แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินงาน สามารถแบ่งออกเป็น 4 ประเภทหลัก ดังนี้

1. Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์โดยบุคคล ที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หากองค์กรมิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ

2. Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ อาจมีสาเหตุมาจากการที่องค์กรมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

3. Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหรือการดำเนินธุรกิจขององค์กรหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบ

คอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หากองค์กรมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

4. Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่องค์กรมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีรวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการดำเนินงานโดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินธุรกิจ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารขององค์กรมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจทางธุรกิจ ดังนั้น องค์กรก็ควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูลและจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินธุรกิจขององค์กรเอง ทั้งนี้ ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ควรจะ

ประเมินเฉพาะความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น โดยไม่ประเมินความเสี่ยงที่ระบุในย่อหน้านี้

แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่ควรให้ความสำคัญ เนื่องด้วยความเสี่ยงดังกล่าวอาจทำให้การดำเนินงานขององค์กรขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อการดำเนินงานขององค์กรเองและลูกค้า จึงควรมีนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรอย่างจริงจัง โดยให้ความสำคัญกับการบริหารจัดการและการควบคุมความเสี่ยงที่เกี่ยวข้องกับระบบซื้อขาย ระบบปฏิบัติการ และระบบงานสำคัญอื่น ในเรื่องดังต่อไปนี้

1. โครงสร้างหน่วยงานและการบริหารจัดการ

1.1 การแบ่งแยกอำนาจหน้าที่ แนวทางการกำกับดูแล ควรให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในหน่วยงานเทคโนโลยีสารสนเทศ โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่ง คนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ

1.2 การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน แนวทางการกำกับดูแล ควรให้ความสำคัญกับความครบถ้วนและความ ชัดเจนของนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน โดยเฉพาะนโยบาย แผนงาน และขั้นตอนการ

ปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์

1.3 การกำกับดูแลและตรวจสอบการปฏิบัติงาน แนวทางการกำกับดูแล ควรให้ความสำคัญกับการรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่ องค์กรกำหนดไว้

2. การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์

2.1 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) แนวทางการกำกับดูแล ควรให้ความสำคัญกับการควบคุมการเข้าออก ศูนย์คอมพิวเตอร์ที่รัดกุมเพียงพอ โดยควรจำกัดสิทธิการเข้าออกศูนย์คอมพิวเตอร์เฉพาะผู้ที่มีหน้าที่ เกี่ยวข้อง และควรมีการตรวจสอบการเข้าออกศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ

2.2 การควบคุมการใช้ข้อมูลและระบบงานคอมพิวเตอร์ และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security) แนวทางการกำกับดูแล ควรให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบ ผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) และการกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์

3. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

แนวทางการกำกับดูแล ควรให้ความสำคัญกับวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ โดยหากการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีการร้องขอจากผู้ใช้งาน

การร้องขอนั้น ก็ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ ควรจัดทำให้เป็นลายลักษณ์อักษร และควรกำหนดให้มีการทดสอบก่อนการใช้งานจริงทั้งจากเจ้าหน้าที่พัฒนาระบบและผู้ใช้งาน เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาแก้ไขหรือเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

4. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

4.1 การสำรองข้อมูลและระบบงานคอมพิวเตอร์ แนวทางการกำกับดูแล ควรให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์ และการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

4.2 การเตรียมพร้อมกรณีฉุกเฉิน แนวทางการกำกับดูแล ควรให้ความสำคัญกับการจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินต่างๆ ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ

5. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ แนวทางการกำกับดูแล ควรให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงาน ประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชา การปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงาน และการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

อ้างอิงข้อมูลมาจาก

http://dir.co.th/th/ข่าวสาร/ข่าวสารวิชาชีพ/item/33-it-manage.html

http://dir.co.th/images/pdf/it-manage.pdf