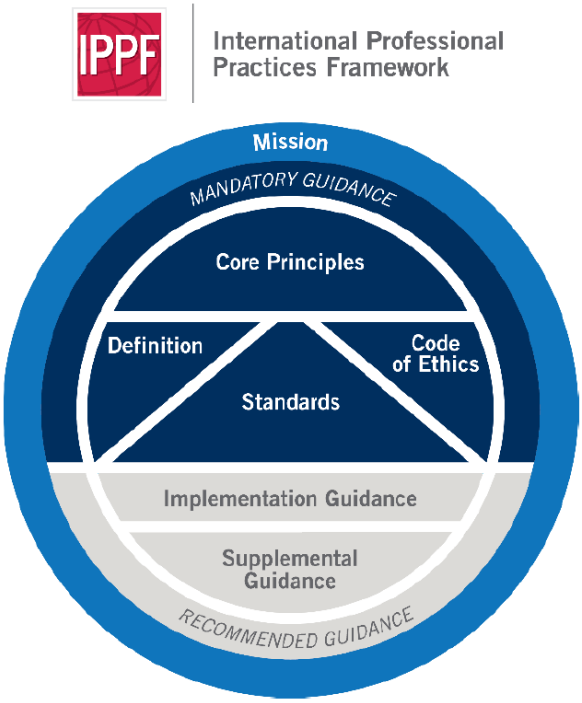
การตรวจสอบโครงการภัยคุกคามจากภายใน

The Institute of Internal Auditors | Global

เกี่ยวกับ IPPF

กรอบโครงสร้างการปฏิบัติงานวิชาชีพสากล (IPPF®) คือ กรอบโครงสร้างการทำงานตามแนวคิดที่ IIA ได้ประกาศใช้เพื่อเป็นแนวทางปฏิบัติสำหรับวิชาชีพตรวจสอบภายในทั่วโลก



แนวทางภาคบังคับ (Mandatory Guidance) ถูกพัฒนาขึ้นตามกระบวนการการศึกษาอย่างละเอียดลึกซึ้ง ซึ่งได้มีการเปิดเผยต่อสาธารณะเพื่อที่ผู้มีส่วนได้เสียจะได้ให้ข้อมูลความคิดเห็นได้

องค์ประกอบภาคบังคับของ IPPF ประกอบไปด้วย

- หลักการพื้นฐานที่สำคัญสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน
- คำจำกัดความความของการตรวจสอบภายใน
- ประมวลจรรยาบรรณ
- *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน*

ในส่วนที่เป็นแนวทางที่แนะนำจะประกอบไปด้วย แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guidance) และ แนวทางเสริม (Supplemental Guidance) แนวทางการนำมาตรฐานไปใช้ปฏิบัติ ได้รับการออกแบบมาเพื่อช่วยให้ผู้ตรวจสอบภายในเข้าใจว่าจะนำเอาข้อกำหนดต่าง ๆ ในแนวทางภาคบังคับไปประยุกต์ใช้และปฏิบัติให้สอดคล้องกับข้อกำหนดเหล่านั้นได้อย่างไร www.globaliia.org/standards-guidance.

สารบัญ

บทสรุปสำหรับผู้บริหาร

ในยุคดิจิทัล องค์กรต้องมีการปฏิบัติต่อข้อมูลเสมือนกับการปฏิบัติต่อเงินสด ในฐานะที่ข้อมูลเป็นสินทรัพย์ขององค์กรที่ต้องถูกปกป้องทั้งจากภายในและภายนอก การปกป้องสินทรัพย์ทางดิจิทัลขององค์กรจากความหายนะอันเกิดจากการล่วงละเมิดข้อมูลไม่ควรจะถูกมองว่าเป็นความรับผิดชอบของผู้บริหารหน่วยงาน IT เท่านั้น ในที่สุดแล้วผู้บริหารระดับสูงและคณะกรรมการมีความรับผิดชอบในการจัดการให้ความเสี่ยงขององค์กรอยู่ในระดับที่ทำให้องค์กรมีความสามารถที่จะบรรลุวัตถุประสงค์ได้

ไม่ว่าภัยคุกคามจากภายในจะเกิดจากการมุ่งร้ายหรือเกิดจากความไม่ได้ตั้งใจ ภัยคุกคามจากภายในมักจะไม่ได้รับความสนใจเท่าที่ควรเมื่อเทียบกับระดับความเสี่ยงอย่างมีนัยสำคัญที่ภัยคุกคามนั้น ก่อให้เกิดขึ้นกับองค์กร ความเสี่ยงที่สำคัญอันเกิดจากภัยคุกคามจากภายในรวมถึง การก่อวินาศกรรม การขโมยข้อมูลขององค์กร การจารกรรม การทุจริต และการกระทำผิดทางอาญา นอกจากนี้ แนวโน้มจากการวิจัยบ่งชี้ว่า ภูมิทัศน์ของภัยคุกคามจากภายในนั้นกำลังเพิ่มขึ้นเพราะว่าองค์กรมีการพึ่งพาระบบข้อมูลสารสนเทศ กระบวนการอัตโนมัติ แอพพลิเคชันที่อาศัยเว็บ (Web -based application) การส่งข้อมูลแบบดิจิทัล และการเก็บข้อมูลบนคลาวด์

องค์กรทั้งหลายกำลังตระหนักว่าการลงทุนในเทคโนโลยีเป็นเพียงทางออกหนึ่งที่มีความสำคัญพอๆ กับการประเมินว่าการกำกับดูแล และการควบคุมในทางการบริหาร (เช่น นโยบายระบบเทคโนโลยีสารสนเทศ การฝึกอบรมและการสร้างการรับรู้) มีความสามารถเพียงพอที่จะจัดการกับภัยคุกคามจากภายในได้

ผู้ตรวจสอบภายในอยู่ในสถานะที่ดีที่จะช่วยให้ผู้บริหารระดับสูงและคณะกรรมการตระหนักถึงความสำคัญของการนำเอาโครงการการจัดการกับภัยคุกคามจากภายในไปลงมือดำเนินการ หรือเสริมสร้างความแข็งแกร่งให้กับโครงการการจัดการกับภัยคุกคามจากภายใน และเพื่อช่วยให้องค์กรปรับปรุงการกำกับดูแล การบริหารความเสี่ยงและกระบวนการควบคุมต่าง ๆ ที่เกี่ยวข้องกับภัยคุกคามจากภายใน

บทนำ

ภัยคุกคามจากภายในหมายถึงความเป็นไปได้ที่สิ่งใดก็ตามที่ได้รับสิทธิการเข้าถึงเขตของความมั่นคงปลอดภัยอย่างถูกต้องจะทำอันตรายต่อระบบเทคโนโลยีสารสนเทศหรือองค์กรโดยการทำลาย เปิดเผย เปลี่ยนแปลงข้อมูล และหรือก่อให้เกิดการปฏิเสธการให้บริการ[1]

ความหมายนี้รวมถึงการโจมตีแบบมุ่งร้ายและแบบไม่ได้มุ่งร้าย (เกิดโดยไม่ตั้งใจ) ต่อสินทรัพย์ขององค์กร รวมถึงบุคลากร

หมายเหตุ: ความหมายของคำที่เป็นตัวหนาถูกกำหนดอยู่ในอภิธานศัพท์ของภาคผนวก ข

แนวทางฉบับนี้มีการใช้ศัพท์เทคนิคที่หลากหลายสำหรับผู้ที่มีความคุ้นเคยกับเรื่องความมั่นคงปลอดภัยของข้อมูล ถ้าในอภิธานศัพท์ไม่ได้มีการระบุความหมายของคำใดไว้ขอให้ท่านขอคำปรึกษาจากแหล่งข้อมูลอ้างอิงหรืออ่านเพิ่มเติมจากแหล่งที่ระบุอยู่ในภาคผนวก ฉ

ตรงข้ามกับภัยคุกคามจากภายนอก (เช่น บุคคลที่ไม่มีสิทธิในการเข้าถึงระบบขององค์กร) คนภายใน เช่น พนักงาน อดีตพนักงาน ผู้รับเหมา และคู่ค้าทางธุรกิจ เป็นผู้ซึ่งมีความรู้และมีการเข้าถึงข้อมูลและระบบขององค์กรในระดับหนึ่งอยู่แล้ว ดังนั้น จึงง่ายมากที่คนเหล่านี้จะสามารถผ่านมาตรการรักษาความมั่นคงปลอดภัยหลายๆ อย่างและใช้สิทธินี้อย่างไม่ถูกต้องในการดูข้อมูล คัดลอก ดาวน์โหลด กระทำทุจริต ลบหรือส่งข้อมูลที่มีความอ่อนไหวและมีความสำคัญออกไปนอกองค์กร

ความเสี่ยง ที่เกี่ยวข้องกับภัยคุกคามจากภายในรวมถึง

- การทุจริต
- การก่อวินาศกรรม
- การขโมยสินทรัพย์ทางปัญญาหรือความลับทางการค้า
- การเปิดเผยข้อมูลที่สำคัญ
- การใช้ทรัพยากรเทคโนโลยีสารสนเทศในกิจกรรมที่ผิดกฎหมาย

การตระหนักรู้ถึงภัยคุกคามจากภายในและความเสี่ยงที่เกี่ยวข้องและโดยการเรียนรู้เกี่ยวกับภัยคุกคามจากภายในจะทำให้ผู้ตรวจสอบภายในมีโอกาสที่จะเพิ่มคุณค่าให้กับองค์กร ด้วยการช่วยทำให้ **การกำกับดูแล** การบริหารความเสี่ยงและ **กระบวนการควบคุม** เพื่อจัดการกับภัยคุกคามภายในมีความเข้มแข็งมากขึ้น

แนวทางการตรวจสอบเทคโนโลยีในระดับสากล (GTAG) มุ่งหมายที่จะช่วยผู้ตรวจสอบภายในให้มีความเข้าใจถึงภัยคุกคามจากภายในและความเสี่ยงที่เกี่ยวข้องโดยการให้ความรู้ถึงภาพรวมของภัยคุกคามจากภายใน ความเสี่ยงที่สำคัญ และผลกระทบที่อาจเกิดขึ้นได้ นอกจากนี้ แนวทางนี้ยังได้ให้ตัวอย่างของกรอบความมั่นคงปลอดภัยจากแหล่งที่ได้รับการยอมรับในระดับสากลซึ่งรวมถึง สถาบันวิศวกรรมซอฟต์แวร์ของมหาวิทยาลัย Carnegie Mellon

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) และ U.S. Intelligence and National Security Alliance (INSA) วิธีการควบคุม และแหล่งข้อมูลอื่น ๆ ที่จะสามารถช่วยผู้ตรวจสอบได้ในระหว่างการวางแผนและลงมือปฏิบัติงานตรวจสอบที่ได้รับมอบหมาย องค์กรควรเลือกกรอบที่เหมาะสมกับสถานการณ์เฉพาะของตนเอง โดยให้น้ำหนักตามปัจจัยที่เกี่ยวข้องกับองค์กรของตน เช่น ประเภทของอุตสาหกรรม ขนาด ความซับซ้อน และความเหมาะสมของการนำกรอบที่เลือกไปใช้ปฏิบัติ

[1] Committee on National Security Systems, *CNSS Instruction No. 4009*, Washington DC: National Security Agency, April 26, 2010: 38. https://www.hsdl.org/?view&did=7447

สำหรับองค์กรที่มีโครงการเกี่ยวกับภัยคุกคามจากภายในอยู่แล้ว ผู้ตรวจสอบภายในอาจใช้แนวทางนี้ในการออกแบบงานการให้ความเชื่อมั่นที่ได้รับมอบหมายในการประเมินความมีประสิทธิผลของโครงการที่มีอยู่ได้

ผลกระทบทางธุรกิจ:
ความเสียหายที่ภัยคุกคามจากภายในทำให้เกิดขึ้นได้นั้นสามารถตีมูลค่าได้เป็นหลักล้านเหรียญสหรัฐ ในช่วงปีที่ผ่านมามีการรายงานว่าพนักงานสามคนของผู้ผลิตSuperconductors ได้ขโมยความลับทางการค้าและขายให้กับคู่แข่งเป็นเวลามากกว่าหกปี ซึ่งมูลค่าโดยประมาณของความลับทางการค้านั้นคือ 800 ล้านเหรียญสหรัฐ อย่างไรก็ตาม ความเสียหายที่เกิดขึ้นกับผู้ถือหุ้นนั้นมีมากถึงเกือบ 1,000 ล้านเหรียญสหรัฐ[2]

แนวทางนี้ยังได้บรรยายถึงแนวทางต่าง ๆ ในงานให้คำปรึกษาซึ่งผู้ตรวจสอบภายในสามารถที่จะใช้ช่วยผู้บริหารในการระบุและประเมินความเสี่ยงซึ่งควรจะได้รับการพิจารณาในการออกแบบและนำโครงการใหม่เกี่ยวกับภัยคุกคามจากภายในออกใช้งาน หรือเพื่อเปรียบเทียบวุฒิภาวะของโครงการในปัจจุบันเพื่อการปรับปรุงให้ดียิ่งขึ้น

ในท้ายที่สุดแล้ว แนวทางการตรวจสอบเทคโนโลยีในระดับสากล (GTAG) ฉบับนี้ยังให้เคล็ดลับในการสื่อสารกับคณะกรรมการเกี่ยวกับความมีนัยสำคัญของความเสี่ยงและความจำเป็นในการระบุ การป้องกัน การตรวจหา การตอบสนอง และการกู้คืนจากเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูลอันเกี่ยวข้องกับภัยคุกคามจากภายใน

ภาพรวมเกี่ยวกับภัยคุกคามจากภายใน

คำว่าภัยคุกคามบางครั้งถูกใช้ในการกล่าวถึงผู้คุกคามหรือการโจมตี ด้วยเหตุผลนี้จึงมีความสำคัญที่จะให้นิยามของคำศัพท์ทางเทคโนโลยีเฉพาะบางคำซึ่งจะถูกใช้ตลอดในแนวปฏิบัติฉบับนี้

ผลกระทบ (Impact) คือผลลัพธ์ในทางบวกหรือในทางลบ หรือผลกระทบอันเกิดจากความเสี่ยง

ภัยคุกคาม (Threat) คือสถานการณ์หรือเหตุการณ์ใด ๆ ก็ตามที่อาจก่อให้เกิดผลเสียหายกับองค์กรทั้งในแง่การดำเนินงาน สินทรัพย์ขององค์กร บุคลากรหรือต่อองค์กรอื่น ๆ

ผู้คุกคาม (Threat actor) คือผู้ที่รับผิดชอบต่อการกระทำ (หรือการไม่กระทำ) ที่เกิดขึ้นอันส่งผลเสียหายต่อองค์กร

แหล่งกำเนิดของภัยคุกคาม (Threat source) คือการจงใจและวิธีการที่พุ่งเป้าตั้งใจที่จะใช้ประโยชน์จากจุดอ่อนที่มีอยู่ หรือเป็นสถานการณ์และวิธีการซึ่งอาจจะใช้ประโยชน์จากจุดอ่อนโดยที่ไม่ได้ตั้งใจ

ความเสี่ยง (Risk) คือความเป็นไปได้ของเหตุการณ์ที่หากเกิดขึ้นจะก่อให้เกิดผลกระทบต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงถูกวัดจากผลกระทบและความเป็นไปได้ที่จะเกิดขึ้น

จุดเปราะบาง (Vulnerability) คือจุดอ่อนในระบบข้อมูล วิธีการปฏิบัติงานของระบบความมั่นคงปลอดภัย วิธีการควบคุมภายใน หรือ การนำเอาระบบไปใช้ปฏิบัติ ซึ่งแหล่งกำเนิดของภัยคุกคามสามารถนำไปใช้ประโยชน์ได้

---

[2] Christopher Burgess, "Sinovel Wind Group found guilty of IP theft, fined $1.5 million," CSO magazine, July 9, 2018, https://www.csoonline.com/article/3256305/loss-prevention/sinovel-wind-group-found-guilty-of-ip-theft-valued-at-800-million.html.

ภัยคุกคามจากภายในอาจเป็นการมุ่งร้ายเมื่อผู้คุกคามจงใจที่จะใช้การเข้าถึงระบบเครือข่ายขององค์กรหรือข้อมูลไปในทางที่ผิดอันก่อให้เกิดผลเสียหายต่อการรักษาความลับ ความถูกต้องครบถ้วน หรือความพร้อมของข้อมูลหรือระบบข้อมูลขององค์กร อย่างไรก็ตาม ภัยคุกคามจากภายในอาจเกิดขึ้นได้จากสิ่งที่ไม่ใช่ภัยคุกคาม (ไม่ได้ตั้งใจ) โดยผู้กระทำได้กระทำการหรือไม่ได้กระทำการอย่างหนึ่งอย่างใดโดยไม่ได้มีการมุ่งร้ายแต่ก่อให้เกิดความเสียหายหรือเพิ่มโอกาสที่จะเกิดความเสียหายต่อการรักษาความลับ ความถูกต้องครบถ้วน หรือความพร้อมใช้ ของข้อมูลหรือระบบสารสนเทศขององค์กร ดังตัวอย่างสรุปโดยย่อใน**ตารางที่** 1

ภาพที่ 1: **ตัวอย่างของภัยคุกคามจากภายใน**

การมุ่งร้าย	ไม่ได้เป็นการมุ่งร้าย
พนักงานขโมยความลับทางการค้าไปขายให้กับคู่แข่ง[3]	ผู้ดูแลระบบปิดเว็ปไซต์โดยไม่ได้ตั้งใจ
อดีตพนักงานทำความเสียหายให้เกิดกับระบบเครือข่ายคอมพิวเตอร์ของอดีตนายจ้าง[4]	ผู้ใช้งานลบไฟล์ทิ้งโดยไม่ได้ตั้งใจ
ที่ปรึกษาใช้ข้อมูลของบัตรเครดิตไปกระทำ **การทุจริต**	พนักงานตกเป็นเหยื่อของ **การถูกหลอกลวงเพื่อเอาความลับ** (social engineering) หรือ อีเมลหลอกลวง (Phishing emails)

การสมรู้ร่วมคิด- เกิดขึ้นเมื่อผู้คุกคามภายในหลายคนร่วมมือกันโจมตีองค์กร คนภายในองค์กรตกเป็นเป้าหมายของผู้คุกคามจากภายนอก (อาชญากรไซเบอร์ แฮกเกอร์ กลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีในการแฮกข้อมูล) และจบลงด้วยการให้ความร่วมมือโดยไม่ได้ตั้งใจ หรือเกิดขึ้นเมื่อคนภายในองค์กรตกเป็นเป้าจากผู้คิดร้ายภายนอกและจบลงด้วยการร่วมมือกันโดยตั้งใจ (หลายครั้งทำไปเพื่อผลประโยชน์)

แนวโน้มของการสมรู้ร่วมคิดก่อให้เกิดการโจมตีที่ใหญ่ขึ้นและมีโอกาสมากขึ้นที่การโจมตีจะประสบความสำเร็จและยากที่จะถูกตรวจพบ สำหรับธุรกิจขนาดกลางและขนาดเล็กซึ่งโดยทั่วไปแล้วไม่มีทรัพยากรที่จำเป็นในการจะฟื้นตัวจากการถูกโจมตีเช่นนั้น ผลกระทบอาจถึงขั้นหายนะ การบรรเทาภัยคุกคามนั้นอาจเป็นการลงทุนราคาแพง แต่เมื่อเทียบกับค่าใช้จ่ายที่ต้องเกิดขึ้นจากการกอบกู้เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่สำคัญ การป้องกันหรือการตรวจจับการโจมตีถือเป็นการลงทุนทางธุรกิจที่คุ้มค่าในระยะยาว

เมื่อดูไปถึงการที่เกิดเหตุการณ์ข้อมูลรั่วไหลอันเกิดจากการกระทำโดยไม่ตั้งใจพบว่า ต้นทุนเฉลี่ยของความเสียหายเพิ่มขึ้นอย่างมีนัยสำคัญ ยิ่งไปกว่านั้น การที่ผู้โจมตีมุ่งร้ายเริ่มมีความชำนาญในการมุ่งหาเป้าหมายบุคคลภายในที่ไม่สงสัยด้วยแล้ว ต้นทุนค่าใช้จ่ายก็น่าจะยิ่งเพิ่มมากขึ้นเรื่อย ๆ

---

3 Kacy Zurkus, "Former Apple Employee Charged with Data Theft," *InfoSecurity Magazine*, July 11, 2018, https://www.infosecurity-magazine.com/news/apple-filed-criminal-complaint-of/.

4 "Former Employee of Transcontinental Railroad Company Found Guilty of Damaging Ex-Employer's Computer Network," U.S. Department of Justice, October 10, 2017, https://www.justice.gov/usao-mn/pr/former-employeetranscontinental-railroad-company-found-guilty-damaging-ex-employer-s.

ตัวอย่างการกระทำที่ไม่ได้ตั้งใจอันมีผลต่อการละเมิดข้อมูล ได้แก่

การเปิดเผยข้อมูลโดยไม่ตั้งใจ - คนภายในองค์กรเผยแพร่ข้อมูลโดยไม่ได้ตั้งใจหรือมีการจัดการข้อมูลที่อ่อนไหวอย่างไม่เหมาะสม หรือส่งข้อมูลไปให้ผู้รับผิดผ่านทาง อีเมล แฟกซ์

Phishing/social engineering – การที่คนนอกสามารถเข้าสู่ระบบภายในองค์กรโดยอาศัยการหลอกลวงเพื่อเอาความลับ จากคนในองค์กร (เช่น การใช้อีเมลหลอกลวง การนำโปรแกรมที่เป็นอันตรายเข้ามาแฝงตัว หรือการใช้ USB ที่ไม่ได้รับอนุญาต) เพื่อให้ได้สิทธิจากคนภายในองค์กร หรือเพื่อวางแผนใส่มัลแวร์เพื่อการเข้าถึงระบบ หรือ การส่งผ่านทางโซเชียลมีเดีย

ต้นทุนของเหตุการณ์ที่เกี่ยวกับคนภายในในช่วง 12 เดือน

- เหตุการณ์เกิดขึ้นทั้งหมด: 3,269
- ต้นทุนเฉลี่ยทั้งหมด: 8.76 ล้านเหรียญสรอ.
- เหตุการณ์ที่เกิดขึ้นจากการละเลย: 64%
- เหตุการณ์อาชญากรรมโดยคนใน: 23%
- เหตุการณ์ที่เป็นการขโมยสิทธิผู้ใช้: 13%

แหล่งที่มา: การวิจัย: Ponemon Institute©, and Sponsorship: Observe IT, 2018 Cost of Insider Threats: Global, เมษายน 2561

การเข้าถึงข้อมูลทางกายภาพโดยไม่ได้รับอนุญาต - ข้อมูลที่ไม่อยู่ในรูปแบบอิเล็กทรอนิกส์ เช่น เอกสารข้อมูลที่เป็นกระดาษ สูญหาย วางทิ้งไว้โดยไม่มีผู้ดูแล หรือถูกขโมย ทำให้ผู้ไม่ได้รับอนุญาตหรือโดยผู้ใช้งานที่ประสงค์ร้ายเข้าถึงข้อมูลได้

การเข้าถึงข้อมูลจากเครื่องมืออุปกรณ์ที่พกพาได้โดยไม่ได้รับอนุญาต - การที่อุปกรณ์ที่ใช้เก็บข้อมูลแบบพกพาได้ เช่น คอมพิวเตอร์โน้ตบุค โทรศัพท์เคลื่อนที่ อุปกรณ์เก็บข้อมูล ซีดี ฮาร์ดไดรฟ์ หรือเทปเก็บข้อมูลสูญหาย ถูกลืมทิ้งไว้ หรือถูกขโมย ทำให้ผู้ไม่ได้รับอนุญาตหรือผู้ใช้งานที่ประสงค์ร้ายข้อมูลเข้าถึงได้

การวิเคราะห์ภัยคุกคามจากภายใน

การสร้างข้อมูลประวัติ (Profile) ของภัยคุกคามจากภายในนั้นจำเป็นจะต้องพิจารณาจากหลายๆ ปัจจัยเช่น ใครคือผู้คุกคาม สินทรัพย์อะไรที่อาจจะตกเป็นเป้าหมายได้ แรงจูงใจของการโจมตี และผลกระทบที่อาจเกิดขึ้นได้กับองค์กร

แหล่งกำเนิดหรือผู้ก่อให้เกิดภัยคุกคาม

ภัยคุกคามจากภายในนั้นตรวจพบได้ยากเพราะว่าภัยนั้นไม่จำเป็นจะต้องเกิดจากแฮกเกอร์ หรือผู้เชี่ยวชาญด้านอาชญากรรมไซเบอร์เท่านั้น คำว่าภายในโดยคำจำกัดความหมายถึง คนในองค์กรหรือหน่วยงานซึ่งมีสิทธิหรือเคยได้รับสิทธิในการเข้าถึงข้อมูลหรือระบบข้อมูลขององค์กรอยู่แล้ว (ไม่ว่าจะเป็นข้อมูลทางกายภาพหรือข้อมูลในระบบ) ผู้คุกคามโดยทั่วไปที่ควรจะต้องคำนึงถึงในการสร้างข้อมูลประวัติหรือสถานการณ์ความเสี่ยงของภัยคุกคามจากภายในนั้นรวมถึง:

- พนักงานในปัจจุบันและอดีตพนักงาน
- พนักงานแบบทำงานเต็มเวลาหรือแบบชั่วคราว
- พนักงานที่ทำงานแบบไม่ประจำหรือผู้รับเหมา
- **หุ้นส่วนทางธุรกิจ** ที่ได้รับความไว้ใจ

แม้จะเป็นการยากที่จะระบุว่าใครคือผู้ที่มีความเสี่ยงสูงสุดในการทำกิจกรรมที่เป็นอันตรายต่อองค์กร การทำความเข้าใจถึงลักษณะบางประการของพฤติกรรมพื้นฐานของผู้คุกคามจากภายในอาจนำมาใช้เป็นประโยชน์ช่วยได้ ในตารางที่ 2 แสดงให้เห็นถึงลักษณะของพฤติกรรมอันตรายที่เผยแพร่โดย National Cybersecurity and Communications Integration Center

มีข้อสังเกตว่ารายการแสดงลักษณะเฉพาะเหล่านี้ไม่ได้แสดงถึงความสำคัญหรือความเป็นไปได้

ตารางที่ 2: ลักษณะเฉพาะของคนภายในที่มีความเสี่ยงจะกลายเป็นการคุกคามได้

ชอบเก็บตัว	มีความกังวลเกี่ยวกับการหลบเลี่ยง ซ่อนเร้น หรือแก้ไขข้อผิดพลาด มากเกินไป
ละโมบ/ต้องการเงิน	ไม่สามารถรับภาระหน้าที่ในการกระทำการต่าง ๆ
มีความอ่อนไหวต่อการถูกแบล็คเมล์	ไม่อดทนต่อคำวิจารณ์
มีพฤติกรรมบังคับขู่เข็ญและทำลายล้าง	ให้คุณค่าตนเองมากกว่าการกระทำ/ผลงานจริง
มีพฤติกรรม ก้าวร้าว ดื้อรั้น	ไม่มีความเห็นเห็นใจผู้อื่น
มีความยืดหยุ่นทางด้านจริยธรรม	มีรูปแบบของความไม่พอใจ ความผิดหวัง
เจ้ายศเจ้าอย่าง หลงตัวเอง (ชอบโอ้อวด)	มีประวัติในการจัดการกับเหตุการณ์วิกฤติอย่างไม่มีประสิทธิผล

แหล่งข้อมูล: National Cybersecurity and Communications Integration Center, การต่อสู้กับภัยคุกคามภายใน 1

เป้าหมาย

กลุ่มเป้าหมายรวมถึงสินทรัพย์หรือสิ่งที่มีค่าทุกอย่าง ขององค์กรซึ่งอาจได้รับผลกระทบจากการคุกคามและก่อให้เกิดผลเสียต่อองค์กร รวมถึง

- บุคลากร
- ข้อมูล
- เทคโนโลยี
- สถานที่ทำงาน เครื่องมือและอุปกรณ์ต่าง ๆ

ตัวบ่งชี้ที่เป็นไปได้ว่าจุดอ่อนกำลังถูกโจมตี/แสวงหาประโยชน์

- การ uploads ขึ้นไปเก็บที่ cloud
- การใช้อุปกรณ์เก็บข้อมูลแบบเคลื่อนย้ายพกพาได้
- การทำงานในเวลาไม่ปกติโดยไม่ได้รับอนุญาต
- การส่งเมลถึงบุคคลภายนอกหรืออีเมลส่วนตัว
- การพิมพ์หรือคัดลอกข้อมูลที่เป็นความลับมากเกินไป
- การขอสิทธิ์เข้าถึงพื้นที่หรือระบบที่เคยถูกปฏิเสธมาก่อนหน้า

แรงจูงใจ

แรงจูงใจของผู้คุกคามจากภายในที่จะทำการอันไม่ได้มีประสงค์ร้ายนั้นมีความแตกต่างและหลากหลายกันไปตั้งแต่เรื่องส่วนตัวนอกที่ทำงาน ปัญหากับเพื่อนร่วมงานและเจ้านายรวมถึงโอกาสและความเบื่อหน่ายซึ่งสามารถทำให้เกิดการกระทำนี้ได้

แรงจูงใจของการโจมตีมุ่งร้าย ได้แก่

- ผลประโยชน์ทางการเงิน
- การทุจริต
- การก่อกวน
- การปองร้าย
- การแก้แค้น
- การโจรกรรม
- การขโมย
- เกี่ยวข้องกับอาชญากร

ผลกระทบในทางลบ

ผลกระทบของการแสวงหาประโยชน์หรือโจมตีจุดอ่อนจากภายในนั้นสามารถจำแนกได้ตามกรอบการบริหารความเสี่ยงทั่วทั้งองค์กรของ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) กล่าวคือ ผลกระทบทางการเงิน การปฏิบัติการ การปฏิบัติตามกฎระเบียบและลูกค้า

เป็นเรื่องปกติที่การโจมตีในครั้งเดียวอาจจะมีผลกระทบต่อองค์กรในหลายๆ ด้าน ยกตัวอย่างเช่น การทำลายระบบข้อมูลที่มีความสำคัญสามารถก่อให้เกิดความเสียหายทางการเงิน (ค่าใช้จ่ายในการกู้คืนระบบ) ความเสียหายด้านการปฏิบัติการ (สูญเสียผลผลิต) รวมถึงผลกระทบต่อลูกค้า (การได้รับบริการที่ไม่ดีในช่วงที่เกิดเหตุขึ้น)

ข้อมูลประวัติ (Profile) ภัยคุกคามจากภายในสามารถพัฒนาขึ้นได้โดยใช้มุมมองที่ได้กล่าวถึงไปก่อนหน้านี้แล้ว ซึ่งได้แสดงในตารางที่ 3 ดังนี้

ตารางที่ 3: การสร้างข้อมูลประวัติภัยคุกคามจากภายใน

	ข้อมูลประวัติ 1	ข้อมูลประวัติ 2
ภัยคุกคาม	การทำลายล้างด้าน IT	การขโมยสินทรัพย์ทางปัญญา
ผู้คุกคาม	อดีตพนักงาน	พนักงานปัจจุบัน
เป้าหมาย	เครือข่ายคอมพิวเตอร์	ความลับทางการค้า
แรงจูงใจ	การมุ่งร้าย แก้แค้น	ผลประโยชน์ทางการเงิน
ผลกระทบเชิงลบ	การดำเนินงานหยุดชะงัก	การสูญเสียความสามารถในการแข่งขัน

นอกจากนี้ องค์กรควรให้ความสำคัญกับการจัดลำดับความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายในโดยพิจารณาจากปัจจัยต่าง ๆ เช่น ความเป็นไปได้ และความรวดเร็วของเหตุการณ์ที่จะเกิด รวมทั้งความพยายามอย่างไม่ลดละขององค์กรในการสร้างข้อมูลประวัติของความเสี่ยงซึ่งสะท้อนถึงระดับและขอบเขตของความเสี่ยงที่ยอมรับได้ขององค์กร

ควรมีการอ้างอิงถึงกันระหว่างความเสี่ยงกับบุคลากรที่อาจก่อให้เกิดภัยคุกคามเพื่อให้สามารถสร้างข้อมูลประวัติของความเสี่ยงที่มีอยู่ตามธรรมชาติสำหรับตำแหน่งงานต่าง ๆ เช่น ผู้ดูแลระบบ พนักงาน help desk ผู้ให้บริการซึ่งในการทำงานจะต้องมีการเข้าถึงข้อมูลที่มีความสำคัญและเป็นความลับ การสร้างข้อมูลประวัติความเสี่ยงตามตำแหน่งงานจะช่วยฝ่ายจัดการในการวางระบบการควบคุมเพื่อที่จะป้องกันและตรวจพบการโจมตีทั้งแบบที่ตั้งใจและไม่ได้ตั้งใจอย่างคุ้มค่า

บทบาทของผู้ตรวจสอบภายในในการบริหารจัดการภัยคุกคามจากภายใน

หน่วยงานตรวจสอบภายใน ใช้แนวทางที่เป็นระบบ มีระเบียบ บนพื้นฐานของความเสี่ยง ในการให้ความเชื่อมั่นอย่างเที่ยงธรรม การให้คำปรึกษา และการให้ข้อมูลเชิงลึก เมื่อพูดถึงการจัดการกับภัยคุกคามจากภายใน ภาระหน้าที่หลักของหน่วยงานตรวจสอบภายในคือ การให้บริการให้ความเชื่อมั่นและให้คำปรึกษาเพื่อช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ โดยการประเมินและมีส่วนช่วยให้เกิดการปรับปรุงกระบวนการ การบริหารความเสี่ยงขององค์กร การควบคุม และการกำกับดูแล ขององค์กรตามที่ระบุไว้ในมาตรฐาน 2100 – ลักษณะของงาน

งานให้คำปรึกษา

ตามมาตรฐาน 2010.C1 กำหนดให้หัวหน้าหน่วยงานตรวจสอบภายในพิจารณาว่า ควรจะรับงานให้คำปรึกษาที่ถูกร้องขอมา ถ้างานนั้นมีแนวโน้มที่จะเพิ่มคุณค่าในการปรับปรุงการบริหารความเสี่ยง และการปฏิบัติการขององค์กรได้

งานให้ความเชื่อมั่นที่ได้รับมอบหมายมีจุดประสงค์เพื่อประเมินประสิทธิผลของการควบคุม รวมถึงโอกาสในการปรับปรุงให้ดีขึ้น อีกทั้งยังช่วยให้ผู้บริหารระดับสูงและคณะกรรมการมีความเข้าใจในเรื่องความเสี่ยงที่ดีขึ้นและความจำเป็นที่จะต้องมีการตอบสนองต่อความเสี่ยง ในอีกด้านหนึ่ง งานบริการให้คำปรึกษาอาจช่วยให้องค์กรพัฒนาหรือปรับปรุงเรื่องการจัดการภัยคุกคามจากภายใน (ซึ่งก็คือ การเข้าไปมีส่วนร่วมตั้งแต่ช่วงต้นๆ) หรืออาจจะช่วยประเมินความเพียงพอของโครงการ (ซึ่งก็คือ การเปรียบเทียบกับมาตรฐาน)

การบริการให้คำปรึกษาอาจสร้างคุณค่าได้เมื่อเจ้าหน้าที่ปฏิบัติการด้าน IT ไม่มีเวลาและทรัพยากรในการประเมินความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายใน รวมถึงการระบุวิธีการควบคุมที่จำเป็นได้ ผู้ตรวจสอบภายในอาจช่วยสนับสนุนพนักงานบริหารระบบและเครือข่ายในการประเมินความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายใน ระบุประเด็นที่ผู้ดูแลบริหารระบบและความมั่นคงปลอดภัยมองข้ามไป หรือสิ่งที่ยังไม่ได้มีการปฏิบัติตามนโยบายอย่างเหมาะสม ในขอบเขตของงานให้คำปรึกษานี้ ผู้ตรวจสอบภายในอาจให้ข้อเสนอแนะในการระบุและจัดการกับจุดอ่อนรวมทั้งให้ความรู้เชิงลึกอย่างเที่ยงธรรม

ผู้ตรวจสอบภายในต้องประเมินและให้ข้อเสนอแนะที่เหมาะสมในการปรับปรุงกระบวนการกำกับดูแลขององค์กรอย่างเป็นอิสระในงานที่ได้รับมอบหมาย (มาตรฐาน 2110 -การกำกับดูแล) ในหลายๆ กรณี องค์กรอาจจะมีวิธีการควบคุมด้านเทคโนโลยีอยู่แล้ว แต่ยังไม่ได้สร้างกรอบการกำกับดูแลอย่างเป็นทางการเพื่อใช้ในการสั่งการ กำกับ บริหารจัดการ และติดตาม กิจกรรมที่มีความสำคัญต่อความสำเร็จขององค์กร ตัวอย่างหนึ่งของสถานการณ์แบบนี้คือ การไม่มีนโยบายหรือวิธีการปฏิบัติงานที่สม่ำเสมอในการควบคุมจัดการกำหนดสิทธิของผู้ใช้งาน ส่งผลให้เกิดการได้รับสิทธิมากเกินความจำเป็น และก่อให้เกิดความเสี่ยงจากภัยคุกคามภายในที่เพิ่มขึ้นแม้ว่าจะมีวิธีการควบคุมทางเทคโนโลยีในการจัดการการเข้าถึงระบบงานของผู้ใช้งานแล้วก็ตาม

ควรมีการประเมินความเสี่ยงและมีการประเมินโครงการการจัดการภัยคุกคามจากภายในใหม่อย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางด้านเทคโนโลยีหรือธุรกิจที่มีนัยสำคัญ การประเมินโครงการในระดับกิจการอาจจะยากขึ้นอยู่กับขนาดขององค์กรและความซับซ้อนของสภาพแวดล้อมด้าน IT

ดังนั้น ผู้ตรวจสอบภายในอาจจะต้องปฏิบัติงานที่ได้รับมอบหมายหลายๆ งานเพื่อที่จะประเมินองค์ประกอบของโครงการที่แตกต่างกันออกไป (เช่น การกำกับดูแล ความมั่นคงปลอดภัยของข้อมูล ความมั่นคงปลอดภัยทางกายภาพ หรือวิธีปฏิบัติในการจ้างงาน) หรืออาจจะรวมองค์ประกอบต่างๆ เหล่านั้นไปในงานตรวจสอบภายในที่ได้รวมขอบเขตของสินทรัพย์ทางดิจิทัลที่มีความสำคัญเข้าไปด้วย ยกตัวอย่างเช่น ผู้ตรวจสอบภายในอาจจะประเมินว่าหน่วยงานที่มีหน้าที่ติดตามเฝ้าระวังด้านความมั่นคงปลอดภัยมีกลไกที่จำเป็นในการตรวจพบความผิดปกติจากภายในซึ่งบ่งบอกถึงการละเมิดสิทธิในการยืนยันตัวตนหรือผู้มีสิทธิในการเข้าถึงใช้สิทธินั้นอย่างไม่เหมาะสม ถ้าองค์กรมีกลไกดังกล่าวและได้ดำเนินการในการเฝ้าระวังติดตามสภาพแวดล้อมทั้งภายในและภายนอกอยู่แล้ว ผู้ตรวจสอบภายในอาจทำการประเมินความมีประสิทธิผลและประสิทธิภาพของกระบวนการควบคุมนั้น และอาจช่วยก่อให้เกิดการปรับปรุงอย่างต่อเนื่อง (มาตรฐาน 2120 การบริหารความเสี่ยง และ 2130 การควบคุม)

หัวหน้าหน่วยงานตรวจสอบภายใน (CAE) ต้องมีการพิจารณาว่า หน่วยงานตรวจสอบภายในโดยรวมแล้วมีหรือได้รับ ความรู้ ทักษะ และความสามารถอื่นๆ ที่จำเป็นต้องนำมาใช้ในการปฏิบัติงานที่ได้รับมอบหมายหรือไม่ (มาตรฐาน 1210 - ความเชี่ยวชาญ) สำหรับงานให้ความเชื่อมั่นที่ได้รับมอบหมายนั้นผู้ตรวจสอบภายในถูกคาดหวังให้มีความรู้ที่เพียงพอในเรื่องความเสี่ยงและวิธีการควบคุมด้าน ITที่สำคัญ อย่างไรก็ตาม พวกเขาไม่ได้ถูกคาดหวังให้ต้องเป็นผู้เชี่ยวชาญเหมือนกับผู้ตรวจสอบภายในเฉพาะด้าน IT (มาตรฐาน 1210.A3) ถ้าหากหน่วยงานตรวจสอบภายในขาดความรู้ความสามารถที่จำเป็นในการปฏิบัติงานให้ความเชื่อมั่นเกี่ยวกับภัยคุกคามจากภายในตามที่ได้รับมอบหมายแล้ว CAE จะต้องแสวงหาหรือขอความช่วยเหลือและคำแนะนำจากผู้มีความสามารถ อันเป็นไปตามมาตรฐาน 1210. A1.

ผู้ตรวจสอบภายในควรร่วมมือกับบุคลากรด้านปฏิบัติการ IT และความมั่นคงปลอดภัยของข้อมูล เพื่อที่จะใช้ความรู้ความสามารถทางเทคนิคในการทำให้แน่ใจว่า การประเมินภัยคุกคามจากภายในครอบคลุมอย่างเพียงพอ นอกจากนี้ CAE ควรมีการประสานงานและแชร์ข้อมูลกับหน่วยงานเหล่านี้เพื่อที่จะใช้ประโยชน์จากความรู้ความสามารถให้เกิดผลสูงสุด และทำให้แน่ใจได้ว่า การให้ความเชื่อมั่นได้มีความครอบคลุมอย่างเหมาะสม และเป็นการลดการทำงานที่ซ้ำซ้อนกัน ดังเช่นที่ระบุไว้ในมาตรฐาน 2050 เรื่องการประสานงานและการพึ่งพาผลงานของผู้อื่น

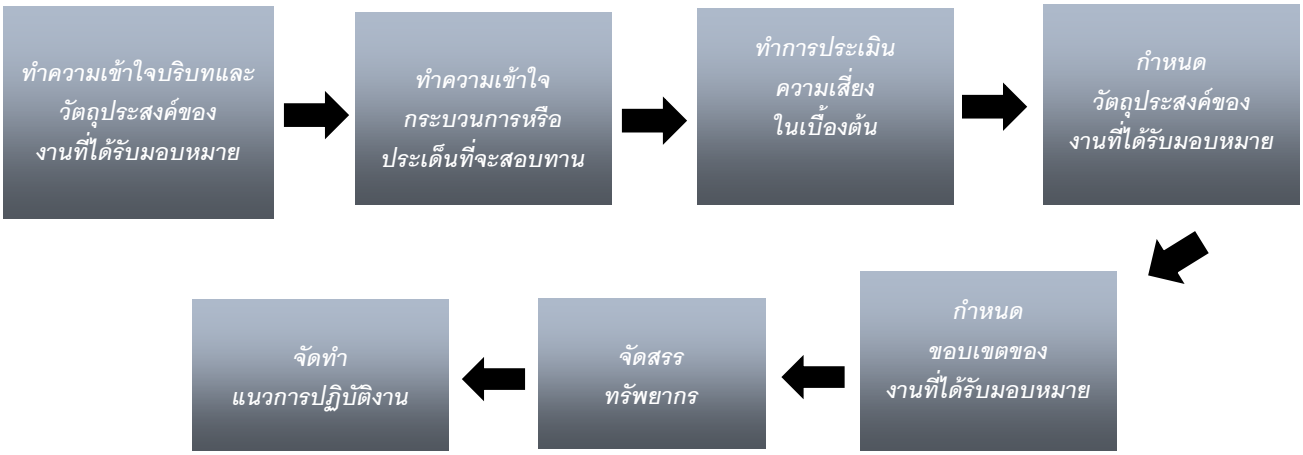
การวางแผนงานเพื่อประเมินโครงการภัยคุกคามจากภายใน

ตามมาตรฐาน 2200 - การวางแผนงานที่ได้รับมอบหมายกำหนดไว้ว่า ผู้ตรวจสอบภายในต้องจัดทำและจดบันทึกแผนสำหรับแต่ละงานที่ได้รับมอบหมาย มาตรฐาน 2201 – ข้อพิจารณาในการวางแผน ได้เสริมไว้ว่า ผู้ตรวจสอบภายในต้องพิจารณาถึง

- กลยุทธ์และวัตถุประสงค์ของงานที่จะสอบทานและวิธีการที่จะควบคุมการปฏิบัติงานนั้น
- ความเสี่ยงที่มีนัยสำคัญต่อ วัตถุประสงค์ ทรัพยากร และการดำเนินงานของกิจกรรมนั้น ตลอดจนหนทางที่จะใช้ในการจัดการกับผลกระทบที่อาจเกิดจากความเสี่ยงนั้น ให้อยู่ในระดับที่ยอมรับได้ความเพียงพอและความมีประสิทธิผลของกระบวนการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมของกิจกรรมนั้นเมื่อเปรียบเทียบกับกรอบ หรือต้นแบบ ที่เกี่ยวข้อง
- โอกาสที่จะปรับปรุงกระบวนการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมสำหรับกิจกรรมนั้นได้อย่างมีนัยสำคัญ

การวางแผนงานที่ได้รับมอบหมายโดยทั่วไปแล้วจะรวมถึงขั้นตอนต่าง ๆ ดังที่แสดงใน **ภาพที่** 4 ซึ่งจะช่วยให้ผู้ตรวจสอบภายในเข้าใจถึงประเด็นและกระบวนการที่จะได้รับการสอบทาน และบันทึกเอกสารข้อมูลที่จะสนับสนุนการวางแผนและแนวการปฏิบัติงานที่ได้รับมอบหมาย เนื่องจากการสอบทานและการจัดทำเอกสารบันทึกข้อมูลต่าง ๆ เป็นงานต่อเนื่องและกระทำในขณะปฏิบัติงาน ขั้นตอนที่แสดงอาจจะไม่ชัดเจนและเป็นเชิงเส้นตรง

ภาพที่ 4: **ขั้นตอนการวางแผนการตรวจสอบภายในที่ได้รับมอบหมาย**



หมายเหตุ: ขั้นตอนที่ระบุในภาพที่ 4 นี้มีรายละเอียดเพิ่มเติมในแนวปฏิบัติ (Practice Guide) อื่นๆ ที่ออกโดย IIA (ดูภาคผนวก ก)

การทำความเข้าใจบริบทและเป้าประสงค์ของงานที่ได้รับมอบหมาย

ขั้นตอนนี้มีความจำเป็นเพื่อที่จะทำให้แน่ใจว่าเป้าหมายและวัตถุประสงค์ที่ระบุไว้ในแผนการตรวจสอบภายในถูกทำให้บรรลุผลรวมทั้งความคาดหวังของผู้มีส่วนได้เสียได้ถูกรวมไว้อย่างเหมาะสมในแผนการทำงานที่ได้รับมอบหมาย สำหรับงานที่ได้รับมอบหมายอย่างเร่งด่วนหรืองานที่ได้รับการร้องขอจากผู้บริหารระดับสูงหรือคณะกรรมการหลังจากมีการเปลี่ยนแปลงที่สำคัญ ในทางธุรกิจหรือสภาพแวดล้อมทางเทคโนโลยี ขั้นตอนนี้มีความสำคัญยิ่งในอันที่จะทำให้ผู้ตรวจสอบภายในมั่นใจได้ว่ามีความเข้าใจอย่างถ่องแท้ถึงความคาดหวังของผู้บริหารระดับสูง ยกตัวอย่างเช่น หลังจากการควบรวมกิจการ ผู้บริหารระดับสูงอาจจะต้องการรู้ว่ามีความเสี่ยงอะไรใหม่ๆ ที่มาพร้อมกับการรวมองค์กร อีกทั้งความเสี่ยงเหล่านั้นได้ถูกนำไปจัดการภายใต้โครงการภัยคุกคามจากภายในที่มีอยู่หรือไม่

การทำความเข้าใจกระบวนการหรือประเด็นที่กำลังสอบทาน

มีสองสิ่งสำคัญที่ผู้ตรวจสอบภายในจะต้องมีความเข้าใจอย่างชัดเจนเมื่อวางแผนงานที่ได้รับมอบหมายในการประเมินว่าองค์กรมีการจัดการกับความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายในได้ดีเพียงใดสิ่งแรกที่ผู้ตรวจสอบภายในควรจะต้องเข้าใจคือลักษณะพื้นฐานของภัยคุกคามจากภายในและการปฏิบัติที่อาจถูกนำไปใช้ในการระบุ ป้องกัน ตรวจหา ตอบสนองและกู้คืนจากเหตุการณ์ความมั่นคงปลอดภัยด้านITในการหาความรู้เหล่านี้ผู้ตรวจสอบภายในอาจนำกรอบปฏิบัติ โปรแกรม และข้อเสนอแนะด้านความมั่นคงปลอดภัยที่มีอยู่แล้วมาพิจารณา ในภาคผนวก จ ได้แสดงรายชื่อของแหล่งข้อมูลที่ได้ให้คำแนะนำและความช่วยเหลือเกี่ยวกับเรื่องความมั่นคงปลอดภัยของข้อมูลไว้ และในภาคผนวกFยังได้ให้แหล่งข้อมูลเพิ่มเติมไว้อีก ผู้ตรวจสอบภายในอาจจะเริ่มจากข้อมูลเหล่านี้แต่ควรจะมีการระบุเจาะจงถึงกรอบปฏิบัติและข้อเสนอแนะที่สามารถนำมาใช้ได้อย่างเหมาะสมกับประเภทของอุตสาหกรรม ตลาด และลักษณะทางภูมิศาสตร์ที่องค์กรดำเนินกิจการอยู่

ความเสี่ยงด้านทุจริต

เนื่องจากการทุจริตเป็นหนึ่งในความเสี่ยงที่สำคัญเกี่ยวข้องกับภัยคุกคามจากภายใน ดังนั้นจึงมีความสำคัญที่จะได้ข้อมูลเกี่ยวกับการกล่าวหาการทุจริต เหตุการณ์ที่เกิดขึ้นและการสอบสวน

สำหรับรายละเอียดคำแนะนำในการรวมความเสี่ยงด้านทุจริตไปในการวางแผนงานที่ได้รับมอบหมายนั้นให้ดูแนวปฏิบัติของ IIA “การวางแผนงานที่ได้รับมอบหมาย” การประเมินความเสี่ยงด้านทุจริต

นอกจากนี้ผู้ตรวจสอบภายในควรมีความเข้าใจในองค์กรและวัตถุประสงค์ขององค์กร การเข้าใจถึงวัตถุประสงค์ทางธุรกิจจะเป็นพื้นฐานให้ผู้ตรวจสอบภายในสามารถจะระบุความเสี่ยงที่ควรจะถูกรวมไว้ในการประเมินความเสี่ยงเบื้องต้นของงานที่ได้รับมอบหมาย(ตามที่ระบุไว้ในมาตรฐาน 2210.A1).

การบริหารจัดการภัยคุกคามจากภายใน

ภัยคุกคามจากภายในไม่สามารถจะกำจัดได้อย่างสิ้นซากแต่จะสามารถถูกบริหารจัดการให้มีการป้องกันหรือลดผลกระทบที่มีนัยสำคัญได้ โครงการภัยคุกคามจากภายในคือการรวมกันของนโยบาย ขั้นตอนการปฏิบัติและการควบคุมในอันที่จะระบุ ป้องกัน ตรวจหา ตอบสนองและกู้คืนจากเหตุการณ์ความมั่นคงปลอดภัยด้าน IT

เป้าประสงค์เบื้องต้นในการนำโครงการภัยคุกคามจากภายในมาปฏิบัติก็เพื่อป้องกันทรัพย์สินที่สำคัญทั้งทางกายภาพและในระบบ รวมถึงบุคลากร อุปกรณ์เครื่องมือ ที่ทำงาน ระบบและข้อมูล การที่จะพยายามป้องกันทรัพย์สินทุกอย่างขององค์กรเป็นเรื่องยากและมีค่าใช้จ่ายที่สูงดังนั้นจึงมีความสำคัญที่จะเริ่มจากการระบุและจำแนกประเภทของทรัพย์สินที่มีความสำคัญก่อน

การพัฒนาโครงการภัยคุกคามจากภายใน

สิ่งหนึ่งที่สำคัญในกระบวนการจัดการกับภัยคุกคามจากภายในให้ประสบผลสำเร็จคือการร่วมมือกันระหว่างหลายส่วนงานที่มีหน้าที่ในการควบคุม (เช่นผู้บริหารระดับสูงและคณะกรรมการ)และคนที่เกี่ยวข้องในการนำโครงการไปปฏิบัติเช่นฝ่ายทรัพยากรบุคคล กฎหมาย ปฏิบัติการ เจ้าของข้อมูล ความมั่นคงปลอดภัยของข้อมูลและวิศวกรรมซอฟท์แวร์เป็นต้น

การกล่าวถึงถึงปัจจัยด้านบุคลากร
โครงการภัยคุกคามจากภายในที่มีประสิทธิภาพนั้นมีการพิจารณาถึงการควบคุมด้านบุคลากรและเทคโนโลยี การกำกับดูแลด้าน ITที่เข้มแข็งและโครงการบริหารความเสี่ยงทั่วทั้งองค์กรสามารถเป็นพื้นฐานในการจัดการและควบคุมปัจจัยด้านบุคลากร

เพื่อเพิ่มโอกาสของความสำเร็จองค์กรควรจัดให้มีโครงการที่ชัดเจนจัดการพัฒนาและนำไปปฏิบัติอย่างเป็นระบบ (เหมือนกับโครงการอื่น) ที่มีการทำเป็นเอกสารอย่างชัดเจนในเรื่องความคาดหวังบทบาทหน้าที่และความรับผิดชอบระยะเวลาและกิจกรรม ซึ่งการมีโครงการหรือแผนงานที่ชัดเจนจะช่วยให้องค์กรสามารถระบุสภาพการณ์ปัจจุบัน(การวิเคราะห์ช่องโหว่)และกำหนดทรัพยากรที่ต้องการในการทำโครงการให้สำเร็จ(เช่น บุคลากร เงิน เวลาและเทคโนโลยี)สิ่งหนึ่งที่สำคัญในกระบวนการจัดการกับภัยคุกคามจากภายในให้ประสบผลสำเร็จคือการร่วมมือกันระหว่างหลายส่วนที่มีหน้าที่ในการควบคุม(เช่นผู้บริหารระดับสูงและคณะกรรมการ)และคนที่เกี่ยวข้องในการนำโครงการไปปฏิบัติเช่นฝ่ายทรัพยากรบุคคล กฎหมาย ปฏิบัติการ เจ้าของข้อมูล ความมั่นคงปลอดภัยของข้อมูลและวิศวกรรมซอฟท์แวร์เป็นต้น

องค์กรสามารถใช้ประโยชน์จากกรอบปฏิบัติในการจัดการภัยคุกคามจากภายในที่มีอยู่แล้วจากภาคเอกชน ภาครัฐและองค์กรที่ไม่แสวงหากำไรในการนำมาประยุกต์ใช้ให้เหมาะสมกับความต้องการที่เฉพาะเจาะจงขององค์กรซึ่งดีกว่าการเริ่มต้นจากไม่มีอะไรเลย โดยการทำเช่นนี้องค์กรสามารถพัฒนาและนำโครงการภัยคุกคามจากภายในไปปฏิบัติได้เร็วขึ้น

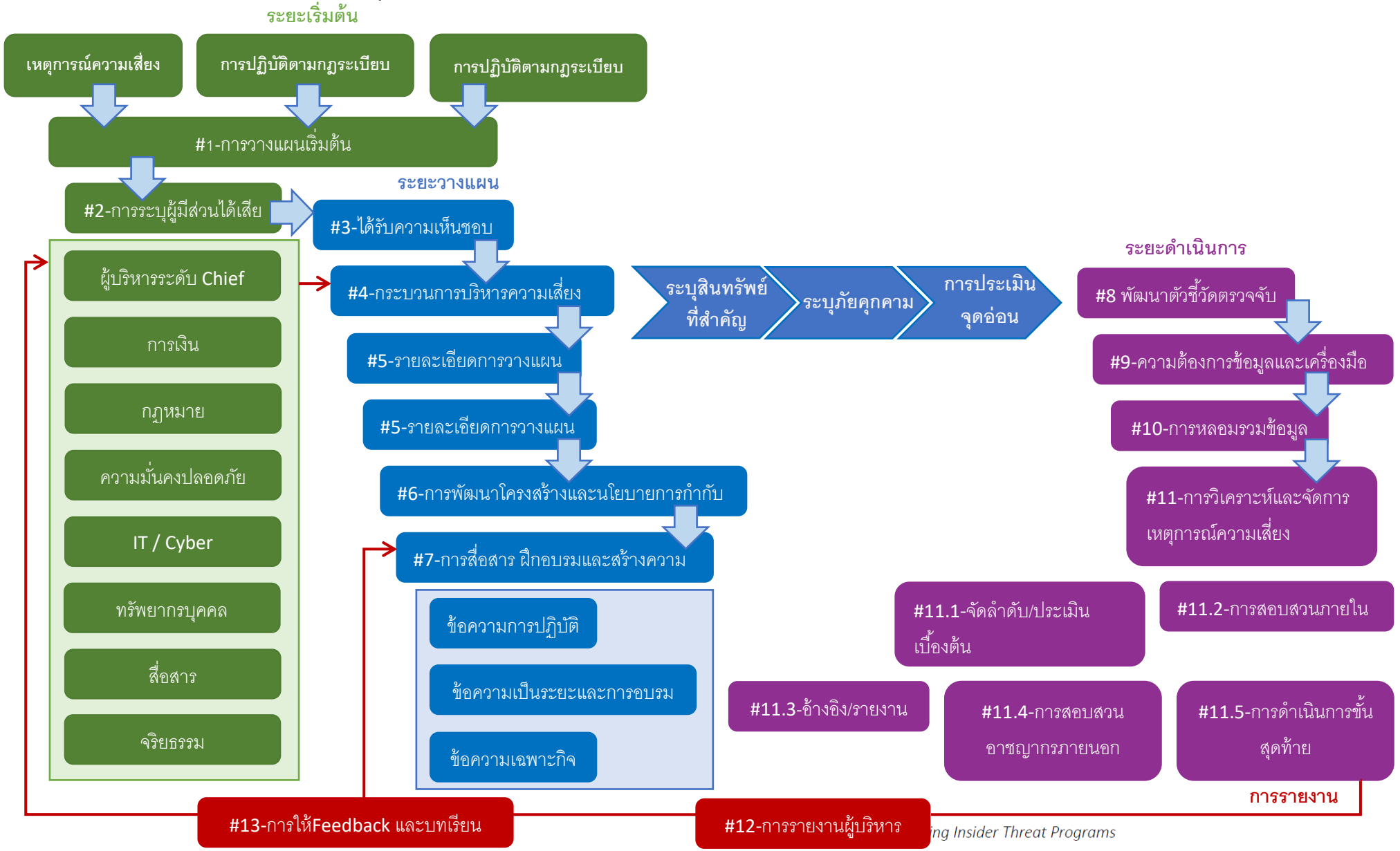
ตัวอย่างของกรอบปฏิบัติซึ่งสามารถถูกนำไปใช้ในการพัฒนาโครงการภัยคุกคามจากภายในได้รวมถึง

- NIST" กรอบปฏิบัติสำหรับการปรับปรุงความมั่นคงปลอดภัยพื้นฐานทางไซเบอร์ที่สำคัญ" (แสดงในภาคผนวก C)ซึ่งได้ให้ชุดของกิจกรรมในการระบุ ป้องกัน ตรวจหา ตอบสนองและกู้คืนจากการโจมตีทางไซเบอร์กรอบปฏิบัตินี้ถูกพัฒนาขึ้นมาด้วยเป้าประสงค์หลักเพื่อช่วยองค์กรทั้งหลายในการจัดการโครงการด้านความมั่นคงปลอดภัยทางไซเบอร์ซึ่งอย่างไรก็ตามกิจกรรมเหล่านี้สามารถนำมาใช้กับการจัดการภัยคุกคามจากภายในได้ด้วย

กรอบปฏิบัติที่ใช้ในการตรวจสอบภายใน
ผู้ตรวจสอบภายในสามารถใช้กรอบปฏิบัติที่เหมือนกันนี้เป็นส่วนหนึ่งในหลักเกณฑ์ที่จะประเมินศักยภาพของโครงการภัยคุกคามจากภายในขององค์กรระหว่างการปฏิบัติงานที่ได้รับมอบหมายทั้งงานที่ให้ความเชื่อมั่นและงานให้คำปรึกษา

- แนวทางพื้นฐานในการจัดการภัยคุกคามจากภายในซึ่งเผยแพร่โดยมหาวิทยาลัย Carnegie Mellon ตามที่แสดงในภาคผนวก D ซึ่งได้ให้คำแนะนำ 20 ข้อในการปฏิบัติเพื่อช่วยให้องค์กรสามารถพัฒนาโครงการภัยคุกคามจากภายในและบรรเทา(สกัดกั้น ตรวจหาและตอบสนอง)การคุกคามจากภายในได้
- The U.S. Intelligence and National Security Alliance(INSA)"การศึกษาเกี่ยวการระบุและต่อต้านภัยคุกคามจากภายใน"ซึ่งได้ให้แผนงาน13ขั้นตอน (หรือองค์ประกอบที่สำคัญ)ในการพัฒนาปฏิบัติและติดตามโครงการภัยคุกคามจากภายในตามที่แสดงในตารางที่ 5

ตารางที่ 5 INSA แผนโครงการภัยคุกคามจากภายใน



ที่มา: U.S. Intelligence and National Security Alliance in partnership with DHS, FBI, and ODNI, Insider Threat Program Roadmap, https://www.insaonline.org/insider-threat-roadmap/. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

ระยะเริ่มต้น

ในระยะนี้องค์กรจะระบุถึงความจำเป็นที่ต้องมีโครงการภัยคุกคามจากภายใน ระบุขอบเขตของโครงการและระบุผู้มีส่วนได้ส่วนเสียหลัก คำถามต่างๆ ที่อาจจะช่วยให้องค์กรระบุและจัดลำดับความสำคัญของการป้องกันสินทรัพย์ที่มีความสำคัญได้แก่:

- อะไรคือสินทรัพย์สำคัญที่เรามีอยู่
- เรารู้ถึงสภานะในปัจจุบันของสินทรัพย์ที่มีความสำคัญหรือไม่
- เราเข้าใจถึงความสำคัญของสินทรัพย์แต่ละชิ้นที่มีความสำคัญหรือไม่ และเราสามารถอธิบายได้หรือไม่ว่าอะไรคือเหตุผลที่สินทรัพย์เหล่านั้นมีความสำคัญกับองค์กร
- เราสามารถจัดลำดับความสำคัญของรายการสินทรัพย์ที่จำเป็นหรือไม่
- เรามีอำนาจหน้าที่ เงิน และทรัพยากรที่จะดูแลเฝ้าระวังสินทรัพย์ที่สำคัญของเราอย่างมีประสิทธิผลหรือไม่

ระยะวางแผน

ระยะวางแผนโดยมากจะเริ่มต้นจากการได้รับความสนับสนุนจากผู้บริหารระดับสูง และระบุถึงสินทรัพย์ที่จะต้องได้รับการปกป้อง ขั้นตอนบางอย่างที่องค์กรอาจจะต้องทำในระยะนี้เพื่อให้การวางแผนเสร็จสมบูรณ์ ได้แก่:

- ระบุระบบและสินทรัพย์ทางดิจิทัล
- ระบุข้อกำหนดในทางกฎหมายที่เกี่ยวข้อง
- ประเมินความเสี่ยง
- พัฒนาแผนการปฏิบัติงานที่เป็นทางการ
- สร้าง (ถ้าจำเป็น) โครงสร้างและนโยบายการกำกับดูแล
- พัฒนาแผนการสื่อสารฝึกอบรมและการรายงาน

ระยะดำเนินการ

ในระยะนี้องค์กรวิเคราะห์ความต้องการช่องโหว่ และจัดลำดับกิจกรรมที่จะจัดการกับสิ่งเหล่านั้น กิจกรรมพื้นฐานที่มักจะเกิดขึ้นในระยะนี้รวมถึง

- การวิเคราะห์ต้นทุนกับผลประโยชน์
- พัฒนาข้อมูลประวัติภัยคุกคามจากภายใน
- ระบุและนำการควบคุมที่สำคัญไปปฏิบัติในการจัดการกับภัยคุกคามจากภายใน (ตัวอย่างของการควบคุมทั่วไปเรื่องความมั่นคงปลอดภัยด้านอยู่ในภาพที่ 6)
- พัฒนาตัวชี้วัดการทำงานที่สำคัญ
- จัดให้มีกระบวนการจัดการกับเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทาง IT

ภาพที่ 6: วิธีการควบคุมด้านความมั่นคงปลอดภัยทาง IT

ทางการบริหาร	ทางกายภาพ	ทางเทคนิค
นโยบายและวิธีการปฏิบัติงาน	อุปกรณ์ดับเพลิงการให้ความร้อน	การเข้ารหัส
นโยบายด้านบุคลากร	การระบายอากาศและการปรับ	เครือข่ายส่วนบุคคลเสมือน (VPNs)
นโยบายด้านรหัสผ่าน	อากาศ	Demilitarized zone (DMZ)
ข้อตกลงกำหนดเวลา/ระดับการให้บริการ	การป้องกันภาวะแม่เหล็กไฟฟ้า	Firewalls
การสร้างการรับรู้และฝึกอบรมเกี่ยวกับการรักษา	(EMI)	Access Control lists
ความปลอดภัย	การเฝ้าระวังด้านสภาพแวดล้อม	Proxy servers
การจัดการกับความเปลี่ยนแปลง	การเฝ้าระวังโดยใช้ Video	การแปลงค่า address เครือข่าย
การบริหารจัดการ Configuration	รั้ว ประตูและกำแพง	การตรวจหา/ป้องกัน การบุกรุก (IDS/IPS)
การบริหารจัดการ Patch	แสงสว่าง	Honeypots
ขั้นตอนปฏิบัติ การเก็บข้อมูลสำคัญ การสำรอง	บัตรผ่านเข้าออก	การจัดแบ่งกลุ่มของเครือข่าย
ข้อมูลและการฟื้นคืนสู่สภาวะปกติ	ยาม	
	ล๊อค ประตูหมุน mantraps	

ที่มา: CERT, Model – Driven Insider Threat Control Selection and Deployment

ระยะการรายงาน

การเฝ้าระวังติดตามและรายงานเป็นสิ่งสำคัญมากที่จะทำให้แน่ใจว่า องค์กรได้จัดการกับความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายในเมื่อสภาพแวดล้อมทั้งภายในและภายนอกเปลี่ยนไป องค์กรสามารถนำขั้นตอนในการวางแผนการปฏิบัติงานมาทำซ้ำได้ตามที่ต้องการ ซึ่งถือเป็นส่วนหนึ่งของแนวทางการปรับปรุงอย่างต่อเนื่อง

ข้อพิจารณาทางกฎหมาย

การควบคุมติดตามพนักงานเป็นสิ่งที่สำคัญในการจัดการกับภัยคุกคามจากภายใน แต่การกระทำเช่นนั้นสามารถทำให้องค์กรมีความเสี่ยงทางด้านกฎหมายที่เกี่ยวข้องทั้งกฎหมายระดับรัฐประเทศและระหว่างประเทศอันเกี่ยวกับเรื่องข้อมูลส่วนบุคคล ตัวอย่างคือ กฎหมายเรื่องการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรปที่มีจุดมุ่งหมายในการปกป้องข้อมูลส่วนบุคคลของทุกคนที่อาศัยอยู่ในยุโรป เพื่อที่จะจัดการกับความเสี่ยงประเภทนี้ จำเป็นต้องประสานกับหน่วยงานกฎหมายและ HR ได้มีการคำนึงถึงสิทธิของพนักงานแล้ว เมื่อพิจารณาถึงวิธีปฏิบัติในการเฝ้าระวังติดตาม

ข้อมูลในการวางแผนงานที่ได้รับมอบหมาย

สิ่งที่ผู้ตรวจสอบภายในควรต้องทำเพื่อให้เข้าใจถึงโครงการภัยคุกคามจากภายในขององค์กรนั้น ได้แก่

การสอบทานเอกสาร

- สอบทานแผนทางธุรกิจในปัจจุบันและผลการประเมินความเสี่ยงสอบทานการประเมินก่อนหน้านี้ (ทั้งภายในและภายนอก)
- สอบทานผังองค์กรเพื่อที่จะระบุผู้มีส่วนได้เสียที่เกี่ยวข้อง

- สอบทานนโยบายและวิธีการปฏิบัติงานที่เกี่ยวกับการบริหารจัดการผู้ใช้งาน การบริหารจัดการการเข้าถึง การบริหารจัดการและการเข้าถึงจากทางไกล (เช่นผู้ขาย) และคู่มือการจัดการเปลี่ยนแปลงควบคุมค่าของระบบ
- สอบทานรายการทะเบียนสินทรัพย์และข้อมูลเพื่อที่จะระบุระบบและข้อมูลที่สำคัญขององค์กร
- สอบทานรายการควบคุมการเข้าออก (access control lists) และ firewall ซึ่งจำกัดการเข้าถึงสู่ระบบและข้อมูลที่มีความสำคัญของเครือข่ายภายใน
- ระบุและสอบทานกฎหมายและกฎระเบียบที่ใช้บังคับ ซึ่งจะส่งผลต่อบริบทของการตรวจสอบภายใน

การสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง

ผู้ตรวจสอบภายในควรมีการรวบรวมข้อมูลโดยอาจได้จากการสัมภาษณ์พนักงานที่ทำหน้าที่งานอันเกี่ยวข้องกับโครงการภัยคุกคามจากภายใน รวมทั้งผู้บริหารที่ทำหน้าที่กำกับดูแล และผู้มีอำนาจในการตัดสินใจ ผู้มีส่วนได้เสียบางกลุ่มที่ควรรวมอยู่ในรายการที่จะสัมภาษณ์ได้แสดงไว้ใน ภาพที่ 7

ข้อพิจารณาในการตรวจสอบ

วิธีปฏิบัติ 20 ข้อของ CERT ได้แสดงไว้ในภาคผนวก ง ซึ่งสามารถนำไปใช้ในการพัฒนาแบบสอบถามการควบคุมภายใน (ICQ) เพื่อที่จะรวบรวมข้อมูลเกี่ยวกับกิจกรรมการควบคุม ในระหว่างการวางแผนงานที่ได้รับมอบหมาย หรือเพื่อสร้างคำถามเพื่อสัมภาษณ์ผู้มีส่วนได้เสีย

ภาพที่ 7: ผู้มีส่วนได้เสียในโครงการภัยคุกคามจากภายใน

ผู้มีส่วนได้เสียด้านธุรกิจ	ผู้มีส่วนได้เสียด้าน IT
ผู้บริหารระดับสูง (C-Level)	เทคโนโลยีสารสนเทศ (CIO/CTO)
ความมั่นคงปลอดภัย (ด้านกายภาพ บุคลากรและข้อมูล)	ผู้ออกแบบข้อมูล (หรือหน่วยงาน)
ทรัพยากรบุคคล (HR)	ผู้ออกแบบระบบเครือข่าย
กฎหมาย/ความเป็นส่วนตัว	ผู้เชี่ยวชาญการให้ความเชื่อมั่นด้านสารสนเทศ
จริยธรรมและการกำกับดูแล	ผู้เชี่ยวชาญการสอบสวนความมั่นคงปลอดภัยทาง IT
การจัดหา/การทำสัญญาจ้าง/การจัดซื้อ	ปฏิบัติการด้าน IT
หน่วยงานทางธุรกิจที่สำคัญ (การผลิต บริการ เจ้าของข้อมูล คู่ค้าทางธุรกิจที่ไว้ใจได้ตามความเหมาะสม)	การพัฒนาซอฟต์แวร์
สื่อสารองค์กร	ทีมตอบสนองต่อเหตุการณ์ความเสี่ยงด้านคอมพิวเตอร์ (CIRT)

ผู้ตรวจสอบภายในอาจเป็นผู้นำในการระดมสมองร่วมกันกับผู้มีส่วนได้เสีย ไม่ว่าจะเป็นส่วนหนึ่งของการสัมภาษณ์ หรือจัดให้มีการระดมสมองแยกไปต่างหาก เพื่อระบุความเสี่ยงที่มีอยู่ตามธรรมชาติก่อนได้รับการจัดการ โดยหลังจากนั้น สามารถนำผลจากการระดม

ก้าวนำหน้าภัยคุกคาม

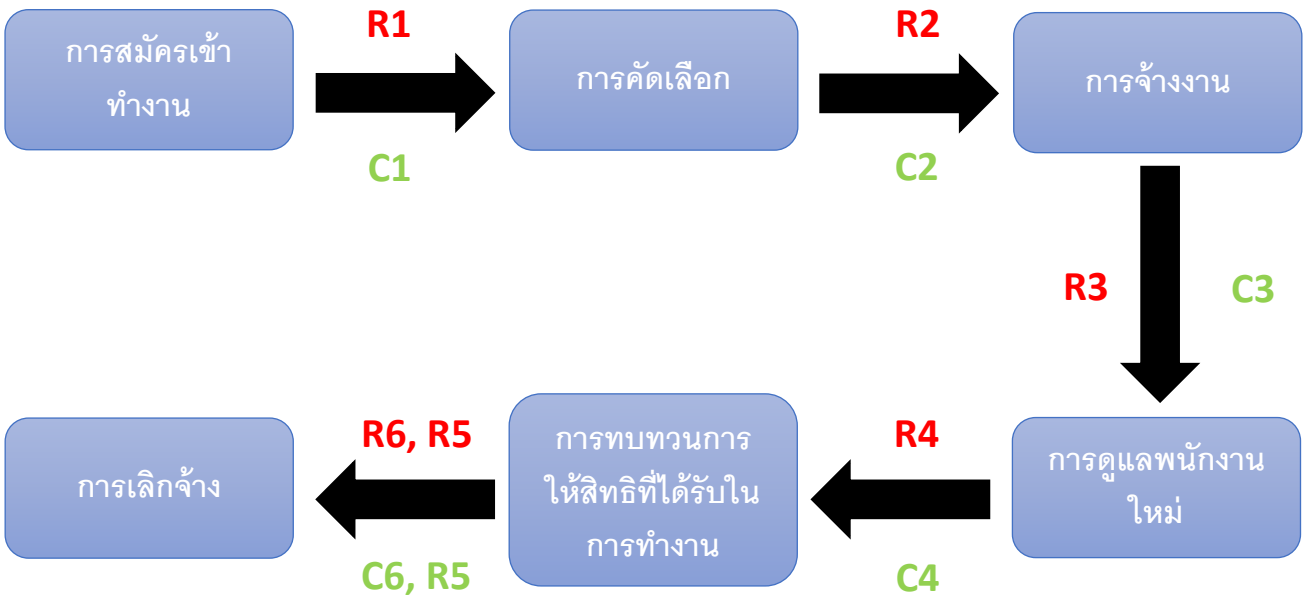
เนื่องจากสภาพการณ์ด้านภัยคุกคามนั้นเปลี่ยนแปลงอย่างรวดเร็ว ผู้ตรวจสอบภายในควรหมั่นหาความรู้เพิ่มเติมอยู่เสมอซึ่งหาได้จากแหล่งข้อมูลที่ระบุไว้ในภาคผนวก ค ถึง จ

สมองที่ได้มาใช้เป็นข้อมูลในการประเมินความเสี่ยงในเชิงลึก เพื่อที่จะกำหนดระดับความเสี่ยงหลังจากได้รับการจัดการและจัดลำดับของความเสี่ยงตามความมีนัยสำคัญ

การทำแผนผังทางเดินของกระบวนการหรือกระบวนการย่อย

วิธีการหนึ่งในการระบุความเสี่ยงและวิธีการควบคุมคือ การจัดทำแผนผังกระบวนการในภาพรวม ซึ่งแสดงให้เห็นถึงข้อมูลนำเข้า ข้อมูลออก การเชื่อมต่อกัน และวิธีการควบคุมต่างๆ การทำแผนผังโครงการภัยคุกคามจากภายในทั้งหมดอาจเป็นเรื่องยาก แต่ผู้ตรวจสอบภายในสามารถเน้นที่กระบวนการที่มีความเสี่ยงสูงก่อนได้ ยกตัวอย่างเช่น เพื่อทำความเข้าใจความเสี่ยงและวิธีการควบคุมที่สำคัญ ผู้ตรวจสอบภายในอาจจะทำแผนผังกระบวนการจัดการบุคลากร การบริหารจัดการผู้ขาย การควบรวมกิจการ การจัดการอัตลักษณ์และการควบคุมการเข้าถึง และการจัดประเภทและลำดับความสำคัญของสินทรัพย์ โดยใน **ภาพที่** 8 นี้ได้ให้ตัวอย่างของแผนผังกระบวนการในภาพรวม

ภาพที่ 8: **ตัวอย่างของแผนผังกระบวนการในภาพรวมของการจัดการบุคลากร**



กระบวนการย่อย	ความเสี่ยง	การควบคุม
การสมัครเข้าทำงาน	R1: มีการจ้างพนักงานจากคู่แข่งที่สำคัญอันเป็นการเพิ่มโอกาสของการถูกขโมยสินทรัพย์ทางปัญญาและสูญเสียความสามารถในการแข่งขัน	C1: มีการประเมินและคัดกรองประวัติการทำงานของผู้สมัครเพื่อที่จะดูว่ามีความเสี่ยงที่จะก่อให้เกิดการคุกคามหรือไม่
การคัดเลือก	R2: มีการจ้างพนักงานที่มีประวัติอาชญากรรมอันเป็นการเพิ่มโอกาสของการทุจริต	C2: มีการตรวจสอบประวัติอาชญากรรมและการเงินตามที่ไม่ขัดกับกฎหมายความเป็นส่วนตัว
การจ้างงาน	R3: มีการจ้างพนักงานจากองค์กรคู่แข่งหลักมาทำงานในตำแหน่งที่ต้องดูแลข้อมูลที่มีความสำคัญ	C3: พนักงานต้องมีการแจ้งเรื่องผลประโยชน์ทับซ้อนในระหว่างกระบวนการจ้างงานและทุก ๆ 12 เดือนหลังจากนั้น
การดูแลพนักงานใหม่	R4: กระบวนการดูแลพนักงานใหม่ไม่ได้มีการอบรมให้ตระหนักรู้เกี่ยวกับภัยคุกคามจากภายในและเกณฑ์วิธีในการการจัดการกับปัญหาเหตุการณ์ความเสี่ยงด้าน IT ที่อาจเกิดขึ้นได้	C4: พนักงานทุกคนต้องเข้ารับการอบรมตระหนักรู้โดยถือเป็นส่วนหนึ่งของกระบวนการดูแลพนักงานใหม่การให้สิทธิในการเข้าถึงระบบเครือข่ายจะให้ก็ต่อเมื่อได้ผ่านการอบรมภาคบังคับมาครบถ้วน
การทบทวนการให้สิทธิที่ได้รับในการทำงาน	R5: พนักงานไม่ได้รับการทบทวนสิทธิที่ได้รับเมื่อมีการเปลี่ยนตำแหน่งงานในองค์กรทำให้เกิดการได้รับสิทธิในการเข้าถึงระบบโดยไม่จำเป็น	C5: มีการสอบทานสิทธิการเข้าถึงของพนักงานอย่างน้อยทุกๆ 6 เดือนหรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน สิทธิการเข้าถึงจะถูกตัดโดยอัตโนมัติถ้าไม่ได้มีการรับรองการได้สิทธิที่มีอยู่อย่างเหมาะสม
การเลิกจ้าง	R6: องค์กรไม่ได้มีการตัดสิทธิการเข้าถึงระบบโดยทันทีเมื่อมีการเลิกจ้างพนักงาน	C6: หน่วยงานทรัพยากรบุคคลมีการแจ้ง help desk ในทันทีที่มีการลาออกหรือเลิกจ้างโดย help desk จะทำการยกเลิกสิทธิในการเข้าถึงระบบที่เกี่ยวข้องทั้งหมด

การดำเนินการประเมินความเสี่ยงในเบื้องต้น

เนื่องจากข้อจำกัดด้านเวลาและทรัพยากรจึงทำให้ไม่สามารถสอบทานความเสี่ยงทั้งหมดได้ในระหว่างการปฏิบัติงานที่ได้รับมอบหมาย ดังนั้น ผู้ตรวจสอบภายในจะต้องทำการประเมินความเสี่ยงในเบื้องต้นและจัดลำดับของความเสี่ยงตามระดับความสำคัญซึ่งจะถูกวัดได้จากปัจจัยความเสี่ยงต่างๆ ที่ประกอบกันในภาพที่ 9 แสดงให้เห็นถึงการประเมินความเสี่ยงของภัยคุกคามจากภายในที่พบเห็นกันได้ทั่วไป

ภาพที่ 9: ตัวอย่างของภัยคุกคามจากภายในและผลของความเสี่ยง

ภัยคุกคาม	ความเสี่ยง	ผลกระทบที่อาจเกิดขึ้นได้
การทุจริต	คนภายในองค์กรใช้ IT ในการเปลี่ยนแปลง เพิ่มเติม หรือลบข้อมูลขององค์กร โดยไม่ได้รับอนุญาตเพื่อผลประโยชน์ส่วนตน	สูญเสียความไว้ใจจากผู้ถือหุ้นอันเป็นผลมาจากรายงานทางการเงินไม่ถูกต้อง การเสื่อมเสียชื่อเสียง
การบ่อนทำลายทาง IT	คนภายในองค์กรใช้ระบบ IT เพื่อไปเจาะจงทำร้ายองค์กรหรือบุคคลโดยตรง	ระบบขัดข้องสูญเสียผลผลิต การปฏิเสธการให้บริการ
การขโมยสินทรัพย์ทางปัญญา	คนภายในองค์กรใช้ระบบ IT เพื่อขโมยสินทรัพย์ทางปัญญาขององค์กรซึ่งรวมถึง การจารกรรมทางอุตสาหกรรมที่เกี่ยวข้องกับคนภายในองค์กร	สูญเสียความได้เปรียบในทางการแข่งขัน สูญเสียรายได้ที่ควรได้
การขโมยหรือเปิดเผยข้อมูลความลับที่ละเอียดอ่อน/ที่สำคัญ	คนภายในองค์กรใช้ระบบ IT เพื่อขโมยข้อมูลความลับหรือข้อมูลส่วนตัวเพื่อผลประโยชน์ทางการเงิน	สูญเสียความไว้วางใจจากลูกค้า ความสูญเสียทางการเงินอันเนื่องมาจากการที่ต้องจ่ายเงินเยียวยาให้แก่ลูกค้า
การขโมยข้อมูลส่วนบุคคล	คนภายในองค์กรใช้ IT เพื่อขโมยหรือเปิดเผยข้อมูลส่วนบุคคล	สูญเสียความไว้วางใจจากลูกค้า ความสูญเสียทางการเงินอันเนื่องมาจากการจ่ายเงินเยียวยาให้แก่ลูกค้า ความสูญเสียทางการเงินอันเนื่องมาจากค่าใช้จ่ายเกี่ยวกับการดำเนินคดี
กิจกรรมที่ผิดกฎหมาย	คนภายในองค์กรใช้สินทรัพย์ดิจิทัลเพื่อผลประโยชน์ทางการเงินเช่น การส่ง spam mail หรือการเล่นการพนัน หรือกิจกรรมที่อาจไม่ถูกต้องตามธรรมนองคลองธรรมตามกฎหมาย	เสียชื่อเสียง ความสูญเสียทางการเงินอันเนื่องมาจากค่าใช้จ่ายเกี่ยวกับการดำเนินคดี

การกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย

วัตถุประสงค์ของงานที่ได้รับมอบหมายนั้นขึ้นอยู่กับบริบทและเป้าหมายของงานนั้น สำหรับการตรวจสอบการปฏิบัติตามกฎระเบียบ วัตถุประสงค์ก็จะได้มาจากข้อกำหนดของกฎระเบียบที่ต้องมีการสอบทานการปฏิบัติตาม สำหรับงานให้ความเชื่อมั่นที่ตั้งบนพื้นฐานของความเสี่ยงนั้น วัตถุประสงค์ก็จะขึ้นอยู่กับจุดมุ่งหมายในเบื้องต้นของงานนั้นและผลของการประเมินความเสี่ยง สำหรับงานให้คำปรึกษานั้นวัตถุประสงค์ก็จะต้องกล่าวถึงเรื่องกระบวนการกำกับดูแล การบริหารความเสี่ยง และกระบวนการควบคุมภายในขอบเขตที่ได้ตกลงไว้กับลูกค้าผู้รับบริการ (มาตรฐาน 2201.C1)

ความช่วยเหลือสำหรับเรื่องการวางแผนงานที่ได้รับมอบหมาย

รายละเอียดคำแนะนำในการจัดทำองค์ประกอบดังต่อไปนี้สามารถดูได้ในแนวปฏิบัติของ IIA เรื่อง "การวางแผนงานที่ได้รับมอบหมาย: การจัดทำวัตถุประสงค์และขอบเขต"

- สถานการณ์ความเสี่ยง
- ตาราง/แมทริกซ์ความเสี่ยงและการควบคุม
- ผังการจัดลำดับความสำคัญของความเสี่ยง เช่นผังระดับความเสี่ยง(heat maps)

ตัวอย่างวัตถุประสงค์ของงานที่ได้รับมอบหมาย

งานให้ความเชื่อมั่นด้าน (การปฏิบัติตามกฎระเบียบ) - งานนี้จะประเมินการปฏิบัติตาม General Data Protection Regulation (GDPR) ซึ่งกำหนดให้มีการปกป้องข้อมูลส่วนบุคคล (PII) ในตัวอย่างนี้เกณฑ์ที่ใช้ในการประเมินซึ่งกล่าวไว้ในมาตรฐาน 2210.A3 ก็คือเกณฑ์ข้อกำหนดเกี่ยวกับข้อมูลส่วนบุคคลและวิธีการควบคุมตามที่ระบุไว้ใน GDPR[5]

งานให้ความเชื่อมั่น (บนพื้นฐานของความเสี่ยง) - งานนี้จะประเมินความมีประสิทธิผลของโครงการบริหารจัดการภัยคุกคามจากภายในโดยการใช้กรอบการปรับปรุงโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญที่เผยแพร่โดย NIST ในตัวอย่างนี้ เกณฑ์ที่ใช้ในการประเมินซึ่งกล่าวไว้ในมาตรฐาน 2210. A3 คือ กรอบของ NIST ที่แสดงในภาคผนวก ค โดยถือเป็น แนวการปฏิบัติงานสำหรับงานที่ได้รับมอบหมาย

งานให้คำปรึกษา - งานนี้จะประเมินความมีประสิทธิผลของกระบวนการในการระบุและจัดประเภทสินทรัพย์ทางดิจิทัล หน่วยงานตรวจสอบภายในจะให้คำแนะนำว่าควรปรับปรุงกระบวนการอย่างไร (หากจำเป็น) ในตัวอย่างนี้ เกณฑ์ที่ใช้ในการประเมินซึ่งกล่าวไว้ในมาตรฐาน 2210. A3 นั้น จะถูกกำหนดโดยผู้มีส่วนได้เสียที่ขอให้มีการสอบทานนั่นเอง

[5] สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ GDPR ดูได้ที่ https://gdpr-info.eu.

การกำหนดขอบเขตของงานที่ได้รับมอบหมาย

ขอบเขตของงานที่ได้รับมอบหมายเป็นการระบุขอบเขตของงานและข้อมูลประวัติของสิ่งที่จะถูกรวมไปในการสอบทาน ขอบเขตของงานอาจจะเป็นการระบุองค์ประกอบบางอย่างเช่น กระบวนการเฉพาะบางกระบวนการหรือประเด็นบางประเด็น หรือพื้นที่ตั้งทางภูมิศาสตร์ และช่วงเวลา (เช่น ณ ขณะใดขณะหนึ่ง ไตรมาสของงบการเงิน หรือปีปฏิทิน) ซึ่งงานที่ได้รับมอบหมายจะครอบคลุม โดยใช้ทรัพยากรที่มีอยู่ในการดำเนินการ
เมื่อได้มีการจัดทำวัตถุประสงค์ของงานที่ได้รับมอบหมายแล้ว ผู้ตรวจสอบภายในต้องระบุขอบเขตที่พอเพียงต่อการบรรลุวัตถุประสงค์นั้น (มาตรฐาน 2220 –ขอบเขตของงานที่ได้รับมอบหมาย)โดยคำนึงถึง สิ่งต่างๆ ที่เกี่ยวข้อง ได้แก่ ระบบงาน การบันทึกข้อมูล บุคลากร และสินทรัพย์ที่จับต้องได้รวมทั้งสินทรัพย์ที่อยู่ในความควบคุมดูแลของกลุ่มบุคคลที่สาม (มาตรฐาน 2220. A1)

ตัวอย่างขอบเขตของงานที่ได้รับมอบหมาย

จากวัตถุประสงค์ของงานที่ได้รับมอบหมายซึ่งได้กำหนดไว้แล้วในหัวข้อก่อนหน้านี้นั้น ตัวอย่างขอบเขตของงานที่ได้รับมอบหมายมีดังนี้

งานให้ความเชื่อมั่น (การปฏิบัติตามกฎระเบียบ)-ขอบเขตของงานนี้จะรวมถึงสิ่งอำนวยความสะดวกทั้งหมด ระบบและกระบวนการที่ใช้ในการบริหารจัดการข้อมูลลูกค้าที่อาศัยอยู่ในสหภาพยุโรป

งานให้ความเชื่อมั่น (บนพื้นฐานของความเสี่ยง)-ขอบเขตของงานนี้จะจำกัดอยู่ที่การสอบทานเอกสารการออกแบบโครงการภัยคุกคามจากภายใน ณ ระดับองค์กร โครงการนี้ จะถูกประเมินโดยใช้กรอบการปรับปรุงโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญ ของ NIST

งานให้คำปรึกษา- ขอบเขตของงานนี้จะจำกัดอยู่ที่การสอบทานกระบวนการในการระบุและจัดประเภทของสินทรัพย์ทางดิจิทัลที่ได้นำไปใช้ปฏิบัติในหน่วยงานด้านวิศวกรรม

การจัดสรรทรัพยากร

ผู้ตรวจสอบภายในต้องมีการกำหนดทรัพยากรที่เพียงพอและเหมาะสมในการบรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายโดยตั้งอยู่บนการประเมินลักษณะและความซับซ้อนของงานแต่ละงาน ข้อจำกัดด้านเวลา และทรัพยากรที่มีอยู่ (มาตรฐาน 2230 - การจัดสรรทรัพยากรให้กับงานที่ได้รับมอบหมาย) .

ในบทตีความของมาตรฐานนี้ ได้อธิบายคำว่า เหมาะสม ไว้

ความสามารถของผู้ตรวจสอบภายใน
ทักษะที่ผู้ตรวจสอบภายในจะต้องมีอย่างน้อยที่สุดได้แก่ จะต้องมีความรู้ความเข้าใจใน 4 องค์ประกอบซึ่งเป็นภาคบังคับของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) อันได้แก่ หลักการที่สำคัญ คำจำกัดความของการตรวจสอบภายใน ประมวลจรรยาบรรณ และมาตรฐานสากลสาหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน

ว่าหมายถึง การผสมผสานกันของความรู้ ทักษะและความสามารถด้านอื่นที่จำเป็นในการปฏิบัติงาน คำว่าเพียงพอ หมายถึงจำนวนของทรัพยากรที่จำเป็นต้องใช้ในการทำงานที่ได้รับมอบหมายให้สำเร็จได้โดยใช้ความระมัดระวังในทางวิชาชีพอย่างเหมาะสม

ทักษะที่สำคัญที่สุดสำหรับผู้ตรวจสอบภายในในการประเมินโครงการภัยคุกคามจากภายในคือ ความรู้ด้านองค์กรและเป้าหมายทางกลยุทธ์ขององค์กร ภัยคุกคาม ความเสี่ยง ความเปราะบาง และผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรที่อาจเกิดขึ้นได้

อันเนื่องมาจากลักษณะในทางเทคนิคของวิธีการควบคุมบางอย่างที่ใช้ในการระบุ ป้องกัน ตรวจหา ตอบสนองและกอบกู้เหตุการณ์ความเสี่ยงด้านไอที จึงมีความจำเป็นที่จะต้องใช้ผู้ตรวจสอบภายในซึ่งมีความเข้าใจหลักการของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ถ้าองค์กรไม่มีผู้ตรวจสอบภายในที่มีความรู้ความสามารถที่จำเป็นแล้ว หัวหน้าหน่วยงานตรวจสอบภายในอาจต้องจัดหาทรัพยากรเพิ่มเติมด้วยการทำงานร่วมกันกับบุคลากรด้านไอทีขององค์กรในฐานะที่เป็นผู้เชี่ยวชาญเฉพาะด้านซึ่งสามารถช่วยให้ข้อมูลได้โดยไม่ทำให้ความสามารถของหน่วยงานตรวจสอบภายในในการให้ความเชื่อมั่นอย่างเที่ยงธรรมเสื่อมเสียลงได้

การจัดทำแนวการปฏิบัติงาน

แนวการปฏิบัติงานคือผลผลิตที่ได้จากขั้นตอนการวางแผนงานที่ได้รับมอบหมาย สำหรับงานให้ความเชื่อมั่นนั้น แนวการปฏิบัติงานควรระบุถึงวัตถุประสงค์ของงานที่ได้รับมอบหมาย ขอบเขต ความเสี่ยง วิธีกการควบคุม และวิธีการที่จะใช้ในการระบุ วิเคราะห์ ประเมิน และบันทึกเอกสารข้อมูล ในขณะปฏิบัติงานที่ได้รับมอบหมาย (มาตรฐาน 2240 – แนวการปฏิบัติงานที่ได้รับมอบหมาย และมาตรฐาน 2240.A1) สำหรับงานให้คำปรึกษานั้น แนวการปฏิบัติงานจะแตกต่างกันออกไปทั้งในรูปแบบและเนื้อหา ทั้งนี้ ขึ้นอยู่กับลักษณะของการปฏิบัติงาน (มาตรฐาน 2240.C1)

สำหรับเป้าหมายของการตรวจสอบโครงการภัยคุกคามจากภายในนั้น ใน**ภาพที่** 10 ได้แสดงรายการ กิจกรรมและวิธีการควบคุมซึ่งแนะนำให้ใช้ในการนำโครงการภัยคุกคามจากภายในไปปฏิบัติภายหลังจากที่ได้มีการจัดทำแผนงานของโครงการภัยคุกคามจากภายในตามที่ได้บรรยายไปแล้วในหัวข้อ ”การพัฒนาโครงการภัยคุกคามจากภายใน” กิจกรรมและวิธีการควบคุมได้มีการจัดทำให้สอดคล้องกับ วิธีปฏิบัติ 20 ข้อของ CERT(ในภาคผนวก ง) และคำจำกัดความของหน้าที่ของการควบคุมที่ให้ไว้ในกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่ถูกพัฒนาโดย NIST ซึ่งในภาคผนวก ค ได้แสดงให้เห็นถึงความสัมพันธ์ระหว่างกัน

รายการกิจกรรมและวิธีการควบคุมในการนำโครงการภัยคุกคามจากภายในไปปฏิบัตินั้น ไม่ได้ครอบคลุมรายการทั้งหมด แต่มุ่งหมายที่จะแสดงให้เห็นถึงการใช้ข้อมูลจากหลายๆ แหล่งที่มีอยู่ในการจัดทำแนวการปฏิบัติงานซึ่งเหมาะกับความต้องการขององค์กร องค์กรควรมีการพัฒนาโรดแมป ซึ่งมีความเหมาะสมตรงกับความต้องการของ

องค์กร โดยคำนึงถึงขนาด ประเภทของอุตสาหกรรม กฎระเบียบ สถานที่ตั้งทางภูมิศาสตร์ และปัจจัยอื่นๆ ที่เกี่ยวข้องในการระบุความเสี่ยงจากภายใน

นอกจากนี้ ในภาคผนวก ค ยังแสดงให้เห็นถึงแผนผังของวัตถุประสงค์การควบคุมและวิธีการควบคุม ตามกรอบความมั่นคงปลอดภัยทางไซเบอร์ที่ถูกพัฒนาโดย NIST กรอบนี้ควบคู่กับวิธีปฏิบัติ 20 ข้อของ CERT ที่มีอยู่ในภาคผนวก ง สามารถช่วยในจัดทำการประเมินความเสี่ยงที่เฉพาะเจาะจงขององค์กร ใช้ช่วยในการตัดสินใจเลือกวิธีการควบคุมที่ควรจะถูกทดสอบ และใช้ในการระบุวิธีการทดสอบที่จะนำไปใช้ในการประเมินความมีประสิทธิผลของวิธีการควบคุมเหล่านั้น สำหรับองค์กรที่มีโครงการภัยคุกคามจากภายในอยู่แล้ว ข้อมูลเหล่านี้สามารถนำไปใช้เป็นเกณฑ์ในการเปรียบเทียบ (benchmark) ผลการดำเนินการได้

ภาพที่ 10: กิจกรรมและการควบคุมที่สำคัญของโครงการภัยคุกคามจากภายใน

ระยะเริ่มต้น		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติของ CERT ข้อที่**	**หน้าที่**
ได้รับการสนับสนุนจากผู้บริหารระดับสูง	2	ระบุ
ระบุกรอบซึ่งเกี่ยวกับภัยคุกคามจากภายในซึ่งสามารถนำไปใช้เป็นพื้นฐานหรือเกณฑ์เปรียบเทียบ	2	ระบุ
ประเมินสภาพการณ์ปัจจุบันของความมั่นคงปลอดภัยของข้อมูล	2	ระบุ
ใช้ประโยชน์จากโครงการที่ครอบคลุมด้านความมั่นคงปลอดภัยของข้อมูล ความมั่นคงปลอดภัยขององค์กร และการกำกับดูแลด้านข้อมูลในการระบุและเข้าใจสินทรัพย์ที่มีความสำคัญ	2	ระบุ
ระบุผู้มีส่วนได้เสียที่สำคัญและสร้างกลไกในการกำกับดูแล	2	ระบุ

ระยะวางแผน		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติของ CERT ข้อที่**	**หน้าที่**
ประเมินและกำหนดขอบเขตของโครงการ	2	ระบุ
รู้ถึงและป้องกันสินทรัพย์ที่มีความสำคัญ	1	ระบุ
ทำให้แน่ใจว่ามีการบูรณาการกับการบริหารความเสี่ยงของทั้งองค์กร	2, 6	ระบุ
สร้างนโยบาย วิธีการ และวิธีปฏิบัติซึ่งได้รับการสนับสนุนจากผู้มีส่วนได้เสียหลักและพิจารณาถึงวัฒนธรรมขององค์กร ตัวอย่างของนโยบายต่างๆ ได้แก่: ■ นโยบายการใช้งานที่ยอมรับได้ ■ ประมวลจรรยาบรรณ ■ วิธีการเลิกจ้างพนักงาน ■ Nonrealization Policy ■ นโยบายการแจ้งเหตุการณ์ผิดปกติ ■ วิธีการรายงานกิจกรรมที่น่าสงสัย ■ วิธีการตอบสนองต่อเหตุการณ์ความเสี่ยง ■ นโยบายการแบ่งแยกหน้าที่การปฏิบัติงาน ■ คำจำกัดความระดับความรุนแรงของเหตุการณ์ ■ ระเบียบพิธีการสื่อสารกับเจ้าหน้าที่ผู้บังคับใช้กฎหมาย	3	ระบุ ป้องกัน ตอบโต้
เริ่มต้นจากกระบวนการจ้างงาน การเฝ้าระวังติดตาม และตอบสนองต่อพฤติกรรมที่น่าสงสัย และพฤติกรรมพนักงานที่เปลี่ยนแปลงไป	4	ระบุ ตอบโต้
ประสานงานกับหน่วยงานทรัพยากรบุคคลในการนำกระบวนการเฝ้าระวังติดตามไปใช้ปฏิบัติ ซึ่งครอบคลุมถึง 30 วันก่อนหน้าและ30 วันหลังจากพนักงานในหน้าที่หลักที่มีข้อมูลของสินทรัพย์ที่สำคัญลาออกจากการเป็นพนักงาน ซึ่งระยะเวลา 60 วันนี้เป็นช่วงเวลาที่มีการระบุว่า ความเสียหายน่าจะเกิดขึ้นได้มากที่สุด	9	ป้องกัน
ประสานงานกับหน่วยงานทรัพยากรบุคคลในการพัฒนาหลักสูตรฝึกอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามจากภายใน ความเสี่ยงที่เกี่ยวข้องและผลกระทบที่อาจเกิดขึ้นได้กับองค์กร	9	ป้องกัน
ประสานงานกับที่ปรึกษากฎหมายแต่เนิ่นๆ และบ่อยๆ เพื่อระบุถึงปัญหาเกี่ยวกับการป้องกันข้อมูลส่วนบุคคลและข้อกำหนดในการปฏิบัติตามเรื่องการส่งข้อมูลระหว่างประเทศ	4	ป้องกัน
คาดการณ์และจัดการกับเรื่องที่ส่งผลลบต่อสภาพแวดล้อมการทำงานโดยประสานงานกับหน่วยงานทรัพยากรบุคคลและกฎหมาย	5	ระบุ
ประสานงานกับผู้มีส่วนได้เสียในการพัฒนาแผนการสื่อสาร	2	ระบุ ตอบโต้ กู้คืน

ระยะวางแผน (ต่อ)		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
ระบุคู่ค้าทางธุรกิจและกลุ่มบุคคลที่สามที่ให้บริการ ซึ่งสามารถเข้าถึงสินทรัพย์ทางดิจิทัลขององค์กรได้	6	ระบุ
นำกระบวนการสอบสวนและการแก้ปัญหาที่ชัดเจนไปปฏิบัติ เพื่อให้แน่ใจว่าเหตุการณ์ความเสี่ยงทั้งหมดถูกจัดการตามกระบวนการอย่างคงเส้นคงวา	20	ระบุ ป้องกัน ตอบโต้ กู้คืน
คัดกรองพนักงานและคู่ค้าเป็นประจำโดยเฉพาะอย่างยิ่งบุคลากรที่อยู่ในตำแหน่งที่มีความเสี่ยงสูง หรือมีการเข้าถึงสินทรัพย์ทางดิจิทัลที่สำคัญ	4,6	ป้องกัน
พัฒนากระบวนการที่สามารถนำมาใช้ได้อย่างต่อเนื่องในการระบุ ป้องกันและตรวจหาภัยคุกคามจากภายใน และการตอบสนองและกู้คืนจากเหตุการณ์	2	ระบุ ป้องกัน ตรวจหา ตอบโต้ กู้คืน
- การจำแนกประเภทสินทรัพย์และข้อมูล และกระบวนการกำกับดูแลได้ถูกนำไปปฏิบัติ เพื่อจัดลำดับความสำคัญของสินทรัพย์ที่สำคัญและมีความละเอียดอ่อนต่อองค์กร สินทรัพย์ที่สำคัญเหล่านี้ควรถูกให้ความสำคัญสูงสุดเมื่อมีการนำวิธีการควบคุมภัยคุกคามจากภายในไปประยุกต์ใช้	1	ระบุ
- การปฏิบัติตามกฎระเบียบของรัฐและระหว่างประเทศในเรื่องการปกป้องข้อมูลที่มีความอ่อนไหวเช่น (HIPPA[6], FERPA[7],GDPR, PCIDSS[8]) ควรถูกนำมาพิจารณาและนำไปปฏิบัติตาม โดยทั่วไปแล้ว กฎระเบียบเหล่านี้มักจะกำหนดวิธีการควบคุมซึ่งมุ่งเน้นไปที่สิทธิในการเข้าถึงที่ต่ำที่สุด หรือเท่าที่จำเป็นต้องใช้ข้อมูลนั้น (need to know) ในการประเมินการเข้าถึงประเภทนี้ อาจเผยให้เห็นถึงบริเวณที่ผู้กระทำภัยคุกคามจากภายในสามารถละเมิดการใช้สิทธิพิเศษต่างๆ เพื่อดูข้อมูลซึ่งผู้นั้นไม่มีความจำเป็นในทางธุรกิจที่จะต้องใช้	2	ระบุ ป้องกัน ตรวจหา
- ระบุสัญญาด้านความมั่นคงปลอดภัยที่ชัดเจนในการใช้บริการคลาวด์โดยเฉพาะอย่างยิ่ง เรื่องการจำกัดสิทธิเข้าถึง และความสามารถในการการเฝ้าระวัง	16	ป้องกัน

6 HIPPA (The Health Insurance Portability and Accountability Act) คือกฎหมายของสหรัฐอเมริกา ซึ่งรวมมาตรฐานความเป็นส่วนตัวในการปกป้องประวัติการรักษาของผู้ป่วยและข้อมูลด้านสุขภาพอื่นๆ ที่ให้ไว้กับผู้ให้บริการทางการแพทย์

7 FERPA (The Family Educational Rights and Privacy Act) คือกฎหมายของสหรัฐอเมริกาซึ่งปกป้องข้อมูลส่วนบุคคลทางการศึกษาของนักเรียน

8 PCIDSS (The Payment Card Industry Data Security Standard) ที่ออกโดย PCI Security Standards Council คือมาตรฐานสากลที่ออกมาเพื่อปกป้องข้อมูลของผู้ถือบัตร

ระยะวางแผน (ต่อ)		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
- มีวิธีการเฝ้าระวังติดตามการสื่อสารของเครือข่ายภายในเหมือนกับการเฝ้าระวังติดตามการสื่อสารที่เข้ามาจากเครือข่ายภายนอก บ่อยครั้งที่องค์กรให้ความสำคัญกับการเฝ้าระวังติดตามภัยคุกคามจากภายนอกแต่ไม่ได้สนใจเรื่องการสื่อสารภายใน ยิ่งประกอบกับการจัดแบ่งประเภทที่ไม่เหมาะสมของระบบที่สำคัญจากผู้ใช้งานทั่วไปด้วยแล้ว เป็นไปได้ที่องค์กรจะไม่พบเห็นการโจมตีซึ่งเป็นภัยคุกคามจากภายในอันเกิดจากการใช้งานผ่านเครือข่าย	12	ตรวจหา
- การส่งเสริมการตระหนักรู้ให้พนักงานทราบว่าองค์กรเฝ้าระวังจับตาดูอยู่	5, 9	ป้องกัน
- รณรงค์ส่งเสริมการตระหนักรู้เรื่องสื่อออนไลน์เพื่อให้พนักงานมีความรู้ถึงความเสี่ยงของการเปิดเผยข้อมูลที่อาจเป็นไปได้	7	ป้องกัน
- การจัดการสิทธิพิเศษในการเข้าถึง ในการป้องกันการโจมตีจากภายในและเพื่อให้มีการปฏิบัติตามกฎเกณฑ์นั้น องค์กรจะต้องติดตามและจัดการสิทธิพิเศษในการเข้าถึงในเชิงรุก การจัดการสิทธิพิเศษในการเข้าถึงนี้จะทำให้องค์กรสามารถติดตามและจำกัดสิทธิพิเศษที่เกินความจำเป็นได้ ซึ่งโดยทั่วไปแล้วสิทธิพิเศษประเภทนี้จะถูกใช้โดยผู้บริหารระบบ ผู้บริหารฐานข้อมูลและพนักงานที่ต้องทำหน้าที่ในการดูแลระบบหรืองานด้านปฏิบัติการ เนื่องจากบัญชีของผู้มีสิทธิพิเศษเหล่านี้จะสามารถข้ามผ่านการควบคุมบางอย่างได้ องค์กรจะต้องมีนโยบาย กระบวนการ และเทคโนโลยีในการป้องกันและตรวจหาการนำสิทธิประเภทนี้ไปใช้งานในทางที่ผิด - จุดประสงค์หลักในการจัดการสิทธิพิเศษในการเข้าถึงแบบนี้คือ การจัดให้มีการจัดการแบบอัตโนมัติและสามารถนำกลับมาใช้ได้อย่างต่อเนื่องในการติดตามการให้สิทธิและการถอดถอนสิทธิที่สำคัญ ยกตัวอย่างเช่นการถอดถอนสิทธิการเข้าถึงระบบที่กำลังพัฒนาและมีการใช้งานจริง และให้สิทธิแบบเฉพาะกาลเพื่อใช้ในกระบวนการเปลี่ยนแปลงแบบฉุกเฉินซึ่งรวมถึง การ login สำหรับกิจกรรมทั้งหมด	10, 11, 15	ป้องกัน
- การบริหารโครงสร้างและเอกสารบรรยายหน้าที่งาน (job descriptions) เพื่อที่จะลดข้อผิดพลาดและความกังวลที่เกิดโดยไม่ได้ตั้งใจของคนในองค์กร	8	ป้องกัน
- การตอบสนองต่อเหตุการณ์ความเสี่ยงในวิถีทางที่เป็นระบบในการตอบสนองและจัดการกับผลจากเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยด้าน IT ที่เกิดขึ้นโดยทั่วไปแล้ว เอกสารที่ระบุคำแนะนำและขั้นตอนปฏิบัติกรณีเหตุการณ์ความผิดปกติด้าน IT ก็คือแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan--IRP) และกลุ่มบุคลากรในวิชาชีพที่มีหน้าที่วิเคราะห์ จัดการ และรายงานเหตุการณ์ผิดปกติด้าน IT เป็นที่รู้จักในชื่อทีมตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยด้านคอมพิวเตอร์ (Computer Security Incident Response Team)	2	ตอบโต้ กู้คืน

ระยะปฏิบัติการ		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
การนำวิธีการควบคุมไปปฏิบัติทั้งทางด้านกายภาพและทางตรรกะในการป้องกัน ตรวจหา ตอบสนอง และกู้คืน ยกตัวอย่างเช่น		ป้องกัน ตรวจหา ตอบโต้ กู้คืน
- การควบคุมทางด้านกายภาพซึ่งรวมถึง ระบบจัดการการเข้าสู่อาคาร และวิดีโอที่ใช้ในการเฝ้าระวัง ซึ่งสามารถใช้ในการตรวจหาสิ่งผิดปกติหรือการเข้ามาโดยไม่ได้รับอนุญาตในพื้นที่ที่สามารถเข้าถึงข้อมูลที่สำคัญได้ ยกตัวอย่างเช่น ▪ ระบบดับเพลิง ▪ HVAC ▪ การติดตามโดยใช้กล้องวิดีโอ ▪ บัตรผ่านเข้าออกการล๊อค ประตูหมุน mantraps	2	ป้องกัน ตรวจหา
- การระบุตัวตนและวิธีการควบคุมอย่างแข็งขัน เพื่อที่จะกำกับดูแลการเข้าถึงระบบงานและข้อมูล (ไม่ว่าจะเป็นข้อมูลทางกายภาพหรือสินทรัพย์ทางดิจิทัล) ซึ่งรวมถึงการให้สิทธิและถอดถอนสิทธิผู้ใช้งาน การสอบทานการเข้าถึงของผู้ใช้งานตามความจำเป็นทางธุรกิจการสอบทานการเข้าถึงระยะไกล (remote access) และการอนุมัติให้ใช้งาน (คู่ค้าและพนักงาน) นโยบายห้ามการใช้สิทธิการเข้าถึงร่วมกัน และการควบคุมผู้ใช้งานภายใน คู่ค้า และกลุ่มบุคคลที่สาม	10, 11, 12, 15	ป้องกัน
มีการติดตั้ง Firewalls ก่อนเข้าสู่ระบบที่สำคัญและมีการตั้งค่าเพื่อที่จะควบคุมให้มีการเชื่อมต่อกับอุปกรณ์ทำงานที่ได้รับอนุญาตเท่านั้น	13	ป้องกัน ตรวจหา
- จำเป็นต้องให้ความสนใจในการจัดแบ่งเครือข่ายภายในและข้อจำกัดต่างๆ เพื่อควบคุมเครือข่าย ควรมีการจำกัดสิทธิในการเข้าถึงระบบสารสนเทศที่เก็บข้อมูลสำคัญขององค์กร โดยควรให้สิทธิเฉพาะผู้ที่มีความจำเป็นทางธุรกิจที่ต้องใช้ข้อมูลเท่านั้น การจัดแบ่งนี้สามารถรวมถึง การแยก Virtual Local Area Network (VLAN) การจัดทำรายการควบคุมการเข้าถึง (Access Control Lists) หรือการตั้งค่า firewall rule เพื่อแยกระบบเหล่านั้น และกำหนดที่ตั้งของเครื่อง Servers ให้ปลอดภัยจากการเข้าถึงหรือการเข้าขัดขวางการทำงานได้โดยตรง	13	ป้องกัน

ระยะปฏิบัติการ (ต่อ)		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
- การจัดแบ่งเครือข่ายภายนอกและการจำกัดการเข้าถึงเครือข่าย การจัดแบ่งนี้สามารถรวมถึง การใช้เขต DMZ (demilitarized zones)เครือข่ายส่วนตัวเสมือน (Virtual Private Network--VPN) และ honeypots และ Proxy servers เพื่อควบคุมการสื่อสารระหว่างสภาพแวดล้อมที่มีความน่าเชื่อถือและที่ไม่น่าเชื่อถือ	13	ป้องกัน ตรวจหา
- การใช้ซอฟต์แวร์บริหารจัดการข้อมูลและเหตุการณ์ (Software Information and Event Management -- SIEM) ร่วมกับ Security Information Management (SIM) และ Security Event Management (SEM) เพื่อการตรวจสอบย้อนหลังและบันทึกการกระทำที่ผิดปกติของผู้ใช้งานที่กระทำต่อระบบแต่ละระบบ ชุดข้อมูล หรือการทำงานในเครือข่ายทั่วไป เช่น การเชื่อมต่อร่วมกัน และทำการแจ้งเตือน ผลจากการ logs ควรได้รับการสอบทานและประเมินอย่างจริงจัง เพื่อตรวจหาความผิดปกติ logs เหล่านี้ควรมีความครอบคลุมเพียงพอที่จะสนับสนุนกิจกรรมการตอบสนองในกรณีที่เกิดเหตุการณ์ผิดปกติที่กระทบความมั่นคงปลอดภัยของข้อมูล	13	ตรวจหา ตอบโต้
- การเฝ้าติดตามด้านความมั่นคงปลอดภัยซึ่งเสริมโดยการใช้เครื่องมือในการวิเคราะห์ข้อมูล เช่น User and Entity Behavior Analytics (UEBA) ในการกำหนดมาตรฐานกิจกรรมการปฏิบัติการทางธุรกิจบนระบบแต่ละระบบ ชุดข้อมูล หรือทรัพยากรของเครือข่าย การเข้าใจรูทีน งานที่ทำเป็นประจำบนเครือข่ายภายในจะช่วยให้เจ้าหน้าที่ ที่ดูแลระบบสามารถระบุความผิดปกติหรือพฤติกรรมผิดปกติอันอาจบ่งบอกถึงการกระทำที่ประสงค์ร้ายได้ (สัญญาณเตือนภัย)	12,14	ตรวจหา
- ควรมีเทคโนโลยีการแจ้งเตือนที่มีประสิทธิผลในอันที่จะสามารถจับการเปลี่ยน เพิ่ม หรือดัดแปลงทรัพยากรของเครือข่าย ระบบงาน หรือการควบคุมด้านความมั่นคงปลอดภัย การแจ้งเตือนนี้ควรส่งไปถึงผู้ที่มีหน้าที่โดยตรงในการจัดการเทคโนโลยีแต่ละอย่างเพื่อที่จะสามารถระบุภัยคุกคามที่เกิดจากการวิเคราะห์ที่ผิดพลาดได้อย่างรวดเร็ว เทคโนโลยีเหล่านี้รวมถึง Intrusion Detection/Prevention Systems (IDS/IPS)	17, 19	ตรวจหา ตอบโต้

ระยะปฏิบัติการ (ต่อ)		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
- นโยบายและกระบวนการรายงานเหตุการณ์ผิดปกติ จะทำให้มั่นใจว่าการแจ้งเตือนเกี่ยวกับภัยคุกคามที่เชื่อถือได้จะถูกสื่อสารไปยังกลุ่มคนในองค์กรที่มีหน้าที่โดยตรงเพื่อลดผลกระทบให้น้อยลงได้ ตัวอย่างเช่น ถ้าการแจ้งเตือนมาจากผู้บริหารระบบงานว่ามีการสร้างบัญชี super user ใหม่โดยไม่ผ่านกระบวนการสอบทานและอนุมัติตามปกติ ข้อมูลนี้ควรสื่อสารไปยังผู้รับผิดชอบที่มีหน้าที่โดยตรงในทันทีเช่น หน่วยงานธุรกิจ เจ้าของข้อมูล และหน่วยงานความมั่นคงปลอดภัยเพื่อป้องกันภัยจู่โจมไม่ให้ขยายผลลึกลงไปถึงการเข้าถึงโดยไม่ได้รับ	3	ตอบโต้ กู้คืน
- การติดตั้งเทคโนโลยีเพื่อป้องกันข้อมูลสูญหายที่ส่วนที่อยู่ขอบของเครือข่าย (network edge) และภายในเทคโนโลยีอีเมล์ เพื่อที่จะระบุกรณีที่มีการส่งข้อมูลที่มีความอ่อนไหวออกไปภายนอกองค์กร นอกจากนี้ ยังควรมีการสอบทานหรือประเมินการควบคุมด้านความมั่นคงปลอดภัย เพื่อกำกับการ upload/download ข้อมูลไปยังผู้ให้บริการคลาวด์ที่ใช้โดยองค์กร และมีการเข้าถึงบริการเหล่านั้นโดยผ่านเครือข่ายสาธารณะเช่น internet ได้หรือไม่ ซึ่งสิ่งนี้ผู้คุกคามภายในสามารถนำไปใช้ในทางที่ผิดโดยใช้ช่องทางตามสิทธิทางธุรกิจนี้ในการ upload ข้อมูลที่มีความอ่อนไหวไปสู่คลาวด์และนำมันกลับมาจากเครือข่ายภายนอกที่ไม่ได้ตั้งอยู่ภายใต้การเฝ้าระวังติดตามขององค์กร	19	ป้องกัน ตรวจหา
- เทคโนโลยีในการควบคุมอื่นๆซึ่งรวมถึงกลไกทั้งด้านกายภาพและด้านตรรกะที่ใช้ในการ ป้องกัน ตรวจหาและตอบสนองต่อเหตุการณ์ความเสี่ยงด้าน IT ยกตัวอย่างเช่น ▪ การจัดการการเปลี่ยนแปลง ▪ การจัดการการตั้งค่า ▪ Patch management ▪ ขั้นตอนการเก็บเอกสารสำคัญ การสำรองและกู้คืน ▪ การทดสอบการเจาะระบบ (Penetration testing)	17,18,19	ป้องกัน ตรวจหา กู้คืน
การใช้เทคนิคการวิเคราะห์ข้อมูล (Data Analytics) เพื่อทำให้โครงการเข้มแข็งขึ้น	12	ตอบโต้
นำคู่มือการตอบสนองต่อเหตุการณ์ความเสี่ยงไปปฏิบัติ	2	ตอบโต้ กู้คืน
รวบรวมหลักฐานและเอกสารของบทเรียนที่ได้รับ	12	ระบุ

ระยะการรายงาน		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
ประเมินโครงการเป็นระยะๆ และปรับปรุงตามความจำเป็น มีหัวข้อและดัชนีชี้วัดความสำเร็จ (KPIs) ที่มักจะได้รับการประเมินโดยทั่วไปตาม maturity scale เพื่อที่จะดูว่าองค์กรกำลังทำสิ่งที่ถูกต้องหรือไม่	2	Recovery
- การกำกับดูแลและพัฒนา	2	กู้คืน
- การประเมิน (ความเสี่ยงจากภัยคุกคาม กลุ่มบุคคลที่สามและสินทรัพย์)	2	กู้คืน
- การเฝ้าระวังติดตาม ■ จำนวนหรือความปกติที่ถูกสอบสวน ■ จำนวนที่สูงขึ้นหรืออัตราการเพิ่มขึ้นของข้อมูลที่ส่งออก ■ จำนวนของผลในทางบวกที่ไม่ถูกต้อง ■ จำนวนของผลในทางลบที่ไม่ถูกต้อง ■ จำนวนของการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยโดยเจ้าหน้าที่ด้านไอที	2	กู้คืน
- การปกป้องสินทรัพย์	2	กู้คืน
- ผลการปฏิบัติงาน ■ ผลงานโดยรวมของทีม ■ อัตราการลาออกของพนักงาน ■ การจัดการงบประมาณ ■ การประเมินตนเองเป็นการภายใน ■ การประเมินจากภายนอก ■ ข้อเสนอแนะการปรับปรุงซึ่งไม่ได้ถูกนำไปดำเนินการแก้ไข ■ พนักงานที่อยู่ในแผนการปรับปรุงผลการทำงาน ■ พนักงานหรือบริเวณที่มีประเด็นร้องเรียนมาทาง HR มากเกินปกติ	2	กู้คืน
- การจัดการเหตุการณ์ความเสี่ยงและการตอบสนอง ■ ประเภทและปริมาณของการสอบสวนภายในช่วงระยะเวลาหนึ่ง ■ จำนวนการสอบสวนที่เสร็จสิ้นแบบน่าพอใจ ■ จำนวนการสอบสวนที่เสร็จสิ้นภายใน 30 วัน คุณภาพของการสื่อสารกับผู้มีส่วนได้เสียภายใน และการบังคับใช้กฎหมาย	2	ระบุ กู้คืน

ระยะการรายงาน (ต่อ)		
กิจกรรม/วิธีการควบคุม	**วิธีปฏิบัติตาม CERT ข้อที่**	**หน้าที่**
- การให้ความรู้และการตระหนักรู้ ■ จำนวนของผู้ใช้งาน ผู้บริหารระบบ ผู้สอบสวนและผู้บริหารระดับสูงซึ่งได้เข้ารับการอบรมภายในระยะเวลาที่กำหนด ■ เปอร์เซ็นต์ของคนที่ผ่านคำถามการประเมินหลังจบการอบรม ■ ความถี่ของการจัดฝึกอบรม ■ เปอร์เซ็นต์ของการเกิดซ้ำ ■ จำนวนของรายงานเหตุการณ์ผิดปกติด้าน IT ■ จำนวนของเหตุการณ์ผิดปกติด้าน IT ที่มีการตรวจพบโดยการใช้กลไกการเฝ้าระวังติดตาม	2	ระบุ กู้คืน
มั่นใจได้ว่ามีการดำเนินการฝึกปฏิบัติบทเรียนที่ได้รับหลังจากเกิดเหตุการณ์เพื่อกำหนดบริเวณที่ควรได้รับการปรับปรุงให้ดีขึ้น	2	
ดำเนินตามแผนการปรับปรุงแก้ไข	2	ตอบโต้ กู้คืน

การให้ความเชื่อมั่นกับคณะกรรมการ

เพื่อให้การสื่อสารเรื่องภัยคุกคามจากภายในถึงคณะกรรมการเป็นไปอย่างมีประสิทธิผล ผู้ตรวจสอบภายในควรสื่อความหมายของประเด็นที่ตรวจพบในรูปของความเสียหายทางการเงิน การสูญเสียชื่อเสียง การดำเนินงานหยุดชะงัก และดัชนีชี้วัดด้านการดำเนินงานขององค์กร

เพื่อแสดงให้เห็นภาพของความเสี่ยงในมุมมองซึ่งมีความหมายต่อผู้บริหารระดับสูง ผู้ตรวจสอบภายในอาจพบว่ามันจะมีประโยชน์หากใช้ข้อมูลรายงานของอุตสาหกรรมที่อธิบายถึงความเสียหายจากข้อมูลที่รั่วไหลหรือมีการละเมิดข้อมูลทั่วโลกอันเป็นผลจากภัยคุกคามภายใน การใช้ข้อมูลที่เกิดขึ้นจริงในโลกนี้จะช่วยในการสื่อสารถึงผลกระทบในเชิงกว้างและลึก และยังช่วยขจัดความเชื่อที่ว่าภัยคุกคามจากภายในอันทำให้เกิดการละเมิดนั้นไม่สามารถเกิดขึ้นกับองค์กรได้

รายงานการตรวจสอบ
สำหรับคำแนะนำเรื่องการจัดเตรียมรายงานการตรวจสอบภายในนั้น ดูได้ที่แนวปฏิบัติของ IIA เรื่อง “รายงานการตรวจสอบ: การสื่อสารรายงานสำหรับงานการให้ความเชื่อมั่น”

การให้ความรู้แก่คณะกรรมการนั้นรวมถึง การช่วยให้มีความเข้าใจว่า "ความปลอดภัยอย่างแน่นอน" นั้นย่อมเป็นไปไม่ได้ ดังนั้น จึงมีความจำเป็นที่จะเน้นไปที่การทำให้ศักยภาพขององค์กรในการตอบสนองต่อเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทาง IT มีความเข้มแข็งมากขึ้น และการทำให้เกิดความสมดุลกันระหว่างความมั่นคงปลอดภัยและความมีประสิทธิผล (ความมั่นคงปลอดภัยนั้นถูกจัดการให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ขององค์กร)

องค์ประกอบที่สำคัญอื่นๆ สำหรับการให้ความเชื่อมั่นต่อคณะกรรมการรวมถึง:

- พัฒนาแนวทางการร่วมมือกันรายงานกับกลุ่มคนที่เกี่ยวข้องเช่น หัวหน้าเจ้าหน้าที่ด้านความมั่นคงปลอดภัยของข้อมูล (CISO) และหัวหน้าเจ้าหน้าที่ด้านความเสี่ยง (CRO) เพื่อแสดงให้เห็นถึงระดับความก้าวหน้าขององค์กรในเรื่องความมั่นคงปลอดภัยอันเกี่ยวกับภัยคุกคามจากภายใน
- การทำให้แน่ใจว่าความเสี่ยงของภัยคุกคามจากภายในนั้นถูกรวมเป็นส่วนหนึ่งในการประเมินความเสี่ยงระดับองค์กร และมีการสื่อสารถึงความพยายามและผลที่เกิดขึ้นไปยังคณะกรรมการ
- หน่วยงานที่ให้ความเชื่อมั่นเห็นพ้องกันที่จะใช้กรอบซึ่งทั้งหมดสามารถใช้ในการประเมินความก้าวหน้าและความมีประสิทธิผลของความพยายามในการบรรเทาภัยคุกคามจากภายใน
- พัฒนาสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ เพื่อแสดงให้เห็นถึงผู้กระทำที่เป็นไปได้ รวมถึงโอกาสและผลกระทบโดยใช้ภาษาที่เชื่อมโยงกับวัตถุประสงค์ทางธุรกิจได้อย่างชัดเจน

- ตัดสินว่าหน่วยงานตรวจสอบภายในมีความรู้ความสามารถที่จำเป็นเพียงพอที่จะประเมินการบริหารจัดการภัยคุกคามจากภายในองค์กร หรือสามารถรับการฝึกอบรมเพิ่มเติม และหากไม่มีก็อาจจะต้องพึ่งพาความเชี่ยวชาญจากภายนอก
- พัฒนาแผนการตรวจสอบภายในโดยใช้ประโยชน์จากงานที่ทำโดยหน่วยงานให้ความเชื่อมั่นอื่นๆ (หน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบ การประเมินตนเองของฝ่ายจัดการ และผลของการบริหารความเสี่ยง)

การใช้ประโยชน์จากงานที่ทำโดยหน่วยงานให้ความเชื่อมั่นอื่นๆ นั้น จำเป็นอย่างยิ่งที่จะต้องมีการกำหนดบทบาทและความรับผิดชอบระหว่าง หน่วยงานธุรกิจ หน่วยงานบริหารความเสี่ยง หน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบ และผู้มีส่วนได้เสียในการให้ความเชื่อมั่นอื่นๆ และจะต้องกำหนดว่าข้อมูลอะไรบ้างที่สามารถนำมาใช้ และการตรวจสอบภายในจะประเมินความเชื่อถือได้ของงานที่ทำโดยแนวป้องกันขั้นที่ 1 และ 2 ได้อย่างไร

การพึ่งพาหน่วยงานที่ให้ความเชื่อมั่น
สำหรับคำแนะนำในการสร้างแผนการให้ความเชื่อมั่น ให้ดูแนวปฏิบัติของ IIA " การประสานงานและการพึ่งพา: การพัฒนาแผนการให้ความเชื่อมั่น"

ภาคผนวก ก มาตรฐานและแนวทางของ IIA ที่เกี่ยวข้อง

ข้อมูลจาก IIA ดังต่อไปนี้ได้มีการอ้างถึงตลอดในแนวปฏิบัตินี้ สำหรับข้อมูลในการนำมาตรฐานวิชาชีพสากลสำหรับการปฏิบัติงานตรวจสอบภายในไปประยุกต์ใช้ ให้ดูได้จากแนวทางการนำมาตรฐานไปใช้ปฏิบัติ Implementation Guides ของ IIA

มาตรฐาน
มาตรฐาน 1210 - ความเชี่ยวชาญ
มาตรฐาน 2010 - การวางแผน
มาตรฐาน 2050 - การประสานงานและการพึ่งพาผลงานของผู้อื่น
มาตรฐาน 2100 - ลักษณะของงาน
มาตรฐาน 2110 - การกำกับดูแล
มาตรฐาน 2120 - การบริหารความเสี่ยง
มาตรฐาน 2130 - การควบคุม
มาตรฐาน 2200 - การวางแผนสำหรับงานที่ได้รับมอบหมาย
มาตรฐาน 2201 - ข้อพิจารณาในการวางแผน
มาตรฐาน 2210 - วัตถุประสงค์ของงานที่ได้รับมอบหมาย
มาตรฐาน 2220 - ขอบเขตของงานที่ได้รับมอบหมาย
มาตรฐาน 2230 - การจัดสรรทรัพยากรสำหรับงานที่ได้รับมอบหมาย
มาตรฐาน 2240 - แนวการปฏิบัติงาน
แนวปฏิบัติ
แนวปฏิบัติ “การประสานงานและการพึ่งพาผลงานของผู้อื่น: การพัฒนาแผนผังการให้ความเชื่อมั่น“ 2561
แนวปฏิบัติ “การวางแผนสำหรับงานที่ได้รับมอบหมาย: การประเมินความเสี่ยงด้านทุจริต" 2560
แนวปฏิบัติ “การวางแผนสำหรับงานที่ได้รับมอบหมาย: การกำหนดวัตถุประสงค์และขอบเขต" 2560
GTAG การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์: บทบาทของแนวป้องกัน 3 ชั้น 2559
GTAG การตรวจสอบการกำกับดูแลด้าน IT 2561

ภาคผนวก ข อภิธานศัพท์

คำที่มีเครื่องหมายดอกจัน (*) นั้น ได้นำมาจากอภิธานศัพท์ของ*มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพด้านการตรวจสอบภายในของ IIA*

การบริการให้ความเชื่อมั่น* – Assurance Services: การตรวจสอบหลักฐานอย่างเที่ยงธรรมเพื่อให้ได้มาซึ่งการประเมินกระบวนการกากับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร อย่างเป็นอิสระ

คณะกรรมการ* – Board: คณะบุคคลในระดับสูงสุดที่ทำหน้าที่ในการกำกับดูแลองค์กร (ตัวอย่างเช่น คณะกรรมการองค์กร (Board of Directors) คณะกรรมการกำกับดูแล (Supervisory Board) หรือ คณะกรรมการนโยบาย หรือทรัสตี (Board of Governors or Trustees) ซึ่งมีหน้าที่ในการสั่งการและ/หรือสอดส่องดูแลกิจกรรมขององค์กร และพิจารณาความรับผิดชอบในผลงานการบริหารของผู้บริหารระดับสูง ถึงแม้การจัดระบบการกำกับดูแลอาจแตกต่างกันไปตามแต่ละขอบเขตอำนาจของแต่ละรัฐ หรือในแต่ละภาคส่วน โดยมากแล้ว คณะกรรมการจะรวมถึงสมาชิกที่ไม่ได้มีส่วนในการบริหารหากในองค์กรไม่มีคณะกรรมการแล้ว คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้จะหมายถึง กลุ่มคนหรือบุคคลที่ทำหน้าที่กำกับดูแลองค์กรนอกจากนั้น คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้ อาจหมายถึง คณะหรือองค์คณะอื่นใดที่ทางองค์คณะซึ่งมีหน้าที่กำกับดูแลได้มอบหมายหน้าที่บางอย่างให้ (เช่น คณะกรรมการตรวจสอบ)

หุ้นส่วนทางธุรกิจ – Business Partners: องค์กรซึ่งเป็นกลุ่มบุคคลที่สามใดๆ ก็ตามที่ได้รับสิทธิในการเข้าถึงลูกค้าขององค์กร เครือข่ายผู้ผลิต ระบบ และข้อมูล

หัวหน้าหน่วยงานตรวจสอบภายใน* - Chief Audit Executive: คำว่า หัวหน้าหน่วยงานตรวจสอบภายใน จะหมายถึง บทบาทของบุคคลซึ่งอยู่ในตำแหน่งงานที่อยู่ในระดับสูง ซึ่งรับผิดชอบในการบริหารหน่วยงานตรวจสอบภายในให้มีประสิทธิผลโดยสอดคล้องกับกฎบัตรของหน่วยงานตรวจสอบภายใน และองค์ประกอบส่วนที่เป็นภาคบังคับของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล หัวหน้าหน่วยงานตรวจสอบภายใน หรือบุคคลที่ต้องรายงานต่อหัวหน้าหน่วยงานตรวจสอบภายใน ควรมีประกาศนียบัตรทางวิชาชีพและคุณสมบัติที่เหมาะสม อย่างไรก็ตามชื่อตำแหน่งสำหรับหัวหน้าหน่วยงานตรวจสอบภายใน อาจแตกต่างกันในแต่ละองค์กร

การบริการให้คำปรึกษา* – Consulting Services: กิจกรรมการให้คำปรึกษา แนะนำ และบริการที่เกี่ยวเนื่องแก่ผู้รับบริการ โดยลักษณะและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกันกับผู้รับบริการโดยมุ่งหมายที่จะเพิ่มคุณค่าและปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร โดยผู้ตรวจสอบภายในต้องไม่เข้าไปรับภาระหน้าที่ในทางการบริหาร ตัวอย่าง ได้แก่ การให้คำปรึกษา คำแนะนำ การอำนวยความสะดวก และการฝึกอบรม

กระบวนการควบคุม* – Control Process: นโยบาย วิธีการปฏิบัติ (ทั้งที่ทำด้วยมือ หรือโดยระบบอัตโนมัติ) และกิจกรรมต่างๆ ขององค์กรซึ่งเป็นส่วนหนึ่งของกรอบโครงสร้างการควบคุมที่ได้รับการออกแบบมาและใช้ปฏิบัติจริง เพื่อที่จะเชื่อมั่นได้ว่าความเสี่ยงได้ถูกจำกัดให้อยู่ในระดับที่ยอมรับได้

การทุจริต* – Fraud: การกระทำผิดกฎหมายของบุคคลหรือองค์กรในลักษณะของการฉ้อฉลหลอกลวง ปกปิด หรือทำลายความเชื่อมั่น การกระทำเหล่านี้ไม่จำเป็นต้องเป็นการคุกคามโดยใช้ความรุนแรงหรือการใช้กำลังบังคับ การทุจริตอาจกระทำโดยกลุ่มบุคคลและองค์กร เพื่อให้ได้มาซึ่งเงินทองทรัพย์สินหรือบริการ เพื่อเลี่ยงการจ่ายเงินหรือการสูญเสียบริการ หรือเพื่อปกป้องผลประโยชน์ของบุคคลหรือผลประโยชน์ทางธุรกิจ

การกำกับดูแล* – Governance: การผสมผสานของกระบวนการและโครงสร้างต่าง ๆ ที่คณะกรรมการนำมาใช้เพื่อบอกกล่าว สั่งการ บริหาร และเฝ้าติดตามกิจกรรมต่างๆ ภายในองค์กรเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

เหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยของ IT[9] – IT Security Incident: การเกิดเหตุการณ์ที่ได้ประเมินแล้วว่าได้เกิดความเสียหายจริงหรืออาจก่อให้เกิดความเสียหายได้ต่อ การรักษาความลับ ความสมบูรณ์ หรือ ความพร้อมใช้งานของระบบข้อมูล หรือข้อมูลที่ระบบประมวลผล การจัดเก็บ หรือการส่งต่อ หรือแม้กระทั่งก่อให้เกิดการละเมิด หรือภัยคุกคามที่จวนเจียนจะเป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัย วิธีปฏิบัติด้านความมั่นคงปลอดภัย หรือนโยบายการใช้งานที่เป็นยอมรับ

หน่วยงานตรวจสอบภายใน*– Internal Audit Activity: ฝ่าย สายงาน คณะที่ปรึกษา หรือ ผู้ปฏิบัติหน้าที่อื่นๆ ที่ให้บริการการให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งออกแบบมาเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กร หน่วยงานตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายได้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุม อย่างเป็นระบบและเป็นระเบียบ

ความเสี่ยง* – Risk : ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่จะส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบจากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น

ระดับความเสี่ยงที่ยอมรับได้*– Risk Appetite: ระดับความเสี่ยงที่องค์กรเต็มใจที่จะยอมรับ

วิศวกรรมทางสังคม[10]– Social Engineering: ภายใต้บริบทด้านความมั่นคงปลอดภัยของข้อมูล หมายถึง การทำให้คนทำการกระทำใดๆ โดยที่ไม่รู้เท่าทัน อันก่อให้เกิดอันตรายหรือเป็นการเพิ่มโอกาสในการก่อให้เกิดอันตรายในอนาคต ต่อการรักษาความลับ ความสมบูรณ์ หรือความพร้อมใช้งานของทรัพยากรหรือสินทรัพย์ขององค์กร ซึ่งรวมทั้งข้อมูล ระบบข้อมูล หรือระบบทางการเงิน

---

[9] คณะทำงานบัญญัติศัพท์เกี่ยวกับระบบรักษาความปลอดภัยแห่งชาติ Committee on National Security Systems Glossary Working Group คำสั่งของ CNSS ที่ 4009 เรื่อง: National Information Assurance Glossary, (Washington, D.C.: National Security Agency, 2010), 35.

[10] ศูนย์ภัยคุกคาม ของ CERT (The CERT® Insider Threat Center) เรื่อง “Unintentional Insider Threats: Social Engineering,” https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf, p. xi

ภาคผนวก ค การประเมินภัยคุกคามจากภายในโดยการใช้กรอบความมั่นคงปลอดภัยทางไซเบอร์ของ NIST

ตามมาตรฐาน 2240.A1 ได้ระบุว่า "แนวการปฏิบัติงานต้องรวมถึง วิธีการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และบันทึกข้อมูลในระหว่างการปฏิบัติงาน" ในการเริ่มต้นการจัดทำแนวการปฏิบัติงาน ผู้ตรวจสอบภายในอาจใช้กรอบของความเสี่ยงและการควบคุมที่มีอยู่ แผนผังข้างล่างนี้ใช้กรอบด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST เป็นเกณฑ์ในการวัดเปรียบเทียบโครงการด้านภัยคุกคามจากภายใน

N. Hanacek/NIST

ผู้ตรวจสอบภายในอาจประยุกต์ใช้ภาพนี้ให้เหมาะสมกับองค์กรและงานเฉพาะที่ได้รับมอบหมาย โดยใช้ภาพนี้ผู้ตรวจสอบอาจพัฒนาตารางความเสี่ยงและการควบคุมและการประเมินความเสี่ยงซึ่งอาจขยายไปสู่แนวการปฏิบัติงาน

กรอบด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST ถูกสร้างมาเพื่อให้เป็นภาษาร่วมเพื่อความเข้าใจ การจัดการและแสดงให้เห็นถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งภายในและภายนอก กรอบนี้ช่วยให้ผู้ใช้งานระบุและจัดลำดับความสำคัญของสิ่งที่ต้องทำเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่รวมถึงภัยคุกคามจากภายในซึ่งสามารถแปลงไปสู่การกระทำเพื่อลดความเสี่ยงด้านภัยคุกคามจากภายในได้

กรอบนี้ได้ถูกจัดออกเป็น หน้าที่ต่างๆ (การระบุ ป้องกัน ตรวจหา ตอบสนอง และกู้คืน) ประเภท และประเภทย่อย ประเภทของวัตถุประสงค์ของการควบคุมในแนวการปฏิบัติงาน และ กิจกรรมการควบคุมย่อยๆ ภายใต้แต่ละวัตถุประสงค์การควบคุม ผู้ตรวจสอบภายในอาจใช้คอลัมน์สุดท้ายในการบันทึกวิธีการควบคุมที่มีอยู่ในองค์กร (การทำซ้ำนี้ ได้รับอนุญาตจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์แห่งสหรัฐอเมริกา ไม่ได้จดลิขสิทธิ์ในสหรัฐอเมริกา)

หน้าที่: ระบุ	
ประเด็นความเสี่ยง: การจัดการสินทรัพย์	
วัตถุประสงค์ของการควบคุม: ข้อมูล บุคลากร เครื่องมือ ระบบและสิ่งอำนวยความสะดวกซึ่งเอื้อให้องค์กรสามารถบรรลุวัตถุประสงค์ทางธุรกิจได้ถูกระบุและจัดการอย่างสอดคล้องกับความสำคัญต่อวัตถุประสงค์ทางธุรกิจและกลยุทธ์ความเสี่ยงขององค์กร	
กิจกรรมการควบคุม	**การประเมิน**
มีการบันทึกทะเบียนรายการเครื่องมือและระบบในองค์กร	
มีการบันทึกทะเบียนรายการ Software platform และ applications ในองค์กร	
สำรวจการสื่อสารขององค์กรและเส้นทางเดินของข้อมูล (data flow)	
ระบบข้อมูลภายนอกได้จัดทำเป็นบัญชีรายชื่อไว้	

หน้าที่: ระบุ (ต่อ)	
ประเด็นความเสี่ยง: สภาพแวดล้อมทางธุรกิจ	
วัตถุประสงค์ของการควบคุม: พันธกิจ วัตถุประสงค์ ผู้มีส่วนได้เสียและกิจกรรมขององค์กรถูกเข้าใจและจัดลำดับความสำคัญ ข้อมูลนี้ถูกใช้ในการแจ้งบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์และการตัดสินใจด้านการบริหารความเสี่ยง	
กิจกรรมการควบคุม	**การประเมิน**
ทรัพยากร เช่น hardware เครื่องมือ ข้อมูล เวลา และ software ได้ถูกจัดลำดับความสำคัญตามการแบ่งแยกประเภท ความสำคัญ และคุณค่าทางธุรกิจ	
มีการกำหนดบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ของทั้งองค์กรและผู้มีส่วนได้เสียอันเป็นบุคคลกลุ่มที่สามเช่น คู่ค้า ลูกค้าและหุ้นส่วน	
ได้มีการระบุและสื่อสารถึงบทบาทขององค์กรในห่วงโซ่อุปทาน	
มีการระบุและสื่อสารถึง ตำแหน่งขององค์กรในโครงสร้างพื้นฐานที่สำคัญ และในภาคอุตสาหกรรมที่องค์กรดำเนินธุรกิจอยู่	
มีการจัดลำดับความสำคัญและสื่อสาร พันธกิจองค์กร วัตถุประสงค์และกิจกรรม	
มีการกำหนดหน่วยงานสำคัญที่ต้องเป็นที่พึ่งและซึ่งมีหน้าที่ให้บริการที่จำเป็น	
มีการกำหนดความยืดหยุ่นในการสนับสนุนการส่งมอบการให้บริการที่สำคัญสำหรับช่วงการปฏิบัติการทั้งหมด (เช่น ระหว่างการถูกคุกคาม/โจมตี ระหว่างการกู้ฟื้นคืน ระหว่างการปฏิบัติการปกติ)	
ประเด็นความเสี่ยง: การกำกับดูแล	
วัตถุประสงค์ของการควบคุม: นโยบาย วิธีการปฏิบัติงาน และกระบวนการในการจัดการและเฝ้าระวังติดตามกฎระเบียบขององค์กร กฎหมาย ความเสี่ยง สภาพแวดล้อม และข้อกำหนดด้านการปฏิบัติการ เป็นที่เข้าใจและมีการแจ้งผู้บริหารถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์	
กิจกรรมการควบคุม	**การประเมิน**
มีการกำหนดนโยบายด้านความมั่นคงปลอดภัยของข้อมูลขององค์กร	
บทบาทและภาระหน้าที่ด้านความมั่นคงปลอดภัยทางข้อมูล ประสานกัน และเป็นไปในทิศทางเดียวกับบทบาทภายในและหุ้นส่วนภายนอก	
มีความเข้าใจและมีการจัดการเกี่ยวกับข้อกำหนดกฎหมายและกฎเกณฑ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งความเป็นส่วนตัวและด้านเสรีภาพของพลเมือง	
การกำกับดูแลและกระบวนการบริหารความเสี่ยงมีการกล่าวถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์	

หน้าที่: ระบุ (ต่อ)	
ประเด็นความเสี่ยง: การประเมินความเสี่ยง	
วัตถุประสงค์ของการควบคุม: องค์กรมีความเข้าใจถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ต่อการปฏิบัติการขององค์กร(รวมถึงพันธกิจ หน้าที่ ภาพพจน์หรือชื่อเสียง) สินทรัพย์ขององค์กรและบุคลากร	
กิจกรรมการควบคุม	**การประเมิน**
มีการระบุและบันทึกจุดอ่อนของสินทรัพย์	
มีการได้รับข้อมูลข่าวสาร เกี่ยวกับภัยคุกคามทางไซเบอร์และจุดอ่อน มาจากแหล่งต่างๆ	
มีการระบุและบันทึกภัยคุกคามทั้งจากภายในและภายนอก	
มีการระบุผลกระทบทางธุรกิจที่อาจเกิดขึ้นรวมถึงโอกาสที่จะเกิด	
มีการคำนึงถึงภัยคุกคาม ความอ่อนแอ/จุดอ่อน โอกาสที่จะเกิด และผลกระทบ ในการกำหนดความเสี่ยง	
มีการระบุและจัดลำดับความสำคัญของการตอบสนองต่อความเสี่ยง	
ประเด็นความเสี่ยง: กลยุทธ์การบริหารความเสี่ยง	
วัตถุประสงค์ของการควบคุม: มีการกำหนดการจัดลำดับความสำคัญขององค์กร ข้อจำกัด ความเสี่ยงที่ยอมรับได้และสมมุติฐานโดยสิ่งเหล่านี้ถูกนำมาใช้ในการสนับสนุนการตัดสินใจด้านความเสี่ยงของการปฏิบัติการ	
กิจกรรมการควบคุม	**การประเมิน**
มีการกำหนดให้มีกระบวนการบริหารความเสี่ยง ได้รับการจัดการ และผู้มีส่วนได้เสียขององค์กรเห็นชอบ	
มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (risk tolerance) ขององค์กร และมีการแสดงออกอย่างชัดเจน	
บทบาทของความเสี่ยงที่ยอมรับได้ (risk tolerance) ที่มีอยู่ในโครงสร้างพื้นฐานที่สำคัญและในการวิเคราะห์ความเสี่ยงเฉพาะกลุ่มอุตสาหกรรมบางกลุ่ม จะบอกถึงค่าความเสี่ยงที่ยอมรับได้ (determination of risk tolerance) ขององค์กร	
ประเด็นความเสี่ยง: การบริหารจัดการห่วงโซ่อุปาทาน	
วัตถุประสงค์ของการควบคุม: มีการกำหนดลำดับความสำคัญ ข้อจำกัด ความเสี่ยงที่ยอมรับได้ขององค์กร รวมทั้งสมมุติฐานต่างๆ โดยสิ่งเหล่านี้จะถูกนำมาใช้ในการสนับสนุนการตัดสินใจด้านความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการห่วงโซ่อุปาทาน องค์กรมีกระบวนการในการระบุ ประเมิน และจัดการความเสี่ยงที่มีในห่วงโซ่อุปาทาน	
กิจกรรมการควบคุม	**การประเมิน**
กระบวนการบริหารจัดการความเสี่ยงที่เกี่ยวกับไซเบอร์ ในห่วงโซ่อุปาทาน ได้ถูกระบุ จัดให้มี ประเมิน จัดการและได้รับความเห็นชอบจากผู้มีส่วนได้เสียขององค์กร	
มีการใช้การประเมินความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องกับกระบวนการการบริหารจัดการห่วงโซ่อุปาทานในการ ระบุ จัดลำดับความสำคัญ และประเมินคู่ค้า และหุ้นส่วนของระบบข้อมูลที่มีความสำคัญ ส่วนประกอบและบริการ	
สัญญามีการกำหนดให้คู่ค้าและหุ้นส่วนดำเนินมาตรการที่เหมาะสมซึ่งออกแบบมาเพื่อที่จะบรรลุวัตถุประสงค์ของโครงการด้านความมั่นคงปลอดภัยของข้อมูล หรือแผนการบริหารความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องกับกระบวนการการบริหารจัดการห่วงโซ่อุปาทาน	
มีการเฝ้าติดตามคู่ค้าและหุ้นส่วนเพื่อจะยืนยันว่า เขาทั้งหลายเหล่านั้นปฏิบัติตามข้อกำหนดตามที่ต้องการได้อย่างน่าพึงพอใจ มีการสอบทานการตรวจสอบ ข้อสรุปของผลการทดสอบหรือการประเมินคู่ค้า/ผู้จัดหาด้วยวิธีการอื่นๆ ที่เทียบเท่า	
การวางแผนการตอบสนองและการกู้คืนรวมทั้งการทดสอบ ได้ถูกนำไปใช้กับคู่ค้า/ผู้จัดหาที่มีความสำคัญ	

หน้าที่: การป้องกัน	
ประเด็นความเสี่ยง: การบริหารเอกลักษณ์ การควบคุมด้านการยืนยันตัวตน และการเข้าถึง	
วัตถุประสงค์ของการควบคุม: มีการจำกัดการเข้าถึงสินทรัพย์ทั้งผ่านทางกายภาพ และผ่านทางระบบ รวมทั้งสิ่งอำนวยความสะดวกที่เกี่ยวข้องให้แก่ผู้ใช้งานที่ได้รับมอบอำนาจ กระบวนการ และเครื่องมือ และได้รับการจัดการให้สอดคล้องกับความเสี่ยงจากการเข้าถึงกิจกรรมและธุรกรรมต่างๆ ที่ได้รับอนุญาต โดยไม่ได้รับอนุญาต	
กิจกรรมการควบคุม	**การประเมิน**
มีการออกเอกลักษณ์และสิทธิ โดนมีการจัดการ ยืนยันความถูกต้อง เรียกคืน ตรวจสอบ เครื่องมือผู้ใช้งานและกระบวนการที่ได้รับอนุญาต	
มีการบริหารจัดการและป้องกันการเข้าถึงสินทรัพย์ทางกายภาพ	
มีการบริหารจัดการการเข้าถึงจากระยะไกล	
มีการบริหารจัดการการให้สิทธิในการเข้าถึง โดยคำนึงถึงหลักของการให้สิทธิขั้นต่ำสุดและการแบ่งแยกหน้าที่	
มีการป้องกันความสมบูรณ์ถูกต้องของเครือข่ายโดยคำนึงถึงการแบ่งแยกเครือข่ายตามความเหมาะสม	
มีการยืนยันตัวตนตามสิทธิที่กำหนดไว้ และให้มีการยืนยันกันโดยทางปฏิสัมพันธ์ ตามความเหมาะสม	
ประเด็นความเสี่ยง: การสร้างความตระหนักรู้ และการฝึกอบรม	
วัตถุประสงค์ของการควบคุม: มีการให้ความรู้เพื่อการตระหนักถึงภัยคุกคามด้านไซเบอร์ให้กับบุคลากรและหุ้นส่วนขององค์กร และมีการให้การฝึกอบรมอย่างเพียงพอเพื่อปฏิบัติหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลโดยสอดคล้องกับนโยบาย วิธีการปฏิบัติงาน และสัญญาต่างๆ ที่เกี่ยวข้อง	
กิจกรรมการควบคุม	**การประเมิน**
มีการแจ้งและฝึกอบรมผู้ใช้งานทั้งหมด	
ผู้ใช้งานที่ได้รับสิทธิพิเศษมีความเข้าใจในบทบาทและภาระหน้าที่	
ผู้มีส่วนได้เสียที่เป็นบุคคลที่สามเช่น ผู้ขาย คู่ค้า ลูกค้า และหุ้นส่วน มีความเข้าใจในบทบาทและภาระหน้าที่	
ผู้บริหารระดับสูงมีความเข้าใจในบทบาทและภาระหน้าที่	
เจ้าหน้าที่ด้านความมั่นคงปลอดภัยทางกายภาพและข้อมูลมีความเข้าใจในบทบาทและภาระหน้าที่	
ประเด็นความเสี่ยง: ความมั่นคงปลอดภัยด้านข้อมูล	
วัตถุประสงค์ของการควบคุม: มีการจัดการข้อมูลและการบันทึกข้อมูลเป็นไปตามกลยุทธ์การบริหารความเสี่ยงขององค์กรในการป้องกันความลับ ความสมบูรณ์ถูกต้อง และความพร้อมใช้งานของข้อมูล	
กิจกรรมการควบคุม	**การประเมิน**
มีการปกป้องข้อมูลระหว่างการส่ง (Data-in-transit)	
มีการจัดการสินทรัพย์อย่างเป็นทางการโดยตลอด ตั้งแต่การถอนออก เคลื่อนย้าย และการตัดจำหน่าย	
มีความสามารถเพียงพอในการทำให้แน่ใจว่า มีความพร้อมในการใช้งาน	
มีการนำเอาวิธีปฏิบัติในการป้องกันการรั่วไหลของข้อมูลไปดำเนินการ	
มีการใช้กลไกในการตรวจสอบความถูกต้องสมบูรณ์ เพื่อที่จะยืนยันซอฟต์แวร์ เฟิร์มแวร์ และความถูกต้องสมบูรณ์ของข้อมูล	
มีการแบ่งแยกสภาพแวดล้อมในการพัฒนาและทดสอบออกจากสภาพแวดล้อมที่ใช้งานจริง	
มีการใช้กลไกในการตรวจสอบความถูกต้องสมบูรณ์เพื่อที่จะยืนยันความถูกต้องสมบูรณ์ของ Hardware	

หน้าที่: การป้องกัน (ต่อ)	
ประเด็นความเสี่ยง: กระบวนการและวิธีการปฏิบัติในการป้องกันข้อมูล	
วัตถุประสงค์ของการควบคุม: มีการคงไว้และนำนโยบายด้านความมั่นคงปลอดภัย (ซึ่งกล่าวถึง วัตถุประสงค์ ขอบเขต บทบาท หน้าที่ความรับผิดชอบ ความรับผิดชอบของผู้บริหาร และการประสานงานกันระหว่างหน่วยงานในองค์กร) กระบวนการ และวิธีการปฏิบัติ มาใช้ในการบริหารจัดการการป้องกันระบบข้อมูลและสินทรัพย์	
กิจกรรมการควบคุม	**การประเมิน**
มีการจัดทำและปรับปรุงค่าพื้นฐานของการกำหนดค่า configuration ของระบบควบคุมเทคโนโลยีสารสนเทศ/อุตสาหกรรม โดยคำนึงถึงหลักการของความมั่นคงปลอดภัยที่เหมาะสม (เช่นแนวคิดการให้สิทธิตามความจำเป็น (least functionality)	
มีการนำวงจรชีวิตการพัฒนาระบบ (System Development Life Cycle) มาปฏิบัติ	
มีกระบวนการควบคุมด้านการเปลี่ยนแปลงการตั้งค่า configuration	
มีการสำรองข้อมูล เก็บรักษา และให้มีการทดสอบนำกลับมาใช้เป็นระยะ	
มีการปฏิบัติตามกฎเกณฑ์เกี่ยวกับสภาพแวดล้อมการปฏิบัติการทางกายภาพสำหรับสินทรัพย์ขององค์กร	
การทำลายข้อมูลเป็นไปตามนโยบาย	
มีการปรับปรุงกระบวนการป้องกันอย่างต่อเนื่อง	
ประสิทธิผลของเทคโนโลยีการป้องกัน มีแบ่งปันให้กับผู้ที่เกี่ยวข้องอย่างเหมาะสม	
มีและบริหารจัดการแผนการตอบสนอง (การตอบสนองต่อเหตุการณ์ความเสี่ยงและความต่อเนื่องทางธุรกิจ) และแผนการกู้คืน (การกู้คืนจากเหตุการณ์ความเสี่ยงและหายนะ)	
มีการทดสอบการตอบสนองและการกู้คืน	
เรื่องความมั่นคงปลอดภัยทางไซเบอร์ได้ถูกรวมไว้ในวิธีปฏิบัติทางทรัพยากรบุคคล เช่นการลดสิทธิของผู้ใช้งาน และการคัดสรรบุคลากร	
มีการพัฒนาแผนการบริหารจัดการความอ่อนแอ/จุดอ่อนและมีการนำแผนไปลงมือปฏิบัติ	
ประเด็นความเสี่ยง: การบำรุงรักษา	
วัตถุประสงค์ของการควบคุม: มีการบำรุงรักษาและซ่อมแซมตามการควบคุมในทางอุตสาหกรรม และองค์ประกอบของระบบข้อมูลมีการดำเนินการตามนโยบายและและวิธีปฏิบัติ	
กิจกรรมการควบคุม	**การประเมิน**
มีการบำรุงรักษาและซ่อมแซมสินทรัพย์ขององค์กรและบันทึกในระยะเวลาที่เหมาะสมด้วยเครื่องมือที่ได้รับการอนุมัติและมีการควบคุม	
การบำรุงรักษาสินทรัพย์ขององค์กรจากระยะไกลได้รับการอนุมัติ บันทึกและปฏิบัติเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่มีสิทธิ	

หน้าที่: การป้องกัน (ต่อ)	
ประเด็นความเสี่ยง: เทคโนโลยีในการป้องกัน	
วัตถุประสงค์ของการควบคุม: มีการจัดการแก้ปัญหาด้านเทคนิคของความมั่นคงปลอดภัยเพื่อให้แน่ใจว่าความมั่นคงปลอดภัยและความยืดหยุ่นของระบบและสินทรัพย์เป็นไปตามนโยบาย วิธีปฏิบัติและสัญญา	
กิจกรรมการควบคุม	**การประเมิน**
มีการกำหนดและปฏิบัติการบันทึกการตรวจสอบ/กิจกรรมรวมทั้งมีการสอบทานตามนโยบาย	
มีการปกป้องสิ่งที่ถอดออกได้ และจำกัดการใช้งานให้เป็นไปตามนโยบาย	
หลักการของการให้สิทธิขั้นต่ำสุด (ตามความจำเป็น) ผนวกด้วยการตั้งค่าระบบโดยให้สิทธิตามความจำเป็นในการใช้งานเท่านั้น	
มีการป้องกันการสื่อสารและการควบคุมทางเครือข่าย	
ระบบมีการปฏิบัติตามหน้าที่ที่ได้กำหนดไว้ล่วงหน้าตามแต่ละช่วงสถานการณ์ เพื่อให้มีความพร้อมใช้งานได้ (เช่น ภายใต้การข่มขู่คุกคาม การโจมตี การกู้คืน และการปฏิบัติงานตามปกติ)	

หน้าที่: การตรวจหา	
ประเภทความเสี่ยง: ความผิดปกติ และเหตุการณ์	
วัตถุประสงค์ของการควบคุม: เหตุการณ์ความผิดปกติถูกตรวจพบในเวลาที่เหมาะสมพร้อมทั้งมีความเข้าใจถึงผลกระทบที่อาจเกิดขึ้นได้จากเหตุการณ์	
กิจกรรมการควบคุม	**การประเมิน**
มีการวิเคราะห์เหตุการณ์ที่ตรวจจับได้เพื่อเข้าใจถึงเป้าหมายและวิธีการโจมตี	
ข้อมูลเหตุการณ์จะถูกรวบรวมและดูความเชื่อมโยงจากแหล่งข้อมูลและและอุปกรณ์ตรวจจับหลายแห่ง	
มีการพิจารณาผลกระทบของเหตุการณ์	
มีการกำหนดระดับที่ควรมีการแจ้งเตือนเหตุการณ์ความเสี่ยง	
ประเด็นความเสี่ยง: การเฝ้าระวังติดตามด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง	
วัตถุประสงค์ของการควบคุม: มีการเฝ้าระวังติดตามข้อมูลและสินทรัพย์ในช่วงเวลาที่เหมาะสม เพื่อที่จะระบุเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ และเพื่อที่จะประเมินความมีประสิทธิผลของมาตรการป้องกัน	
กิจกรรมการควบคุม	**การประเมิน**
มีการเฝ้าระวังติดตามด้านครือข่ายเพื่อตรวจหาเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นได้	
มีการเฝ้าระวังติดตามสภาพแวดล้อมทางกายภาพเพื่อตรวจหาเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นได้	
มีการเฝ้าระวังติดตามกิจกรรมของบุคลากรเพื่อตรวจหาเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นได้	
มีการตรวจพบ code ที่ประสงค์ร้าย	
มีการตรวจพบ mobile code ที่ไม่ได้รับอนุญาต	
มีการเฝ้าระวังติดตามกิจกรรมของผู้ให้บริการภายนอกเพื่อตรวจหาเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นได้	
มีการเฝ้าระวังติดตามการเชื่อมต่อของบุคลากร เครื่องมือ และ software ที่ไม่ได้รับอนุญาต	
มีการ scan ตรวจหาจุดอ่อน	
ประเด็นความเสี่ยง: กระบวนการตรวจหา	
วัตถุประสงค์ของการควบคุม: มีการคงไว้ของกระบวนการและวิธีการปฏิบัติของการตรวจหาและมีการทดสอบ เพื่อให้แน่ใจในการตระหนักถึงเหตุการณ์ความผิดปกติอย่างทันเวลาเพียงพอ	
กิจกรรมการควบคุม	**การประเมิน**
มีการกำหนดบทบาทและภาระหน้าที่ในการตรวจหาอย่างชัดเจนเพื่อให้แน่ใจถึงความรับผิดชอบที่มี	
กิจกรรมการตรวจหาเป็นไปตามข้อกำหนดที่เกี่ยวข้อง	
มีการทดสอบกระบวนการตรวจหา	
มีการสื่อสารข้อมูลการตรวจพบเหตุการณ์ไปยังผู้ที่เกี่ยวข้อง	
มีการปรับปรุงกระบวนการตรวจหาอย่างต่อเนื่อง	

หน้าที่: การตอบสนอง	
ประเด็นความเสี่ยง: การวางแผนการตอบสนอง	
วัตถุประสงค์ของการควบคุม: กระบวนการและวิธีการปฏิบัติของการตอบสนองได้ถูกนำไปปฏิบัติและรักษาไว้เพื่อให้แน่ใจว่ามีการตอบสนองอย่างทันท่วงทีต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ตรวจพบ	
กิจกรรมการควบคุม	**การประเมิน**
แผนการตอบสนองถูกนำไปใช้ในระหว่างหรือภายหลังเกิดเหตุการณ์	
ประเด็นความเสี่ยง: การสื่อสาร	
วัตถุประสงค์ของการควบคุม: มีการประสานงานกิจกรมการตอบสนองกับผู้มีส่วนได้เสียทั้งภายในและภายนอกตามความเหมาะสม รวมถึงการสนับสนุนภายนอกจากหน่วยงานบังคับใช้กฎหมาย	
กิจกรรมการควบคุม	**การประเมิน**
บุคลากรรู้ถึงบทบาทหน้าที่และลำดับของการปฏิบัติการเมื่อต้องมีการตอบสนอง	
มีการรายงานเหตุการณ์ที่เป็นไปตามเกณฑ์ที่ตั้งไว้	
มีการแชร์ข้อมูลที่เป็นไปตามแผนการตอบสนอง	
การประสานงานกับผู้มีส่วนได้เสียเกิดขึ้นเป็นไปตามแผนการตอบสนอง	
มีการแบ่งปันข้อมูลโดยสมัครใจกับผู้มีส่วนได้เสียภายนอกเพื่อให้มีการตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่กว้างขึ้น	
ประเด็นความเสี่ยง: การวิเคราะห์	
วัตถุประสงค์ของการควบคุม: มีการวิเคราะห์เพื่อให้แน่ใจว่ามีการตอบสนองอย่างเพียงพอและสนับสนุนกิจกรรมการกู้คืน	
กิจกรรมการควบคุม	**การประเมิน**
มีการสอบสวนเมื่อได้รับการแจ้งเตือนจากระบบตรวจหา	
มีความเข้าใจถึงผลกระทบของเหตุการณ์ความเสี่ยง	
การตรวจสอบเชิงนิติวิทยาศาสตร์	
มีการจัดประเภทเหตุการณ์ความเสี่ยงตามแผนการตอบสนอง	
ประเด็นความเสี่ยง: การบรรเทา	
วัตถุประสงค์ของการควบคุม: มีการดำเนินการเพื่อป้องกันการขยายตัวของเหตุการณ์ บรรเทาผลกระทบที่เกิดขึ้นและกำจัดเหตุการณ์ความเสี่ยง	
กิจกรรมการควบคุม	**การประเมิน**
มีการจำกัดเหตุการณ์ความเสี่ยง	
มีการบรรเทาเหตุการณ์ความเสี่ยง	
มีการบรรเทาความเสี่ยงของจุดอ่อนที่เพิ่งถูกระบุใหม่ หรือมีการบันทึกความเสี่ยงที่ได้ยอมรับ	
ประเภทความเสี่ยง: การปรับปรุง	
วัตถุประสงค์ของการควบคุม: มีการปรับปรุงการตอบสนองขององค์กรโดยนำบทเรียนจากการตรวจพบหรือการตอบสนองจากทั้งในอดีตและปัจจุบันมาพิจารณา	
กิจกรรมการควบคุม	**การประเมิน**
มีการรวมบทเรียนที่ได้รับไปในแผนการตอบสนอง	
มีการปรับกลยุทธ์การตอบสนองให้เป็นปัจจุบัน	

หน้าที่: การกู้คืน	
ประเด็นความเสี่ยง: แผนการกู้คืน	
วัตถุประสงค์ของการควบคุม: กระบวนการและวิธีการปฏิบัติของการกู้คืนได้ถูกนำไปปฏิบัติและรักษาไว้เพื่อให้แน่ใจว่ามีการทำให้ระบบหรือสินทรัพย์ฟื้นคืนอย่างทันท่วงทีจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์	
กิจกรรมการควบคุม	**การประเมิน**
แผนการกู้คืนได้ถูกนำไปใช้ในระหว่าง หรือภายหลังเหตุการณ์	
ประเภทความเสี่ยง: การปรับปรุง	
วัตถุประสงค์ของการควบคุม: มีการปรับปรุงแผนและกระบวนการกู้คืนโดยรวมบทเรียนที่ได้รับมาพิจารณากิจกรรมในอนาคต	
กิจกรรมการควบคุม	**การประเมิน**
มีการรวมบทเรียนที่ได้รับเข้าไปในแผนกู้คืน	
มีการปรับกลยุทธ์การกู้คืนให้เป็นปัจจุบัน	
ประเภทความเสี่ยง: การสื่อสาร	
วัตถุประสงค์ของการควบคุม: มีการประสานงานกิจกรรมการกู้คืนกับทั้งภายในและภายนอกเช่น ศูนย์ประสานงาน ผู้ให้บริการอินเตอร์เน็ต เจ้าของระบบที่ถูกโจมตี ผู้เสียหาย ทีมตอบสนองต่อความมั่นคงปลอดภัยทางคอมพิวเตอร์อื่นๆ และผู้ขาย	
กิจกรรมการควบคุม	**การประเมิน**
มีการจัดการด้านการประชาสัมพันธ์	
มีการชี้แจงเพื่อกอบกู้ชื่อเสียงหลังจากเกิดเหตุการณ์	
มีการสื่อสารกิจกรรมการกู้คืนกับผู้มีส่วนได้เสียภายในและคณะผู้บริหารระดับสูง	

ภาคผนวก ง วิธีปฏิบัติที่เป็นเลิศของ CERT เพื่อบรรเทาภัยคุกคามจากภายใน

ตารางข้างล่างนี้มีปรากฏอยู่ใน "แนวทางพื้นฐานในการบรรเทาภัยคุกคามจากภายใน พิมพ์ครั้งที่ 5" ซึ่งเขียนโดย CERT® แห่งศูนย์ภัยคุกคามจากภายใน ซึ่งอยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (SEI) ของมหาวิทยาลัยคาร์เนกี้ เมลลอน สหรัฐอเมริกา วิธีปฏิบัติที่เป็นเลิศทั้ง 20 ข้อนี้ มีความมุ่งหมายที่จะให้เป็นที่อ้างอิงขององค์กรซึ่งต้องการจะจัดทำหรือ ปรับปรุงโครงการภัยคุกคามจากภายในให้เป็นปัจจุบัน และควรจะต้องมีการปรับแก้ให้เข้ากับ ความต้องการ วัฒนธรรมและความเสี่ยงที่ยอมรับได้ขององค์กร การจัดลำดับของแนวปฏิบัติที่เป็นเลิศของ CERT นี้ตั้งใจที่จะทำให้กระบวนในการนำโครงการภัยคุกคามจากภายในไปปฏิบัตินั้นง่ายขึ้น

วิธีปฏิบัติที่เป็นเลิศทั้ง 20 ข้อนี้ เป็นข้อความหรือวัตถุประสงค์การควบคุมที่อยู่ในระดับสูง และในแต่ละวิธีปฏิบัติก็ได้มีการแตกเป็นข้อย่อยที่เป็นกิจกรรมการควบคุมที่เฉพาะเจาะจงไว้ในแนวปฏิบัตินี้

ลำดับ	แนวปฏิบัติที่เป็นเลิศ
1	รู้จักและป้องกันสินทรัพย์ที่สำคัญของท่าน
2	พัฒนาโครงการภัยคุกคามจากภายในที่เป็นทางการ
3	มีเอกสารที่ชัดเจนและมีการบังคับใช้นโยบายและวิธีการควบคุมอย่างสม่ำเสมอ
4	เริ่มจากกระบวนการจ้างงาน การเฝ้าติดตาม และตอบโต้พฤติกรรมที่น่าสงสัยหรือก้าวร้าว
5	คาดการณ์และจัดการกับปัญหาที่ก่อให้เกิดผลในทางลบในสภาพแวดล้อมการทำงาน
6	พิจารณาภัยคุกคามจากภายในและหุ้นส่วนทางธุรกิจในกระบวนการประเมินความเสี่ยงทั่วทั้งองค์กร
7	ควรให้ความระแวดระวังเป็นพิเศษในเรื่อง Social Media
8	มีการกำหนดโครงสร้างทางการบริหารและงานต่างๆ เพื่อที่จะลดความเครียด และความผิดพลาดที่เกิดขึ้นโดยไม่ตั้งใจให้เหลือน้อยที่สุด
9	รวบรวมเรื่องเกี่ยวกับภัยคุกคามและภัยภายในองค์กรที่เกิดขึ้นโดยไม่ได้ตั้งใจและบรรจุไว้ในการฝึกอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยให้กับพนักงานทุกคนเป็นระยะ
10	นำนโยบายและวิธีปฏิบัติเรื่องรหัสผ่านที่เข้มงวดและการจัดการ account มาลงมือปฏิบัติ
11	จัดให้มีวิธีการควบคุมการเข้าถึงอย่างเข้มงวด รวมทั้งนโยบายการเฝ้าติดตามผู้ใช้งานที่ได้รับสิทธิพิเศษ
12	ใช้เทคโนโลยีในการติดตามกิจกรรมของพนักงานและรวบรวมข้อมูลที่สัมพันธ์กันจากแหล่งข้อมูลที่หลากหลาย
13	เฝ้าระวังติดตามและควบคุมการเข้าถึงทางไกลจากอุปกรณ์ปลายทางที่ใช้งานทั้งหมด รวมถึงอุปกรณ์ที่เคลื่อนที่ได้
14	จัดทำค่าพื้นฐาน (baseline) ของพฤติกรรมปกติสำหรับทั้งเครือข่ายและพนักงาน
15	บังคับใช้การแบ่งแยกหน้าที่และการได้รับสิทธิพิเศษขั้นต่ำสุดตามความจำเป็น
16	กำหนดข้อตกลงด้านความมั่นคงปลอดภัยที่ชัดเจนสำหรับผู้ให้บริการคลาวด์โดยเฉพาะเรื่องการจำกัดการเข้าถึงและความสามารถในการเฝ้าระวังติดตาม
17	จัดให้มีวิธีการควบคุมการเปลี่ยนแปลงระบบ
18	นำเรื่องการจัดทำสำรองเพื่อความมั่นคงปลอดภัยและกระบวนการกู้คืนมาใช้ปฏิบัติ
19	ห้ามทำการโอนถ่ายข้อมูลโดยไม่ได้รับอนุญาต
20	พัฒนาวิธีปฏิบัติอย่างครอบคลุมสำหรับพนักงานที่ถูกให้ออก

ภาคผนวก จ องค์กรและหน่วยงานที่ออกประกาศคำแนะนำ

แหล่งข้อมูลข้างล่างนี้อาจให้ข้อมูลที่ช่วยให้องค์กรระบุ เฝ้าระวังติดตาม และจัดการกับภัยคุกคามจากภายใน แม้จะไม่ใช่รายละเอียดทั้งหมด แต่แหล่งข้อมูลเหล่านี้จะช่วยให้ผู้ตรวจสอบภายในเพิ่มพูนความรู้และทักษะได้ นอกจากนี้ มาตรฐานและกฎเกณฑ์ด้านความมั่นคงปลอดภัยของอุตสาหกรรมและในประเทศก็ต้องได้รับการพิจารณาในช่วงระหว่างการวางแผนงานที่ได้รับมอบหมาย เพื่อให้แน่ใจว่า ได้มีการจัดสรรทรัพยากรให้แก่ความเสี่ยงที่มีความสำคัญที่สุดต่อองค์กรบางองค์กรโดยเฉพาะ

American National Standards Institute/ International Society of Automation

ANSI เป็นกระบอกเสียงของมาตรฐานของประเทศสหรัฐอเมริกาและระบบการประเมินความสอดคล้องกับมาตรฐานและเป็นตัวแทนอย่างเป็นทางการของอเมริกาในองค์กรสำหรับมาตรฐานสากล (International Organization for Standardization) และ International Electrotechnical Commission (IEC) โดยผ่านทาง U.S. National Committee. พันธกิจของ ANSI คือการเพิ่มขีดความสามารถในการแข่งขันในระดับสากลของอเมริกาและคุณภาพของธุรกิจอเมริกันและความเป็นอยู่ของชาวอเมริกัน โดยการส่งเสริมและสนับสนุนมาตรฐานสากลแบบสมัครใจและระบบการประเมินความสอดคล้องกับมาตรฐานรวมถึง และการปกป้องความมั่นคงของมาตรฐานเหล่านั้น. https://www.ansi.org/cyber/

Australian Government: Attorney-General's Department

กรอบนโยบายความมั่นคงปลอดภัยในเชิงป้องกัน (The Protective Security Policy Framework -- PSPF) อันประกอบไปด้วย แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของรัฐบาลออสเตรเลีย และแนวทางในการสนับสนุนการนำไปปฏิบัติอย่างมีประสิทธิผล PSPF นี้รวมถึงข้อกำหนดหลัก 3 ประการเกี่ยวกับความมั่นคงปลอดภัยด้านบุคลากรซึ่งเป็นสิ่งสำคัญในการบรรเทาภัยคุกคามอันเกิดจากคนในที่ได้รับความไว้วางใจ https://www.protectivesecurity.gov.au/personnel/Pages/default.aspx

Center for Internet Security

CIS คือองค์กรที่ไม่แสวงหากำไรซึ่งจัดทำมาตรฐานสากลและแนวปฏิบัติที่ดีสำหรับความมั่นคงปลอดภัยของระบบ IT และข้อมูล เพื่อปกป้องค์กรภาคเอกชนและภาครัฐจากภัยคุกคามด้านไซเบอร์โดยอาศัยผลงานของประชาคมด้าน IT สากลเป็นพื้นฐาน https://www.cisecurity.org

CERT Australia

CERT Australia คือทีมตอบสนองเหตุการณ์ฉุกเฉินด้านคอมพิวเตอร์แห่งชาติซึ่งตั้งขึ้นเมื่อปี 2553 CERT คือจุดติดต่อเบื้องต้นของรัฐบาลสำหรับธุรกิจหลักๆ ของออสเตรเลียเพื่อ:

- รับและตอบสนองต่อรายงานเหตุการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์
- ได้รับการสนับสนุนและคำแนะนำในการตอบสนองและบรรเทาเหตุการณ์ด้านไซเบอร์

- เฝ้าระวังติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์หรือการโจมตี เพื่อพัฒนาภาพของการคุกคาม
- ให้คำปรึกษาและแจ้งเตือนแก่หุ้นส่วนของ CERT ที่เกี่ยวข้องเพื่อที่จะเพิ่มความยืดหยุ่นด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity resilience) คือเพิ่มขีดความสามารถในการรองรับการโจมตีและสามารถให้บริการได้อย่างต่อเนื่อง

https://www.cert.gov.au/

CERT-SEI

CERT เป็นหน่วยงานหนึ่งของสถาบันวิศวกรรมซอฟต์แวร์ (SEI) ของมหาวิทยาลัยคาร์เนกี้ เมลลอน สหรัฐอเมริกา ซึ่งได้ทำการศึกษาและแก้ปัญหาที่ซับซ้อนและมีผลกระทบเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ในวงกว้าง ทำการวิจัยหาจุดอ่อนด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ซอฟต์แวร์ สนับสนุนการเปลี่ยนแปลงในระยะยาวในเรื่องระบบเครือข่าย รวทั้งทำการพัฒนาข้อมูลและการฝึกอบรมที่ทันสมัยเพื่อช่วยในการปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์ ศูนย์ภัยคุกคามจากภายในของ CERT ยังให้ข้อมูลเพื่อช่วยให้องค์กรพัฒนาและนำโครงการจัดการกับภัยคุกคามภายในไปปฏิบัติ

http://www.cert.org

CSA Singapore

- The Cyber Security Agency of Singapore (CSA) เป็นหน่วยงานระดับชาติในการดูแลกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ การปฏิบัติการ การให้การศึกษา การขยายบริการในเชิงรุกและพัฒนาระบบนิเวศในสิงคโปร์ หน่วยงานนี้เป็นส่วนหนึ่งของสำนักนายกรัฐมนตรีและอยู่ภายใต้การจัดการข
- CSA มีหน้าที่หลักๆ คือ
- การติดต่อประสานและขยายงานออกไปในวงกว้าง - ทำงานกับอุตสาหกรรมสากลและท้องถิ่นและผู้นำทางความคิด เพิ่มขีดความสามารถในการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ผ่านทางโครงการขยายความรู้ไปสู่สังคม และการส่งเสริมความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ (security-by-design)
- การพัฒนาระบบนิเวศ - พัฒนาระบบนิเวศด้านความมั่นคงปลอดภัยทางไซเบอร์ที่แข็งแกร่ง (นั่นคืออุตสาหกรรมที่โด่งดังซึ่งมีกำลังคนในการตอบสนองและบรรเทาผลกระทบจากการโจมตีทางไซเบอร์)
- การปกป้องภาคอุตสาหกรรมที่สำคัญ – เสริมความแข็งแกร่งด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับภาคอุตสาหกรรมที่สำคัญ เช่น พลังงาน น้ำ และธนาคาร
- การปฏิบัติการ - เชื่อมั่นได้ในการประสานงานและการใช้วิธีการตอบสนองภัยคุกคามด้านไซเบอร์ที่มีประสิทธิผล

https://www.csa.gov.sg

Intel® Corporation

Insider Threat Filed Guide เป็นรายงานที่ระบุ 60 เหตุการณ์การโจมตีอันเกิดจากภัยคุกคามจากภายในที่มีโอกาสเกิดขึ้นได้มาก เพื่อให้องค์กรมีแนวทางเดียวกันในการแบ่งปันข้อมูลทั้งภายในและภายนอก และทำให้เกิดประสิทธิผลมากขึ้นในเรื่องกลยุทธ์ด้านความมั่นคงปลอดภัย และการตอบสนองการโจมตีจากภายในองค์กร
https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html

Intelligence and National Security Alliance

ด้วยการเป็นพันธมิตรกับกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) สำนักงานสอบสวนกลาง (Federal Bureau of Investigation -- FBI) และ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ (Office of the Director of National Intelligence) INSA ช่วยประสานความร่วมมือของพันธมิตรระหว่างสมาชิกของภาคเอกชนและทีมประชาคมนักวิเคราะห์ข่าวกรองที่มีประสบการณ์ การให้แนวทางในการระบุและต่อต้านภัยคุกคามจากภายในเป็นหนึ่งในหน้าที่หลักที่สำคัญสูงสุดของหน่วยงานนี้
https://www.insaonline.org

International Organization for Standardization/International Electrotechnical Commission

ISO เป็นองค์กรอิสระสากลที่ไม่ใช่หน่วยงานของรัฐ มีสมาชิกจาก 161 องค์กรมาตรฐานระดับชาติ ISO นำผู้เชี่ยวชาญโดยผ่านทางสมาชิก มาแบ่งปันความรู้และพัฒนามาตรฐานสากลที่เกี่ยวข้องกับตลาดโดยความสมัครใจและใช้วิธีฉันทามติในการเห็นพ้องกัน เพื่อที่จะสนับสนุนนวัตกรรมและการแก้ปัญหาระดับโลก IEC เป็นองค์กรชั้นนำระดับโลกสำหรับการจัดทำและเผยแพร่มาตรฐานสากลสำหรับเทคโนโลยีไฟฟ้า (ที่เกี่ยวกับไฟฟ้า อิเล็กทรอนิคส์และเทคโนโลยีที่เกี่ยวข้อง) IEC มีการประสานงานกับ ISO ตามความเหมาะสมเพื่อให้แน่ใจว่ามาตรฐานสากลเข้ากันได้อย่างดี และสนับสนุนส่งเสริมซึ่งกันและกัน
https://www.iso.org

INTERPOL

INTERPOL (ตำรวจสากล) เป็นองค์กรตำรวจระหว่างประเทศที่ใหญ่ที่สุดในโลก มีสมาชิก 192 ประเทศINTERPOL เผยแพร่แนวทางทั่วไปเกี่ยวกับอาชญากรรมทางไซเบอร์และอาชญากรรมที่ใช้ไซเบอร์เข้ามาช่วย
https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

National Institute of Standards and Technology

NIST's Cybersecurity Framework เป็นชุดของมาตรฐานและแนวปฏิบัติที่ดีซึ่งถูกสร้างขึ้นจากความร่วมมือระหว่างภาครัฐและเอกชนเพื่อที่จะช่วยองค์กรจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ กรอบฉบับนี้ใช้ภาษาทั่วๆ ไป เพื่อที่จะกล่าวถึงและจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์โดยให้เกิดความคุ้มค่าตามความต้องการของธุรกิจ https://www.nist.gov/cyberframework

ภาคผนวก ฉ ข้อมูลอ้างอิงและแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลข้างล่างนี้ อาจให้ข้อมูลที่จะช่วยให้องค์กรระบุ เฝ้าระวังติดตาม และจัดการภัยคุกคามจากภายในได้ แม้จะไม่ใช่ทั้งหมด แต่ก็พอจะช่วยให้ผู้ตรวจสอบภายในเพิ่มพูนความรู้และทักษะได้ นอกจากนี้แล้ว ผู้ตรวจสอบภายในยังต้องคำนึงถึงมาตรฐานและกฎระเบียบด้านความปลอดภัยของอุตสาหกรรมในช่วงของการวางแผนสำหรับงานที่ได้รับมอบหมาย เพื่อที่จะได้มั่นใจว่า ได้มีการจัดสรรทรัพยากรไปให้แก่ความเสี่ยงที่สำคัญต่อองค์กรเฉพาะบางประเภทอุตสาหกรรมแล้ว

ข้อมูลอ้างอิง

CERT Insider Threat Center. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Pittsburgh, PA: Carnegie Mellon University, 2016. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

CERT Insider Threat Center. Unintentional Insider Threats: Social Engineering. Pittsburgh, PA: Carnegie Mellon University, 2014. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf.

INSA. “Insider Threat Program Roadmap.” https://www.insaonline.org/insider-threat-roadmap/. National Cybersecurity and Communications Integration Center. U.S. Department of Homeland Security, Combating the Insider Threat. Washington, DC: DHS/US-CERT, 2014. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf.

Ponemon Institute ©. 2018 Cost of Insider Threats: Global. New York, NY: ObservIT 2018. https://www.observeit.com/ponemon-report-cost-of-insider-threats/.

Stoneburner, Gary; Alice Goguen, and Alexis Feringa. National Institute of Standards and Technology (NIST), Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.

International Professional Practices Framework, 2017 Edition. Lake Mary, FL: The Institute of Internal Auditors, 2017.

Trzeciak, Randy, and Dan Costa. Model-Driven Insider Threat Control Selection. Pittsburgh, PA: Carnegie Mellon University, 2017.
https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_509187.pdf.

แหล่งข้อมูลเพิ่มเติม

American National Standards Institute/International Society of Automation. ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an

Industrial Automation and Control Systems Security Program. https://tinyurl.com/ANSI-ISA-62443-2-1.

American National Standards Institute/International Society of Automation. ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels. https://tinyurl.com/ANSI-ISA-62443-3-3.

A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector. https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/.

Australian Government Attorney-General's Department. 13 Ongoing assessment of personnel. เข้าดูเมื่อ June 27, 2018, https://www.protectivesecurity.gov.au/personnel/ongoing-assessment-of-personnel/Pages/default.aspx.

Center for Internet Security. CIS Critical Security Controls™ for Effective Cyber Defense (CIS Controls). https://www.cisecurity.org/controls/.

CERT Australia. Insider threat: Beyond technical controls. March 26, 2018. https://www.cert.gov.au/news/insider-threat-beyond-technical-controls.

Costa, Daniel. "CERT Definition of 'Insider Threat' – Update." Insider Threat Blog, Carnegie Mellon University Software Engineering Institute, SEI Insights. March 7, 2017. https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html.

Intel® Corporation. Insider Threat Field Guide. https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 27001: 2013, Information Technology — Security Techniques — Information Security Management Systems — Requirements. https://www.iso.org/standard/54534.html.

Miller, Sarah. ""The Frequency and Impact of Insider Collusion," Insider Threat Blog, Carnegie Mellon University Software Engineering Institute, SEI Insights, June 22, 2016. https://insights.sei.cmu.edu/insider-threat/2016/06/the-frequency-and-impact-of-insider-collusion.html.

National Institute of Standards and Technology. NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Ponemon Institute©. 2017 Cost of Cyber Crime Study. New York, NY: Accenture, 2017. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.

Ponemon Institute©. 2016 Cost of Cyber Crime Study. Traverse City, MI: Ponemon Institute, 2016. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

กิตติกรรมประกาศ

ทีมงานพัฒนาแนวปฏิบัติ

Himi Tina Kim, CIA, CGAP, CRMA, United States (Chairman)

Joseph Keating, United States

Michael Lynn, CRMA, United States

Sajay Rai, United States

Terence Washington, CIA, CRMA, United States

ผู้ให้คำแนะนำแนวปฏิบัติที่มาจากทั่วโลก (Global Guidance Contributors)

Jared Hoffman, United States

Yadeli Ibarra, CISA, Mexico

Brad McGary, United States

Phillip Nemmers, CISA, United States

Patricia Rowe Seale, CIA, CRMA, CISA, CRISC, Barbados

Andriy Rybalchenko, CISA, CISM, Ukraine

Deb Snyder, United States

มาตรฐานและแนวทางปฏิบัติระดับสากลของ IIA

Eva Sweet, CISA, CISM, IT and PS Director, (Project Lead)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President

Debi Roth, CIA, Managing Director

Anne Mercer, CIA, QIAL, Director

Jeanette York, CCSA, FS Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

IIA ใคร่ขอขอบคุณคณะผู้มีหน้าที่กำกับดูแลที่ให้การสนับสนุน อันได้แก่ คณะอนุกรรมการจัดทำแนวปฏิบัติเกี่ยวกับเทคโนโลยีสารสนเทศ (Information Technology Guidance Committee) สภาที่ปรึกษาเกี่ยวกับแนวปฏิบัติในทางวิชาชีพ (Professional Guidance Advisory Council) คณะกรรมการมาตรฐานการตรวจสอบภายในสากล (International Internal Audit Standards Board) คณะกรรมการกำกับดูแลหน้าที่และจริยธรรมในทางวิชาชีพ (Professional Responsibility and Ethics Committee) และ และสภาผู้ดูแลกรอบการปฏิบัติงานวิชาชีพสากล (International Professional Practices Framework Oversight Council)

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

DISCLAIMER

COPYRIGHT

August 2018

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org