต้องการนี้มีจุดประสงค์เพื่อใช้งานกับบุคลากรทั้งหมด — รวมไปถึงผู้ใช้ทั่วไป ผู้ดูแลระบบ และผู้ขาย (สำหรับการสนับสนุน หรือบำรุงรักษา) ที่เชื่อมต่อทางไกลเข้าสู่ระบบ — ซึ่งการเชื่อมต่อเหล่านั้นสามารถนำไปสู่ สิ่งแวดล้อมข้อมูลผู้ถือบัตรได้<br><br>หากการเชื่อมต่อทางไกลเชื่อมมายังเครือข่ายของหน่วยงานซึ่งมีการแยกส่วนที่เหมาะสม ผู้ใช้ทางไกลเหล่านั้นจะไม่สามารถเข้าถึงหรือ ส่งผลกระทบต่อสิ่งแวดล้อมข้อมูลผู้ถือบัตรได้ การรับรอง 2 ปัจจัยไม่จำเป็นสำหรับเครือข่ายในกรณีนี้ อย่างไรก็ตามการรับรอง 2 ปัจจัยยังคงเป็นความต้องการสำหรับการเข้าถึงที่นำไปสู่สิ่งแวดล้อมข้อมูลผู้ถือบัตรได้ และเป็นที่แนะนำสำหรับการเข้าถึงทางไกลไปยังเครือข่ายของหน่วยงานทั้งหมด |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.4 จัดทำเอกสาร และ สื่อสารกระบวนการและนโยบายการรับรองตัวตนไปยังผู้ใช้ทั้งหมดดังนี้:<br>• คำแนะนำการเลือกข้อมูลการรับรองส่วนตัวที่เข้มงวด<br>• คำแนะนำวิธีการปกป้องข้อมูลการรับรองส่วนตัวของพวกเขา<br>• แนวทางการไม่ใช้รหัสผ่านที่เคยใช้แล้ว<br>• แนวทางการเปลี่ยนรหัสผ่านเมื่อต้องสงสัยว่าอาจถูกเจาะข้อมูล | 8.4.a ตรวจสอบกระบวนการ และสัมภาษณ์บุคลากรเพื่อตรวจสอบว่ากระบวนการและนโยบายการรับรองตัวตนได้ส่งไปยังผู้ใช้ทั้งหมดแล้ว | สื่อกระบวนการเกี่ยวกับ password/การรับรองตัวตน ไปยังผู้ใช้งานทั้งหมด เพื่อช่วยให้พวกเขาเข้าใจ และ ยึดถือนโยบายเป็นหลัก<br>เช่น คำแนะนำการเลือกรหัสผ่านที่เข้มงวดอาจมีการเสนอแนะเพื่อช่วยให้บุคลากรสามารถเลือกรหัสผ่านที่ยากต่อการคาดเดาซึ่งไม่มีอยู่ในพจนานุกรม และไม่มีข้อมูลซึ่งเป็นข้อมูลเกี่ยวกับผู้ใช้ได้ (เช่น user ID, ชื่อสมาชิกครอบครัว, วันเกิด, และอื่นๆ) คำแนะนำสำหรับการปกป้องข้อมูลการรับรองส่วนตัวอาจแสดงให้เห็นว่าไม่ควรเขียนรหัสผ่านลงบนกระดาษ หรือsaveเป็นไฟล์ที่ไม่ปลอดภัยไว้ และคอยระวังผู้ประสงค์ร้ายที่พยายามฉวยรหัสผ่านของตน (เช่น ด้วยการโทรหา และสอบถามรหัสผ่านเพื่อผู้โทรจะได้ “ตรวจสอบปัญหา”)<br>แนะนำผู้ใช้ให้เปลี่ยนรหัสผ่านเมื่อไม่ปลอดภัยอีกต่อไป จะช่วยป้องกันผู้ประสงค์ร้ายจากการใช้รหัสผ่านจองตนในการเข้าถึงได้ |
| | 8.4.b ตรวจทานกระบวนการและนโยบายการรับรองตัวตนซึ่งส่งไปยังผู้ใช้ทั้งหมดว่ามี:<br>• คำแนะนำการเลือกข้อมูลการรับรองส่วนตัวที่เข้มงวด<br>• คำแนะนำวิธีการปกป้องข้อมูลการรับรองส่วนตัวของพวกเขา<br>• แนวทางการไม่ใช้รหัสผ่านที่เคยใช้แล้ว<br>• แนวทางการเปลี่ยนรหัสผ่านเมื่อต้องสงสัยว่าอาจถูกเจาะข้อมูล | |
| | 8.4.c สัมภาษณ์ตัวอย่างผู้ใช้งาน เพื่อตรวจสอบว่าพวกเขาคุ้นเคยกับกระบวนการและนโยบายการรับรองตัวตน | |
| 8.5 ไม่ใช้ ID รหัสผ่าน หรือ การรับรองตัวตน เป็นกลุ่ม ร่วมกัน หรือทั่วๆไปดังต่อไปนี้:<br>• ID ผู้ใช้ทั่วไปจะต้องถูกปิดการใช้งาน หรือ ลบออก<br>• จะต้องไม่มี ID ที่ใช้ร่วมกันสำหรับผู้ดูแลระบบและฟังก์ชั่นสำคัญอื่นๆ<br>• ID ทั่วไป หรือ ที่ใช้ร่วมกัน จะต้องไม่ถูกใช้สำหรับการจัดการส่วนประกอบระบบใดๆ | 8.5.a สำหรับตัวอย่างส่วนประกอบระบบ ตรวจสอบรายการ ID ผู้ใช้งาน เพื่อตรวจสอบดังนี้:<br>• ID ผู้ใช้ทั่วไปจะต้องถูกปิดการใช้งาน หรือ ลบออก<br>• จะต้องไม่มี ID ที่ใช้ร่วมกันสำหรับผู้ดูแลระบบและฟังก์ชั่นสำคัญอื่นๆ<br>• ID ทั่วไป หรือ ที่ใช้ร่วมกัน จะต้องไม่ถูกใช้สำหรับการจัดการส่วนประกอบระบบใดๆ | หากผู้ใช้หลายคนแบ่งปันข้อมูลการรับรองตัวตนกัน (เช่น ชื่อบัญชี และรหัสผ่าน) จะเป็นเรื่องที่เป็นไปไม่ได้เลยในการติดตามการเข้าถึงระบบ และกิจกรรมของแต่ละคน ทำให้หน่วยงานไม่สามารถติดตามความรับผิดชอบ หรือ เก็บประวัติได้อย่างมีประสิทธิภาพ สำหรับการกระทำของแต่ละบุคคลได้ เนื่องจากการกระทำอาจเกิดจากใครก็ได้ในกลุ่มนั้น |
| | 8.5.b ตรวจสอบนโยบาย/กระบวนการการรับรองตัวตน เพื่อตรวจสอบว่ามีการห้ามไม่ให้ใช้งาน ID และ/หรือ รหัสผ่าน หรือการรับรองตัวตนอื่นๆ เป็นกลุ่ม หรือใช้ร่วมกัน | |
| | 8.5.c สัมภาษณ์ผู้ดูแลระบบ เพื่อตรวจสอบว่าไม่มีการให้ ID และ/หรือ รหัสผ่าน หรือการรับรองตัวตนอื่นๆ เป็นกลุ่ม หรือใช้ ร่วมกันแม้มีการร้องขอก็ตาม | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 8.5.1 **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ผู้ให้บริการที่มีการเข้าถึงทางไกลไปยังสถานที่ของลูกค้า (เช่น เพื่อสนับสนุน ระบบหรือ บริการ POS) จะต้องใช้ข้อมูลการรับรองส่วนตัวที่แตกต่าง (เช่น password/phrase) สำหรับลูกค้าแต่ละคน<br><br>หมายเหตุ: ความต้องการนี้ไม่ได้มีจุดประสงค์เพื่อใช้งานกับผู้ให้บริการ *shared hosting* ที่เข้าถึงสิ่งแวดล้อมที่ตน *host* ซึ่งสิ่งแวดล้อมของลูกค้าหลายคนถูก *hosted* ไว้<br><br>หมายเหตุ: ความต้องการ *8.5.1* คือวิธีการที่ดีที่สุดจนถึง 30 มิถุนายน 2556 2556 หลังจากเป็นส่วนหนึ่งของความต้องการ | 8.5.1 **กระบวนการทดสอบเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจสอบนโยบาย และกระบวนการการรับรองตัวตน และสัมภาษณ์บุคลากรเพื่อตรวจสอบว่ามีการใช้การรับรองที่แตกต่างออกไปสำหรับลูกค้าแต่ละคน | เพื่อป้องกันการเจาะระบบของลูกค้าหลายคนผ่านข้อมูลส่วนตัวเพียงชุดเดียว ผู้ขายที่มีการเข้าถึงทางไกลควรใช้ข้อมูลการรับรองส่วนตัวที่แตกต่างกันสำหรับลูกค้าแต่ละคน<br><br>เทคโนโลยี เช่น กลไกการรับรอง 2 ปัจจัย ซึ่งจะสร้างการรับรองที่แตกต่างกันในการเชื่อมต่อแต่ละครั้ง (เช่น ด้วยรหัสผ่านที่ใช้ครั้งเดียว) สามารถบรรลุจุดประสงค์ของความต้องการนี้ได้ |
| 8.6 สถานที่ใดที่กลไกการรับรองถูกใช้งาน (เช่น ทางกายภาพ ทางการเข้าระบบด้วย token ความปลอดภัย smart card ใบรับรอง และอื่นๆ) การใช้กลไกเหล่านี้จะต้องมีการจัดตั้งดังนี้:<br><br>• กลไกการรับรองตัวตนต้องได้รับการจัดตั้งบนบัญชีแต่ละบุคคล และไม่มีการแบ่งปันระหว่างบัญชีหลายบัญชี<br>• จะต้องมีการใช้งานการควบคุมทางกายภาพ และ/หรือ ทางการเข้าระบบเพื่อให้มั่นใจว่าบัญชีที่ต้องการสามารถใช้กลไกนั้นๆเพื่อการเข้าถึงได้ | 8.6.a ตรวจสอบนโยบาย และกระบวนการการรับรองตัวตน เพื่อตรวจสอบว่ากระบวนการที่ใช้ในกลไกการรับรอง เช่น token ทางกายภาพ smart card และ ใบรังรอง ได้ถูกกำหนดไว้ดังนี้:<br><br>• กลไกการรับรองตัวตนต้องได้รับการจัดตั้งบนบัญชีของแต่ละบุคคลและไม่มีการแบ่งปันระหว่างบัญชีหลายบัญชี<br>• จะต้องมีการใช้งานการควบคุมทางกายภาพ และ/หรือ ทางการเข้าระบบเพื่อให้มั่นใจว่าบัญชีที่ต้องการสามารถใช้กลไกนั้นๆเพื่อการเข้าถึงได้ | หากกลไกการรับรองตัวตนผู้ใช้ เช่น token smart cards และใบรับรองสามารถใช้กับบัญชีหลายบัญชีได้ มันเป็นไปไม่ได้เลยที่จะระบุตัวตนผู้ใช้การมีการควบคุม ทางกายภาพ และ/หรือ ทางการเข้าถึงระบบ (เช่น PIN, ข้อมูลชีวภาพ (biometric data) หรือ รหัสผ่าน) เพื่อระบุเอกลักษณ์ตัวตนผู้ใช้บัญชีนั้นๆเพื่อป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตจากการเข้าถึงโดยการรับรองที่แบ่งปันกันใช้งาน |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 8.6.b สัมภาษณ์บุคลากรด้านความปลอดภัยเพื่อตรวจสอบว่ากลไกการรับรองตัวตนได้ถูกจัดตั้งบนบัญชีเดียวและไม่มีการแบ่งปันให้กับหลายบัญชี | |
| | 8.6.c ตรวจสอบการตั้งค่าระบบ และ/หรือ การควบคุมทางกายภาพเท่าอย่างเหมาะสม เพื่อตรวจสอบว่าการควบคุมได้มีการดำเนินการ เพื่อให้มั่นใจว่าบัญชีที่ต้องการสามารถใช้กลไกนั้นๆเพื่อการเข้าถึงได้ | |
| 8.7 การเข้าถึงทั้งหมดไปยังฐานข้อมูลซึ่งบรรจุข้อมูลผู้ถือบัตร (รวมไปถึงการเข้าถึงโดยแอปพลิเคชั่น, ผู้ดูแลระบบ, และผู้ใช้อื่นๆทั้งหมด) ได้รับการจำกัดดังนี้:<br>• การเข้าถึงทั้งหมดของผู้ใช้ไปยัง, การค้นหาของผู้ใช้, และการกระทำทั้งหมดของผู้ใช้ไปยังฐานข้อมูลต้องผ่านวิธีการทางโปรแกรมเท่านั้น<br>• เฉพาะผู้ดูแลฐานข้อมูลจึงจะสามารถเข้าถึงหรือค้นหาในฐานข้อมูลโดยตรงได้<br>• แอปพลิเคชั่น ID สำหรับ แอปพลิเคชั่นฐานข้อมูลสามารถใช้งานได้เฉพาะจากแอปพลิเคชั่นเท่านั้น (และไม่สามารถใช้ได้โดยผู้ใช้ใดๆ หรือกระบวนการที่ไม่ได้มาจากแอปพลิเคชั่น) | 8.7.a ตรวจทานการตั้งค่าฐานข้อมูลและแอปพลิเคชั่น และตรวจสอบว่าผู้ใช้งานทั้งหมดได้รับการตรวจการรับรองก่อนการเข้าถึง | หากไม่มีการรับรองตัวตนผู้ใช้ในการเข้าถึงฐานข้อมูล และแอปพลิเคชั่น ความเป็นไปได้ที่ผู้ไม่ได้รับอนุญาต หรือ ผู้ประสงค์ร้ายจะเจาะเข้ามาจะเพิ่มขึ้น และการเข้าถึงจะไม่ได้รับการบันทึกประวัติเนื่องจากผู้ใช้ไม่ได้รับการรับรองตัวตน และยิ่งกว่านั้น ไม่ได้รู้จักโดยระบบ อีกทั้งการเข้าถึงฐานข้อมูลควรให้สิทธิผ่านกระบวนการทางโปรแกรมเท่านั้น (เช่นผ่านกระบวนการการจักเก็บข้อมูล) ดีกว่าผ่านการเข้าถึงโดยตรงไปยังฐานข้อมูลโดยผู้ใช้ (ยกเว้นสำหรับ DBAs, ผู้อาจต้องการการเข้าถึงโดยตรงไปยังฐานข้อมูลสำหรับหน้าที่การดูแลระบบ) |
| | 8.7.b ตรวจสอบการตั้งค่าฐานข้อมูล และแอปพลิเคชั่น เพื่อตรวจสอบว่าการเข้าถึงของผู้ใช้ทั้งไปยัง, การค้นหาของผู้ใช้, และการกระทำทั้งหมดของผู้ใช้ (เช่น การเคลื่อนย้าย คัดลอก ลบ) ไปยังฐานข้อมูลต้องผ่านวิธีการทางโปรแกรมเท่านั้น (เช่น ผ่านกระบวนการจัดเก็บ) | |
| | 8.7.c ตรวจสอบการตั้งค่าการควบคุมการเข้าถึงฐานข้อมูล และการตั้งค่าแอปพลิเคชั่นฐานข้อมูล เพื่อตรวจสอบว่าการเข้าถึงโดยตรงของผู้ใช้ไปยังฐานข้อมูล หรือการค้นหาข้อมูลได้รับการจำกัดให้มีสิทธิเฉพาะผู้ดูแลเท่านั้น | |
| | 8.7.d ตรวจสอบการตั้งค่าการควบคุมการเข้าถึงฐานข้อมูล การตั้งค่าแอปพลิเคชั่นฐานข้อมูล และแอปพลิเคชั่น ID ที่เกี่ยวข้อง เพื่อตรวจสอบว่าแอปพลิเคชั่น ID สามารถถูกใช้เฉพาะโดยแอปพลิเคชั่น (และไม่สามารถใช้ได้โดยผู้ใช้ใดๆ หรือ กระบวนการที่ไม่ได้มาจากแอปพลิเคชั่น) | |
| 8.8 ทำให้มั่นใจว่านโยบายความปลอดภัย และกระบวนการดำเนินการสำหรับการระบุตัวตน และการรับรองได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และเป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 8.8 ตรวจสอบเอกสารการ และสัมภาษณ์บุคลากร เพื่อตรวจสอบว่านโยบายความปลอดภัย และกระบวนการดำเนินการในการระบุตัวตน และรับรองนั้น:<br>• ได้รับการจัดทำเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักสำหรับผู้ที่มีผลกระทบทั้งหมด | บุคลากรต้องตระหนัก และดำเนินการตามนโยบายความปลอดภัย และกระบวนการดำเนินการการจัดการการระบุตัวตน และการรับรองอย่างต่อเนื่อง |

# ความต้องการที่ 9: จำกัดการเข้าถึงทางกายภาพไปยังข้อมูลผู้ถือบัตร

การเข้าถึงข้อมูลหรือระบบใดๆโดยตรงซึ่งเป็นที่อยู่ของข้อมูลผู้ถือบัตร อาจทำให้เกิดความเสี่ยงที่บุคคลใดๆสามารถเข้าถึงอุปกรณ์ หรือ ข้อมูล เพื่อลบระบบ หรือ hardcopy ได้ และควรมีการจำกัดไว้อย่างเหมาะสม สำหรับจุดประสงค์ของความต้องการที่ 9 “บุคลกรในสถานที่ (onsite)” หมายถึงลูกจ้าง full-time และ part-time ลูกจ้างชั่วคราว ลูกจ้างสัญญาจ้าง และ ผู้ให้คำปรึกษาผู้ที่ปรากฏตัวทางกายภาพในพื้นที่ของหน่วยงาน “ผู้มาเยือน” หมายถึงผู้ขาย, แขกของบุคลากรในสถานที่, ผู้ทำงานบริการ หรือใครก็ตามที่ต้องการเข้าไปยังสถานที่ในระยะเวลาอันสั้น ปกติแล้วไม่เกิน 1 วัน “สื่อ” หมายถึงทั้งกระดาษ และ อิเล็กทรอนิกส์ ที่บรรจุข้อมูลผู้ถือบัตรไว้

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.1 ใช้การควบคุมการเข้าตัวอาคารอย่างเหมาะสม เพื่อจำกัด และ เฝ้าติดตามการเข้าถึงระบบทางกายภาพในสิ่งแวดล้อมข้อมูลผู้ถือบัตร | 9.1 ตรวจสอบว่ามีการควบคุมความปลอดภัยทางกายภาพอยู่หรือไม่ สำหรับห้องที่มีคอมพิวเตอร์ ศูนย์ข้อมูล (data center) และพื้นที่ทางกายภาพอื่นๆที่มีระบบในสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br>• ตรวจสอบว่าการเข้าถึงได้รับการควบคุมด้วยเครื่องอ่านบัตร หรือ อุปกรณ์อื่นๆ ที่มีบัตรอนุญาต ล็อค และกุญแจ<br>• สังเกตประวัติความพยายามในการเข้าถึง console ของผู้ดูแลระบบสำหรับระบบที่สุ่มเลือกขึ้นมาจากสิ่งแวดล้อมข้อมูลผู้ถือบัตรและตรวจสอบว่าสิ่งเหล่านั้นได้รับการ “ล็อค” เพื่อป้องกันการใช้งานที่ไม่ได้รับอนุญาต | หากไม่มีการควบคุมการเข้าถึงทางกายภาพ เล่นระบบอ่านบัตร และการควบคุมประตูแล้ว ผู้ที่ไม่ได้รับอนุญาตอาจได้รับการเข้าถึงไปยังตัวอาคารเพื่อขโมย ปิดการใช้งาน รบกวน หรือ ทำลายระบบสำคัญและข้อมูลผู้ถือบัตรได้<br>ล็อคหน้าจอการ login console เพื่อป้องกันผู้ไม่ได้รับอนุญาตจากการเข้าถึงข้อมูลที่สุ่มเสี่ยง เปลี่ยนแปลงการตั้งค่าระบบ สร้างช่องโหว่ในเครือข่าย หรือทำลายบันทึกต่างๆ |
| 9.1.1 ใช้กล้องบันทึกวีดีโอ และ/หรือ กลไกควบคุมการเข้าถึงเพื่อติดตามการเข้าถึงทางกายภาพของบุคคลไปยังพื้นที่ที่สุ่มเสี่ยง ทบทวนข้อมูลที่รวบรวมไว้ และ เทียบกับรายการอื่นๆ จัดเก็บไว้อย่างน้อย 3 เดือน เว้นแต่ได้มีข้อจำกัดทางกฎหมาย<br><br>หมายเหตุ: “พื้นที่สุ่มเสี่ยง” หมายถึง ศูนย์ข้อมูลใดๆ (*data center*) ห้องเซิฟเวอร์ หรือพื้นที่ใดๆที่จัดเก็บ หรือส่งข้อมูลผู้ถือบัตร พื้นที่นี้ไม่รวมพื้นที่ที่เปิดเผยต่อสาธารณะซึ่งเฉพาะ *point-of- sale terminals* ถูกเปิดเผยเช่นพื้นที่แคชเชียร์ในร้านค้าปลีก | 9.1.1.a ตรวจสอบว่ากล้องวีดีโอ และ/หรือ กลไกควบคุมการเข้าถึง มีการใช้งาน เพื่อติดต่อมการ เข้า/ออก ไปยังพื้นที่สุ่มเสี่ยง<br><br>9.1.1.b ตรวจสอบว่ากล้องวีดีโอ และ/หรือ กลไกควบคุมการเข้าถึงได้รับการป้องกันจากการสอดแนม หรือ ปิดการใช้งาน | เมื่อมีการฝ่าความปลอดภัยทางการภาพ การควบคุมเหล่านี้สามารถช่วยระบุผู้ที่มีการเข้าถึงโดยตรงไปยังพื้นที่สุ่มเสี่ยงได้ รวมไปถึง เวลาที่เข้า หรือออกจากพื้นที่<br>ความพยายามในการโจรกรรม เพื่อได้รับการเข้าถึงทางกายภาพไปยังพื้นที่สุ่มเสี่ยงมักจะพยายามที่จะปิด หรือ bypass การควบคุมการเฝ้าติดตาม เพื่อป้องกันการควบคุมเหล่านี้จากการถูกสอดแนม กล้องวีดีโอควรอยู่ในตำแหน่งที่ไม่สามารถเอื้อมถึงได้ และ/หรือ ได้รับการเฝ้าติดตามการสอดแนม เช่นเดียวกัน กลไกการควบคุมการเข้าถึงควรได้รับการเฝ้าติดตาม หรือ มีการติดตั้งการป้องกันทางกายภาพเพื่อป้องกันจากความเสียหาย หรือ การปิดการใช้งายโดยผู้ประสงค์ร้าย |

*(มีต่อหน้าถัดไป)*

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 9.1.1.c ตรวจสอบว่า กล้องวีดีโอ และ/หรือกลไกการควบคุมการเข้าถึงได้รับการเฝ้าติดตาม และข้อมูลจากกล้อง หรือ กลไกอื่นๆได้รับการบันทึกไว้อย่างน้อย 3 เดือน | ตัวอย่างของพื้นที่สุ่มเสี่ยง ได้แก่ ห้องเซิฟเวอร์ฐานข้อมูลขององค์กร ห้อง back-office ที่สถานที่ค้าปลีกซึ่งเก็บข้อมูลผู้ถือบัตร และ ส่วนจัดเก็บสำหรับข้อมูลผู้ถือบัตรจำนวนมาก พื้นที่สุ่มเสี่ยงควรได้รับการระบุโดยองค์กรเพื่อให้มั่นใจว่ามีการดำเนินการควบคุมการเฝ้าติดตามทางกายภาพอย่างเหมาะสม |
| 9.1.2 มีการจำกัดการเข้าถึงทางกายภาพและ/หรือทางการเข้าสู่ระบบไปยังช่องทางที่สามารถเข้าถึงเครือข่ายได้จากสาธารณะ (publicly accessible network jack)<br><br>ตัวอย่าง เช่น ช่องทางเครือข่าย ที่อยู่ในพื้นที่สาธารณะและพื้นที่ที่เข้าถึงได้โดยผู้มาเยือนสามารถปิดการใช้งานหรือเปิดการใช้งานได้เมื่อมีการเข้าถึงเครือข่ายด้วยอำนาจการเข้าถึง ในอีกทางหนึ่ง อาจดำเนินการตามกระบวนการเพื่อที่ผู้มาเยือนจะได้รับการนำพาไปยังพื้นที่ที่มีช่องทางเครือข่ายที่เปิดใช้งานอยู่ทุกครั้ง | 9.1.2 สัมภาษณ์บุคลากรที่รับผิดชอบและสังเกตสถานที่ของช่องทางเครือข่าย ที่สามารถเข้าถึงได้จากสาธารณะ เพื่อตรวจสอบว่าการควบคุมทางกายภาพ และ/หรือทางการเข้าสู่ระบบมีการใช้งานเพื่อจำกัดการเข้าถึงไปยังช่องทางเครือข่ายนั้นๆ | จำกัดการเข้าถึงช่องทางเครือข่าย (หรือ Port เครือข่าย) จะป้องกันผู้ประสงค์ร้ายจากการเชื่อมต่อเข้าไปยังช่องทางเครือข่ายอย่างง่ายดาย และได้รับสิทธิการเข้าถึงแหล่งเครือข่ายภายในได้<br><br>ไม่ว่าจะมีการใช้งานการควบคุมทางการเข้าสู่ระบบ หรือ ทางกายภาพ หนทอ ผสมผสานทั้ง 2 วิธี วิธีการเหล่านั้นควรจะเพียงพอที่จะป้องกันบุคคล หรือ อุปกรณ์ซึ่งไม่มีอำนาจการเข้าถึงที่ชัดเจนจากการเชื่อมต่อไปยังเครือข่ายได้ |
| 9.1.3 จำกัดการเข้าถึงทางกายภาพไปยังGateway ของจุดการเข้าถึงการเชื่อมต่อแบบไร้สาย wireless access points gateway, อุปกรณ์พกพา hardware เครือข่าย/การสื่อสาร, และคู่สายโทรคมนาคม | 9.1.3 ตรวจสอบว่าการเข้าถึงทางกายภาพไปยังGateway ของจุดการเข้าถึงการเชื่อมต่อแบบไร้สาย wireless access points gateway, อุปกรณ์พกพา hardware เครือข่าย/การสื่อสาร, และคู่สายโทรคมนาคมได้รับการจำกัดไว้ | หากไม่มีความปลอดภัยเหนือการเข้าถึงส่วนประกอบและอุปกรณ์ไร้สาย ผู้ประสงค์ร้ายอาจใช้อุปกรณ์ไร้สายขององค์กรที่ไม่ได้รับการสนใจในการเข้าถึงแหล่งเครือข่าย หรือ แม้แต่เชื่อมต่ออุปกรณ์ของพวกเขาเองไปยังเครือข่ายไร้สายเพื่อรับสิทธิในการเข้าถึงที่ไม่ได้รับอนุญาต นอกจากนั้นแล้วการจัดตั้งเครือข่าย และhardware การสื่อสารอย่างปลอดภัยจะป้องกันไม่ให้ผู้ประสงค์ร้ายขัดขวางการส่งข้อมูลเครือข่าย หรือ เชื่อมต่อทางกายภาพด้วยอุปกรณ์ของพวกเขาเองไปยังแหล่งเครือข่ายแบบมีสายได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.2 พัฒนากระบวนการเพื่อแยกแยะระหว่างบุคลากรในสถานที่ และ ผู้มาเยือนให้มี:<br>• การระบุตัวตนบุคลากรในสถานที่ และผู้มาเยือน (เช่น การให้บัตรผ่าน)<br>• การเปลี่ยนแปลงยังความต้องการการเข้าถึง<br>• การเพิกถอน หรือ กำจัด สิ่งระบุตัวตนที่หมดอายุของ บุคลากรในสถานที่ และผู้มาเยือน (เช่น ID บัตรผ่าน) | 9.2.a ตรวจทานเอกสารกระบวนการเพื่อตรวจสอบว่า กระบวนการได้รับการกำหนดสำหรับแยกแยะระหว่างบุคลากรในสถานที่ และ ผู้มาเยือน<br>ตรวจสอบว่ากระบวนการมีเงื่อนไขดังนี้:<br>• การระบุตัวตนบุคลากรในสถานที่ และผู้มาเยือน (เช่น การให้บัตรผ่าน)<br>• การเปลี่ยนแปลงยังความต้องการการเข้าถึง<br>• การเพิกถอน หรือ กำจัด สิ่งระบุตัวตนที่หมดอายุของ บุคลากรในสถานที่ และผู้มาเยือน (เช่น ID บัตรผ่าน) | ระบุผู้มาเยือนที่ได้รับการอนุมัติ เพื่อที่พวกเขาจะได้ถูกแยกแยะออกจากบุคลกรในพื้นที่อย่างง่ายดาย เพื่อป้องกันผู้ไม่ได้รับอนุญาตจากการได้รับสิทธิการเข้าถึงพื้นที่ที่มีข้อมูลผู้ถือบัตร |
| | 9.2.b สังเกตกระบวนว่าการเพื่อระบุและแยกแยะระหว่างบุคลากรในสถานที่ และ ผู้มาเยือนนั้น:<br>• มีการระบุผู้มาเยือนอย่างแม่นยำ และ<br>• เป็นเรื่องง่ายในการแยกแยะระหว่างบุคลากรในสถานที่ และ ผู้มาเยือน | |
| | 9.2.c ตรวจสอบว่าการเข้าถึงไปยังกระบวนการระบุตัวตน (เช่น ระบบบัตรผ่าน) ถูกจำกัดไว้เพียงเฉพาะบุคลากรที่ได้รับการอนุมัติเท่านั้น | |
| | 9.2.d ตรวจสอบวิธีการระบุตัวตน (เช่น บัตรผ่าน) ที่ใช้งานอยู่เพื่อตรวจสอบว่าได้มีการระบุอย่างชัดเจนถึงผู้มาเยือนหรือไม่ และสามารถแยกบุคลากรในสถานที่ออกอย่างง่ายดายหรือไม่ | |
| 9.3 ควบคุมการเข้าถึงทางกายภาพสำหรับบุคลากรในสถานที่ไปยังพื้นที่สุ่มเสี่ยงดังต่อไปนี้:<br>• การเข้าถึงจะต้องได้รับการรับรองตัวตน และมีพื้นฐานบนแต่ละบทบาทการทำงาน<br>• การเข้าถึงจะต้องถูกเพิกถอนทันทีหากสิทธินั้นสิ้นสุด และกลไกการเข้าถึงทางกายภาพทั้งหมด เช่น กุญแจ บัตรผ่าน และอื่นๆ ต้องได้รับการส่งคืน หรือ ปิดการใช้งาน | 9.3.a สำหรับตัวอย่างของบุคลากรในสถานที่ที่มีการเข้าถึงทางกายภาพไปยัง สัมภาษณ์บุคลากรที่รับผิดชอบ และสังเกตรายการการควบคุมการเข้าถึงเพื่อตรวจสอบว่า:<br>• การเข้าถึงไปยัง CDE นั้นได้รับการรับรองตัวตน<br>• การเข้าถึงร้องขอจากผู้ที่มีบทบาทหน้าที่ที่ต้องการ | การควบคุมการเข้าถึงทางกายภาพไปยัง CDE ช่วยให้มั่นใจว่าเฉพาะผู้ที่ได้รับการรับรองที่มีความต้องการทางธุรกิจตามกฎหมายเท่านั้นจึงได้รับการเข้าถึง<br>เมื่อบุคลากรลาออกจากองค์กร กลไกการเข้าถึงทางกายภาพทั้งหมดต้องได้รับการส่งคืน หรือ ปิดการใช้งานทันที (เร็วที่สุดเท่าที่ทำได้) จากเวลาที่ออกจากองค์กรไป เพื่อให้มั่นใจว่าจะไม่มีสิทธิการเข้าถึงทางกายภาพไปยัง CDE เมื่อสิ้นสุดการว่าจ้างแล้ว |
| | 9.3.b สังเกตการเข้าถึงของบุคลากรไปยัง CDE เพื่อตรวจสอบว่าบุคลากรทั้งหมดได้รับการรับรองตัวตนก่อนเข้าถึงได้ | |
| | 9.3.c เลือกตัวอย่างของบุคลากรล่าที่สิ้นสุดสิทธิการเข้าถึงเพื่อตรวจสอบว่า บุคลากรผู้นั้นไม่มีสิทธิการเข้าถึงทางกายภาพไปยัง CDE จากในรายการควบคุมการเข้าถึง | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.4 ดำเนินการกระบวนการเพื่อระบุตัวตนและอนุญาตผู้มาเยือน<br><br>กระบวนการควรมีดังนี้: | 9.4 ตรวจสอบว่าการอนุญาตผู้มาเยือน และการควบคุมการเข้าถึงมีการใช้งานดังต่อไปนี้: | การควบคุมผู้มาเยือนเป็นสิ่งสำคัญเพื่อช่วยลดความสามารถของผู้ไม่ได้รับอนุญาต และผู้ประสงค์ร้ายจากการได้รับการเข้าถึงอาคาร (และความเสี่ยงไปยังข้อมูลผู้ถือบัตร)<br><br>การควบคุมผู้มาเยือน ทำให้มั่นใจว่าผู้มาเยือนได้รับการระบุตัวตน เพื่อที่บุคลากรจะได้เฝ้าติดตามกิจกรรมของผู้มาเยือน และการเข้าถึงของพวกเขา ว่าได้รับการจำกัดเอาไว้ในระยะเวลาที่ถูกต้องในการมาเยือนหรือไม่<br><br>ทำให้มั่นใจว่าบัตรผ่านของผู้มาเยือนได้รับการส่งคืนเมื่อถึงเวลาหมดอายุ หรือ เมื่อการมาเยือนสำเร็จลุล่วง เพื่อป้องกันไม่ให้ผู้ประสงค์ร้ายใช้การอนุญาตก่อนหน้าเพื่อเข้าถึงอาคารกายภาพหลังการมาเยือนสิ้นสุดลง<br><br>ประวัติผู้มาเยือนเก็บข้อมูลที่เพียงพอกับผู้มาเยือนเพื่อง่ายต่อการบำรุงรักษา และจะสามารถช่วยระบุตัวตนการเข้าถึงทางกายภาพไปยังห้องภายในอาคาร และการเข้าถึงข้อมูลผู้ถือบัตรได้ |
| 9.4.1 ผู้มาเยือนต้องได้รับการอนุญาตก่อนเข้าและได้รับการพาไปยังพื้นที่ซึ่งข้อมูลผู้ถือบัตรถูกดำเนินการหรือบำรุงรักษาอยู่ทุกครั้ง | 9.4.1.a สังเกตกระบวนการ และสัมภาษณ์บุคลากรเพื่อตรวจสอบว่าผู้มาเยือนs must be authorized before they are granted access to, and escorted at all times within, areas whereข้อมูลผู้ถือบัตร มีการดำเนินการ หรือ บำรุงรักษา. | |
| | 9.4.1.b สังเกตการณ์ใช้งานบัตรผ่าน หรือ การระบุตัวตนอื่นๆของผู้มาเยือนเพื่อตรวจสอบว่า token ทางกายภาพ ไม่ได้เข้าถึงส่วนที่ไม่ได้พาไป ไปยังพื้นที่ซึ่งข้อมูลผู้ถือบัตร มีการดำเนินการ หรือ บำรุงรักษาอยู่ | |
| 9.4.2 ผู้มาเยือนได้รับการระบุตัวตนและได้รับบัตรผ่าน หรือ การระบุตัวตนอื่นๆซึ่งจะหมดอายุ และสามารถแยกแยะออกจากบุคลากรในสถานที่ได้ด้วยการมองเห็น | 9.4.2.a สังเกตผู้คนภายในอาคารเพื่อตรวจสอบการใช้งานบัตรผ่าน หรือ การระบุตัวตนอื่นๆของผู้มาเยือน และผู้มาเยือนสามารถถูกแยกแยะจากบุคลากรในพื้นที่ได้อย่างง่ายดายหรือไม่ | |
| | 9.4.2.b ตรวจสอบว่าบัตรผ่าน หรือ การระบุตัวตนอื่นๆของผู้มาเยือนมีการหมดอายุ | |
| 9.4.3 ผู้มาเยือนต้องถูกสอบถามเพื่อมอบบัตรผ่านหรือการระบุตัวตนคือก่อนออกจากอาคารหรือเมื่อถึงเวลาหมดอายุ | 9.4.3 สังเกตการออกจากอาคารของผู้มาเยือนเพื่อตรวจสอบว่าผู้มาเยือนได้รับการสอบถามให้คืน บัตรผ่านหรือการระบุตัวตนอื่นๆก่อนออกจากอาคารหรือเมื่อถึงเวลาหมดอายุหรือไม่ | |
| 9.4.4 มีการบันทึกประวัติผู้มาเยือนเพื่อบำรุงรักษาประวัติการตรวจสอบทางกายภาพของกิจกรรมของผู้มาเยือนที่ไปยังอาคาร รวมไปถึงห้องคอมพิวเตอร์ และศูนย์ข้อมูลซึ่งจัดเก็บ หรือ ส่งข้อมูลผู้ถือบัตร<br><br>บันทึกชื่อผู้มาเยือน เป็นตัวแทนจากบริษัทใด บุคลากรในสถานที่ผู้อนุมติการเข้าถึงทางกายภาพลงบนประวัติ<br><br>เก็บรักษาประวัตินี้เอาไว้อย่างน้อย 3 เดือน เว้นแต่มีข้อจำกัดทางกฎหมาย | 9.4.4.a ตรวจสอบว่า มีการบันทึกประวัติผู้มาเยือนเพื่อบันทึกการเข้าถึงทางกายภาพไปยังอาคาร รวมไปถึงห้องคอมพิวเตอร์ และ ศูนย์ข้อมูลซึ่งจัดเก็บ หรือ ส่งข้อมูลผู้ถือบัตร | |
| | 9.4.4.b ตรวจสอบว่าประวัติผู้มาเยือนมี:<br>• ชื่อผู้มาเยือน<br>• เป็นตัวแทนจากบริษัทใด และ<br>• บุคลากรในสถานที่ผู้อนุมติการเข้าถึง | |
| | 9.4.4.c ตรวจสอบว่าประวัติถูกเก็บรักษาเอาไว้อย่างน้อย 3 เดือน. | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.5 ความปลอดภัยทางกายภาพของสื่อทั้งหมด | 9.5 ตรวจสอบว่ากระบวนการปกป้องข้อมูลผู้ถือบัตรได้มีการควบคุมสำหรับความปลอดภัยทางกายภาพของสื่อทั้งหมด (รวมไปถึง คอมพิวเตอร์, อุปกรณ์อิเล็กทรอนิกส์ที่เคลื่อนที่ได้, ใบเสร็จ, รายงาน, และ แฟกซ์)(เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) | กาควบคุมความปลอดภัยสื่อทางกายภาพมีจุดประสงค์เพื่อป้องกันผู้ไม่ได้รับอนุญาตจากการได้รับสิทธิเข้าถึงข้อมูลผู้ถือบัตรบนสื่อประเภทใดก็ตาม ข้อมูลผู้ถือบัตรนั้นไม่ควรจะถูก พบเห็น คัดลอก หรือ แสกน หากข้อมูลไม่ได้รับการป้องกันขณะที่อยู่บนอุปกรณ์ที่เคลื่อนที่ได้ หรืออุปกรณ์พกพา เอกสารตีพิมพ์ หรือ ถูกทิ้งไว้บนโต๊ะสักแห่ง |
| 9.5.1 จัดเก็บสื่อ backup ในสถานที่ที่ปลอดภัย ทางที่ดีให้เป็นอาคารที่อยู่นอกสถานที่ เช่น พื้นที่อื่นๆ หรือสถานที่ backup site หรือ สถานที่เก็บข้อมูลเชิงพาณิชย์ ตรวจสอบความปลอดภัยของสถานที่อย่างน้อยปีละครั้ง | 9.5.1.a สังเกตความปลอดภัยทางกายภาพของสถานที่จัดเก็บข้อมูลเพื่อยืนยันว่า สื่อ backup ปลอดภัย | หากจัดเก็บข้อมูลไว้ในสถานที่ที่ไม่ปลอดภัย ข้อมูล backups ซึ่งมีข้อมูลผู้ถือบัตร อาจสูญหาย ถูกขโมย หรือ คัดลอกจากผู้ประสงค์ร้ายได้ง่าย |
| | 9.5.1.b ตรวจสอบว่าสถานที่จัดเก็บข้อมูลนั้นได้รับการตรวจสอบอย่างน้อยปีละครั้ง | ตรวจสอบสถานที่จัดเก็บข้อมูลเป็นช่วงๆหากทำได้ เพื่อองค์กรจะได้จัดการปัญหาด้านความปลอดภัยที่พบ และลดความเสี่ยงได้ทันท่วงที |
| 9.6 บำรุงรักษาการควบคุมอย่างเข้มงวดบนการกระจายสื่อใดๆก็ตามทั้งภายใน และภายนอก (distribution) ดังนี้: | 9.6 ตรวจสอบว่ามีนโยบายการควบคุมการกระจายสื่อ และนโยบายนั้นครอบคลุมการกระจายสื่อทั้งหมดรวมทั้งกระจายสื่อไปยังส่วนบุคคลใดๆ | ขั้นตอน และ กระบวนการช่วยปกป้องข้อมูลผู้ถือบัตรบนการกระจายสื่อไปยังผู้ใช้ภายใน และ/หรือภายนอก หากไม่มีกระบวนการเหล่านี้ ข้อมูลอาจสูญหาย ถูกขโมย หรือถูกใช้เพื่อจุดประสงค์การปลอมแปลง |
| 9.6.1 แยกประเภทสื่อ เพื่อจะได้ทราบว่าสื่อใดที่สุ่มเสี่ยง | 9.6.1 ตรวจสอบว่าสื่อทั้งหมดได้รับการแยกประเภทเพื่อสื่อที่สุ่มเสี่ยงจะได้รับการกำหนด | เป็นสิ่งสำคัญในการระบุประเภทของสื่อที่สถานการณ์แยกประเภทจะสามารถมองเห็นได้อย่างง่ายดาย สื่อที่ไม่ได้รับการระบุว่าเป็นความลับ อาจไม่ได้รับการปกป้องที่เทียบเท่า อาจสูญหาย หรือถูกขโมยได้<br>หมายเหตุ: สิ่งนี้ไม่ได้หมายความว่าสื่อจะต้องมีฉลากเขียนว่า "เป็นความลับ" กำกับไว้; *จุดประสงค์คือให้องค์กรสามารถระบุได้ว่าสื่อใดที่บรรจุข้อมูลที่สุ่มเสี่ยงไว้* เพื่อจะได้ปกป้องได้ |
| 9.6.2 ส่งข้อมูลสื่อด้วยการจัดส่งที่ปลอดภัย หรือ วิธีการอื่นๆซึ่งสามารถติดตามได้อย่างแม่นยำ | 9.6.2.a สัมภาษณ์บุคลากรและตรวจสอบประวัติเพื่อตรวจสอบว่าสื่อทั้งหมดที่ส่งออกไปข้างนอกอาคารได้รับการบันทึกประวัติและส่งด้วยการจัดส่งที่ปลอดภัย หรือด้วยวิธีการส่งอื่นๆที่สามารถติดตามได้ | สื่ออาจสูญหาย หรือถูกขโมยได้หากถูกส่งด้วยวิธีการที่ติดตามไม่ได้ เช่น การส่งจดหมายทั่วไป การใช้การจัดส่งที่ปลอดภัยเพื่อส่งสื่อใดๆก็ตามซึ่งบรรจุข้อมูลผู้ถือบัตร ทำให้องค์กรสามารถติดตามเพื่อรักษาคลัง และสถานที่การส่งได้ |
| | 9.6.2.b เลือกตัวอย่างภายในไม่กี่วันของประวัติการติดตามสำหรับสื่อทั้งหมด และตรวจสอบว่ารายละเอียดการติดตามได้ถูกบันทึกไว้หรือไม่ | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.6.3 ทำให้แน่ใจว่ามีการจัดการการอนุมัติสื่อทุกๆสื่อ และสื่อใดๆก็ตามซึ่งเคลื่อนย้ายจากพื้นที่ปลอดภัย (รวมไปถึง เมื่อได้รับการแจกจ่ายไปยังส่วนบุคคลใดๆ) | 9.6.3 เลือกตัวอย่างที่ผ่านมาไม่กี่วันของประวัติการติดตามนอกสถานที่ เพื่อตรวจสอบประวัติ และสัมภาษณ์บุลากรที่รับผิดชอบ มีการตรวจสอบการจัดการการอนุญาตที่เหมาะสมเมื่อใดก็ตามที่สื่อได้รับการเคลื่อนย้ายจากพื้นที่ปลอดภัย (รวมไปถึง เมื่อได้รับการแจกจ่ายไปยังส่วนบุคคลใดๆ) | หากไม่มีกระบวนการที่ดีเพื่อให้มั่นใจว่าการเคลื่อนย้ายสื่อทั้งหมดได้รับการอนุมัติก่อนเคลื่อนย้ายจากพื้นที่ปลอดภัยก่อน สื่อที่ไม่สามารถติดตามได้ หรือ ไม่ได้รับการป้องกันที่เหมาะสม ซึ่งไม่สามารถทราบถึงสถานที่ได้ อาจนำไปสู่การสูญหาย หรือ ถูกขโมยได้ |
| 9.7 บำรุงรักษาการควบคุมที่เข้มงวดบนการจัดเก็บ และการเข้าถึงสื่อ | 9.7 ขอรับและตรวจสอบนโยบายการควบคุมการจัดเก็บ และบำรุงรักษาสื่อทั้งหมด และตรวจสอบว่านโยบายได้มีการจัดการคลังสื่อเป็นระยะๆหรือไม่ | หากไม่มีวิธีการจัดการคลัง และการจัดเก็บสื่อที่รอบคอบ การสูญหาย หรือถูขโมยอาจเกิดขึ้นได้โดยไม่มีผู้ใดทราบ และไม่ทราบว่าเกิดขึ้นบ่อยแค่ไหน<br>หากสื่อไม่ได้รับการจัดเก็บในคลัง อาจไม่ทราบถึงการถูกขโมย หรือ สูญหาย เป็นเวลานาน หรือไม่ทราบเลยก็ได้ |
| 9.7.1 บำรุงรักษาประวัติคลังสื่อทั้งหมด และจัดการคลังสื่ออย่างน้อยปีละครั้ง | 9.7.1 ตรวจสอบประวัติคลังสื่อ เพื่อตรวจสอบว่าประวัติได้รับการบำรุงรักษา และคลังสื่อได้รับการจัดการคลังสื่ออย่างน้อยปีละครั้ง | |
| 9.8 ทำลายสื่อทั้งหมดเมื่อธุรกิจไม่ต้องการอีกต่อไป หรือตามเหตุผลทางกฎหมายดังนี้: | 9.8 ตรวจสอบนโยบายการทำลายสื่อตามระยะเวลา และตรวจสอบว่านโยบายครอบคลุมสื่อทั้งหมด และกำหนดความต้องการดังนี้:<br>• วัสดุที่จับต้องได้ (Hard-copy) ได้รับการ ตัด (crosscut) ฉีก เผา หรือบด เพื่อความมั่นใจว่าสื่อเหล่านั้นจะได้ไม่ถูกนำไปรื้อฟื้นใหม่<br>• แหล่งบรรจุข้อมูลที่ใช้สำหรับวัสดุซึ่งจะถูกทำลาย เพื่อตรวจสอบว่ามีความปลอดภัย<br>• ข้อมูลผู้ถือบัตรบนสื่ออิเล็กทรอนิกส์ถูก render ให้ไม่สามารถกู้คืนได้ ด้วยโปรแกรมการล้างข้อมูลร่วมกับ มาตรฐานที่ยอมรับในระดับอุตสาหกรรมสำหรับการลบข้อมูลอย่างปลอดภัย หรือ ทำลายสื่อนั้นๆทางกายภาพ) | หากไม่มีขั้นตอนการทำลายข้อมูลที่บรรจุใน hard disk อุปกรณ์พกพา CD/DVD หรือสิ่งพิมพ์ เพื่อการกำจัดทิ้ง ผู้ประสงค์ร้ายอาจสามารถกู้ข้อมูลกลับมาได้ และนำไปสู่การเจาะข้อมูล เช่น ผู้ประสงค์ร้ายอาจใช้เทคนิคที่เรียกว่า “การค้นข้อมูลจากถังขยะ (dumpster diving)” ซึ่งเป็นการค้นหาจากถังขยะ และถังรีไซเคิล เพื่อหาข้อมูลซึ่งอาจใช้โจมตีได้<br>การรักษาความปลอดภัยแหล่งบรรจุใช้สำหรับวัสดุซึ่งจะถูกทำลาย ป้องกันไม่ให้ข้อมูลที่สุ่มเสี่ยงรั่วไหล เช่นแหล่งบรรจุสื่อที่ “กำลังจะถูกฉีก” ควรมีการล็อคการเข้าถึงไว้ เพื่อป้องกันการเข้าถึงทางกายภาพ<br>ตัวอย่างวิธีการรักษาความปลอดภัยสื่ออิเล็กทรอนิกส์ ได้แก่ การล้างข้อมูล (wipe) ล้างสนามแม่เหล็ก (degaussing) หรือทำลายทางกายภาพ (เช่น บด หรือ ฉีก hard disk) |
| 9.8.1 ฉีก เผา หรือบด วัสดุที่เป็นกระดาษ หรือสัมผัสได้ (hard copy) เพื่อข้อมูลผู้ถือบัตรจะได้ไม่ถูกนำไปรื้อฟื้นใหม่ รักษาความปลอดภัยของแหล่งบรรจุข้อมูลที่ใช้สำหรับวัสดุซึ่งจะถูกทำลาย | 9.8.1.a สัมภาษณ์บุคลากร และตรวจสอบกระบวนการ เพื่อตรวจสอบว่าวัสดุที่เป็น hard-copy ได้รับการ ตัด (crosscut) ฉีก เผา หรือบด เพื่อความมั่นใจว่าสื่อเหล่านั้นจะได้ไม่ถูกนำไปรื้อฟื้นใหม่ | |
| | 9.8.1.b ตรวจสอบแหล่งบรรจุข้อมูลที่ใช้สำหรับวัสดุซึ่งจะถูกทำลาย เพื่อตรวจสอบว่ามีความปลอดภัยหรือไม่ | |
| 9.8.2 Render ข้อมูลผู้ถือบัตร บนสื่ออิเล็กทรอนิกส์ให้ไม่สามารถกู้คืนได้เพื่อที่ข้อมูลผู้ถือบัตรจะได้ไม่ถูกนำมาฟื้นฟูใหม่ | 9.8.2 ตรวจสอบว่าข้อมูลผู้ถือบัตรบนสื่ออิเล็กทรอนิกส์ถูก render ให้ไม่สามารถกู้คืนได้ด้วยโปรแกรมการล้างข้อมูลร่วมกับ มาตรฐานที่ยอมรับในระดับอุตสาหกรรมสำหรับการลบข้อมูลอย่างปลอดภัย หรือ ทำลายสื่อนั้นๆทางกายภาพ) | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.9 ปกป้องอุปกรณ์ซึ่งตรวจจับข้อมูล (capture) บัตรชำระเงินด้วยวิธีการทางกายภาพจากการปลอมแปลง (tampering)และ การทำแทน (substitution)<br><br>หมายเหตุ: ความต้องการนี้ใช้กับ อุปกรณ์อ่านบัตรซึ่งใช้ในธุรกรรมที่มีการแสดงบัตรจริง (เช่นการรูด หรือเสียบบัตร) ในสถานที่ขาย ความต้องการนี้ไม่ได้มีจุดประสงค์สำหรับการป้อนคีย์ด้วยมือ เช่นจากคีย์บอร์ดคอมพิวเตอร์ แล *POS keypad*<br><br>หมายเหตุ: ความต้องการ *9.9* คือวิธีการที่ดีที่สุดจนถึง 30 มิถุนายน 2556 หลังจากกลายเป็นความต้องการ | 9.9 ตรวจสอบเอกสารนโยบายและกระบวนการ เพื่อตรวจว่าได้มี:<br>• การบำรุงรักษารายการของอุปกรณ์<br>• การตรวจสอบอุปกรณ์เพื่อตรวจตราการปลอมแปลง หรือ ทำแทน เป็นระยะๆ<br>• ฝึกฝนบุคลากรให้ตระหนักถึงการกระทำที่มีพิรุธ และรายงายการปลอมแปลง หรือการทำแทนของอุปกรณ์ | ความพยายามโจรกรรมข้อมูลผู้ถือบัตรโดยการขโมยและ/หรือ ควบคุมอุปกรณ์อ่านบัตร เช่น พยายามขโมยอุปกรณ์ไปเพื่อศึกษาว่าจะสามารถเจาะเข้าไปได้อย่างไร และมักมีการพยายามแทนที่อุปกรณ์ที่ถูกต้องด้วยอุปกรณ์ที่ปลอมแปลงซึ่งส่งข้อมูลบัตรชำระเงินไปให้พวกเจา ผู้โจรกรรมจะพยายาม “ดักข้อมูล (skimming)” โดยส่วนประกอบภายนอกของอุปกรณ์ ซึ่งออกแบบมาให้ตรวจจับข้อมูลรายละเอียดบัตรชำระเงินก่อนที่จะใส่บัตรเข้าไป — เช่น ด้วยการสวมเครื่องอ่านบัตรเพิ่มเติมเหนือเครื่องอ่านบัตรที่ถูกต้องซึ่งทำให้ข้อมูลถูกตรวจจับ 2 ครั้ง: ซึ่งทำให้การทำธุรกรรมเป็นไปอย่างสำเร็จ แต่ผู้โจรกรรมจะได้ข้อมูลบัตรไปพร้อมกันด้วย<br><br>ความต้องการนี้แนะนำ แต่ไม่ได้เป็นความต้องการ ในการป้อนข้อมูลด้วยมือ เช่น ผ่านคีย์บอร์ดคอมพิวเตอร์ และ POS keypad<br><br>วิธีการที่ดีที่สุดอื่นๆในการป้องกันการ ดักข้อมูล (skimming) มีให้ศึกษาบนเว็บไซต์ PCI SSC |
| 9.9.1 บำรุงรักษารายการอุปกรณ์ให้เป็นปัจจุบัน รายการควรมี:<br>• รุ่น และการผลิตของอุปกรณ์<br>• สถานที่ของอุปกรณ์ (เช่น สถานที่ของอาคาร ซึ่งอุปกรณ์นี้ตั้งอยู่)<br>• Serial number หรือ วิธีการระบุตัวตนอื่นๆของอุปกรณ์ | 9.9.1.a ตรวจสอบรายการอุปกรณ์เพื่อตรวจสอบว่ามี:<br>• รุ่น และการผลิตของอุปกรณ์<br>• สถานที่ของอุปกรณ์ (เช่น สถานที่ของอาคาร ซึ่งอุปกรณ์นี้ตั้งอยู่)<br>• Serial number หรือ วิธีการระบุตัวตนอื่นๆของอุปกรณ์<br><br>9.9.1.b เลือกตัวอย่างจากอุปกรณ์ในรายการ และสังเกตสถานที่ของอุปกรณ์ เพื่อตรวจสอบว่ารายการนั้นแม่นยำ และเป็นปัจจุบัน<br><br>9.9.1.c สัมภาษณ์บุคลากรเพื่อตรวจสอบว่ารายการนั้นเป็นปัจจุบัน เมื่อมีการเพิ่ม ย้าย ปลด อุปกรณ์ หรืออื่นๆ | อัพเดทรายการอุปกรณ์ ช่วยให้องค์กรสามารถติดตามอุปกรณ์ให้อยู่ในที่ที่ควรเป็นได้ และสามารถรู้ได้รวดเร็วหากอุปกรณ์สูญหายหรือถูกขโมย<br><br>วิธีการจัดการรายการอุปกรณ์ อาจทำโดยกระบวนการอัตโนมัติ (เช่น ด้วยระบบจัดการอุปกรณ์) หรือทำด้วยมือ (เช่น เอกสารบันทึกอิเล็กทรอนิกส์ หรือ สิ่งพิมพ์) สำหรับอุปกรณ์ที่ไม่ใช่อุปกรณ์ที่ใช้สำหรับนอกสถานที่ สถานที่อุปกรณ์อาจระบุชื่อบุคลากรผู้ได้รับมอบหมายไว้ด้วยก็ได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.9.2 การตรวจสอบอุปกรณ์เป็นระยะๆสำหรับตรวจการปลอมแปลง (เช่น อุปกรณ์ดักข้อมูล) หรือ การทำแทน (เช่น ด้วยการตรวจสอบ serial number หรือ ลักษณะเฉพาะอื่นๆเพื่อตรวจสอบว่าไม่ได้มีการนำอุปกรณ์ปลอมมาทดแทน)<br><br>หมายเหตุ: ตัวอย่างสัญญาณที่บ่งชี้ว่าอุปกรณ์อาจถูกปลอมแปลง หรือแทนที่ ได้แก่ สายที่เชื่อมต่อ หรือ ส่วนต่อเติมที่ไม่ทราบที่มาที่ไป การสูญหาย หรือ เปลี่ยนแปลงของฉลากความปลอดภัย การแตกหัก หรือ สีที่แตกต่างจากเดิน หรือการเปลี่ยนแปลงของ *serial number* หรือ การทำเครื่องหมายอื่นๆ | 9.9.2.a ตรวจสอบเอกสารกระบวนการ เพื่อตรวจสอบว่าได้มีสิ่งต่อไปนี้กำหนดไว้:<br>• มีกระบวนการสำหรับตรวจสอบอุปกรณ์<br>• ความถี่ของกระบวนการ<br><br>9.9.2.b สัมภาษณ์บุคลากรที่รับผิดชอบ และสังเกตกระบวนการตรวจสอบเพื่อดูว่า:<br>• บุคลากรตระหนักถึงกระบวนการตรวจสอบอุปกรณ์<br>• อุปกรณ์ทั้งหมดได้รับการตรวจสอบหลักฐานการปลอมแปลง หรือ ทำแทน เป็นระยะๆ | การตรวจสอบอุปกรณ์อย่างสม่ำเสมอช่วยให้องค์กรสามารถตรวจจับการปลอมแปลง หรือ แทนที่อุปกรณ์ได้รวดเร็วขึ้น และ ลดความเสี่ยงผลกระทบจากการกระทำดังกล่าว<br><br>ประเภทของการตรวจสอบขึ้นอยู่กับอุปกรณ์ — เช่น การถ่ายรูป ซึ่งทำให้สามารถเปรียบเทียบได้ว่าอุปกรณ์ปัจจุบันมีการเปลี่ยนแปลงไปหรือไม่<br>อีกทางเลือกคือการใช้การทำเครื่องหมาย เช่น UV light marker (การทำเครื่องหมายซึ่งสามารถมองเห็นเมื่อฉายแสง) เพื่อทำเครื่องหมายบนพื้นผิวอุปกรณ์ ผู้โจรกรรมมักเปลี่ยนเคสด้านนอกของอุปกรณ์เพื่อ ปิดบังการปลอมแปลง และวิธีการเหล่านี้ช่วยให้ตรวจจับได้ ผู้ขายอุปกรณ์อาจให้คำแนะนำความปลอดภัย และคำแนะนำ “ทำอย่างไร (how to)” เพื่อช่วยตรวจสอบการปลอมแปลง<br><br>ความถี่การตรวจสอบขึ้นอยู่กับปัจจัย เช่นสถานที่ตั้งของอุปกรณ์ และอุปกรณ์ได้รับการดูแลใส่ใจหรือไม่ เช่น อุปกรณ์ถูกวางทิ้งไว้ในที่สาธารณะ โดยไม่มีผู้ดูแล ซึ่งบุคลากรจากองค์กรอาจต้องตรวจสอบบ่อยครั้งกว่าอุปกรณ์ที่เก็บไว้ในที่ปลอดภัย วิธีการตรวจสอบอุปกรณ์และความถี่ ขึ้นอยู่กับการกำหนดของผู้ขาย อย่างที่ได้กำหนดไว้ในการประเมินความเสี่ยงประจำปี |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 9.9.3 ให้การฝึกฝนสำหรับบุคลากรเพื่อตระหนักถึงความพยายามในการปลอมแปลงหรือการแทนที่อุปกรณ์ การฝึกฝนควรมีดังต่อไปนี้:<br>• ตรวจสอบการระบุตัวตนบุคคลที่ 3 ใดๆ ที่อ้างว่าเป็นบุคลากรด้านการซ่อมแซม หรือบำรุงรักษา ก่อนให้สิทธิพวกเขาเข้าถึงการปรับแต่ง หรือแก้ปัญหาของอุปกรณ์<br>• ไม่ติดตั้ง แทนที่ หรือ ส่งคืนอุปกรณ์โดยไม่มีการตรวจสอบ<br>• ตระหนักถึงการกระทำที่มีพิรุธรอบๆอุปกรณ์ (เช่น ความพยายามโดยบุคคลที่ไม่รู้จักในการถอดสาย หรือ งัดแงะอุปกรณ์)<br>• รายงานการกระทำที่มีพิรุธ และส่อถึงการปลอมแปลง หรือ ทำแทน อุปกรณ์ไปยังบุคลากรที่เหมาะสม (เช่น รายงานไปยังผู้จัดการ หรือพนักงานรักษาความปลอดภัย) | 9.9.3.a ตรวจทานวัสดุการฝึกฝนสำหรับบุคลากรในสถานที่ point-of-sale เพื่อตรวจสอบว่ามีการฝึกฝนดังต่อไปนี้:<br>• ตรวจสอบตัวตนของบุคคลที่ 3 ใดๆ ที่อ้างว่าเป็นบุคลากรด้านการซ่อมแซม หรือบำรุงรักษา ก่อนให้สิทธิพวกเขาเข้าถึงการปรับแต่ง หรือ แก้ปัญหาของอุปกรณ์<br>• ไม่ติดตั้ง แทนที่ หรือ ส่งคืนอุปกรณ์โดยไม่มีการตรวจสอบ<br>• ตระหนักถึงการกระทำที่มีพิรุธรอบๆอุปกรณ์ (เช่น ความพยายามโดยบุคคลที่ไม่รู้จักในการถอดสาย หรือ งัดแงะอุปกรณ์)<br>• รายงานการกระทำที่มีพิรุธ และส่อถึงการปลอมแปลง หรือ ทำแทน อุปกรณ์ไปยังบุคลากรที่เหมาะสม (เช่น รายงานไปยังผู้จัดการ หรือพนักงานรักษาความปลอดภัย)<br><br>9.9.3.b สัมภาษณ์ตัวอย่างบุคลากรในสถานที่ point-of-sale เพื่อตรวจสอบว่าพวกเขาได้รับการฝึกฝนและตระหนักถึงขั้นตอนดังนี้:<br>• ตรวจสอบตัวตนของบุคคลที่ 3 ใดๆ ที่อ้างว่าเป็นบุคลากรด้านการซ่อมแซม หรือบำรุงรักษา ก่อนให้สิทธิพวกเขาเข้าถึงการปรับแต่ง หรือ แก้ปัญหาของอุปกรณ์<br>• ไม่ติดตั้ง แทนที่ หรือ ส่งคืนอุปกรณ์โดยไม่มีการตรวจสอบ<br>• ตระหนักถึงการกระทำที่มีพิรุธรอบๆอุปกรณ์ (เช่น ความพยายามโดยบุคคลที่ไม่รู้จักในการถอดสาย หรือ งัดแงะอุปกรณ์)<br>• รายงานการกระทำที่มีพิรุธ และส่อถึงการปลอมแปลง หรือ ทำแทน อุปกรณ์ไปยังบุคลากรที่เหมาะสม (เช่น รายงานไปยังผู้จัดการ หรือพนักงานรักษาความปลอดภัย) | ผู้โจรกรรมมักจะแสดงตนเป็นบุคลากรด้านการซ่อมแซม หรือบำรุงรักษาเพื่อได้รับสิทธิเข้าถึงอุปกรณ์ POS การร้องขอการเข้าถึงอุปกรณ์จากบุคคลที่ 3 ใดๆก็ตาม ควรได้รับการตรวจสอบเสมอ — เช่น โดยการตรวจสอบกับผู้จัดการ หรือ โทรศัพท์ไปสอบถามบริษัทบำรุงรักษา POS (เช่น ผู้ขาย หรือผู้ให้บริการแก่ผู้รับบัตร) ผู้โจรกรรมส่วนใหญ่มักพยายามหลอกล่อบุคลากรโดยการแต่งกาย (เช่น ถือกล่องเครื่องมือ และแต่งชุดทำงาน) และ อาจมีความรู้เกี่ยวกับสถานที่ของอุปกรณ์ จึงเป็นสิ่งสำคัญที่บุคลากรควรได้รับการฝึกฝนให้ดำเนินการตามนั้นตอนทุกครั้ง<br><br>อีกกลวิธีที่ผู้โจรกรรมมักใช้คือการส่ง ระบบ POS “ใหม่” พร้อมวิธีการสับเปลี่ยนอุปกรณ์กับอุปกรณ์ที่ถูกต้อง และ “ส่งคืน” ระบบที่ถูกต้องไปยังสถานที่ที่ระบุ ผู้โจรกรรมอาจแม้แต่ให้หมายเลขที่อยู่ที่จัดส่งคืนเพื่อจะได้ครอบครองอุปกรณ์เหล่านี้ บุคลากรต้องตรวจสอบกับผู้จัดการหรือ ผู้สนับสนุน (supplier) ว่าอุปกรณ์นั้นถูกต้อง และมาจากแหล่งที่เชื่อถือได้ก่อนติดตั้ง และนำมาใช้กับธุรกิจ |
| 9.10 ทำให้มั่นใจว่านโยบายความปลอดภัย และกระบวนการดำเนินการเพื่อจำกัดการเข้าถึงทางกายภาพไปยังข้อมูลผู้ถือบัตร are ได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และ เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 9.10 ตรวจสอบเอกสาร และสัมภาษณ์บุคลากร เพื่อตรวจสอบว่านโยบายความปลอดภัย และกระบวนการดำเนินการ for restricting การเข้าถึงทางกายภาพไปยังข้อมูลผู้ถือบัตรนั้น:<br>• ได้รับการบันทึกเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรต้องตระหนักถึงและดำเนินการตามนโยบายความปลอดภัย และกระบวนการดำเนินการ for restricting การเข้าถึงทางกายภาพไปยังข้อมูลผู้ถือบัตรและCDE systems อย่างต่อเนื่อง |

# เฝ้าติดตาม และ ทดสอบเครือข่าย

**ความต้องการที่ 10: ติดตาม และ เฝ้าดูการเข้าถึงเครือข่ายทั้งหมดไปยังแหล่งเครือข่ายและข้อมูลผู้ถือบัตร**

กลไกการบันทึกประวัติ และความสามารถในการติดตามกิจกรรมของผู้ใช้ เป็นสิ่งสำคัญในการป้องกัน การตรวจจับ หรือ การลดผลกระทบจากการเจาะข้อมูลให้น้อยที่สุด การมีการบันทึกประวัติในทุกๆสิ่งแวดล้อมช่วยในการติดตาม การแจ้งเตือน และการวิเคราะห์เมื่อเกิดสิ่งผิดปกติ การรำบุสาเหตุการเจาะข้อมูลนั้นเป็นเรื่องที่ยากมาก หากไม่มีระบบประวัติกิจกรรมแล้ว แทบเป็นไปไม่ได้เลย

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.1 ดำเนินการตรวจสอบประวัติ เพื่อเชื่อมโยงไปยังการเข้าถึงทั้งหมดไปสู่ส่วนประกอบระบบของผู้ใช้งานแต่ละคน | 10.1 ตรวจสอบ ผ่านการสังเกตและสัมภาษณ์ผู้ดูแลระบบว่า:<br>• มีการเปิดใช้งานและการดำเนินการ การตรวจสอบประวัติในส่วนประกอบระบบ<br>• การเข้าถึงไปยังส่วนประกอบระบบ มีการเชื่อมโยงไปยังผู้ใช้แต่ละคน | เป็นสิ่งสำคัญที่จะมีกระบวนการ หรือระบบซึ่งเชื่อมโยงไปยังการเข้าถึงของผู้ใช้ไปยังส่วนประกอบระบบ ระบบนี้จะสร้างประวัติการเข้าถึง และ ให้ความสามารถในการติดตามการกระทำไปยังเฉพาะผู้ใช้ที่มีพิรุธ |
| 10.2 ดำเนินการตรวจสอบประวัติสำหรับส่วนประกอบระบบทั้งหมด เพื่อสร้างสิ่งเหล่านี้ขึ้นมาใหม่: | 10.2 จากการสัมภาษณ์บุคลากรที่รับผิดชอบ การสังเกตการตรวจสอบประวัติ และ การตรวจสอบการตั้งค่าการตรวจสอบประวัติ ดำเนินการดังนี้: | สร้างการตรวจสอบประวัติการกระทำที่น่าสงสัยเพื่อแจ้งเตือนผู้ดูแลระบบ ส่งข้อมูลไปยังกลไกการเฝ้าติดตามอื่นๆ (เช่น ระบบตรวจจับการบุกรุก) และให้ประวัติการกระทำ มีการติดตามต่อหลังเหตุการณ์ การบันทึกประวัติของเหตุการณ์จะช่วยให้สามารถติดตามกิจกรรมที่มีความเสี่ยงได้ |
| 10.2.1 การเข้าถึงข้อมูลผู้ถือบัตรของผู้ใช้แต่ละคน | 10.2.1 ตรวจสอบว่าการเข้าถึงไปยังข้อมูลผู้ถือบัตรของแต่ละคนได้รับการบันทึก | ผู้ประสงค์ร้าย อาจรับมีข้อมูลบัญชีผู้ใช้ พร้อมสิทธิการเจ้าถึงไปยังระบบใน CDE หรือพวกเขาอาจสร้างบัญชีที่ไม่ได้รับอนุญาตขึ้นมาใหม่ เพื่อเข้าถึงข้อมูลผู้ถือบัตร บันทึกของการเข้าถึงของบุคคลใดๆ ไปยังข้อมูลผู้ถือบัตรสามารถช่วยระบุได้ว่าบัญชีไหนที่อาจถูกเจาะข้อมูล หรือนพไปใช้ในทางที่ผิด |
| 10.2.2 การกระทำโดยผู้ใช้ใดๆก็ตามที่มีสิทธิรากฐาน (root) หรือ สิทธิผู้ดูแลระบบ | 10.2.2 ตรวจสอบว่าการกระทำทั้งหมดที่ทำโดยผู้ใช้ใดๆก็ตามที่มีสิทธิรากฐาน (root) หรือ สิทธิผู้ดูแลระบบได้รับการบันทึกประวัติ | บัญชีที่มีสิทธิพิเศษเพิ่มขึ้นมา เช่น ผู้ดูแลระบบ หรือ สิทธิรากฐาน (root) มีผลกระทบอย่างมากต่อความปลอดภัย หรือ ฟังก์ชั่นการทำงานของระบบ หากไม่มีการบันทึกประวัติ องค์กรไม่สามารถติดตามปัญหาใดๆได้จากการใช้ สิทธิผู้ดูแลในทางที่ผิด หรือเกิดข้อผิดพลาด หรือติดตามการกระทำกลับไปหาบุคคลได้ |

| . | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.2.3 การเข้าถึงไปยังการตรวจสอบประวัติ | 10.2.3 ตรวจสอบว่าการเข้าถึงทั้งหมดไปยังการตรวจสอบประวัติได้รับการบันทึก | ผู้ประสงค์ร้ายมักพยายามแก้ไขประวัติของการกระทำของพวกเขา ประวัติการเข้าถึง จะช่วยให้องค์กรสามารถติดตามความไม่สอดคล้อง หรือ โอกาสในการปลอมแปลงของประวัติกลับไปยังผู้ใช้ได้ การเข้าถึงส่วนประวัติ เปลี่ยนแปลง เพิ่ม และลบ จะช่วยให้สามารถติดตามประวัติย้อนกลับไปยังบุคลากรที่กระทำได้ |
| 10.2.4 ความพยายามการเข้าระบบที่ไม่สมบูรณ์ | 10.2.4 ตรวจสอบว่าความพยายามการเข้าระบบที่ไม่สมบูรณ์ได้รับการบันทึก | ผู้ประสงค์ร้ายมักพยายามเข้าถึงระบบเป้าหมายหลายครั้ง ความพยายามการเข้าระบบที่ไม่สมบูรณ์อาจแสดงให้เห็น การพยายามใช้การคาดเดาจากผู้ที่ไม่ได้รับอนุญาตในการเข้าระบบ |
| 10.2 5 การใช้ และการเปลี่ยนแปลงการระบุตัวตน กลไกการรับรองตัวตน — รวมไปถึง (เป็นเพียงตัวอย่างไม่ได้จำกัดไว้เพียงเท่านี้) การสร้างบัญชีใหม่ และการยกระดับสิทธิพิเศษ — การเปลี่ยนแปลงทั้งหมด การเพิ่ม หรือ การลบ บัญชีรากฐาน (root) หรือ บัญชีที่มีสิทธิผู้ดูแล | 10.2.5.a ตรวจสอบว่าการใช้การระบุตัวตน กลไกการรับรองตัวตนได้รับการบันทึก<br>10.2.5.b ตรวจสอบว่าการยกระดับสิทธิพิเศษได้รับการบันทึก<br>10.2.5.c ตรวจสอบว่า การเปลี่ยนแปลงทั้งหมด การเพิ่ม หรือ การลบ บัญชีรากฐาน (root) หรือ บัญชีที่มีสิทธิผู้ดูแลได้รับการบันทึก | หากไม่ทราบว่าผู้ใดเป็นผู้ log on ในเวลาที่เกิดเหตุการณ์ มันเป็นไปไม่ได้เลยที่จะระบุตัวตนผู้ใช้บัญชี นอกจากนั้น ผู้ประสงค์ร้าย อาจพยายามจัดการกับการควบคุมการรับรองตัวตนเพื่อจะ bypass หรือ แอบอ้างบัญชีที่มีอยู่ได้ |
| 10.2.6 การเริ่ม หยุด หรือ หยุดชั่วคราวของการตรวจสอบประวัติ | 10.2.6 ตรวจสอบว่าสิ่งเหล่านี้ได้รับการบันทึก:<br>• การเริ่มของการตรวจสอบประวัติ<br>• การหยุด หรือ หยุดชั่วคราวของการตรวจสอบประวัติ | การปิดการตรวจสอบประวัติ (หรือหยุดชั่วคราว) ก่อนการกระทำที่ผิดกฎหมายเป็นวิธีการที่ผู้ประสงค์ร้ายมักใช้เพื่อหลักเลี่ยงการตรวจจับ การเริ่มใหม่ของการตรวจสอบประวัติอาจแสดงให้เห็นว่ามีการหยุดระบบโดยผู้ใช้เพื่อปิดบังการกระทำของพวกเขา |
| 10.2.7 การสร้าง และลบ object ระดับระบบ (system object) | 10.2.7 ตรวจสอบว่าการสร้าง และลบ object ระดับระบบ (system object) ได้รับการบันทึก | Software ที่ประสงค์ร้าย เช่น malware มักสร้าง หรือ แทนที่ system object บนระบบเป้าหมายเพื่อควบคุมฟังก์ชั่นที่ต้องการ หรือดำเนินการใดๆบนระบบนั้นๆ การบันทึกประวัติเมื่อ system object เช่น ตารางฐานข้อมูล หรือ กระบวนการที่บันทึกไว้ ได้รับการสร้าง หรือลบ จะเป็นการง่ายขึ้นในการระบุว่าการเปลี่ยนแปลงเหล่านั้นได้รับการอนุญาตหรือไม่ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.3 สำหรับส่วนประกอบระบบทั้งหมด บันทึกกิจกรรมอย่างน้อยดังต่อไปนี้: | 10.3 จากการจากการสัมภาษณ์ และสังเกตประวัติการตรวจสอบสำหรับแต่ละเหตุการณ์ที่ตรวจสอบได้ (จาก 10.2) ดำเนินการดังนี้: | จากการบันทึกรายละเอียดเหล่านี้สำหรับเหตุการณ์ที่ตรวจสอบได้ใน 10.2 ความเสี่ยงในการเกิดการเจาะข้อมูลจะสามารถถูกตรวจพบได้อย่างรวดเร็ว และหากมีข้อมูลเพียงพอ จะสามารถทราบได้ว่า ใคร ทำอะไร ที่ไหน เมื่อไร และ อย่างไร |
| 10.3.1 การระบุตัวตน | 10.3.1 ตรวจสอบว่า การระบุตัวตนได้รับการบันทึก | |
| 10.3.2 ประเภทเหตุการณ์ | 10.3.2 ตรวจสอบว่า ประเภทเหตุการณ์ได้รับการบันทึก | |
| 10.3.3 วันที่ และ เวลา | 10.3.3 ตรวจสอบว่า วันที่ และ เวลาได้รับการบันทึก | |
| 10.3.4 การบ่งชี้ ความสำเร็จ และ ล้มเหลว | 10.3.4 ตรวจสอบว่า การบ่งชี้ ความสำเร็จ และ ล้มเหลวได้รับการบันทึก | |
| 10.3.5 ต้นกำเนิดของเหตุการณ์ | 10.3.5 ตรวจสอบว่า ต้นกำเนิดของเหตุการณ์ได้รับการบันทึก | |
| 10.3.6 เอกลักษณ์ หรือ ชื่อ ของข้อมูล ส่วนประกอบระบบ หรือสิ่งแวดล้อมที่ได้รับผลกระทบ | 10.3.6 ตรวจสอบว่า เอกลักษณ์ หรือ ชื่อ ของข้อมูล ส่วนประกอบระบบหรือสิ่งแวดล้อมที่ได้รับผลกระทบได้รับการบันทึก | |
| 10.4 การใช้เทคโนโลยีการประสานเวลา (time-synchronization) เพื่อsync นาฬิกาและเวลาของระบบสำคัญทั้งหมด และทำให้มั่นใจว่ามีการดำเนินการข้างต้นกับเวลาในการดำเนินการสำหรับการ ค้นหา แจกจ่าย และจัดเก็บ<br>หมายเหตุ: ตัวอย่างของ time synchronization คือ Network Time Protocol (NTP) | 10.4 ตรวจสอบการมาตรฐานการตั้งค่าและกระบวนการ เพื่อตรวจสอบว่าเทคโนโลยี time-synchronization ได้มีการดำเนินการและทำให้เป็นปัจจุบัน ตามความต้องการ PCI DSS 6.1 และ 6.2 | เทคโนโลยี Time synchronization ใช้เพื่อการ sync นาฬิกาบนระบบหลายๆระบบ หากนาฬิกาไม่รับได้รับ sync ให้ตรงกัน ไม่เป็นไปไม่ได้ก็เป็นสิ่งที่ยากในการเปรียบเทียบไฟล์ประวัติจากระบบที่ต่างกันและสร้างลำดับเหตุการณ์ (สิ่งสำคัญสำหรับการวิเคราะห์ทางกฎหมายถึงกิจกรรมการฝ่าระบบ) สำหรับทีมพิสูจน์หลักฐาน เวลาที่แม่นยำ และ ความเที่ยงตรงสอดคล้องกันระหว่างระบบทุกระบบเป็นสิ่งสำคัญในการระบุวิธีการที่ระบบถูกเจาะข้อมูลได้ |
| 10.4.1 ระบบที่สำคัญมีเวลาที่ถูกต้อง และตรงกัน | 10.4.1.a ตรวจสอบกระบวนการ ค้นหา แจกจ่าย และจัดเก็บมีเวลาที่ถูกต้องตรงกันภายในองค์กรเพื่อตรวจสอบว่า:<br>• เฉพาะเซิฟเวอร์ศูนย์เวลากลาง (central time server) ที่กำหนดเท่านั้นที่จะได้รับสัญญาณเวลาจากแหล่งภายนอก และแหล่งภายนอกนั้นมีพื้นฐานบน International Atomic Time หรือ UTC<br>• ในที่ที่มีการกำหนดเซิฟเวอร์เวลามากกว่าหนึ่ง ให้เซิฟเวอร์เวลาเปรียบเทียบเวลาเข้าหากันเพื่อรักษาความเที่ยงตรง<br>• ระบบต่างๆรับข้อมูลเวลาจากเฉพาะจากเซิฟเวอร์ศูนย์เวลากลาง (central time server) ที่กำหนดเท่านั้น | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 10.4.1.b สังเกตการตั้งค่าตัวแปรที่เกี่ยวข้องกับเวลาในระบบสำหรับตัวอย่างส่วนประกอบระบบเพื่อตรวจสอบว่า:<br>• เฉพาะเซิฟเวอร์ศูนย์เวลากลาง (central time server) ที่กำหนดเท่านั้นที่จะได้รับสัญญาณเวลาจากแหล่งภายนอก และแหล่งภายนอกนั้นมีพื้นฐานบน International Atomic Time หรือ UTC<br>• ในที่ที่มีการกำหนดเซิฟเวอร์เวลามากกว่าหนึ่ง ให้เซิฟเวอร์เวลาเปรียบเทียบเวลาเข้าหากันเพื่อรักษาความเที่ยงตรง<br>• ระบบต่างๆรับข้อมูลเวลาจากเฉพาะจากเซิฟเวอร์ศูนย์เวลากลาง (central time server) ที่กำหนดเท่านั้น | |
| 10.4.2 ข้อมูลเวลาได้รับการปกป้อง | 10.4.2.a ตรวจสอบการตั้งค่าระบบและการตั้งค่า time- synchronization เพื่อตรวจสอบว่าการเข้าถึงข้อมูลเวลาได้ถูกจำกัดเอาไว้เฉพาะบุคลากรที่มีความต้องการทางธุรกิจในการเข้าถึงเท่านั้น | |
| | 10.4.2.b ตรวจสอบการตั้งค่าระบบ การตั้งค่า time synchronization และ ประวัติและกระบวนการ เพื่อตรวจสอบว่าการเปลี่ยนแปลงใดๆไปยังการตั้งค่าเวลาระบบที่สำคัญได้รับการบันทึก เฝ้าติดตาม และตรวจทาน | |
| 10.4.3 การตั้งค่าเวลามาจากแหล่งที่ได้รับการยอมรับระดับอุตสาหกรรม | 10.4.3 ตรวจสอบการตั้งค่าระบบ เพื่อตรวจสอบว่า เซิฟเวอร์เวลา ยอมรับการอัพเดทจากแหล่งภายนอกที่ได้รับการยอมรับระดับอุตสาหกรรม (เพื่อป้องกันไม่ให้ผู้ประสงค์ร้ายเปลี่ยนนาฬิกาได้) ตัวเลือกเพิ่มเติมคือ การอัพเดทเหล่านั้นสามารถถูกเข้ารหัสได้ด้วย การเข้ารหัสข้อมูลด้วยกุญแจเดี่ยว (symmetric key) และรายการการควบคุมการเข้าถึง สามารถถูกสร้าง ซึ่งให้เฉพาะ IP address ที่กำหนดของเครื่องลูกค้า (client machine)ที่จะได้รับการอัพเดทเวลา (เพื่อป้องกันผู้ไม่ได้รับอนุญาตจากการใช้เซิฟเวอร์เวลาภายใน) | |
| 10.5 รักษาความปลอดภัยการตรวจสอบประวัติการตรวจตราว่าไม่สามารถถูกเปลี่ยนแปลงได้ | 10.5 สัมภาษณ์ผู้ดูแลระบบ และตรวจสอบการตั้งค่าระบบและการอนุญาต เพื่อตรวจสอบว่าการตรวจสอบประวัติการตรวจตราได้รับการรักษาความปลอดภัยให้ไม่สามารถถูกเปลี่ยนแปลงได้ | บ่อยครั้งที่ผู้ประสงค์ร้ายผู้สามารถเข้าเครือข่ายได้จะพยายามแก้ไขประวัติการตรวจสอบเพื่อปิดบังการกระทำของตน หากไม่มีการป้องกันที่เหมาะสมต่อประวัติการตรวจสอบ ก็ไม่สามารถการันตีความสมบูรณ์ และแม่นยำได้ และประวัติการตรวจสอบอาจถูก render ให้ใช้ประโยชน์ไม่ได้จากการเจาะข้อมูลก็เป็นได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.5.1 จำกัดการเข้าดูการตรวจสอบประวัติการตรวจตราให้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น | 10.5.1 เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องที่สามารถดูการตรวจสอบประวัติการตรวจตราได้ | การป้องกันที่เหมาะสมสำหรับการตรวจสอบประวัติการตรวจตรา ได้แก่ การควบคุมการเข้าถึงที่เข้มงวด (จำกัดการเข้าถึงประวัติบนพื้นฐาน “ความต้องการที่รู้ของขอ (need to know)” เท่านั้น) และใช้การแบ่งการเข้าถึงทางกายภาพ หรือ ทางเครือข่ายเพื่อให้ประวัติถูกพบ และปรับแต่งได้ยากขึ้น<br>การ Back up ไฟล์การตรวจสอบประวัติการตรวจตราอย่างรวดเร็ว เพื่อรวมเซิฟเวอร์ประวัติหรือสื่อซึ่งยากต่อการเปลี่ยนแปลง ทำให้ประวัติได้รับการป้องกันแม้ว่าระบบสร้างประวัติจะถูกเจาะข้อมูล |
| 10.5.2 ป้องกันการตรวจสอบประวัติการตรวจตราจากการปรับแต่งที่ไม่ได้รับอนุญาต | 10.5.2 การตรวจสอบประวัติการตรวจตราปัจจุบันต้องได้รับการป้องกัน from จากการปรับแต่งที่ไม่ได้รับอนุญาตด้วยกลไกการควบคุมการเข้าถึง การแบ่งการเข้าถึงทางกายภาพ และ/หรือ การแบ่งการเข้าถึงทางเครือข่าย | |
| 10.5.3 Back up ไฟล์การตรวจสอบประวัติการตรวจตราอย่างรวดเร็ว เพื่อรวมเซิฟเวอร์ประวัติหรือสื่อซึ่งยากต่อการเปลี่ยนแปลง | 10.5.3 ไฟล์การตรวจสอบประวัติการตรวจตราปัจจุบันจะต้องได้รับการ backed up อย่างรวดเร็ว เพื่อรวมเซิฟเวอร์ประวัติหรือสื่อซึ่งยากต่อการเปลี่ยนแปลง | |
| 10.5.4 เขียนประวัติสำหรับเทคโนโลยีที่เปิดเผยสู่สาธารณะบน เซิฟเวอร์ประวัติ หรือ สื่อที่ปลอดภัย ภายในของส่วนกลาง | 10.5.4 ประวัติสำหรับเทคโนโลยีที่เปิดเผยสู่สาธารณะบน เซิฟเวอร์ประวัติ หรือ สื่อที่ปลอดภัย ภายในของส่วนกลาง | ด้วยการเขียนประวัติสำหรับเทคโนโลยีที่เปิดเผยสู่สาธารณะ เช่น wireless, firewall, DNS, และ mail server ความเสี่ยงที่ประวัติเหล่านั้นจะสูญหาย หรือ ถูกเปลี่ยนแปลงจะลดน้อยลง เนื่องจากสิ่งเหล่านี้จะปลอดภัยมากกว่าเมื่ออยู่ในเครือข่ายภายใน<br>ประวัติอาจถูกเขียนโดยตรง โหลดมาจากหรือคัดลอกจากระบบภายนอกไปยังระบบหรือสื่อภายในที่ปลอดภัย |
| 10.5.5 การใช้การเฝ้าติดตามความสมบูรณ์ของไฟล์ หรือ software การตรวจความเปลี่ยนแปลง กับประวัติ ทำให้มั่นใจว่าข้อมูลประวัติที่มีอยู่จะไม่ถูกเปลี่ยนแปลงหากไม่มีการแจ้งเตือน (อย่างไรก็ตาม ข้อมูลใหม่ที่เพิ่มเข้ามาไม่ควรทำให้เกิดการแจ้งเตือน) | 10.5.5 ตรวจสอบการตั้งค่าระบบ เฝ้าติดตามไฟล์ และ ผลจากการติดตามการกระทำต่างๆ เพื่อตรวจสอบการใช้การเฝ้าติดตามความสมบูรณ์ของไฟล์ หรือ software การตรวจความเปลี่ยนแปลง กับประวัติ | การติดตามความสมบูรณ์ของไฟล์ หรือ ระบบการตรวจความเปลี่ยนแปลง จะตรวจสอบการเปลี่ยนแปลงไปยังไฟล์ที่สำคัญ และแจ้งเตือนเมื่อมีการจดบันทึกการเปลี่ยนแปลง สำหรับจุดประสงค์การติดตามความสมบูรณ์ หน่วยงานมักติดตามไฟล์ซึ่งไม่มีการเปลี่ยนแปลงเป็นประจำ เมื่อเกิดการเปลี่ยนแปลงก็จะแสดงให้เห็นถึงความเป็นไปได้ในการเจาะข้อมูล |
| 10.6 ตรวจทานประวัติ และ กิจกรรมความปลอดภัยสำหรับส่วนประกอบระบบทั้งหมดเพื่อระบุ to identify ความผิดปกติ หรือกิจกรรมที่ต้องสงสัย<br>หมายเหตุ: การรวบรวมประวัติ วิเคราะห์ และเครื่องมือการแจ้งเตือน อาจถูกนำมาใช้ได้เพื่อให้บรรลุความต้องการนี้ | 10.6 ดำเนินการดังต่อไปนี้: | การฝ่าระบบส่วนมากเกิดขึ้นหลายวัน หรือเดือน ก่อนการตรวจพบ การตรวจสอบประวัติทุกๆวันช่วยเพิ่มขีดความปลอดภัย และลดระยะเวลาในการตรวจหาการเจาะระบบ<br>ตรวจสอบประวัติอยู่เป็นประจำโดยบุคลากร หรือด้วยระบบอัตโนมัติ สามารถระบุ และ จัดการการเข้าถึงที่ไม่ได้รับอนุญาตไปยังสิ่งแวดล้อมข้อมูลผู้ถือบัตรล่วงหน้าได้<br>กระบวนการตรวจสอบประวัติไม่จำเป็นจะต้องทำด้วยมือ การใช้การรวบรวมประวัติ วิเคราะห์ และเครื่องมือการแจ้งเตือน สามารถอำนวยความสะดวกได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.6.1 ตรวจสอบสิ่งต่อไปนี้ อย่างน้อยวันละครั้ง:<br>• กิจกรรมความปลอดภัยทั้งหมด<br>• ประวัติทั้งหมดของส่วนประกอบระบบซึ่งจัดเก็บ ดำเนินการ หรือ ส่ง CHD และ/หรือ SAD หรือ ซึ่งสามารถส่งผลกระทบต่อ CHD และ/หรือ SAD ได้<br>• ประวัติของส่วนประกอบระบบสำคัญทั้งหมด<br>• ประวัติของเซิฟเวอร์และส่วนประกอบระบบทั้งหมดซึ่งดำเนินการฟังก์ชั่นด้านความปลอดภัย (เช่น firewall, ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก (IDS/IPS), เซิฟเวอร์การรับรอง, เซิฟเวอร์การเปลี่ยนเส้นทางของ e-commerce และอื่นๆ) | 10.6.1.a ตรวจสอบนโยบายและกระบวนการความปลอดภัย เพื่อตรวจสอบว่ากระบวนการได้รับการกำหนดสำหรับตรวจสอบดังต่อไปนี้ อย่างน้อยวันละครั้งด้วยมือ หรือ ด้วยเครื่องมือประวัติ (log tool):<br>• กิจกรรมความปลอดภัยทั้งหมด<br>• ประวัติทั้งหมดของส่วนประกอบระบบซึ่ง จัดเก็บ ดำเนินการ หรือ ส่ง CHD และ/หรือ SAD หรือ ซึ่งสามารถส่งผลกระทบต่อ CHD และ/หรือ SAD ได้<br>• ประวัติของส่วนประกอบระบบสำคัญทั้งหมด<br>• ประวัติของเซิฟเวอร์และส่วนประกอบระบบทั้งหมดซึ่งดำเนินการฟังก์ชั่นด้านความปลอดภัย (เช่น firewall, ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก (IDS/IPS), เซิฟเวอร์การรับรอง, เซิฟเวอร์การเปลี่ยนเส้นทางของ e-commerce และอื่นๆ) | การฝ่าระบบส่วนมากเกิดขึ้นหลายวัน หรือเดือน ก่อนการตรวจพบ การตรวจสอบประวัติทุกๆวันช่วยเพิ่มขีดความปลอดภัย และลดระยะเวลาในการตรวจหาการเจาะระบบ<br><br>การตรวจสอบกิจกรรมความปลอดภัยทุกๆวัน — เช่น การแจ้งเตือน ซึ่ง แสดงให้เห็นกิจกรรมที่ผิดปกติ หรือ น่าสงสัย — รวมทั้งประวัติจากส่วนประกอบระบบที่สำคัญ และประวัติของเซิฟเวอร์และส่วนประกอบระบบทั้งหมดซึ่งดำเนินการฟังก์ชั่นด้านความปลอดภัย เช่น firewall ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก (IDS/IPS) การติดตามความสมบูรณ์ของไฟล์ (FIM) และอื่นๆ เป็นสิ่งสำคัญในการระบุปัญหาที่อาจเกิดขึ้น จำไว้ว่าการกำหนด “กิจกรรมความปลอดภัย” อาจแตกต่างกันไปขึ้นอยู่กับแต่ละองค์กร ซึ่งอาจรวมไปถึงการพิจารณาประเภทของเทคโนโลยี สถานที่ และฟังก์ชั่นของอุปกรณ์ องค์กรต่างๆ อาจต้องการบำรุงรักษาพื้นฐานของการส่งข้อมูล “ธรรมดา” ด้วยเพื่อระบุถึงพฤติกรรมที่น่าสงสัยหรือผิดปกติ |
| | 10.6.1.b สังเกตกระบวนการและสัมภาษณ์บุคลากร เพื่อตรวจสอบว่าสิ่งต่อไปนี้ได้รับการตรวจสอบอย่างน้อยวันละครั้ง:<br>• กิจกรรมความปลอดภัยทั้งหมด<br>• ประวัติทั้งหมดของส่วนประกอบระบบซึ่ง จัดเก็บ ดำเนินการ หรือ ส่ง CHD และ/หรือ SAD หรือ ซึ่งสามารถส่งผลกระทบต่อ CHD และ/หรือ SAD ได้<br>• ประวัติของส่วนประกอบระบบสำคัญทั้งหมด<br>• ประวัติของเซิฟเวอร์และส่วนประกอบระบบทั้งหมดซึ่งดำเนินการฟังก์ชั่นด้านความปลอดภัย (เช่น firewall, ระบบตรวจจับการบุกรุก/ระบบป้องกันการบุกรุก (IDS/IPS), เซิฟเวอร์การรับรอง, เซิฟเวอร์การเปลี่ยนเส้นทางของ e-commerce และอื่นๆ) | |
| 10.6.2 ตรวจสอบประวัติของส่วนประกอบระบบอื่นๆทั้งหมดเป็นระยะๆบนพื้นฐานนโยบายขององค์กร และแผนการจัดการความเสี่ยงที่กำหนดโดยการประเมินความเสี่ยงประจำปี | 10.6.2.a ตรวจสอบนโยบายและกระบวนการความปลอดภัย เพื่อตรวจสอบว่ากระบวนการได้รับการกำหนดให้มีการตรวจสอบตรวจสอบประวัติของส่วนประกอบระบบอื่นๆทั้งหมดเป็นระยะๆ — ไม่ว่าด้วยมือ หรือ เครื่องมือประวัติ (log tool) — บนพื้นฐานของนโยบายขององค์กร และแผนการจัดการความเสี่ยง | Logs for all other ส่วนประกอบระบบ should also be periodically reviewed to identify indications of potential issues or attempts to ได้รับสิทธิเข้าถึงsensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment. |
| | 10.6.2.b ตรวจสอบเอกสารการประเมินความเสี่ยงขององค์กร และสัมภาษณ์บุคลากรเพื่อตรวจสอบว่าการตรวจสอบได้มีการดำเนินการตามนโยบาย และแผนการ | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 10.6.3 ติดตามข้อยกเว้น และ ความผิดปกติที่ถูกระบุระหว่างกระบวนการตรวจสอบ | 10.6.3.a ตรวจสอบนโยบายและกระบวนการความปลอดภัย เพื่อตรวจสอบว่ากระบวนการได้รับการกำหนดสำหรับข้อยกเว้น และ ความผิดปกติที่ถูกระบุระหว่างกระบวนการตรวจสอบหรือไม่ | หากการระบุถึงข้อยกเว้น หรือความผิดปกติระหว่างการตรวจสอบประวัติไม่ได้รับการวินิจฉัย หน่วยงานอาจไม่ได้มีการตระหนักถึงการไม่ได้รับอนุญาต และกิจกรรมที่มีความเสี่ยงในเครือข่ายของตน |
| | 10.6.3.b สังเกตกระบวนการและสัมภาษณ์บุคลากร เพื่อตรวจสอบว่ามีการติดตามข้อยกเว้น และ ความผิดปกติหรือไม่ | |
| 10.7 จัดเก็บประวัติการตรวจสอบการตรวจตราอย่างน้อย 1 ปี และที่สามารถเข้าถึงเพื่อทำการวิเคราะห์ได้ทันทีอย่างน้อย 3 เดือน (เช่น online, ไฟล์จัดเก็บ (archived หรือ ไฟล์ประเภท Zip , หรือ ที่สามารถกู้คืนได้จากการ backup) | 10.7.a ตรวจสอบนโยบายและกระบวนการความปลอดภัย เพื่อตรวจสอบว่าได้มีการกำหนดดังต่อไปนี้หรือไม่:<br>• การตรวจสอบประวัตินโยบายการเก็บรักษา<br>• กระบวนการสำหรับจัดเก็บสำหรับประวัติการตรวจตราอย่างน้อย 1 ปี และที่สามารถเข้าถึงแบบ online เพื่อทำการวิเคราะห์ได้ทันทีอย่างน้อย 3 เดือน | การจัดเก็บประวัติอย่างน้อย 1 ปี ช่วยในเรื่อง ความล่าช้าในการตรวจพบการเจาะระบบซึ่งได้เกิดขึ้น หรือกำลังเกิดขึ้น และช่วยให้ผู้วินิจฉัยมีข้อมูลประวัติเพียงพอเพื่อการพิจารณาระยะเวลาการเกิดเหตุการณ์และผลกระทบที่ดียิ่งขึ้น ด้วยการที่สมารถเข้าถึงข้อมูลได้ทันที่อย่างน้อย 3 เดือน หน่วยงานสามารถระบุและลดผลกระทบจากการฝ่าระบบได้อย่างเร็วยิ่งขึ้น การจัดเก็บประวัติแบบ Off-line จะทำให้ไม่สามารถเปิดใช้งานได้ทันที ทำให้มีกรอบเวลาในการกู้ข้อมูลประวัติ วิเคราะห์ และ ระบุผลกระทบต่อระบบ และข้อมูลยาวนานขึ้น |
| | 10.7.b สัมภาษณ์บุคลากร และตรวจสอบประวัติการตรวจสอบเพื่อดูว่าประวัติการตรวจตราสามารถเข้าถึงได้อย่างน้อย 1 ปี | |
| | 10.7.c สัมภาษณ์บุคลากรและสังเกตกระบวนการเพื่อตรวจสอบว่าสามารถเข้าถึงได้ทันทีเพื่อทำการวิเคราะห์ได้อย่างน้อย 3 เดือน | |
| 10.8 ทำให้มั่นใจว่านโยบายความปลอดภัย และกระบวนการดำเนินการ เพื่อติดตามการเข้าถึงทั้งหมดไปยังแหล่งเครือข่าย และข้อมูลผู้ถือบัตรนั้นได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และ เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 10.8 ตรวจสอบเอกสาร สัมภาษณ์บุคลากร เพื่อตรวจสอบว่านโยบายความปลอดภัยและกระบวนการดำเนินการ เพื่อติดตามการเข้าถึงทั้งหมดไปยังแหล่งเครือข่าย และข้อมูลผู้ถือบัตรนั้น:<br>• ได้รับการบันทึกเป็นเอกสาร<br>• มีการใช้งาน และ<br>• เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรต้องตระหนักถึงและดำเนินการตามนโยบายความปลอดภัยและdaily กระบวนการดำเนินการ เพื่อติดตามการเข้าถึงทั้งหมดไปยังแหล่งเครือข่าย และข้อมูลผู้ถือบัตร อย่างต่อเนื่อง |

# ความต้องการที่ 11: ทดสอบระบบและกระบวนการรักษาความปลอดภัยอยู่เป็นประจำ

การค้นพบช่องโหว่ของจากผู้ประสงค์ร้ายและนักวิจัยจะเกิดขึ้นอย่างต่อเนื่อง และจะได้เกิดขึ้นบน Software ใหม่ๆ ส่วนประกอบระบบ กระบวนการ และ software ที่กำหนดเอง (custom software) ควรได้รับการทดสอบบ่อยครั้ง เพื่อให้มั่นใจว่าการควบคุมความปลอดภัยยังคงต่อเนื่องบนสิ่งแวดล้อมที่เปลี่ยนแปลง

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.1 ดำเนินการกระบวนการทดสอบสำหรับจุดเชื่อมต่อเครือข่ายไร้สาย (wireless access point) (802.11), ตรวจหาและระบุทั้ง wireless access point ที่ได้รับและไม่ได้รับอนุญาตทั้งหมดทุกๆไตรมาส<br><br>หมายเหตุ: วิธีการที่ใช้สำหรับกระบวนการนี้ ได้แก่ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) การแสกนเครือข่ายไร้สาย การตรวจสอบทางกายภาพ/ทางระบบ ของส่วนประกอบระบบ และโครงสร้าง, การควบคุมการเข้าถึงเครือข่าย *(NAC)* หรือ *wireless IDS/IPS*<br>ไม่ว่าวิธีการไหนถูกใช้งาน จะต้องเพียงพอที่จะตรวจหาและ ระบุทั้งอุปกรณ์ wireless access point ที่ได้รับและไม่ได้รับอนุญาตทั้งหมด | 11.1.a ตรวจสอบนโยบายและกระบวนการ เพื่อตรวจสอบว่ากระบวนการได้รับการกำหนดเพื่อการตรวจหาและระบุทั้ง wireless access point ที่ได้รับ และไม่ได้รับอนุญาตทั้งหมดทุกๆไตรมาส<br><br>11.1.b ตรวจสอบว่าวิธีการที่ใช้ เพียงพอสำหรับตรวจหาและทั้ง wireless access point ที่ได้รับ และไม่ได้รับอนุญาต รวมทั้งเงื่อนไขดังนี้:<br>• มีการใส่ WLAN card เข้าไปยังส่วนประกอบระบบ<br>• อุปกรณ์พกพา หรือ อุปกรณ์มือถือ มีการต่อเข้ากับส่วนประกอบระบบ เพื่อสร้าง wireless access point (เช่น ด้วย USB และอื่นๆ)<br>• อุปกรณ์ไร้สายมีการเชื่อมต่อเข้าสู่ network port หรือ อุปกรณ์เครือข่าย<br><br>11.1.c ตรวจสอบการแสดงผล (output) จากการแสกน wireless ล่าสุดเพื่อตรวจสอบว่า:<br>• มีการระบุทั้ง wireless access point ที่ได้รับ และไม่ได้รับอนุญาต<br>• มีการแสกนอย่างน้อยไตรมาสละครั้ง สำหรับส่วนประกอบระบบและอาคารทั้งหมด<br><br>11.1.d หากมีการใช้งาน การติดตามอัตโนมัติ (เช่น wireless IDS/IPS, NAC, และ อื่นๆ) ตรวจสอบว่ามีการตั้งค่าให้สร้างการแจ้งเตือนไปยังบุคลากร | การดำเนินการและ/หรือการใช้ประโยชน์จากเทคโนโลยีไร้สายภายในเครือข่าย เป็นวิธีการที่ผู้ประสงค์ร้ายส่วนหนึ่งจะได้รับสิทธิเข้าถึงเครือข่าย และ ข้อมูลผู้ถือบัตร หากมีการติดตั้งอุปกรณ์ไร้สาย หรือเครือข่ายไร้สายโดยปราศจากความรู้ขององค์กร อาจทำให้ผู้โจมตีเข้าสู่เครือข่ายอย่างง่ายดาย และอย่างไร้ร่องรอย อุปกรณ์ไร้สายที่ไม่ได้รับอนุญาตอาจถูกซ่อนไว้ใน หรือ เชื่อมต่อไว้ที่คอมพิวเตอร์หรือส่วนประกอบระบบอื่นๆ หรือเชื่อมต่อโดยตรงไปยัง network port หรืออุปกรณ์เครือข่าย เช่น switch หรือ เราเตอร์อุปกรณ์เหล่านี้อาจทำให้เกิดการไม่ได้รับอนุญาตที่เข้าถึงสิ่งแวดล้อมได้<br><br>การรู้ว่าอุปกรณ์ไร้สายใดได้รับอนุญาต ช่วยให้ผู้ดูแลสามารถระบุอุปกรณ์ที่ไม่ได้รับอนุญาต และตอบสนองได้อย่างรวดเร็วในการลดความเสี่ยงที่อาจเกิดขึ้นต่อ CDE จากผู้ประสงค์ร้าย.<br><br>เนื่องจากความง่ายดายที่ wireless access point สามารถเชื่อมต่อเข้าไปยังเครือข่ายได้ จึงเป็นสิ่งที่ยากในการตรวจหาตัวตนของสิ่งเหล่านั้น กระบวนการเหล่านี้จะต้องได้รับการดำเนินการ แม้ว่ามีนโยบายในการห้ามการใช้เทคโนโลยีไร้สายก็ตาม<br><br>ขนาดและความซับซ้อนของแต่ละสิ่งแวดล้อมจะเป็นตัวกำหนดเครื่องมือ และกระบวนการที่เหมาะสมที่จะใช้เพื่อให้ความมั่นใจว่าไม่มีการติดตั้งอุปกรณ์ไร้สายของผู้ไม่หวังดีเข้ามายังเครือข่าย<br><br>*(มีต่อหน้าถัดไป)* |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.1.1 บำรุงรักษาคลัง จุดเชื่อมต่อเครือข่ายไร้สาย (wireless access point) ที่ได้รับอนุญาต รวมทั้งเอกสารการแสดงสิทธิทางธุรกิจ (business justification) | 11.1.1 ตรวจสอบเอกสารการบันทึกเพื่อตรวจสอบว่า คลัง จุดเชื่อมต่อเครือข่ายไร้สาย (wireless access point)และ เอกสารการแสดงสิทธิทางธุรกิจ (business justification) ได้รับการบันทึกไว้ สำหรับ wireless access point ที่ได้รับอนุญาต | ตัวอย่าง เช่น: ในกรณีที่แผงขายปลีกในห้างสรรพสินค้า ซึ่งส่วนประกอบการสื่อสารทั้งหมดบรรจุไว้ในบรรจุภัณฑ์ป้องกันการงัดแงะ (*tamper-resistant*) และบรรจุภัณฑ์บ่งชี้ร่องรอยการงัดแงะ (*tamper-evident casing*) ดำเนินการตรวจสอบทางกายภาพในแผงอาจเพียงพอแล้วที่จะทำให้มั่นใจว่า ไม่มี *wireless access point* ของผู้ไม่หวังดี ได้รับการเชื่อมต่อ หรือติดตั้ง อย่างไรก็ตามในสิ่งแวดล้อมที่มี *node* มากมาย *(*เช่น ในร้านค้าปลีก, *call center*, ห้องเซิฟเวอร์ หรือ ฐานข้อมูล*)* การตรวจสอบทางกายภาพอย่างละเอียดเป็นเรื่องยาก ในกรณีนี้ การใช้วิธีผสมผสานระหว่างหลายวิธีการจะทำให้บรรลุความต้องการได้ เช่น ตรวจสอบทางกายภาพพร้อมกับการดูผลวิเคราะห์เครือข่ายไร้สาย(*wireless analyzer*) |
| 11.1.2 ดำเนินการกระบวนการตอบโต้ เมื่อมีการตรวจพบ ในเหตุการณ์ที่wireless access point ซึ่งไม่ได้รับอนุญาตถูกตรวจพบ | 11.1.2.a ตรวจสอบแผนการตอบโต้ขององค์กร (ความต้องการ 12.10) เพื่อตรวจสอบว่าได้มีการกำหนด และร้องขอกระบวนการตอบโต้ เมื่อมีการตรวจพบในเหตุการณ์ที่ wireless access point ซึ่งไม่ได้รับอนุญาตถูกตรวจพบ. | |
| | 11.1.2.b สัมภาษณ์บุคลากรที่รับผิดชอบ และ/หรือ ตรวจสอบการแสกน wireless ล่าสุด และการตอบสนองที่เกี่ยวข้องเพื่อตรวจสอบว่ามีการเมื่อ wireless access point ที่ไม่ได้รับอนุญาตถูกตรวจพบ | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.2 ดำเนินการสแกนช่องโหว่ภายในและภายนอก อย่างน้อยไตรมาสละ 1 ครั้ง และหลังจากการเปลี่ยนแปลงใหญ่ของเครือข่าย (เช่น การติดตั้งส่วนประกอบระบบใหม่ การเปลี่ยนแปลงโครงสร้างเครือข่าย (topology) การเปลี่ยนแปลงกฎ firewall การอัพเดทสินค้า)<br>หมายเหตุ: อาจมีการผสมผสานจากหลายรายงานการแสกน สำหรับการแสกนประจำไตรมาสเพื่อแสดงให้เห็นว่าระบบได้ถูกแสกน และช่องโหว่ทั้งหมดได้ถูกจัดการแล้ว อาจมีความต้องการขอเอกสารเพิ่มเติมเพื่อตรวจสอบว่าช่องโหว่ที่ไม่ได้รับการซ่อมแซมนั้นอยู่ในกระบวนการจัดการแล้ว<br>สำหรับการเริ่มต้นการปฏิบัติตาม *PCI DSS* ไม่ได้มีความต้องการให้การแสกนที่ผ่านทั้ง 4 ไตรมาสจะต้องสมบูรณ์ หากผู้ประเมินเห็นว่า 1) ผลการแสกนส่วนใหญ่ผ่าน 2) หน่วยงายมีเอกสารนโยบาย และกระบวนการที่ร้องขอการแสกนทุกๆไตรมาส และ 3) ช่องโหว่ที่ได้รับการบันทึกในผลการแสกนถูกแก้ไขเมื่อทำการแสกนอีกครั้ง ในปีถัดมาหลังการเริ่มต้นการตรวจสอบ *PCI DSS* การแสกนทั้ง *4* ไตรมาสจะต้องผ่านทั้งหมด | 11.2 ตรวจสอบรายงานการแสกน และเอกสารการสนับสนุน เพื่อตรวจสอบว่าการแสกนช่องโหว่ภายในและภายนอกได้รับการดำเนินการดังนี้: | การแสกนช่องโหว่ คือเครื่องมืออัตโนมัติในการดำเนินการทั้งภายนอกและภายในอุปกรณ์เครือข่าย และเซิฟเวอร์ ออกแบบมาให้เปิดเผยช่องโหว่ที่เป็นไปได้ซึ่งสามารถถูกพบและใช้ประโยชน์จากผู้ประสงค์ร้าย<br>การแสกนหาช่องโหว่มี 3 ประเภท ที่ PCI DSS ต้องการ:<br>• การแสกนช่องโหว่ภายในประจำไตรมาส โดยบุคลากรที่ผ่านคุณสมบัติ (Qualified) (การใช้ผู้แสกนที่ได้รับการอนุมัติจาก PCI SSC (ASV) นั้นไม่ได้เป็นความต้องการ)<br>• การแสกนช่องโหว่ภายนอกประจำไตรมาส ซึ่งต้องดำเนินการโดย ASV (ผู้แสกนที่ได้รับการอนุมัติ)<br>• การแสกนภายในและภายนอกเมื่อจำเป็นหลังจากการเปลี่ยนแปลงใหญ่<br>เมื่อจุดอ่อนเหล่านี้ได้รับการระบุ ให้หน่วยงานแก้ไขและทำการแสกนใหม่อีกครั้งจนกว่าช่องโหว่ทั้งหมดจะได้รับการแก้ไข<br>การระบุและจัดการกับช่องโหว่อย่างทันท่วงที จะลดความเป็นไปได้จากการถูกฉวยโอกาส และลดความเสี่ยงการเจาะเข้าส่วนประกอบระบบหรือข้อมูลผู้ถือบัตร |
| 11.2.1 ดำเนินการแสกนช่องโหว่ภายในทุกๆไตรมาส และ แสกนใหม่หากจำเป็น จนกว่าช่องโหว่ที่ “มีความเสี่ยงสูง” (ดังที่กล่าวในความต้องการ 6.1) จะได้รับการแก้ไข การแสกนควรจะดำเนินการโดยบุคลากรที่ผ่านคุณสมบัติ (Qualified) | 11.2.1.a ตรวจทานรายงานการแสกน และตรวจสอบว่าการแสกนทั้ง 4 ไตรทาส เกิดขึ้นภายใน 12 เดือนล่าสุดหรือไม่<br>11.2.1.b ตรวจทานรายงานการแสกนและตรวจสอบว่า ได้มีกระบวนการแสกนจนกว่าช่องโหว่ที่ “มีความเสี่ยงสูง” (ดังที่กล่าวในความต้องการ 6.1) จะได้รับการแก้ไขหรือไม่ | กระบวนการที่จัดตั้งขึ้นสำหรับการระบุหาช่องโหว่ สำหรับระบบภายใน ต้องมีการแสกนทุกๆไตรมาส ช่องโหว่ที่มีความเสี่ยงร้ายแรง (เช่น ได้รับการจัดว่าเป็น “ความเสี่ยงสูง” ตามความต้องการ 6.1) ควรได้รับการจัดอันดับความสำคัญให้จัดการโดยเร็ว |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 11.2.1.c สัมภาษณ์บุคลากร เพื่อตรวจสอบว่าการแสกนถูกดำเนินการโดยแหล่งภายในหรือบุคคลที่ 3 ที่ผ่านคุณสมบัติ (qualified) และหากทำได้ ให้องค์กรอิสระจากผู้รับการทดสอบ (ไม่จำเป็นว่าต้องเป็น QSA หรือ ASV) | การแสกนช่องโหว่ภายในสามารถดำเนินการได้โดยทีมงานภายในซึ่งผ่านคุณสมบัติ และมีความเป็นเอกเทศน์จากส่วนประกอบระบบที่ได้รับการแสกน (เช่น ผู้ดูแลfirewall ไม่ควรเป็นผู้แสกน firewall) หรือหน่วยงานอาจเลือกให้มีการแสกนภายในโดยบริษัทที่เชี่ยวชาญทางด้านการแสกน |
| 11.2.2 ดำเนินการแสกนช่องโหว่ภายนอกโดย ผู้แสกนที่ได้รับการอนุมัติ (ASV) โดย สภามาตรฐานความปลอดภัยการชำระเงินผ่านบัตร (PCI SSC) ดำเนินการแสกนใหม่เท่าที่จำเป็น จนกว่าจะการแสกนจะผ่าน<br>หมายเหตุ: การแสกนช่องโหว่ภายนอกจะต้องดำเนินการโดย ผู้แสกนที่ได้รับการอนุมัติ *(ASV)* โดย สภามาตรฐานความปลอดภัยการชำระเงินผ่านบัตร *(PCI SSC)*<br>โปรดดู คำแนะนำโปรแกรม *ASV* ที่เผยแพร่บนเว็บไซต์ของ *PCI SSC* สำหรับความรับผิดชอบการแสกนของลูกค้า การเตรียมการ และ อื่นๆ | 11.2.2.a ตรวจสอบการแสดงผล (output) จากการแสกนช่องโหว่ภายนอก 4 ไตรมาสล่าสุด และตรวจสอบว่าการแสกนทั้งหมดเกินขึ้นใน 12 เดือนล่าสุดหรือไม่<br>11.2.2.b ตรวจสอบผลการแสกนแต่ละไตรมาสและการแสกนใหม่ เพื่อตรวจสอบว่าได้บรรลุ คำแนะนำโปรแกรม ASV ที่ต้องการสำหรับผ่านการแสกนหรือไม่ (เช่น ไม่มีช่องโหว่ที่ได้รับการจัดอันดับความเสี่ยงที่ 4.0 หรือ สูงกว่าโดย CVSS และไม่มีกระบวนการอัตโนมัติที่ล้มเหลว)<br>11.2.2.c ตรวจทานรายงานการแสกน เพื่อตรวจสอบว่าการแสกนสมบูรณ์ โดย ผู้แสกนที่ได้รับการอนุมัติจาก PCI SSC | เนื่องจากเครือข่ายภายนอกมีความเสี่ยงต่อการเจาะข้อมูลมาก การแสกนช่องโหว่ภายนอกประจำไตรมาสจึงต้องดำเนินการโดยผู้แสกนที่ได้รับการอนุมัติจาก PCI SSC |
| 11.2.3 ดำเนินการแสกนภายในและภายนอก และทำการแสกนใหม่เท่าที่จำเป็น หลังการเปลี่ยนแปลงใหญ่ การแสกนจะต้องดำเนินการโดยบุคลากรที่ผ่านคุณสมบัติ (qualified) | 11.2.3.a ตรวจสอบและเทียบเอกสารการควบคุมการเปลี่ยนแปลง และรายงานการแสกน เพื่อตรวจสอบว่าส่วนประกอบระบบเป็นไปตามการเปลี่ยนแปลงที่ได้รับการแสกน<br>11.2.3.b ตรวจทานรายงานการแสกนและตรวจสอบว่ากระบวนการแสกนมีการแสกนใหม่จนกว่า:<br>• สำหรับการแสกนภายนอก ไม่มีช่องโหว่ที่ได้รับการจัดอันดับความเสี่ยงที่ 4.0 หรือ สูงกว่าโดย CVSS<br>• สำหรับการแสกนภายใน ช่องโหว่ที่ได้รับการจัดอันดับความเสี่ยง “ความเสี่ยงสูง” ดังที่ระบุไว้ในความต้องการ PCI DSS 6.1 ได้รับการแก้ไขทั้งหมด | การกำหนดว่าสิ่งใดเรียกว่าเป็นการเปลี่ยนแปลงใหญ่ขึ้นอยู่กับการตั้งค่าของสิ่งแวดล้อมนั้นๆ หากการอัพเกรด หรือ ปรับเปลี่ยน ทำให้มีการให้การเข้าถึงไปยังข้อมูลผู้ถือบัตร หรือกระทบต่อความปลอดภัยของสิ่งแวดล้อมข้อมูลผู้ถือบัตร จึงเรียกว่าเป็นการเปลี่ยนแปลงใหญ่<br>การแสกนสิ่งแวดล้อมหลังการเปลี่ยนแปลงใหญ่ใดๆก็ตาม ทำเพื่อให้มั่นใจว่าการเปลี่ยนแปลงนั้นสมบูรณ์ และเหมาะสม ซึ่งไม่ทำให้เกิดการเจาะข้อมูลของสิ่งแวดล้อม ส่วนประกอบระบบทั้งหมดที่ได้รับผลกระทบจะต้องได้รับการแสกนเช่นกัน |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| | 11.2.3.c ตรวจสอบว่ามีการดำเนินการแสกนโดยแหล่งภายในหรือบุคคลที่ 3ที่ผ่านคุณสมบัติ และหากเป็นไปได้ให้เป็นองค์กรอิสระจากผู้รับการทดสอบ (ไม่จำเป็นว่าต้องเป็น QSA หรือ ASV) | |
| 11.3 ดำเนินการวิธีการสำหรับทดสอบการเจาะระบบซึ่งมีเงื่อนไขดังนี้:<br>• มีพื้นฐานบนวิธีการทดสอบการเจาะระบบการยอมรับระดับอุตสาหกรรม (เช่น NIST SP800-115)<br>• ครอบคลุมตัวแปร CDE และระบบสำคัญทั้งหมด<br>• ทดสอบจากเครือข่ายทั้งภายในและภายนอก<br>• มีการทดสอบการตรวจขอบเขตการแบ่งการเข้าถึงและการควบคุมการลดขอบเขต<br>• กำหนดการทดสอบการเจาะ Layer แอปพลิเคชั่น ให้อย่างน้อยมีช่องโหว่ที่ระบุไว้ในความต้องการ 6.5<br>• กำหนดการทดสอบการเจาะ Layer เครือข่ายให้มีส่วนประกอบซึ่งสนับสนุนฟังก์ชั่นเครือข่ายรวมทั้งระบบปฏิบัติการ<br>• ให้มีการตรวจทานและพิจารณาภัยอันตรายและช่องโหว่ที่พบใน 12 เดือนก่อนหน้า<br>• ระบุการเก็บรักษาผลการทดสอบการเจาะระบบ และผลการซ่อมแซมแก้ไข<br><br>หมายเหตุ: สิ่งนี้อัพเดทไปยังความต้องการ *11.3* เป็นวิธีการที่ดีที่สุดจนถึง 30 มิถุนายน 2556 หลังจากกลายเป็นความต้องการ จะต้องดำเนินการตามความต้องการ *PCI DSS v2.0* สำหรับทดสอบการเจาะระบบจนกว่าจะมีการใช้ *v3.0* | 11.3 ตรวจสอบวิธีการทดสอบการเจาะระบบ และสัมภาษณ์บุคลากรที่รับผิดชอบว่าวิธีการที่ใช้ได้มีเงื่อนไขดังต่อไปนี้:<br>• มีพื้นฐานบนวิธีการทดสอบการเจาะระบบการยอมรับระดับอุตสาหกรรม (เช่น NIST SP800-115)<br>• ครอบคลุมตัวแปร CDE และระบบสำคัญทั้งหมด<br>• ทดสอบจากเครือข่ายทั้งภายในและภายนอก<br>• มีการทดสอบการตรวจขอบเขตการแบ่งการเข้าถึงและการควบคุมการลดขอบเขต<br>• กำหนดการทดสอบการเจาะ Layer แอปพลิเคชั่น ให้อย่างน้อยมีช่องโหว่ที่ระบุไว้ในความต้องการ 6.5<br>• กำหนดการทดสอบการเจาะ Layer เครือข่ายให้มีส่วนประกอบซึ่งสนับสนุนฟังก์ชั่นเครือข่ายรวมทั้งระบบปฏิบัติการ<br>• ให้มีการตรวจทานและพิจารณาภัยอันตรายและช่องโหว่ที่พบใน 12 เดือนก่อนหน้า<br>• ระบุการเก็บรักษาผลการทดสอบการเจาะระบบ และผลการซ่อมแซมแก้ไข | จุดประสงค์การทดสอบการเจาะระบบคือการจำลองการโจมตีจริงโดยมีเป้าหมายเพื่อตรวจว่าผู้โจมตีสามารถเจาะเข้าสิ่งแวดล้อมได้มากเท่าใดซึ่งจะทำให้เข้าใจถึงความเสี่ยง และสามารถพัฒนาแผนการป้องกันได้ดีขึ้น<br><br>การทดสอบการเจาะระบบแตกต่างจากการแสกน โดยการทดสอบนั้นเป็นกระบวนการซึ่งอาจนำช่องโหว่ไปใช้ การแสกนเสมือนเป็นส่วนแรกของการเจาะระบบเพื่อที่จะวางแผนการเจาะระบบ อย่างไรก็ตาม มันไม่ได้เป็นวิธีการเดียวที่ใช้ แม้ไม่มีการพบช่องโหว่ ผู้ทดสอบมักจะสามารถรวบรวมข้อมูลเพียงพอที่จะระบุจุดอับของความปลอดภัยได้<br><br>การทดสอบการเจาะระบบปกติแล้วเป็นกระบวนการที่ทำด้วยมือเป็นส่วนมาก แต่ก็มีการใช้เครื่องมืออัตโนมัติร่วมด้วย ผู้ทดสอบจะใช้ความรู้ในระบบเพื่อเจาะเข้าไปในสิ่งแวดล้อม บ่อยครั้งที่ผู้ทดสอบจะเชื่อมโยงหลายๆสิ่งเพื่อนำมาใช้ประโยชน์ในการเจาะผ่านชั้นการป้องกัน เช่น หากผู้ทดสอบหาวิธีการได้มาซึ่งการเข้าถึงเซิฟเวอร์แอปพลิเคชั่นได้ พวกเขาจะเจาะเข้าเซิฟเวอร์เพื่อเข้าถึงแหล่งที่เซิฟเวอร์ถูกตั้งอยู่ ในกรณีนี้ ผู้ทดสอบจะสามารถจำลองวิธีการที่ผู้โจมตีใช้ เพื่อตรวจสอบได้ว่าบริเวณใดที่มีจุดอ่อนภายในสิ่งแวดล้อม<br><br>เทคนิคการทดสอบการเจาะระบบอาจแตกต่างกันออกไปในแต่ละองค์กร และ ประเภท ความลึก และความซับซ้อนของการทดสอบขึ้นอยู่กับสิ่งแวดล้อมแต่ละแหล่งและการประเมินความเสี่ยงขององค์กร |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.3.1 ดำเนินการ การทดสอบการเจาะระบบภายนอกอย่างน้อยปีละ 1 ครั้ง และหลังจากการอัพเกรด หรือปรับเปลี่ยนครั้งใหญ่ของโครงสร้าง หรือ แอปพลิเคชั่น (เช่น การอัพเกรดระบบปฏิบัติการ การเพิ่มเครือข่ายย่อย (sub-network) ภายใต้สิ่งแวดล้อม หรือ การเพิ่มเว็บเซิฟเวอร์ไปยังสิ่งแวดล้อม) | 11.3.1.a ตรวจสอบขอบเขตงาน และผลล่าสุดจากการทดสอบการเจาะระบบภายนอกเพื่อตรวจสอบว่าการทดสอบการเจาะระบบมีการดำเนินการดังนี้:<br>• ดำเนินการตามวิธีการที่กำหนดไว้<br>• อย่างน้อยปีละ 1 ครั้ง<br>• หลังจากการเปลี่ยนแปลงใหญ่ไปยังสิ่งแวดล้อม | ดำเนินการการทดสอบการเจาะระบบเป็นประจำ และหลังจากการเปลี่ยนแปลงใหญ่ไปยังสิ่งแวดล้อม เพื่อเป็นการสร้างมาตรการความปลอดภัยล่วงหน้า ซึ่งช่วยลดความเสี่ยงการเข้าถึง CDE โดยผู้ประสงค์ร้าย<br><br>การกำหนดว่าสิ่งใดเรียกว่าเป็นการเปลี่ยนแปลงใหญ่ขึ้นอยู่กับการตั้งค่าของสิ่งแวดล้อมนั้นๆ หากการอัพเกรด หรือ ปรับเปลี่ยน ทำให้มีการให้การเข้าถึงไปยังข้อมูลผู้ถือบัตร หรือกระทบต่อความปลอดภัยของสิ่งแวดล้อมข้อมูลผู้ถือบัตร จึงเรียกว่าเป็นการเปลี่ยนแปลงใหญ่ การดำเนินการทดสอบการเจาะระบบการอัพเกรดเครือข่าย และการปรับเปลี่ยน ทำให้มั่นใจว่ายังมีการควบคุม และใช้งานได้ดีหลังการอัพเกรด หรือเปลี่ยนแปลง |
| | 11.3.1.b ตรวจสอบว่าการทดสอบได้ดำเนินการโดยแหล่งภายในหรือบุคคลที่ 3 ที่ผ่านคุณสมบัติ และและหากเป็นไปได้ให้เป็นองค์กรอิสระจากผู้รับการทดสอบ (ไม่จำเป็นว่าต้องเป็น QSA หรือ ASV) | |
| 11.3.2 ดำเนินการ การทดสอบการเจาะระบบภายในอย่างน้อยปีละ 1 ครั้งและหลังจากการอัพเกรด หรือปรับเปลี่ยนครั้งใหญ่ของโครงสร้าง หรือ แอปพลิเคชั่น (เช่น การอัพเกรดระบบปฏิบัติการ การเพิ่มเครือข่ายย่อย (sub-network) ภายใต้สิ่งแวดล้อม หรือ การเพิ่มเว็บเซิฟเวอร์ไปยังสิ่งแวดล้อม) | 11.3.2.a ตรวจสอบขอบเขตงาน และผลล่าสุดจากการทดสอบการเจาะระบบภายในเพื่อตรวจสอบว่าการทดสอบการเจาะระบบมีการดำเนินการอย่างน้อยปีละ 1 ครั้ง และหลังจากการเปลี่ยนแปลงใหญ่ไปยังสิ่งแวดล้อม<br>• ดำเนินการตามวิธีการที่กำหนดไว้<br>• อย่างน้อยปีละ 1 ครั้ง<br>• หลังจากการเปลี่ยนแปลงใหญ่ไปยังสิ่งแวดล้อม | |
| | 11.3.2.b ตรวจสอบว่าการทดสอบได้ดำเนินการโดยแหล่งภายในหรือบุคคลที่ 3 ที่ผ่านคุณสมบัติ และและหากเป็นไปได้ให้เป็นองค์กรอิสระจากผู้รับการทดสอบ (ไม่จำเป็นว่าต้องเป็น QSA หรือ ASV) | |
| 11.3.3 ช่องโหว่ที่พบระหว่างการทดสอบการเจาะระบบได้รับการแก้ไข และมีการทดสอบซ้ำว่าช่องโหว่นั้นได้แก้ไขแล้ว | 11.3.3 ตรวจสอบผลการทดสอบการเจาะระบบ เพื่อตรวจสอบว่าช่องโหว่ที่ได้รับการบันทึก ได้รับการแก้ไข และมีการทดสอบซ้ำว่าช่องโหว่นั้นได้แก้ไขแล้ว | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.3.4 หากมีการใช้การแบ่งส่วนการเข้าถึงเพื่อแยก CDE ออกจากเครือข่ายอื่นๆ ดำเนินการทดสอบการเจาะระบบอย่างน้อยปีละ 1 ครั้งและหลังจากการเปลี่ยนแปลงใดๆไปยัง การควบคุม/วิธีการของการแบ่งส่วน เพื่อตรวจสอบว่าวิธีการแบ่งส่วนนั้นยังใช้งานได้และมีประสิทธิภาพ และทำการแยกระบบที่อยู่นอกขอบเขตทั้งหมดออกจากที่อยู่ในขอบเขต | 11.3.4.a ตรวจสอบการควบคุมการแบ่งส่วนและตรวจสอบวิธีการทดสอบการเจาะระบบ เพื่อตรวจสอบว่ากระบวนการทดสอบการเจาะระบบได้ถูกกำหนดให้ทดสอบวิธีการแบ่งส่วนทั้งหมดเพื่อยืนยันว่ายังใช้งานได้และมีประสิทธิภาพ และทำการแยกระบบที่อยู่นอกขอบเขตทั้งหมดออกจากที่อยู่ในขอบเขต<br><br>11.3.4.b ตรวจสอบผลของการทดสอบการเจาะระบบส่วนมาก เพื่อตรวจสอบการทดสอบการเจาะระบบว่าได้ตรวจสอบให้การควบคุมการแบ่งส่วน:<br>• มีการดำเนินการอย่างน้อยปีละ 1 ครั้งและหลังจากการเปลี่ยนแปลงใดๆไปยัง การควบคุม/วิธีการของการแบ่งส่วน<br>• ครอบคลุมการควบคุม/วิธีการของการแบ่งส่วนที่ใช้ทั้งหมด<br>• ตรวจสอบว่าวิธีการแบ่งส่วนนั้นใช้งานได้และมีประสิทธิภาพ และทำการแยกระบบที่อยู่นอกขอบเขตทั้งหมดออกจากที่อยู่ในขอบเขต | การทดสอบการเจาะระบบเป็นเครื่องมือสำคัญในการยืนยันว่าการแบ่งส่วนการเข้าถึงใดๆก็ตามนั้นมีประสิทธิภาพ และทำการแยกระบบที่อยู่นอกขอบเขตทั้งหมดออกจากที่อยู่ในขอบเขต การทดสอบการเจาะระบบควรมุ่งเน้นไปที่การควบคุมการแบ่งส่วน ทั้งจากภายนอกเครือข่ายองค์กร และจากภายในเครือข่ายแต่อยู่ภายนอก CDE เพื่อยืนยันว่าสิ่งเหล่านั้นไม่สามารถผ่านการควบคุมการแบ่งส่วนเพื่อเข้าถึง CDE ได้ เช่นการทดสอบเครือข่าย และ/หรือ การแสกนหา port ที่เปิดไว้ เพื่อตรวจสอบว่าไม่มีการเชื่อมต่อระหว่างเครือข่ายที่อยู่ในขอบเขต และนอกขอบเขต |
| 11.4 ใช้การตรวจจับการบุกรุก และ/หรือ เทคนิคการป้องกันการบุกรุก เพื่อตรวจจับและ/หรือป้องกันการบุกรุกเข้าเครือข่าย เฝ้าติดตามการส่งข้อมูลทั้งหมดที่ค่าตัวแปรของสิ่งแวดล้อมข้อมูลผู้ถือบัตร รวมทั้งจุดที่สำคัญของสิ่งแวดล้อมข้อมูลผู้ถือบัตร และแจ้งเตือนบุคลากรเพื่อให้ทราบถึงสิ่งที่มีพิรุธถึงการเจาะข้อมูล<br><br>รักษาให้กลไกการตรวจจับการบุกรุก และ/หรือ เทคนิคการป้องกันการบุกรุก ข้อมูลพื้นฐาน และลายเซ็น (signature หรือ ลักษณะการส่งข้อมูลของเครือข่าย) เป็นปัจจุบัน | 11.4.a ตรวจสอบการตั้งค่าระบบและแผนภาพเครือข่าย เพื่อตรวจสอบว่าเทคนิค (เช่น ระบบการตรวจจับการบุกรุก และ/หรือ ระบบการป้องกันการบุกรุก) มีการนำมาใช้งานเพื่อเฝ้าติดตามการส่งข้อมูลทั้งหมด:<br>• ที่ค่าตัวแปรของสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br>• ที่จุดสำคัญของสิ่งแวดล้อมข้อมูลผู้ถือบัตร<br><br>11.4.b ตรวจสอบการตั้งค่าระบบและสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อยืนยันว่าการตรวจจับการบุกรุก และ/หรือ เทคนิคการป้องกันการบุกรุกได้แจ้งเตือนบุคลากรถึงแนวโน้มในการเจาะระบบ<br><br>11.4.c ตรวจสอบการตั้งค่า IDS/IPS และเอกสารจากผู้ขายเพื่อตรวจสอบว่าการตรวจจับการบุกรุก และ/หรือ เทคนิคการป้องกันการบุกรุกได้รับการตั้งค่า บำรุงรักษา และอัพเดอทตามคำแนะนำของผู้ขายเพื่อให้มั่นใจถึงการป้องกันที่ดีเยี่ยม | การตรวจจับการบุกรุก และ/หรือ เทคนิคการป้องกันการบุกรุก (เช่น IDS/IPS) เทียบการส่งข้อมูลที่เข้ามาในเครือข่าย ซึ่งเรียกกันว่า ลายเซ็น “signatures” และ/หรือ วิสัยรูปแบบการเจาะข้อมูลส่วนมาก (behaviors of thousands of compromise types) (เครื่องมือการเจาะระบบ (hacker tool) Trojan และ malware อื่นๆ) และส่งการแจ้งเตือน และ/หรือ ยับยั้งความพยายามเมื่อตรวจพบ หากไม่มีการเตรียมการล่วงหน้าสำหรับการตรวจจับกิจกรรมที่ไม่ได้รับอนุญาต การโจมตี (หรือการใช้งานในทางที่ผิดของ) แหล่งคอมพิวเตอร์ อาจทำให้เกิดสิ่งเหล่านั้นขึ้นโดยไม่มีผู้ใดรับทราบ การแจ้งเตือนความปลอดภัยที่เกิดจากกระบวนการเหล่านี้ ควรได้รับการติดตามเพื่อจะได้ยับยั้งความพยายามบุกรุกทันทีที่เกิด |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 11.5 ดำเนินการใช้กลไกการตรวจจับการเปลี่ยนแปลง(เช่น เครื่องมือติดตามความสมบูรณ์ของไฟล์)ให้แจ้งเตือนบุคลากร สำหรับการปรับแต่งที่ไม่ได้รับอนุญาตของไฟล์สำคัญของระบบ ไฟล์การตั้งค่า หรือ ไฟล์เนื้อหา; และตั้งค่า software ให้ดำเนินการเปรียบเทียบไฟล์สำคัญอย่างน้อยสัปดาห์ละครั้ง<br><br>หมายเหตุ: สำหรับเหตุผลทางการตรวจจับการเปลี่ยนแปลง ไฟล์สำคัญ คือไฟล์ที่มักไม่ได้มีการเปลี่ยนแปลงเป็นประจำ ซึ่งการเปลี่ยนแปลงอาจแสดงถึงการเจาะระบบ หรือ ความเสี่ยงได้ กลไกการตรวจจับการเปลี่ยนแปลง เช่น เครื่องมือติดตามความสมบูรณ์ของไฟล์ มักมาพร้อมกับการตั้งค่าเริ่มต้น (pre- configured) และไฟล์สำคัญที่เกี่ยวข้องกับระบบปฏิบัติการ ไฟล์สำคัญอื่นๆ เช่น จากแอปพลิเคชั่นที่กำหนดเอง จะต้องได้รับการประเมินและกำหนดโดยหน่วยงาน (ซึ่งก็คือ ผู้ขาย หรือ ผู้ให้บริการ) | 11.5.a Verify the use of a กลไกการตรวจจับการเปลี่ยนแปลงwithin theสิ่งแวดล้อมข้อมูลผู้ถือบัตร by สังเกตการตั้งค่าระบบและmonitored files, as well as reviewing results from monitoring activities.<br><br>Examples of files that should be monitored:<br>■ ระบบการปฏิบัติการ (System executables)<br>■ แอปพลิเคชั่นการปฏิบัติการ (Application executable)<br>■ ไฟล์การตั้งค่าและตัวแปร<br>■ ไฟล์ประวัติ และการตรวจสอบที่จัดเก็บอยู่ที่ส่วนกลาง<br>■ ไฟล์สำคัญอื่นๆที่กำหนดโดยหน่วยงาน (เช่น ด้วยกระบวนการประเมินความเสี่ยง หรือ ด้วยกระบวนการอื่นๆ) | การตรวจจับการเปลี่ยนแปลง เช่น เครื่องมือติดตามความสมบูรณ์ของไฟล์ (FIM) จะตรวจสอบการเปลี่ยนแปลงไปยังไฟล์สำคัญ และแจ้งเตือนเมื่อมีการเปลี่ยนแปลงถูกตรวจพบ หากไม่มีการใช้งานอย่างเหมาะสม และ ไม่มีการติดตามผลของการตรวจจับการเปลี่ยนแปลง ผู้ประสงค์ร้ายอาจเปลี่ยนไฟล์การตั้งค่า ไฟล์เนื้อหา โปรแกรมในระบบปฏิบัติการ หรือ แอปพลิเคชั่นการปฏิบัติการได้ หากเกิดการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต อาจมีการทำให้การควบคุมความปลอดภัยไร้ผลได้ และ/หรือ ทำให้เกิดการขโมยข้อมูลผู้ถือบัตร โดยไม่สามารถสังเกตได้โดยกระบวนการปรกติได้ |
| | 11.5.b ตรวจสอบว่ากลไกถูกตั้งค่าให้แจ้งเตือนบุคลากร สำหรับการปรับแต่งที่ไม่ได้รับอนุญาตของไฟล์สำคัญ และเพื่อดำเนินการเปรียเทียบไฟล์สำคัญอย่างน้อยสัปดาห์ละครั้ง | |
| 11.5.1 ดำเนินการกระบวนการตอบโต้การแจ้งเตือนที่เกิดจากระบบติดตามการเปลี่ยนแปลง | 11.5.1 สัมภาษณ์บุคลากร เพื่อตรวจสอบว่าการแจ้งเตือนทั้งหมดได้รับการตรวจสอบและแก้ไขแล้ว | |
| 11.6 ทำให้มั่นใจว่านโยบายความปลอดภัย และกระบวนการดำเนินการเฝ้าติดตามความปลอดภัยและการทดสอบได้รับการบันทึกเป็นเอกสาร มีการใช้งาน และ เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | 11.6 ตรวจสอบเอกสาร สัมภาษณ์บุคลากร เพื่อตรวจสอบว่านโยบายความปลอดภัยและกระบวนการดำเนินการสำหรับการเฝ้าติดตามความปลอดภัยและการทดสอบ:<br>● ได้รับการบันทึกเป็นเอกสาร<br>● มีการใช้งาน และ<br>● เป็นที่รู้จักต่อผู้ที่มีผลกระทบทั้งหมด | บุคลากรต้องตระหนักถึงและดำเนินการตามนโยบายความปลอดภัย และกระบวนการดำเนินการเฝ้าติดตามความปลอดภัยและการทดสอบอย่างต่อเนื่อง |

# บำรุงรักษาข้อมูลนโยบายความปลอดภัย

**ความต้องการที่ 12: บำรุงรักษานโยบายซึ่งกล่าวถึงความปลอดภัยของข้อมูลสำหรับบุคลากรทั้งหมด**

นโยบายความปลอดภัยที่เข้มแข็ง จะกำหนดแนวทางความปลอดภัยสำหรับทั้งหน่วยงาน และแจ้งให้บุคลากรทราบว่าหน่วยงานคาดหวังอะไรกับพวกเขา บุคลากรทั้งหมดควรตระหนักถึงความสุ่มเสี่ยงของข้อมูลและความรับผิดชอบของพวกเขาในการปกป้องข้อมูลเหล่านั้น ในจุดประสงค์ความต้องการที่ 12 “บุคลากร” หมายถึง ลูกจ้าง full-time และpart-time ลูกจ้างชั่วคราว สัญญา และที่ปรึกษา ผู้ซึ่ง “อาศัย” อยู่ในสถานที่ของหน่วยงาน หรือ มีสิทธิการเข้าถึงสิ่งแวดล้อมข้อมูลผู้ถือบัตร

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.1 จัดตั้ง ตีพิมพ์ บำรุงรักษา และเผยแพร่ นโยบายความปลอดภัย | 12.1 ตรวจสอบข้อมูลนโยบายความปลอดภัยความปลอดภัยและตรวจสอบว่าได้มีการจัดตั้ง ตีพิมพ์ บำรุงรักษา และเผยแพร่ไปยังบุคลากรที่เกี่ยวข้องทั้งหมดหรือไม่ (รวมทั้งผู้ขาย และคู่ค้าทางธุรกิจ) | ข้อมูลนโยบายความปลอดภัยความปลอดภัยขององค์กร สร้างแผนขั้นตอนการทำงาน สำหรับการดำเนินการด้านความปลอดภัยเพื่อปกป้องทรัพย์สินที่มีค่ามากที่สุด บุคลากรทั้งหมดควรตระหนักถึงความสุ่มเสี่ยงของข้อมูล และและความรับผิดชอบของพวกเขาในการปกป้องข้อมูลเหล่านั้น |
| 12.1.1 ตรวจสอบนโยบายความปลอดภัย อย่างน้อยปีละ 1 ครั้ง และอัพเดทนโยบายเมื่อสิ่งแวดล้อมเปลี่ยนแปลง | 12.1.1 ตรวจสอบว่าข้อมูลนโยบายความปลอดภัยความปลอดภัยได้รับการตรวจทานอย่างน้อยปีละ 1 ครั้งและอัพเดทเมื่อจำเป็นเพื่อให้ทันต่อการเปลี่ยนแปลงของจุดประสงค์ทางธุรกิจ หรือ ความเสี่ยงของสิ่งแวดล้อม | อันตรายด้านความปลอดภัย และกระบวนการป้องกัน ได้รับการวิวัฒนาการอย่างรวดเร็ว หากไม่มีการอัพเดทนโยบายความปลอดภัย เพื่อให้ทันต่อการเปลี่ยนแปลง วิธีการป้องกันใหม่ในการต่อสู้กับภัยอันตรายเหล่านี้ก็จะไม่ถูกนำมาใช้ |
| 12.2 ดำเนินการ การประเมินความเสี่ยงซึ่ง:<br>• มีการดำเนินการอย่างน้อยปีละ 1 ครั้งและเมื่อเกิดการเปลี่ยนแปลงขนาดใหญ่ไปยังสิ่งแวดล้อม (เช่น การเข้าซื้อกิจการ รวมกิจการ ย้ายสถานที่ และอื่นๆ)<br>• ระบุถึง ทรัพย์สิน ภัยอันตราย ช่องโหว่ และ<br>• ผลลัพธ์ ในรูปแบบการประเมินความเสี่ยงอย่างเป็นทางการ<br>ตัวอย่างของวิธีการการประเมินความเสี่ยง ได้แก่ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) *OCTAVE, ISO 27005* และ *NIST SP 800-30* | 12.2.a ตรวจสอบว่ากระบวนการประเมินความเสี่ยงประจำปีได้รับการบันทึกเป็นเอกสาร ซึ่งระบุถึง ทรัพย์สิน ภัยอันตราย ช่องโหว่ และผลลัพธ์ ในรูปแบบการประเมินความเสี่ยงอย่างเป็นทางการ<br>12.2.b ตรวจทานเอกสารการประเมินความเสี่ยง เพื่อตรวจสอบว่ากระบวนการประเมินความเสี่ยงมีการดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อเกิดการเปลี่ยนแปลงขนาดใหญ่ไปยังสิ่งแวดล้อม | การประเมินความปลอดภัย ทำให้องค์กรสามารถระบุถึงภัยอันตราย และช่องโหว่ที่เกี่ยวข้อง พร้อมทั้งความเสี่ยงของผลกระทบในทางลบกับธุรกิจ ทำให้สามารถจัดสรรหาแหล่งข้อมูลเพื่อดำเนินการควบคุมซึ่งลดโอกาส และ/หรือ ความเสี่ยงจากอันตราย<br>ดำเนินการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้งและและเมื่อเกิดการเปลี่ยนแปลงขนาดใหญ่ในองค์กร เพื่อรักษาความเป็นปัจจุบันกับการเปลี่ยนแปลง และให้ทันต่อภัยอันตรายที่วิวัฒนาการ แนวโน้ม และเทคโนโลยี |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.3 พัฒนานโยบายการใช้สำหรับสำหรับเทคโนโลยีสำคัญและกำหนดการใช้งานที่เหมาะสมสำหรับเทคโนโลยีเหล่านี้<br><br>*Note:* ตัวอย่างของเทคโนโลยีสำคัญ ได้แก่ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) การเข้าถึงทางไกล (remote access) และเทคโนโลยีไร้สาย (wireless technology) แลปท็อป แทบเล็ท สื่ออิเล็กทรอนิกส์ที่เคลื่อนที่ได้ การใช้ e-mail และการใช้อินเทอร์เน็ต<br><br>ทำให้มั่นใจว่านโยบายการใช้งานเหล่านี้ร้องขอสิ่งต่อไปนี้: | 12.3 ตรวจสอบนโยบายการใช้สำหรับเทคโนโลยีสำคัญและสัมภาษณ์บุคลากรที่รับผิดชอบ เพื่อตรวจสอบว่านโยบายต่อไปนี้มีการดำเนินการ และปฏิบัติตาม: | นโยบายการใช้งานโดยบุคลากร สามารถห้ามการใช้อุปกรณ์ และเทคโนโลยีอื่นๆบางประเภทที่นอกเหนือจากนโยบายองค์กรกำหนด หรือให้คำแนะนำสำหรับบุคลากรสำหรับการใช้งานที่ถูกต้องและการปฏิบัติตาม หากไม่มีการใช้นโยบายการใช้งาน บุคลากรอาจใช้เทคโนโลยีที่ละเมิดนโยบายขององค์กร ซึ่งอาจทำให้ผู้ประสงค์ร้ายสามารถได้รับสิทธิเข้าถึงระบบสำคัญและข้อมูลผู้ถือบัตรได้ |
| 12.3.1 ต้องได้รับการอนุมัติที่ชัดเจนจากบุคคลที่มีอำนาจ | 12.3.1 ตรวจสอบว่า นโยบายการใช้งาน มีกระบวนการอนุมัติที่ชัดเจนจากบุคคลที่มีอำนาจสำหรับเทคโนโลยี | หากไม่มีการขอการอนุมัติในการดำเนินการใช้เทคโนโลยีบุคลากรแต่ละคนอาจดำเนินการกระบวนการซึ่งตามความต้องการของธุรกิจอย่างรู้เท่าไม่ถึงการณ์ และทำให้เกิดช่องโหว่ซึ่งกระทบต่อระบบและข้อมูลสำคัญได้ |
| 12.3.2 ต้องได้รับการรับรองในการใช้เทคโนโลยี | 12.3.2 ตรวจสอบว่า นโยบายการใช้งาน มีกระบวนการสำหรับการรับรองอุปกรณ์ที่ใช้ทั้งหมด ด้วย user ID และ รหัสผ่าน หรือ วิธีการรับรองอื่นๆ (เช่น token) | หากมีการใช้เทคโนโลยีโดยไม่ได้รับการรับรองที่เหมาะสม (user ID รหัสผ่าน token VPN และ อื่นๆ) ผู้ประสงค์ร้ายอาจฉวยโอกาสจากการไม่มีการป้องกันนี้เพื่อเข้าถึงระบบสำคัฐและข้อมูลผู้ถือบัตรได้ |
| 12.3.3 รายการของอุปกรณ์ทั้งหมด และบุคลากรทั้งหมดที่ได้รับการเข้าถึง | 12.3.3 ตรวจสอบว่านโยบายการใช้ได้กำหนดรายการของอุปกรณ์ทั้งหมดและบุคลากรทั้งหมดที่ได้รับการเข้าถึงอุปกรณ์นั้นๆ | ผู้ประสงค์ร้ายอาจฝ่าระบบความปลอดภัยทางกายภาพ และเชื่อมอุปกรณ์ของตนเข้ากับเครือข่าย “ประตูหลัง (back door)” หรือบุคลากรอาจลัดขั้นตอน และอุปกรณ์ คลังอุปกรณ์ที่มีฉลากอุปกรณ์ที่เหมาะสมจะทำให้สามารถตรวจพบการติดตั้งอุปกรณ์ที่ไม่ได้รับอนุญาตได้อย่างรวดเร็ว |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.3.4 วิธีการที่แม่นยำและง่ายดายในการตรวจหาเจ้าของ ข้อมูลการติดต่อ (contact information) และจุดประสงค์ (เช่น การติดฉลาก หมายเลข (code) และ/หรือ การจัดทำคลังอุปกรณ์) | 12.3.4 ตรวจสอบว่า นโยบายการใช้งาน กำหนดให้มีวิธีการที่แม่นยำและง่ายดายในการตรวจหาเจ้าของ ข้อมูลการติดต่อ (contact information) และจุดประสงค์ (เช่น การติดฉลาก หมายเลข (code) และ/หรือ การจัดทำคลังอุปกรณ์) | ผู้ประสงค์ร้ายอาจฝ่าระบบความปลอดภัยทางกายภาพ และเชื่อมอุปกรณ์ของตนเข้ากับเครือข่าย “หลังบ้าน (back door)” หรือบุคลากรอาจลัดขั้นตอน และอุปกรณ์ คลังอุปกรณ์ที่มีฉลากอุปกรณ์ที่เหมาะสมจะทำให้สามารถตรวจพบการติดตั้งอุปกรณ์ที่ไม่ได้รับอนุญาตได้อย่างรวดเร็ว พิจารณาจัดการตั้งชื่ออย่างเป็นทางการของอุปกรณ์ และบันทึกอุปกรณ์ทั้งหมดด้วยกวรควบคุมคลังที่ได้จัดตั้ง การติดฉลากทางระบบ อาจให้ข้อมูล เช่น หมายเลข (code) ซึ่งสามารถบ่งชี้ผู้เป็นเจ้าของ ข้อมูลการติดต่อ (contact information) และจุดประสงค์ได้ |
| 12.3.5 การใช้เทคโนโลยีที่ยอมรับได้ | 12.3.5 ตรวจสอบว่า นโยบายการใช้งานได้กำหนดการใช้เทคโนโลยีที่ยอมรับได้ | ด้วยการกำหนดการใช้งานทางธุรกิจที่ยอมรับได้ และสถานที่ของอุปกรณ์และเทคโนโลยีที่องค์กรยอมรับได้ องค์กรสามารถจัดการ และควบคุมช่องว่างของการตั้งค่า และการดำเนินการควบคุมได้ง่ายยิ่งขึ้น เพื่อให้มั่นใจว่า “ประตูหลัง (back door)” ไม่ได้ถูกเปิดไว้ให้สำหรับผู้ประสงค์ร้ายเพื่อได้รับสิทธิเข้าถึงระบบสำคัญและข้อมูลผู้ถือบัตร |
| 12.3.6 ตำแหน่งเครือข่ายสำหรับเทคโนโลยีที่ยอมรับได้ | 12.3.6 ตรวจสอบว่า นโยบายการใช้งานได้กำหนดตำแหน่งเครือข่ายสำหรับเทคโนโลยีที่ยอมรับได้ | |
| 12.3.7 รายการสินค้าที่ได้รับการอนุมัติจากองค์กร | 12.3.7 ตรวจสอบว่า นโยบายการใช้งานได้กำหนดรายการสินค้าที่ได้รับการอนุมัติจากองค์กร | |
| 12.3.8 ปิดการเชื่อมต่ออัตโนมัติสำหรับเซสชั่น (session) ของเทคโนโลยีการเข้าถึงทางไกลหลังไม่มีการใช้งานในช่วงเวลาที่กำหนด | 12.3.8.a ตรวจสอบว่า นโยบายการใช้งาน ได้มีการให้ปิดการเชื่อมต่ออัตโนมัติสำหรับเซสชั่น (session) ของเทคโนโลยีการเข้าถึงทางไกลหลังไม่มีการใช้งานในช่วงเวลาที่กำหนด | เทคโนโลยีการเข้าถึงทางไกลมักเป็น “ประตูหลัง” ไปยังแหล่งที่สำคัญ และ ข้อมูลผู้ถือบัตร ด้วยการปิดการเชื่อมต่อเมื่อไม่มีการใช้งาน (เช่น ที่ใช้สำหรับสนับสนุนระบบโดยผู้ขาย POS ผู้ขายอื่นๆ หรือ คู่ค้าทางธุรกิจ) การเข้าถึง และความเสี่ยงต่อเครือข่ายก็จะลดลง |
| | 12.3.8.b ตรวจสอบการตั้งค่าเทคโนโลยีการเข้าถึงทางไกล เพื่อตรวจสอบว่ามีการปิดการเชื่อมต่ออัตโนมัติหลังไม่มีการใช้งานในช่วงเวลาที่กำหนด | |
| 12.3.9 การเปิดการใช้งานของเทคโนโลยีการเข้าถึงทางไกลสำหรับผู้ขาย และคู่ค้าทางธุรกิจเฉพาะเมื่อต้องการ และมีการปิดการใช้งานทันทีหลังสิ้นสุด | 12.3.9 ตรวจสอบว่า นโยบายการใช้งานมีการให้เปิดการใช้งานของเทคโนโลยีการเข้าถึงทางไกลสำหรับผู้ขาย และคู่ค้าทางธุรกิจเฉพาะเมื่อต้องการ และมีการปิดการใช้งานทันทีหลังสิ้นสุด | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.3.10 ห้ามการคัดลอก เคลื่อนย้าย และจัดเก็บข้อมูลผู้ถือบัตรลงบน local hard drive และสื่ออิเล็กทรอนิกส์ที่สามารถเคลื่อนที่ได้ สำหรับบุคลากรที่เข้าถึงข้อมูลผู้ถือบัตรผ่านเทคโนโลยีการเข้าถึงทางไกล เว้นแต่ได้รับการรับรองอย่างชัดเจนที่กำหนดโดยความต้องการทางธุรกิจ<br>หากมีความต้องการทางธุรกิจที่ได้รับการรับรอง นโยบายการใช้งานจะต้องร้องขอให้ข้อมูลนั้นๆได้รับการปกป้องตามความต้องการ PCI DSS | 12.3.10.a ตรวจสอบว่านโยบายการใช้งานห้ามการคัดลอก เคลื่อนย้าย และจัดเก็บข้อมูลผู้ถือบัตรลงบน local hard drive และสื่ออิเล็กทรอนิกส์ที่สามารถเคลื่อนที่ได้ เมื่อมีการเข้าถึงด้วยเทคโนโลยีการเข้าถึงทางไกล<br>12.3.10.b สำหรับบุคลากรที่มีการอนุญาตที่เหมาะสม ตรวจสอบว่านโยบายการใช้งานร้องขอให้มีการปกป้องข้อมูลผู้ถือบัตรตามความต้องการ PCI DSS หรือไม่ | เพื่อให้มั่นใจว่าบุคลากรทั้งหมดตระหนักถึงความรับผิดชอบในการจัดเก็บ หรือคัดลอกข้อมูลผู้ถือบัตรลงบนคอมพิวเตอร์หรือสื่อส่วนตัว นโยบายความห้ามการกระทำเหล่านี้อย่างชัดเจน เว้นแต่สำหรับบุคลากรซึ่งมีการรับรองที่ชัดเจน การจัดเก็บ หรือ คัดลอกข้อมูลผู้ถือบัตรลงบน local hard drive หรือ สื่ออื่นๆจะต้องดำเนินการตามความต้องการ PCI DSS |
| 12.4 ทำให้มั่นใจว่านโยบายความปลอดภัยและกระบวนการกำหนดความรับผิดชอบของบุคลากรทั้งหมดต่อความปลอดภัยของข้อมูลไว้อย่างชัดเจน | 12.4.a ตรวจสอบว่า ข้อมูลนโยบายความปลอดภัยความปลอดภัยได้กำหนดอย่างชัดเจนในเรื่องความรับผิดชอบในความปลอดภัยของข้อมูลสำหรับบุคลากร<br>12.4.b สัมภาษณ์ตัวอย่างบุคลากรที่รับผิดชอบเพื่อตรวจสอบว่าพวกเขาเข้าใจนโยบายความปลอดภัยหรือไม่ | หากไม่มีการกำหนดบทบาทความปลอดภัยอย่างชัดเจน และมอบหมายความรับผิดชอบ อาจทำให้มีความไม่แน่นอนในการตอบสนองต่อกลุ่มความปลอดภัย ทำให้เกิดการดำเนินการใช้เทคโนโลยีที่ไม่ปลอดภัย หรือการใช้เทคโนโลยีที่ล้าสมัย |
| 12.5 มอบหมายการจัดการความปลอดภัยของข้อมูลให้บุคคล หรือ ทีม: | 12.5 ตรวจสอบข้อมูลนโยบายความปลอดภัยและกระบวนการความปลอดภัยเพื่อตรวจสอบว่า:<br>• มีการมอบหมายอย่างเป็นทางการในด้านความปลอดภัยของข้อมูลไปยังหัวหน้าพนักงานด้านความปลอดภัย หรือ สมาชิกอื่นๆที่มีความรู้ด้านความปลอดภัย หรือ การจัดการ<br>• ความรับผิดชอบด้านความปลอดภัยของข้อมูลต่อไปนี้ได้รับการมอบหมายอย่างเฉพาะเจาะลง และ อย่างเป็นทางการ: | แต่ละบุคคล หรือ ทีม ที่มีความรับผิดชอบในการจัดการความปลอดภัยของข้อมูลควรตระหนักอย่างชัดเจนถึงความรับผิดชอบและหน้าที่ที่เกี่ยวข้องผ่านนโยบาย หากไม่มีความรับผิดชอบนี้อาจเกิดช่องว่างในการเข้าถึงระบบสำคัญและข้อมูลผู้ถือบัตรได้ |
| 12.5.1 จัดตั้ง เอกสารและแจกจ่ายนโยบายและกระบวนการความปลอดภัย | 12.5.1 ตรวจสอบว่าความรับผิดชอบในการจัดตั้ง เอกสารและแจกจ่ายนโยบายและกระบวนการความปลอดภัยได้รับการมอบหมาย | |
| 12.5.2 ติดตามและวิเคราะห์การแจ้งเตือนความปลอดภัย ข้อมูล และการแจกจ่ายไปยังบุคลากรที่เหมาะสม | 12.5.2 ตรวจสอบว่า ความรับผิดชอบในการติดตามและวิเคราะห์การแจ้งเตือนความปลอดภัย ข้อมูล และการแจกจ่ายไปยังบุคลากรที่เหมาะสมได้รับการมอบหมายอย่างเป็นทางการ | |
| 12.5.3 จัดตั้ง จัดทำเอกสารและ แจกจ่ายการตอบสนองต่อเหตุการณ์การรักษาความปลอดภัย และกระบวนการเพิ่มเติมเพื่อให้มั่นใจว่าการจัดการที่ทันท่วงทีและมีประสิทธิภาพสำหรับทุกสถานการณ์ | 12.5.3 ตรวจสอบว่าความรับผิดชอบในการจัดตั้ง จัดทำเอกสารและ แจกจ่ายการตอบสนองต่อเหตุการณ์การรักษาความปลอดภัย และกระบวนการเพิ่มเติมได้รับการมอบหมายอย่างเป็นทางการ | |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.5.4 บัญชีผู้ดูแลระบบ รวมไปถึงการเพิ่ม ลบ และปรับแต่ง | 12.5.4 ตรวจสอบว่าความรับผิดชอบสำหรับการดูแลระบบ (เพิ่ม ลบ และปรับแต่ง) บัญชีผู้ใช้และ การจัดการการรับรองได้รับการมอบหมายอย่างเป็นทางการ | |
| 12.5.5 เฝ้าติดตาม และ ควบคุมการเข้าถึงทั้งหมดไปยังข้อมูล | 12.5.5 ตรวจสอบว่าความรับผิดชอบสำหรับการเฝ้าติดตาม และการควบคุมการเข้าถึงไปยังข้อมูลทั้งหมด ได้รับการมอบหมายอย่างเป็นทางการ | |
| 12.6 ดำเนินการให้มีโปรแกรมการเฝ้าระวังความปลอดภัยอย่างเป็นทางการ เพื่อทำให้บุคลากรทั้งหมดตระหนักถึงความสำคัญของความปลอดภัยของข้อมูลผู้ถือบัตร | 12.6.a ตรวจทานโปรแกรมการเฝ้าระวังความปลอดภัย เพื่อตรวจสอบว่า ได้ให้ความตระหนักกับบุคลากรทั้งหมดเกี่ยวกับความสำคัญของความปลอดภัยของข้อมูลผู้ถือบัตร | หากบุคลากรไม่ได้รับการให้ความรู้ เกี่ยวกับความรับผิดชอบด้านความปลอดภัย การรักษาความปลอดภัย และกระบวนการของพวกเขา อาจทำให้บุคลากรไม่มีประสิทธิภาพ จากการกระทำผิดพลาด หรือ กระทำโดยเจตนา |
| | 12.6.b ตรวจสอบกระบวนการและเอกสารโปรแกรมการเฝ้าระวังความปลอดภัย และดำเนินการดังนี้: | |
| 12.6.1 ให้ความรู้บุคลากรเมื่อว่าจ้าง และอย่างน้อยปีละ 1 ครั้ง<br>หมายเหตุ: วิธีการอาจแตกต่างออกไปขึ้นอยู่กับบทบาทหน้าที่ของบุคลากรและระดับการเข้าถึงข้อมูลผู้ถือบัตรของพวกเขา | 12.6.1.a ตรวจสอบว่าโปรแกรมการเฝ้าระวังความปลอดภัยใช้วิธีการหลากหลายในการ เฝ้าระวังการสื่อสารและให้ความรู้บุคลากร (เช่น ผ่านโปสเตอร์ จดหมาย บันทึกช่วยจำ การฝึกผ่านเว็บ การประชุม และ การเลื่อนตำแหน่ง) | หากโปรแกรมการเฝ้าระวังความปลอดภัยไม่ได้มีการทบทวนเป็นระยะๆ กุญแจสำคัญและกระบวนการความปลอดภัยอาจถูกลืมหรือลัดขั้นตอน ซึ่งอาจทำให้เกิดการเปิดเผยแหล่งข้อมูลสำคัญและข้อมูลผู้ถือบัตรได้ |
| | 12.6.1.b ตรวจสอบว่าบุคลากร เข้าร่วมการฝึกฝนการระวังความปลอดภัยเมื่อว่าจ้างและอย่างน้อยปีละ 1 ครั้ง | |
| | 12.6.1.c สัมภาษณ์ตัวอย่างของบุคลากร เพื่อตรวจสอบว่าพวกเขาบรรลุการฝึกและตระหนักถึงความสำคัญของความปลอดภัยของข้อมูลผู้ถือบัตร | |
| 12.6.2 ร้องขอให้มีการรับทราบบุคลากรทราบว่าพวกเขาได้อ่าน และเข้าใจนโยบาย และกระบวนการความปลอดภัยอย่างน้อยปีละ 1 ครั้ง | 12.6.2 ตรวจสอบว่าโปรแกรมการเฝ้าระวังความปลอดภัย ร้องขอให้บุคลากรทราบว่าพวกเขาต้องอ่าน และเข้าใจนโยบายและกระบวนการความปลอดภัยอย่างน้อยปีละ 1 ครั้ง ซึ่ง | ร้องขอให้มีการรับทราบโดยบุคลากรเป็นเอกสาร หรือทางอิเล็กทรอนิกส์ให้มั่นใจว่าพวกเขาได้อ่าน และเข้าใจนโยบาย และกระบวนการความปลอดภัย ซึ่งพวกเขาปฏิบัติตาม และจะปฏิบัติตามนโยบายเหล่านี้อย่างต่อเนื่อง |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.7 กลั่นกรองบุคลากรที่อาจแฝงเร้นก่อนการว่าจ้างเพื่อลดความเสี่ยงจากภายใน (ตัวอย่างของการตรวจสอบข้อมูลปูมหลัง ได้แก่ ประวัติการจ้างงาน บันทึกอาชญากรรม ประวัติเครดิต และการอ้างอิงอื่นๆ)<br><br>หมายเหตุ: บุคลากรที่อาจแฝงเร้นอาจถูกจ้างเข้ามาในตำแหน่งเช่น แคชเชียร์ร้ายค้า ผู้มีการเข้าถึงไปยังหมายเลขบัตร เมื่อทำธุรกรรม ความต้องการนี้เป็นเพียงการแนะนำเท่านั้น | 12.7 ตรวจสอบกับหน่วยงานการจัดการทรัพยากรมนุษย์ และตรวจสอบว่าได้มีการตรวจสอบข้อมูลปูมหลัง (ภายใต้ข้อจำกัดของกฎหมาย) ก่อนการจ้างงานบุคลากร ผู้ซึ่งมีการเข้าถึงไปยังข้อมูลผู้ถือบัตร หรือสิ่งแวดล้อม ข้อมูลผู้ถือบัตร | กลั่นกรองบุคลากรที่อาจแฝงเร้นก่อนการว่าจ้างผู้ที่มีการเข้าถึงข้อมูลผู้ถือบัตร จะช่วยลดความเสี่ยงของการนำ PAN และข้อมูลผู้ถือบัตรอื่นๆไปใช้โดยไม่ได้รับอนุญาตจากบุคคลน่าสงสัย หรือผู้ที่มีประวัติอาชญากรรม |
| 12.8 บำรุงรักษาและดำเนินการให้มีนโยบายและกระบวนการเพื่อจัดการผู้ให้บริการผู้ที่มีการแบ่งปันข้อมูลผู้ถือบัตร หรือที่อาจกระทบต่อความปลอดภัยของข้อมูลผู้ถือบัตรดังนี้: | 12.8 จากการสังเกตการตรวจทานนโยบายและกระบวนการ และการตรวจทานเอกสารการสนับสนุน ให้ตรวจสอบว่ามีการดำเนินการกระบวนการสำหรับผู้ให้บริการผู้ซึ่งมีการแบ่งปันข้อมูลผู้ถือบัตร หรือที่อาจกระทบต่อความปลอดภัยของข้อมูลผู้ถือบัตร (เช่น อาคารจัดเก็บ backup tape, ผู้ให้บริการการจัดการ เช่น บริษัท hosting ที่มีพื้นฐานบนเว็บ, บริษัทหรือผู้ให้บริการความปลอดภัย ผู้ซึ่งได้รับข้อมูลสำหรับจุดประสงค์การจำลองการปลอมแปลง และอื่นๆ) ดังนี้: | หากผู้ขาย หรือผู้ให้บริการ แบ่งปันข้อมูลผู้ถือบัตร กับผู้ให้บริการความต้องการบางข้อจะต้องนำไปใช้เพื่อทำให้มั่นใจว่า ผู้ให้บริการเหล่านี้มีการปกป้องของข้อมูลนี้อย่างต่อเนื่อง |
| 12.8.1 บำรุงรักษารายการผู้ให้บริการ | 12.8.1 ตรวจสอบว่ารายการผู้ให้บริการได้รับการบำรุงรักษา | ตามตามการระบุผู้ให้บริการทั้งหมด ซึ่งทำให้มีความเสี่ยงขยายออกไปภายนอกองค์กร |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.8.2 บำรังรักษาเอกสารการข้ออตกลงซึ่งรวมไปถึงการรับทราบว่าผู้ให้บริการคือผู้รับผิดชอบสำหรับความปลอดภัยของข้อมูลผู้ถือบัตรที่ผู้ให้บริการครอบครองหรือทำการ จัดเก็บ ดำเนินการ หรือส่งข้อมูลในนามของลูกค้า หรือในขอบเขตที่พวกเขาอาจส่งผลกระทบต่อความปลอดภัยของสิ่งแวดล้อม ข้อมูลผู้ถือบัตรของลูกค้า<br><br>หมายเหตุ: การกำหนดคำที่แน่นอน สำหรับ การรับทราบขึ้นอยู่กับข้อตกลงระหว่างสองบุคคลและรายละเอียดของการให้บริการ และความรับผิดชอบที่มอบหมายให้สำหรับแต่ละบุคคล การรับทราบ (Acknowledgement) ไม่จำเป็นต้องรวมถึงการกำหนดคำที่แน่นอนในความต้องการนี้ | 12.8.2 สังเกตเอกสารข้อตกลงและยืนยันว่าได้มี การรับทราบ โดยผู้ให้บริการซึ่งเป็นผู้รับผิดชอบต่อความปลอดภัยของข้อมูลผู้ถือบัตร ที่ผู้ให้บริการครอบครองหรือทำการ จัดเก็บ ดำเนินการ หรือส่งข้อมูลในนามของลูกค้า หรือในขอบเขตที่พวกเขาอาจส่งผลกระทบต่อความปลอดภัยของสิ่งแวดล้อม ข้อมูลผู้ถือบัตรของลูกค้า | การรับทราบของผู้ให้บริการ เป็นหลักฐานของข้อผูกพันธ์ในการรักษาความปลอดภัยอย่างเหมาะสมของข้อมูลผู้ถือบัตรซึ่งได้รับมาจากลูกค้า<br><br>พร้อมด้วยความต้องการ 12.9 ความต้องการสำหรับเอกสารข้อตกลงระหว่างองค์กรและผู้ให้บริการนี้ มีจุดประสงค์เพื่อเพิ่มระดับความมั่นคงของความเข้าใจระหว่างบุคคลเกี่ยวกับความรับผิดชอบ PCI DSS ที่เหมาะสม เช่น ข้อตกลงอาจมีให้มีการบำรุงรักษาความต้องการ PCI DSS ในฐานะส่วนหนึ่งของการให้บริการ |
| 12.8.3 ทำให้มั่นใจว่ามีการจัดตั้งกระบวนการสำหรับผู้ให้บริการที่มีส่วนร่วม รวมทั้งข้อกำหนดที่เหมาะสม ก่อนการเข้ามามีส่วนร่วม | 12.8.3 ตรวจสอบว่านโยบาย และกระบวนการได้รับการบันทึกเป็นเอกสารและดำเนินการ รวมทั้งข้อกำหนดที่เหมาะสม ก่อนการเข้ามามีส่วน | กระบวนการนี้จะทำให้มั่นใจว่าการมีส่วนร่วมของผู้ให้บริการได้มีการตรวจสอบอย่างละเอียดโดยองค์กร ซึ่งควรให้มีการวิเคราะห์ความเสี่ยงก่อนการจัดตั้งความสัมพันธ์อย่างเป็นทางการกับผู้ให้บริการ<br><br>กระบวนการและเป้าหมายของข้อกำหนดที่เหมาะสมอาจต่างออกไปในแต่ละองค์กร เช่น การพิจารณาอาจรวมไปถึงรายงานวิธีการของผู้ให้บริการ, การแจ้งเตือนการฝ่าระบบและกระบวนการรับมือต่อเหตุการ, รายละเอียดวิธีการการมอบหมายความรับผิดชอบ PCI DSS ระหว่างบุคคล, วิธีการและหลักฐานของผู้ให้บริการในการตรวจสอบการปฏิบัติตาม PCI DSS ของพวกเขา และอื่นๆ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.8.4 บำรุงรักษาโปรแกรมเฝ้าติดตามสถานะการปฏิบัติตาม PCI DSS ของผู้ให้บริการอย่างน้อยปีละ 1 ครั้ง | 12.8.4 ตรวจสอบว่าหน่วยงาน บำรุงรักษาโปรแกรมเฝ้าติดตามสถานะการปฏิบัติตาม PCI DSS ของผู้ให้บริการอย่างน้อยปีละ 1 ครั้ง | การรู้ถึงสถานะการปฏิบัติตาม PCI DSS ของผู้ให้บริการช่วยให้มั่นใจและตระหนักว่าพวกเขายอมรับความต้องการเดียวกันกับองค์กรของคุณ หากผู้ให้บริการเสนอบริการที่หลากหลาย ความต้องการนี้ควรใช้กับบริการที่ส่งมอบให้กับลูกค้า และบริการที่อยู่ภายใต้ขอบเขตการประเมิน PCI DSS เหล่านั้นด้วย<br><br>ข้อมูลเฉพาะของการบำรุงรักษาหน่วยงานขึ้นอยู่กับข้อตกลงกับผู้ให้บริการ ประเภทบริการ และอื่นๆ จุดประสงค์คือการทำให้หน่วยงานเข้าใจว่าความต้องการ PCI DSS ใดที่ผู้ให้บริการยินยอมที่จะดำเนินการตาม |
| 12.8.5 บำรุงรักษาข้อมูลเกี่ยวกับการจัดการความต้องการ PCI DSS โดยผู้ให้บริการแต่ละคน และโดยหน่วยงาน | 12.8.5 ตรวจสอบหน่วยงาน บำรุงรักษาข้อมูลเกี่ยวกับการจัดการความต้องการ PCI DSS โดยผู้ให้บริการแต่ละคน และโดยหน่วยงาน | |
| 12.9 **กระบวนการเพิ่มเติมสำหรับผู้ให้บริการ**: ผู้ให้บริการแจ้งการรับทราบเป็นเอกสารไปยังลูกค้าว่าพวกเขาเป็นผู้รับผิดชอบในความปลอดภัยของข้อมูลผู้ถือบัตรซึ่งผู้ให้บริการ ครอบครองหรือ จัดเก็บ ดำเนินการ หรือส่งข้อมูลในนามของลูกค้า หรือในขอบเขตที่พวกเขาอาจส่งผลกระทบต่อความปลอดภัยของสิ่งแวดล้อม ข้อมูลผู้ถือบัตรของลูกค้า<br><br>หมายเหตุ: ความต้องการนี้เป็นวิธีการที่ดีที่สุดจนถึง 30 มิถุนายน 2558 หลังจากกลายเป็นความต้องการ<br><br>หมายเหตุ: การกำหนดคำที่แน่นอน สำหรับ การรับทราบขึ้นอยู่กับข้อตกลงระหว่างสองบุคคลและรายละเอียดของการให้บริการ และความรับผิดชอบที่มอบหมายให้สำหรับแต่ละบุคคล การรับทราบ (Acknowledgement) ไม่จำเป็นต้องรวมถึงการกำหนดคำที่แน่นอนในความต้องการนี้ | 12.9 **กระบวนการเพิ่มเติมสำหรับผู้ให้บริการ**: ตรวจทาน นโยบายของผู้ให้บริการและกระบวนการและ สังเกตรูปแบบเอกสารข้อตกลงเพื่อยืนยันว่า ผู้ให้บริการแจ้งการรับทราบเป็นเอกสารไปยังลูกค้าว่าผู้ให้บริการจะบำรุงรักษาการปฏิบัติตามความต้องการ PCI DSS ในขอบเขตที่ผู้ให้บริการดูแล มีการเข้าถึงไปยัง หรือ จัดเก็บ ดำเนินการ หรือ ส่งข้อมูล ข้อมูลผู้ถือบัตรของลูกค้า หรือการรับรองข้อมูลที่สุ่มเสี่ยง หรือ จัดการสิ่งแวดล้อมข้อมูลผู้ถือบัตรของลูกค้าในนามของลูกค้า | ความต้องการนี้ใช้ก็ต่อเมื่อหน่วยงานที่ได้รับการประเมินคือผู้ให้บริการ พร้อมกับความต้องการ 12.8.2 ความต้องการนี้มีจุดประสงค์เพื่อเพิ่มระดับความมั่นคงของความเข้าใจระหว่างบุคคลเกี่ยวกับความรับผิดชอบ การรับทราบของผู้ให้บริการ เป็นหลักฐานการยินยอมว่าพวกเขาจะบำรุงรักษา ความปลอดภัยอย่างเหมาะสมสำหรับข้อมูลผู้ถือบัตรซึ่งได้รับมาจากลูกค้า<br><br>วิธีการที่ผู้ให้บริการมอบเอกสารการรับทราบ ควรได้รับการตกลงระหว่างผู้ให้บริการและลูกค้าของพวกเขา |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.10 ดำเนินการให้มีการเตรียมแผนการรับมือต่อเหตุการณ์เพื่อตอบสนองอย่างทันทีไปยังการฝ่าระบบ | 12.10 ตรวจสอบว่าหน่วยงานได้มีการเตรียมแผนการรับมือต่อเหตุการและกระบวนการที่เกี่ยวข้องเพื่อตรวจสอบไว้ เพื่อตอบสนองอย่างทันทีไปยังการฝ่าระบบโดยการดำเนินการต่อไปนี้: | หากไม่มีแผนการรับมือต่อเหตุการความปลอดภัยที่รอบคอบ ซึ่งมีการเผยแพร่อ่าน และเข้าใจโดยบุคคลที่มีความรับผิดชอบอย่างเหมาะสม ความสับสน และการตอบโต้ที่ไม่พร้อมเพรียงอาจทำให้ยิ่งเกิดความเสียหายต่อธุรกิจ หรือใช้เวลานานกว่าปรกติในการฟื้นฟู อาจเกิดการการเปิดเผยข้อมูลไปยังสาธารณะอย่างไม่จำเป็น หรือเกิดหนี้สินตามกฎหมาย |
| 12.10.1 สร้างแผนการรับมือต่อเหตุการเพื่อดำเนินการใน หตุการณ์การฝ่าระบบ ทำให้มั่นใจว่าแผนการสามรถจัดการกับสิ่งต่อไปนี้เป็นอย่างน้อย:<br>• บทบาท ความรับผิดชอบ และแผนการสื่อสาร เมื่อเกิดเหตุการณ์การฝ่าระบบ รวมทั้งการแจ้งเตือนแบรนด์การชำระเงินเป็นอย่างน้อย<br>• กระบวนการรับมือต่อเหตุการเฉพาะ<br>• การกู้คืนธุรกิจ และกระบวนการต่อเนื่อง<br>• กระบวนการ Backup ข้อมูล<br>• การวิเคราะห์ของความต้องการทางกฎหมายในการรายงานการเจาะข้อมูล<br>• การคุ้มครอง และการรับมือสำหรับส่วนประกอบระบบสำคัญทั้งหมด<br>• การอ้างอิง หรือ การรวบรวมกระบวนการรับมือต่อเหตุการณ์จากแบรนด์การชำระเงิน | 12.10.1.a ตรวจสอบว่าแผนการรับมือต่อเหตุการได้มี:<br>• บทบาท ความรับผิดชอบ และแผนการสื่อสาร เมื่อเกิดเหตุการณ์การฝ่าระบบ รวมทั้งการแจ้งเตือนแบรนด์การชำระเงินเป็นอย่างน้อย<br>• กระบวนการรับมือต่อเหตุการเฉพาะ<br>• การกู้คืนธุรกิจ และกระบวนการต่อเนื่อง<br>• กระบวนการ Backup ข้อมูล<br>• การวิเคราะห์ของความต้องการทางกฎหมายในการรายงานการเจาะข้อมูล (เช่น กฎหมาย California Bill 1386 ซึ่งเรียกร้องให้มีการแจ้งเตือนของผู้บริโภคที่ได้รับผลกระทบในเหตุการการเจาะระบบจริงหรือเหตุการณ์น่าสงสัยสำหรับธุรกิจใดๆก็ตามในที่มีผู้ที่อาศัยใน California อยู่ในฐานข้อมูล)<br>• การคุ้มครอง และการรับมือสำหรับส่วนประกอบระบบสำคัญทั้งหมด<br>• การอ้างอิง หรือ การรวบรวมกระบวนการรับมือต่อเหตุการณ์จากแบรนด์การชำระเงิน<br><br>12.10.1.b สัมภาษณ์บุคลากร และตรวจทานการจัดทำเอกสารจากตัวอย่างของเหตุการณ์ที่ได้รับการรายงานล่าสุดหรือการแจ้งเตือน เพื่อตรวจสอบว่ามีการดำเนินการตามเอกสารและกระบวนการ แผนการรับมือต่อเหตุการ | แผนการรับมือต่อเหตุการณ์ควรมีความรอบคอม และ มีองค์ประกอบสำคัญทั้งหมดที่ทำให้องค์กรสามารถรับมือได้อย่างมีประสิทธิภาพเมื่อเกิดเหตุการณ์การฝ่าระบบซึ่งกระทบต่อข้อมูลผู้ถือบัตร |
| 12.10.2 ทดสอบแผนการอย่างน้อยปีละ 1 ครั้ง | 12.10.2 ตรวจสอบว่ามีการทดสอบแผนการ อย่างน้อยปีละ 1 ครั้ง | หากไม่มี การทดสอบที่เหมาะสม อาจเกิดการพลาดกระบวนการสำคัญไป ซึ่งอาจทำให้เพิ่มการเปิดเผยขณะเกิดเหตุการณ์ได้ |

| ความต้องการ PCI DSS | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| 12.10.3 กำหนดบุคลากรเฉพาะที่สามารถปฏิบัติงาน 24 ชั่วโมง เพื่อตอบสนองต่อการแจ้งเตือน | 12.10.3 ตรวจสอบจากการสังเกตการตรวจทานนโยบาย และการสัมภาษณ์บุคลากรที่รับผิดชอบ ซึ่งกำหนดให้บุคลากร สามารถปฏิบัติงาน 24 ชั่วโมง เพื่อตอบสนองต่อการแจ้งเตือนและการเฝ้าติดตาม การคุ้มครองหลักฐานการกระทำที่ไม่ได้รับอนุญาต, การตรวจจับ wireless access point ที่ไม่มีการรับรอง การแจ้งเตือน IDS สำคัญ และ/หรือ รายงานการเปลี่ยนแปลงไปยังระบบหรือไฟล์เนื้อหาสำคัญ | หากไม่มีทีมรับมือเหตุการณ์ที่ได้รับการฝึกฝน และพร้อมปฏิบัติงาน จะทำให้ความเสียหายของเครือข่ายแพร่กระจายมากขึ้น และข้อมูลและระบบสำคัญอาจ “ปนเปื้อน” โดยการจัดการที่ไม่เหมาะสมในระบบที่เป็นเป้าหมาย สิ่งนี้อาจขัดความความสำเร็จในการวินิจฉัยหลังเหตุการณ์เจาะระบบได้ |
| 12.10.4 ให้มีการฝึกฝนที่เหมาะสมสำหรับทีมงานที่มีความรับผิดชอบในการรับมือการฝ่าความปลอดภัย | 12.10.4 ตรวจสอบจากการสังเกตการตรวจทานนโยบาย และการสัมภาษณ์บุคลากรที่รับผิดชอบ ว่าทีมงานที่มีความรับผิดชอบในการรับมือการฝ่าความปลอดภัยได้รับการฝึกฝนเป็นระยะๆ | |
| 12.10.5 ให้มีการแจ้งเตือนจากระบบการเฝ้าติดตามความปลอดภัยได้แก่ (เป็นเพียงตัวอย่าง ไม่ได้จำกัดไว้เพียงเท่านี้) การตรวจจับการบุกรุก ระบบป้องกันการบุกรุก Firewall และระบบการติดตามความสมบูรณ์ของไฟล์ | 12.10.5 ตรวจสอบจากการสังเกต และการตรวจทานของ กระบวนการการเฝ้าติดตาม และตอบสนองการแจ้งเตือนจากระบบการเฝ้าติดตามความปลอดภัย ได้แก่ ตรวจจับ wireless access points ที่ไม่มีการรับรอง ครอบคลุมอยู่ในแผนการรับมือต่อเหตุการณ์ | ระบบการเฝ้าติดตามเหล่านี้ได้รับการออกแบบเพื่อมุ้งเน้นในโอกาสที่จะเกิดความเสี่ยงกับข้อมูล ลสำคัญในการดำเนินการอย่างรวดเร็วเพื่อป้องกันการเจาะระบบ และจะต้องรวมไปถึงวิธีการรับมือต่อสถานการณ์ |
| 12.10.6 พัฒนากระบวนการเพื่อปรับแต่งและวิวัฒนาการแผนการรับมือต่อเหตุการณ์ตามบทเรียนที่เรียนรู้ ร่วมกับการพัฒนาอุตสาหกรรม | 12.10.6 ตรวจสอบจากการสังเกตการตรวจทานนโยบาย และการสัมภาษณ์บุคลากรที่รับผิดชอบ พัฒนากระบวนการเพื่อปรับแต่งและวิวัฒนาการแผนการรับมือต่อเหตุการณ์ตามบทเรียนที่เรียนรู้ ร่วมกับการพัฒนาอุตสาหกรรม | รวม “บทเรียนที่เรียนรู้” เข้ากับแผนการรับมือต่อเหตุการณ์หลังเหตุการณ์ช่วยให้แผนการณ์เป็นปัจจุบัน และรับมือกับแนวโน้มความปลอดภัยและอันตรายที่เกิดขึ้นใหม่ |

# ภาคผนวกA: ความต้องการเพิ่มเติมสำหรับผู้ให้บริการ Shared Hosting

**ความต้องการ A.1: ผู้ให้บริการ Shared Hosting ที่มีการเข้าถึงไปยังสิ่งแวดล้อมข้อมูลผู้ถือบัตร**

ตามที่กล่าวในความต้องการ 12.8 และ 12.9 ผู้ให้บริการทั้งหมดที่มีการเข้าถึงไปยังข้อมูลผู้ถือบัตร (รวมไปถึง ผู้ให้บริการ Shared Hosting) จะต้องยึดมั่นกับ PCI DSS นอกจากนั้น ความต้องการ 2.6 กล่าวไว้ว่า ผู้ให้บริการ Shared Hosting จะต้องปกป้องสิ่งแวดล้อมและข้อมูลของแต่ละหน่วยงานที่ทำการ Host ดังนั้นผู้ให้บริการ Shared Hosting จะต้องดำเนินตามความต้องการในภาคผนวกนี้

| ความต้องการ | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| **A.1** ปกป้องสิ่งแวดล้อมและข้อมูลของแต่ละหน่วยงาน (ซึ่งก็คือ ผู้ขาย ผู้ให้บริการ หรือหน่วยงานอื่นๆ) ตาม A.1.1 - A.1.4:<br>ผู้ให้บริการจะต้องบรรลุความต้องการเหล่านี้รวมทั้งส่วนอื่นๆที่เกี่ยวข้องของ PCI DSS<br><br>หมายเหตุ: แม้ผู้ให้บริการบรรลุความต้องการเหล่านี้ก็ไม่ได้เป็นการยืนยันการปฏิบัติตามของหน่วยงานซึ่งใช้บริการผู้ให้บริการ แต่ละหน่วยงานจะต้องดำเนินการตาม *PCI DSS* และตรวจสอบการปฏิบัติตามตามความเหมาะสม | **A.1** เฉพาะสำหรับการประเมิน PCI DSS ของผู้ให้บริการ Shared Hosting ตรวจสอบว่าผู้ให้บริการ ปกป้องสิ่งแวดล้อมและข้อมูลของหน่วยงาน (ผู้ขาย และ ผู้ให้บริการ) เลือกตัวอย่างของเซิฟเวอร์ (Microsoft Windows และ Unix/Linux) ท่ามกลางตัวอย่างที่เป็นตัวแทนของผู้ขายและผู้ให้บริการ และดำเนินการตาม A.1.1 - A.1.4 ด้านล่าง: | ภาคผนวก A ของ PCI DSS มีจุดประสงค์สำหรับ ผู้ให้บริการ Shared Hosting ผู้ซึ่งต้องการให้บริการ Host สิ่งแวดล้อมซึ่งปฏิบัติตาม PCI DSS แก่ผู้ขายและ/หรือผู้ให้บริการ |
| **A.1.1** ทำให้มั่นใจว่าแต่ละดำเนินการเฉพาะกระบวนการ ซึ่งมีการเข้าถึงไปยังสิ่งแวดล้อม ข้อมูลผู้ถือบัตร ของหน่วยงาน | **A.1.1** หากผู้ให้บริการ shared hosting อนุญาตให้หน่วยงาน (เช่น ผู้ขาย หรือผู้ให้บริการ) run แอปพลิเคชั่นของตนเอง ตรวจสอบกระบวนการแอปพลิเคชั่นเหล่านี้ดำเนินการโดยใช้ user ID ที่มีเอกลักษณ์ของหน่ยงาน เช่น:<br>• ไม่มีหน่วยงานใดในระบบสามารถใช้ user ID ของ shared web server ได้<br>• สคริปต์ CGI ทั้งหมดที่ใช้โดยหน่วยงาน จะต้องสร้างและดำเนินการด้วย user ID ที่มีเอกลักษณ์ของหน่วยงาน | หากผู้ขายหรือผู้ให้บริการ ได้รับอนุญาตให้ run แอปพลิเคชั่นของพวกเขาเองบน shared server ควร run ด้วย user ID ของผู้ขายหรือผู้ให้บริการ ดีกว่าการใช้ user ที่มีสิทธิพิเศษ |

| ความต้องการ | กระบวนการทดสอบ | คำแนะนำ |
|---|---|---|
| A.1.2 จำกัดการเข้าถึงและสิทธิพิเศษของแต่ละหน่วยงานให้มีเฉพาะสิ่งแวดล้อม ข้อมูลผู้ถือบัตรของหน่วยงานเองเท่านั้น | A.1.2.a ตรวจสอบว่า user ID ของกระบวนการแอปพลิเคชั่นใดๆไม่ใช่ user ที่มีสิทธิ root/admin | เพื่อทำให้มั่นใจว่าการเข้าถึงและสิทธิพิเศษได้รับการจำกัดซึ่งผู้ขายหรือผู้ให้บริการแต่ละคนเข้าถึงได้เฉพาะสิ่งแวดล้อมของตนเองเท่านั้น พิจารณาดังนี้:<br>1. สิทธิพิเศษของ user ID ของ web server ของ ผู้ขายหรือผู้ให้บริการ;<br>2. อนุญาตให้สำหรับ อ่าน เขียน และจัดการไฟล์;<br>3. อนุญาตให้เขียนถึงไบนารีของระบบ (system binary);<br>4. มีการอนุญาตไฟล์ประวัติ (log) ของผู้ขายและผู้ให้บริการ; และ<br>5. ควบคุมเพื่อทำให้มั่นใจว่า ไม่มีผู้ขายหรือผู้ให้บริการใด สามารถยึดแหล่งข้อมูลระบบได้ |
| | A.1.2.b ตรวจสอบว่าแต่ละหน่วยงาน (ผู้ขาย และ ผู้ให้บริการ) ได้รับอนุญาตการ อ่าน เขียน หรือจัดการไฟล์และ directory ของตนเองหรือไฟล์ระบบที่จำเป็นเท่านั้น (จำกัดโดย การอนุญาตไฟล์ระบบ, รายการการควบคุมการเข้าถึง, คำสั่ง chroot, jailshell, และอื่นๆ)<br>**สำคัญ**: ไฟล์ข้องหน่วยงานจะต้องไม่มีการแบ่งปันในกลุ่ม | |
| | A.1.2.c ตรวจสอบว่า user หน่วยงาน ไม่สามารถ เขียน(write) ไปยังไบนารีระบบได้ (system binary) | |
| | A.1.2.d ตรวจสอบว่าการดูประวัติ ถูกจำกัดไว้เฉพาะที่หน่วยงานเป็นเจ้าของเท่านั้น | |
| | A.1.2.e เพื่อทำให้มั่นใจว่าแต่ละหน่วยงานไม่สามารถยึดแหล่งข้อมูลระบบเซิฟเวอร์เพื่อใช้ประโยชน์จากช่องโหว่ได้ (เช่น error, race, และ เงื่อนไขการ restart ที่ทำให้เกิดเหตุการณ์เช่น การส่งข้อมูลเกินขอบเขต (buffer overflow)) ตรวจสอบว่ามีการจำกัดสำหรับการใช้แหล่งข้อมูลระบบ:<br>• พื้นที่ (Disk space)<br>• แบนด์วิท (Bandwidth)<br>• หน่วยความจำ (Memory)<br>• หน่วยประมวลผล (CPU) | |
| A.1.3 ทำให้มั่นใจว่าการบันทึกประวัติ และการตรวจสอบการตรวจตราเปิดให้ใช้งาน และเป็นเอกเทศน์สำหรับแต่ละหน่วยงาน สิ่งแวดล้อม ข้อมูลผู้ถือบัตร และสอดคล้องกับความต้องการ PCI DSS 10 | A.1.3 ตรวจสอบว่าผู้ให้บริการ shared hosting ได้เปิดให้ใช้งาน ารบันทึกประวัติ และการตรวจสอบการตรวจตราสำหรับแต่ละสิ่งแวดล้อมของผู้ขายและผู้ให้บริการ:<br>• ประวัติได้มีการเปิดให้ใช้งานสำหรับแอปพลิเคชั่นบุคคลที่ 3 ทั่วไป<br>• ประวัติได้มีการเปิดการใช้งานโดยค่าตั้งต้น<br>• ประวัติได้มีการเปิดให้ใช้งานการตรวจทานโดยหน่วยงานที่เป็นเจ้าของ<br>• ตำแหน่งของประวัติ ได้รับการแข้งอย่างชัดเจนให้กับหน่วยงานที่เป็นเจ้าของ | ประวัติควรสามารถใช้งานได้ในสิ่งแวดล้อมการ shared hosting เพื่อที่ผู้ขายและผู้ให้บริการจะสามารถเข้าถึงและสามารถตรวจทาน ประวัติในสิ่งแวดล้อม ข้อมูลผู้ถือบัตรเฉพาะได้ |
| A.1.4 เปิดให้ใช้งานกระบวนการเพื่อให้มีการวินิจฉัยการเจาะระบบตามกฎหมายเป็นระยะๆ สำหรับผู้ขายหรือผู้ให้บริการที่ Host | A.1.4 ตรวจสอบว่าผู้ให้บริการ shared hosting มีเอกสารนโยบายซึ่งให้มีการวินิจฉัยการเจาะระบบตามกฎหมายบนเซิฟเวอร์ที่เกี่ยวข้องเมื่อเกิดเหตุการณ์เจาะระบบ | ผู้ให้บริการ Shared Hosting จพต้องมีกระบวนการที่รวดเร็วและง่ายดาย เมื่อมีความต้องการการวินิจฉัยการเจาะระบบตามกฎหมาย ในระดับรายละเอียดที่เหมาะสม ซึ่งสามารถใช้งานข้อมูลผู้ขายหรือผู้ให้บริการได้ |

# ภาคผนวก B: การควบคุมแบบทดแทน

การควบคุมแบบทดแทนอาจนำมาพิจารณาสำหรับความต้องการ PCI DSS ส่วนมาก เมื่อหน่วยงานไม่สามารถบรรลุความต้องการได้อย่างชัดเจนในการเริ่มต้นเนื่องจากความถูกต้องทางเทคนิค หรือเอกสารข้อจำกัดทางธุรกิจ แต่มีการลดทอนความเสี่ยงเพียงพอกับความต้องการในการปฏิบัติตามหรือการควบคุมการทดแทนอื่นๆ

การควบคุมแบบทดแทนจะต้องบรรลุเกณฑ์ต่อไปนี้:

1. บรรลุจุดประสงค์และความเข้มงวดของความต้องการ PCI DSS ดั้งเดิม
2. ให้ความปลอดภัยใน ระดับเดียวกัน กับความต้องการ PCI DSS ดั้งเดิม การควบคุมแบบทดแทนที่ ป้องกันความเสี่ยงอย่างเพียงพอ เท่าที่ความต้องการ PCI DSS ดั้งเดิมถูกออกแบบมาให้ป้องกัน (โปรดดู การแนะนำ *PCI DSS* สำหรับจุดประสงค์ของแต่ละความต้องการ PCI DSS)
3. สามารถ “บรรลุ และ เหนือ” ความต้องการ PCI DSS อื่นๆ (การอยู่ในการปฏิบัติตามความต้องการ PCI DSS อื่นๆไม่ถือว่าเป็นการควบคุมแบบทดแทน)

   เมื่อประเมินการ “บรรลุ และ เหนือ” ความต้องการ สำหรับการควบคุมแบบทดแทน พิจารณาดังนี้:

หมายเหตุ: ข้อ *a) - c)* ด้านล่างมีจุดประสงค์เพื่อเป็นตัวอย่างเท่านั้น การควบคุมแบบทดแทนทั้งหมดจะต้องได้รับการตรวจทาน และตรวจสอบความถูกต้องสำหรับความเพียงพอโดยผู้ประเมิน ประสิทธิภาพของการควบคุมแบบทดแทนขึ้นอยู่กับ ความเฉพาะของสิ่งแวดล้อมซึ่งดำเนินการ การควบคุมความปลอดภัยโดยรอบ และการตั้งค่าการควบคุม องค์กรควรตระหนักการควบคุมแบบทดแทนใดๆไม่สามารถมีประสิทธิภาพในทุกๆสิ่งแวดล้อมใด

a) ความต้องการ PCI DSS ที่มีอยู่ **ไม่สามารถ** พิจารณาว่าเป็นการควบคุมแบบทดแทนหากได้มีการร้องขออยู่แล้วภายใต้ส่วนที่ทำการตรวจสอบ เช่น รหัสผ่าน ของ การเข้าถึงระดับผู้ดูแลแบบ non-console จะต้องถูกส่งแบบเข้ารหัสเพื่อลดความเสี่ยงในการดักรหัสผ่านผู้ดูแลระบบที่อ่านได้ (clear-text) หน่วยงานไม่สามารถใช้ความต้อวการรหัสผ่าน PCI DSS อื่นๆได้ (การล็อคผู้บุกรุก (intruder lockout) รหัสผ่านที่ซับซ้อน (complex password) และอื่นๆ) เพื่อทดแทนการไม่มีการเข้ารหัสของรหัสผ่านได้ เนื่องจาก ความต้องการรหัสผ่านอื่นๆ ไม่ได้ลดความเสี่ยงในการดักข้อมูลที่อ่านได้ อีกทั้งความต้องการรหัสผ่านอื่นๆยังอยู่ในความต้องการ PCI DSS สำหรับส่วนที่กำลังตรวจสอบอยู่แล้ว (password)

b) ความต้องการ PCI DSS ที่มีอยู่อาจนำมาพิจารณาแทนการควบคุมแบบทดแทนได้หากถูกร้องขอไปยังส่วนอื่น แต่ไม่ใช่ส่วนที่อยู่ในการตรวจทาน เช่น การรับรอง 2 ปัจจัย (Two-factor authentication) คือความต้องการ PCI DSS สำหรับการเข้าถึงทางไกล การรับรองนี้ จากเครือข่ายภายในอาจนำมาพิจารณาว่าเป็นการควบคุมทดแทนได้สำหรับการเข้าถึงระดับผู้ดูแลแบบ non-console เมื่อการส่งข้อมูลรหัสผ่านที่เข้ารหัสไม่อยู่ในการสนับสนุนการรับรอง 2 ปัจจัย อาจเป็นสิ่งที่ยอมรับได้หาก: (1) บรรลุจุดประสงค์ของความต้องการดั้งเดิม โดยจัดการความเสี่ยงในการดักข้อมูลรหัสผ่านที่อ่านได้ของผู้ดูแลระบบ; และ (2) มีการติดตั้งอย่างเหมาะสมในสิ่งแวดล้อมที่ปลอดภัย

c) ความต้องการ PCI DSS ที่มีอยู่อาจนำไปผนวกกับการควบคุมใหม่เพื่อให้เป็นการทดแทน เช่น หากองค์กรไม่สามารถ render ข้อมูลผู้ถือบัตร ให้ไม่สามารถอ่านได้ตามความต้องการ 3.4 (เช่น โดยการเข้ารหัส) การควบคุมแบบทดแทนสามารถประกอบไปด้วยอุปกรณ์ หรือการผสมผสานระหว่างอุปกรณ์ แอปพลิเคชั่น และการควบคุมซึ่งจัดการสิ่งดังต่อไปนี้: (1) การแบ่งการเข้าถึงเครือข่ายภายใน; (2) การกรอง IP address หรือ MAC address; และ (3) การรับรอง 2 ปัจจัยจากภายในของเครือข่ายภายใน

4. เทียบเท่ากันได้กับความเสี่ยงเพิ่มเติมที่เกิดจากการไม่ได้ยึดถือความต้องการ PCI DSS

ผู้ประเมินจะต้องประเมินการควบคุมแบบทดแทนอย่างรอบคอบในระหว่างการประเมิน PCI DSS ประจำปี เพื่อตรวจสอบว่าการควบคุมแบบทดแทน แต่ละส่วนจัดการความเสี่ยงได้เทียบเท่ากับที่ความต้องการ PCI DSS ดั้งเดิมถูกออกแบบมาให้ป้องกัน ตามข้อ 1-4 ด้านบน เพื่อรักษาการปฏิบัติตาม กระบวนการและการควบคุมจะต้องถูกใช้งานเพื่อทำให้มั่นใจว่าการควบคุมแบบทดแทนมีประสิทธิภาพหลังการประเมินลุล่วง

# ภาคผนวก C: เอกสารการควบคุมแบบทดแทน

เอกสารนี้ใช้เพื่อกำหนดการควบคุมแบบทดแทนสำหรับความต้องการใดๆซึ่งมีการใช้การทดแทนเพื่อบรรลุความต้องการ PCI DSS จำไว้ว่าการควบคุมแบบทดแทนจะต้องได้รับการบันทึกในรายงานการปฏิบัติตามตาที่สอดคล้องกับความต้องการ PCI DSS

หมายเหตุ: เฉพาะองค์กรซึ่งได้ดำเนินการวิเคราะห์ความเสี่ยงและเอกสารทางเทคนิคที่ถูกต้องตามกฎหมาย หรือเอกสารข้อจำกัดทางธุรกิจสามารถพิจารณาใช้การควบคุมแบบทดแทนเพื่อบรรลุการปฏิบัติตามได้

ลำดับของความต้องการและความหมาย:

| | ข้อมูลที่ต้องการ | คำอธิบาย |
|---|---|---|
| 1. ข้อจำกัด | รายการข้อจำกัดที่ไม่สามารถปฏิบัติตามความต้องการดั้งเดิมได้ | |
| 2. วัตถุประสงค์ | กำหนดวัตถุประสงค์ของการควบคุมดั้งเดิม; ระบุวัตถุประสงค์ที่บรรลุโดยการควบคุมแบบทดแทน | |
| 3. ความเสี่ยงที่พบ | ระบุ ความเสี่ยงเพิ่มเติมใดๆที่มีหากไม่มีการควบคุมดั้งเดิม | |
| 4. ความหมายของการควบคุมแบบทดแทน | กำหนดการควบคุมแบบทดแทนและอธิบายวิธีการบรรลุวัตถุประสงค์ของการควบคุมดั้งเดิมและความเสี่ยงที่เพิ่มขึ้นหากมี | |
| 5. การตรวจสอบการควบคุมแบบทดแทน | กำหนดวิธีการที่การควบคุมแบบทดแทนจะได้รับการตรวจสอบและทดสอบ | |
| 6. การบำรุงรักษา | กำหนดกระบวนการและการควบคุมที่ใช้เพื่อบำรุงรักษาการควบคุมแบบทดแทน | |

# เอกสารการควบคุมแบบทดแทน – ตัวอย่างที่สมบูรณ์

เอกสารนี้ใช้เพื่อกำหนดการควบคุมแบบทดแทนสำหรับความต้องการใดๆที่ระบุไว้ว่า "มีการใช้งาน" ด้วยการควบคุมแบบทดแทน

ลำดับของความต้องการ: 8.1.1 – ผู้ใช้ทั้งหมดได้รับการระบุตัวตนด้วย user ID ที่มีเอกลักษณ์ ก่อนได้รับการเข้าถึงส่วนประกอบระบบหรือข้อมูลผู้ถือบัตรหรือไม่?

| | ข้อมูลที่ต้องการ | คำอธิบาย |
|---|---|---|
| 1. ข้อจำกัด | รายการข้อจำกัดที่ไม่สามารถปฏิบัติตามความต้องการดั้งเดิมได้ | องค์กร *XYZ* ว่าจ้าง Unix Server ที่เป็นเอกเทศน์ (*stand alone*) หากไม่มี *LDAP* ซึ่งต้องการ *"root"* ในการ *login* แต่ละครั้ง เป็นไปไม่ได้เลยที่องค์กร *XYZ* จะสามารถจัดการการ *login "root"* และ เป็นไปไม่ได้ที่จะบันทึกประวัติการทำกิจกรรมที่ใช้สิทธิ *"root"* โดยผู้ใช้แต่ละคน |
| 2. วัตถุประสงค์ | กำหนดวัตถุประสงค์ของการควบคุมดั้งเดิม; ระบุวัตถุประสงค์ที่บรรลุโดยการควบคุมแบบทดแทน | วัตถุประสงค์ของความต้องการการ *login* อย่างเป็นเอกเทศน์ มี 2 ข้อ ข้อแรกคือเป็นสิ่งที่ยอมรับไม่ได้จากมุมมองความปลอดภัยในการใช้ข้อมูลส่วนตัวการ *login* ร่วมกัน ข้อสองคือการมีการแบ่งปันการ *login* ทำให้ไม่สามารถบ่งชี้การกระทำของบุคคลใดๆได้ |
| 3. ความเสี่ยงที่พบ | ระบุ ความเสี่ยงเพิ่มเติมใดๆที่มีหากไม่มีการควบคุมดั้งเดิม | ความเสี่ยงเพิ่มเติมที่เกิดขึ้นบนระบบควบคุมการเข้าถึง โดยการไม่มีการยืนยันให้ผู้ใช้มี *ID* ที่แตกต่างกันคือการไม่สามารถทำการติดตามได้ |
| 4. ความหมายของการควบคุมแบบทดแทน | กำหนดการควบคุมแบบทดแทนและอธิบายวิธีการบรรลุ วัตถุประสงค์ของการควบคุมดั้งเดิมและความเสี่ยงที่เพิ่มขึ้น หากมี | องค์กร *XYZ* จะให้ผู้ใช้ทั้งหมด *login* เข้าไปในเซิฟเวอร์จาก *desktop* โดยใช้คำสั่ง *"SU" (substitute user)* ซึ่งทำให้ผู้ใช้สามารถเข้าถึงบัญชี *"root"* และ ดำเนินการภายใต้บัญชี *"root"* แต่ไม่มีการบันทึกเกิดขึ้นใน *directory* ของ *SU-log* (ประวัติ *SU*) ในกรณีนี้การกระทำของผู้ใชแต่ละคนสามารถถูกติดตามได้ในบัญชี *SU* หากรหัสผ่าน *"root"* ไม่ถูกแบ่งปันระหว่างผู้ใช้ |
| 5. การตรวจสอบการควบคุมแบบทดแทน | กำหนดวิธีการที่การควบคุมแบบทดแทนจะได้รับการตรวจสอบ และทดสอบ | องค์กร *XYZ* แสดงให้ผู้ประเมินเห็นว่าคำสั่ง *SU* ได้รับการจัดการ และกิจกรรมที่ดำเนินการทั้งหมดถูกกระทำโดยผู้ใช้งานคำสั่งซึ่งได้รับการบันทึกเพื่อระบุว่าบุคคลผู้นั้นดำเนินการภายใต้สิทธิ root |
| 6. การบำรุงรักษา | กำหนดกระบวนการและการควบคุมที่ใช้เพื่อบำรุงรักษาการควบคุมแบบทดแทน | องค์กร *XYZdocuments* มีขั้นตอนและกระบวนการเพื่อทำให้มั่นใจว่าการตั้งค่า *SU* ไม่ถูกเปลี่ยนแปลงหรือลบ เพื่อให้ผู้ใช้สามารถใช้คำสั่ง *root* ได้โดยหากไม่มีการระบุตัวตน การติดตาม และการบันทึกประวัติ |

# ภาคผนวก**D:** การแบ่งการเข้าถึงและการสุ่มตัวอย่างของ อาคาร/ส่วนประกอบระบบ