ประเด็นคำถามที่ถามบ่อย (FAQ) (เพิ่มเติม)

ลำดับ	คำถาม	คำตอบ
1. บทนิยาม		
1.1	"งานที่สำคัญ" หมายถึง งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้า การดำเนินงานธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ขอคำอธิบายเพิ่มเติมของคำว่า "มีนัยสำคัญ"	ผู้ประกอบธุรกิจต้องประเมินความเสี่ยงของงานที่ต้องพึ่งพาระบบสารสนเทศ โดยในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่รองรับงานดังกล่าว และก่อให้เกิดความเสียหายต่อข้อมูลหรือทรัพย์สินของลูกค้าและการประกอบธุรกิจ ผลการดำเนินงานและชื่อเสียงของผู้ประกอบธุรกิจ ซึ่งเกินกว่าระดับที่ผู้ประกอบธุรกิจยอมรับได้ ให้ถือว่าผลกระทบดังกล่าวมีนัยสำคัญ และผู้ประกอบธุรกิจต้องจัดให้งานดังกล่าวเป็นงานที่สำคัญ
2. การปฏิบัติงานจากภายนอกบริษัท (teleworking)		
2.1	จากหลักเกณฑ์ที่กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้องและเพื่อน เป็นต้น ผู้ประกอบธุรกิจต้องดำเนินการอย่างไรเพื่อให้มั่นใจว่าได้ปฏิบัติเป็นไปตามหลักเกณฑ์ดังกล่าว	ผู้ประกอบธุรกิจอาจใช้วิธีการกำหนดนโยบายเพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานจากภายนอกบริษัท เช่น จัดให้มีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) การ log-off จากระบบเมื่อใช้งานเสร็จสิ้น และการกำหนดรหัสผ่าน เป็นต้น พร้อมทั้งจัดให้มีการซักซ้อมและสร้างความตระหนักรู้แก่พนักงานเพื่อให้มีการปฏิบัติตามนโยบายดังกล่าวอย่างเคร่งครัด
3. การใช้บริการ cloud computing		
3.1	จากหลักเกณฑ์ที่กำหนดให้ผู้ประกอบธุรกิจต้องจัดทำข้อตกลงกับผู้ให้บริการ cloud computing โดยกำหนดใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication ข้อกำหนดดังกล่าวครอบคลุมถึงระบบที่ผู้ประกอบธุรกิจให้บริการลูกค้าหรือไม่	ผู้ประกอบธุรกิจสามารถใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication กับระบบที่ให้บริการลูกค้าได้ โดยขั้นต่ำต้องครอบคลุมถึงกรณีการให้บริการเปลี่ยนแปลงข้อมูลส่วนตัว (profile) และรหัสผ่านเพื่อใช้งานระบบดังกล่าว

ลำดับ	คำถาม	คำตอบ
3.2	กรณีที่ผู้ประกอบธุรกิจใช้บริการผ่านตัวแทนจัดจำหน่าย (cloud distributor) ของผู้ให้บริการ cloud computing (cloud provider) ถือเป็นการ sub cloud หรือไม่ และ cloud distributor ต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศในระดับสากล (เช่น ISO27001) ด้วยหรือไม่	กรณีดังกล่าว cloud distributor เป็นเพียงผู้จัดหาระบบ cloud computing จึงไม่จัดเป็นการ sub cloud ดังนั้น cloud distributor จึงไม่ต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศในระดับสากล อย่างไรก็ดี cloud provider ที่ cloud distributor จัดหาให้ยังคงต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศดังกล่าว
4. <u>การจัดทำ penetration test</u>		
4.1	ควรกำหนดขอบเขตการจัดทำ penetration test อย่างไร	ผู้ประกอบธุรกิจต้องประเมินความเสี่ยงของระบบงานที่สำคัญ โดยอาจพิจารณาจากการวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) ทั้งนี้ กรณีระบบงานที่มีผลกระทบสูง ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบอย่างเข้มงวด เพื่อทราบถึงช่องโหว่ของระบบ (vulnerability scanning) และการใช้ประโยชน์จากช่องโหว่ (exploitation test) ทั้งนี้ ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการควบคุมเพื่อให้กระบวนการทดสอบส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด
5. การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)		
5.1	ในการจัดเก็บหลักฐานการเข้าถึงระบบฐานข้อมูล (authentication log) หากผู้ประกอบธุรกิจใช้บริการจากผู้ให้บริการภายนอก โดยมีเครื่องแม่ข่ายของระบบฐานข้อมูล (database server) อยู่ที่ผู้ให้บริการภายนอก และผู้ให้บริการภายนอกมีการว่าจ้างผู้ตรวจสอบภายนอก (external auditor) ให้ตรวจสอบการเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจแล้ว ผู้ประกอบธุรกิจไม่ต้องจัดเก็บและติดตามวิเคราะห์ log ดังกล่าวได้หรือไม่	ผู้ประกอบธุรกิจต้องจัดเก็บและติดตามวิเคราะห์ log การเข้าถึงระบบฐานข้อมูลดังกล่าว เว้นแต่กรณีที่ผู้ประกอบธุรกิจได้จัดให้มีข้อกำหนดที่ทำให้มั่นใจว่าผู้ให้บริการภายนอกได้ให้ผู้ตรวจสอบภายนอกตรวจสอบ log การเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจ และจัดให้มีการเปิดเผยผลการตรวจสอบให้ผู้ประกอบธุรกิจรับทราบ โดยผลการตรวจสอบดังกล่าวต้องมีรายละเอียดขั้นต่ำเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน

ลำดับ	คำถาม	คำตอบ
6. การจัดเก็บข้อมูล electronic messaging		
6.1	electronic messaging ครอบคลุมถึงอะไรบ้าง ต้องจัดเก็บเนื้อหาอะไร และจัดเก็บเฉพาะกรณีผู้ติดต่อกับลูกค้าได้หรือไม่	electronic messaging คือ การสื่อสารผ่านช่องทางอิเล็กทรอนิกส์ เช่น การสนทนาโดยใช้จดหมายอิเล็กทรอนิกส์ (e-mail) โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) และระบบเครือข่ายสังคมออนไลน์ (social networking) เป็นต้น โดยต้องจัดเก็บเนื้อหาการสนทนาทั้งหมดสำหรับบุคคลที่เป็น access person ตามประกาศว่าด้วยแนวทางปฏิบัติเกี่ยวกับระบบงานในการป้องกันมิให้เกิดการกระทำที่อาจมีความขัดหรือแย้งกับประโยชน์ของลูกค้า
7. <u>การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์</u> <u>(communication security)</u>		
7.1	ผู้ประกอบธุรกิจต้องดำเนินการอย่างไร ในกรณีที่มีบุคลากรไม่เพียงพอที่จะแบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ได้	ในระยะแรกผู้ประกอบธุรกิจอาจจัดให้มีมาตรการหรือวิธีการควบคุมอื่นใดที่แสดงให้เห็นได้ว่าสามารถแบ่งแยกหน้าที่ความรับผิดชอบดังกล่าวได้อย่างมีประสิทธิภาพ เช่น จัดให้มีการบันทึก จัดเก็บหลักฐาน (log) การปฏิบัติงานของบุคลากรผู้ปฏิบัติหน้าที่ network administrator และ computer administrator รวมทั้งจัดให้มีการติดตามวิเคราะห์หลักฐานดังกล่าวอย่างสม่ำเสมอโดยบุคคลที่เป็นอิสระจากผู้ปฏิบัติหน้าที่ network administrator และ computer administrator เป็นต้น
8. <u>การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ</u> <u>(information Security incident management)</u>		
8.1	กรณีที่ระบบ settrade หยุดชะงัก ผู้ประกอบธุรกิจที่เป็นบริษัทหลักทรัพย์ทุกแห่งต้องรายงานสำนักงานให้ทราบหรือไม่	ผู้ประกอบธุรกิจแต่ละรายต้องรายงานสำนักงานเมื่อระบบ settrade หยุดชะงัก เฉพาะในกรณีที่ส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของ

ลำดับ	คำถาม	คำตอบ
		ผู้ประกอบธุรกิจอย่างมีนัยสำคัญเท่านั้น เพื่อให้สำนักงานรับทราบถึงผลกระทบและแนวทางดำเนินการรองรับเหตุการณ์ดังกล่าว