# แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

## บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานของบริษัทหลักทรัพย์ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่างๆ โดยเฉพาะระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจหลักทรัพย์ประเภทการเป็นนายหน้าซื้อขายหลักทรัพย์ เช่น ระบบซื้อขายหลักทรัพย์ (front office system) และระบบปฏิบัติการหลักทรัพย์ (back office system) เป็นต้น เทคโนโลยีสารสนเทศทำให้การดำเนินงานของบริษัทหลักทรัพย์มีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสแข่งขันในทางธุรกิจได้ อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง โดยหากบริษัทหลักทรัพย์ไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อบริษัทหลักทรัพย์เองและลูกค้าได้ ดังนั้น การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องที่สำนักงานให้ความสำคัญ โดยสำนักงานมีนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์อย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการประกอบธุรกิจหลักทรัพย์เกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น

## วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อเผยแพร่ความรู้ความเข้าใจเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ และเพื่อสื่อสารเกี่ยวกับแนวทางการกำกับดูแลและตรวจสอบของสำนักงานเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์

## ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบบริษัทหลักทรัพย์เกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานพิจารณาแล้วเห็นว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัทหลักทรัพย์ สามารถแบ่งออกเป็น 4 ประเภทหลัก ดังนี้

**1. Access Risk :** เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์[1] โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากบริษัทหลักทรัพย์มิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการกำหนดรหัสผ่าน (password)ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

**2. Integrity Risk :** เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่บริษัทหลักทรัพย์มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

**3. Availability Risk :** เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหรือการดำเนินธุรกิจของบริษัทหลักทรัพย์หยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากบริษัทหลักทรัพย์มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access

---

[1] ระบบคอมพิวเตอร์ หมายถึง โปรแกรม ระบบงาน เครือข่าย และอุปกรณ์คอมพิวเตอร์

risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

**4. Infrastructure Risk :** เป็นความเสี่ยงเกี่ยวกับการที่บริษัทหลักทรัพย์มิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินธุรกิจ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารของบริษัทหลักทรัพย์มิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจทางธุรกิจ ดังนั้น บริษัทหลักทรัพย์ก็ควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินธุรกิจของบริษัทหลักทรัพย์เอง ทั้งนี้ ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ สำนักงานจะประเมินเฉพาะความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น โดยไม่ประเมินความเสี่ยงที่ระบุในย่อหน้านี้

**แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ**

ด้วยสำนักงานมีเป้าหมายในการกำกับดูแลการประกอบธุรกิจของบริษัทหลักทรัพย์ให้มีความน่าเชื่อถือ มีประสิทธิภาพ และให้มีการดำเนินงานและการให้บริการที่ได้มาตรฐานสากล โดยปัจจุบันสำนักงานได้พัฒนากรอบในการกำกับดูแลบริษัทหลักทรัพย์ ซึ่งให้ความสำคัญกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจของบริษัทหลักทรัพย์ (Risk-Based Approach) โดยความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่สำนักงานให้ความสำคัญ เนื่องด้วยความเสี่ยงดังกล่าวอาจทำให้การประกอบธุรกิจของบริษัทหลักทรัพย์ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อการประกอบธุรกิจของบริษัทหลักทรัพย์เองและลูกค้า ดังนั้น สำนักงานจึงมีนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์อย่างจริงจัง โดยให้ความสำคัญกับการบริหาร

จัดการและการควบคุมความเสี่ยงที่เกี่ยวข้องกับระบบซื้อขายหลักทรัพย์ ระบบปฏิบัติการหลักทรัพย์ และระบบงานสำคัญอื่น ในเรื่องดังต่อไปนี้

**1. โครงสร้างหน่วยงานและการบริหารจัดการ** หากหน่วยงานเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ก็อาจก่อให้เกิดความเสี่ยงด้าน infrastructure risk ได้ ซึ่งสำนักงานให้ความสำคัญในเรื่องของการแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน และการกำกับดูแลและควบคุมการปฏิบัติงานเป็นหลัก ดังนี้

**1.1 การแบ่งแยกอำนาจหน้าที่** การแบ่งแยกอำนาจหน้าที่และความรับผิดชอบภายในหน่วยงานเทคโนโลยีสารสนเทศนั้น ควรเป็นไปตามหลักการควบคุมภายในที่ดี โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ซึ่งการมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย (integrity risk) เช่น การมอบหมายเจ้าหน้าที่พัฒนาระบบงาน (system developer) ซึ่งควรปฏิบัติงานเฉพาะในส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (test environment) ให้ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับส่วนของการใช้งานจริง (production environment) ควบคู่กัน ซึ่งมีความเสี่ยงในกรณีที่เจ้าหน้าที่พัฒนาระบบงาน อาจแก้ไขเปลี่ยนแปลงข้อมูลจริงหรือการทำงานของระบบคอมพิวเตอร์ได้โดยง่าย เนื่องจากมีความรู้ความเข้าใจในการทำงานของโปรแกรมต่าง ๆ และโครงสร้างของข้อมูล เป็นต้น

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในหน่วยงานเทคโนโลยีสารสนเทศ โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ทั้งนี้ หากบริษัทหลักทรัพย์มีข้อจำกัดด้านบุคลากรโดยมีความจำเป็นต้องมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กัน บริษัทหลักทรัพย์ก็ควรกำหนดมาตรการหรือวิธีการกำกับดูแลและควบคุมการปฏิบัติงานของบุคลากรรายดังกล่าวให้รอบคอบและรัดกุมเพียงพอ เช่น กำหนดให้มีบันทึกการทำงาน (log files) ของบุคลากรรายดังกล่าว และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ เป็นต้น

**1.2 การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน** การกำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่ชัดเจน จะทำให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องครบถ้วน และเป็นไปในแนวทางเดียวกัน ซึ่งจะส่งผลให้การปฏิบัติงานโดยรวมมีประสิทธิภาพ นอกจากนี้ ยังลดโอกาสการปฏิบัติงานผิดพลาดในกรณีที่มีการสับเปลี่ยนหน้าที่และความรับผิดชอบหรือมีการมอบหมายงานให้บุคลากรรายใหม่

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับความครบถ้วนและความชัดเจนของนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน โดยเฉพาะนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ การพัฒนาแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการปฏิบัติงานประจำอื่นที่สำคัญ

**1.3 การกำกับดูแลและตรวจสอบการปฏิบัติงาน** การกำกับดูแลและตรวจสอบการปฏิบัติงานของพนักงานระดับปฏิบัติการอย่างใกล้ชิดโดยผู้บังคับบัญชา จะทำให้การปฏิบัติงานโดยรวมมีความถูกต้องและละเอียดรอบคอบมากขึ้น ซึ่งจะเป็นการลดโอกาสการเกิดข้อผิดพลาดและป้องกันการปฏิบัติงานนอกเหนืออำนาจหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับการรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่บริษัทกำหนดไว้ นอกจากนี้ ในกรณีที่บริษัทหลักทรัพย์ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกไม่ว่าทั้งหมดหรือบางส่วน สำนักงานก็ให้ความสำคัญกับระบบการกำกับดูแลและควบคุมการปฏิบัติงานของบุคคลภายนอกเช่นกัน โดยบริษัทหลักทรัพย์ควรมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น มีการตรวจสอบบันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

**2. การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์** ในการดำเนินธุรกิจ บริษัทหลักทรัพย์มักจะรับรู้ข้อมูลของลูกค้าซึ่งเป็นข้อมูลที่ไม่ควรเปิดเผย เช่น ข้อมูลวงเงิน ข้อมูลการซื้อขายหลักทรัพย์ของลูกค้า และข้อมูลทรัพย์สินของลูกค้า เป็นต้น นอกจากนี้ บริษัทหลักทรัพย์ยังรับรู้ข้อมูลบางอย่างที่อาจเป็นสาระสำคัญต่อการเปลี่ยนแปลงราคาหลักทรัพย์ เช่น ข้อมูลที่ได้จากการประกอบธุรกิจการเป็นที่ปรึกษาทางการเงินและการจัดจำหน่ายหลักทรัพย์ เป็นต้น ซึ่งในปัจจุบันบริษัทหลักทรัพย์ได้จัดเก็บข้อมูลสำคัญตามที่กล่าวข้างต้นไว้ในระบบคอมพิวเตอร์และในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ ดังนั้น การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ จึงเป็นเรื่องที่สำนักงานให้ความสำคัญอย่างมาก โดยในการกำกับดูแลและตรวจสอบ สำนักงานจะให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย และการควบคุมการใช้ข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการป้องกันการบุกรุกระบบเครือข่าย ดังนี้

**2.1 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย**

**(Physical Security)** เนื่องด้วยข้อมูลที่เกี่ยวข้องกับการดำเนินธุรกิจได้ถูกจัดเก็บไว้ในระบบคอมพิวเตอร์และในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ตามที่กล่าวข้างต้น ดังนั้น การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ซึ่งเป็นสถานที่ตั้งของเครื่องแม่ข่ายที่ใช้เก็บฐานข้อมูล และยังเป็นสถานที่ในการประมวลผลและจัดทำรายงานต่างๆ จึงมีความสำคัญอย่างมากในการป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) นอกจากนี้ ระบบป้องกันความเสียหายภายในศูนย์คอมพิวเตอร์ก็มีความสำคัญในการป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ที่รัดกุมเพียงพอ โดยควรจำกัดสิทธิการเข้าออกศูนย์คอมพิวเตอร์เฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง และควรมีการตรวจสอบการเข้าออกศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ นอกจากนี้ สำนักงานยังให้ความสำคัญกับการจัดให้มีระบบป้องกันความเสียหายภายในศูนย์คอมพิวเตอร์จากปัจจัยสภาวะแวดล้อมและภัยพิบัติต่างๆ เช่น ระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ ระบบไฟฟ้าสำรอง เป็นต้น ทั้งนี้ หากบริษัทหลักทรัพย์จัดให้มีสถานที่อื่นใดนอกเหนือจากศูนย์คอมพิวเตอร์ เพื่อใช้เป็นสถานที่ตั้งเครื่องแม่ข่ายที่ใช้เก็บฐานข้อมูล หรือเป็นสถานที่ประมวลผลและจัดทำรายงานต่างๆ บริษัทหลักทรัพย์ก็ควรจัดให้มีระบบควบคุมการเข้าออก รวมทั้งระบบป้องกันความเสียหายภายในสถานที่ดังกล่าวอย่างรอบคอบและรัดกุมเพียงพอด้วยเช่นกัน

**2.2 การควบคุมการใช้ข้อมูลและระบบงานคอมพิวเตอร์ และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security)** กรณีการเข้าถึง ล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลและการทำงานของระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องนั้น (access risk และ integrity risk) อาจเกิดจากบุคคลภายในบริษัทหลักทรัพย์เอง ซึ่งอาจมีสาเหตุมาจากการมิได้มีระบบป้องกันที่ดีพอ เช่น มิได้มีการกำหนดรหัสผ่านในการเข้าสู่ระบบงานอย่างรัดกุม หรือกำหนดสิทธิให้แก่ผู้ใช้งานภายในเพื่อเข้าถึงข้อมูลและระบบงานคอมพิวเตอร์ที่มากเกินความจำเป็น เป็นต้น นอกจากนี้ เทคโนโลยีในปัจจุบันได้พัฒนาให้มีการเชื่อมต่อระบบเครือข่ายภายในกับภายนอกมากขึ้น ซึ่งหากบริษัทหลักทรัพย์มิได้มีวิธีการควบคุมที่รอบคอบและรัดกุมเพียงพอ การเชื่อมต่อในลักษณะดังกล่าวก็อาจเป็นช่องทางให้บุคคลภายนอกสามารถเข้าถึงข้อมูลและการทำงานของระบบคอมพิวเตอร์ผ่านระบบเครือข่ายได้ (access risk) อีกทั้งไวรัสหรือ malicious code อื่นๆ ก็อาจผ่านเข้ามาทางการเชื่อมต่อระบบเครือข่ายและสร้างความเสียหายแก่ข้อมูลและระบบคอมพิวเตอร์ได้เช่นกัน (availability risk)

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) และการกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ โดยรหัสผ่านดังกล่าว ควรมีการกำหนดความยาวขั้นต่ำ อายุ จำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิด และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา นอกจากนี้ บริษัทหลักทรัพย์ก็ควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และสำหรับกรณีที่บริษัทหลักทรัพย์มีการเชื่อมต่อระบบเครือข่ายภายในกับภายนอก สำนักงานก็ให้ความสำคัญกับการจัดให้มีระบบป้องกันการบุกรุกจากบุคคลภายนอก เช่น Firewall เป็นต้น และระบบป้องกันไวรัสหรือ malicious code อื่นๆ ทั้งนี้ ระบบต่างๆ ตามที่กล่าว รวมทั้งการใช้รหัสผ่านและสิทธิของผู้ใช้งาน ก็ควรมีการตรวจสอบอย่างสม่ำเสมอ

**3. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)** โดยทั่วไประบบงานคอมพิวเตอร์ มักมีการพัฒนา แก้ไขหรือเปลี่ยนแปลงอยู่ตลอดเวลา ด้วยเหตุนี้ วิธีการจัดการและการควบคุมเกี่ยวกับการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์จึงเป็นเรื่องที่สำนักงานให้ความสำคัญ โดยหากมิได้มีวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ระบบงานคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้อง หรืออาจไม่เป็นไปตามความต้องการของผู้ใช้งานได้ (integrity risk)

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ โดยหากการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีการร้องขอจากผู้ใช้งาน การร้องขอนั้น ก็ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ ควรจัดทำให้เป็นลายลักษณ์อักษร และควรกำหนดให้มีการทดสอบก่อนการใช้งานจริงทั้งจากเจ้าหน้าที่พัฒนาระบบและผู้ใช้งาน เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา แก้ไขหรือเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน นอกจากนี้ ควรจัดให้มีเอกสารประกอบการพัฒนา แก้ไขหรือเปลี่ยนแปลงโปรแกรมของระบบงานคอมพิวเตอร์ที่มีรายละเอียดเพียงพอเกี่ยวกับโปรแกรมที่ใช้อยู่ปัจจุบัน ทั้งนี้ การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของสำนักงาน ดังนั้น จึงควรมีการสอบทานกฎเกณฑ์ที่เกี่ยวข้องก่อนการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์

**4. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน** ในการดำเนินธุรกิจ มีหลายกรณีที่อาจทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย เช่น การติดไวรัส สภาวะแวดล้อมหรือภัยพิบัติต่างๆ หรืออาจเกิดจากการปฏิบัติงานที่ผิดพลาดของผู้ใช้งาน เป็นต้น ดังนั้น สำนักงานจึงให้ความสำคัญกับการสำรองข้อมูลและระบบงานคอมพิวเตอร์ รวมทั้งการเตรียมพร้อมกรณีฉุกเฉินต่างๆ ดังนี้

**4.1 การสำรองข้อมูลและระบบงานคอมพิวเตอร์** หากมิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ที่เพียงพอในกรณีที่เกิดเหตุการณ์ที่ทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย บริษัทหลักทรัพย์ก็อาจไม่มีข้อมูลหรือระบบงานคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของบริษัทหลักทรัพย์เองและอาจก่อให้เกิดความเสียหายต่อลูกค้าได้

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์ และการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

**4.2 การเตรียมพร้อมกรณีฉุกเฉิน** การสำรองข้อมูลและระบบงานคอมพิวเตอร์เพียงอย่างเดียวอาจไม่เพียงพอแก่การป้องกันการหยุดชะงักของการดำเนินธุรกิจ ดังนั้น การจัดให้มีแผนฉุกเฉินเพื่อรองรับในกรณีที่อาจเกิดเหตุการณ์ฉุกเฉิน จะทำให้การควบคุมความเสี่ยงด้าน availability risk มีประสิทธิภาพมากขึ้น

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับการจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินต่างๆ ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งควรมีการทดสอบแผนดังกล่าวเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

**5. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์** การปฏิบัติงานประจำด้านคอมพิวเตอร์ที่สำคัญคือ การควบคุมการประมวลผลข้อมูล ซึ่งการประมวลผลข้อมูลที่ถูกต้องและครบถ้วนมีความสำคัญต่อการประกอบธุรกิจของบริษัทหลักทรัพย์ ซึ่งหากมิได้มีวิธีการปฏิบัติและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน (integrity risk) ซึ่งอาจก่อให้เกิดความเสียหายต่อบริษัทหลักทรัพย์เองและลูกค้าได้ นอกจากที่กล่าว ยังมีงานประจำอื่นที่สำคัญ เช่น การดูแลการทำงานของระบบคอมพิวเตอร์ การย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริง การสำรองข้อมูลและระบบงานคอมพิวเตอร์ เป็นต้น ซึ่งหากมิได้มีวิธีการปฏิบัติและควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ เช่น ความเสี่ยงด้าน integrity risk ในกรณีที่ย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริงไม่ครบถ้วน ความเสี่ยงด้าน availability risk ในกรณีที่มิได้มีการดูแลการทำงานของระบบคอมพิวเตอร์อย่างเพียงพอ เป็นต้น

**แนวทางการกำกับดูแล** สำนักงานให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงาน

ประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชา การปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงาน และการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ