หลักสูตร IT Audit for Non IT Auditor
วันที่ ๑๓ พฤศจิกายน ๒๕๖๔
ผ่านโปรแกรม Microsoft Teams

สารบัญ

หลักสูตร IT Audit for Non IT Auditor
วันที่ ๑๓ พฤศจิกายน ๒๕๖๔
ผ่านโปรแกรม Microsoft Teams

๑. ความหมายของ IT Audit หมายถึง “การตรวจสอบการควบคุมการจัดการภายในระบบหรือฝ่ายเทคโนโลยีสารสนเทศ (IT) ซึ่งการตรวจสอบจะพิจารณา โครงสร้างพื้นฐาน ด้วยการประเมินผลจากหลักฐานที่ได้เข้าไปตรวจสอบแล้วพบว่าข้อมูลที่ได้มีการปกป้อง ที่เป็นสินทรัพย์ขององค์กร/บริษัท ยังคงสภาพของข้อมูลสมบูรณ์ และมีการดำเนินงานได้อย่างมีประสิทธิภาพ เพื่อให้บรรลุเป้าหมายขององค์กร หรือ วัตถุประสงค์ นอกจากนี้ผู้ตรวจสอบ IT Audit อาจจะเข้าไปตรวจสอบในส่วนของ "งบการเงิน" "ระบบเงินเดือน" "ระบบสิทธิ์ของพนักงาน" และสภาพแวดล้อมการทำงานทั่วไปของฝ่ายเทคโนโลยีสารสนเทศการตรวจสอบด้าน IT จะมีชื่อเรียกเป็นที่รู้จักกัน "Automated data processing audit" (ADP) หรือ การประมวลผลข้อมูลอัตโนมัติ ในขณะที่การตรวจสอบเครื่องคอมพิวเตอร์ จะเรียกว่า "Electronic data processing audit" (EDP)”

๒. วัตถุประสงค์การตรวจสอบ IT

การตรวจสอบจะมีความแตกต่างกันแยกไปตามวัตถุประสงค์ของการตรวจ อาทิ

๑) การตรวจสอบทางการเงิน คือ การประเมินว่าองค์กรจะยึดมั่นที่จะปฏิบัติตามมาตรฐานการบัญชีในระดับสากล และความถูกต้องของข้อมูลที่เป็นตัวเลข การเชื่อมโยงของฐานข้อมูลที่เป็นตัวเลขกับหน่วยงานต่าง ๆ ที่นำไปวิเคราะห์ต่อ

๒) การตรวจสอบด้าน IT คือ การประเมินระบบควบคุมการใช้งานให้มีความปลอดภัย มีมาตรฐานการป้องกันผู้บุกรุกจากภายนอก มีระบบป้องกันความปลอดภัยของ Data Center หรือ Data Warehouse และการออกแบบระบบปฏิบัติการที่มีความเหมาะสม หรือ ตรวจสอบด้าน IT Governance

๓. ประเภทของการตรวจสอบด้าน IT

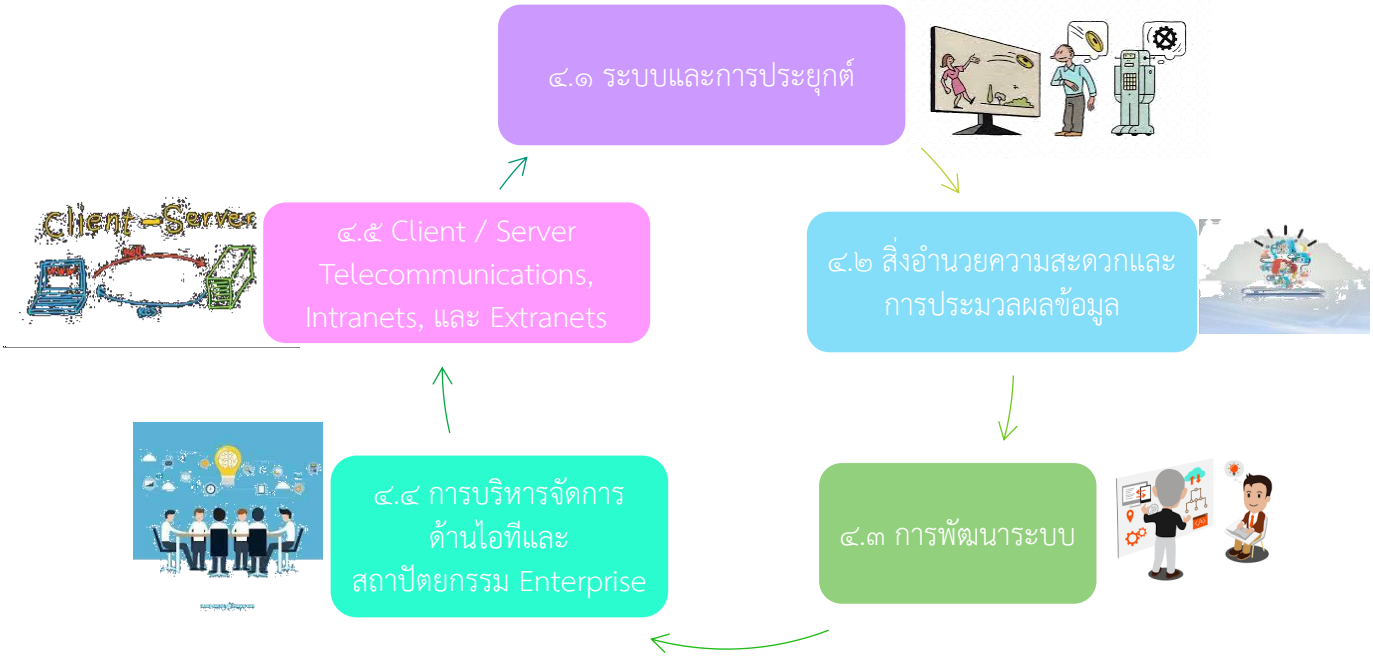
หน่วยงานชั้นนำทั้งในประเทศและต่างประเทศก็จะมีมาตรฐานในการตรวจด้าน IT ที่แตกต่างกัน เพราะงบประมาณที่จะนำมาใช้ในการดำเนินงานต่างกัน ความสามารถของพนักงานต่างกัน และความสำคัญของฐานข้อมูลและระบบเครือข่ายที่เชื่อมโยงกับหน่วยงานต่าง ๆ ทั้งภายในองค์กร และ ภายนอกองค์กร ที่ต่างกัน ดังนั้นขอยกตัวอย่างของประเภทของการตรวจสอบด้าน IT ดังนี้

๓.๑ การตรวจสอบกระบวนการและนวัตกรรมเทคโนโลยีสารสนเทศ (Technological innovation process audit) การตรวจสอบลักษณะนี้จะเป็นการตรวจสอบของหน่วยงานขนาดใหญ่ ที่มีแผนที่จะเข้าจดทะเบียนในตลาดหลักทรัพย์ หรือ จะควบรวมกิจการกัน เพราะจำเป็นอย่างมากที่จะต้องมีทีมงานตรวจสอบที่มีความรู้ความสามารถเฉพาะทางเกี่ยวกับเทคโนโลยีประเภทนั้น ๆ หรือ เป็นผู้เชี่ยวชาญในสาขานั้น ๆ กันเลย เพราะจะต้องให้ความเห็นว่าเทคโนโลยีที่องค์กร A ใช้อยู่มีความล้าสมัยประการใด และมีทางที่จะบำรุงรักษาหรือไม่ รวมทั้งจะต้องมีการประเมินมูลค่าของเทคโนโลยีที่เป็นนวัตกรรมใหม่ ๆ อีกด้วย ซึ่งมีความสลับซับซ้อนอย่างสูง

๓.๒ การตรวจสอบเปรียบเทียบนวัตกรรม (Innovative comparison audit)การตรวจสอบลักษณะนี้เป็นการวิเคราะห์ความสามารถด้านนวัตกรรมของบริษัท ที่ถูกตรวจสอบด้วยการนำนวัตกรรมไปเปรียบเทียบกับคู่แข่ง ที่มีความสามารถใกล้เคียงกัน ซึ่งการตรวจสอบลักษณะนี้ส่วนมากจะเป็นบริษัทวิจัยต่าง ๆ จะรับเข้าไปทำการตรวจสอบบริษัทให้ เพราะจำเป็นจะต้องมีการนำผลการวิจัยในด้านต่าง ๆ มาอ้างอิงสิ่งที่ตรวจสอบพบ หรือให้ความเห็นในด้านคุณค่าของนวัตกรรมที่ได้เข้าไปตรวจสอบ

๓.๓ การตรวจสอบตำแหน่งเทคโนโลยี (Technological position audit) การตรวจสอบลักษณะนี้จะเป็นการให้ความเห็นและความเชื่อมั่นแก่ผู้รับตรวจว่า เทคโนโลยีของบริษัท ยังมีความเป็นปัจจุบันอยู่หรือไม่ และเป็นเทคโนโลยีในกลุ่มประเภทใด อาทิ "base", "key", "pacing", หรือ "emerging"

๔. ประเภทของการตรวจสอบด้าน IT ให้แยกย่อยออกไปอีก ก็จะได้เป็น ๕ ประเภท ดังนี้



๔.๑ ระบบและการประยุกต์ : การตรวจสอบระบบและการประยุกต์ใช้ว่ามีความเหมาะสมและมีประสิทธิภาพ และมีการควบคุมความปลอดภัยอย่างเพียงพอ เพื่อให้แน่ใจว่าข้อมูลยังมีความถูกต้อง น่าเชื่อถือ และยังมีความทันสมัยอยู่เสมอ หรือมีความปลอดภัยในการประมวลผลและการส่งออกไปยังหน่วยงานต่าง ๆ ในทุกระดับกิจกรรมของระบบ

๔.๒ สิ่งอำนวยความสะดวกและการประมวลผลข้อมูล : การตรวจสอบว่าสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลจะถูกบริหารจัดการและมีระบบการควบคุมเพื่อให้แน่ใจว่าการประมวลผลข้อมูลทันเวลา ถูกต้อง และมีประสิทธิภาพของการใช้งานภายใต้สภาวะปกติ และมีระบบป้องกันการก่อกวนทั้งจากภายในและภายนอก

๔.๓ การพัฒนาระบบ : การตรวจสอบว่าระบบภายใต้การพัฒนาตรงกับวัตถุประสงค์ขององค์กร เพื่อให้แน่ใจว่าระบบได้การพัฒนาขึ้นตามมาตรฐานที่ยอมรับโดยทั่วไปสำหรับการพัฒนาระบบ

๔.๔ การบริหารจัดการด้านไอทีและสถาปัตยกรรม Enterprise : การตรวจสอบว่าการบริหารจัดการด้าน IT ได้มีการพัฒนาโครงสร้างองค์กรและวิธีการเพื่อให้แน่ใจว่าสภาพแวดล้อมการควบคุมและมีประสิทธิภาพสำหรับการประมวลผลข้อมูล

๔.๕ Client / Server Telecommunications, Intranets, และ Extranets: เป็นการตรวจสอบว่าการสื่อสารโทรคมนาคม มีระบบการควบคุมอยู่ในสถานะที่ดี พร้อมใช้งาน มีคุณภาพเหมาะสม มีประสิทธิภาพในการเชื่อมต่อกับเครื่องลูกข่ายได้อย่างเหมาะสม และเกิดประโยชน์สูงสุด

๕. กระบวนการตรวจสอบด้าน IT

๕.๑ การวางแผน
๕.๒ การศึกษาและการประมินผลการควบคุม
๕.๓ การทดสอบและการประเมินผลการควบคุม
๕.๔ การรายงาน
๕.๕ การติดตามผล

๖. หลักการตรวจสอบระบบเทคโนโลยีสารสนเทศ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ จะเป็นการตรวจสอบการควบคุม ภายในด้านคอมพิวเตอร์ที่แบ่งออกได้เป็น ๒ ลักษณะ คือ

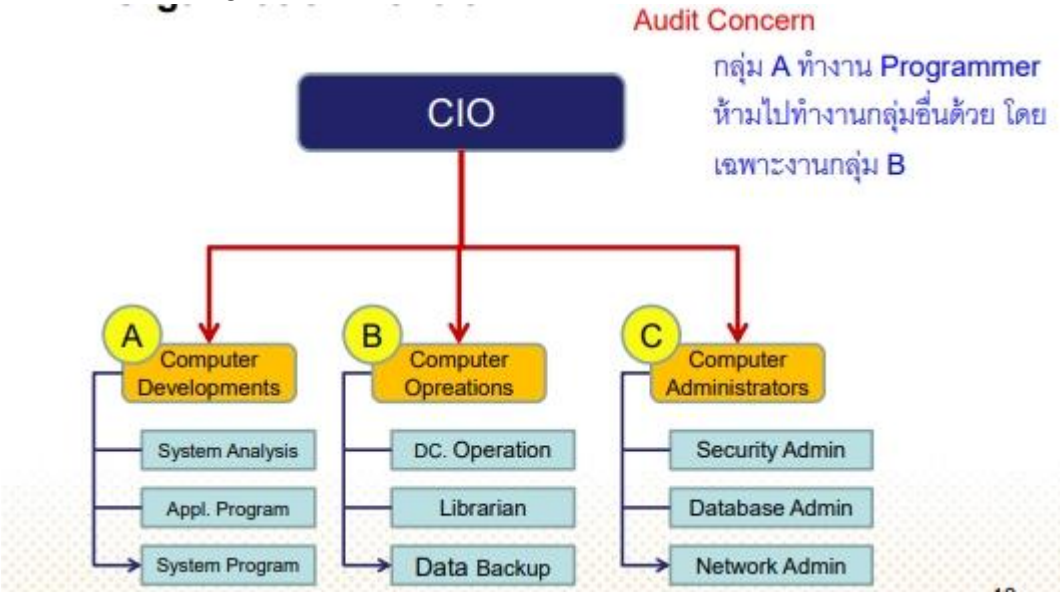
๖.๑ การควบคุมภายในทั่วไป (General Controls) เป็นการควบคุมที่อาศัยนโยบาย และระเบียบปฏิบัติงาน เป็นหลักในการควบคุมกิจกรรมของ หน่วยงานคอมพิวเตอร์

๖.๑.๑ IT Planning and Organization

– IT Steering Committee

- กำหนดนโยบายด้านเทคโนโลยีสารสนเทศ
- พิจารณาโครงการและงบประมาณ IT
- ติดตามผลการดา เนินการด้านสารสนเทศขององค์กร

- IT Organization Control



๖.๑.๒ Development and Implementation Control

– Business Requirement

– Feasibility Study (User agree & signoff)

– System Analysis and Design (Documentation & User signoff)

– Coding Program

– Program Testing (Test Scenario , UAT , User Signoff)

– Data Conversion (Data Reconciliation & User signoff)

– Implementation (System doc. & Training Manual)

– Post Implementation Review (Problem logging & Change Procedure)

๖.๑.๓ Information Security Control

– IT security Policy and Procedure

• นโยบายด้านความปลอดภัยและระเบียบปฏิบัติ

• จัดความสำคัญของระบบและข้อมูล

• มีการกำหนดหน้าที่รับผิดชอบ

– User Access Control Feature

• Password Policy

• User Authorized Matrix

– Logging and Monitoring

• ระยะเวลาการเก็บ Log

– Physical Security

• การควบคุมการเข้าออก , Room Environment

๖.๑.๔ Maintenance of Existing System Control

– ตรวจการปฏิบัติตามระเบียบการพัฒนาระบบ (SDLC)

– Change Management

• Changed Detection Program

• Changed Request Form

ทุกการเปลี่ยนแปลงในระบบ จะต้องมี Request Form

๖.๑.๕ Computer Operation Control

- Operation Schedule/Time table/Control Procedure

• ต้องทำงานตามคู่มือและขั้นตอนการปฏิบัติงาน

– Service Level Agreement: SLA

– Data Backup Procedure

– Disaster and Recovery Plan: DRP

• การเขียนแผน การทดสอบแผน และการปรับปรุงแผน

๖.๒ การควบคุมภายในเฉพาะงาน (Application Controls) เป็นการควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของ ข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม

๖.๒.๑ วัตถุประสงค์

- Completeness (ให้ความมั่นใจในความสมบูรณ์ของข้อมูล)
- Accuracy (ความถูกต้องตรงกันทุกประการของข้อมูล)
- Validity (ความสมเหตุสมผลของข้อมูล)
- Restricted Access to Data and Physical asset

(การจำกัดการเข้าถึงข้อมูลและสินทรัพย์)

C A V R ทำได้โดยการควบคุมข้อมูล

– ข้อมูลนำเข้า (Input Control) วิธีการ ที่มา ความถูกต้อง

– การประมวลผล (Processing Control)

– ข้อมูลผลลัพธ์ (Output Control)

๖.๒.๒ ตัวอย่างการควบคุมความถูกต้องของรายการข้อมูล

– Check digit validation (การคำนวณเลขหลักสุดท้ายของเลขบัญชี)

– Range Check (เช่น ข้อมูลช่วงอายุของลูกค้า)

– Limit Check (เช่น จำกัดวงเงินในการถอนจากตู้ ATM)

– Sequence Check (เช่น เลขที่เอกสารไม่ซ้ำกัน)

เทคนิคการใช้ระบบคอมพิวเตอร์ช่วยในการตรวจสอบ เพื่อหาสาระในเชิงลึก (Substantive Test) ไม่มีความเชื่อถือในระบบการควบคุมภายใน และต้องทำการทดสอบความถูกต้องของรายการ

– Generalized Audit Software: GAS เช่น ACL software

– Custom Audit Software: เขียนหรือพัฒนาขึ้นมาเอง เพื่อเปรียบเทียบ Output กับรายงาน User

– Test Data โดยการสร้าง Test script และนำ Program ของ User มา Run กับ Data test

– Concurrent Auditing Techniques : การตรวจสอบหาความผิดปกติของข้อมูลที่เกิดขึ้นในระบบ

เช่น ACL software เขียนหรือพัฒนาขึ้นมาเอง เพื่อเปรียบเทียบ Output กับรายงาน User โดยการสร้าง Test script และนำ Program ของ User มา Run กับ Data test การตรวจสอบหาความผิดปกติของข้อมูลที่เกิดขึ้นในระบบ

• **Concurrent Auditing Techniques** เป็นการตรวจสอบข้อมูลในระบบเพื่อหา ข้อผิดพลาด ความผิดปกติ ของข้อมูลที่ส่อในทางทุจริต หรือความบกพร่องของระบบควบคุมภายในและระเบียบ

ผลที่จะได้

-พบว่าไม่ปฏิบัติตามระเบียบ

-ข้อมูลส่อในทางทุจริต

-พบข้อบกพร่องของระบบ IT

-พบข้อบกพร่องของการควบคุมภายใน

-ได้ทราบถึงพฤติกรรมของผู้ปฏิบัติงาน

-ฯลฯ

๖.๒.๓ การตรวจสอบความถูกต้องของอัตราดอกเบี้ยในระบบเปรียบเทียบกับผลิตภัณฑ์

– กวาดข้อมลูตามผลิตภัณฑ์ ดูว่ามีรายใดที่มีอัตราดอกเบี้ยไม่ตรงตามข้อกำหนด

– เปรียบเทียบดอกเบี้ยสะสมประจำเดือน ว่ามีรายใดที่มีการเปลี่ยนแปลงสูง

– ดู Audit trail Log ที่แก้ไขอัตราดอกเบี้ย

๖.๒.๔ การตรวจข้อมูลการจ่ายเงินเดือน ค่ารักษาพยาบาล

– ดูยอดเบิกจ่ายที่สูงและมีความถี่สูง และดูความสัมพันธ์ของผู้ทำรายการกับผู้เบิก

๖.๒.๕ การดูการเคลื่อนไหวของรายการที่สูงผิดปกติ หรือการเกิดซ้ำเกิดนอกเวลาทำการ

- ดูจากบัญชีเงินฝากที่มีเงินเข้าแต่ละเดือนสูงกว่ารายรับที่ควรจะเป็น และเกิดต่อเนื่อง

- มีการทำรายการทางการเงิน นอกเวลาทำการ

๖.๓ การตรวจสอบโครงการเทคโนโลยีสารสนเทศ (Quality Assurance IT Project) เป็นการเข้าร่วมสังเกตการณ์ ให้ข้อเสนอแนะโครงการ ตั้งแต่เริ่มโครงการ

๖.๓.๑ วัตถุประสงค์

การสร้างความมั่นใจและให้คำปรึกษาในการทำงานโครงการที่ยังไม่เสร็จสิ้น เพื่อให้ได้โครงการประสบความสำเร็จ

๖.๓.๒ ระยะเวลาการตรวจสอบ

– ช่วงการวางแผนโครงการ คือการตรวจสอบในช่วงที่เริ่มวางแผนว่าจะดำเนินโครงการ ว่าได้จัดทำข้อกำหนดครบถ้วนหรือไม่

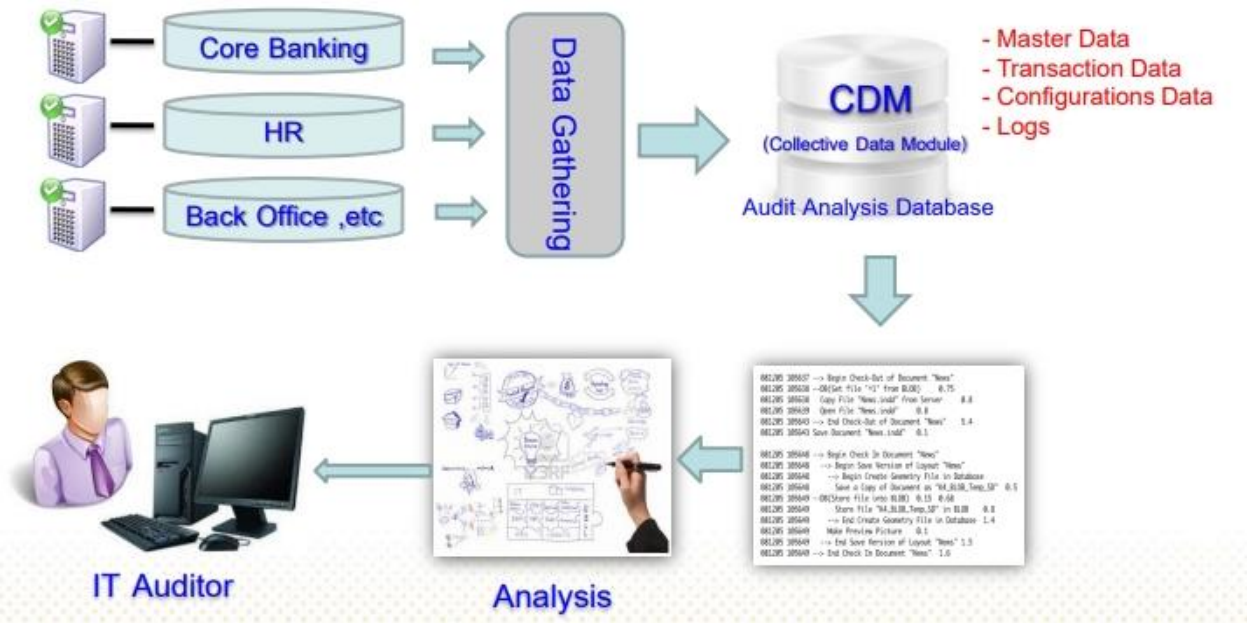
– ในช่วงการจัดหาบริษัทที่ปรึกษา คือการตรวจสอบว่าได้จัดหาบริษัทที่ปรึกษามาอย่างถูกต้องตามหลักเกณฑ์หรือไม่

– ในช่วงการดำเนินโครงการ คือการตรวจสอบการท าโครงการว่าถูกต้องหรือไม่

– ในช่วงหลังการติดตั้งใช้งานผลของโครงการ คือการตรวจสอบว่าโครงการได้ผลตามที่ ต้องการหรือไม่

๗. วิธีการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Steps of an IT Audit)

๘. ระบบฐานข้อมูลเพื่อการตรวจสอบ (Audit Analysis Database)



๙. ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit)

๑๐.๑ ทักษะด้านการตรวจสอบ

๑๐.๑.๑ ผ่านงานผู้ตรวจสอบ

๑๐.๑.๒ มี Certificated ผู้ตรวจสอบ IT

๑๐.๒ ทักษะด้าน IT

๑๐.๒.๑ ผ่านงานด้าน IT

๑๐.๒.๒ จบการศึกษาด้าน IT

๑๐.๓ ทักษะด้านธุรกรรมหลักขององค์กร

๑๐.๓.๑ ผ่านงานด้านธุรกรรมหลักขององค์กรในระดับ Supervisor

๑๐. สมาคมผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ (Information Technology Auditor)

- Internal Auditor ->
- Information Technology Auditor ->
- Information Security Auditor ->

.....