– Practice Guide

สารบัญ

บทสรุปสำหรับผู้บริหาร..... 1
บทนำ..... 2
บทบาทของตรวจสอบภายในและงานที่ได้รับมอบหมาย..... 7
การประเมินองค์ประกอบ BCM ที่สำคัญโดยตรวจสอบภายใน..... 10
กิจกรรมตรวจสอบภายในก่อนภาวะวิกฤต..... 13
กิจกรรมตรวจสอบภายในในระหว่างภาวะวิกฤตและหลังภาวะวิกฤต..... 14
ภาคผนวก..... 17
ผู้เขียน & ผู้สอบทาน..... 35

บทสรุปสำหรับผู้บริหาร

การบริหารเพื่อความต่อเนื่องทางธุรกิจ (Business continuity management หรือ BCM) เป็นการเตรียมความพร้อมขององค์กร สำหรับเหตุการณ์ในอนาคตหรือภาวะวิกฤตที่อาจขัดขวางการบรรลุวัตถุประสงค์ในทางธุรกิจ การบริหารภาวะวิกฤต (Crisis management หรือ CM) เป็นองค์ประกอบสำคัญของ BCM และเกี่ยวข้องกับการสื่อสารข้อมูลเกี่ยวกับภาวะวิกฤตไปยังผู้มีส่วนได้เสียขององค์กร

ทักษะรวมทั้งคุณสมบัติที่กว้างขวางและลึกซึ้งของตรวจสอบภายใน ตำแหน่งภายในองค์กร และความรู้ในเชิงลึกเกี่ยวกับการดำเนินงานทั่วทั้งองค์กร ทำให้ตรวจสอบภายในอยู่ในสถานะที่จะช่วยในการพัฒนา การดำเนินการ และการประเมินโครงการเกี่ยวกับ BCM และ CM ขององค์กรได้ ตรวจสอบภายในอาจมีบทบาทได้หลากหลายทั้งในบทบาทหลักและบทบาทที่เป็นผู้ให้การสนับสนุน ทั้งนี้ ขึ้นอยู่กับการมีอยู่ และ/หรือวุฒิภาวะของโครงการที่เกี่ยวกับ BCM และ CM รวมถึงความรุนแรงและสถานการณ์ของภาวะวิกฤต

บทบาทของตรวจสอบภายในอาจเกี่ยวข้องกับการให้บริการให้ความเชื่อมั่นและให้คำปรึกษา ทั้งก่อน ระหว่าง และหลังการเกิดภาวะวิกฤต ทั้งบริการให้ความเชื่อมั่นและบริการให้คำปรึกษาจำเป็นต้องมีความรู้อย่างเชี่ยวชาญเกี่ยวกับองค์ประกอบที่สำคัญของ BCM ซึ่งรวมถึง การกำกับดูแลโครงการ การบริหารความเสี่ยง การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) รวมทั้งการวางแผนเพื่อความต่อเนื่องทางธุรกิจและการกอบกู้สถานการณ์ (BCRP)

- งานให้ความเชื่อมั่น อาจดำเนินการเพื่อสอบทานว่า BCM และ CM นั้นมีประสิทธิผล
- งานบริการให้คำปรึกษา อาจดำเนินการเพื่อช่วยให้ฝ่ายบริหารมุ่งเน้นในกิจกรรมการวางแผน และเชื่อมโยง BCM และ CM กับความเสี่ยงและวิธีการควบคุม

ในระหว่างสถานการณ์วิกฤตผู้ตรวจสอบภายในอาจได้รับการคาดหวังและได้รับอนุญาตให้แสดงบทบาทสำคัญซึ่งเป็นงานที่ไม่ได้เกี่ยวกับการตรวจสอบ เพื่อสนองความต้องการขององค์กร

บทนำ

แนวทางการตรวจสอบทางเทคโนโลยีระดับโลก ของ IIA (The IIA Global Technology Audit Guide หรือ GTAG) ฉบับที่ 10 เรื่อง *การบริหารเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity Management)* ซึ่งกล่าวถึงความสำคัญของ BCM สามารถใช้เป็นข้อมูลอ้างอิงที่มีค่ายิ่งสำหรับองค์ประกอบหลักต่างๆ ซึ่งจะต้องมีในแผนงาน BCM ที่มีประสิทธิผล และให้ทิศทางสำหรับความต่อเนื่องของโครงสร้างพื้นฐานด้านไอทีที่สำคัญ และระบบแอพพลิเคชั่นด้านธุรกิจทั้งในระหว่างภาวะวิกฤตและหลังภาวะวิกฤตแล้ว แนวปฏิบัติ (practice guide) นี้ขยายเรื่องการบริหารเพื่อความต่อเนื่องทางธุรกิจออกไปให้กว้างขึ้น โดยได้พูดคุยถึงบทบาทที่เป็นไปได้ของผู้ตรวจสอบในการจัดการภาวะวิกฤต และได้ให้แนวทางเกี่ยวกับ:

- กิจกรรมของตรวจสอบภายในก่อนภาวะวิกฤต ระหว่างภาวะวิกฤต และภายหลังภาวะวิกฤต
- การประเมินองค์ประกอบที่สำคัญของการบริหารเพื่อความต่อเนื่องทางธุรกิจ (BCM) ของตรวจสอบภายใน

คู่มือช่วยปฏิบัติ (Practice aid) ที่ได้ให้ไว้ในภาคผนวกประกอบด้วย รายการเช็คสอบ (checklist) การประเมินความเสี่ยง ตัวอย่างแนวทางการตรวจสอบ อภิธานศัพท์ และข้อมูลอ้างอิง

ความสำคัญทางธุรกิจและความเสี่ยงที่เกี่ยวข้อง

องค์กรทั้งหลายในที่สุดแล้วย่อมจะต้องเผชิญกับการหยุดชะงักทางธุรกิจ แผน BCM/CM ที่ได้กำหนดไว้เป็นอย่างดีนั้นเปรียบเสมือนเป็นกรมธรรม์ประกันภัยสำหรับองค์กร กล่าวคือ ช่วยให้มั่นใจได้ว่าองค์กรจะยังคงทำงานและตอบสนองความคาดหวังของผู้มีส่วนได้ส่วนเสียได้ แผน BCM/CM ยังเป็นอีกเวทีหนึ่งสำหรับตรวจสอบภายในที่จะใช้ในการอัพเดทข้อมูลและสื่อสารอย่างต่อเนื่องเกี่ยวกับการบริหารความเสี่ยงและการควบคุมที่มีประสิทธิผลได้ทั่วองค์กร

แผนการบริหารจัดการภาวะวิกฤต (Crisis management plans หรือ CMP) เป็นการรวมเอามาตรการในการบริหารความเสี่ยงเชิงป้องกันและการตอบสนองสำหรับสถานการณ์ภาวะวิกฤตเฉียบพลันเข้าไว้ด้วยกัน CMP ที่จัดทำหรือสื่อสารไม่ดีรวมทั้งมีการทดสอบหรือการฝึกอบรมที่ไม่เพียงพอ อาจยกระดับความเสี่ยงขององค์กรจากภาวะวิกฤตจนไปถึงระดับที่ไม่สามารถยอมรับได้ CMP ที่พัฒนาขึ้นภายหลังจากเกิดภาวะวิกฤตโดยอาศัยข้อมูลของภาวะวิกฤตที่เพิ่งผ่านมาเป็นหลักในการจัดทำเนื้อหา อาจจะไม่ครอบคลุมเพียงพอที่จะทำให้มีประสิทธิผลได้ สำหรับองค์กรภาครัฐ รวมถึงรัฐบาลผลกระทบจากภาวะวิกฤตหรือเหตุการณ์ต่างๆ อาจกระทบเป็นวงกว้างทั้งในประเทศและระหว่างประเทศได้

CMP ที่ครอบคลุมและมีการสื่อสารเป็นอย่างดีอาจช่วยนำทางให้องค์กรต่างๆ ผ่านวิกฤตและความเสี่ยงที่เกี่ยวข้องได้อย่างมีประสิทธิผล ยิ่งกว่านั้น CMP อาจช่วยปรับปรุงความยืดหยุ่น (resilience) ขององค์กรให้ดีขึ้นได้เมื่อเผชิญกับภาวะวิกฤต เครื่องมือและโครงการ CM เมื่อได้มีการจัดทำอย่างรอบคอบ มีการสอบยันเป็นระยะๆ ได้รับการสนับสนุนและอนุมัติโดยฝ่ายบริหารและ/หรือคณะกรรมการ จะช่วยให้องค์กรสามารถบริหารจัดการเหตุการณ์ต่างๆ และบรรเทาความเสี่ยงโดยรวมในด้านการดำเนินงาน ชื่อเสียง ด้านการเงินกฎระเบียบ รวมทั้งปัจจัยเสี่ยงทางด้านกฎหมายสำหรับผู้มีส่วนได้เสียที่สำคัญทั้งภายในและภายนอกได้

มาตรฐานและแนวทางของ IIA ที่เกี่ยวข้อง

มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (มาตรฐาน) ในส่วนที่เกี่ยวข้องกับ BCM และ CM ได้แก่:

มาตรฐาน 2100: ลักษณะของงาน

หน่วยงานตรวจสอบภายในต้องประเมินและมีส่วนร่วมในการปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กรโดยใช้วิธีการที่เป็นระบบมีระเบียบ

มาตรฐาน 2110: การกำกับดูแล

หน่วยงานตรวจสอบภายในต้องประเมินและให้คำแนะนำที่เหมาะสมเพื่อปรับปรุงกระบวนการกำกับดูแลขององค์กรในการบรรลุวัตถุประสงค์ดังต่อไปนี้:

- การเสริมสร้างความมีจริยธรรมและคุณค่าที่เหมาะสมภายในองค์กร
- การทำให้เชื่อมั่นได้ในเรื่องการบริหารผลการปฏิบัติงานขององค์กรและความรับผิดชอบในผลของงานที่มีประสิทธิผล
- การสื่อสารข้อมูลเกี่ยวกับความเสี่ยงและการควบคุมไปยังส่วนงานต่าง ๆ ที่เหมาะสมภายในองค์กร
- การประสานกิจกรรมและสื่อสารข้อมูลระหว่างคณะกรรมการ ผู้สอบบัญชี ผู้ตรวจสอบภายใน และผู้บริหารขององค์กร

มาตรฐาน 2120: การบริหารความเสี่ยง

หน่วยงานตรวจสอบภายในต้องประเมินความมีประสิทธิผลและมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง

มาตรฐาน 2400: การสื่อสารผลการปฏิบัติงาน

ผู้ตรวจสอบภายในต้องสื่อสารผลของการปฏิบัติงานที่ได้รับมอบหมาย

นิยามของแนวคิดหลัก

BCM คือกระบวนการที่องค์กรเตรียมการสำหรับอุบัติการณ์หรือภาวะวิกฤตในอนาคตที่อาจเป็นอันตรายต่อพันธกิจหลักขององค์กร รวมทั้งความสามารถในการดำเนินงานได้อย่างต่อเนื่องทั้งระยะสั้นและระยะยาวและตอบสนองความคาดหวังของผู้มีส่วนได้เสียได้ CM (ซึ่งถือว่าเป็นองค์ประกอบสำคัญของ BCM) จะกล่าวถึงวิธีการที่องค์กรจะแจ้งให้สาธารณชน พนักงาน หุ้นส่วนทางธุรกิจ และผู้มีส่วนได้ส่วนเสียต่างๆ ทราบถึงภัยพิบัติหรือภาวะวิกฤตรวมทั้งขั้นตอนต่างๆ ที่กำลังกระทำอยู่เพื่อให้ธุรกิจกลับมาดำเนินการได้ และลดผลกระทบต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก CMP เป็นการรวมรายการกิจกรรมต่างๆ ซึ่งเป็นมาตรการเชิงป้องกันและการตอบสนองต่อสถานการณ์ที่ดำเนินการโดยองค์กรใดๆ เพื่อบรรเทาและจัดการกับความเสี่ยงที่เกิดจากภาวะวิกฤตหรือเหตุการณ์ได้อย่างมีประสิทธิผล

การบริหารเพื่อความต่อเนื่องทางธุรกิจ (BCM)

BCM เป็นแนวทางการบริหารความเสี่ยงโดยอิงตามคุณค่าในทางธุรกิจ ซึ่งจัดทำเพื่อให้ความสามารถในการดำเนินงานทางธุรกิจอย่างต่อเนื่องเป็นไปในทิศทางเดียวกันกับความเสี่ยงต่างๆ เป้าหมายของ BCM คือการทำให้องค์กรสามารถกอบกู้กิจกรรมการปฏิบัติงานที่สำคัญ บริหารการสื่อสาร และลดผลกระทบทางการเงินรวมทั้งผลกระทบอื่นๆ ที่มาจากภัยพิบัติ การหยุดชะงักทางธุรกิจ หรือเหตุการณ์สำคัญอื่นๆ BCM เป็นเรื่องของการบริหารความเสี่ยงที่ออกแบบมาเพื่อก่อให้เกิดความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่องโดยเข้าได้กับความเสี่ยงที่อาจเกิดขึ้นบนพื้นฐานของคุณค่าทางธุรกิจ ในขณะที่คำศัพท์ที่ใช้ในหนังสือตำราของบางสายอาชีพอาจแตกต่างกันออกไป คำว่า BCM ที่ใช้ในแนวปฏิบัตินี้ จะกล่าวถึงนโยบาย/ต้นแบบ/กรอบ สำหรับการบริหารการหยุดชะงักในการให้บริการประเภทต่างๆ ที่ถูกกระตุ้นโดยเหตุการณ์ภายในหรือภายนอกองค์กร คำนิยามนี้อาจประยุกต์ใช้กับองค์กรภาครัฐ เช่นรัฐบาลด้วยก็ได้ สำหรับองค์กรภาครัฐเหล่านี้ คำว่าธุรกิจหมายถึงหน่วยงานภาครัฐ การดำเนินงานสำหรับสาธารณะที่สำคัญ ความปลอดภัยของประชาชน และความมั่นคงปลอดภัยขององค์ประกอบต่างๆ ของหน่วยงานเหล่านั้น

ส่วนประกอบที่สำคัญของ BCM ได้แก่:

- **การสนับสนุนจากฝ่ายบริหาร** – ฝ่ายบริหารแสดงให้เห็นถึงการสนับสนุนในการเตรียมการ การรักษาไว้ และดำเนินการตามแผนเพื่อความต่อเนื่องทางธุรกิจ (BCP) อย่างเหมาะสม ด้วยการจัดให้มีทรัพยากร บุคลากร และงบประมาณที่เพียงพอ
- **การประเมินความเสี่ยงและการลดความเสี่ยง** – การระบุความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคาม เช่น ไฟไหม้หรือน้ำท่วม และมีการตัดสินถึงความน่าจะเป็นและผลกระทบที่อาจเกิดขึ้นต่อองค์กร การประเมินนี้จัดทำในระดับพื้นที่ปฏิบัติงานและในระดับสายงาน เพื่อให้มั่นใจว่ามีความเข้าใจในความเสี่ยงจากเหตุการณ์ต่างๆ ที่เป็นไปได้และความเสี่ยงเหล่านั้นได้รับการบริหารจัดการอย่างเหมาะสม
- **การวิเคราะห์ผลกระทบทางธุรกิจ** (Business Impact Analysis **หรือ** BIA) – การระบุกระบวนการทางธุรกิจต่างๆ ที่เป็นส่วนสำคัญที่จะทำให้ธุรกิจยังคงทำงานได้ในช่วงภัยพิบัติ และเพื่อตัดสินว่ากระบวนการทางธุรกิจที่สำคัญเหล่านี้ควรได้รับการกอบกู้ภายหลังจากภัยพิบัติเร็วมากน้อยเพียงใด
- **กลยุทธ์ในการกอบกู้และเพื่อความต่อเนื่องทางธุรกิจ** – ระบุขั้นตอนจริง บุคลากร และทรัพยากรที่จำเป็นสำหรับการกอบกู้กระบวนการทางธุรกิจที่สำคัญ และควรระบุกลไกการสื่อสารและระเบียบพิธีการที่สำคัญไว้ด้วย กลยุทธ์นี้อาจพิจารณาจากมาตรฐาน หรือเกณฑ์มาตรฐานของบริษัทหรืออุตสาหกรรม
- **การตระหนักรู้ในแผนและการฝึกอบรม** - การให้ความรู้และความตระหนักรู้ในแผน BCP มีความสำคัญยิ่งต่อการดำเนินการตามแผน BCM การฝึกอบรมอาจรวมถึงการทำแบบฝึกหัด และ/หรือการฝึกซ้อม (drill) สำหรับบางส่วนของแผน BCP
- **การรักษาไว้** – ความสามารถและเอกสารประกอบเกี่ยวกับ BCM ต้องได้รับการดูแลรักษาเพื่อให้มั่นใจได้ว่า ยังคงมีประสิทธิผลและสอดคล้องกับลำดับความสำคัญของธุรกิจ

การบริหารภาวะวิกฤต (Crisis Management)

CM เป็นองค์ประกอบสำคัญของ BCM ที่เกิดขึ้นเมื่อการหยุดชะงักของการให้บริการทางธุรกิจเพิ่มขึ้นจนถึงระดับที่เรียกว่าเป็นภาวะวิกฤตหรือภัยพิบัติ CM จะบันทึกวิธีการที่ใช้ในการตอบสนองต่อสภาพความเป็นจริงและการรับรู้ถึงภาวะวิกฤต CM ยังเกี่ยวข้องกับการสร้างเกณฑ์วัดเพื่อกำหนดว่าสถานการณ์ใดที่ก่อให้เกิดภาวะวิกฤต และดังนั้น จะเป็นตัวกระตุ้นกลไกในการตอบสนองที่จำเป็น ซึ่งจะประกอบด้วยการสื่อสารที่เกิดขึ้นในระยะของการตอบสนองของสถานการณ์การบริหารเหตุฉุกเฉิน

ประเภทของการหยุดชะงัก

BCM จะหาหนทางที่จะจัดการกับภัยคุกคามที่เกิดขึ้นทั้งภายในและภายนอก ภัยคุกคาม แต่ละอย่างมีระดับผลกระทบต่อกระบวนการทางธุรกิจขององค์กรที่แตกต่างกัน ซึ่งอาจส่งผลเสียต่อการปฏิบัติตามกฎระเบียบความปลอดภัยของบุคลากร การปกป้องสิ่งแวดล้อม ความสามารถในการรักษามาตรฐานการปฏิบัติงานและการปฏิบัติตามข้อกำหนดในสัญญา รวมทั้งเครื่องหมายการค้า/ชื่อเสียงขององค์กร ประเภทของการหยุดชะงักได้แก่:

- การโจมตีทางไซเบอร์
- เชื้อโรค / โรคระบาด
- แผ่นดินไหว / สึนามิ
- อัคคีภัย
- อุทกภัย
- พายุเฮอริเคน / พายุทอร์นาโด
- การนัดหยุดงาน
- ความล้มเหลวในการผลิต / การหยุดการผลิต
- การปนเปื้อนของผลิตภัณฑ์
- การก่อวินาศกรรม
- การหยุดให้บริการหรือผลิตภัณฑ์ที่ขาดหายไป สำหรับคู่ค้า / ผู้ขายที่สำคัญ
- ระบบขัดข้อง
- การก่อการร้าย
- ไฟฟ้าดับ

บทบาทของตรวจสอบภายในและงานที่ได้รับมอบหมาย

การกำหนดบทบาทของตรวจสอบภายใน

ผู้ตรวจสอบภายในอยู่ในสถานะที่ช่วยในการบริหารภาวะวิกฤตได้ด้วยการให้ข้อมูลเชิงลึกเกี่ยวกับการปฏิบัติงานให้แก่องค์กร หัวหน้าหน่วยงานตรวจสอบภายใน (CAE) ควรกำหนดบทบาทของตรวจสอบภายในทั้งก่อนภาวะวิกฤต ระหว่างภาวะวิกฤต และหลังภาวะวิกฤต โดยต้องระวังที่จะไม่เข้าไปทำหน้าที่เป็นเจ้าของหรือเป็นผู้บริหารความเสี่ยงต่างๆ ที่เกี่ยวข้องกับภาวะวิกฤต บ่อยครั้งที่หน่วยงานตรวจสอบภายในอาจจะได้เข้าร่วมในการประชุมเกี่ยวกับกระบวนการวางแผนการบริหารภาวะวิกฤต ในขั้นต้น CAE พร้อมทั้งผู้บริหารที่สำคัญของหน่วยงานตรวจสอบภายในควรทำความคุ้นเคยกับวิธีปฏิบัติชั้นนำเกี่ยวกับ BCM จากเอกสารอ้างอิงและมาตรฐานต่างๆ จากภายนอก สำหรับแหล่งข้อมูลต่างๆ ได้มีอยู่ในคู่มือช่วยปฏิบัติ (Practice aid) ที่ 3 ของแนวปฏิบัติฉบับนี้แล้ว เมื่อได้กำหนดบทบาทหน้าที่ต่างๆ ขึ้นมาแล้ว ควรจัดทำเป็นเอกสารและสื่อสารภายในหน่วยงานตรวจสอบ แล้วจึงค่อยสื่อสารไปยังผู้มีส่วนได้เสียภายนอกที่สำคัญซึ่งจะได้รับผลกระทบโดยตรง

หากตรวจสอบภายในหรือ CAE ไม่มีบทบาทในกระบวนการบริหารภาวะวิกฤต ควรแจ้งให้คณะกรรมการตรวจสอบทราบเพื่อไม่ให้เกิดช่องว่างในความคาดหวัง เมื่อตรวจสอบภายในให้บริการในบทบาทที่ปรึกษาแก่ฝ่ายบริหารภายในบริบทของการพัฒนาแผน BCP/CMP ควรจะต้องระบุผลกระทบที่อาจเกิดขึ้นกับความเป็นอิสระและความเที่ยงธรรมของตรวจสอบภายในให้ชัดเจน เมื่อได้มีการระบุบทบาทแล้ว ควรได้รับการอนุมัติตามสายการบังคับบัญชาทั้งจากสายการรายงานทางการบริหารและสายการรายงานตามหน้าที่ของ CAE และอาจจะบันทึกไว้ในกฎบัตรของหน่วยงานตรวจสอบภายในด้วยก็ได้

งานการให้คำปรึกษาหรืองานการให้ความเชื่อมั่นที่เกี่ยวกับ BCM

ภาระหน้าที่ของผู้ตรวจสอบภายในในการเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานและการบริหารความเสี่ยงขององค์กรนั้น ควรขยายไปสู่งานการให้ความเชื่อมั่นหรืองานการให้คำปรึกษาที่เกี่ยวกับ BCM ทั้งนี้ ขึ้นอยู่กับวุฒิภาวะของโครงการ BCM ขององค์กรด้วย การรวมเอาหน่วยงานตรวจสอบภายในให้เข้าไปมีส่วนร่วมในการวางแผน BCM และ CM หรือในกระบวนการปรับแต่งให้ดีขึ้นนั้น อาจเป็นกุญแจสำคัญไปสู่ความสำเร็จของโครงการก็ได้ โดยเฉพาะอย่างยิ่ง สำหรับองค์กรที่มีวุฒิภาวะในเรื่องนี้ในระดับต่ำ ด้วยการมีปฏิสัมพันธ์และความเข้าใจในความต้องการของคณะกรรมการและผู้บริหารระดับสูงขององค์กร ตรวจสอบภายในจะสามารถให้มุมมองและช่วยปรับภาพกิจกรรมการวางแผนให้ชัดเจนได้ การทำให้มั่นใจได้ว่าหน่วยงาน/บริเวณหลักที่

BCM จะต้องมุ่งเน้นนั้น เป็นไปในทิศทางเดียวกันกับระดับความต้องการของคณะกรรมการและผู้บริหารระดับสูง จะเป็นสิ่งสำคัญยิ่งต่อการประสบความสำเร็จ

งานการให้ความเชื่อมั่น

ตรวจสอบภายในอาจปฏิบัติงานให้ความเชื่อมั่นเป็นระยะๆ โดยทำการสอบทานว่าแผน BCP และ CMP มีความครอบคลุมพอ มีความเกี่ยวข้องกับสภาพแวดล้อมของการดำเนินธุรกิจในปัจจุบัน และได้มีการสื่อสารไปยังผู้มีส่วนได้เสียทั้งภายในและภายนอกที่เหมาะสม ความถี่ ลักษณะ และขอบเขตของงานที่ปฏิบัติจะถูกขับเคลื่อนโดยความเสี่ยงต่างๆ หรือจากการร้องขอจากผู้มีส่วนได้เสีย เพื่อให้สอบยันถึงประสิทธิผลและความเกี่ยวข้องของแผนงานที่จัดทำขึ้น

ขอบเขตของงานการให้ความเชื่อมั่นอาจรวมถึงแผนงาน BCM ทั้งหมดหรือเฉพาะบางองค์ประกอบก็ได้ (เช่น การทดสอบการเกิดขึ้น และความถี่ในการปรับปรุงข้อมูลให้เป็นปัจจุบันของแผน BCP และวุฒิภาวะ/ความสมบูรณ์ของ CMP) ความรู้ของตรวจสอบภายในเกี่ยวกับความเสี่ยงที่บรรเทาลงได้โดยแผน BCP หรือ CMP และการมีส่วนร่วมในฐานะที่ปรึกษาในช่วงระหว่างการพัฒนาแผนอาจช่วยให้กระบวนการวางแผนสำหรับงานที่ได้รับมอบหมายมีประสิทธิภาพมากขึ้นได้
งานการให้ความเชื่อมั่นอาจได้แก่:

- การร้องขอให้มีการสอบทานโครงการ BCP โดยคณะกรรมการตรวจสอบหรือผู้บริหารระดับสูง โดยทั้งหมดหรือบางส่วน ซึ่งรวมถึงการสอบทานผู้ขายหรือพันธมิตรทางธุรกิจด้วย
- การสอบทาน BCM เพื่อประเมินความสมบูรณ์ของแผน ระดับวุฒิภาวะ และความเหมาะสมโดยอิงตามความเสี่ยง การเติบโต หรือการถอนการลงทุน ขององค์กร
- การประเมินความเสี่ยงของโครงการ
- การสอบทานข้อความ/เงื่อนไขที่มีอยู่เกี่ยวกับแผน BCP/CMP ขององค์กร หรือของพันธมิตรทางธุรกิจตามที่กำหนดโดยเงื่อนไขสัญญา (ซึ่งก็คือ สิทธิ์ในการตรวจสอบ หรือข้อตกลงเกี่ยวกับระดับการให้บริการที่กำหนดไว้)

ดูคู่มือช่วยปฏิบัติ (Practice Aid) ที่ 1 สำหรับแนวทางเพิ่มเติมเกี่ยวกับการให้ความเชื่อมั่น

งานการให้คำปรึกษา

จุดสนใจของ BCM สามารถเริ่มที่การสอบทานและวิเคราะห์โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (ไอที) ได้อย่างรวดเร็ว เพราะว่าการเข้าถึงและถ่ายโอนข้อมูลถือเป็นหน้าที่งานทางธุรกิจที่สำคัญ อย่างไรก็ตาม เมื่อ

ให้บริการด้านที่ปรึกษาเกี่ยวกับ BCM/CM ตรวจสอบภายในควรพิจารณาถึงวัตถุประสงค์และความเสี่ยงขององค์กรในภาพกว้าง และไม่จำกัดอยู่เฉพาะประเด็นด้านไอที งานการให้คำปรึกษาเกี่ยวกับ BCM ไม่ควรทำให้ความเที่ยงธรรมของตรวจสอบภายในเสื่อมลง ควรใช้ความระมัดระวังโดยไม่เข้าไปยอมรับภาระหน้าที่ในการเป็นเจ้าของหรือเป็นผู้บริหารความเสี่ยงในการดำเนินธุรกิจอย่างต่อเนื่อง

การประเมินองค์ประกอบ BCM ที่สำคัญโดยตรวจสอบภายใน

โครงการ BCM ประกอบด้วยองค์ประกอบทั่วๆ ไป เช่น การกำกับดูแล การบริหารความเสี่ยง การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) และแผนเพื่อความต่อเนื่องในการดำเนินธุรกิจและการกอบกู้ระบบ (BCRP) เป็นสิ่งสำคัญยิ่งที่แต่ละองค์ประกอบนี้จะต้องเกี่ยวข้องกับผู้ให้การสนับสนุน ผู้มีส่วนได้เสีย และพันธมิตรทางธุรกิจที่ถูกต้อง เพื่อช่วยให้มั่นใจได้ว่ามีการพัฒนาแผนที่ครอบคลุม ได้รับการสนับสนุน และสามารถนำไปดำเนินการได้ ควรสื่อสารเกี่ยวกับองค์ประกอบต่างๆ รวมทั้งข้อมูลที่เกี่ยวข้องโดยรวมภายในแผนให้แก่ผู้มีส่วนได้เสียหลัก กิจกรรมของตรวจสอบภายในอาจรวมถึงการประเมินประสิทธิผลของ BCM และ CMP ด้วย

การกำกับดูแลโครงการ

กุญแจสู่ความสำเร็จของ BCM คือการสนับสนุนและทุนอุดหนุนจากผู้บริหารระดับสูง ตรวจสอบภายในสามารถช่วยระบุและสร้างความสัมพันธ์ระหว่างผู้มีส่วนได้เสียหลักใน BCM ที่อยู่ภายในองค์กร กิจกรรมต่อไปนี้อาจดำเนินการโดยตรวจสอบภายในได้ระยะเริ่มต้นของการประเมิน BCM:

- การตัดสินว่าตำแหน่งที่เป็นผู้นำสำคัญได้รับการบันทึกเป็นเอกสารและอนุมัติแล้วหรือไม่ เพื่อช่วยให้มั่นใจได้ว่ามีผู้เป็นเจ้าของและรับผิดชอบต่อโครงการขององค์กร ภาวะความเป็นผู้นำมีความสำคัญยิ่งต่อการระบุความพึ่งพาซึ่งกันและกันในแผน การส่งเสริมให้มีการปรับปรุงพัฒนาอย่างต่อเนื่อง และการเรียนรู้จากกิจกรรมต่างๆ หลังภาวะวิกฤต
- การแนะนำให้มีการสร้างกฎบัตรของ BCM กฎบัตรจะช่วยในการจัดตั้งผู้ให้ทุนอุดหนุนแก่โครงการและผู้ให้การสนับสนุนภายในระดับสูงสุดขององค์กร นอกเหนือจากการตรวจสอบการมีอยู่จริงของโครงการ BCM แล้ว กฎบัตรซึ่งกำหนดไว้เป็นอย่างดีจะกำหนดโครงสร้างการกำกับดูแล BCM (ซึ่งก็คือคณะอนุกรรมการ BCM) รวมทั้งให้แนวทางเกี่ยวกับการประเมินกฎบัตรเป็นระยะ โครงสร้างการกำกับดูแลจะเป็นผู้อนุมัติการตัดสินใจ BCM หรือ CM และก่อให้เกิดเวทีเพื่ออภิปรายความคิดเห็นสำหรับความชัดเจนในการพัฒนา การปรับปรุงแก้ไขแผน BCP หรือ CMP ทั่วทั้งองค์กร รวมทั้งการสื่อสารภายในและภายนอกที่เกี่ยวข้อง
- การประเมินว่า โครงสร้างการกำกับดูแล BCM และ CM ที่จัดตั้งขึ้นมานั้นได้รับเงินทุนสนับสนุนอย่างเพียงพอ เหมาะสม และมีประสิทธิผลในการสนองต่อความต้องการของคณะกรรมการ คณะกรรมการตรวจสอบ หรือผู้บริหารระดับสูงหรือไม่ ตรวจสอบภายในอาจมีบทบาทโดยเข้าร่วมเป็นสมาชิกที่ไม่มี

สิทธิออกเสียงลงคะแนน (nonvoting member) หรือเข้าร่วมการประชุมเพื่อให้ข้อเสนอแนะเกี่ยวกับบทบาท กฎบัตร และการทำงานของคณะดังกล่าว

- การสื่อสารและให้คำปรึกษาเกี่ยวกับการกำกับดูแล BCM ว่า มีความเหมาะสมและมีประสิทธิผลตอบสนองต่อความต้องการของคณะกรรมการ คณะกรรมการตรวจสอบ และผู้บริหารระดับสูง หรือไม่
- การแจ้งให้คณะกรรมการ (คณะกรรมการตรวจสอบ) ทราบถึงความเสี่ยงที่เกี่ยวข้อง และวิธีปฏิบัติที่เป็นเลิศในปัจจุบันสำหรับความต่อเนื่องทางธุรกิจและ CMPs

การบริหารความเสี่ยง

เพื่อให้ BCM มีประสิทธิผล จะต้องพิจารณาถึงความเสี่ยงที่ได้จัดลำดับความสำคัญที่เกี่ยวข้องไว้ซึ่งองค์กรต้องเผชิญในภาวะวิกฤต ตรวจสอบภายในมักมีความเข้าใจในรายละเอียดเกี่ยวกับความเสี่ยงหลักในทางธุรกิจ ความเสี่ยงอาจจะเพิ่มขึ้นและถูกจัดลำดับใหม่ในช่วงภาวะวิกฤต ทั้งนี้ ขึ้นอยู่กับลักษณะและขอบเขตของเหตุการณ์ที่องค์กรกำลังเผชิญอยู่ ตรวจสอบภายในอาจแบ่งปันข้อมูลเกี่ยวกับความเสี่ยงหลักขององค์กรในระหว่างการจัดตั้งโครงการและการประเมิน BCM

ความเข้าใจความเสี่ยงที่สำคัญของ BCM จะสามารถช่วยให้การพัฒนาแผนการตรวจสอบภายในที่นำเสนอเพื่อขออนุมัติให้แข็งแกร่งขึ้นได้ การเข้าร่วมกิจกรรม BCM ขององค์กร จะช่วยให้ผู้ตรวจสอบภายในสามารถระบุถึงบริเวณ/หน่วยงานที่มีความเสี่ยงที่สำคัญ ซึ่งรวมถึงทัศนคติและการสนับสนุนขององค์กร กิจกรรมการควบคุมการปฏิบัติงาน และกระบวนการหลัก และความพึ่งพาในระบบ/ข้อมูล/ผู้ขายที่เป็นไปได้ จุดอ่อนหรือความล้มเหลวในบริเวณเหล่านี้สามารถกระตุ้นให้หน่วยงานตรวจสอบภายในเน้นทรัพยากรไปที่งานการให้ความเชื่อมั่นหรือการให้คำปรึกษา โดยมุ่งไปที่การเพิ่มคุณค่าและการปรับปรุงองค์กรให้ดีขึ้น การรวบรวมข้อมูลความเสี่ยงจะช่วยเป็นแนวทางในการวางแผนการตรวจสอบภายใน และช่วยให้ตรวจสอบภายในทำการวิเคราะห์เพื่อประเมินความน่าจะเป็นของความเสี่ยง ผลกระทบ ความครอบคลุม และความน่าเชื่อถือได้ ในคู่มือช่วยปฏิบัติ (Practice Aid) ที่ 1 ได้ให้ตัวอย่างรายการตรวจสอบการประเมินความเสี่ยง (risk assessment checklist) ไว้

การวิเคราะห์ผลกระทบทางธุรกิจ (BIA)

ตรวจสอบภายในอาจให้แนวทางแก่ฝ่ายบริหารว่าจะทำการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ซึ่งเป็นองค์ประกอบสำคัญของ BCM ได้อย่างไร การวิเคราะห์ BIA นี้จะสนับสนุนการระบุสินทรัพย์ทางธุรกิจ หน้าที่งาน ระบบงาน คู่ค้าผู้ขายทรัพยากรที่สำคัญ รวมไปถึงการประเมินผลขั้นสุดท้ายถึงการสูญเสียที่อาจเกิดขึ้นกับ

องค์กรในกรณีที่เกิดภาวะวิกฤต *GTAG ฉบับที่ 10 เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)* ได้ให้แนวทางที่เป็นประโยชน์ในการทำการวิเคราะห์ BIA ผลลัพธ์ของ BIA มีแนวโน้มที่จะผลักดันระดับการกระทำที่ได้มีการวางแผนไว้ล่วงหน้า ความครอบคลุม และระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ขององค์กร หากมีการวิเคราะห์ BIA อย่างมีประสิทธิผลแล้ว BIA จะให้ภาพการดำเนินงานที่สำคัญ ทรัพยากรที่สำคัญ และกระบวนการต่างๆ (อาคารสถานที่สิ่งอำนวยความสะดวกต่างๆ บุคลากร และเทคโนโลยี ซึ่งรวมถึง การรักษาความปลอดภัยในเชิงตรรกะและทางกายภาพ) และในที่สุด อาจผลักดันความเร่งด่วนในการลงทุนให้แก่แผน BCP และ CMP ที่เกี่ยวข้องได้

การวางแผนเพื่อความต่อเนื่องทางธุรกิจและการกอบกู้สถานการณ์ (BCRP)

แผน BCRP จะก่อให้เกิดวิธีการเชิงรุกที่องค์กรสามารถระบุมาตรการเพื่อความต่อเนื่องและการกอบกู้ทางธุรกิจเพื่อบริหารจัดการ และบรรเทาความเสี่ยงที่สำคัญขององค์กรซึ่งเกิดจากภาวะวิกฤต ตรวจสอบภายในอาจให้บริการให้คำปรึกษาหรือการให้ความเชื่อมั่นที่เกี่ยวข้องกับแผน BCRP

กิจกรรมตรวจสอบภายในก่อนภาวะวิกฤต

การประเมินผล BCM โดยตรวจสอบภายใน และโดยเฉพาะอย่างยิ่งแผน CMP นั้น อาจช่วยให้มั่นใจได้ว่าแผน CMP ยังคงสอดคล้องกับลำดับความสำคัญขององค์กรในกรณีที่เกิดภาวะวิกฤต

ต่อไปนี้เป็นกิจกรรมบางอย่างที่ตรวจสอบภายในอาจกระทำได้ก่อนเกิดภาวะวิกฤต:

- แบ่งปันความรู้เกี่ยวกับการพัฒนา BCM ชั้นนำกับผู้บริหารระดับสูงและคณะกรรมการตรวจสอบ
- พิจารณา BCM โดยเฉพาะว่าเป็นความเสี่ยงที่องค์กรกำลังเผชิญ รวมทั้งพิจารณาความเสี่ยงที่เหลืออยู่ในการพัฒนาแผนการตรวจสอบประจำปี
- ประเมินการจัดแจงของพันธมิตรทางธุรกิจที่สำคัญ โดยประเมินข้อกำหนดในสัญญาที่เหมาะสม ซึ่งรวมถึงข้อตกลงระดับการให้บริการ เงื่อนไขที่ให้สิทธิในการตรวจสอบ และการรายงานที่จำเป็นต่อฝ่ายบริหารเกี่ยวกับสภาพแวดล้อมการควบคุมของพันธมิตร
- การให้คำแนะนำแก่ผู้บริหารเกี่ยวกับผลจากการประเมินความเสี่ยงของ BCM หรือประเมินความถูกต้องของการประเมินความเสี่ยงที่มีใน BCM ด้วยตนเอง ของฝ่ายบริหาร
- ปฏิบัติงานให้ความเชื่อมั่นที่เกี่ยวข้องกับแผน BCP และ/หรือ CMP ซึ่งเป็นส่วนหนึ่งของแผนการตรวจสอบประจำปี งานให้ความเชื่อมั่นอาจรวมถึงการประเมินองค์ประกอบของแผน ระเบียบพิธีการสื่อสารภายในแผน และด้านการปฏิบัติงานของแผน
- หากไม่มีการกำหนดไว้เป็นอย่างอื่นในกฎบัตรของหน่วยงานตรวจสอบภายในหรือคำสั่งจากคณะกรรมการแล้ว จะต้องมีการอธิบายและกำหนดบทบาทใน BCM สำหรับตรวจสอบภายในและ CAE ไว้

กิจกรรมตรวจสอบภายในในระหว่างภาวะวิกฤตและหลังภาวะวิกฤต

หัวข้อต่อไปนี้อธิบายกิจกรรมทั่วไปที่ตรวจสอบภายในอาจดำเนินการได้ในระหว่างและหลังภาวะวิกฤต

ในระหว่างภาวะวิกฤต:

- เฝ้าติดตามและประเมินการตอบสนองต่อเหตุการณ์ขององค์กร และเป็นผู้มีส่วนร่วมอย่างแข็งขันในทีมบริหารภาวะวิกฤต
- เฝ้าติดตามรายละเอียดของการหยุดชะงักต่างๆ เพื่อใช้สำหรับการตรวจสอบในภายหลัง
- ทำหน้าที่เป็นคณะอนุกรรมการบริหารภาวะวิกฤต เพื่อให้เชื่อมั่นได้ว่า มีความเข้าใจในความเสี่ยงที่มีมากับภาวะวิกฤต และให้คำแนะนำเกี่ยวกับทางเลือกในการดำเนินการให้แก่ฝ่ายบริหารตามความเหมาะสม
- มีส่วนร่วมในการบริหารภาวะวิกฤตและกระบวนการกอบกู้ที่กว้างขึ้นสำหรับองค์กร ตามที่ได้รับความเห็นชอบและได้รับอนุมัติ

มาตรฐาน อนุญาตให้มีส่วนร่วมกับกิจกรรมดังกล่าวนี้ได้ โดยมีเงื่อนไขว่าจะต้องเปิดเผยรายละเอียดเกี่ยวกับอุปสรรคหรือความเสื่อมต่อความเป็นอิสระของหน่วยงานตรวจสอบภายในต่อผู้ที่เหมาะสม (เช่น คณะกรรมการตรวจสอบและหัวหน้าทีม BCM) การมีส่วนร่วมของตรวจสอบภายในอาจมีมากในช่วงแรกๆ ของภาวะวิกฤตเมื่อทรัพยากรขององค์กรมีอยู่อย่างจำกัด แต่ความต้องการการสนับสนุนจากทรัพยากรดังกล่าวมีอยู่ในระดับสูง

ภายหลังภาวะวิกฤต:

- ประเมินและรายงานประสิทธิผลของความพยายามในการกอบกู้สถานการณ์ขององค์กร
- ยังคงดำเนินการประเมินความเสี่ยงต่อไป ให้แนวทาง และช่วยพัฒนาในการทำการปรับปรุงกระบวนการทางธุรกิจ
- ทำการสอบทานเมื่อภาวะวิกฤตผ่านไป (post-crisis reviews) เพื่อระบุโอกาสสำหรับกิจกรรม BCM และโดยเฉพาะอย่างยิ่งสำหรับการพัฒนาแผนการบริหารภาวะวิกฤต (CMP)
- ปฏิบัติงานการให้ความเชื่อมั่น เพื่อประเมินว่าฝ่ายบริหารได้ดำเนินการและคำนึงถึงผลจากการวิเคราะห์สาเหตุที่แท้จริง (root-cause analysis) อย่างเหมาะสม เพื่อปรับปรุงแผน BCP และ CMP

ตามความจำเป็นแล้วหรือไม่ มีส่วนร่วมในกระบวนการกอบกู้สถานการณ์ทั่วทั้งองค์กรและเป็นไปตามที่ตกลงกันไว้และได้รับอนุมัติตามแผน BCP และ CMP

กิจกรรมเหล่านี้จะกล่าวในรายละเอียดมากขึ้นในหัวข้อที่ตามมา

ทำการตรวจสอบประสิทธิผลของกระบวนการกอบกู้สถานการณ์และของแผน

แผนกอบกู้ภัยพิบัติ (disaster recovery plan) ซึ่งเป็นองค์ประกอบหนึ่งของ BCM อาจรวมถึงข้อกำหนดสำหรับตรวจสอบภายในเพื่อให้ปฏิบัติงานตรวจสอบกระบวนการกอบกู้ภัยพิบัติ ในกรณีดังกล่าว งานเพิ่มเติมมานี้จะต้องรวมอยู่ในแผนที่ร่างมาตั้งแต่ต้น และอาจนำไปสู่การเปลี่ยนแปลงลำดับความสำคัญของงานต่างๆ ได้

นอกจากนี้ ในกรณีที่บทบาทดังกล่าวไม่ได้รับการมอบหมายอย่างชัดเจน CAE ควรพิจารณา (โดยอาศัยการประเมินความเสี่ยง) ว่าตนควรจะแนะนำทีมผู้นำในแผน BCP ว่า การกอบกู้ข้อมูลและ/หรือ CMP ในด้านใดที่ควรได้รับการตรวจสอบ

ประเภทของงานตรวจสอบที่อาจดำเนินการได้ ได้แก่:

- การสอบทานกระบวนการกอบกู้ตั้งแต่ต้นทางถึงปลายทาง (end-to-end review) ซึ่งก็คือ สอบทานว่าเป็นไปตามกระบวนการที่วางแผนไว้หรือไม่ และแผนได้พิสูจน์ให้เห็นแล้วว่ามีรายละเอียดเพียงพอที่จะจัดการกับปัญหาที่เกิดขึ้นหรือไม่
- การตรวจสอบประสิทธิผลของกระบวนการกอบกู้ ซึ่งรวมถึงการวัดผลการปฏิบัติงานเทียบกับตัวชี้วัดที่กำหนด หรือองค์ประกอบของแผน รวมทั้งการสื่อสารให้ผู้มีส่วนได้เสียและพันธมิตรทางธุรกิจทั้งภายในและภายนอกอย่างมีประสิทธิผลและเหมาะแก่กาลเวลา
- การสอบทานวิธีการควบคุมและกระบวนการพิเศษต่างๆ ที่อยู่นอกกรอบการควบคุมตามปกติ และผลกระทบที่อาจเกิดขึ้นต่อความเสี่ยงด้านการปฏิบัติงานหรือทางด้านการเงินสำหรับองค์กร
- การตรวจสอบกระบวนการกอบกู้ข้อมูลของฝ่ายบริหาร ซึ่งอาจรวมถึงการตรวจสอบการกระทบยอดข้อมูลที่สำคัญที่กระทำโดยฝ่ายบริหาร เพื่อให้แน่ใจถึงครบถ้วนและถูกต้องของข้อมูล
- การสอบทานความแตกต่างของแผน BCP และ CMP ที่เกิดขึ้นจริง ภายหลังจากได้ดำเนินงานตามแผน ซึ่งรวมถึงคำแนะนำที่จะช่วยให้เกิดการพัฒนาแผนได้อย่างมีประสิทธิผล สิ่งเหล่านี้ควรนำไปปรับใช้กับแผนของหน่วยงานตรวจสอบภายในด้วย

การเข้าร่วมในกระบวนการกอบกู้ที่กว้างขึ้น

ผู้ตรวจสอบภายในอาจได้รับการร้องขอจากผู้นำขององค์กรเพื่อให้การสนับสนุนเพิ่มเติมแก่พนักงานฝ่ายปฏิบัติการผู้ซึ่ง:

- อาจจะทำงานอยู่ในกระบวนการกอบกู้
- อาจจะทำงานเกี่ยวกับการแก้ไขกระบวนการทางธุรกิจตามปกติ ซึ่งเป็นผลมาจากการที่ระบบไอทีไม่พร้อมใช้งาน
- อาจจะกำลังใช้วิธีการสำรองตามที่กำหนดไว้เพื่อดำเนินกิจกรรมซึ่งปกติกระทำโดยกระบวนการซึ่งกำลังมีการหยุดชะงัก

มันจะเป็นสิ่งสำคัญสำหรับ CAE ที่ต้องพิจารณาคำขอที่ได้รับอนุมัติมาจากคณะกรรมการตรวจสอบล่วงหน้าก่อนการกำหนดบทบาทของตรวจสอบภายในเกี่ยวกับแผน BCP / CMP นอกจากนี้ เมื่อพนักงานตรวจสอบภายในได้รับการมอบหมายให้ไปช่วยเหลือใน CM หรือไปช่วยในการกอบกู้ หน้าที่ที่ได้รับมอบหมายควรดำเนินการภายใต้การสั่งการของผู้บริหารด้านปฏิบัติการ เพื่อปกป้องความเที่ยงธรรม CAE ควรคำนึงถึงหน้าที่ด้านการปฏิบัติงานที่ปฏิบัติโดยผู้ตรวจสอบภายในและหลีกเลี่ยงการมอบหมายงานการให้ความเชื่อมั่นของตรวจสอบภายในในอนาคตในส่วนงานที่เขาได้ไปปฏิบัติ

ภาคผนวก

คู่มือช่วยปฏิบัติ (Practice Aid) ที่ 1: ตัวอย่างแนวทางการปฏิบัติงานสำหรับงานการให้ความเชื่อมั่นหรือให้คำปรึกษาเกี่ยวกับแผน BCM

หน่วยงานตรวจสอบภายในมีบทบาทสำคัญในการสอบทานความครบถ้วนของ BCM โดยรวมอย่างเป็นอิสระ การลงรายละเอียดในเชิงลึกและความถี่ของกิจกรรมตรวจสอบและการรายงาน ควรถูกปรับให้เข้ากับความสำคัญของการดำเนินงาน ในขณะที่ขอบเขตของกิจกรรมตรวจสอบและการส่งมอบผลงานอาจแตกต่างกันไปในแต่ละกรณี แต่ในทุกๆ กรณี จะต้องเป็นการประเมินประสิทธิผลของแผนการทดสอบอย่างเป็นอิสระและเที่ยงธรรม หน่วยงานตรวจสอบภายในควรคำนึงถึงความสมเหตุสมผลของสมมติฐานพื้นฐานที่ใช้ในการพัฒนาแผนการทดสอบ รวมทั้งความเพียงพอของแผนการทดสอบ สถานการณ์ กำหนดการ และรายงานควรได้รับการประเมินโดยสัมพันธ์กับขนาดและความซับซ้อนขององค์กร ความสำคัญของสายธุรกิจ และความเสี่ยงและผลกระทบจากการที่ธุรกิจหยุดชะงักซึ่งอาจเกิดขึ้นได้ ตรวจสอบภายในควรเข้าสังเกตการณ์การทดสอบฝึกซ้อม เพื่อประเมินสภาพแวดล้อมการควบคุมของสถานที่ที่เป็นสถานที่ทางเลือก สอบยันผลลัพธ์ ประเมินว่ามีการรายงานที่เหมาะสม รวมทั้งมีการกำหนดและใช้กลไกการยกระดับการรายงานที่เหมาะสม และประเมินว่ามีการปรับปรุงแผนการทดสอบเพื่อสะท้อนถึงผลการทดสอบครั้งก่อนหรือไม่ ในการตรวจสอบแต่ละงานจะพิจารณา BCM ในด้านทั่วๆ ไปห้าด้าน ดังนี้:

1. **สภาพแวดล้อมและกลยุทธ์ทางธุรกิจ**
2. **กระบวนวิธีและกลยุทธ์ของแผน BCP**
3. **การวิเคราะห์ผลกระทบทางธุรกิจ (การประเมินความเสี่ยงและวิธีการควบคุม)**
4. **แผนการกอบกู้ข้อมูล**
5. **การตระหนักรู้ การทดสอบ และการฝึกอบรม**

ตัวอย่างที่ 1

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
1. **สภาพแวดล้อมและกลยุทธ์ทางธุรกิจ**	อุตสาหกรรม	1. มาตรฐานอุตสาหกรรมที่สำคัญสำหรับ BCM
		2. ข้อกำหนดทางกฎหมายสำหรับอุตสาหกรรมที่บริษัทดำเนินธุรกิจอยู่
		3. ประวัติเกี่ยวกับจุดอ่อนโดยเฉพาะของอุตสาหกรรม
		4. รายชื่อของหน่วยงานและเจ้าหน้าที่ภาครัฐ (หน่วยงานภายนอก)
	ความพึ่งพาจากภายนอก	1. มีการระบุและคำนึงถึงความพึ่งพาจาก ความสัมพันธ์กับพันธมิตรทางธุรกิจและผู้มีส่วนได้เสียที่สำคัญ (ซึ่งรวมถึงผู้ผลิต ผู้ขาย และผู้ให้บริการจากภายนอกที่สำคัญ)
		2. มีการระบุสัญญาพันธมิตรทางธุรกิจที่สำคัญ และข้อตกลงระดับการให้บริการ (service-level agreements) และมีการจัดทำเอกสารสำหรับการจัดหาที่สำคัญๆ
		3. มีการใช้สิทธิในการตรวจสอบเป็นระยะและได้รับรายงานคำชี้แจงเกี่ยวกับ Statement on Auditing Standards (SAS) 70/Statement on Standards for Attestation Engagements (SSAE) 16 หรือรายงานพันธมิตรทางธุรกิจที่เทียบเท่า (นั่นคือมีการสอบพิสูจน์ความถูกต้องของระบบ ซึ่งรวมถึงความสามารถในการกอบกู้ข้อมูลสำรอง และการตรวจสอบความมั่นคงปลอดภัยเป็นระยะ)

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
2. **การเชื่อมโยงแผน BCP กับการดำเนินธุรกิจและกลยุทธ์ทางการเงิน**	กลยุทธ์ทางธุรกิจ	1. แผน BCP ขึ้นอยู่กับกลยุทธ์ทางธุรกิจของบริษัท
		2. หน่วยงานที่เกี่ยวข้องและหน้าที่ที่สำคัญทั้งหมดได้รับการพิจารณาในแผน BCP
	การปฏิบัติงาน / กลยุทธ์ทางเทคนิค	1. ทั้งการปฏิบัติงานและไอทีได้ถูกบูรณาการเข้าด้วยกัน
		2. การวางแผน BCM ได้รับการพิจารณาในทุกๆ การตัดสินใจทางธุรกิจที่เกี่ยวข้อง
		3. หน้าที่ในแผน BCP/CMP ซึ่งรวมถึงการบำรุงรักษาได้ผนวกรวมอยู่ในแบบบรรยายลักษณะงาน (job descriptions) ของพนักงาน และการประเมินผลบุคลากรที่ใช้บังคับอยู่
		4. แผน BCP ได้รับการปรับปรุง สอบทาน และทดสอบตามความถี่ที่เหมาะสมกับความเสี่ยง จุดอ่อนและคุณค่าของหน่วยธุรกิจ
	กลยุทธ์ทางการเงิน	1. ได้รับทรัพยากรทางการเงินที่เพียงพอสำหรับการเตรียมการและการบำรุงรักษา BCP
3. **การวิเคราะห์ผลกระทบ (รวมถึงการวิเคราะห์ผลกระทบทางธุรกิจ [BIA] การประเมินความเสี่ยงและการควบคุมต่าง ๆ)**	ทัศนคติที่สื่อมาจากผู้บริหารระดับสูง (Tone at the top)	1. คณะกรรมการและผู้บริหารระดับสูงให้การสนับสนุนความคิดริเริ่ม BCM
		2. ผู้บริหารระดับสูงมีหน้าที่ในการทำให้มั่นใจว่า การนำ BCM ไปลงมือปฏิบัติ การบำรุงรักษา และการปรับปรุงแผนต่างๆ ที่สนับสนุน BCM จะประสบความสำเร็จได้
		3. มีนโยบาย/กฎบัตร BCM และได้รับการปรับปรุงเป็นระยะ
		4. แผนต่างๆ ที่เกี่ยวข้องกับ BCM รวมถึงแผน BCP และ CMP ได้รับการอนุมัติโดยคณะกรรมการรและฝ่ายบริหารในแต่ละระดับตามความเหมาะสม

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
	การประเมินความเสี่ยง	1. มีการวิเคราะห์ผลกระทบอย่างครอบคลุม/มีการทำ BIA และจัดทำขึ้นจากข้อมูลที่ได้รับจากสายงานธุรกิจ
		2. มีการอธิบายอย่างชัดเจนถึงเหตุการณ์ประเภทต่างๆ ที่สามารถกระตุ้นให้เกิดการประกาศภาวะวิกฤตหรือภัยพิบัติอย่างเป็นทางการ รวมทั้งกระบวนการเพื่อเริ่มนำ BCP และ CMP มาใช้
		3. หากผู้นำองค์กรเห็นว่ามีความจำเป็น ให้ดำเนินการวิเคราะห์ทางเดินของงาน (Work flow analysis) และมีการจดบันทึกผลที่ได้ไว้เป็นเอกสาร
		4. มีการจัดลำดับความสำคัญของหน้าที่งานทางธุรกิจไว้อย่างเพียงพอ
		5. การประเมินความเสี่ยงรวมถึง ผลกระทบและความน่าจะเป็นที่จะเกิดการหยุดชะงักของธุรกิจทั้งหมด การดำเนินงานและด้านไอทีทั้งหมด และพิจารณาระยะเวลาของการหยุดชะงักที่ยอมรับได้
		6. มีวิธีการในการดำเนินการตามแผนที่มีความสำคัญเร่งด่วน เทียบกับหน้าที่งานที่ไม่สำคัญ การให้บริการและกระบวนการต่างๆ
		7. ผลกระทบทางการเงินในกรณีฉุกเฉิน ได้สะท้อนถึงต้นทุนในกรณีฉุกเฉินได้อย่างถูกต้อง
		8. พิจารณาความเสี่ยงด้านชื่อเสียง และมีการคำนึงถึงผู้มีส่วนได้เสียที่เกี่ยวข้องทั้งหมดใน BIA

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
	การบรรเทา	1. การบรรเทาความเสี่ยงที่เพียงพอ ซึ่งรวมถึง การเตรียมความพร้อมและกลยุทธ์การป้องกันที่ควรได้รับการพิจารณาเช่น: a) สถานที่ทางเลือกและความสามารถในการรองรับ (แน่ใจได้ในความหลากหลายของสถานที่) b) มั่นใจได้ว่า มีการสำรองข้อมูล แอพพลิเคชั่นการสื่อสารโทรคมนาคม และข้อมูลที่เกี่ยวข้องอื่นๆ และวิธีการต่างๆ ยังคงมีอยู่ c) ช่องทางการสื่อสารในกรณีฉุกเฉินได้กำหนดไว้อย่างชัดเจน (แผนผังการสื่อสาร)
		2. มีการระบุบุคลากรที่สำคัญทั้งหมดและรายชื่อผู้ติดต่อต้องมีการปรับปรุงให้เป็นปัจจุบัน
		3. พนักงานเข้าใจบทบาทของตนในกรณีฉุกเฉิน
		4. มีการกำหนดผู้ให้บริการในการสนับสนุนสำรอง
4. **แผนการกอบกู้ข้อมูล**	ระยะเวลานานที่สุดที่ยอมให้ข้อมูลสูญหายได้ (Recovery Point Objective -- RPO)	1. มีการกำหนด RPO อย่างชัดเจน และได้สื่อสารออกไป
		2. RPO ได้คำนึงถึงความจำเป็นขององค์กรในการกอบกู้ข้อมูล
	เวลากู้คืนระบบที่ยอมรับได้ (Recovery Time Objective -- RTO)	1. มีการกำหนด RTO อย่างชัดเจน และได้สื่อสารออกไป
		2. เวลาในการกู้คืนระบบจะสะท้อนได้ดีถึงระยะเวลาหยุดชะงักที่องค์กรสามารถจะทนได้
		3. ผลลัพธ์ของ BIA ได้ถูกนำมาพิจารณาในการกำหนด RPO และ RTO

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
5. **การตระหนักรู้ การทดสอบ และการฝึกอบรม**	นโยบายการทดสอบ	1. ภายในแผน BCP องค์กรได้กำหนดข้อกำหนดต่างๆ ในการทดสอบสำหรับหน้าที่งาน สายธุรกิจ หน่วยงานสนับสนุน ที่ต้องมีความต่อเนื่อง ทั่วทั้งองค์กร รวมทั้งการทดสอบ CM ด้วย
		2. มีการกำหนดบทบาทและภาระหน้าที่ที่สำคัญในนโยบายการทดสอบ
		3. มีการกำหนดรอบการทดสอบโดยเพิ่มระดับขอบเขตการทดสอบและความซับซ้อน
	กลยุทธ์การทดสอบ	1. กลยุทธ์การทดสอบ รวมถึงเอกสารที่บันทึกแผนการทดสอบและสถานการณ์ต่างๆ เพื่อการทดสอบที่เกี่ยวข้อง วิธีการ และกำหนดเวลาที่จะทำการทดสอบ
		2. ระบุความคาดหวังถึงความเป็นอิสระในการทดสอบทั้งภายในและภายนอกองค์กร
		3. กลยุทธ์การทดสอบสอดคล้องกับสมมติฐานและความคาดหวังของฝ่ายบริหาร
		4. มีการสอบยัน BCP เป็นประจำทุกปี หรือในวงจรการทดสอบที่ถี่กว่านั้น
	การสังเกตการณ์การทดสอบ	1. ทำการทดสอบโดยไม่ได้แจ้งให้พนักงานทราบล่วงหน้า หน่วยงานตรวจสอบภายในอาจสังเกตการดำเนินการทดสอบของผู้บริหารโดยมุ่งเน้นหัวข้อต่อไปนี้: a) พนักงานที่เกี่ยวข้องทั้งหมดพร้อมทำงานและได้รับการสื่อสารในเวลาที่เหมาะสม b) สถานที่และอุปกรณ์สำรอง (Back-up facilities) และทรัพยากรต่างๆ สนองความต้องการของหน่วยงานทางธุรกิจได้ c) วิธีการสำรองต่างๆ ที่เกี่ยวข้องทำงานได้ตามที่กำหนดไว้ d) พันธมิตรทางธุรกิจที่สำคัญได้รวมอยู่ในการทดสอบ e) กระบวนการทางธุรกิจได้ถูกกำหนดขึ้นใหม่ในกรอบเวลาที่คาดหวัง
		2. หน่วยงานตรวจสอบภายในบันทึกสิ่งที่ตรวจพบ

ตัวอย่างแนวการปฏิบัติงาน (WORK PROGRAM) เกี่ยวกับ BCM		
หัวข้อย่อย	**รายการ**	**ข้อพิจารณาที่เป็นไปได้**
	ภายหลังการทดสอบ	1. มีการวิเคราะห์ช่องว่าง (Gap analysis) ที่ดำเนินการโดยทีมผู้นำ BCM
		2. ตรวจสอบภายในได้บันทึกสิ่งที่ตรวจพบอย่างเป็นอิสระและสื่อสารผลการตรวจสอบ (ถ้ามี)
		3. สิ่งที่พบจาก BCM หรือบริเวณ/ประเด็นที่ควรได้รับการปรับปรุง ได้รับการระบุ และแก้ไข ผู้นำทีม BCM ปรึกษาหารือเกี่ยวกับการดำเนินการแก้ไขและสื่อสารสิ่งที่พบให้ผู้มีส่วนได้เสียอย่างเหมาะสมข้อมูลดังกล่าวอาจสนับสนุนความจำเป็นที่ต้องมีการพัฒนาหรือปรับปรุงแผน BCM
		4. ข้อสรุปเกี่ยวกับการทดสอบ และความเหมาะสมกับขนาด ความซับซ้อน และความเสี่ยงขององค์กร ได้มีการจดบันทึกไว้เป็นเอกสาร โดยเดินตามเนื้อหาของแผน
		5. คณะกรรมการและ/หรือฝ่ายบริหารระดับสูง ได้รับการแจ้งผลการทดสอบ
	การอบรม	1. พนักงานทุกคนได้รับการฝึกอบรมและตระหนักถึงความรับผิดชอบของตน
		2. มีการจดบันทึกรายละเอียดที่เกี่ยวกับการฝึกอบรม เช่น เนื้อหา ผู้เข้าร่วม และช่วงเวลา

ตัวอย่างที่ 2

การประเมินบางส่วนที่คัดเลือกมาด้านล่างนี้ เพื่อแสดงตัวอย่างของเนื้อหาที่เป็นไปได้

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
จุดมุ่งหมาย ขอบเขต และวัตถุประสงค์			
กำหนดโครงการ	โครงการ BCM ได้จัดทำเอกสารเพื่อกำหนดสิ่งเหล่านี้หรือไม่? • จุดมุ่งหมาย ขอบเขต และวัตถุประสงค์ • วิธีการต่างๆ ใน BCM • ทรัพยากรบทบาทและภาระหน้าที่ใน BCM • การวัดผล และการสอบยัน BCM • การปรับปรุง BCM อย่างต่อเนื่อง	ใช่	ใช่ – มีการจัดทำขอบเขตโดยรวมของโครงการไว้เป็นเอกสารแล้ว
	ขอบเขต BCM ครอบคลุมการปฏิบัติงานทั้งหมดหรือไม่ ซึ่งรวมถึงกระบวนการและการดำเนินงานทางธุรกิจทั้งหมด สถานที่ สิ่งอำนวยความสะดวกและพนักงานที่เกี่ยวข้อง ที่เป็นความรับผิดชอบของบริษัท?	ไม่ใช่	ไม่ได้มีการระบุสิ่งอำนวยความสะดวกทั้งหมดไว้
วิธีการทำงาน			
การประเมินความเสี่ยง ได้รับการออกแบบมาเพื่อระบุสถานการณ์ภัยคุกคาม (เหตุการณ์ที่เชื่อได้ว่าจะเกิด) ที่สามารถทำให้ธุรกิจหยุดชะงักได้ ในการประเมินความเสี่ยง BCM ให้เสร็จสมบูรณ์นั้น ผู้ที่มีความรู้เกี่ยวกับภัยคุกคามต่อองค์กร สิ่งแวดล้อม และภูมิภาคควรเข้าร่วมด้วย ผู้ที่ควรมีส่วนร่วมอาจรวมถึง พนักงานรักษาความปลอดภัย พนักงานดูแลอาคารและสิ่งอำนวยความสะดวกต่างๆ เป็นต้น	ได้มีการดำเนินการประเมินความเสี่ยง BCM สำหรับองค์กรแล้วหรือไม่?	NI (จำเป็นต้องมีการปรับปรุง)	มีความจำเป็นต้องทำให้เป็นทางการมากขึ้น และต้องมีการจัดทำเป็นเอกสาร
	ในการประเมินความเสี่ยง ได้มีการพิจารณาประเภทของความเสี่ยงเหล่านี้หรือไม่: • อันตรายจากธรรมชาติ • ผู้ประท้วง/คน • ปัจจัยมนุษย์/ไอที • การปฏิบัติงาน	NI	พิจารณาเหตุการณ์ในภูมิภาค

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
วิธีการทำงาน			
ควรประเมินความเสี่ยง BCM ณ สถานที่ประกอบการ ให้เสร็จสมบูรณ์ และแบ่งปันข้อมูลกับผู้ดูแลสถานที่และสิ่งอำนวยความสะดวก/ผู้เช่าสถานที่	มีการระบุกลยุทธ์การบรรเทาความเสี่ยงหรือไม่?		
	ความเสี่ยงบรรเทาลงหรือไม่?		
	การประเมินความเสี่ยง BCM (เช่น สถานการณ์ภัยพิบัติ) เป็นไปในทิศทางเดียวกันกับองค์กรอื่นในสถานที่ประกอบการของท่านหรือไม่?		
การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ระบุกระบวนการธุรกิจที่สำคัญที่ต้องกอบกู้หลังจากเกิดเหตุภัยพิบัติ หลังจากเสร็จสิ้นการทำ BIA ระบุหนทางแก้ไขปัญหาในการกอบกู้สถานการณ์ เพื่อให้กระบวนการทางธุรกิจที่สำคัญกลับคืนมาดำเนินการได้ตามปกติ	มีการทำ BIA สำหรับองค์กร (ซึ่งรวมถึงทีมธุรกิจทั้งหมด) หรือไม่?		
	มีการระบุกระบวนการทางธุรกิจที่สำคัญแล้วหรือไม่?		
	ทีมผู้นำได้อนุมัติรายชื่อกระบวนการทางธุรกิจที่สำคัญซึ่งได้ระบุไว้ระหว่างการทำ BIA รวมทั้งข้อเสนอวิธีการแก้ปัญหาในการกอบกู้สถานการณ์ที่เกี่ยวข้องหรือไม่?		
การแก้ปัญหาการกอบกู้ข้อมูล มีการพัฒนาวิธีแก้ปัญหาการกอบกู้สถานการณ์ขึ้น และมีการจัดทำรายการทรัพยากรที่จำเป็นในการสนับสนุนความพยายามในการทำ CM (การกอบกู้) ขององค์กรและ/หรือทีม	ได้มีการระบุวิธีแก้ปัญหาการกอบกู้ข้อมูลและความต้องการทรัพยากรสำหรับแต่ละกระบวนการที่สำคัญไว้หรือไม่?		
	ทีมทุกทีมได้จดบันทึกทรัพยากรที่จำเป็นในการกอบกู้กระบวนการทางธุรกิจที่สำคัญหรือไม่?		
	ได้มีการประเมินความต้องการด้านไอทีหรือไม่?		
แผนงานที่เป็นลายลักษณ์อักษร	ได้มีการจัดทำแผน BCP ที่เป็นลายลักษณ์อักษรซึ่งได้รวมทีมธุรกิจทั้งหมด กระบวนการทางธุรกิจที่สำคัญ และแผน CMP ขององค์กรหรือไม่?		

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
วิธีการทำงาน			
ข้อตกลงระดับการให้บริการ (SLAs) บันทึกความเข้าใจ (MOU) และสัญญา	มีการจัดทำ SLAs และ/หรือ MOU สำหรับหัวข้อเหล่านี้หรือไม่: • พื้นที่สำนักงาน (ทำกับผู้บริหารสิ่งอำนวยความสะดวก) • ไอที/การสื่อสาร (ทำกับผู้ให้บริการด้านไอที)? • การกอบกู้ข้อมูล (ทำกับผู้ให้บริการไอที)? • สัญญาที่ทำกับบุคคลที่สามอื่น ๆ?		
	ได้มีการกระทำการเพื่อปกป้องผลประโยชน์ของบริษัท เมื่อสัญญาของบุคคลที่สามได้มีเงื่อนไขเกี่ยวกับ "เหตุสุดวิสัย"		
การวางแนวทาง	ท่านได้มีส่วนร่วมในการวางแผนการประสานงานสำหรับผู้เช่าหลายราย หรือผู้เช่าหลายที่ตั้งหรือไม่		
	องค์กรของท่านได้จัดได้ทำแผนการสื่อสารสำหรับเหตุฉุกเฉิน ซึ่งรวมถึงการส่งถึงพนักงานทั้งหมดหรือไม่?		
	ท่านได้จัดแนวทางของแผน BCP ให้สอดคล้องกับ CM และการสนองตอบต่อสถานการณ์ฉุกเฉินหรือไม่?		

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
วิธีการทำงาน			
การฝึกอบรมและการฝึกซ้อม	ผู้บริหารระดับสูงของ BCM และผู้จัดการของ BCM ได้รับการฝึกอบรมหรือไม่?		
	ผู้ประสานงาน BC ได้รับการฝึกอบรมหรือไม่?		
	สมาชิกทั้งหมดของทีม BCM ได้รับการฝึกอบรมที่เกี่ยวข้องกับบทบาทและภาระหน้าที่ของตนหรือไม่?		
	ได้มีการฝึกซ้อมกิจกรรม BCM ที่สำคัญเป็นประจำทุกปี หรือถี่มากกว่านั้นหรือไม่? • การฝึกซ้อมการแจ้งเตือน • การฝึกซ้อมบนโต๊ะ • การฝึกซ้อมตามหน้าที่ • การฝึกซ้อมเต็มรูปแบบ		
ทรัพยากร บทบาท และภาระหน้าที่			
พนักงานที่สนับสนุน BCM	มีการตรวจสอบว่าพนักงานสำรองที่จะทำงานที่สำคัญเหล่านั้น มีความสามารถ (ความรู้ การเข้าถึงข้อมูล เป็นต้น) ที่จะทำหน้าที่เหล่านั้นหรือไม่?		
ผู้บริหารระดับสูงของ BCM ทำหน้าที่เป็นผู้สนับสนุนขององค์กรสำหรับ BCM (รวมถึงความสอดคล้องกับทีมผู้นำ) สนับสนุนการสร้าง และการยอมรับแผน BCM โดยผ่านการประสานงานอย่างมีประสิทธิผลในด้านเงินทุน บุคลากร และการพิจารณาแผนธุรกิจขององค์กรและความเสี่ยงต่างๆ	ทีมผู้นำขององค์กรได้ระบุผู้บริหารระดับสูงของ BCM หรือไม่?		
	ผู้บริหารระดับสูงของ BCM เข้าถึงทีมผู้นำได้หรือไม่		
	เงินทุน บุคลากร และ ทรัพยากร มีเพียงพอหรือไม่		
	มีการประสานงาน BCM กับกระบวนการอื่นๆ ขององค์กร และเชื่อมโยงกับแผนธุรกิจขององค์กรหรือไม่?		

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
ทรัพยากร บทบาท และภาระหน้าที่			
ผู้จัดการ BCM	มีการระบุผู้จัดการ BCM สำหรับทั่วทั้งองค์กรหรือไม่?		
	ผู้จัดการ BCM ประสานงานและเป็นผู้นำในการนำ BCM ไปปฏิบัติหรือไม่?		
	ผู้จัดการ BCM มั่นใจหรือไม่ว่า มีทรัพยากรข้ามสายงานต่างๆ พร้อมใช้งาน และได้รับการมอบหมายงานอย่างเหมาะสมเมื่อมีความจำเป็น?		
	ผู้จัดการ BCM มั่นใจว่ามีการวัดผล ตรวจสอบและสอบทานประสิทธิผล และประสิทธิภาพของ CM เป็นระยะเพื่อการปรับปรุงในโอกาสต่อไปหรือไม่?		
ผู้ประสานงาน BCM	มีการระบุผู้ประสานงาน BCMทั่วทั้งองค์กรหรือไม่?		
	ผู้ประสานงาน BCM บริหารการวางแผนความต่อเนื่องทางธุรกิจ ณ ระดับองค์กร ระดับหน่วยธุรกิจ (BU) หน่วยธุรกิจตามภูมิภาคต่างๆ หรือระดับย่อยอื่นๆ หรือไม่		
	ผู้ประสานงาน BCM มีส่วนร่วมในกิจกรรมการประสานงานสำหรับผู้เช่าหลายราย ผู้เช่าหลายพื้นที่ ตามความเหมาะสมหรือไม่?		

ความเสี่ยง BCM หรือการประเมินตนเอง			
รายการ		**สถานะ**	**ข้อสังเกตจากการประเมิน**
การวัดผล และสอบยัน			
	มีการวัดและกระบวนการสอบยันที่กระทำเป็นประจำทุกปีว่าได้มีการระบุข้อกำหนดของ BCM ในลักษณะที่สอดคล้องกับความต้องการทางธุรกิจในปัจจุบันหรือไม่		
	ความต้องการทางด้านไอทีได้ผ่านการตรวจพิสูจน์แล้ว ซึ่งรวมถึงความต้องการทางด้านไอทีที่จำเป็นในการสนับสนุนการวางแผนเพื่อการย้ายสถานที่เครือข่าย หรือการเข้าถึงระบบจากระยะไกล ข้อมูลในท้องถิ่นหรือข้อมูลที่ส่วนกลาง เป็นต้น หรือไม่?		
	การวัดผลและระบวนการสอบยันได้เชื่อมโยงกับกระบวนการปรับปรุงอย่างต่อเนื่องหรือไม่?		
	ท่านได้ติดตามการกระทำที่จำเป็นเพื่อแก้ปัญหาช่องว่างของ BCM ที่พบเห็นได้ในระหว่างการฝึกซ้อม BCM เพื่อให้แน่ใจว่าจะเสร็จทันเวลาหรือไม่?		
	ท่านมีกระบวนการเพื่อประเมินประสิทธิผลของโครงการ BCM หรือไม่?		

คู่มือช่วยปฏิบัติ (Practice Aid) ที่ 2: คำศัพท์ที่สำคัญ

แผนเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity Plan--BCP) - ความสามารถในการวางแผนเพื่อความต่อเนื่องของกระบวนการทางธุรกิจที่สำคัญ ปกป้องสินทรัพย์ที่สำคัญ และเพื่อให้บริการและสนับสนุนแก่ลูกค้าได้เมื่อเผชิญกับภาวะวิกฤต ภัยพิบัติเหตุการณ์ หรือเหตุฉุกเฉิน ซึ่งแผนดังกล่าวช่วยให้องค์กรสามารถกอบกู้สถานการณ์และฟื้นตัวได้อย่างมีประสิทธิผล รวมทั้งจัดการความเสี่ยงที่เกี่ยวข้องกับภาวะวิกฤต สิ่งนี้มักจะรวมอยู่ในโครงการบริหารภาวะวิกฤต (crisis management program)

แผนเพื่อความต่อเนื่องในการดำเนินธุรกิจและการกอบกู้สถานการณ์ (Business Continuity and Recovery Planning--BCRP) – วิธีการเชิงรุกที่องค์กรสามารถระบุความต่อเนื่องทางธุรกิจและมาตรการกอบกู้สถานการณ์ เพื่อบริหารและบรรเทาความเสี่ยงที่สำคัญขององค์กรที่เกิดจากภาวะวิกฤต

ภาวะวิกฤต (Crisis) – เหตุการณ์ที่ (หากไม่ได้รับการจัดการอย่างเหมาะสม) อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความสามารถขององค์กรในการดำเนินงาน สร้างผลกำไร และบริหารจัดการความเสี่ยงด้านชื่อเสียง โดยทั่วไป สิ่งเหล่านี้ ได้แก่ ภัยพิบัติทางธรรมชาติหรือทางกายภาพ ความล้มเหลวของการดำเนินงานที่สำคัญ และ/หรือการเชื่อมต่อ การชะงักงันในความสัมพันธ์กับพันธมิตรทางธุรกิจที่สำคัญ รวมทั้งความเสี่ยงทางเทคโนโลยี

โครงการบริหารภาวะวิกฤต (Crisis Management Program--CMP) – เป็นการรวมของกิจกรรมต่างๆ ที่ประกอบด้วยมาตรการป้องกันและมาตรการตอบโต้ที่ดำเนินการโดยองค์กรเพื่อบรรเทาและบริหารความเสี่ยงจากภาวะวิกฤตหรือเหตุการณ์นั้นๆ อย่างมีประสิทธิผล CMP มักจะรวมถึงแผนเพื่อความต่อเนื่องทางธุรกิจและแผนการฟื้นฟูจากภัยพิบัติ

ภัยพิบัติ (Disaster) – เหตุการณ์ภัยพิบัติที่เกิดขึ้นกะทันหันโดยไม่ได้วางแผนล่วงหน้า ทำให้เกิดความเสียหายหรือการสูญเสียที่ไม่สามารถยอมรับได้ ซึ่งอาจรวมถึงเหตุการณ์ที่ทำให้ความสามารถขององค์กรในการทำหน้าที่ กระบวนการ หรือบริการที่สำคัญเสื่อมเสียได้ นี่คือตัวอย่างหนึ่งของเหตุการณ์ที่แผนเพื่อความต่อเนื่องธุรกิจและ/หรือแผนการฟื้นฟูจากภัยพิบัติมักจะถูกนำมาใช้งานโดยเป็นส่วนหนึ่งของ CMP โดยรวม

กรณีฉุกเฉิน (Emergency) – เหตุการณ์ที่ไม่คาดคิด อุบัติการณ์ที่ใกล้กำลังจะเกิด หรือสถานการณ์ที่อาจทำให้เกิดการบาดเจ็บ การเสียชีวิต การทำลายทรัพย์สิน หรือการแทรกแซง การสูญเสีย หรือการหยุดชะงักของ

การดำเนินธุรกิจตามปกติ เหตุการณ์ดังกล่าวอาจยกระดับขึ้นเป็นภาวะวิกฤตได้หากไม่ได้รับการควบคุมหรือการบริหารจัดการ

เหตุการณ์ (Incident) – เหตุการณ์ที่ไม่ได้เป็นส่วนหนึ่งของมาตรฐานในการปฏิบัติงาน ซึ่งอาจส่งผลกระทบต่อธุรกิจเป็นการชั่วคราว และในบางกรณีอาจนำไปสู่กรณีฉุกเฉินหรือภัยพิบัติได้

การวิเคราะห์ผลกระทบ (Impact Analysis) – กระบวนการในการวิเคราะห์หน้าที่ด้านการปฏิบัติงานที่สำคัญ หรือข้อมูลที่สำคัญ ด้วยมุมมองที่จะทำความเข้าใจในผลกระทบทั้งภายในหรือภายนอกซึ่งมาจากการสูญเสีย/การหยุดชะงักที่อาจเกิดขึ้น การวิเคราะห์ผลกระทบรวมถึง การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ซึ่งเกี่ยวข้องกับการระบุสินทรัพย์ทางธุรกิจ หน้าที่ และทรัพยากร ที่สำคัญ รวมทั้งการประเมินความเสียหายหรือการสูญเสียที่อาจเกิดขึ้นกับองค์กรซึ่งเป็นผลมาจากการหยุดชะงัก หรือการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจหรือทางการดำเนินงาน BIA ควรระบุ: ก) แหล่งที่มาของความเสียหาย การหยุดชะงัก หรือการสูญเสีย ข) ขอบเขต (extent) ที่เมื่อเวลาผ่านไปจะขยายความเสียหายที่เกิดจากการหยุดชะงักหรือการสูญเสียที่อาจเกิดขึ้น ค) ระดับของการบริการหรือทรัพยากรที่จำเป็นสำหรับการประคับประคองให้กิจกรรมทางธุรกิจหลักดำเนินต่อไปได้ และ ง) ลำดับช่วงเวลาที่สินทรัพย์ทางธุรกิจ หน้าที่งาน และทรัพยากรที่สำคัญทั้งหมดควรได้รับการกอบกู้ขึ้นมาได้ เพื่อหลีกเลี่ยงความสูญเสียที่มีนัยสำคัญอย่างถาวรสำหรับองค์กร

ระยะเวลานานที่สุดที่ยอมให้ข้อมูลสูญหายได้ (Recovery Point Objective -- RPO) – จุดเวลาที่ระบบและข้อมูลต้องได้รับการกอบกู้หลังจากการไม่มีระบบใช้งาน (เช่น เมื่อสิ้นสุดการประมวลผลของวันก่อนหน้า) RPOs มักจะถูกใช้เป็นพื้นฐานในการพัฒนากลยุทธ์การสำรองข้อมูล และเพื่อกำหนดจำนวนของข้อมูลที่อาจต้องสร้างขึ้นใหม่หลังจากระบบหรือฟังก์ชั่นได้รับการกอบกู้

เวลากู้คืนระบบที่ยอมรับได้ (Recovery Time Objective -- RTO) – ระยะเวลาที่ระบบ แอพพลิเคชั่น หรือหน้าที่งาน ต้องได้รับการกอบกู้หลังจากไม่มีระบบใช้งาน (ปกติคือหนึ่งวันทำการ) RTOs มักจะถูกใช้เป็นพื้นฐานสำหรับการพัฒนากลยุทธ์การกอบกู้และเพื่อตัดสินว่าจะใช้กลยุทธ์เหล่านั้นในช่วงที่เกิดภัยพิบัติหรือไม่ เวลาหยุดทำงานสูงสุดที่อนุญาตให้มีได้ (Maximum allowable downtime) มักจะเป็นคำที่ใช้ตามมา

การประเมิน/วิเคราะห์ความเสี่ยง (Risk Assessment/Analysis) – กระบวนการในการระบุความเสี่ยงให้กับองค์กร การประเมินหน้าที่งานที่สำคัญซึ่งจำเป็นสำหรับองค์กรในการดำเนินธุรกิจต่อไป การกำหนดวิธีการควบคุมที่มีเพื่อลดความเสี่ยงขององค์กร และการประเมินต้นทุนสำหรับวิธีการควบคุมดังกล่าว การวิเคราะห์

ความเสี่ยงมักเกี่ยวข้องกับการประเมินความน่าจะเป็นและโอกาสของเหตุการณ์บางเหตุการณ์ ภาวะวิกฤตเป็นตัวอย่างของเหตุการณ์

คู่มือช่วยปฏิบัติ (Practice Aid) ที่ 3: มาตรฐาน และแหล่งข้อมูลที่ให้แนวทางเกี่ยวกับ BCM

มีอยู่หลายแห่งที่ให้มาตรฐานและแนวทางที่เกี่ยวกับ BCM แหล่งข้อมูลต่างๆ ได้แก่ กรอบ และแบบจำลองวุฒิภาวะ (maturity models) เพื่อใช้ในการเทียบเคียงบทบาทของผู้ตรวจสอบภายในในการสนับสนุนวงจรการพัฒนาแผนเพื่อความต่อเนื่องทางธุรกิจ (BCP) และแผนการจัดการภาวะวิกฤต (CMP) แหล่งที่มาของข้อมูลจำนวนมากอาจให้ความรู้แก่ผู้ตรวจสอบภายใน และให้โอกาสในการแบ่งปันความรู้แก่ฝ่ายบริหารขององค์กรที่ต้องการสร้าง ปรับปรุง หรือสอบยัน BCM แหล่งข้อมูลต่างๆ ณ เดือนเมษายน 2556 ได้แก่:

- *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน ของ IIA (The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing--Standards)* และแนวทางที่เกี่ยวข้อง (www.theiia.org) ซึ่งได้แก่:
    - *แนวทางการตรวจสอบทางเทคโนโลยีระดับโลก ของ IIA (The IIA Global Technology Audit Guide หรือ GTAG) ฉบับที่ 10 เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)* แนวทางนี้รวมถึง:1) สถานการณ์ภัยพิบัติทั่วไป 2) บทบาทของฝ่ายบริหารระหว่างการหยุดชะงักทางธุรกิจ 3) การแก้ไขปัญหาในการฟื้นฟูจากภัยพิบัติ 4) การประเมินความเสี่ยงและการบรรเทาความเสี่ยง 5) การกอบกู้ธุรกิจและกลยุทธ์เพื่อความต่อเนื่อง และ 6) การทดสอบแผน CM
    - การสำรวจและผลการสำรวจโดย GAIN ปี 2553 – การบริหารภาวะวิกฤต
    - Audit Executive Center's 2011 Knowledge Alert – เรื่อง สามสิ่งจำเป็นสำหรับ CAE ในการบริหารภาวะวิกฤต (Three Crisis Management Imperatives for CAEs)
- *ANSI/ASIS/BSI CM.01:2010*, *Business Continuity Management Systems–Requirements With Guidance for Use* (2010) ความร่วมมือระหว่างสถาบันมาตรฐานแห่งชาติสหรัฐอเมริกา (American National Standards Institute หรือ ANSI), American Society for Industrial Security (ASIS International) และ สถาบันมาตรฐานแห่งบริติช (British Standards Institute หรือ BSI) เพื่อจัดทำกรอบของเกณฑ์การตรวจสอบพร้อมทั้งแนวทางเพิ่มเติมที่สามารถปรับแต่งให้ตอบสนองต่อความต้องการขององค์กรในการดำเนินงานที่ตั้งอยู่ทั่วโลก

- Disaster Recovery Institute (www.drii.org), *Professional Practices for Business Continuity Planners* (2008) กรอบที่ใช้กันอย่างแพร่หลายโดยมีข้อมูลเกี่ยวกับ: 1) การริเริ่มจัดตั้งโครงการและการบริหารโครงการ 2) การประเมินความเสี่ยงและการควบคุม 3) การวิเคราะห์ผลกระทบทางธุรกิจ 4) กลยุทธ์เพื่อความต่อเนื่องทางธุรกิจ 5) การตอบสนองภาวะฉุกเฉินและการปฏิบัติงาน 6) แผนเพื่อความต่อเนื่องทางธุรกิจ 7) โครงการสร้างการรับรู้และการฝึกอบรม 8) การตรวจสอบและการดูแลรักษา 9) การสื่อสาร และ 10) การประสานงานกับหน่วยงานภายนอก
- Federal Financial Institutions Examination Council (www.ffiec.gov/), *Business Continuity Planning, IT Examination Handbook* (2008) คู่มือซึ่งประกอบด้วยเจ็ดองค์ประกอบ: 1) ความรับผิดชอบของคณะกรรมการและฝ่ายบริหาร 2) กระบวนการวางแผนเพื่อความต่อเนื่องทางธุรกิจ 3) การวิเคราะห์ผลกระทบทางธุรกิจ 4) การประเมินความเสี่ยง 5) การบริหารความเสี่ยง 6) การเฝ้าติดตามและการทดสอบความเสี่ยง และ 7) นโยบายอื่น ๆ มาตรฐาน และกระบวนการต่างๆ
- The Business Continuity Institute's (www.thebci.org/) *Good Practice Guidelines* (2010) แนวทางซึ่งประกอบด้วยหกองค์ประกอบ: 1) นโยบายและการบริหารโครงการ 2) การปลูกฝัง CM ในวัฒนธรรมขององค์กร 3) การทำความเข้าใจองค์กร 4) กำหนดกลยุทธ์ของ CM 5) การพัฒนาและนำวิธีการตอบสนองของ CM ไปใช้ และ 6) การฝึกซ้อม ดูแลรักษา และทบทวน
- แนวทางต่างๆ จากองค์กรกำหนดมาตรฐานสากล (International Organization for Standardization หรือ ISO) (www.iso.org/) ได้แก่:
    - ISO/Publicly Available Specification (PAS) 22399, *Societal Security–Guideline for Incident Preparedness and Operational Continuity Management* (2007) "ให้แนวทางทั่วไปสำหรับองค์กร (เอกชน รัฐบาล และองค์กรที่ไม่ใช่รัฐบาล) เพื่อพัฒนาเกณฑ์การปฏิบัติงานเฉพาะของตนเองสำหรับการเตรียมความพร้อมรับเหตุการณ์และความต่อเนื่องในการปฏิบัติงานรวมทั้งออกแบบระบบการบริหารที่เหมาะสม"
    - ISO/IEC 24762, *Guidelines for Information and Communications Technology Disaster Recovery Services* (2008) "ให้แนวทางเกี่ยวกับการให้บริการกอบกู้ภัยพิบัติจากเทคโนโลยีข้อมูลและการสื่อสารและ (ICT DR) ซึ่งเป็นส่วนหนึ่งของ BCM โดยใช้บังคับกับผู้ให้บริการ ICT DR (ทั้งภายในองค์กร และที่ว่าจ้างมาจากภายนอก) ซึ่งให้บริการในด้านสถานที่และสิ่งอำนวยความสะดวกและบริการอื่นๆ"

- ISO 27001, *Information Security Management* (2002) ช่วยเหลือองค์กรในการพัฒนาระบบการบริหารความปลอดภัยของข้อมูลที่บูรณาการ ครอบคลุม และรวมเอาวิธีปฏิบัติที่เป็นเลิศซึ่งเป็นที่ยอมรับกันทั่วโลก
- ISO 22301, *Societal Security–Business Continuity Management Systems–Requirements* ซึ่งใช้แทนมาตรฐาน BS 25999 ได้ระบุข้อกำหนดของระบบ BCM ทั่วๆ ไป ที่ใช้บังคับกับทุกองค์กรหรือบางส่วนขององค์กรเหล่านั้น

- สถาบันมาตรฐานแห่งบริติช (British Standards Institute หรือ BSI) (www.bsigroup.com/)
  - PAS 200 (2011) แนะนำองค์กรต่างๆ เกี่ยวกับประเภทของกิจกรรม และทรัพยากรที่จำเป็นในการพัฒนาและบำรุงรักษา เพื่อก่อให้เกิดการตรวจจับภาวะวิกฤต การเตรียมความพร้อม และการตอบสนองอย่างมีประสิทธิผล ข้อกำหนดจำเพาะ (specification) นี้ได้รับการสนับสนุนจากสำนักคณะรัฐมนตรีแห่งสหราชอาณาจักร และข้อกำหนดจำเพาะเกี่ยวกับการบริหารภาวะวิกฤตได้รับการพัฒนาโดยผ่านการปรึกษาหารือกับองค์กรธุรกิจชั้นนำและหน่วยงานภาครัฐหลายแห่งในสหราชอาณาจักร ข้อกำหนดจำเพาะเหล่านี้ได้ระบุข้อกำหนดสำหรับ CM เพิ่มเติมจากแนวทางใน BS 25999: เรื่อง การบริหารเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity Management) และ ISO 27001
  - BS 25777: *Information and Communications Technology Continuity Management–Code of Practice* (2008) “ให้คำแนะนำสำหรับการบริหารความต่อเนื่องของเทคโนโลยีสารสนเทศและการสื่อสาร โดยอยู่ภายในกรอบของการบริหารเพื่อความต่อเนื่องทางธุรกิจที่จัดทำโดย BS 25999-1”

องค์กรที่กล่าวมาข้างต้นหลายแห่งได้ให้การอบรม และออกวุฒิบัตรที่เกี่ยวกับ BCP ด้วย สำหรับองค์กรอื่นๆ ที่มีการจัดการฝึกอบรมและออกวุฒิบัตรรับรอง ได้แก่:

- สถาบันการบริหารเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity Management Institute - www.CM-institute.org)
- สมาคมผู้วางแผนเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity Planners Association - www.bcpa.org/)
- สถาบันระหว่างประเทศเพื่อความยืดหยุ่นทางธุรกิจ (Business Resilience Certification Consortium International - www.brcci.org/)

ผู้เขียน:

David Bentley, CIA

Brian Foster, CIA

Brian Peterson

Brian Reed, CIA

Erich Schumann, CIA, CRMA

Rita Thakkar, CIA

Benito Ybarra, CIA

ผู้สอบทาน:

Steven E. Jameson, CIA, CCSA, CFSA, CRMA

เกี่ยวกับสมาคม

ก่อตั้งขึ้นในปีพ.ศ. 2484 สมาคมผู้ตรวจสอบภายใน (IIA) เป็นสมาคมทางด้านวิชาชีพตรวจสอบภายในระดับสากล สำนักงานใหญ่ของสมาคมตั้งอยู่ที่ Altamonte Springs มลรัฐฟลอริดา สหรัฐอเมริกา IIA เป็นกระบอกเสียงให้แก่ผู้ปฏิบัติวิชาชีพตรวจสอบภายในทั่วโลก เป็นหน่วยงานที่ได้รับการยอมรับว่าเป็นผู้นำในการเป็นผู้ให้การสนับสนุน และผู้ให้ความรู้หลัก

เกี่ยวกับแนวปฏิบัติ (Practice Guides)

แนวปฏิบัติให้แนวทางสำหรับการดำเนินกิจกรรมตรวจสอบภายในโดยละเอียด ซึ่งรวมถึงรายละเอียดของกระบวนการและวิธีการต่างๆ เช่น เครื่องมือและเทคนิค โปรแกรม และขั้นตอนทีละขั้น รวมถึงตัวอย่างผลงานที่ส่งมอบ แนวปฏิบัติเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) และเป็นส่วนหนึ่งของที่แนะนำเป็นอย่างยิ่ง การปฏิบัติตามแนวปฏิบัตินี้จึงไม่มีการบังคับ แต่ก็แนะนำเป็นอย่างยิ่งให้ใช้แนวปฏิบัติได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว สำหรับเอกสารแนะนำแนวทางอื่นๆ ที่จัดทำและรับรองโดยสมาคมผู้ตรวจสอบภายใน ท่านสามารถเยี่ยมชมเว็บไซต์ของเราได้ที่ www.theiia.org/standards-guidance/

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

ลิขสิทธิ์ © 2014 สมาคมผู้ตรวจสอบภายใน หากต้องการขออนุญาตทำซ้ำ โปรดติดต่อ guidance@theiia.org

The Institute of Internal Auditors

GLOBAL HEADQUARTERS
247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.theiia.org