รายงานสรุปผลการอบรมโครงการจัดการความรู้
เพื่อสร้างเครือข่ายงานตรวจสอบ (IA Networking)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

กลุ่มตรวจสอบภายใน (กตส.) ได้ดำเนินโครงการจัดการความรู้เพื่อสร้างเครือข่ายงานตรวจสอบ (IA Networking) ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ครั้งที่ ๑ - ๓ ประกอบด้วย ๓ หัวข้อ ได้แก่ ๑) Risk Based Audit ๒) IT Governance Audit Workshop และ ๓) IT Governance Audit โดยมีรายละเอียด ดังนี้

วัตถุประสงค์ของการอบรม

๑) เพื่อพัฒนาศักยภาพของบุคลากร กตส. โดยจัดให้มีการอบรมและการพัฒนาตนเอง อย่างต่อเนื่อง ส่งผลให้การปฏิบัติงานตรวจสอบมีประสิทธิภาพ และเป็นไปตามแนวทางการเพิ่มประสิทธิภาพ การปฏิบัติงานตรวจสอบภายในของ สบน.

๒) เพื่อส่งเสริมการมีส่วนร่วมในการแสดงความคิดเห็น แลกเปลี่ยนความรู้ ประสบการณ์ กับวิทยากร ผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญจากภายนอก และผู้เข้ารับการอบรมสามารถนำความรู้และประสบการณ์ที่ได้รับไปปรับใช้ในการปฏิบัติงานเพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร

๓) เพื่อพัฒนาเครือข่ายด้านตรวจสอบภายในกับหน่วยงานภายนอก ให้มีการแลกเปลี่ยนความรู้ ประสบการณ์ด้านตรวจสอบภายในร่วมกัน และสร้างความสัมพันธ์ที่ดี

ผู้เข้าร่วมอบรม : ผู้ตรวจสอบภายใน สบน. จำนวน ๗ คน และเครือข่ายตรวจสอบภายใน สังกัดกระทรวงการคลัง จำนวน ๑๓ คน รวมทั้งสิ้น ๒๐ คน

หัวข้อการอบรม ครั้งที่ ๑ : Risk Based Audit

วิทยากร : นายไพรัช ศรีวิไลฤทธิ์ CIA, CISA, CCSA, CFSA, CISSP, CFE บริษัท ทิสโก้ไฟแนนเชียลกรุ๊ป จำกัด (มหาชน)

สาระสำคัญของการอบรมสรุปได้ดังนี้

๑. <u>วัตถุประสงค์</u>

๑) เพื่อให้ผู้ตรวจสอบภายในสามารถวางแผนการตรวจสอบประจำปีและนำเสนอแผนอย่างเป็นระบบ

๒) เพื่อให้ผู้ตรวจสอบภายในสามารถวางแผนภารกิจการตรวจสอบตามมาตรฐานวิชาชีพและเป็นที่ยอมรับตามมาตรฐานสากล

๒. <u>การวางแผนตามความเสี่ยง</u> โดยนำการประเมินความเสี่ยงมาเป็นเครื่องมือกำหนดลำดับกิจกรรมการตรวจสอบและความถี่ของการตรวจสอบ ซึ่งประโยชน์ของการวางแผนตามความเสี่ยง เช่น (๑) ทำให้กิจกรรมที่มีความเสี่ยงสูงได้รับการตรวจสอบก่อนและบ่อยครั้ง (๒) ใช้ทรัพยากรได้อย่างมีประสิทธิผลและคุ้มค่า (๓) สอดคล้องเป้าหมายองค์กร (๔) ทราบปัญหาและสาเหตุปัจจัยเสี่ยง และ (๕) เป็นมาตรฐานวิชาชีพที่กำหนด

๓. <u>การกำหนดวิธีการเลือกผู้รับการตรวจสอบ</u> วิธีการแบ่งกิจกรรมขององค์กรเป็นส่วนๆ เพื่อทราบขอบเขตทั้งหมดขององค์กรที่ต้องรับผิดชอบในการตรวจสอบ

- โครงสร้างองค์กร แบ่งตามหน่วยงานหรือหน้าที่ เช่น งานบัญชี งานบุคคล เป็นต้น
  แบ่งตามประเภทหน้าที่ เช่น บัญชีลูกหนี้ บัญชีเจ้าหนี้ บัญชีต้นทุน เป็นต้น
  แบ่งตามโครงการต่างๆ
- สถานที่ตั้ง เป็นการแบ่งตามสถานที่ทำงาน เช่น โรงงาน สาขา คลังสินค้า ภูมิภาค เป็นต้น
- มูลค่าที่วัดเป็นจำนวนเงิน แบ่งโดยพิจารณาผลกระทบทางการเงิน ซึ่งสะท้อนความเสี่ยงทางการเงิน เช่น พิจารณาแผนกที่มีเงินทุนหมุนเวียนมากน้อย หรือมีทรัพย์สินที่มีสภาพคล่องสูง

/- ความซับซ้อน ...

- ความซับซ้อนของงานหรือวิธีการทำงานพิจารณาจากกระบวนการและวิธีการ ทำงานว่าซับซ้อนมากหรือไม่ ถ้ามากต้องแบ่งเป็นวิธีการย่อยเพื่อแยกกิจกรรมที่จะตรวจสอบ

- ระดับการจัดการ พิจารณาโดยความเห็นร่วมกันของผู้บริหารว่างานใดมีการจัดการที่ชัดเจนหรือยังคงมีความเสี่ยงในด้านการบริหาร เช่น ไม่มีโครงสร้างที่ชัดเจน ไม่มีผู้รับผิดชอบโดยตรง เป็นต้น

- วงจรหรือกระบวนการทำงาน พิจารณากระบวนการทำงานในแต่ละฝ่ายงาน หรือระบบงานที่ต้องเกี่ยวข้องกับหลายฝ่ายงาน

- ศูนย์ความรับผิดชอบพิจารณาตามบุคคลหรือหน่วยงานที่รับผิดชอบงาน

๔. <u>ตัวอย่างเกณฑ์ Audit Universe</u> การกำหนดกิจกรรมเพื่อการตรวจสอบ (Audit Universe)

- หน่วยธุรกิจ เช่น ฝ่ายประกันภัยธนกิจ บริหารสินเชื่อรายย่อย
- สาขา เช่น สาขาระยอง สาขาสุราษฎร์ธานี สำนักงานใหญ่
- หน่วยงานสนับสนุน เช่น ศูนย์ชำระเงิน บริการคัสโตเดียน
- ระบบงานสารสนเทศ เช่น ระบบโอนเงินอิเล็กทรอนิกส์
- การควบคุมสารสนเทศ เช่น แผนฉุกเฉิน Outsourcing
- กฎระเบียบ เช่น ข้อกำหนดของบริษัทข้อมูลเครดิตแห่งชาติ
- ประเด็นที่อยู่ในความสนใจของผู้บริหาร เช่น การจัดการความเสี่ยงด้านสภาพคล่องนโยบายการกำกับดูแลกิจการ

๕. <u>การระบุและการจัดลำดับผู้รับการตรวจ</u>

ระบุแนวการเลือกผู้รับการตรวจสอบให้ครอบคลุมทั้งองค์กร จัดลำดับการตรวจสอบจากการประเมินความเสี่ยง กำหนดปัจจัยเสี่ยงและจัดลำดับงานที่จะตรวจสอบ

<u>ตัวอย่าง</u> การระบุผู้รับการตรวจสอบ

การกำหนดตามโครงสร้างองค์กร	
กิจกรรม	**กิจกรรมการตรวจสอบ**
๑	ฝ่ายตลาด - แผนกพัฒนา คุณภาพสินค้า - แผนกส่งเสริมการตลาด
๒	ฝ่ายผลิต - สายการผลิตที่ ๑ - สายการผลิตที่ ๒ - แผนกควบคุมคุณภาพสินค้า
๓	ฝ่ายคลังสินค้า - แผนกควบคุมการเบิกจ่ายสินค้า - แผนกจัดเก็บสินค้า - แผนกขนส่ง
๔	ฝ่ายขาย

การกำหนดตามกระบวนการดำเนินงาน	
กิจกรรม	**กิจกรรมการตรวจสอบ**
๑	การบริหารงานบุคคล
๒	การจ่ายค่าตอบแทน
๓	การจัดหาพัสดุ
๔	การเก็บรายได้
๕	การจ่ายค่าวัสดุค่าใช้จ่าย

/๖. <u>แผนการ</u> ...

๖. <u>แผนการตรวจสอบประจำปี</u> ควรครอบคลุมเรื่องดังต่อไปนี้

๑) วัตถุประสงค์ของหน่วยงานตรวจสอบภายในและทิศทางการดำเนินงานของหน่วยงาน

๒) ตัวชี้วัดผลการดำเนินงาน (Key Performance Indicator)

๓) ตารางการตรวจสอบ

๔) แผนงบประมาณและแผนบุคลากร

๕) รายงานกิจกรรมการตรวจสอบหรือผลการปฏิบัติงานของปีก่อน

๗. <u>มาตรฐานการปฏิบัติงาน</u>

๒๐๒๐ - การนำเสนอและอนุมัติแผนงานตรวจสอบ ต้องนำเสนอแผนและทรัพยากรที่จำเป็นต้องใช้ตลอดจนการปรับเปลี่ยนแผนที่มีนัยสำคัญต่อผู้บริหารระดับสูงและคณะกรรมการขององค์กรเพื่อสอบทานและอนุมัติ

๒๐๓๐ - การจัดการทรัพยากรต้องมั่นใจว่าทรัพยากรเหมาะสม เพียงพอ

๒๐๔๐ - นโยบายและวิธีการปฏิบัติงาน ต้องกำหนดนโยบายและวิธีการปฏิบัติงานให้ชัดเจน

๒๐๕๐ - การประสานงานควรแลกเปลี่ยนข้อมูลและประสานงานกับผู้ให้บริการด้านการให้ความเชื่อมั่นและให้คำปรึกษาอื่น

๒๒๐๐ - การวางแผนภารกิจต้องจัดทำแผนภารกิจ รวมถึงขอบเขต วัตถุประสงค์ เวลา และทรัพยากรที่ต้องใช้ในภารกิจ

๒๒๐๑ - ข้อพิจารณาในการวางแผน วัตถุประสงค์ วิธีควบคุม ความเสี่ยง ทรัพยากร การดำเนินงานตลอดจนวิธีจัดการความเสี่ยง ความเพียงพอ ประสิทธิผล และโอกาสปรับปรุงการบริหารความเสี่ยงและการควบคุมสำหรับกิจกรรม

๒๒๐๑.A๑ - ภารกิจให้บริการแก่องค์กรภายนอก ต้องทำความเข้าใจกับผู้รับบริการเป็นลายลักษณ์อักษร

๒๒๐๑.C๑ - ต้องทำความเข้าใจกับผู้รับบริการเกี่ยวกับวัตถุประสงค์ ขอบเขต ความรับผิดชอบและความคาดหวัง

หัวข้อการอบรม ครั้งที่ ๒ : IT Governance Audit Workshop

วิทยากร : นายมานิต พาณิชย์กุล CIA, CISA, CISM, CRMA

สาระสำคัญของการอบรมสรุปได้ดังนี้

๑. <u>วัตถุประสงค์</u> ประกอบด้วย ๓ ข้อ ดังนี้

๑) การขับเคลื่อน IT Governance ไปสู่มาตรฐานขั้นต่ำที่กำหนดโดยกระทรวงการคลังและแนวปฏิบัติที่ดี/สากล

๒) ขับเคลื่อนการบริหาร การควบคุมด้าน IT Governance ไปสู่มาตรฐานของ COBIT (หรือมาตรฐานอื่นๆ) ที่มุ่งไปสู่กรอบของ IT Governance โดยสั่งการจากระดับเบื้องบน

๓) การเพิ่มคุณค่าสารสนเทศ ซึ่งสามารถสร้าง Value Added ให้องค์กรได้ รวมทั้งการปฏิบัติตามกฎหมายและบริการที่มีคุณภาพ

- วัตถุประสงค์ของ IT ที่สำคัญในการดำเนินธุรกิจ
  ๑) ความสามารถของระบบและการบริการที่ดี รวดเร็ว ตรงเวลา
  ๒) ความไม่มั่นคงและความเสี่ยงลดลง เน้นการป้องกัน
  ๓) การใช้ต้นทุนในการดำเนินงานอย่างมีประสิทธิภาพ
  ๔) ความเชื่อถือได้ การควบคุมมีประสิทธิผลและตรวจสอบได้
  ๕) Strategic Alignment & Value Delivery
- การใช้เทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี
  - การปรับใช้ IT ให้เข้ากับธุรกิจ
  - IT ทำให้การดำเนินธุรกิจง่ายขึ้น และทำให้ได้รับผลประโยชน์สูงสุด
  - IT ทำให้เกิดความเชื่อถือ
  - IT ทำให้เกิดการบริหารความเสี่ยงที่เหมาะสม

องค์รวมหลัก (Domains) ของกระบวนการควบคุมกระบวนการทางเทคโนโลยีที่นำไปสู่กระบวนการบริหาร ทางธุรกิจแบบผสมผสานในการบรรลุวัตถุประสงค์ขององค์กรระดับสูงที่เชื่อมโยงกับเทคโนโลยีสารสนเทศ

องค์รวมหลัก (Domains)	
การวางแผนและจัดการองค์การ (Planning & Organization)	- การวางกลยุทธ์ และยุทธวิธี ตลอดจนการหาหนทางที่จะทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญที่จะทำให้ธุรกิจบรรลุวัตถุประสงค์ - การดำเนินงานให้เป็นไปตามวิสัยทัศน์เชิงกลยุทธ์และจำเป็นต้องมีการวางแผนงานสื่อสารและจัดการในหลายๆ ด้าน - องค์กรจำเป็นต้องมีการจัดการองค์กรที่สัมพันธ์กับโครงสร้างพื้นฐานด้านเทคโนโลยีตาม Business Processes และ IT Processes อย่างเหมาะสม
การจัดหาและการนำระบบออกใช้งานจริง (Acquisition & Implementation)	- การดำเนินงานตามกลยุทธ์ที่วางไว้ องค์กรจะต้องมีการระบุถึงเทคโนโลยีสารสนเทศต่างๆ ที่ต้องใช้ในการดำเนินงาน และจะต้องมีการพัฒนาหรือจัดซื้อจัดหาเพื่อการนำระบบออกใช้งานจริง โดยมีแผนงานรองรับอย่างเหมาะสม - จัดให้มีการผนวกรวมเทคโนโลยีสารสนเทศเข้าเป็นส่วนหนึ่งของกระบวนการทางธุรกิจ - ปรับปรุงเปลี่ยนแปลงระบบงานที่มีอยู่แล้วเพื่อให้วงจรของระบบงานเหล่านี้ดำเนินต่อไป
การส่งมอบและการบำรุงรักษา (Delivery & Support)	- เกี่ยวข้องกับการส่งมอบบริการด้านข้อมูลและสารสนเทศรวมตั้งแต่การดำเนินงานด้านการรักษาความปลอดภัย ความต่อเนื่องของการให้บริการไปจนถึงการฝึกอบรมฯ - จัดให้มีกระบวนการสนับสนุนสำหรับการส่งมอบการให้บริการทางด้าน IT และอื่นๆ - การประมวลผลข้อมูลจริงโดยระบบงานประยุกต์ (Application System) ซึ่งมักจัดอยู่ในส่วนของการควบคุมเฉพาะระบบงาน

/องค์รวม ...

องค์รวมหลัก (Domains)	
การติดตาม (Monitoring)	- กระบวนการด้านเทคโนโลยีสารสนเทศทั้งหมด จะต้องได้รับการประเมินเป็นประจำ เพื่อรับประกันได้ถึงคุณภาพและการปฏิบัติตามกฎเกณฑ์ และข้อบังคับด้านการควบคุม ทั้งจากภายนอกและภายในองค์การ - ระบุการกำกับดูแลการดำเนินงานโดยผู้บริหารในด้านกระบวนการควบคุมขององค์การ และประเมินโดยหน่วยงานอิสระทั้งจากผู้ตรวจสอบภายในและภายนอกหรือจากแหล่งทางเลือกอื่น

๒. <u>แนวทางการตรวจสอบ</u>

- การกำกับดูแลด้าน IT เกี่ยวข้องโดยตรงกับการกำกับดูแลองค์กร และความเสี่ยงด้าน IT เป็นความรับผิดชอบร่วมกันของผู้บริหารระดับสูงและคณะกรรมการบริหารองค์กร โดยผู้บริหารระดับสูงมีการวางทิศทางให้สอดคล้องกับแนวทางเชิงกลยุทธ์ขององค์กร โดยมีเป้าหมายเพื่อให้มั่นใจว่า การใช้ทรัพยากรด้าน IT มีประสิทธิภาพและเป็นที่ยอมรับ โดยผลลัพธ์ของการกำกับดูแลที่มีประสิทธิภาพ ได้แก่

๑) กลยุทธ์ด้าน IT ต้องสอดคล้องกับวัตถุประสงค์ขององค์กร

๒) มีการระบุและจัดการความเสี่ยงอย่างเหมาะสม

๓) การลงทุนด้าน IT ได้รับการจัดสรรให้เหมาะสมเพื่อส่งมอบคุณค่าให้กับองค์กร

๔) ประสิทธิภาพด้าน IT ถูกกำหนดและวัดผลรวมทั้งและรายงาน โดยใช้ตัวชี้วัดที่มีค่าเป้าหมายในการกำกับดูแล

๕) ทรัพยากรด้าน IT ได้รับการจัดการอย่างมีประสิทธิภาพ

- การกำกับดูแลด้าน IT ที่ไม่เพียงพออาจส่งผลกระทบในทางลบอย่างมีนัยสำคัญต่อองค์กร ทั้งด้านการเงินและชื่อเสียง การฟื้นตัวจากผลกระทบดังกล่าวอาจจะต้องใช้เวลาและจำนวนเงินที่สูงมาก ดังนั้นการเชื่อมโยงระหว่างผู้บริหารระดับสูงกับฝ่าย IT จึงมีความสำคัญ เนื่องจากสมัยก่อนเชื่อว่า IT ที่มีอยู่ก็เพื่อให้บริการแบบวันต่อวันเท่านั้น ซึ่งในความเป็นจริงแล้วฝ่าย IT มีความสำคัญอย่างยิ่งในการพัฒนาความได้เปรียบในการแข่งขัน รวมทั้งสนับสนุนการบรรลุเป้าหมายขององค์กรและวัตถุประสงค์เชิงกลยุทธ์

- การตรวจสอบภายในจะประเมินว่า การกำกับดูแลเทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่

๓. <u>การอบรมเชิงปฏิบัติการ (Workshop)</u>

๑) ยกประเด็นการควบคุมตามแนวทาง COBIT

๒) ร่วมอภิปราย ข้อเท็จจริงของหน่วยงาน เพื่อหาประเด็นอภิปรายหรือกำหนดแนวทางตรวจสอบร่วมกัน

๓) บันทึกข้อมูลไว้เพื่อนำไปพิจารณากลั่นกรอง หรือดำเนินการต่อไป

๔) แบ่งปันเอกสารของ ISACA เพื่อประโยชน์ในการนำไปประยุกต์ใช้ในการตรวจสอบ

จากวัตถุประสงค์ของการควบคุมและคำอธิบายวัตถุประสงค์การควบคุมของ COBIT เป็นข้อมูลจากผลการสำรวจการปฏิบัติงานของผู้ใช้งานจริง ซึ่งหน่วยงานสามารถนำมาประยุกต์โดยสร้างแนวทางการตรวจสอบธรรมาภิบาลด้าน IT และนำไปพัฒนา Audit Program ได้ตามความเหมาะสม

/หัวข้อ ...

หัวข้อการอบรม ครั้งที่ ๓ : IT Governance Audit

วิทยากร : นายวราฤทธิ์ แสงแดง CIA, CISA บริษัท ศูนย์ประมวลผล จำกัด

สาระสำคัญของการอบรมสรุปได้ดังนี้

ธรรมาภิบาล (Governance) ประกอบด้วย (๑) ธรรม = คุณธรรม ความดี

(๒) อภิบาล = บำรุงรักษา, ปกปักรักษา, คุ้มครอง

ธรรมมาภิบาล หมายถึง การปกครอง การบริหาร การจัดการการควบคุมดูแลกิจการต่างๆ ให้เป็นไปในครรลองธรรม นอกจากนี้ยังหมายถึงการบริหารจัดการที่ดี ซึ่งสามารถนำไปใช้ได้ทั้งภาครัฐและเอกชน โดยบางครั้งใช้คำว่า “การกำกับดูแลที่ดี (Good Governance)”

๑) หลักนิติธรรม (The Rule of Law) การปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับต่างๆ โดยถือว่าเป็นการปกครองภายใต้กฎหมายมิใช่ตามอำเภอใจ หรืออำนาจของตัวบุคคล

๒) หลักคุณธรรม (Morality) การยึดมั่นในความถูกต้อง ดีงาม เพื่อให้บุคลากรมีความซื่อสัตย์ จริงใจ ขยัน อดทน มีระเบียบ วินัย

๓) หลักความโปร่งใส (Accountability) การทำงานด้วยความโปร่งใส เปิดเผยข้อมูลข่าวสารอย่างตรงไปตรงมา สามารถตรวจสอบความถูกต้องได้อย่างชัดเจน

๔) หลักการมีส่วนร่วม (Participation) การเปิดโอกาสให้บุคลากรหรือผู้มีส่วนเกี่ยวข้อง มีส่วนร่วมตัดสินใจในการดำเนินการต่างๆ เช่น เป็นคณะกรรมการ คณะอนุกรรมการ และหรือคณะทำงานโดยร่วมปรึกษาวางแผน ปฏิบัติงาน และเคารพในความคิดเห็นที่แตกต่าง

๕) หลักความรับผิดชอบ (Responsibility) การตระหนักในสิทธิและหน้าที่ ความสำนึกในความรับผิดชอบต่อสังคม การใส่ใจปัญหาการบริหารจัดการ การกระตือรือร้นในการแก้ปัญหา รวมทั้งความกล้าที่จะยอมรับผลปฏิบัติงานจากกระทำของตนเอง

๖) หลักความคุ้มค่า (Cost - effectiveness or Economy) การบริหารจัดการและใช้ทรัพยากรด้วยความประหยัด คุ้มค่า เพื่อให้เกิดประโยชน์สูงสุดแก่ส่วนรวม และรักษาทรัพยากรแบบสมบูรณ์ยั่งยืน

Governance ต่างจาก Management อย่างไร

- Governance การสร้างความเชื่อมั่นว่าองค์กรจะบรรลุวัตถุประสงค์ด้วยการประเมินความต้องการของผู้มีส่วนได้ส่วนเสีย เงื่อนไขและทางเลือกต่างๆ กำหนดทิศทางด้วยการกำหนดลำดับความสำคัญและการตัดสินใจ การติดตามดูแลผลการประกอบการ และความก้าวหน้าของงานตามทิศทางที่ได้กำหนดไว้
- Management การทำหน้าที่วางแผนสร้าง ดำเนินการและติดตามดูแลกิจกรรมต่างๆ ให้สอดคล้องเป็นแนวเดียวกันกับที่คณะกรรมการธรรมาภิบาลได้กำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

COBIT Control Objectives for Information and Related Technology

- พัฒนาขึ้นโดย ISACA และ IT Governance Institute เพื่อองค์กรที่ต้องการมุ่งสู่การเป็น “ไอทีภิบาล” หรือ “IT Governance”
- COBIT เป็นแนวคิดและแนวทางปฏิบัติสำหรับผู้บริหารระบบสารสนเทศ และขณะเดียวกันก็เป็นแนวทางปฏิบัติสาหรับตรวจสอบระบบสารสนเทศด้วย
- โครงสร้างของ COBIT มี ๓๗ กระบวนการใน ๕ Domain
- เป็น Framework สามารถ Download ได้ที่ Web Site ของ ISACA

หลักการของ COBIT ๕ ข้อ

๑) Meeting Stakeholder Needs ระบุและกำหนดวิธีสร้างคุณค่าที่สอดคล้องกับความต้องการของผู้มีส่วนได้ส่วนเสีย

๒) Converging the Enterprise End to End การระบุสิ่งที่ต้องการจะทำผ่านกระบวนการกำกับดูแล

/๓) Applying ...

๓) Applying a Single integrated Framework ใช้แนวทางปฏิบัติเดียวกันหมดทั้งองค์กร

๔) Enabling a Holistic Approach สร้างมุมมองภาพรวมของการกำกับดูแลด้าน IT

๕) Separating Governance from Management แบ่งแยกกระบวนการบริหารออกจากการกำกับดูแล

ปัจจัยก่อเกิดการบรรลุเป้าหมายระดับองค์กร (๗ Enablers)

๑) หลักเกณฑ์, นโยบาย, แนวทางปฏิบัติ (Principles, Policies, Frameworks) หมายถึง แนวคิดหลัก นโยบายและแนวทางในการปฏิบัติการดำเนินงานเพื่อเป็นเครื่องมือที่ถูกนำมาใช้ควบคุมองค์กรในภาพรวม ซึ่งเป็นหน้าที่ของผู้บริหารระดับสูงต้องกำหนดนโยบายให้ชัดเจน

๒) กระบวนการ (Processes) องค์กรต้องมีกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ ซึ่งจะนำไปสู่การบรรลุซึ่งเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและเป้าหมายระดับองค์กรได้ MAP process เข้าสู่ “IT Related Goals”

๓) โครงสร้างบุคลากร (Organizational structures) หมายถึง ส่วนของโครงสร้างขององค์กรในการบริหารจัดการก็เป็นเรื่องสำคัญที่ผู้บริหารระดับสูง (C-level) รวมถึง Board of Director ต้องใส่ใจกับเรื่อง IT Governance และ Enterprise Governance

๔) วัฒนธรรม จริยธรรม และความประพฤติ (Culture, ethics, behaviors) เน้นไปที่บุคลากรและองค์กรในเรื่องของวัฒนธรรมองค์กร ทัศนคติของพนักงานและผู้บริหารระดับสูง

๕) ข้อมูล (Information) หมายถึง "สารสนเทศ" หรือ "ข้อมูล" ที่เราต้องจัดเก็บดูแลเพื่อนำมาใช้ประโยชน์ในองค์กร

๖) โครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service Infrastructure Applications) หมายถึง โครงสร้างพื้นฐาน (Infrastructure), เทคโนโลยี (Technology) และโปรแกรมประยุกต์ (Applications) ประกอบเป็นระบบสารสนเทศ (Information System) ที่ถูกนำมาใช้ในการสนับสนุนการปฏิบัติงานในองค์กรและการประกอบธุรกิจ

๗) ทักษะ ความรู้ และความสามารถของบุคลากร (People Skills and competencies) มุ่งเน้นไปที่สมรรถนะของบุคลากรในองค์กร หากองค์กรมีพนักงานที่มีคุณภาพก็จะช่วยเสริมให้บรรลุเป้าหมายในภาพรวมขององค์กรได้ง่ายยิ่งขึ้น มุ่งเน้นเรื่อง “Soft Skills”

ตัวอย่างแนวทางการกำกับดูแลบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (IT Governance Practice) ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ มีรายละเอียด ดังนี้

- การกำหนดกรอบการกำกับดูแลและบริหารจัดการ (Governance Framework Setting and Maintenance)

เพื่อให้การกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศมีความสอดคล้องกับวัตถุประสงค์ขององค์กร มีประสิทธิผล มีความโปร่งใส และเป็นไปตามกฎหมายและข้อบังคับต่างๆ ผู้ประกอบธุรกิจควรมีการกำหนดและจัดทำนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี เพื่อกำหนดกรอบการกำกับดูแลระบบและกระบวนการทางด้านเทคโนโลยีสารสนเทศ โดยนโยบายดังกล่าวประกอบด้วยหัวข้อ ดังนี้

๑) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

๒) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรให้ได้เพียงพอตามที่กำหนดไว้

๓) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ขั้นตอนในการจัดทำนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี อาจดำเนินการดังนี้

- วิเคราะห์และระบุถึงปัจจัยสภาพแวดล้อมภายในและภายนอกองค์กร ทั้งด้านกฎหมาย ระเบียบข้อบังคับและภาระผูกพันของสัญญาต่างๆ รวมทั้งแนวโน้มทางธุรกิจที่อาจมีผลต่อการออกแบบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

/• พิจารณา ...

• พิจารณาระดับความสำคัญของเทคโนโลยีสารสนเทศ รวมทั้งบทบาทของเทคโนโลยีสารสนเทศต่อการดำเนินธุรกิจขององค์กร

• พิจารณาการนำเทคโนโลยีสารสนเทศมาใช้และประเมินผลกระทบจากการดำเนินการดังกล่าวที่มีต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกขององค์กร รวมทั้งความสอดคล้องกับเป้าหมายและวัตถุประสงค์โดยรวมขององค์กร

• พิจารณานัยสำคัญของสภาพแวดล้อมของการควบคุมโดยทั่วไปของผู้ประกอบธุรกิจที่มีต่อเทคโนโลยีสารสนเทศ

• กำหนดหลักการสำคัญที่จะใช้เป็นแนวทางสำหรับการออกแบบการกำกับดูแลและการตัดสินใจที่สำคัญเกี่ยวกับเทคโนโลยีสารสนเทศ รวมทั้งทำความเข้าใจเกี่ยวกับวัฒนธรรมขององค์กรในการตัดสินใจและพิจารณากำหนดรูปแบบการตัดสินใจเกี่ยวกับเทคโนโลยีสารสนเทศที่เหมาะสมสำหรับองค์กร (Optimal Decision-Making Model) อาจมีรูปแบบปัจจัยและลำดับความสำคัญในการพิจารณาและตัดสินใจที่แตกต่างกันไปในแต่ละองค์กร เช่น ปัจจัยด้านผลประโยชน์ตอบแทน ปัจจัยด้านผลกระทบต่อบุคลากร ปัจจัยด้านการปฏิบัติตามข้อกำหนดทางกฎหมาย เป็นต้น

• กำหนดระดับการมอบหมายอำนาจอนุมัติ รวมทั้งข้อกำหนดที่เกี่ยวข้องสำหรับการตัดสินใจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่เหมาะสม

- การจัดการความเสี่ยงที่เหมาะสม (Risk Optimization)

เพื่อให้ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอยู่ในระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Appetite) และลดความผิดพลาดที่อาจเกิดขึ้นจากการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ ผู้ประกอบธุรกิจควรมีกระบวนการดังนี้

๑) การจัดทำนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องและเป็นไปในแนวทางเดียวกันกับนโยบายและการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

๒) การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

๓) การกำหนดความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) จากความเสี่ยงที่ได้รวบรวมในขั้นตอนข้างต้น โดยอาจพิจารณาจากระดับความเสี่ยงที่ผู้ประกอบธุรกิจสามารถยอมรับได้ รวมถึงวัฒนธรรมองค์กรหรือระดับการยอมรับความเสี่ยงของคณะกรรมการบริษัท

๔) การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ หลังจากกำหนดสถานการณ์ความเสี่ยงและกำหนดปัจจัยความเสี่ยงที่เหมาะสม รวมทั้งกำหนดความเสี่ยงที่สามารถยอมรับได้แล้ว จึงประเมินถึงโอกาสเกิดและผลกระทบของเหตุการณ์ความเสี่ยงที่กำหนดไว้ โดยอาจจัดทำในรูปแบบของแผนภาพความเสี่ยง (Risk Map) และทำทะเบียนความเสี่ยง (Risk Register) เพื่อบรรยายข้อมูลรายละเอียดของความเสี่ยง จากนั้นจึงจัดทำโครงร่างของความเสี่ยง (Risk Profile) เพื่อรวบรวมความเสี่ยงที่เกี่ยวข้องทั้งหมด

๕) การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ กรณีที่ความเสี่ยงที่หลงเหลืออยู่เกินกว่าระดับที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการตอบสนองต่อความเสี่ยงนั้น (Risk Response) โดยการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงสามารถดำเนินการได้ใน ๔ ลักษณะ ได้แก่ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance), การยอมรับความเสี่ยง (Risk Acceptance), การร่วมรับความเสี่ยง/ถ่ายโอน (Risk Sharing/Transfer) และการลดความเสี่ยง (Risk Mitigation)

๖) การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) รายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไปประกอบการตัดสินใจได้ รวมถึงรายงานผลการบริหารจัดการความเสี่ยง ประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบจากรายการความเสี่ยง

/๗) การกำหนด ...

๗) การกำหนดหน้าที่และความรับผิดชอบของบุคลากร ผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคณะกรรมการของผู้ประกอบธุรกิจควรเป็นผู้รับผิดชอบ (Accountable person) และผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยง (Responsible person) เป็นผู้ทำหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ผู้บริหารหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ในการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

- การส่งมอบผลประโยชน์ (Benefit Delivery) และการใช้ทรัพยากรสารสนเทศให้ได้ประโยชน์สูงสุด (Resource Optimization) เพื่อให้มีการใช้ทรัพยากรสารสนเทศอย่างคุ้มค่าและตอบสนองต่อความต้องการทางด้านธุรกิจอย่างมีประสิทธิภาพและมีประสิทธิผล โดยมีต้นทุนในระดับที่ยอมรับได้ ผู้ประกอบธุรกิจควรมีการจัดทำแผนกลยุทธ์และนโยบาย ดังนี้

๑) การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ และงบประมาณด้านเทคโนโลยีสารสนเทศ เช่น ความต้องการของผู้มีส่วนได้ส่วนเสีย, ความคุ้มค่าในการใช้งานทรัพยากรสารสนเทศ, ความสอดคล้องของกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศและกลยุทธ์ขององค์กรในภาพรวม บทบาทหน้าที่ ความรับผิดชอบและโครงสร้างการตัดสินใจในการดำเนินการ การจัดระดับความสำคัญในการตัดสินใจลงทุนทางด้านเทคโนโลยีสารสนเทศ, การจัดทำงบประมาณอย่างรอบคอบ ครอบคลุมและรัดกุม ต้นทุนทางตรง/ทางอ้อม แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ หรือด้านเทคโนโลยีสารสนเทศและงบประมาณด้านเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมาย และสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ รวมทั้งมีการมอบหมายให้ผู้บริหารนำไปปฏิบัติเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศในภาพรวมสอดคล้องกับแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ

๒) การจัดทำนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ และการจัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศพิจารณา และกหนดกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศสหรับปัจจุบัน และในอนาคตทางเลือกต่างๆ กำหนดหลักเกณฑ์เพื่อใช้เป็นแนวทางในการจัดสรรและบริหารทรัพยากรสารสนเทศ รวมทั้งขีดความสามารถจัดทำแผนการจัดสรรทรัพยากรสารสนเทศที่สอดคล้องกับการจัดสรรทรัพยากรขององค์กร รวมทั้งการบริหารทรัพยากรบุคคลโดยรวมขององค์กรด้วย กหนดเป้าหมาย ตัวชี้วัดความสเร็จและกระบวนการที่เกี่ยวข้องสำหรับการจัดสรรทรัพยากรสารสนเทศ กำหนดหลักเกณฑ์ในการป้องกันรักษาทรัพยากรสารสนเทศ ที่รวมถึงการสูญเสียทรัพยากรบุคคลที่สำคัญด้วย ติดตามผลการทำงานของทรัพยากรสารสนเทศโดยเทียบกับเป้าหมายที่วางไว้ ถ้ามีข้อบกพร่องหรือผลการทำงานที่ไม่เป็นไปตามเป้าหมาย ควรมีการตรวจสอบหาสาเหตุและวางแผนการแก้ไขอย่างเหมาะสม

- ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency) เพื่อให้มั่นใจว่าการรายงานและการสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศกับผู้มีส่วนได้ส่วนเสียมีประสิทธิผลและทันเวลา การดำเนินงานโดยรวมควรมีการพัฒนาอย่างต่อเนื่องและวัตถุประสงค์รวมทั้งกลยุทธ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนกลยุทธ์ขององค์กรซึ่งแนวทางปฏิบัติที่ควรพิจารณามีดังนี้

๑) การประเมินความต้องการของผู้มีส่วนได้ส่วนเสียในการรายงานผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศ

• ผู้ประกอบธุรกิจควรพิจารณาข้อกำหนดด้านการรายงานภาคบังคับ (Mandatory Reporting) ทั้งในปัจจุบันและอนาคตที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศภายในองค์กร รวมทั้งขอบเขตและรอบระยะเวลาในการรายงานที่เหมาะสม

• นอกเหนือจากประเด็นข้างต้น การรายงานยังอาจต้องพิจารณาถึงความต้องการด้านการรายงานสำหรับผู้มีส่วนได้ส่วนเสียอื่นๆ ทั้งในปัจจุบันและอนาคตที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศในองค์กร รวมถึงขอบเขตและเงื่อนไขในการรายงานที่แตกต่างกัน

/• ผู้ประกอบ ...

• ผู้ประกอบธุรกิจควรจัดให้มีหลักเกณฑ์การรายงานต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร รวมทั้งรูปแบบและช่องทางการสื่อสารอย่างเหมาะสม

๒) การสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสม

• ผู้ประกอบธุรกิจควรมีการกำหนดกลยุทธ์ในการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร

• ควรมีการกำหนดวิธีการสอบทานเพื่อให้มั่นใจว่าข้อมูลการรายงานเป็นไปตามหลักเกณฑ์สำหรับข้อกำหนดของการรายงานภาคบังคับของผู้ประกอบธุรกิจทั้งหมด

• ควรมีกระบวนการในการตรวจสอบความถูกต้องและอนุมัติรายงานภาคบังคับ

• มีกระบวนการและลำดับชั้นการรายงาน

๓) การติดตามการสื่อสารกับผู้มีส่วนได้ส่วนเสีย

• ผู้ประกอบธุรกิจควรมีการประเมินความมีประสิทธิผลของการรายงานผลอย่างสม่ำเสมอเพื่อให้มั่นใจในความถูกต้องและความน่าเชื่อถือของรายงานภาคบังคับที่จัดทำขึ้น

• ผู้ประกอบธุรกิจควรมีการประเมินความมีประสิทธิผลของวิธีการสื่อสารและผลลัพธ์ของการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กรและประเมินว่าการสื่อสารดังกล่าว สามารถตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียที่หลากหลายอย่างครบถ้วน

กลุ่มตรวจสอบภายใน สำนักงานบริหารหนี้สาธารณะ
๑ กันยายน ๒๕๖๕