ความเสี่ยงและผลกระทบต่อผู้สอบบัญชีเมื่อบริษัทใช้งาน Robotic Process Automation RPA

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

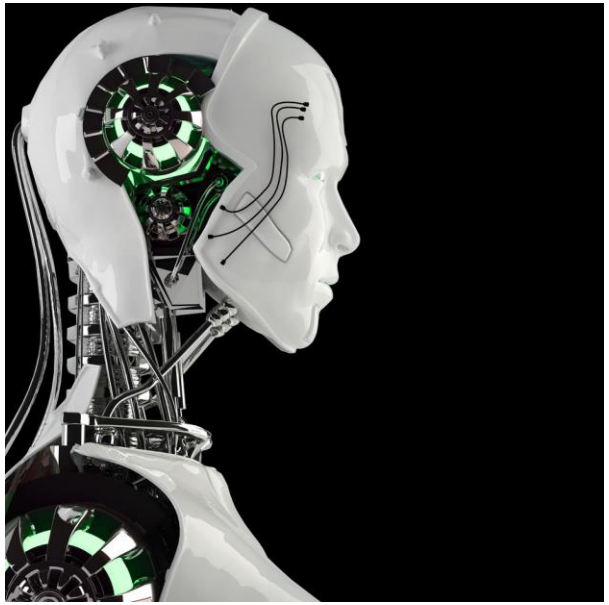
หัวข้อ

- อะไรคือ RPA
- ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน RPA
- ประเภทของ RPA
- ตัวอย่าง RPA Risk and Controls

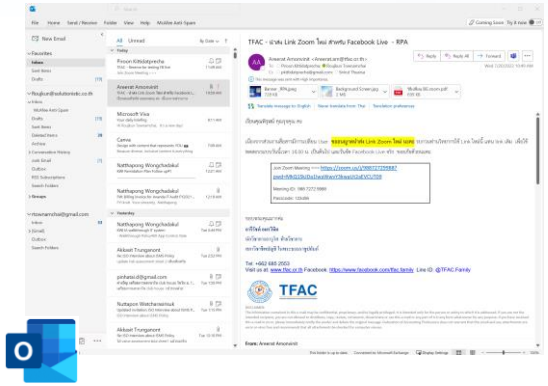
อะไรคือ RPA

- สามารถลอกเลียนแบบ (Mimic) การใช้งานของผู้ใช้งาน
- สามารถ Automation หลายระบบงาน
- เป็น โปรแกรม Computer coded software

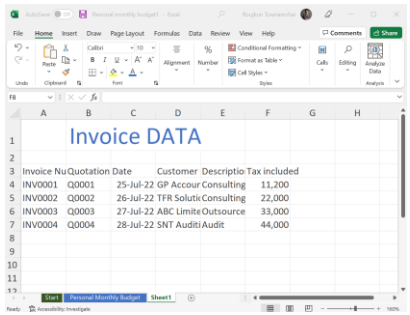
- ไม่ใช่ หุ่นยนต์ (Physically)
- ไม่ใช่ AI หรือ Voice recognition



ตัวอย่างการใช้งาน RPA

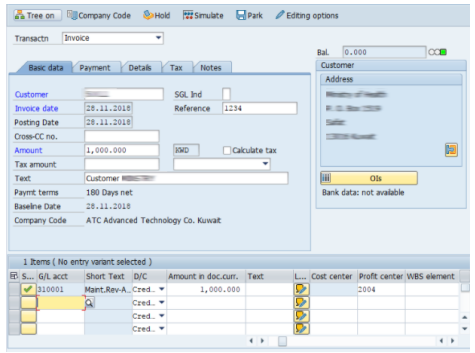


1. Bot อ่านอีเมล์แล้ว Save file PDF (Invoice) ออกมาทั้งหมด



2. Bot อ่าน PDF (Invoice) ไฟล์แล้ว นำมาจัดในรูปแบบ Excel

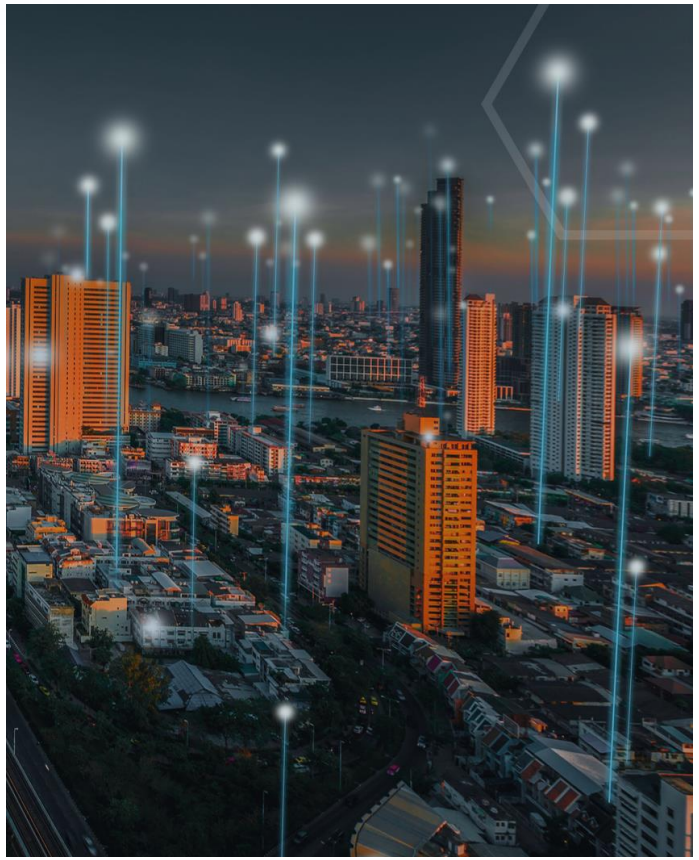
3. Bot การ login เข้าสู่ระบบงาน (ERP)



4. Bot อ่านข้อมูลบน Excel file แล้ว นำมากรอกบนหน้าจอระบบงาน ERP จนเสร็จสิ้น

ข้อดีของการใช้งาน RPA

- ทำงานรูปแบบอัตโนมัติ รวดเร็ว และ แม่นยำ
- การพัฒนา Automation ไม่กระทบกับระบบงาน
- ลดความผิดพลาด (Human Error)
- ลดค่าใช้จ่าย



RPA เหมาะกับงานจำนวนมากที่มีรูปแบบตรรกะที่ชัดเจน

ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน RPA

- การใช้งาน RPA อาจมีความเสี่ยงที่มีผลกระทบต่อ งบการเงิน

ผู้สอบบัญชีควร:

- ทำความเข้าใจว่าบริษัทนำ RPA ไปใช้ที่กระบวนการใด และ ใช้อย่างไร
- ทำความเข้าใจผลกระทบของการใช้งาน RPA ดังต่อไปนี้
  - ผลกระทบต่อ Application Control - มีการตัด หรือ ละเลย Application control หรือไม่
  - ผลกระทบต่อ Manual Control - บางควบคุมอาจหายไป เช่น Maker Checker
  - ผลกระทบต่อ General IT control - การใช้งานอาจส่งผลกระทบต่อกระบวนการการควบคุมทั่วไปเทคโนโลยีสารสนเทศ

ประเภทของ RPA

ประเภทของ RPA

Attended

- Bot สั่งการโดยผู้ใช้งานเอง
- ผู้ใช้งานสังเกตการณ์การทำงานของ Bot แบบ Realtime
- ผู้ใช้งานใช้ Username และ Password ของตนเอง

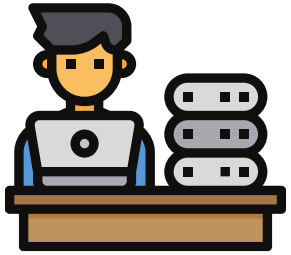
Unattended

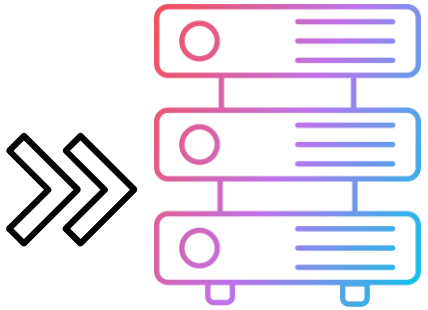
- Bot สั่งการโดย bot controller (IT Operator etc.)
- ผู้ใช้งานสอบทานความถูกต้องของการทำงานหลัง Bot ดำเนินการแล้วเสร็จ
- Username และ Password ของผู้ใช้งาน(เจ้าของ) ถูกบริหารและจัดเก็บโดย bot controller

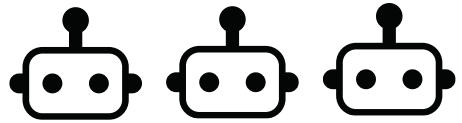
Unattended RPA – ภาพรวมที่ 1

Bot จะถูก Run โดย

Bot Controller





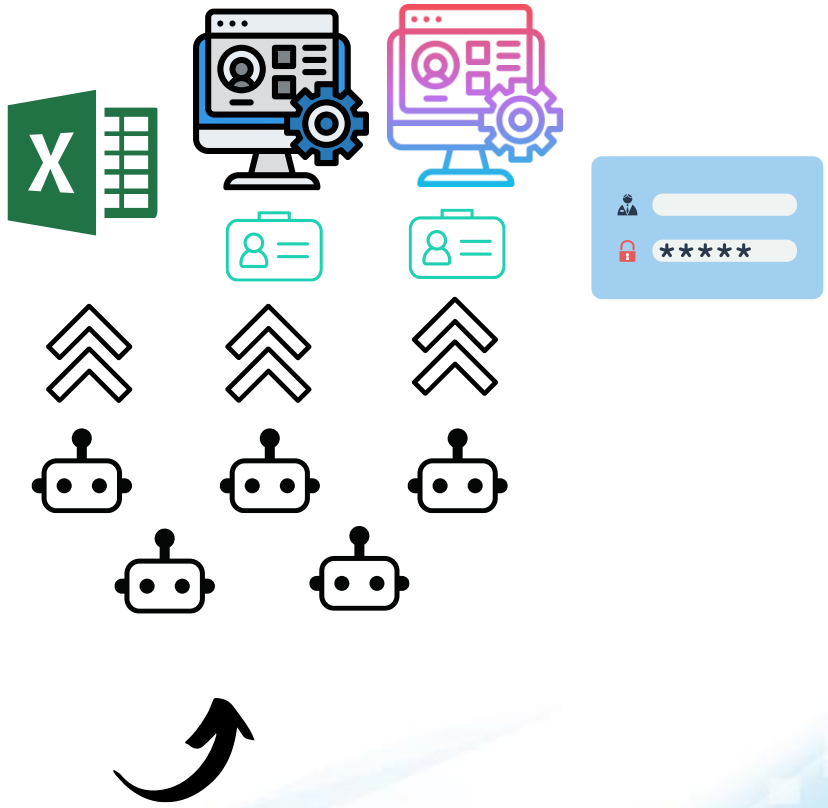


bot controller สามารถ run bot หลายตัวพร้อมกัน

bot จะดำเนินการแบบอัตโนมัติ ตาม Scenario ที่ได้กำหนดไว้ (อาจจัดเก็บในรูปแบบ File หรือ โปรแกรม)

Unattended RPA – ภาพรวมที่ 2

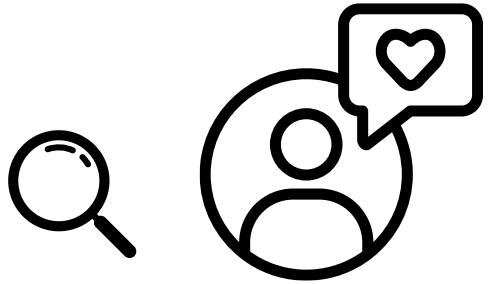
Bot สามารถทำงานเสมือนมนุษย์ โดยสามารถทำงานร่วมกับหลายระบบงานและไฟล์ จึงมีความจำเป็นต้องใช้ User ID และ Password ของผู้ใช้งานในการ Login เข้าระบบงาน



การจัดเก็บ User ID และ Password อาจจัดเก็บในรูปแบบ File หรือ ฐานข้อมูล

File ที่จัดเก็บ User Credential

Unattended RPA – ภาพรวมที่ 3



ผู้ใช้งานระบบ (เจ้าของ) สามารถสอบทานการดำเนินงานผ่านระบบงาน

Bot controller สอบทาน Log file เพื่อติดตามการดำเนินงานของ bot

เมื่อ bot ทำงานเสร็จแล้ว RPA จะทำการบันทึกการทำงานของ bot ในรูปแบบ Log file

นิยาม

- Bot หรือ บอท – คือโปรแกรม RPA ที่ทำหน้าที่ลอกเลียนการทำงานของมนุษย์
- Bot user ID หรือ รหัสผู้ใช้งานที่ใช้โดยบอท – คือ ผู้ใช้งาน (ระบบงาน) ที่สร้างขึ้นมาเพื่อให้บอทสามารถนำไปใช้ในการทำงานบนระบบงาน
- User ID หรือ รหัสผู้ใช้งาน – คือ รหัสผู้ใช้งานที่ใช้โดยผู้ใช้งานระบบ (User) หรือเจ้าของ (Owner)

ตัวอย่างความเสี่ยงและการควบคุม RPA

ตัวอย่างความเสี่ยงด้าน RPA

1. การบริหารจัดการความเสี่ยงและกำกับดูแล RPA (Risk and Governance)
2. การเข้าถึงและสิทธิการใช้งาน RPA (Authentication of bots)
3. การติดตามการดำเนินงานของ Bot (Bot monitoring)
4. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

1. การบริหารจัดการความเสี่ยงและกำกับดูแล RPA (Risk and Governance)

ความเสี่ยง	การควบคุม
การใช้งาน RPA ไม่สอดคล้องกับนโยบายบริษัทฯ	จัดทำ RPA Policy โดยมีรายละเอียดและหัวข้อดังต่อไปนี้เป็นอย่างน้อย 1. แนวทางการใช้งาน RPA 2. การประเมินความเสี่ยง RPA 3. หน้าที่รับผิดชอบ 4. แนวทางการจัดทำ RPA Inventory list 5. RPA Naming Convention 6. การควบคุมการเข้าถึง RPA 7. การควบคุมการเปลี่ยนแปลง RPA 8. การสอบทาน RPA (RPA monitoring)

1. การบริหารจัดการความเสี่ยงและกำกับดูแล RPA (Risk and Governance) - ต่อ

ความเสี่ยง	การควบคุม
รหัสผู้ใช้งานที่ใช้งานโดย bot ไม่มีเจ้าของ (Ownerless) ทำให้อาจเป็นเป้าหมายของผู้ไม่ได้รับอนุญาตสามารถเข้าถึงระบบงานและดำเนินการแก้ไขข้อมูลด้านธุรกิจ หรืองบการเงิน	จัดทำทะเบียน RPA inventory list และปรับปรุงให้เป็นปัจจุบัน จัดทำเอกสารระเบียบปฏิบัติการใช้งานการบันทึก RPA Inventory list
ปัญหาหรือแนวทางการปฏิบัติการใช้งาน RPA ไม่ได้รับการสนับสนุนจากผู้บริหาร หรือ ไม่มีการกำกับดูแลอย่างเหมาะสม	จัดตั้ง RPA Committee เพื่อสนับสนุนการดำเนินงานของ RPA โดยคณะทำงานควรมีหน้าที่หลักในการให้แนวทาง ข้อเสนอแนะ และอนุมัติ การใช้งานด้าน RPA

2. การเข้าถึงและสิทธิการใช้งาน RPA (Authentication of bots)

ความเสี่ยง	การควบคุม
มีการให้สิทธิสูงแก่รหัสผู้ใช้งานที่นำไปใช้งานโดยบอท ทำให้อาจมีความเสี่ยงในการเข้าถึงระบบงานพร้อมสิทธิสูง ซึ่งอาจมีสามารถในการยกเว้นการควบคุมที่สำคัญได้ หรืออาจทำการแก้ไขข้อมูล ด้านงบการเงิน โดยไม่ได้รับอนุญาต	ควรจัดทำนโยบายให้มีการจำกัดสิทธิการใช้งานสิทธิสูงสำหรับ bot รวมถึงควรมีการควบคุมด้านความปลอดภัยให้สอดคล้องตามนโยบายของบริษัท เช่น รหัสผ่าน สิทธิการเข้าถึงระบบ การบริหารจัดการผู้ใช้งาน เป็นต้น

RPA ได้รับสิทธิสูง สามารถทำรายการทั้ง Maker และ Approver ได้

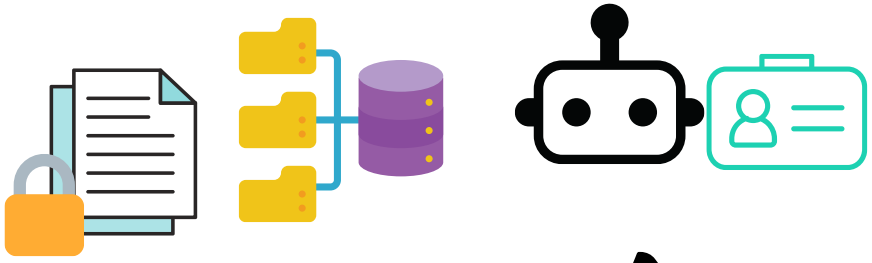
Maker

Approver

2. การเข้าถึงและสิทธิการใช้งาน RPA (Authentication of bots) – (ต่อ)

ความเสี่ยง	การควบคุม
มีการเข้าถึง File ที่สำคัญของ RPA เช่น File ที่จัดเก็บข้อมูล Username Password ของเจ้าของผู้ใช้งาน หรือ File สำคัญที่ใช้ในการทำงานของ RPA ซึ่งอาจทำให้กระบวนการทำงานของ RPA ไม่ถูกต้อง หรือ ทำให้งบการเงินผิดพลาด	ควรจำกัดการเข้าถึง File ที่สำคัญของ RPA

หากไม่มีการเข้ารหัส File User credential username และ password อาจรั่วไหลไปยังผู้ไม่เหมาะสม



User Credential

File สำคัญที่ RPA ใช้ในการดำเนินงาน

2. การเข้าถึงและสิทธิการใช้งาน RPA (Authentication of bots) – (ต่อ)

ความเสี่ยง	การควบคุม
กระบวนการบริหารจัดการผู้ใช้งานไม่มีการปรับปรุงให้ครอบคลุมกรณีใช้งาน RPA ทำให้มีความเสี่ยงด้านการเข้าถึงระบบงานเพิ่มเติม	ควรมีกระบวนการบริหารจัดการผู้ใช้งานที่เหมาะสมและครอบคลุมถึงรหัสผู้ใช้งานที่ใช้โดย bot (RPA)

ข้อควรระวัง:

- เจ้าหน้าที่บางคนอาจมีผู้ใช้งานเกิน 1 บัญชี (Multiuser ID) ซึ่งอาจไม่สอดคล้องต่อนโยบายด้านความมั่นคงปลอดภัยของบริษัท
- รหัสผ่านของรหัสผู้ใช้งานที่ใช้โดยบอท ควรได้รับการควบคุมอย่างเหมาะสม e.g. password age
- ไม่ควรแชร์ User account / password
- กระบวนการสอบทานสิทธิผู้ใช้งานควรครอบคลุมถึงผู้ใช้งาน RPA
- ควรปรับปรุงกระบวนการระงับสิทธิการใช้งาน e.g. กรณีพนักงานที่มีผู้ใช้งาน RPA ลาออก

3. การติดตามการดำเนินงานของ Bot (Bot monitoring)

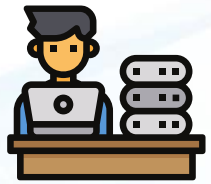
ความเสี่ยง	การควบคุม
การทำงานของ bot ผิดพลาดส่งผลต่อความผิดพลาดต่องบการเงิน	ควรมีการติดตามการทำงานของ bot หากพบเหตุการณ์ หาก bot ทำงานผิดพลาดหรือไม่ครบถ้วน ควรดำเนินการแก้ไข ควรจัดทำคู่มือการปฏิบัติงานกรณีฉุกเฉินเช่น bot ไม่สามารถใช้งานได้

ข้อควรระวัง:

- หากระบบงานมีการแก้ไข bot อาจไม่สามารถทำงานได้อย่างถูกต้อง
- การเขียน logic ของ bot ให้ครอบคลุมทุกกรณีข้อผิดพลาด อาจทำได้ยาก
- Log ที่บันทึกการทำงานของ bot อาจมีข้อมูลที่อ่อนไหว เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน เป็นต้น ควรได้รับการจำกัดสิทธิการเข้าถึง log ดังกล่าว

Log บันทึกการทำงานของ bot

Bot controller ทำหน้าที่ในการสอบทานการทำงานของ bot

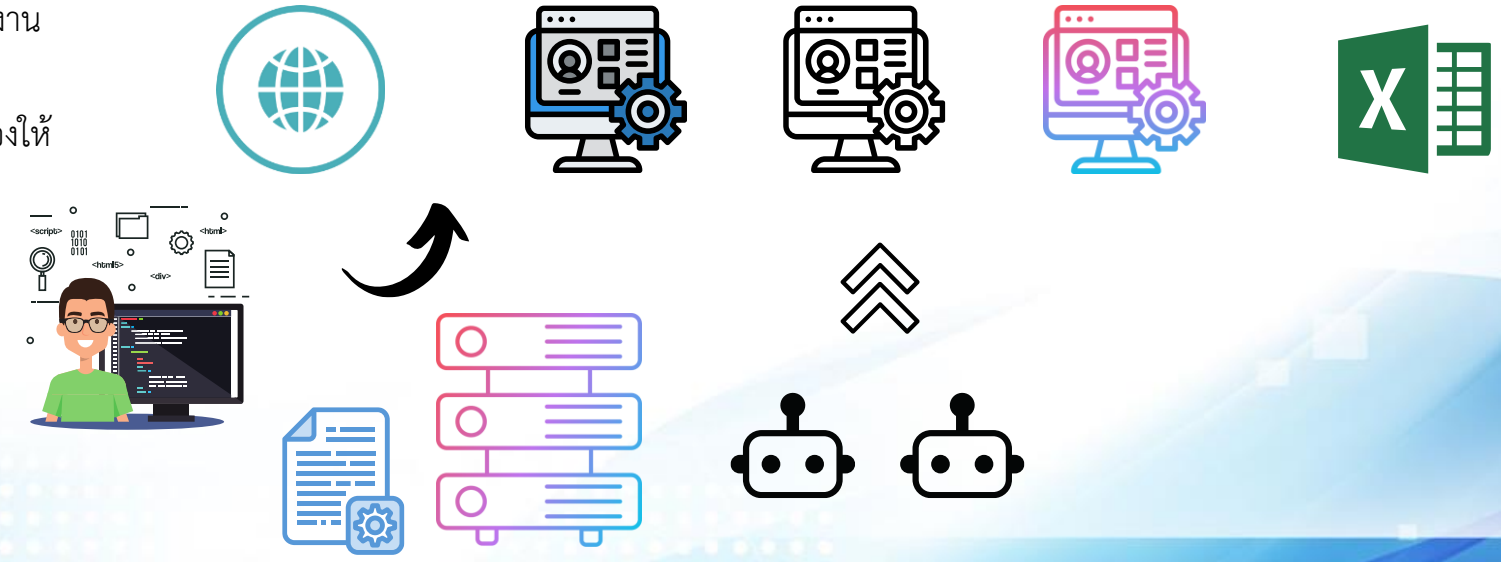


4. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

ความเสี่ยง	การควบคุม
มีการให้สิทธิการเข้าถึงระบบงาน (Production) แก่ผู้พัฒนาระบบ RPA (bot programmer) ทำให้อาจมีความเสี่ยงด้านการเข้าถึงระบบงานที่สำคัญโดยผู้ที่ไม่เหมาะสม	การพัฒนา หรือ เปลี่ยนแปลง RPA ควรดำเนินตามนโยบายการพัฒนาระบบ และ การเปลี่ยนแปลงระบบ ของบริษัท

ข้อควรระวัง:

- เนื่องจากการพัฒนา Automation ระบบงาน RPA มีทำงานกับหลายๆระบบทำให้อาจไม่สามารถพัฒนา bot บนระบบงานทดสอบ (test environment) ได้ จึงจำเป็นต้องให้สิทธิการเข้าถึงระบบงานใช้จริงแก่ผู้พัฒนา bot



บทสรุป

บทสรุป

- เมื่อบริษัทนำ RPA มาใช้งาน ผู้สอบควรทำความเข้าใจการใช้งานของ RPAดังต่อไปนี้
  - ประเภทของ RPA
  - ผลกระทบของ RPA ต่อ Application Control, Manual Control และ IT General Control
- หากมีการใช้ RPA ควรคำนึงถึงความเสี่ยง 4 ด้านดังต่อไปนี้
  1. การบริหารจัดการความเสี่ยงและกำกับดูแล RPA (Risk and Governance)
  2. การเข้าถึงและสิทธิการใช้งาน RPA (Authentication of bots)
  3. การติดตามการดำเนินงานของ Bot (Bot monitoring)
  4. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

THANK YOU

https://www.tfac.or.th

@TFAC.FAMILY

tfac@tfac.or.th

https://www.facebook.com/TFAC.FAMILY

https:// www.youtube.com/TFACFamily

02 685 2500