บันทึกข้อความ

ส่วนราชการ ฝ่ายตรวจสอบ ๒ กลุ่มตรวจสอบภายใน โทร. ๐๒-๕๙๐๔๑๐๐๒ โทรสาร. ๐๒-๕๙๐๔๑๐๐๑

ที่ สธ ๐๙๒๕.๐๓/ ๑๒๑ **วันที่** ๒๙ กรกฎาคม ๒๕๖๑

เรื่อง สรุปรายงานการอบรม CGIA หลักสูตร Advance ด้าน Information Technology

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน (ผ่านหัวหน้าฝ่ายตรวจสอบ ๒)

ตามที่กลุ่มตรวจสอบภายใน ได้อนุมัติให้ดิฉัน เข้ารับการอบรมประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA) หลักสูตร Advanced ด้าน Information Technology ครั้งที่ ๑ ระหว่างวันที่ ๒๙ มีนาคม – ๑ เมษายน ๒๕๖๑ ณ โรงแรมนารายณ์ กรุงเทพฯ นั้น สรุปผลการเข้ารับการอบรม ดังนี้

IT Governance & Importance IT Governance Frameworks and Standards

โดย อาจารย์มานิตย์ พาณิชย์กุล และ ดร.พรเทพ อนุสสรนิติสาร

ประเภทของการตัดสินใจหลักที่เกี่ยวข้องกับการบริหารจัดการระบบ IT เป็นบทบาทของระบบ IT ที่เกี่ยวข้องกับกลยุทธ์ขององค์กร

๑) IT Principles : ด้านยุทธศาสตร์ของระบบ

๒) IT Architecture : ด้านสถาปัตยกรรม เป็นทางเลือกด้านเทคนิคที่จะช่วยผลักดันให้องค์กรบรรลุเป้าหมาย (Network →Internet ภาครัฐ เป็น Mobile)

๓) IT Infrastructure : ด้านโครงสร้างพื้นฐานของระบบ **ซึ่งเป็นปัจจัยพื้นฐานที่สะท้อนให้เห็นถึง** ศักยภาพของระบบ เช่น ความเร็วของ IT

๔) Business Application Need : ด้านความต้องการขององค์กร ซึ่งเป็นรูปแบบของระบบที่จะช่วยสนับสนุนกิจกรรมขององค์กร

๕) Prioritization and Investment : ลำดับความสำคัญและการลงทุน เช่น การกำหนดงบประมาณการลงทุนที่จุดใด

ลักษณะโครงสร้างการตัดสินใจในการจัดการระบบ IT

๑) Business Monarchy : เป็นระบบรวมศูนย์ที่สุด คือ CEO หรือ CIO ตัดสินใจโดยลำพัง

๒) IT Monarchy : การตัดสินใจโดยผู้เกี่ยวข้องด้าน IT เท่านั้น

๓) Federal : การตัดสินใจร่วมกันในหลาย ๆ ฝ่าย รวมทั้งแผนก IT ในรูปแบบคณะกรรมการ

๔) IT Duopoly : การตัดสินใจร่วมกันสองส่วน ซึ่งมักจะเป็นแผนก IT กับ หัวหน้าหน่วยงานที่ใช้ระบบ

ในการบริหารความเสี่ยงระบบ IT จะต้องมี Feedback เป็นการติดตามความเสี่ยง (Monitor and Track Risk)

Organizational structure in IT risk governance process (โครงสร้างขององค์กรในกระบวนการบริหารความเสี่ยงระบบ IT) ประกอบด้วย

- ผู้บริหาร ซึ่งต้องมีบทบาทสร้างความตื่นตัวในองค์กร (Risk – aware culture)
- IT risk management team บทบาท คือ ทบทวนติดตามความเสี่ยง
- Local manager and experts บทบาท คือ เป็นผู้ใช้และเป็นผู้บริหารความเสี่ยง เพื่อ Feedback on policies and processes / reduce risk เป็นผู้ควบคุมหรือลดผลกระทบด้านความเสี่ยงเมื่อเกิดปัญหาขึ้น

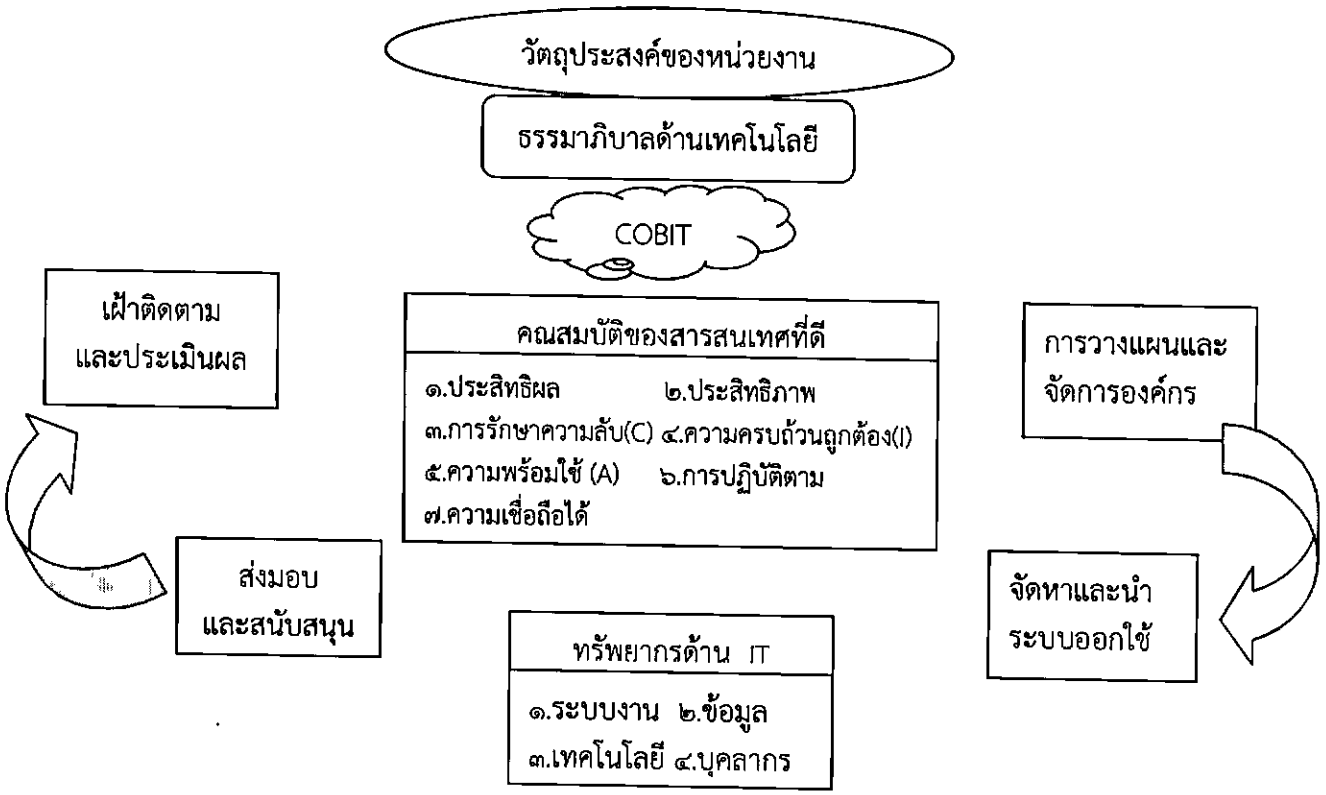
ทำไมเราต้องมาสนใจการจัดทำระบบ IT Governance

๑) เพราะระบบการดำเนินการขององค์กรต่าง ๆ ต้องอาศัยระบบคอมพิวเตอร์เป็นกลไกหลักในการดำเนินการ เช่น ระบบ GFMIS

๒) มูลค่าในการลงทุนระบบ IT มีแนวโน้มสูงขึ้นเรื่อย ๆ ในอนาคต

๓) มีความเสี่ยงต่อการมีปัญหาด้านความปลอดภัย เช่น ไวรัส e-mailขยะ ระบบถูกบุกรุก

เครื่องมือที่ใช้ในการปรับปรุง (Availability Risk) คือ BCP หรือ BCM (Business Continuity management) ความเข้าใจและการลดผลกระทบอันเกิดจากเหตุการณ์ที่ร้ายแรง ที่ส่งผลการดำเนินการที่สำคัญขององค์กร)



ต้นเหตุของความเสี่ยงด้านระบบ IT

๑) ขาดประสิทธิภาพในการบริหารจัดการระบบ IT

๒) การขยายตัวของความซ้ำซ้อนของระบบ IT

๓) ความไม่ใส่ใจต่อความเสี่ยงด้าน IT

- ขาดความรู้ ความชำนาญ
- โครงสร้างพื้นฐานของระบบ IT ไม่ดี
- ความไม่ใส่ใจต่อความเสี่ยงของเจ้าหน้าที่
- การขาดระบบในการเตือนภัย

อุปสรรคของการบริหารคามเสี่ยงด้าน IT ระดับองค์กร

คือ การขาดภาพรวมของการดำเนินการของระบบ IT ที่เชื่อมโยงกับการดำเนินงานและเป้าหมายขององค์กร

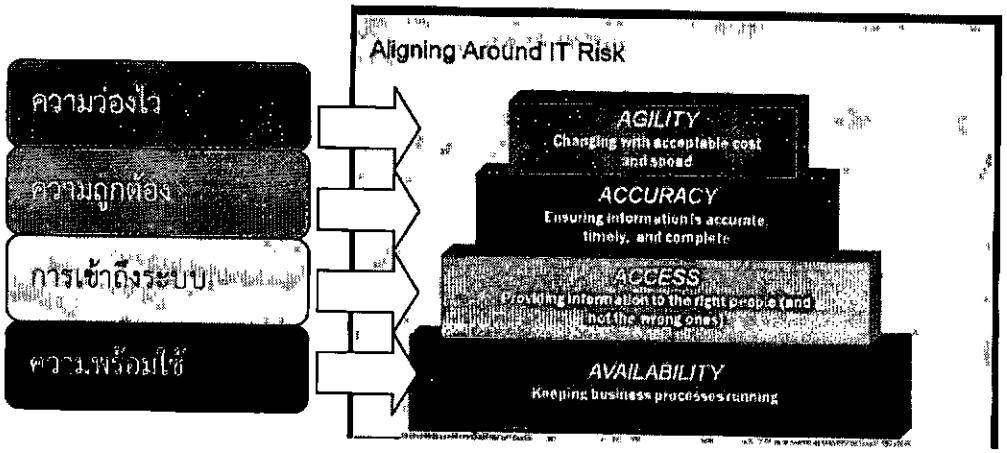
องค์ประกอบสำคัญในการสร้างคุณค่าทางสังคม (Public Value) ของรัฐบาลอิเล็กทรอนิกส์ (e - Government) ได้แก่ การให้บริการต่าง ๆ (Citizen Service Applications) คุณภาพและประสิทธิภาพการให้บริการ ความน่าเชื่อถือ (Trust)

ภาครัฐ ควรดู →ความไม่พอใจของประชาชน

ประโยชน์ของ ๔A Framework

ใช้แลกเปลี่ยนความคิดเห็นระหว่างผู้บริหารกับ IT ได้คุยกันและเข้าใจความเสี่ยงที่เกิดขึ้น

กรอบการประเมินความเสี่ยงด้าน IT



การเริ่มต้นการประเมินความเสี่ยง Where to start IT Risk?

๑) ดูพื้นฐานของระบบ IT (Foundation) ทำให้ง่าย ไม่ซับซ้อน

๒) ดูกระบวนการ (Process) การจัดการความเสี่ยงและติดตาม

๓) ดูความตื่นตัว (Awareness) วัฒนธรรมขององค์กร

ขั้นตอนในการปรับปรุงโครงสร้างพื้นฐาน (Foundation)

เริ่มต้นจาก ๑) จัดการกับ Availability risk (ความพร้อมใช้)

๒) ค้นหาปัญหาและรีบแก้ไข

๓) พัฒนาและปรับปรุง ใช้แนวทางการควบคุมในการติดตามสถานะของระบบ IT

งานที่สำคัญของ IT ๔ กลุ่ม มี ๓๔ กระบวนการ แต่มีกระบวนการที่สำคัญ ได้แก่ PO AI DS ME

Domain ที่ ๑ (PO) Planning & Organization: การวางแผนและการจัดการองค์กร ให้ความสำคัญ ๓ เรื่อง คือ PO๑ : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ

PO๙ : การประเมินความเสี่ยง

PO๑๐ : การจัดการโครงการ

มิติในเชิงป้องกัน Prevention ใช้ต้นทุนต่ำสุด

Domain ที่ ๒ (AI) Acquisition & Implementation: การจัดหาและการนำไปใช้งานจริง คือ ดำเนินการามแผนกลยุทธ์ที่วางไว้ โดยการพัฒนาจัดหาและถูกนำไปใช้งานจริง ให้ความสำคัญกับ

AI๖ : การจัดการแก้ไขโปรแกรมและระบบงาน

Domain ที่ ๓ (DS) Delivery & Support: การส่งมอบและสนับสนุน ให้ความสำคัญกับ ๒ เรื่อง คือ

DS๕ : การสร้างความมั่นใจในความปลอดภัยของระบบ

DS๑๑: การจัดการข้อมูลสารสนเทศ

Domain ที่ ๔ (ME) Monitor & Evaluate การติดตามและประเมินผล ให้ความสำคัญกับ ๓ เรื่อง คือ

ME๑ : การติดตามและประเมินผลการปฏิบัติงาน

ME๓ : การปฏิบัติตามกฎหมายและกฎเกณฑ์

ME๔ : ความเป็นธรรมาภิบาล

Control – Based คือ การควบคุมและกำกับดูแล

๑) ต้องควบคุมในเชิงเป้าหมายของธุรกิจ
   - ออกกฎระเบียบ นโยบายที่ปฏิบัติ
   - การควบคุมระบบกระบวนการ
   - การควบคุม IT ทั่วไป

๒) การควบคุมด้าน IT มี ๒ Control คือ
   ๒.๑ IT General Controls : ด้านทั่วไป
   ๒.๒ Application Controls : ภายในระบบ

Measurement – driven

คือ แนวคิดการขับเคลื่อนโดยการวัดผล ใช้เครื่องมือดังนี้

๑) Dashboard : เป็นกระบวนการติดตามอย่างต่อเนื่องในเรื่องของเป้าหมายกับผลการปฏิบัติ โดยการเปรียบเทียบเป็นระยะ ๆ เพื่อแก้ไขปรับปรุง

๒) Scorecard : กำหนดให้มี ๔ ตัวชี้วัด ในการวัดผล โดยวัดทั้ง ๔ ตัว แล้วแต่ให้น้ำหนักตัวไหน แต่ต้องครบ ๔ ตัว Financial – Customer – Process – Learning & Development

๓) Benchmark : เทียบกับหน่วยงานที่ทำแล้วดี

IT Governance Focus Areas เป้าหมาย ๕ เรื่อง คือ

๑) Strategic Alignment ความสอดคล้องกับกลยุทธ์
๒) Value Delivery การสร้างคุณค่า ผลตอบแทน
๓) Risk Management การบริหารความเสี่ยง
๔) Performance Measurement การวัดผลการดำเนินงาน
๕) Resource Management การบริหารทรัพยากร

Business – Focus คือ ทุกอย่างต้องเชื่อมเป้าหมายทางธุรกิจ เน้นความต้องการของธุรกิจ จะใช้วงจรคุณภาพเข้ามาจัดการ (Plan - Do - Check - Act) โดยมีพื้นฐาน IT ประกอบด้วย ข้อมูล (Information) ระบบงาน (Application) เครือข่าย (Infrastructure) บุคลากร (People)

What is COBIT ? COBIT : Control Objective for Information and related Technologies

COBIT มาจากพื้นฐานของธรรมาภิบาลหลายตัว เช่น ITIL , ISO ๑๗๗๙๙ , CMM , COSO
สรุป COBIT เป็น High Level ไม่เน้นรายละเอียด ประกอบด้วย ISO ๑๗๗๙๙ , CMM , ITIL จะมีขอบเขตตั้งแต่ Process Control จนถึง Strategic

IT Governance จะสำเร็จได้อยู่ที่ Top คือ เป็นความรับผิดชอบของผู้บริหารระดับสูงและคณะกรรมการที่กำกับดูแล

คุณลักษณะที่สำคัญของ COBIT ประกอบด้วย

- Business – Focus เน้นความต้องการของธุรกิจ
- Process – Oriented เน้นกระบวนการในการบริหารงาน IT (PO AI DS ME)
- Control – Based มุ่งเน้นการควบคุมกำกับดูแล
- Measurement – Driven ตั้งเป้าวัดผลมีตัวชี้วัดทุกขั้นตอน ขับเคลื่อนด้วยตัวชี้วัด

แนวคิดการควบคุมด้าน IT ระดับสูง

๑) ต้องเข้าใจธุรกิจ (เข้าใจการให้บริการหน่วยงาน)
๒) แนะนำแนวปฏิบัติที่ดี (Good Practices) ในการปฏิบัติงาน IT
๓) เน้นการควบคุม (Control) แต่ไม่เน้นรายละเอียดเป็นกรอบใหญ่
๔) ช่วยให้หน่วยงานประสบผลสำเร็จในการลงทุน หรืองบประมาณด้าน IT
๕) ช่วยบอกวิธีการแก้ปัญหาถ้ามีข้อผิดพลาดเกิดขึ้น

Who does COBIT serve ?

๑) Stakeholders (หัวหน้าส่วนราชการ ประชาชน ลูกค้า)
๒) ผู้มาใช้บริการภายในและภายนอก
๓) ผู้ทำหน้าที่ควบคุมและรับผิดชอบความเสี่ยงทั้งภายในและภายนอก

ประโยชน์ของการใช้ COBIT

๑) ความสอดคล้องกับกลยุทธ์ เช่น แผนกลยุทธ์ทางด้าน IT ต้องเข้ากันกับแผนธุรกิจหรือหน่วยงาน
๒) การสร้างคุณค่าเพิ่ม เช่น สะสางบทบาทหน้าที่ของแต่ละคน ธรรมาภิบาลบอกว่าใครทำหน้าที่อะไร
๓) การบริหารความเสี่ยง เช่น เป็นที่ยอมรับของผู้มารับบริการ
๔) การวัดผลการดำเนินงาน เป็นตัวบอกแนวคิดวิธีการบริหารจัดการด้าน IT ทั่วไป
๕) การบริหารทรัพยากร โดย COBIT ใช้หลักการควบคุมของ COSO ด้วย

จึงเรียนมาเพื่อโปรดทราบ จะเป็นพระคุณ

(นางจรัญญา สะเริญรัมย์)
นักวิชาการตรวจสอบภายในปฏิบัติการ

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน

เพื่อโปรดทราบสรุปรายงานผลการอบรม CGIA หลักสูตร Advanced ด้าน IT ข้างต้นด้วย จะเป็นพระคุณ

(นางสาวอรุณี มนปราณีต)
นักวิชาการตรวจสอบภายในชำนาญการพิเศษ
หัวหน้าฝ่ายตรวจสอบ ๒

(นางสาวพิมพ์ภวดี ศรีจันทร์)
ผู้อำนวยการกลุ่มตรวจสอบภายใน