ผลการตรวจสอบ

ขอบเขตการตรวจสอบ

การตรวจสอบการดำเนินงานของบริษัทหลักทรัพย์ เอสบีไอ ไทย ออนไลน์ จำกัด (“บริษัท”) ครั้งนี้เป็นการตรวจสอบครั้งที่ 2 ระหว่างวันที่ 6 - 17 มิถุนายน 2565 โดยมีขอบเขตข้อมูลที่ใช้ในการตรวจสอบระหว่างวันที่ 1 เมษายน 2564 ถึง 31 มีนาคม 2565

วัตถุประสงค์ของการตรวจสอบ

เพื่อประเมินประสิทธิภาพของบริษัทในการกำกับดูแลตนเองและความเสี่ยงในการดำเนินงานของบริษัทตามแนวทาง RBA โดยให้ความสำคัญในเรื่องการกำกับดูแลของบริษัทแม่และการเข้าถึงข้อมูลลูกค้าของบริษัทโดยบริษัทแม่ การทำความรู้จักและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Know Your Customer/Customer Due Diligence : “KYC/CDD”) การป้องกันการส่งคำสั่งซื้อขายที่ไม่เหมาะสม การให้กู้ยืมเงินเพื่อซื้อหลักทรัพย์ การปฏิบัติงานด้านการดูแลรักษาทรัพย์สินและข้อมูลของลูกค้า การจัดทำแบบรายงานสำคัญ และการกำกับดูแลการปฏิบัติงาน

ผลการตรวจสอบ

ผลการประเมินความเสี่ยงตามแนวทาง RBA ของบริษัทพบว่า บริษัทมีความเสี่ยง (risk)[1] โดยรวม อยู่ในระดับปานกลาง ดังนี้

ประเด็นจากการตรวจสอบ	การติดตามแก้ไขของบริษัท	การดำเนินการ/สั่งการของสำนักงาน
1. Prudential Risk อยู่ในระดับปานกลาง ไม่มีข้อสังเกต		
2. Operational/Management Risk อยู่ในระดับปานกลาง		

[1] Risk มี 5 ระดับ คือ 1 = ต่ำ 2 = ค่อนข้างต่ำ 3 = ปานกลาง 4 = ค่อนข้างสูง 5 = สูง

ประเด็นจากการตรวจสอบ	การติดตามแก้ไขของบริษัท	การดำเนินการ/สั่งการของสำนักงาน
<u>ประเด็นสำคัญ</u> 2.1 การดำเนินการเพื่อแบ่งแยกหน้าที่ระหว่าง front office และ back office ของบริษัทยังไม่รัดกุมเพียงพอ โดยบริษัทกำหนดสิทธิให้หน่วยงาน Customer Services (“CS”) ซึ่งทำหน้าที่ให้บริการลูกค้าและตอบคำถามเกี่ยวกับบริการด้านการซื้อขายแก่ลูกค้า ซึ่งถือว่าเป็นงานด้าน front office แต่หน่วยงานดังกล่าวสามารถเข้าถึงข้อมูลลูกค้าได้มากเกินความจำเป็น โดยสามารถเข้าถึงรายละเอียดธุรกรรมของลูกค้าทั้งหมดในระบบงานด้าน back office ซึ่งอาจทำให้ข้อมูลลูกค้ารั่วไหลและไม่เป็นไปตามหลักการควบคุมภายในที่ดี	บริษัทได้ยกเลิกสิทธิในการเข้าถึงข้อมูลในระบบงานด้าน back office ของหน่วยงาน CS โดยให้หน่วยงาน CS ดูข้อมูลจากแหล่งอื่น หรือสอบถามข้อมูลจากฝ่ายปฏิบัติการหลักทรัพย์เป็นรายกรณี	ให้บริษัทพิจารณาความเหมาะสมในการกำหนดสิทธิการเข้าถึงข้อมูลโดยคำนึงถึงหลัก need to know เพื่อรักษาความลับของข้อมูลลูกค้า หลักการแบ่งแยกหน้าที่ระหว่าง front และ back office ให้มีความรัดกุมเพื่อไม่ให้เป็นช่องทางให้เกิดการทุจริต และปฏิบัติให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act : PDPA) รวมทั้งควบคุมดูแลการปฏิบัติงานให้เป็นไปตามแนวทางที่บริษัทแก้ไขอย่างเคร่งครัด
2.2 การดำเนินการในการทำ KYC/CDD ลูกค้าบางกรณีไม่รัดกุมเพียงพอที่จะทำให้มั่นใจได้ว่าบริษัทรู้จักและระบุตัวตนหรือผู้รับผลประโยชน์ที่แท้จริงของลูกค้า รวมทั้งป้องกันการกระทำที่อาจไม่เหมาะสมได้อย่างมีประสิทธิภาพ กล่าวคือ บริษัทมีการเปิดบัญชีซื้อขายได้ทั้งแบบ online และ offline ซึ่งบริษัทจะมีตรวจสอบเพื่อป้องกันไม่ให้ลูกค้าใช้ข้อมูลซ้ำกับลูกค้ารายอื่น และฝ่ายปฏิบัติการหลักทรัพย์จะมีการตรวจสอบความสัมพันธ์ระหว่างลูกค้ากับพนักงานอีกครั้ง	บริษัทดำเนินการดังนี้ 1. ตรวจสอบข้อมูลลูกค้าที่มีข้อมูลซ้ำกัน ซึ่งพบว่าลูกค้ามีความสัมพันธ์กัน รวมทั้งแจ้งให้ลูกค้าแก้ไขข้อมูลให้เป็นข้อมูลที่แท้จริงของลูกค้าดังกล่าว 2. ปรับปรุงระบบให้สามารถ update ข้อมูลพร้อมกันทุกระบบได้ 3. ปรับปรุงโปรแกรมตรวจสอบข้อมูลซ้ำให้สามารถ	ให้บริษัทระมัดระวังการปฏิบัติงานเพื่อให้ทราบตัวตนของลูกค้าและเจ้าของบัญชีที่แท้จริง รวมทั้งควบคุมดูแลการปฏิบัติงานให้เป็นไปตามแนวทางที่บริษัทแก้ไขอย่างเคร่งครัด

ประเด็นจากการตรวจสอบ	การติดตามแก้ไขของบริษัท	การดำเนินการ/สั่งการของสำนักงาน
แต่จากการตรวจสอบยังพบว่า มีลูกค้าบางรายมีการใช้ e-mail address และหมายเลขโทรศัพท์เดียวกัน	ตรวจสอบข้อมูลในขั้นตอนการเปิดบัญชีและกรณีลูกค้าขอเปลี่ยนแปลงข้อมูลภายหลังได้ 4. กำชับฝ่ายปฏิบัติการหลักทรัพย์ให้เพิ่มความระมัดระวังในการติดตามลูกค้าเมื่อพบว่า ลูกค้ามีการใช้ข้อมูลซ้ำกัน	
3. Customer Relationship Risk อยู่ในระดับปานกลาง ไม่มีข้อสังเกต		

ข้อมูล ณ วันที่ 24 สิงหาคม 2565