# การสัมมนาหัวข้อ “การพัฒนาเทคโนโลยีดิจิทัล (Digital Technology : DT)”



TRIS CORP Idea Solution Performance

16 กันยายน 2563

# กำหนดการสัมมนาการ
# ด้านการพัฒนาเทคโนโลยีดิจิทัล
# (Digital Technology : DT)
# ของระบบประเมินผลฯ ใหม่
# (State Enterprise Assessment Model: SE-AM)

| | |
|---|---|
| 09.00 – 09.30 | ลงทะเบียน |
| 09.30 – 10.30 | การชี้แจงคำถามที่พบบ่อย ระบบประเมินผลฯใหม่ หัวข้อ "การพัฒนาเทคโนโลยีดิจิทัล (Digital Technology : DT)" |
| 10.30 - 10.50 | พักรับประทานอาหารว่าง |
| 10.50 - 12.00 | ถาม - ตอบ |
| 12.00 – 13.00 | รับประทานอาหารกลางวัน |

# ประเด็นคำถาม

Q: รส. ไม่มีบอร์ดด้าน IT เป็นการเฉพาะ มีแต่คณะกรรมารด้าน IT ที่เป็นหัวหน้าหน่วยงานในสังกัด ควรจะเชิญคนใดคนหนึ่งจากบอร์ดที่มีความรู้ด้าน IT มาเป็นประธานของชุดคณะกรรมการ IT ของหน่วยงานได้หรือไม่

A: ขึ้นอยู่กับการพิจารณาขององค์กร แนวทาง Best Practices ขององค์กรขนาดใหญ่ โครงสร้างการกำกับด้านดิจิทัลควรมีคณะกรรมการ รส. มาเป็นองค์ประกอบของคณะกรรมการดิจิทัล เพื่อขับเคลื่อนการนำดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร แต่ถ้าองค์กรขนาดเล็กอาจไม่จำเป็น อย่างไรก็ตาม โดยลักษณะของ รส. ของเรา การจะขับเคลื่อนเรื่องใดๆ ให้มีประสิทธิภาพ ส่วนมากก็ควรจะได้รับการสนับสนุนจากคณะกรรมการ รส. เกณฑ์การประเมินจะไม่จำกัดรูปแบบโครงสร้างการกำกับดูแล แต่จะดูผลลัพธ์ที่มีประสิทธิภาพของการกำกับดูแลมากกว่า

Q: คู่มือหน้า 136 ระดับ 3 บอกว่า รส. มีการถ่ายทอดกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปีแก่ผู้รับผิดชอบและผู้มีส่วนได้เสีย หมายถึงว่าการถ่ายทอดกระบวนการจัดทำหรือขั้นตอนการจัดทำแผน 2 แผน หรือถ่ายทอดเล่มแผนที่เสร็จแล้ว

A: ทั้ง 2 มุม ใครเกี่ยวข้องกับกระบวนการจัดทำ เราก็ต้องสื่อสารให้เข้าใจเพื่อให้การสนับสนุนในการจัดทำ เช่นเดียวกันเมื่อแผนฯ แล้วเสร็จก็ต้องสื่อสารผู้เกี่ยวข้องให้รับทราบ

Q: ให้อธิบายการดูผลลัพธ์ที่มีประสิทธิภาพของการกำกับดูแลด้วย พร้อมช่วยยกตัวอย่างที่นำไปใช้ได้

A: หัวใจของกระบวนการกำกับดูแลด้านการพัฒนาเทคโนโลยีดิจิทัลตามเกณฑ์จะมี 3 เรื่อง คือ การบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม การดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส และการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ตัวชี้วัดประสิทธิผลที่จะตอบว่าการกำกับมีคุณภาพ เช่น ร้อยละความสำเร็จของโครงการตามแผนปฏิบัติการดิจิทัล จำนวนพนักงานที่ละเมิดกฎระเบียบข้อบังคับด้านการกำกับดูแลด้านดิจิทัล ร้อยละโครงการที่ดำเนินการตามกรอบกำกับดูแลด้านดิจิทัลเรื่องต่างๆ เช่นการวิเคราะห์ความคุ้มค่าโครงการ การจัดสรรทรัพยากรด้านต่างๆ เป็นต้น ปัจจัยเสี่ยงด้านดิจิทัลที่บริหารจัดการได้

# ประเด็นคำถาม

Q: การกำหนดกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการ Digital Governance จำเป็นต้องมีการจัดทำนโยบายหรือไม่

A: โดยปกติการกำกับดูแลจะต้องมีนโยบายกำกับดูแลฯ ที่ครอบคลุมการพัฒนาเทคโนโลยีดิจิทัลทั้งองค์ เพื่อนำไปเป็นกำหนดแนวทางในการปฏิบัติในแต่ละด้าน ซึ่งหัวใจหลักของการกำกับมี 3 อย่างคือ การบริหารจัดการทรัพยากรอย่างเหมาะสม การดำเนินงานที่มีประสิทธิภาพและโปร่งใส และการบริหารจัดการความเสี่ยงด้านการพัฒนาเทคโนโลยีดิจิทัล

Q: หากมีการปรับปรุงคำสั่งอำนาจหน้าที่คณะ IT Steering แต่ไม่ได้ระบุอำนาจหน้าที่ว่าให้รายงานคณะกรรมการรัฐวิสาหกิจและไม่ได้ระบุความถี่ แต่จะรายงานให้ผู้อำนวยการแทนซึ่งมีฐานะเป็นคณะกรรมการท่านหนึ่งและเป็นเลขานุการคณะกรรมการฯ ด้วย เพื่อนำเข้าที่ประชุมให้รับทราบ จะถือว่าได้ปฏิบัติตามเกณฑ์แล้วหรือไม่

A: เกณฑ์ไม่กำหนดรูปแบบโครงสร้างและกระบวนการ ขึ้นอยู่กับรัฐวิสาหกิจ แต่จะต้องมีแนวทางที่กำหนดไว้อย่างชัดเจนในทุกเรื่อง และที่สำคัญต้องสามารถบอกได้ว่าสิ่งที่เราดำเนินการตามแนวทางนั้นมีประสิทธิภาพ เช่น กำหนด KPI วัดประสิทธิผลของกระบวนการ

Q: จากสถานการณ์ระบาด covid ทำให้บางสถานที่พนักงานต้อง work from home นี่มีเกณฑ์ข้อ 6.4 การบริหารจัดการความต่อเนื่องทางธุรกิจ และอาจโยงไปเกี่ยวกับเกณฑ์ข้ออื่นด้วย มีแนวโน้มจะถูกเอามาพิจารณาสอบถามถึงความพร้อมการจัดการในสถานการณ์จริงของแต่ละรัฐวิสาหกิจในการตรวจประเมินด้วยไหม

A: ถูกต้อง เพราะการวิเคราะห์ Business Impact Analysis โดยปกติจะต้องวิเคราะห์ให้ครบถ้วนรอบด้านภัยพิบัติต่างๆ เหตุการณ์ไม่คาดคิด โรคระบาด และอื่นๆ ล้วนแล้วจะถูกนำมาใช้ในการพิจารณา เพื่อหาแผนการรองรับในกรณีที่เกิดเหตุการณ์นั้นๆ

# ประเด็นคำถาม

Q: เรื่อง BCM ที่ระดับ L3 ต้องมีการประเมินการรับรู้ฯ อันนี้คือประเมินใคร แล้วต้องประเมินระดับไหน

A: หลักการพื้นฐานของการประเมินข้อ DT ทุกกระบวนการจะต้องมีการวิเคราะห์ ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการให้ครบถ้วน เพื่อถ่ายทอดแนวทางของกระบวนการ/ผลผลิตของกระบวนการ ให้ผู้มีส่วนได้ส่วนเสียรับรู้ และมีการประเมินการรับรู้ดังกล่าวด้วย โดยที่แต่ละกระบวนการจะมีผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องมากน้อยต่างกันไปขึ้นอยู่ที่การวิเคราะห์

Q: BCM ตามเกณฑ์ด้านที่ 5 ข้อ 6.4 หมายถึงเฉพาะที่เกี่ยวข้องกับ IT หรือว่าต้องบริหารความต่อเนื่องทางธุรกิจทุกเรื่อง ซึ่งรวมถึงการบริหารจัดการพนักงานในช่วงที่โควิดระบาดในตอนนี้ด้วยหรือเปล่า เพราะเคยได้ยินมาว่าต้องดูทุกเรื่อง จึงขอสอบถามเพื่อความชัดเจน

A: ข้อนี้ดู BCM องค์กร ดังนั้นจะดูทั้ง BCP และ DRP คือ ไม่ใช่ดูแค่ IT ดังนั้นการจัดการต่อสภาวะโรคระบาดก็ถือว่าเกี่ยวข้องด้วย โดยปกติการวิเคราะห์ Business Impact Analysis BIA โรคระบาดควรถูกนำมาวิเคราะห์ด้วยอยู่แล้ว แต่ที่ผ่านมาไม่เคยมีเหตุการณ์รุนแรงแบบนี้เราอาจละเลยกัน ดังนั้นจากเหตุการณ์นี้ การประเมินผลในส่วนนี้ต้องดูการจัดการของรัฐวิสาหกิจต่อเหตุการณ์นี้ด้วย

Q: หัวข้อ 6.4 การบริหารจัดการความต่อเนื่องทางธุรกิจระดับ 2 การวิเคราะห์ BIA ที่ครอบคลุมระบบงานที่สำคัญอย่างครบถ้วน (ทั้ง 8 เกณฑ์) อยากทราบว่า 8 เกณฑ์คืออะไร

A: ทั้ง 8 Enablers

# ประเด็นคำถาม

Q: งานจ้างที่ปรึกษาเพื่อจัดทำแผนใดแผนหนึ่งหรือเพื่อจัดทำขอบเขตงานหรือคุมงานที่เกี่ยวกับงานไอที ต้องมีการวิเคราะห์ความคุ้มค่าด้วยหรือไม่ มองว่าคิดเป็นตัวเงินไม่ได้ ขอคำแนะนำด้วย

A: การวิเคราะห์ความคุ้มค่าในการลงทุนด้านการพัฒนาเทคโนโลยีดิจิทัล องค์กรจะต้องมีแนวทางที่ชัดเจนว่าโครงการแบบไหนประเภทอะไรมูลค่าเท่าไหร่ถึงจะต้องมีการวิเคราะห์ความคุ้มค่า เช่น การลงทุนเปลี่ยนอุปกรณ์เดิมที่ชำรุด ก็ไม่จำเป็นต้องวิเคราะห์ เป็นต้น การวิเคราะห์ความคุ้มค่าก็ไม่ใช่ด้านการเงินเท่านั้น สามารถวิเคราะห์ผลประโยชน์ที่ได้รับในรูปแบบอื่นได้ ดังนั้นสรุปคือ ขึ้นอยู่ที่องค์กรกำหนดแนวทาง แต่การประเมินก็จะดูความสมเหตุสมผลของการกำหนดหลักเกณฑ์ดังกล่าวเป็นส่วนประกอบด้วย รวมถึงผลการวัดประสิทธิผลของแนวทางนั้นด้วย ในกรณีโครงการจ้างที่ปรึกษามาดำเนินการเรื่องใดเรื่องหนึ่งก็ต้องสามารถประเมินผลลัพธ์จากโครงการดังกล่าวได้

Q: Enabler 5 ในส่วนเฉพาะข้อ 5 ที่เป็นเรื่อง ISMS ไปรษณีย์ไทย ทำ ISO 27001 โดยมีขอบเขตเฉพาะสายงานดิจิทัล ประเมินแล้วครบถ้วนตามที่ SE-AM กำหนด คำถามคือ ต้องขยาย ISO 27001 ไปทั้งองค์กร จึงจะได้คะแนนหรือเปล่า

A: ถูกต้อง การประเมินเป็นการประเมิน ISMS ขององค์กร ดังนั้นกรณีที่บางองค์ได้ Cert. ISO 27001 แค่บางพื้นที่ จะต้องนำแนวทางดังกล่าวใช้ครอบคลุมทั่วถึงทั้งองค์กร แต่การนำแนวทาง ISO 27001 ไปใช้ทั่วทั้งองค์กรไม่จำเป็นต้อง Certified

# ประเด็นคำถาม

Q: กรณีอยากได้ ระดับ 3 ในหลายหัวข้อ ให้มีการถ่ายทอดและประเมินผลไปยังผู้มีส่วนได้ส่วนเสียให้ครบ นอกจากบันทึกเวียนกับแบบสอบถาม มีมุมอื่นอีกไหม

A: การสื่อสารถ่ายทอดไปยังผู้มีส่วนได้ส่วนเสียต้องมีการวัดการรับรู้ด้วย ไม่ว่าจะใช้วิธีการใด สุดท้ายต้องประเมินประสิทธิผลของการรับรู้ด้วย โดยเฉพาะ ISMS มีวิธีการรูปแบบการสื่อสารทั้งทางตรง เช่น หนังสือเวียน อบรม แบบสอบถาม และอื่นๆ สื่อสารทางอ้อม เช่น ลองส่งอีเมล์ปลอม phishing mail แล้วดูร้อยละของเมล์ที่ส่งไปว่าพนักงานติดกับเท่าไหร่ เป็นต้น แล้วต้องมาสรุปว่ามีการรับรู้เรื่อง ISMS มากน้อยแค่ไหน ซึ่งหัวข้ออื่นในส่วนของการพัฒนาเทคโนโลยีดิจิทัลก็ต้องมีกระบวนการเหมือนกัน

Q: อยากจะขอความชัดเจนหัวข้อ 6.4 การบริหารจัดการความต่อเนื่องทางธุรกิจ ทางหน่วยงานเพิ่งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) เสร็จเรียบร้อย อยากทราบว่าตรงกับวัตถุประสงค์ข้อนี้หรือเปล่าที่ให้ รส. จัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพราะกำลังสับสนว่าให้ รส. จัดทำแผน BCM หรือ BCP

A: BCM คือ Business Continuity Management คือ การบริหารจัดการความต่อเนื่องทางธุรกิจ ส่วน BCP คือ Business Continuity Plan คือ แผนบริหารความต่อเนื่องทางธุรกิจ ดังนั้น BCM คือการจัดการ ซึ่งจะประกอบด้วย BCP และ DRP (Disaster recovery plan)

Q: คะแนน BCM จะอยู่ใน Enabler 3 หรือ Enabler 5

A: อยู่ Enable 5 การพัฒนาเทคโนโลยีดิจิทัลที่เดียว เป็นคะแนนของ BCM องค์กร ไม่ใช่เฉพาะ IT

# ประเด็นคำถาม

Q: ขอสอบถามด้าน DT ประเด็น 2.3 การจัดการคุณภาพ QM จากการอ่านคู่มือ จะพูดถึง QMS (Quality Management System) (ซึ่งผมก็นึกถึง ISO9001) แต่ภาพประกอบในคู่มือ มีภาพ PQM (Project Management System) จึงอยากขอรับคำแนะนำว่า รส. ควรเอามุมไหนมาตอบโจทย์นี้

A: จริงๆ แล้วคือภาพรวม QMS ถูกต้องแล้ว ตัวอย่างในคู่มือคือการนำ QMS มาใช้กับ Project Management ซึ่งก็จะเป็น Project Quality Management จะสังเกตเห็นได้ว่าจะมีการใช้ Quality Management Tools and Techniques ที่หลากหลายเครื่องมือ ซึ่งล้วนแล้วจะเป็นองค์ประกอบของกระบวนการ QMS ดังนั้นการประเมินจะมองภาพรวม QMS ของการพัฒนาเทคโนโลยีดิจิทัลขององค์กร และจะดู OUTPUT/OUTCOME ที่เกิดขึ้นว่านำไปใช้อย่างไรในส่วนต่างๆ ที่เกี่ยวกับการพัฒนาเทคโนโลยีดิจิทัลอย่างไร

Q: ภาพรวม 2.3 ของ DT คือ QMS ภาพ PQM คือตัวอย่างหนึ่งเท่านั้น ถ้าบอกว่าระบบดิจิทัลของ รส. ทำ ISO9001 (QMS แบบหนึ่ง) ในทุกกระบวนการ ก็ถือว่าตอบโจทย์ได้

A: ถูกต้อง แต่พอการประเมินเป็นกระบวนการก็ต้องดูว่า IS 09001 อย่างเดียวเพียงพอไหม โดยต้องมีการประเมินประสิทธิผลของกระบวนการด้วย ซึ่งถ้าเพียงพอก็ไม่มีปัญหา แต่ถ้าไม่เพียงพอควรจะต้องนำ Quality Management Tools and Techniques อื่นๆ มาพิจารณาเพิ่มเติม

Q: สอบถามเกณฑ์ ในหัวข้อที่ 5.5 IT asset , data and infomation security management) กับ ในหัวข้อที่ 6.1 การบริหารทรัพย์สินด้านสารสนเทศ (IT asset management)มีความหมายแตกต่างกันอย่างไร

A: จริงๆ ไม่ต่าง ทำ 1 ได้ถึง 2 แต่เนื่องจากมุมมองความปลอดภัยและความพร้อมใช้ของเทคโนโลยีสารสนเทศสะท้อนผ่าน IT asset management จึงมีอยู่ทั้ง 2 ที่เพื่อครบองค์ประกอบและตอบวัตถุประสงค์ของแต่ละข้อ

# ประเด็นคำถาม

Q: IT Asset ตามเกณฑ์ ในหัวข้อที่ 5.5 กับ หัวข้อที่ 6.1 คือตัวเดียวกันไหม มองเป็น IT Asset ทั้งหมดขององค์กร หรือมองเป็นแยกตามเกณฑ์รายข้อ เป็น Asset ของระบบ ISMS กับ Asset ของระบบ BCM

A: ตัวเดียวกันถ้าองค์กรทำครบทั้งองค์กรได้คะแนนทั้ง 2 จุด

Q: ในข้อ 2.3 การจัดการด้านคุณภาพ มีการกล่าวถึงการตรวจสอบด้านดิจิทัล (Digital Audit) หรือ Computer Audit และหัวข้อ 5.5 Information security management system audit ตามมาตรฐาน ISO/IEC 27001:2013 ทั้ง 2 หัวข้อหมายถึงการทำ IT Audit ใช่หรือไม่ หรือว่ามีแนวทางในการตรวจสอบที่ต่างกัน

A: การทำ ISMS Audit เป็นส่วนหนึ่งของ Computer หรือ Digital Audit แต่เนื่องจาก Computer หรือ Digital Audit จะวางแผนการตรวจสอบจากฐานความเสี่ยง ซึ่งบางระบบจะไม่ได้ถูกตรวจสอบทุกปี แต่อย่างไรก็ตาม ตามแนวปฏิบัติที่ดี ISMS Audit จะต้องทำการตรวจสอบทุกปี

Q: ขอสอบถามการพัฒนาเทคโนโลยีดิจิทัล เรื่องการประเมินการรับรู้กระบวนการจัดทำแผนปฏิบัติการดิจิทัล หมายถึงเราต้องประเมินถึงความเข้าใจในกระบวนการจัดทำแผนฯ หรือประเมินแค่การรับรู้ว่ามีกระบวนการจัดทำแผนฯ

A: ทั้ง 2 ประเด็น การประเมินข้อ DT ทุกหัวข้อจะมีการประเมินการสื่อสารกระบวนการต่างๆให้ผู้มีส่วนได้ส่วนเสียแต่ละกระบวนการทราบ โดยผู้มีส่วนได้ส่วนเสียแต่ละกระบวนการจะแตกต่างกัน บทบาทหน้าที่แต่ละผู้มีส่วนได้ส่วนเสียก็จะไม่เหมือนกัน บางคนต้องมีส่วนร่วมในกระบวนการ ก็ต้องเข้าใจกระบวนการ บางคนต้องนำผลลัพธ์ของกระบวนการไปใช้ต่อก็อาจจะไม่ต้องเข้าใจกระบวนการก็ได้แต่ต้องรู้ว่าผลลัพธ์จะได้เมื่อไหร่ เป็นต้น ดังนั้นต้องวิเคราะห์ ผู้มีส่วนได้ส่วนเสีย ว่าแต่ละคนเกี่ยวข้องอะไรกับกระบวนการแล้วสื่อสารให้เข้าใจ โดยมีการประเมินผลการสื่อสารผ่านการรับรู้

# ประเด็นคำถาม

Q: รบกวนสอบถามข้อมูลด้านที่ 5 DT ดังนี้

1. เรื่องการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล ในเกณฑ์ระบุว่าควรมีระดับคณะกรรมการขององค์กรในการกำกับดูแลและรับผิดชอบ ไม่ทราบว่าจำเป็นต้องตั้งคณะกรรมการชุดใหม่ขึ้นมาดูแลเรื่องนี้โดยเฉพาะหรือไม่ และจำเป็นต้องเป็นคณะที่มีคณะกรรมการขององค์กรครบทุกท่านหรือไม่

2. ในเกณฑ์ทุกหัวข้อระบุว่า ควรมีกระบวนการและแนวปฏิบัติที่ชัดเจน สามารถทำซ้ำได้ ไม่ทราบว่ากระบวนการแต่ละหัวข้อ จำเป็นต้องได้รับการอนุมัติจากผู้บริหารหรือไม่ ถ้าจำเป็นต้องเป็นระดับไหน

A: 1. โครงสร้างการกำกับดูแลด้านการพัฒนาเทคโนโลยีดิจิทัลที่เหมาะสม จะขึ้นอยู่กับองค์กร หัวใจหลักของการประเมินคือการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร ตามแนวทาง Best practices ที่ได้ใส่ไว้ในคู่มือการประเมินผลฯ แนะนำว่าควรมีคณะกรรมการที่มีองค์ประกอบของคณะกรรมการองค์กร ซึ่งอาจเป็นประธานของคณะกรรมการชุดนี้ รวมถึงประกอบด้วยบุคลากรด้าน IT และ Business อยู่ในองค์ประกอบ เพื่อสามารถขับเคลื่อนการนำดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร อย่างไรก็ตาม จะต้องมีการประเมินประสิทธิผลของกระบวนการการกำกับดูแลด้านการพัฒนาเทคโนโลยีดิจิทัลซึ่งโครงสร้างการกำกับดูแลก็อาจจะสามารถถูกเปลี่ยนแปลงได้ถ้าผลลัพธ์ของการกำกับดูแลออกมาไม่เป็นไปตามเป้าหมายที่กำหนด

2. การมีแนวปฏิบัติที่ชัดเจน ถ้ายกตัวอย่างให้เห็นชัดก็คือ การทำคู่มือการปฏิบัติงานเนื่องใดเรื่องหนึ่ง ซึ่งจะระบุอำนาจหน้าที่ความรับผิดชอบไว้อย่างชัดเจน รวมถึงการอนุมัติอนุญาตเช่นเดียวกัน ไม่ว่าจะให้อำนาจระดับใดอนุมัติอนุญาต ก็จะต้องมีกลไกการกำกับดูแลติดตามและรายงานผลให้คณะกรรมการในระดับกำกับดูแลรับทราบ

# ประเด็นคำถาม

Q: IT Audit กับ การทำ Computer Audit ในหัวข้อ DT 2.3 การจัดการด้านคุณภาพ ต่างกันอย่างไร

A: อันเดียวกัน

Q: การเชื่อมโยงข้อมูลระหว่างหน่วยงานดูจากเกณฑ์แล้วเข้าใจว่าเป็นการมีกระบวนการขั้นตอนการเชื่อมโยงข้อมูลเท่านั้น อยากทราบว่าต้องมีการเชื่อมโยงข้อมูลจริงๆ ไหม และคำว่าระหว่างหน่วยงาน หมายถึง หน่วยงานเดียวกันแต่ต่างสาขา หรือว่าต่างหน่วยงานต่างกระทรวง

A: ตามนี้รูปด้านล่าง เน้นการเชื่อมโยงข้อมูลและกระบวนการทำงานกับหน่วยงานภายนอก


Q: เกณฑ์ ด้าน DT ข้อ 5.3 ISMS Audit ผู้ตรวจสอบประเมิน ควรเป็นหน่วยงานตรวจสอบภายใน หรือไม่อย่างไร

A: การตรวจสอบ ISMS จะเป็นหน่วยงานภายใน หรือหน่วยงานภายนอกก็ได้ แต่ตามเกณฑ์ระบุ คือ มีความเป็นกลางและความเป็นธรรม ซึ่งตามหลักการการตรวจสอบ ISMS ก็ไม่ต่างจาก Computer หรือ IT Audit คือ ผู้ตรวจสอบต้องมีความรู้ความสามารถเฉพาะในการตรวจสอบเรื่องดังกล่าว ดังนั้นผู้จะสามารถตรวจสอบ ISMS ก็ต้องต้องมีความรู้ความเข้าใจด้าน ISMS โดยวัดความสามารถจากการได้รับ Citification ด้าน ISMS เป็นต้น

# ประเด็นคำถาม

Q: วัตถุประสงค์ของการบริหารจัดการ IT vs. IS vs. DT เหมือนหรือแตกต่างกัน

A: ขออธิบายโดยละเอียดดังนี้นะ

Technology เทคโนโลยี หมายถึง การประยุกต์เอาความรู้ทางด้านวิทยาศาสตร์ ความจริงเกี่ยวกับธรรมชาติและสิ่งแวดล้อม มาทำให้เกิดประโยชน์ต่อมวลมนุษย์ เทคโนโลยีจึงเป็นวิธีการในการสร้างมูลค่าเพิ่มของสิ่งต่าง ๆ ให้เกิดประโยชน์มากยิ่งขึ้น

Information สารสนเทศ หมายถึง ข้อมูลที่เป็นประโยชน์ต่อการดำเนินชีวิตของมนุษย์ ข้อมูลดังกล่าวต้องผ่านการเก็บรวบรวม จัดเก็บ ตรวจสอบความถูกต้อง แบ่งกลุ่มจัดประเภทของข้อมูล และสรุปออกมาเป็นสารสนเทศ และมนุษย์นำเอาสารสนเทศนั้นไปใช้ในชีวิตประจำวันได้ เช่น รายงาน ผลงานการวิจัย ข่าวสารต่าง ๆ

IT (Information Technology) เทคโนโลยีสารสนเทศ หมายถึง การนำความรู้ต่าง ๆ มาประยุกต์ใช้ในการดำเนินชีวิตประจำวัน โดยผ่านกระบวนการประมวลผลเพื่อให้สามารถสร้างสรรค์สิ่งต่าง ๆ มาใช้แก้ปัญหาหรือตอบสนองความต้องการของมนุษย์ได้ โดยที่เทคโนโลยีถูกนำมาใช้ เพราะเทคโนโลยีสารสนเทศสามารถทำงานได้อย่างรวดเร็ว สม่ำเสมอ แม่นยำ และเชื่อถือได้

IS (Information system) ระบบสารสนเทศ หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศเพื่อช่วยในการตัดสินใจ และการควบคุมในองค์กรในการทำงานของระบบสารสนเทศประกอบไปด้วยกิจกรรม 3 อย่างคือ การนำข้อมูลเข้าสู่ระบบ การประมวลผล และ การนำเสนอผลลัพธ์ ระบบสารสนเทศอาจจะมีการสะท้อนกลับ เพื่อการประเมินและปรับปรุงข้อมูลนำเข้า ระบบสารสนเทศอาจจะเป็นระบบทีประมวลด้วยมือ หรือระบบที่ใช้คอมพิวเตอร์ก็ได้

# ประเด็นคำถาม

Q: วัตถุประสงค์ของการบริหารจัดการ IT vs. IS vs. DT เหมือนหรือแตกต่างกัน (ต่อ)

A: ดังนั้นความแตกต่างระหว่าง IT กับ IS คือ IT เป็นเทคโนโลยีในการสร้างมูลค่าให้กับสารสนเทศ เพื่อให้สารสนเทศสามารถนำมาใช้ประโยชน์ได้ IS เป็นระบบของการจัดเก็บ ประมวลผลข้อมูลโดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ นอกจากนี้ยังมีอีกหนึ่งคำ คือ ICT

ICT (Information and Communication Technology) หรือ เทคโนโลยีสารสนเทศและการสื่อสาร ความหมายคล้ายกับเทคโนโลยีสารสนเทศ (IT) เพียงแต่ขยายขอบเขตเพิ่มขึ้นโดยเน้นเรื่องบทบาทของการสื่อสาร (Communications) กับบูรณาการของสิ่งต่อไปนี้ได้แก่ โทรคมนาคม (ไม่ว่าจะเป็นโทรศัพท์ ระบบสื่อสารข้อมูลดาวเทียมหรือเครื่องมือสื่อสารใด ๆ ทั้งมีสายและไร้สาย) คอมพิวเตอร์ตลอดจนถึงซอฟต์แวร์ หน่วยเก็บข้อมูลและระบบโสตทัศน์ต่าง ๆ ซึ่งทั้งหมดช่วยให้ผู้ใช้สามารถเข้าถึง เก็บบันทึก ส่งผ่าน และจัดดำเนินการสารสนเทศได้ ซึ่งไม่ว่าจะ IS IT หรือ ICT ส่วนใหญ่เป็นงานที่เน้นการปฏิบัติและเป็นประโยชน์ขององค์กร การใช้งานเพื่อให้เกิดประโยชน์ต่อคนทำงานมีบ้างแต่ยังไม่มาก ดังนั้นจึงเริ่มมีการคิดค้นเทคโนโลยีและโปรแกรมที่สามารถช่วยในการทำงานต่างๆ ของคนทั่วไปได้มากขึ้น เช่น คอมพิวเตอร์ตั้งโต๊ะที่ยกไปไหนมาไหนได้ลำบาก ถูกออกแบบให้เป็นเครื่องขนาดเล็กที่ถือติดตัวไปได้ ทำให้เกิด Notebook และ Tablet ต่อมาก็คิดวิธีพัฒนาโทรศัพท์มือถือธรรมดาให้เป็น Smart Phone ที่สามารถช่วยงานผู้ใช้ได้มากมายหลายอย่าง การประยุกต์เหล่านี้ต้องสร้างเทคโนโลยีขึ้นรองรับมากมาย เทคโนโลยีเหล่านี้ ไม่ได้มุ่งที่จะช่วยการคำนวณโดยตรง และ ไม่ได้มุ่งที่จะนำข้อมูลมาจัดทำเป็นสารสนเทศเหมือนที่ใช้กันใน IS IT หรือ ICT อีกแล้ว เพราะเป้าหมายของเทคโนโลยีใหม่นี้ขยายตัวไปมากกว่าเป้าหมายของ IS IT หรือ ICT จึงเรียกเทคโนโลยีที่ขยายตัวออกไปนี้ว่า เทคโนโลยีดิจิทัล (Digital Technology)

# ประเด็นคำถาม

Q: วัตถุประสงค์ของการบริหารจัดการ IT vs. IS vs. DT เหมือนหรือแตกต่างกัน (ต่อ)

A: ดังนั้น Digital Technology จะหมายถึงทั้งอุปกรณ์และการประยุกต์ที่เกี่ยวข้องกับ เทคโนโลยีคอมพิวเตอร์ รวมกับ IS IT หรือ ICT และ ความสามารถในการทำงานและวิเคราะห์ข้อมูลจำนวนมหาศาล เช่น ภาพยนตร์, คลิปวีดิทัศน์, แผนที่ ฯลฯ (ซึ่งรวมเป็นข้อมูลขนาดใหญ่ หรือ big data) รวมกับความสามารถในการทำงานทำงานแบบอัตโนมัติ และรวมไปถึงความสามารถในการเรียนรู้เองของอุปกรณ์ (machine learning) ซึ่งใช้วิทยาการด้านปัญญาประดิษฐ์ (artificial intelligence หรือ AI) เป็นพื้นฐาน เกณฑ์การประเมินผลใหม่จึงใช้ชื่อว่า “การพัฒนาเทคโนโลยีดิจิทัล” (Digital Technology : DT) เพื่อให้ รส.มุ่งเน้นการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร และทุกส่วนของธุรกิจ บนพื้นฐานของการกำกับดูแลด้านเทคโนโลยีดิจิทัลที่ดี รวมทั้งการบริหารจัดการด้านเทคโนโลยีดิจิทัลตามแนวทาง Best Practices และ มาตรฐานต่างๆ ที่เป็นที่ยอมรับในระดับสากล

# ประเด็นคำถาม

Q: ทาง DT ข้อ Digital Governance ดูเหมือน ทาง Tris นำ COBIT5 และ ISO 38500 มาผนวกกัน ตาม evaluate direct monitor กับ 6 principle คือ respon, strategy, acquire, perform, conform, human อยากให้ขยายความด้วยว่า 2 มาตรฐานมารวมกันอย่างไร และเรื่อง 2) คือ การ governances จะไปเกี่ยว กับ ข้อ 1 การกำกับดูแลโดย board อย่างไร เพราะที่ข้อกำกับดูแล แผนและ monitor ด้าน digital หาก รส. ไม่มี board digital มีแต่ IT steering ที่มี CEO เป็นประธาน และประเด็นที่ 3) ด้าน digital ไปเกี่ยวกับ ด้านอื่นๆ risk compliance KM stakeholder น่าจะครบทั้ง 8 ควรที่คนด้าน digital ที่ รส. มีน้อย จะทำทั้งหมดมี ข้อแนะนำไหม ถ้าใช้ resource เยอะ ข้อ resource optimization ก็จะต่ำอีกด้วย 4) TRIS ใช้มาตรฐานด้าน IT 10-20 standard มาผสมกัน มี รส. ด้านไหนทำได้เกือบหมดไหม

A: 1. เข้าใจถูกต้องว่าเกณฑ์ได้นำเอาทั้ง COBIT ISO 38500 มารวมกัน ซึ่งได้พูดถึงทุกครั้งในตอนชี้แจง/อบรมเกณฑ์ที่จัดโดย สคร. นอกจาก 2 มาตรฐานดังกล่าว ยังมีการนำแนวทางกรอบกำกับดูแลตัวอื่นๆมาพิจารณาอีก เช่น KING IV ขออธิบายโดยหลักการดังนี้ การกำกับดูแลพื้นฐานจะประกอบด้วย Evaluate (การประเมิน) Direct (การสั่งการ) และ Monitor (การติดตาม) ซึ่งเป็นพื้นฐานทั้งของ COBIT และ ISO38500 COBIT มีวัตถุประสงค์ของ Governance อยู่ 3 อย่างคือ 1. Benefits Realization 2. Risk Optimization และ 3. Resource Optimization ซึ่งได้ออกมาเป็น Framework ที่สำคัญ 3 เรื่อง คือ Benefits Delivery and Resource Optimization Framework Performance Measurement and Stakeholder Transparency Framework และ Risk Optimization Framework ส่วน ISO 38500 มี Governance guiding principle 6 อย่างคือ การกำหนดความรับผิดชอบ (Responsibility) กลยุทธ์ขององค์กรที่สอดคล้องกับความสามารถด้านเทคโนโลยีดิจิทัล (Strategy) การจัดหา (Acquisition) ประสิทธิภาพการดำเนินงาน (Performance) ความสอดคล้องกับระเบียบและข้อบังคับ (Conformance) และความรู้ความสามารถด้านดิจิทัลของบุคลากร (Human Behavior)

# ประเด็นคำถาม

A: จะสังเกตเห็นได้ว่าถ้าศึกษาเข้าไปในรายละเอียดของ COBIT แต่ละ Framework จะมีบางประเด็นที่ระบุเกี่ยวกับ Governance guiding principle ของ ISO 38500 อย่างชัดเจน แต่บางประเด็นต้องตีความว่าเกี่ยวข้องหรือไม่ ดังนั้นการจัดทำเกณฑ์การประเมินผลไม่ได้ประเมินตาม COBIT หรือ ISO 38500 แต่เป็นการกำหนดกรอบกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัลที่สำคัญให้ครบถ้วน โดยลดความเข้าใจคลาดเคลื่อนของผู้ถูกประเมินจึงต้องกำหนดรายละเอียดที่ชัดเจน

2. หลักการกำกับดูแลที่ดีจะต้องแยกส่วนระหว่าง Governance และ Management อย่างชัดเจน Digital Governance เป็นเครื่องมือของ Board ในการกำกับดูแลด้านการพัฒนาเทคโนโลยีดิจิทัล ดังนั้น รส. คงต้องทบทวนโครงสร้างการกำกับดูแลของตัวเองในปัจจุบันว่าเหมาะสมหรือไม่ เพราะหัวใจหลักของการประเมินการพัฒนาเทคโนโลยีดิจิทัล คือการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร และทุกส่วนของธุรกิจ ดังนั้นโครงสร้างตามแนวทาง Best Practices แนะนำ IT Steering Committee จึงควรมีสมาชิกของ Board ที่ไม่ใช่ CEO มาเป็นประธาน เพื่อขับเคลื่อนการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรได้อย่างแท้จริง

3. ต่อเนื่องจากข้อ 2 ถ้ามี IT Steering Committee ตามข้อ 2 ก็จะสามารถบริหารจัดการปัญหาต่างๆ ได้อย่างมีประสิทธิภาพ

4. ตอนนี้ยังไม่มี รส. ไหนทำได้ครบทั้งหมด เนื่องจากหลายตัวเป็นเกณฑ์การประเมินใหม่ ซึ่งแนวทางการประเมินผลที่ดีคงไม่ใช่คำนึงว่ามีคนทำได้แล้วหรือยัง แต่เป็นการกำหนดแนวทางการประเมินที่ รส. ควรจะทำและนำมาใช้เป็นกรอบในการพัฒนามากกว่า อย่างไรก็ตาม จากการประเมิน Baseline ที่ผ่านมามีหลายประเด็นที่ รส. อาจจะยังไม่ดำเนินการแต่มีแผนที่จะดำเนินการอยู่แล้วในช่วง 3-5 ปีด้วยตนเอง แม้ไม่มีเกณฑ์การประเมินกำหนดเนื่องจากเป็นแนวทางตาม Best Practices แต่เมื่อมีเกณฑ์ประเมินกำหนดจึงเร่งรัดดำเนินการให้เร็วกว่าที่วางแผนไว้

# ประเด็นคำถาม

Q: รบกวนสอบถามการแจ้งชื่อผู้ใช้งานระบบ it ตามหนังสือ สคร.ที่ กค0804.2/ว.492 ลว. 27 พ.ค. 63 ผู้บันทึกและผู้อนุมัติจำเป็นต้องมีคุณสมบัติเฉพาะอะไรหรือไม่ เช่น ต้องดำรงตำแหน่งหรือมีระดับชั้นใดขึ้นไป

A: ขึ้นอยู่ที่การบริหารจัดการของ รส. แต่โดยหลักการผู้อนุมัติจะเป็นผู้ Submit ส่งเอกสารทั้งหมดที่ผู้บันทึกได้ Upload ไว้ โดยก่อนจะ Submit ต้องตรวจสอบความถูกต้องและครบถ้วนของเอกสารให้เรียบร้อย เพราะจะ Submit ส่งเอกสารได้ครั้งเดียวเท่านั้น และไม่สามารถแก้ไขได้ จนกว่าระบบจะเปิดให้ส่งเอกสารอีกครั้งหลักจากที่ที่ปรึกษาทำการ Site visit แล้วเสร็จ

Q: หัวข้อ 7.2 Green IT Management มีแนวทางการดำเนินการตามกระบวนการหรือมาตรฐานที่เกี่ยวข้องหรือไม่ เช่น ISO หรือ GMMI

A: ตอนนี้ Green IT จะไม่มี ISO หรือ Standard โดยตรง แต่สามารถใช้ Green IT Framework ของ ISACA หรือแนวทาง Green IT อื่นๆ มาประกอบการพิจารณาได้ เช่น GUIDELINES FOR GREEN ICT ของ NIA (National Information Society Agency) Korea เป็นต้น

Q: ขอสอบถามว่าในข้อที่ 1. การจัดทำแผน BCP จะต้องได้รับอนุมัติจากคณะกรรมการ และคณะกรรมการขององค์กร หมายถึง คณะกรรมการ BCM ของหน่วยงานใช่ไหม

A: ไม่ใช่ คณะกรรมการบริหารองค์กรจะเป็นผู้อนุมัติ ซึ่งคณะกรรมการ BCM ก็จะถูกแต่งตั้งจาก คณะกรรมการองค์กร คณะ BCM คือ Sub ของ คณะกรรมการองค์กร คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ BCM Steering Committee ควรประกอบด้วย ผู้ตัดสินใจ ผู้เป็นเจ้าของธุรกิจ ผู้เชี่ยวชาญทางด้านเทคโนโลยีและผู้ชำนาญการทางด้านการบริหารความต่อเนื่องทางธุรกิจ ทำหน้าที่ดำเนินการตัดสินใจเชิงกลยุทธ์เรื่องการวางแผนเกี่ยวกับการเรียกคืนและดำเนินธุรกิจต่อเนื่องขององค์กร ทั้งนี้ คณะกรรมการบริหารฯ มีความแตกต่างจากคณะกรรมการบริหารโครงการโดยทั่วไป ซึ่งจะถูกยกเลิกไปเมื่อโครงการต่างๆ สิ้นสุดลง คณะกรรมการบริหารฯ จะคงอยู่ตลอดไป โดยที่คณะกรรมการบริหารฯ ควรมีประธานเป็น ผู้บริหารระดับสูงคนหนึ่งขององค์กร

# ประเด็นคำถาม

Q: สรุปว่าแผน BCP จะต้องได้รับการอนุมัติจาก คณะกรรมการรัฐวิสาหกิจใช่ไหมหรือแค่คณะกรรมการ BCM ขององค์กร

A: คณะกรรมการ BCM ขององค์กร

Q: ขอสอบถามเกี่ยวกับเกณฑ์ด้าน 5 (DT) คำถามข้อ 7.1 การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม ต้องแสดงรายละเอียดภาพรวมขององค์กร ไม่ใช่เฉพาะสายงานเทคโนโลยีสารสนเทศเพียงอย่างเดียวใช่หรือไม่ เนื่องจากในเกณฑ์การประเมินผลลัพธ์ระบุว่าต้องครอบคลุมทั้งด้านทรัพยากรทางการเงิน คน เทคโนโลยีดิจิทัล ระยะเวลา และทรัพยากรพื้นฐานต่างๆ

A: ถูกต้อง ต้องสอดคล้องกัน เพราะอยู่บนสมมติฐานทรัพยากรเดียวกันทั้งหมดทั้งองค์กร ไม่ว่า งบประมาณ เทคโนโลยี บุคลากร และอื่นๆ ซึ่งจะเห็นได้ว่า ทั้งเกณฑ์ข้อ SP และ DT จะมีการพูดถึงเรื่องนี้ทั้งคู่

Q: กระบวนการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management Implementation) ของรัฐวิสาหกิจ ในข้อ 7.1 นั้น

1. อยากทราบว่าการเขียน SIPOC จำเป็นต้องเป็นไปในทิศทางเดียวกันกับข้อ 5.3 เรื่องกระบวนการจัดสรรทรัพยากร หรือแยกกระบวนการ

2.หากเป็นรูปแบบเดียวกัน ทางด้าน DT ต้องรอผลจากด้าน SP ก่อนหรือไม่

A: ถ้าองค์กรมีการกำหนดหลักการจัดสรรทรัพยากรขององค์กรอยู่แล้ว 7.1 จะต้องนำมาเป็น Input ของกระบวนการเพื่อ ดำเนินการจัดทำการบริหารทรัพยากรด้านเทคโนโลยีดิจิทัล กระบวนการ SP 5.3 และ DT 7.1 จะมีลักษณะเดียวกัน เพื่อให้เกิดแผนการจัดสรรทรัพยากรที่เหมาะสม

# ประเด็นคำถาม

Q: ขอคำแนะนำหรือ ตัวอย่างการวิเคราะห์และจัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture) เพื่อมุ่งเน้นการนำเทคโนโลยีดิจิทัลมาปรับใช้กับ ทุกส่วนขององค์กร และทุกส่วนของธุรกิจ ทั้งในส่วนของกระบวนการ ทำงาน การสร้างสรรค์ผลิตภัณฑ์สักหน่อย

A: สามารถดูแนวทางของ EGA ซึ่งปัจจุบันเป็น DGA ได้ โดย EGA เอาตัวอย่างการทำ EA ของตัวเองมาเปิดเผยให้ศึกษากัน

Q: ขออนุญาตสอบถามหมวด DT ในระดับสาม ที่เกี่ยวกับการประเมินผลการรับรู้ของผู้ที่เกี่ยวข้อง ขอตัวอย่างการวัดผลการรับรู้ได้ไหมว่าใช้อะไรวัดได้บ้าง

A: การประเมินผลการรับรู้มีได้มากมายหลายรูปแบบ เพื่อวัดว่าผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องรับรู้สิ่งที่สื่อสารออกจริงหรือไม่ และขึ้นอยู่กับช่องทางที่ใช้ในการสื่อสารด้วย ตัวอย่างการประเมินผลการรับรู้ผ่านการกำหนดตัวชี้วัด เช่น จำนวนการเข้าร่วมรับฟังการชี้แจงกระบวนการฯ การเซ็นรับทราบนโยบาย จำนวนพนักงานที่ละเมิดกฎระเบียบต่างๆ รวมไปถึงการนำระบบหรือออกข้อบังคับต่างๆ มาใช้ในการแสดงการรับรู้ก็ได้ เช่น การบังคับเปลี่ยน Password ทุก 3 เดือน ไม่เปลี่ยนเข้าใช้ระบบไม่ได้ การขึ้น Pop up ให้อ่านถ้าไม่ติ๊กอ่านก็ไม่สามารถปิดหน้า Pop up ได้ เป็นต้น ดังนั้นให้คิดถึงพื้นฐานที่ว่าเราจะแสดงให้ผู้ประเมินทราบได้อย่างไรว่าผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการฯ ได้รับรู้แล้วจริงๆ

# ประเด็นคำถาม

Q: ขอสอบถามรายละเอียดเกี่ยวกับ Enablers ด้าน DT ตามคู่มือการประเมินผลการดำเนินงานของรัฐวิสาหกิจตามระบบประเมินผลใหม่ ข้อ 5.3 การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management) (ISMS) Audit) ระดับ 1 – 2 เป็นของ IA รับผิดชอบ ส่วนค่าระดับ 3 - 5 จะเป็นของด้าน IA หรือ IT เป็นผู้รับผิดชอบอย่างไร

A: คำตอบคือต้องดูว่าใครเป็นผู้รับผิดชอบกระบวนการ โดยปกติกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management) (ISMS) Audit) จะเป็นกระบวนการของการตรวจสอบ หรือ IA ดังนั้นไม่ว่าระดับไหน ระดับ 1-5 ผู้รับผิดชอบก็ต้องเป็น IA แต่ IT มีหน้าที่ในการเป็นผู้รับตรวจที่ดี แลแก้ไขข้อสังเกตต่างๆที่ตรวจพบให้เรียบร้อยและรายงาน ดังนั้น ระดับ 3 สื่อสาร หรือระดับ 4-5 ที่เป็นการวัดประสิทธิผลกระบวนการ และนำมาปรับปรุงกระบวนการอย่างต่อเนื่องก็จะเป็น IA

Q: ขออนุญาตสอบถาม ด้าน dt เกณฑ์ระดับ 4 ที่ ให้มีการกำหนด วัด ติดตาม วิเคราะห์ กระบวนการ กรณีที่ดำเนินการปิด gap ด้วยวิธีการสอบทานกระบวนการต่างๆ อาทิ เช่น สอบทานการบริหารจัดการโครงการ ในที่นี้คือให้หน่วยงานเจ้าของกระบวนการดำเนินวัดผลการดำเนินงานของกระบวนการดังกล่าวเพื่อ นำผลมาปรับปรุงกระบวนการใช่หรือไม่

A: ใช่ แต่ลักษณะการวัดประสิทธิผลของกระบวนการ จะต้องวัดผลได้ จากตัวอย่างที่ยกมา ก็ควรกำหนดเป็นตัววัด เช่น ร้อยละของโครงการที่มีการสอบทานตามแนวทางที่กำหนด เป็นต้น รวมถึงตัววัดของกระบวนการบริหารจัดการที่นิยมใช้ในการวัดผลจะเป็น ร้อยละความสำเร็จของโครงการที่ดำเนินการได้ตามเป้าหมายที่กำหนด เป็นต้น

# ประเด็นคำถาม

Q: รบกวนสอบถามข้อมูลเพิ่มเติมดังนี้

1. องค์กรได้รับการรับรองมาตรฐาน ISO 22301: 2012 ระบบบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) แล้วสามารถแนบเอกสารใบรับรองมาตรฐาน แทนเอกสารแผน BCP เลยได้หรือไม่ เพราะมาตรฐาน ISO 22301 ครอบคลุมประเด็นต่างๆ ตามที่เกณฑ์ถามเรียบร้อยแล้ว

2. หากข้อ 1 ไม่สามารถทำได้ โดยจำเป็นจะต้องมีเอกสารรายละเอียดเพื่อให้ผู้ตรวจประเมินพิจารณานั้น จะมีคำถามตามมา ซึ่งรบกวนผู้แทน สคร. และ TRIS ช่วยชี้แจงแนวทางเพิ่มเติม ดังนี้

2.1 ในเกณฑ์ SE-AM ระบุให้รัฐวิสาหกิจมีการจัดทำแผน BCP โดยครอบคลุมบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ การประเมินความเสี่ยง การวิเคราะห์ผลกระทบทางธุรกิจและการกำหนด RTO การจัดลำดับความสำคัญ การกำหนดกลยุทธ์การบริหารความต่อเนื่องทางธุรกิจ การจัดทำแผน BCP การสื่อสารและฝึกอบรม การทดสอบ ปรับปรุง และสอบทาน ซึ่งทั้งหมดนี้ ไม่ได้อยู่ในรูปเอกสารที่เรียกว่า “แผน BCP” เพียงฉบับเดียว แต่แยกออกเป็นเอกสารทั้งสิ้น 15 รายการ และหากนับเฉพาะแผน BCP เพียงรายการเดียวนั้น มีการจัดทำไว้ทั้งหมด 75 ฉบับ (จัดทำเป็นรายสาขาทั้งในประเทศและต่างประเทศ) ดังนั้น จึงอยากสอบถามว่าต้องแนบเอกสารทั้งหมดลงในระบบ SE-AM ไหม เนื่องจากนับเฉพาะเอกสารที่ตรงกับหัวข้อที่กำหนดไว้ในเกณฑ์ก็จะมีจำนวน File ค่อนข้างมากแล้ว (ประมาณ 150-200 File) และบางไฟล์อาจจะมีขนาดใหญ่เกิน 15 MB

2.2 สืบเนื่องคำถามในข้อ 2.1 เอกสารบางรายการนั้น จัดอยู่ในชั้นความลับขององค์กร และจำเป็นต้องถูกควบคุมการจัดส่งและเข้าถึงเอกสารทั้งในรูปแบบของ Hard copy และ Soft file ซึ่งเป็นไปตาม Document management procedure ที่กำหนดไว้ และเอกสารบางรายการ มีเนื้อหาที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ทั้งในส่วนของคนไทยซึ่งควรจะต้องมีการปฏิบัติให้สอดคล้องกับ “พ.ร.บ.ข้อมูลส่วนบุคคล”

# ประเด็นคำถาม

Q: ซึ่งกำลังจะบังคับใช้ และข้อมูลของลูกจ้าง และหรือ ผู้มีส่วนได้ส่วนเสียที่เป็นชาวต่างประเทศ ซึ่งถูกคุ้มครองด้วย “กฎหมาย GDPR” ของสหภาพยุโรป ที่บังคับใช้อยู่แล้ว ดังนั้น จึงขอสอบถาม ดังนี้

- รส. จำเป็นจะต้องส่งข้อมูลที่อยู่ในชั้น “ความลับ” และ เอกสารที่มี “ข้อมูลส่วนบุคคล” นำเข้าระบบ SE-EM ไหม หากไม่ส่งจะมีผลต่อการประเมินให้คะแนนของผู้ตรวจหรือไม่
- หากจำเป็นต้องส่ง ขอทราบแนวทางการจัดการเอกสาร/ไฟล์ ของทาง สคร. และ TRIS ดังนี้

  1) ระบบ SE-EM มีการกำหนดสิทธิ์ในการเข้าถึงไฟล์เอกสารที่เป็นชั้นความลับของ รส. หรือไม่ หากมี รบกวนขอทราบรายละเอียด เพื่อที่จะได้เสนอขออนุมัติผู้มีอำนาจให้เปิดเผยเอกสารในชั้น “ความลับ”

  2) ระบบ SE-EM มีการดูแลเรื่องความมั่นคงปลอดภัยทาง Cyber ของระบบไหม ในประเด็นใดบ้าง เพื่อให้มั่นใจว่าข้อมูลในระบบ จะไม่ถูกผู้ไม่หวังดี (hacker) เข้ามาโจมตี

  3) ระหว่าง สคร. และ TRIS มีการเซ็นต์ “สัญญาปกปิดความลับ (Non-disclosure agreement: NDA) ด้วยกันไว้อยู่แล้วใช่ไหม ครอบคลุมถึงข้อมูลที่ รส. ส่งให้ด้วยไหมและหากจะขอให้ TRIS เซ็น NDA กับ รส. โดยตรงอีกทางหนึ่งด้วย ไม่ทราบว่า สคร. และ TRIS มีความเห็นอย่างไร

A: โดยหลักการถ้าเอกสารที่มีความลับทางธุรกิจ รส. สามารถส่งเฉพาะ หน้าปก ของเอกสาร หรือเอกสารบางหน้าได้ แล้วเตรียมเอกสารจริงสำหรับการตรวจประเมินตอน Site visit ซึ่งที่ปรึกษายินดีดูที่ทำการของท่าน พร้อมทั้งเซ็น Disclosure อย่างไรก็ตาม การดำเนินการ BCM ตามเกณฑ์ ISO 22301 จะต้องมีการระบุขอบเขตของการขอรับ Cert. รวมถึงจะต้องมีภาพรวมของกระบวนการ BCM ขององค์กร รวมถึงโครงสร้าง High level structure ของ BCM ขององค์กร ซึ่งเอกสารเหล่านี้ควรส่งมาให้ผู้ประเมินดูเบื้องต้นด้วย อาจส่งเป็นบางหน้าก็ได้ ไม่ต้องทั้งเล่ม


Q&A

# ขอบพระคุณ

# SE-AM chat group

Invite friends you want to share this OpenChat with.