**บันทึกประชุมปิดการตรวจสอบ**

**กองตรวจสอบบริหารการเงินและบัญชี ฝ่ายตรวจสอบกระบวนงานสนับสนุน**

วันที่5 กันยายน 2560

**เรื่อง** การตรวจสอบระบบ SAP (System Application and Products in data processing) System Audi

**วัตถุประสงค์การตรวจสอบ**

* 1. เพื่อให้มั่นใจว่า วงจรรายจ่าย ของการประปานครหลวงนั้น ถูกต้อง ครบถ้วน ทันเวลา กระบวนการจัดซื้อมีการควบคุมการใช้ข้อมูลอย่างถูกต้อง ทันเวลา และผ่านการอนุมัติโดยผู้บริหารหรือผู้มีอำนาจ มีการควบคุมและบริหารวัสดุสำรองคลังอย่างมีประสิทธิภาพ เอกสารที่เกี่ยวข้องถูกบันทึกอย่างถูกต้อง ทันเวลา รวมถึงการบันทึกทางบัญชีที่เกี่ยวข้องกับวัสดุสำรองคลัง การบันทึกบัญชีเจ้าหนี้จากการซื้อสินค้าหรือบริการ การควบคุมดูแลบัญชีเจ้าหนี้ตั้งพัก (GR/IR account) และการป้องกันต่าง ๆ เพื่อให้การบันทึกบัญชีเจ้าหนี้เป็นไปอย่าง ถูกต้อง ครบถ้วน ทันเวลา กระบวนการชำระเงินที่ถูกต้อง ครบถ้วน ทันเวลา ไม่ซ้ำซ้อน หรือ มีการเปลี่ยนแปลง รวมถึงวงจรรายจ่ายที่เกี่ยวเนื่องจากระบบ SAP
  2. เพื่อให้มั่นใจว่า มีการแบ่งแยกหน้าที่รหัสผู้ใช้งานในระบบ SAP (System Application and Products in data processing) อย่างถูกต้องและเหมาะสม
  3. เพื่อให้มั่นใจว่า ระบบการควบคุมภายในด้าน Application Control ที่เกี่ยวข้องกับระบบรายจ่ายของการประปานครหลวง มีความเพียงพอและมีประสิทธิผล

**ขอบเขตการตรวจสอบ** วงจรทางรายจ่าย (SAP Expenditure Process)

**วันเริ่มต้น-สิ้นสุดการตรวจสอบ** 28 เมษายน 2560 – 30 สิงหาคม 2560

**หน่วยรับตรวจ** ฝ่ายพัฒนาและสนับสนุนเทคโนโลยี

กองพัฒนาระบบงานบริหาร

**ผู้รับตรวจ** 1.นางขนิษฐา ผลเจริญ ผอ.ฝพท **ทีมผู้ตรวจสอบ** 1. นางสุชาดา นาคย้อย ผอ.กตง.ฝตน.

2. นายธานินทร์ จตุพฤกษ์ ผอ.กพบ. 2. นางสาวจารุณี รอตเจริญ ผส.7 สตส.

3. นายรัฐธนินท์ ไตรมณีพงศ์ ที่ปรึกษา

**ผลการตรวจสอบ**

1. **กระบวนการจัดซื้อ**

กระบวนการจัดซื้อนั้นเป็นกระบวนการแรกที่เกี่ยวข้องกับค่าใช้จ่ายที่กำลังจะเกิดขึ้น ตามแผนงบประมาณประจำปีที่ได้กำหนดไว้ ซึ่งถือเป็นกระบวนการสำคัญที่จะต้องมีกระบวนการทำงานที่ถูกต้อง ครบถ้วนและทันเวลา โดยได้ทำจากการตรวจสอบการติดตั้ง (Configuration) ในระบบ SAP ของรายการเอกสารต่าง ๆ ที่เกี่ยวข้อง ทั้งเอกสารใบขอซื้อ (Purchase Requisition) และ ใบสั่งซื้อ (Purchase Order) ว่าเป็นไปตามหลักมาตรฐานสากล (SAP Standard) และมีรายการเอกสารคงค้างหรือไม่ รวมถึงการตรวจสอบการใช้ข้อมูลหลักว่ามีการใช้งานอย่างถูกต้อง รวมถึงการเข้าถึงข้อมูลของผู้ใช้งานในส่วนงานต่าง ๆ นั้นมีความเหมาะสมตรงตามหลักเกณฑ์ที่กำหนด ในกระบวนการจัดซื้อในระบบ SAP

จากการตรวจสอบ พบการควบคุมภายในของกระบวนการต่าง ๆ ที่ไม่เหมาะสม ดังนี้

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 2 | การติดตั้งลักษณะการแสดงผลของหน้าจอ (Selection Screen) สำหรับใบสั่งซื้อที่ไม่เหมาะสม |
| Information ข้อเท็จจริง | 1. ไม่มีการกำหนดฟิลด์ สาขา (Plant) ให้เป็นฟิลด์ข้อมูลที่จำเป็น (Required Field) สำหรับหน้าจอการสร้างเอกสารใบสั่งซื้อ (T.Code: ME21N, ME22N, ME23N) ในทุกประเภทเอกสารใบสั่งซื้อ ซึ่งทำให้ผู้ใช้งานสามารถบันทึกเอกสารใบสั่งซื้อได้โดยที่เอกสารใบนั้นยังไม่สมบูรณ์ 2. ตรวจสอบเอกสารใบสั่งซื้อ ที่ถูกสร้างไม่สมบูรณ์ ณ วันที่ 29 สิงหาคม 2560 พบว่ามี 199 รายการ   กระดาษทำการ : WEXP2.02.1 |
| Scales of Justice หลักเกณฑ์ | ฟิลด์สาขา (Plant) ควรจะถูกกำหนดให้เป็นฟิลด์จำเป็น (Required Field) สำหรับการสร้างเอกสารใบสั่งซื้อ |
| DNA สาเหตุ | การกำหนดลักษณะการแสดงผลของหน้าจอมาจากการติดตั้งระบบ SAP หรือมีการเปลี่ยนแปลงจาก SAP version 4.6 |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **ต่ำ**  เอกสารใบสั่งซื้อที่ไม่ถูกต้องจะถูกสร้างเพิ่มขึ้นในระบบโดยไม่ได้รับการแก้ไขและอาจจะเกิดความสับสนในการใช้งาน |
| Tools ข้อเสนอแนะ | 1. จากการประชุมกับฝ่ายจัดซื้อจัดจ้างพบว่าควรมีการปรับปรุงหน้าจอของเอกสารใบสั่งซื้อให้มีการกำหนดฟิลด์ที่จำเป็น เพื่อป้องกันการสร้างเอกสารที่ผิดพลาดหรือไม่สมบูรณ์ 2. ให้ใช้ T.Code 'SPRO' และตามด้วย "SAP Reference IMG เลือก "Materials Management" และไปที่ "Purchasing ไปที่ "Purchase Order" และเลือก "Define Screen Layout at Document Level เมื่อหน้าจอ Change View Screen Layout: Purchase Orders : Overview ปรากฏ ให้ดับเบิ้ลคลิ๊กบนบรรทัดของ Field Selection Keys ตามนี้:   - ME21N (สร้างใบสั่งซื้อ)  - ZPO0 (ใบสั่งซื้อ)  - AKTH (ประเภท Activity การสร้าง)  ดับเบิ้ลคลิ๊กบน Basic Data, Item  กำหนดฟิลด์สาขา (Plant) ให้เป็นฟิลด์จำเป็น (Required Field) ในหน้าจอการแสดงผลของใบสั่งซื้อสินค้า |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 3 | การเข้าถึงข้อมูลและการแบ่งแยกอำนาจหน้าที่ |
| Information ข้อเท็จจริง | 1. ตรวจพบรหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการจัดซื้อ 2. ตรวจสอบรหัสผู้ใช้งานที่สามารถสร้างเอกสารใบสั่งซื้อทุกรหัส จำนวน 43 รหัส สามารถสร้างเอกสารใบขอเสนอซื้อ (Purchase Requisition) และ อนุมัติเอกสารใบสั่งซื้อได้ด้วยตนเอง 3. ตรวจพบรหัสผู้ใช้งานที่ไม่มีการล็อค หลังจากหมดอายุ   กระดาษทำการ : Segregation of Duties |
| Scales of Justice หลักเกณฑ์ | อ้างอิง หลักเกณฑ์จาก สมาคม ISACA เรื่องการแก้ไขปัญหาความขัดแย้งทางหน้าที่ (Segregation of Duties) เรื่องการแบ่งแยกรหัสผู้ใช้งานสำหรับการสร้างเอกสารใบสั่งซื้อและการอนุมัติใบสั่งซื้อ |
| DNA สาเหตุ | 1. รหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN ได้รับ Profile : SAP\_ALL 2. รหัสผู้ใช้งานในแต่ละสาขา ของการประปานครหลวง มีจำนวนจำกัดซึ่งทำให้ต้องมีการใช้งานรหัสผู้ใช้เดียวกันในหลายๆ หน้าที่ |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **สูง**   1. รหัสผู้ใช้งานสามารถถูกนำไปใช้ในทางที่ไม่เหมาะสม และอาจจะนำไปสู่ความเสียหายทางธุรกิจ ชื่อเสียงและภาพลักษณ์ได้ 2. สินค้าหรือบริการที่องค์กรได้รับหรือไม่ได้รับ อาจจะถูกสร้างโดยไม่มีการอนุมัติ หรือ สร้างจากผู้ที่ไม่มีความเกี่ยวข้อง |
| Tools ข้อเสนอแนะ | 1. นำ Profile : SAP\_ALL ออกจากรหัสผู้ใช้งานข้างต้น และสร้าง Role ใหม่ที่เหมาะสมกับหน้าที่ของแต่ละรหัสผู้ใช้งาน 2. ประชุมหารือกับผู้ที่เกี่ยวข้องหรือผู้ที่ดูแลรับผิดชอบในการหาข้อสรุปเพื่อแบ่งแยกหน้าที่ของแต่ละรหัสผู้ใช้งานเพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้น 3. กำหนดขอบเขตของใบสั่งซื้อเช่น มูลค่าของใบสั่งซื้อ ที่สามารถทำการสั่งซื้อได้ เพื่อลดทอนความเสี่ยงที่อาจจะเกิดขึ้น 4. ทำการตรวจสอบการใช้งานของรหัสผู้ใช้งานที่หมดอายุ เช่น Background job ต่าง ๆ ในระบบ หากพบว่าไม่มีการใช้งาน ให้ทำการล็อครหัสผู้ใช้งานเพื่อป้องกันการใช้งานในลักษณะที่ไม่พึงประสงค์ หรือหากพบว่ามีการใช้งานอยู่ให้ทำการเปลี่ยนเป็นรหัสผู้ใช้งานอื่นที่มีส่วนเกี่ยวข้องกับลักษณะงานนั้น ๆ |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**2. กระบวนการจัดการวัสดุสำรองคลัง**

หลังจากได้รับวัสดุหรือบริการตามรายละเอียดที่ถูกกำหนดไว้ในใบสั่งซื้อเรียบร้อยแล้วนั้น ในระบบ SAP จะต้องมีการยืนยันการรับวัสดุหรือบริการภายในระบบ หรือที่เรียกว่าการรับสินค้า (Goods Receipt) โดยเฉพาะวัสดุสำรองคลังนั้นหลังจากที่มีการรับเข้าสู่ระบบเรียบร้อยแล้วนั้น จะต้องมีการควบคุมดูแลวัสดุสำรองคลังให้มีความถูกต้อง ครบถ้วนและทันเวลาอยู่เสมอ ซึ่งโดยกระบวนการทั้งหมดถูกเรียกเป็น กระบวนการจัดการวัสดุสำรองคลัง โดยขอบเขตของโครงการนี้นั้นมุ่งเน้นไปที่กระบวนการบริหารมาตรวัดน้ำซึ่งเป็น ค่าใช้จ่ายที่ส่งผลโดยตรงต่อรายได้หลักของการประปานครหลวง โดยได้มีการตรวจสอบการติดตั้ง (Configuration) ต่าง ๆ ที่ส่งผลต่อการดำเนินรายการมาตรวัดน้ำ เอกสารทางบัญชีและการบันทึกบัญชีที่เกี่ยวข้องกับรายการมาตรวัดน้ำ รายการที่ผิดพลาดหรือไม่ถูกต้องตามหลักเกณฑ์ที่กำหนดไว้ ข้อมูลหลักหรือรหัสวัสดุที่ถูกใช้งานนั้นมีความถูกต้องและซ้ำซ้อนหรือไม่ รวมถึงการเข้าถึงข้อมูลของรหัสผู้ใช้งานต่าง ๆ ได้มีการแบ่งแยกหน้าที่อย่างถูกต้องหรือไม่ ในกระบวนการบริหารจัดการวัสดุสำรองคลังในระบบ SAP จากการตรวจสอบ พบการควบคุมภายในของกระบวนการต่าง ๆ ที่ไม่เหมาะสม ดังนี้

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 5 | บัญชีเจ้าหนี้ตั้งพักคงค้าง (GR/IR Account) |
| Information ข้อเท็จจริง | 1. ตรวจสอบเอกสารใบสั่งซื้อ ณ วันที่ 4 สิงหาคม 2560 รายการคงค้างทางกระบวนการจัดซื้อและกระบวนการทางพัสดุที่ได้ถูกปรับปรุงรายการบัญชีเจ้าหนี้ตั้งพักด้วย Transaction Code : FB1S เรียบร้อยแล้วจำนวน 8 รายการ รวมยอดเงิน 1,587,683.00 บาท   กระดาษทำการ :WEXP5.04.1, WEXP12.02.1, |
| Scales of Justice หลักเกณฑ์ | บัญชีเจ้าหนี้ตั้งพัก (GR/IR Account) ควรจะมีมูลค่ายอดสะสมข้ามปีงบประมาณ หรือควรจะถูกบริหารให้คงเหลือน้อยที่สุดในแต่ละรอบปีงบประมาณ |
| DNA สาเหตุ | 1. พนักงานบัญชีทำการปลดการบันทึกบัญชีอัตโนมัติ (Automatic posting) ใน G/L Account Master ออก และใช้ Transaction Code : FB1S ในการปรับปรุงบัญชีเจ้าหนี้ตั้งพัก (GR/IR Account) แทนการใช้ Transaction Code : MR11 |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **สูง**   1. ส่งผลกระทบต่องบการเงินขององค์กร เนื่องจากถือเป็นรายการบัญชีค่าใช้จ่ายค้างจ่ายชนิดหนึ่ง หากไม่มีการควบคุมดูแลอย่างเหมาะสมจะทำให้เกิดการสะสมและเป็นผลกระทบต่อองค์กรได้ 2. ส่งผลให้เกิดความล่าช้าในกระบวนการจัดซื้อและการบริหารวัสดุสำรองคลัง |
| Tools ข้อเสนอแนะ | 1. สร้าง Role หรือกำหนดสิทธิ์ในการใช้งาน Transaction Code: MR11 เพื่อใช้สำหรับการปรับปรุงรายการบัญชี GR/IR Account แทน T.Code : FB1S 2. ประชุมหารือเพื่อหาผู้ดูและและรับผิดชอบในการตรวจสอบรายการบัญชีเจ้าหนี้ตั้งพักคงค้างในระบบ SAP |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 6 | การกำหนดการบันทึกบัญชีอัตโนมัติ (Automatic Posting) ไม่สอดคล้องกัน |
| Information ข้อเท็จจริง | 1. ตรวจพบ Movement type 951, 952 และ Z51, Z52 ซึ่งเป็น Movement type ที่สร้างขึ้นมาโดยเฉพาะ เพื่อเดินรายการหักล้างระหว่างกัน แต่มีการติดตั้งเงื่อนไขการบันทึกบัญชีไม่สอดคล้องกัน |
| Scales of Justice หลักเกณฑ์ | เนื่องจากเป็น Movement type ที่ถูกกำหนดมาเพื่อให้เดินรายการกลับบัญชีกัน เพราะฉะนั้นการบันทึกบัญชีอัตโนมัติในระบบควรจะต้องมีความสอดคล้องกัน |
| DNA สาเหตุ | การติดตั้งการบันทึกบัญชีอัตโนมัติมีการกำหนดตั้งแต่แรกหรือมีการเปลี่ยนแปลง |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **ปานกลาง**  รายการบัญชีจากการบันทึกเอกสารของ Movement type 951, 952 และ Z51, Z52 จะไม่สอดคล้องกันซึ่งทำให้เกิดความผิดพลาดและไม่ถูกต้องตามหลักเกณฑ์ที่กำหนด |
| Tools ข้อเสนอแนะ | 1. ให้ใช้ T.Code 'SPRO' และตามด้วย "SAP Reference IMG   เลือก "Materials Management" และไปที่ "Inventory Management and Physical Inventory ไปที่ "Movement types" และเลือก "Copy, Change Movement type”  เมื่อหน้าจอ Field Selection : ปรากฏ ให้เลือก Movement type ตามนี้:  และทำการแก้ไข Account Modification ของ ระหว่าง Movement type 951, 952 และMovement type Z51 และ Z52 ให้สอดคล้องกัน |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 7 | การบันทึกรายการวัสดุสำรองคลังที่ผิดปกติหรือไม่ถูกต้อง |
| Information ข้อเท็จจริง | ตรวจสอบพบรายการที่ผิดปกติหรือไม่ถูกต้อง ณ วันที่ 6 สิงหาคม 2560 โดยเลือกเฉพาะรายการที่เกี่ยวข้องกับมาตรวัดน้ำ ของทุกฝ่ายและสาขาในการประปานครหลวง พบว่า  1. รายการที่บันทึกรหัสยี่ห้อ ของมาตรวัดน้ำไม่ถูกต้อง หรือถูกยกเลิกด้วย Movement type ที่ไม่ใช่คู่ที่หักล้างกันจำนวน 6 รายการ  2. รายการตัดมาตรวัดน้ำเพื่อติดตั้งใหม่ ด้วย Movement Type 913,914 โดยอ้างอิงคู่มือปฏิบัติงานการบันทึกเลขที่ใบสั่งงานภายใน (Internal Order) จากกองบัญชีต้นทุน ฝ่ายบัญชี ณ มกราคม 2553 ควรจะต้องบันทึกโดยอ้างอิงเลขที่ใบสั่งงานภายใน (Internal Order) ซึ่งตรวจพบ 14,499 รายการ จากทั้งหมด 144,689 รายการ คิดเป็น 10% ของรายการทั้งหมด  3. รายการตัดมาตรวัดน้ำเพื่อติดตั้งใหม่ ด้วย Movement Type 959,960 โดยอ้างอิงคู่มือปฏิบัติงานการบันทึกเลขที่ใบสั่งงานภายใน (Internal Order) จากกองบัญชีต้นทุน ฝ่ายบัญชี ณ มกราคม 2553 ควรจะต้องบันทึกโดยอ้างอิงเลขที่ใบสั่งงานภายใน (Internal Order) ซึ่งตรวจพบ 2,376 จากทั้งหมด 7,338 คิดเป็น 32% ของรายการทั้งหมด  4. รายการตัดมาตรวัดน้ำครบวาระ ด้วย Movement Type 961 ซึ่งเป็นการตัดมาตรวัดน้ำเพื่อ เปลี่ยนลดขนาด จำนวน 6 รายการ ซึ่งผิดประเภทการใช้งาน  5. รายการตัดมาตรวัดน้ำด้วย Movement type 201 ซึ่งเป็นการเบิกงบทำการ จำนวน 400 ตัว มูลค่า 276,400 บาท อ้างอิง Material Document No. 3000092005 ปี 2557 |
| Scales of Justice หลักเกณฑ์ | การบันทึกรายการวัสดุสำรองคลังควรจะถูกกระทำด้วยหลักเกณฑ์เดียวกันทั้งองค์กร |
| DNA สาเหตุ | การขาดการควบคุมที่ดีในระบบเพื่อป้องกันการบันทึกรายการที่ไม่ถูกต้อง |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **ปานกลาง**   1. ส่งผลกระทบต่อการควบคุมยอดหรือมูลค่าการใช้วัสดุสำรองคลังอย่างถูกต้อง 2. รายการที่ผิดพลาดของวัสดุสำรองคลังในรายการทางบัญชี 3. การบันทึกรายการวัสดุสำรองคลังที่ไม่ถูกอนุมัติตามกระบวนการเนื่องจากไม่ผ่านเอกสารอ้างอิง |
| Tools ข้อเสนอแนะ | 1. ตรวจสอบหาสาเหตุของรายการที่ผิดพลาดและทำการอบรมพนักงานเพื่อทำความเข้าใจการใช้งานในแต่ละ Movement type 2. ขัดการอบรมเพื่อเพิ่มความเข้าใจในการใช้ Movement type หรือประเภทการเบิก รวมถึงเอกสารอ้างอิงให้ถูกต้อง |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 8 | การเข้าถึงข้อมูลและการแบ่งแยกอำนาจหน้าที่ |
| Information ข้อเท็จจริง | 1. ตรวจพบรหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการจัดการวัสดุสำรองคลัง 2. ตรวจพบรหัสผู้ใช้งานจำนวน 22 รหัส สามารถดำเนินการรับสินค้าโดยไม่อ้างอิงเอกสารอื่น ๆ ด้วย Movement type ซึ่งขึ้นต้นด้วย 5 ( Movement type : 5XX) 3. ตรวจพบรหัสผู้ใช้งานจำนวน 16 รหัส สร้างใบขอเสนอซื้อ สร้างใบสั่งซื้อ อนุมัติใบสั่งซื้อ และสามารถดำเนินการรับ เบิก โอน วัสดุได้ด้วยตนเอง 4. ตรวจพบรหัสผู้ใช้งานจำนวน 10 รหัส สามารถดำเนินการรับ เบิก โอน วัสดุ และปรับสต็อคได้ด้วยตนเอง 5. ตรวจพบรหัสผู้ใช้งาน 7 รหัส ที่สามารถ สร้างรหัสพัสดุ คน สร้างใบขอเสนอซื้อ สร้างใบสั่งซื้อ อนุมัติใบสั่งซื้อ และสามารถดำเนินการรับ เบิก โอน วัสดุได้ด้วยตนเอง   กระดาษทำการ: Segregation of Duties |
| Scales of Justice หลักเกณฑ์ | อ้างอิง หลักเกณฑ์จาก สมาคม ISACA เรื่องการแก้ไขปัญหาความขัดแย้งทางหน้าที่ (Segregation of Duties) เรื่องการแบ่งแยกรหัสผู้ใช้งานสำหรับการสร้างเอกสารใบสั่งซื้อและการรับเบิกวัสดุ และ รหัสผู้ใช้งานที่สามารถทำการรับ เบิก โอนวัสดุ และ ปรับสต็อคได้ด้วยตนเอง |
| DNA สาเหตุ | 1. รหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN ได้รับ Profile : SAP\_ALL 2. รหัสผู้ใช้งานแต่ละสาขามีจำนวนจำกัดซึ่งทำให้ต้องมีการใช้งานกันในหลายๆ หน้าที่ 3. ตรวจพบรหัสผู้ใช้งานที่ไม่มีการล็อค หลังจากหมดอายุ |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **สูง**   1. รหัสผู้ใช้งานสามารถถูกนำไปใช้ในทางที่ไม่เหมาะสม และอาจจะนำไปสู่ความเสียหายทางธุรกิจ ชื่อเสียงและภาพลักษณ์ได้ 2. วัสดุสำรองคลังสูญเสีย หรือ สูญหาย ซึ่งทำให้เกิดความเสียหายต่อองค์กร ภาพลักษณ์ หรือชื่อเสียงได้ |
| Tools ข้อเสนอแนะ | 1. แก้ไข Role ที่มีสิทธิ์สร้างเอกสารโดยใช้ Movement type 5\* โดยการกำหนด Movement type เฉพาะที่ การประปานครหลวงใช้เท่านั้น 2. ประชุมหารือกับผู้ที่เกี่ยวข้องหรือผู้ที่ดูแลรับผิดชอบในการหาข้อสรุปเพื่อแบ่งแยกหน้าที่ของแต่ละรหัสผู้ใช้งานเพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้น 3. นำ Profile : SAP\_ALL ออกจากรหัสผู้ใช้งานข้างต้น และสร้าง Role ใหม่ที่เหมาะสมกับหน้าที่ของแต่ละรหัสผู้ใช้งาน 4. กำหนดขอบเขตของหน้าที่ในแต่ละรหัสผู้ใช้หรือมีกระบวนการควบคุมภายนอกเพื่อลดทอนความเสี่ยง 5. ทำการตรวจสอบการใช้งานของรหัสผู้ใช้งานที่หมดอายุ เช่น Background job ต่าง ๆ ในระบบ หากพบว่าไม่มีการใช้งาน ให้ทำการล็อครหัสผู้ใช้งานเพื่อป้องกันการใช้งานในลักษณะที่ไม่พึงประสงค์ หรือหากพบว่ามีการใช้งานอยู่ให้ทำการเปลี่ยนเป็นรหัสผู้ใช้งานอื่นที่มีส่วนเกี่ยวข้องกับลักษณะงานนั้น ๆ |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

1. **กระบวนการตั้งเจ้าหนี้**

เป็นกระบวนการรับใบแจ้งหนี้จากผู้ขายหลังจากที่ได้รับวัสดุสำรองคลังหรือบริการต่าง ๆ ตามรายละเอียดของการจ้างเสร็จสิ้นเรียบร้อย ซึ่งในระบบจะถูกเรียกว่ากระบวนการตั้งเจ้าหนี้ (Invoice Receipt) โดยที่ระบบจะนำจำนวนหรือมูลค่าใบสั่งซื้อ เปรียบเทียบกับจำนวนหรือมูลค่าที่รับวัสดุสำรองคลังหรือบริการ แล้วเปรียบเทียบกับจำนวนหรือมูลค่าที่กำลังจะดำเนินการตั้งเจ้าหนี้ โดยเป็นกระบวนเปรียบเทียบ 3 ทาง (3-Ways Matching) ซึ่งสามารถกำหนดเงื่อนไขต่าง ๆ เพื่อเป็นการป้องกันใบแจ้งหนี้ที่มากกว่าข้อกำหนดความแตกต่าง (Tolerance limit) ไม่ให้ถูกนำไปสู่กระบวนการจ่ายเงินหากมีความไม่ถูกต้องหรือครบถ้วน โดยได้ทำการตรวจสอบการติดตั้ง (Configuration) ต่าง ๆ ในระบบ รวมทั้งรายการเอกสาร และข้อมูลหลักที่เกี่ยวข้อง รวมถึงการเข้าถึงข้อมูลและการแบ่งแยกหน้าที่ของรหัสผู้ใช้งานที่เกี่ยวข้องกับกระบวนการตั้งเจ้าหนี้ ในระบบ SAP

จากการตรวจสอบ พบการควบคุมภายในของกระบวนการต่าง ๆ ที่ไม่เหมาะสม ดังนี้

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 10 | รหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการตั้งเจ้าหนี้ |
| Information ข้อเท็จจริง | 1. ตรวจพบรหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการเจ้าหนี้ 2. ตรวจพบรหัสผู้ใช้งาน จำนวน 27 คน ที่สามารถเปิดใบสั่งซื้อ อนุมัติใบสั่งซื้อ และตั้งหนี้เจ้าหนี้ได้ ด้วยตนเอง 3. ตรวจพบรหัสผู้ใช้งาน จำนวน 8 คน ที่สามารถเปิดใบสั่งซื้อ อนุมัติใบสั่งซื้อ รับ เบิก โอน วัสดุ และตั้งหนี้เจ้าหนี้ได้ ด้วยตนเอง   กระดาษทำการ: Segregation of Duties |
| Scales of Justice หลักเกณฑ์ | อ้างอิง หลักเกณฑ์จาก สมาคม ISACA เรื่องการแก้ไขปัญหาความขัดแย้งทางหน้าที่ (Segregation of Duties) เรื่องการแบ่งแยกรหัสผู้ใช้งานสำหรับการสร้างเอกสารใบสั่งซื้อและการรับเบิกวัสดุ และการตั้งเจ้าหนี้ |
| DNA สาเหตุ | 1. รหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN ได้รับ Profile : SAP\_ALL 2. รหัสผู้ใช้งานแต่ละสาขามีจำนวนจำกัดซึ่งทำให้ต้องมีการใช้งานกันในหลายๆ หน้าที่ 3. ตรวจพบรหัสผู้ใช้งานที่ไม่มีการล็อค หลังจากหมดอายุ |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **สูง**   1. รหัสผู้ใช้งานสามารถถูกนำไปใช้ในทางที่ไม่เหมาะสม และอาจจะนำไปสู่ความเสียหายทางธุรกิจ ชื่อเสียงและภาพลักษณ์ได้ 2. บัญชีเจ้าหนี้เกิดความไม่ถูกต้อง เกิดหนี้ที่ไม่สอดคล้องกับสินค้าหรือบริการที่ได้รับ |
| Tools ข้อเสนอแนะ | 1. นำ Profile : SAP\_ALL ออกจากรหัสผู้ใช้งานข้างต้น และสร้าง Role ใหม่ที่เหมาะสมกับหน้าที่ของแต่ละรหัสผู้ใช้งาน 2. ประชุมหารือกับผู้ที่เกี่ยวข้องหรือผู้ที่ดูแลรับผิดชอบในการหาข้อสรุปเพื่อแบ่งแยกหน้าที่ของแต่ละรหัสผู้ใช้งานเพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้น 3. กำหนดขอบเขตของหน้าที่ในแต่ละรหัสผู้ใช้หรือมีกระบวนการควบคุมภายนอกเพื่อลดทอนความเสี่ยง 4. ทำการตรวจสอบการใช้งานของรหัสผู้ใช้งานที่หมดอายุ เช่น Background job ต่าง ๆ ในระบบ หากพบว่าไม่มีการใช้งาน ให้ทำการล็อครหัสผู้ใช้งานเพื่อป้องกันการใช้งานในลักษณะที่ไม่พึงประสงค์ หรือหากพบว่ามีการใช้งานอยู่ให้ทำการเปลี่ยนเป็นรหัสผู้ใช้งานอื่นที่มีส่วนเกี่ยวข้องกับลักษณะงานนั้น ๆ |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**4. กระบวนการจ่ายเงิน**

กระบวนการจ่ายเงินเป็นกระบวนการสุดท้ายในส่วนของ วงจรรายจ่าย (Expenditure Process) ซึ่งหลังจากที่ได้รับวัสดุสำรองคลังหรือบริการต่าง ๆ จากผู้ขายและได้ดำเนินการตั้งเจ้าหนี้เมื่อได้รับเอกสารใบแจ้งหนี้ จากนั้นเมื่อถึงกำหนดเงื่อนไขการขำระเงิน จะต้องดำเนินการจ่ายเงินให้กับผู้ขายตามรายละเอียดงานที่ถูกกำหนดไว้ ซึ่งได้ทำการตรวจสอบการติดตั้ง (Configuration) ที่อาจจะมีความเสี่ยงในการจ่ายเงินให้กับเจ้าหนี้รายอื่น ๆ หรือมีการเปลี่ยนแปลงรายการ หรือรายละเอียดข้อมูลหลักเจ้าหนี้ เพื่อป้องกันการชำระเงินที่ซ้ำซ้อนหรือไม่ถูกต้องที่อาจจะเกิดขึ้นได้ รวมถึงการเข้าถึงข้อมูลและการแบ่งแยกหน้าของรหัสผู้ใช้งานที่เกี่ยวข้องกับกระบวนการจ่ายเงิน ในระบบ SAP จากการตรวจสอบ พบการควบคุมภายในของกระบวนการต่าง ๆ ที่ไม่เหมาะสม ดังนี้

|  |  |
| --- | --- |
| Unlock ประเด็นที่ 11 | ตรวจพบรหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการจ่ายเงิน |
| Information ข้อเท็จจริง | 1. ตรวจพบรหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN สามารถเข้าถึงและดำเนินการได้ทุกส่วนงานของกระบวนการจ่ายเงิน 2. ตรวจสอบพบรหัสผู้ใช้งานจำนวน 11 รายสามารถ ตั้งหนี้เจ้าหนี้และทำจ่ายได้ ด้วยตนเอง 3. ตรวจสอบพบรหัสผู้ใช้งานจำนวน 9 รายสามารถ สามารถแก้ไขข้อมูลหลักเจ้าหนี้ ทำจ่ายได้ ด้วยตนเอง 4. ตรวจสอบพบรหัสผู้ใช้งานจำนวน 9 รายสามารถ สามารถแก้ไขข้อมูลหลักเจ้าหนี้ ทำตั้งหนี้ และทำรายการจ่ายได้ ด้วยตนเอง   กระดาษทำการ : Segregation of Duties |
| Scales of Justice หลักเกณฑ์ | รหัสผู้ใช้งานควรถูกกำหนดให้มีการแบ่งแยกหน้าที่อย่างเหมาะสม |
| DNA สาเหตุ | รหัสผู้ใช้งาน ALEREMOTE, BASIS, DDIC และ SOLMAN\_ADMIN ได้รับ Profile : SAP\_ALL |
| High Voltage ผลกระทบและ  ความเสี่ยง | ระดับความเสี่ยง : **สูง**   1. รหัสผู้ใช้งานสามารถถูกนำไปใช้ในทางที่ไม่เหมาะสม และอาจจะนำไปสู่ความเสียหายทางธุรกิจ ชื่อเสียงและภาพลักษณ์ได้ 2. อาจจะเกิดการเปลี่ยนแปลงข้อมูลการจ่ายเงินโดยแก้ไขข้อมูลหลักเจ้าหนี้เพื่อประโยชน์ส่วนตน |
| Tools ข้อเสนอแนะ | 1. นำ Profile : SAP\_ALL ออกจากรหัสผู้ใช้งานข้างต้น และสร้าง Role ใหม่ที่เหมาะสมกับหน้าที่ของแต่ละรหัสผู้ใช้งาน 2. ประชุมหารือกับผู้ที่เกี่ยวข้องหรือผู้ที่ดูแลรับผิดชอบในการหาข้อสรุปเพื่อแบ่งแยกหน้าที่ของแต่ละรหัสผู้ใช้งานเพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้น 3. กำหนดขอบเขตของหน้าที่ในแต่ละรหัสผู้ใช้หรือมีกระบวนการควบคุมภายนอกเพื่อลดทอนความเสี่ยง 4. ทำการตรวจสอบการใช้งานของรหัสผู้ใช้งานที่หมดอายุ เช่น Background job ต่าง ๆ ในระบบ หากพบว่าไม่มีการใช้งาน ให้ทำการล็อครหัสผู้ใช้งานเพื่อป้องกันการใช้งานในลักษณะที่ไม่พึงประสงค์ หรือหากพบว่ามีการใช้งานอยู่ให้ทำการเปลี่ยนเป็นรหัสผู้ใช้งานอื่นที่มีส่วนเกี่ยวข้องกับลักษณะงานนั้น ๆ |

**ความเห็นของผู้รับตรวจ…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

**ความเห็นเพิ่มเติม…………….…...........................…………………...........……………….……………………..………**

**………….………………………………………………………………………………………….....................................................**

ลงชื่อ **...........................................**ผอ.กอง/ฝ่าย ลงชื่อ……………………………………………..ผู้รับตรวจ

**(**นางสุชาดา นาคย้อย**) (**นายธานินทร์ จตุพฤกษ์**)**

ตำแหน่งผู้อำนายการกองตรวจสอบบริหารการเงินและบัญชี ตำแหน่งผู้อำนายการกองพัฒนาระบบงานบริหาร