จุลสารตรวจสอบภายใน

www.cgd.go.th

ปีที่ 21 ฉบับที่ 116 ประจำเดือน กุมภาพันธ์ – มีนาคม 2560

สวัสดีค่ะ ฉบับนี้ บก. ได้เก็บเกี่ยวความรู้มาฝาก เรื่อง "แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ" ซึ่งเป็นบทความจากสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย หวังเป็นอย่างยิ่งว่าจะเป็นประโยชน์กับผู้ตรวจสอบภายใน ในการนำไปประยุกต์ใช้ตรวจสอบด้าน IT นอกจากนี้ได้ update กฎหมายใหม่ๆ ของกรมบัญชีกลาง ที่จะเป็นประโยชน์กับการปฏิบัติงานของผู้ตรวจสอบภายใน มาให้รับทราบทั่วกันค่ะ

ช่วงนี้อากาศแปรปรวน อุณหภูมิสูงขึ้น รักษาสุขภาพกันด้วยนะคะ

แล้วพบกันฉบับหน้าค่ะ ...

แนวทางการกำกับดูแล ด้านเทคโนโลยีสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่าง ๆ เทคโนโลยีสารสนเทศทำให้การดำเนินงานขององค์กรมีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสให้กับองค์กร อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการ ดังนั้น การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องที่ผู้ตรวจสอบภายในต้องให้ความสำคัญกับนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการการควบคุมความเสี่ยงอย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

Integrity Risk :

- ความเสี่ยงจากความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์
- สาเหตุ : การถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ไม่มีระบบควบคุมและตรวจสอบ การบันทึกข้อมูล การประมวลผล และการแสดงผลอย่างเพียงพอ การจัดการและควบคุมการพัฒนาระบบคอมพิวเตอร์ไม่รอบคอบและรัดกุมเพียงพอ

Availability Risk :

- ความเสี่ยงจากการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ
- สาเหตุ : การไม่ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ไม่มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ และไม่จัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน

Access Risk :

- ความเสี่ยงจากการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่ หรือบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ
- สาเหตุ : การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นการใช้งาน การไม่กำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์

Infrastructure Risk :

- ความเสี่ยงจากการไม่จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี
- สาเหตุ : การแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ไม่มีนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ละเอียดเพียงพอในงานที่สำคัญ ไม่จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการดำเนินงาน

มีต่อหน้าถัดไป

"การบริหารจัดการ และการควบคุมความเสี่ยงที่สำคัญ"

1. โครงสร้างหน่วยงานและการบริหารจัดการ

การแบ่งแยกอำนาจหน้าที่ ควรเป็นไปตามหลักการควบคุมภายในที่ดี โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ซึ่งการมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย (integrity risk)

แนวทางการกำกับดูแล ให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในหน่วยงาน กรณีมีข้อจำกัดของบุคลากร ก็ควรกำหนดวิธีการกำกับดูแลและควบคุมการปฏิบัติงานของบุคลากรดังกล่าวอย่างรอบคอบและรัดกุม

การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน จะทำให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้อง ครบถ้วน และเป็นไปในแนวทางเดียวกัน ซึ่งจะส่งผลให้การปฏิบัติงานโดยรวมมีประสิทธิภาพ นอกจากนี้ ยังลดโอกาสการปฏิบัติงานผิดพลาดในกรณีที่มีการสับเปลี่ยนหน้าที่และความรับผิดชอบหรือมีการมอบหมายงานให้บุคลากรรายใหม่

แนวทางการกำกับดูแล ให้ความสำคัญกับความครบถ้วนและความชัดเจนของนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ การพัฒนา แก้ไขหรือเปลี่ยนแปลง การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการปฏิบัติงานประจำอื่นที่สำคัญ

การกำกับดูแลและตรวจสอบการปฏิบัติงานของพนักงานระดับปฏิบัติการอย่างใกล้ชิดโดยผู้บังคับบัญชา จะทำให้การปฏิบัติงานโดยรวมมีความถูกต้องและละเอียดรอบคอบมากขึ้น ซึ่งจะเป็นการลดโอกาสการเกิดข้อผิดพลาดและป้องกันการปฏิบัติงานนอกเหนืออำนาจหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

แนวทางการกำกับดูแล ให้ความสำคัญกับการรายงานการปฏิบัติงานและตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่องค์กรกำหนด

2. การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) จะเป็นการป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ซึ่งรวมถึงความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)

แนวทางการกำกับดูแล ให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ที่รัดกุมเพียงพอ โดยจำกัดสิทธิการเข้าออกและการตรวจสอบการเข้าออกอย่างสม่ำเสมอ รวมทั้งจัดให้มีระบบป้องกันความเสียหายจากปัจจัยสภาวะแวดล้อมและภัยพิบัติที่อาจเกิดขึ้น

การควบคุมการใช้ข้อมูลและระบบงานคอมพิวเตอร์ และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security) อาจเกิดจากบุคคลภายในองค์กร เช่น ไม่ได้มีการกำหนดรหัสผ่านในการเข้าสู่ระบบงานอย่างรัดกุม หรือกำหนดสิทธิให้แก่ผู้ใช้งานภายในเพื่อเข้าถึงข้อมูลและระบบงานคอมพิวเตอร์ที่มากเกินความจำเป็น เป็นต้น อาจเกิดจากการเชื่อมต่อระบบเครือข่ายภายในกับภายนอก ที่จะเป็นช่องทางให้บุคคลภายนอกเข้าถึงข้อมูลและระบบคอมพิวเตอร์ รวมทั้งไวรัสหรือ malicious code อื่นๆ ผ่านเข้ามาทางระบบเครือข่าย

แนวทางการกำกับดูแล ให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) การกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ การกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และระบบป้องกันการบุกรุกจากบุคคลภายนอกผ่านระบบเครือข่าย

มีต่อหน้าถัดไป

"การบริหารจัดการและการควบคุมความเสี่ยงที่สำคัญ" (ต่อ)

3. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ (Change Management)

เป็นเรื่องที่ต้องให้ความสำคัญ โดยหากไม่มีวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ระบบงานคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องหรืออาจไม่เป็นไปตามความต้องการของผู้ใช้งานได้ (integrity risk)

แนวทางการกำกับดูแล ให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) และการกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ โดยรหัสดังกล่าว ควรมีการกำหนดความยาวขั้นต่ำ อายุการใช้งาน จำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิด และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา และควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ

4. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

การสำรองข้อมูลและระบบงานคอมพิวเตอร์ หากมิได้ดำเนินการที่เพียงพอจะทำให้ไม่มีข้อมูลหรือระบบงานคอมพิวเตอร์สำหรับใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ

แนวทางการกำกับดูแล ให้ความสำคัญกับการสำรองข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ ในเรื่องความครบถ้วนของการเก็บรักษาสื่อที่ใช้บันทึก และการทดสอบความถูกต้องครบถ้วนของข้อมูลและระบบงานคอมพิวเตอร์ที่สำรองไว้

การเตรียมพร้อมกรณีฉุกเฉิน เป็นการจัดทำแผนฉุกเฉินเพื่อรองรับเหตุการณ์ฉุกเฉินที่อาจเกิดขึ้น ซึ่งจะทำให้การควบคุมความเสี่ยงด้าน availability risk มีประสิทธิภาพมากขึ้น

แนวทางการกำกับดูแล ให้ความสำคัญกับการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินต่างๆ ที่ควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งการทดสอบแผนดังกล่าวเพื่อให้มั่นใจว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

5. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

เป็นเรื่องของการควบคุมการประมวลผล การดูแลการทำงานของระบบคอมพิวเตอร์ การย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริง การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และงานประจำอื่นๆ หากไม่ได้มีวิธีการปฏิบัติและควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจก่อให้เกิดความเสี่ยงในด้านต่างๆ เช่น ความเสี่ยงด้าน integrity risk ในกรณีที่ย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริงไม่ครบถ้วน ความเสี่ยงด้าน availability risk ในกรณีที่มิได้มีการดูแลการทำงานของระบบคอมพิวเตอร์อย่างเพียงพอ เป็นต้น

แนวทางการกำกับดูแล ให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชา การปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงาน และการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

... อ้างอิง: แนวทางการกำกับดูแลเทคโนโลยีสารสนเทศ จากเว็บไซต์ สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย ...

Update กฎหมาย

การเรียกรายงาน จัดเก็บ นำส่งรายได้แทนกัน ในระบบ GFMIS

กรมบัญชีกลาง ได้มีการพัฒนารายงานจัดเก็บ นำส่งรายได้แทนกัน ในระบบ GFMIS ทั้งในระบบปฏิบัติการ (SAP R3) และในระบบ GFMIS Web Online และได้จัดทำหนังสือเวียนแจ้งวิธีการเรียกรายงานจัดเก็บ นำส่งรายได้แทนกันในระบบ GFMIS **ตามหนังสือกรมบัญชีกลาง ที่ กค 0414.3/ว 103 ลงวันที่ 27 มีนาคม 2560** ทั้งนี้ สามารถศึกษารายละเอียดของหนังสือได้ที่เว็บไซต์กรมบัญชีกลาง www.cgd.go.th หัวข้อ กฎหมาย/ระเบียบ/หนังสือเวียน ภารกิจการควบคุมการเบิกจ่ายเงินแผ่นดิน

Update กฎหมาย

ขยายเวลาเบิกจ่ายเงินงบประมาณ

กระทรวงการคลังได้มีการขยายเวลาเบิกจ่ายเงินงบประมาณ เนื่องจากส่วนราชการ รัฐวิสาหกิจ และหน่วยงานอื่นของรัฐ **ไม่สามารถเบิกจ่ายเงินงบประมาณได้เสร็จสิ้นภายในวันทำการสุดท้ายของเดือนมีนาคม 2560** ดังนั้น เพื่อให้สามารถใช้จ่ายเงินงบประมาณได้อย่างต่อเนื่องและบรรลุวัตถุประสงค์ กระทรวงการคลังจึงได้มีหนังสือเวียนแจ้งการขยายเวลาเบิกจ่ายเงินงบประมาณ ตามหนังสือ**กระทรวงการคลัง ที่ กค 0402.5/ว 42 ลงวันที่ 30 มีนาคม 2560** โดยได้**กำหนดหลักเกณฑ์การขยายเวลาเบิกจ่ายเงินงบประมาณ** ดังนี้

1 อนุมัติให้ขยายเวลาเบิกจ่ายเงินงบประมาณปี พ.ศ. 2552 - 2559 กรณีมีหนี้ผูกพันและกรณีไม่มีหนี้ผูกพันทุกรายการที่ได้รับอนุมัติให้ขยายเวลาเบิกจ่ายเงินและก้นเงินไว้เบิกเหลื่อมปีถึงวันทำการสุดท้ายของเดือนมีนาคม 2560 ต่อไปได้ถึงวันทำการสุดท้ายของเดือนกันยายน 2560 ทั้งนี้ ไม่รวมถึงเงินงบประมาณรายการต่อไปนี้

เงินงบประมาณปี พ.ศ. 2558

- รายการเงินงบประมาณสมทบโครงการเงินกู้จากต่างประเทศ

เงินงบประมาณปี พ.ศ. 2559

- รายการตามโครงการตามมาตรการกระตุ้นการลงทุนขนาดเล็กทั่วประเทศ
  (1) งบกลาง รายการเงินสำรองจ่ายเพื่อกรณีฉุกเฉินหรือจำเป็น
  (2) งบกลาง รายการค่าใช้จ่ายเสริมสร้างความเข้มแข็งและก้าวหน้าของประเทศตามแนวทางปฏิรูป
- รายการที่ก่อหนี้ผูกพันไว้ก่อนสิ้นปีงบประมาณ พ.ศ. 2559 และวันครบกำหนดอายุสัญญาเกินวันทำการสุดท้ายของเดือนมีนาคม 2560 ได้รับอนุมัติให้ก้นเงินไว้เบิกเหลื่อมปีและขยายเวลาเบิกจ่ายเงินกรณีมีหนี้ผูกพันถึงวันทำการสุดท้ายของเดือนกันยายน 2560 ตามหนังสือกระทรวงการคลัง ด่วนที่สุด ที่ กค 0402.5/ว 112 ลงวันที่ 15 กันยายน 2559

เงินงบประมาณปี พ.ศ. 2555 - 2558

- รายการที่คณะรัฐมนตรีอนุมัติให้ขยายระยะเวลาก่อหนี้ผูกพันได้ถึงวันทำการสุดท้ายของเดือนมีนาคม 2560

2 ให้ส่วนราชการ รัฐวิสาหกิจ และหน่วยงานอื่นของรัฐ ตรวจสอบผลการพิจารณาเรื่องดังกล่าว ในระบบ GFMIS โดยใช้คำสั่งงานตามที่กรมบัญชีกลางกำหนด

"จุลสารตรวจสอบภายใน" จัดทำขึ้นเพื่อเป็นสื่อกลางในการเผยแพร่ข้อมูลข่าวสารบทความเชิงวิชาการ และกิจกรรมต่าง ๆ ที่เกี่ยวกับการตรวจสอบภายในภาครัฐ ตลอดจนการเผยแพร่ผลงานของกรมบัญชีกลางในการพัฒนางานตรวจสอบภายใน หากท่านใดมีข้อติชมหรือต้องการแสดงความเห็นหรือมีปัญหาเกี่ยวกับงานตรวจสอบภายใน สามารถติดต่อได้ที่ :
กองบรรณาธิการ โทร. 0 2127 7285 โทรสาร 0 2127 7127
E-mail : iastd@cgd.go.th และ เว็บไซต์ http : // www.cgd.go.th /เรื่องที่น่าสนใจ/ตรวจสอบภายใน /จุลสารตรวจสอบภายใน
ที่ปรึกษา : นายณพงศ์ ศิริขันตยกุล **บรรณาธิการ** : นางสุรีพร ศิริขันตยกุล
กองบรรณาธิการ : นางนพรัตน์ พรหมนารท นางสาวกชพร รักอยู่ นางวัลนา ภู่สำลี และนายสมพล ลิมปมาลัยพร
เลขานุการกองบรรณาธิการ : นางสาวน้ำเพชร วงษ์ประทีป นางรัชดาภรณ์ อดิศรสมบูรณ์ นางสาวปภาสินี คลอวุฒิเสถียร นางอัญชลี เพ็ชรสุกใส และนางสาวเจนจิรา เววา
ผู้จัดส่ง : นางระวีวรรณ จันทร์อินทร์ นางธัญญารัตน์ สีโสภาพันธุ์ และนางสาวพรรณนิภา อำพันกาญจน์

ชำระค่าฝากส่งเป็นรายเดือน
ใบอนุญาตที่ 21/2530
ปทฝ.กระทรวงการคลัง