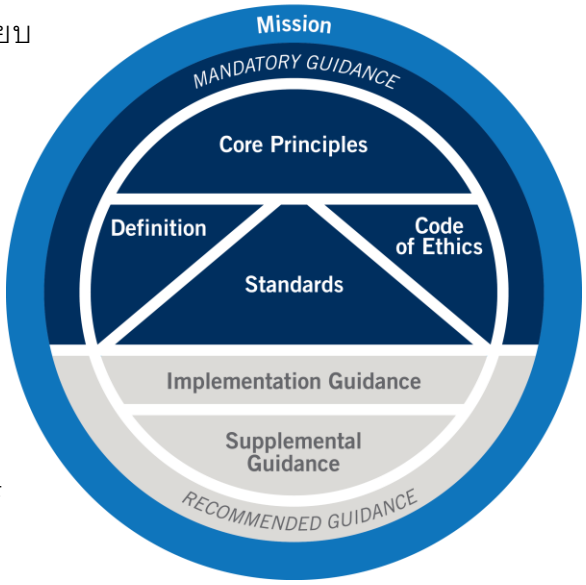
การตรวจสอบการบริหาร
การระบุตัวตนและการเข้าถึง

พิมพ์ครั้งที่ 2

The Institute of Internal Auditors | Global

เกี่ยวกับ IPPF

กรอบโครงสร้างการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (International Professional Practices Framework® หรือ IPPF®) เป็นกรอบแนวคิดที่จัดระเบียบแนวทางปฏิบัติที่เชื่อถือได้ซึ่งประกาศใช้โดย IIA สำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายในทั่วโลก



แนวทางภาคบังคับ (**Mandatory Guidance**) ได้รับการพัฒนาตามกระบวนการสอบทานมาเป็นอย่างดีตามที่ได้ถูกกำหนดไว้ซึ่งรวมถึงช่วงที่เปิดเผยต่อสาธารณะเพื่อที่ผู้มีส่วนได้ส่วนเสียจะได้ให้ข้อมูลความคิดเห็นได้ องค์ประกอบภาคบังคับของ IPPF ประกอบไป:

- หลักการพื้นฐานที่สำคัญ (Core principles) สำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน
- คำจำกัดความ (Definition) ของการตรวจสอบภายใน
- ประมวลจรรยาบรรณ (Code of Ethics)
- *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (Standards)*

แนวทางที่แนะนำจะประกอบไปด้วย แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guidance) และแนวทางเสริม (Supplemental Guidance) แนวทางการนำมาตรฐานไปใช้ปฏิบัติได้รับการออกแบบมาเพื่อช่วยให้ผู้ตรวจสอบภายในเข้าใจว่าจะนำเอาข้อกำหนดต่างๆ ในแนวทางภาคบังคับไปประยุกต์ใช้และปฏิบัติให้สอดคล้องกับข้อกำหนดเหล่านั้นได้อย่างไร

เกี่ยวกับแนวทางเสริม (Supplemental Guidance)

แนวทางเสริมจะให้ข้อมูลเพิ่มเติม คำแนะนำ และวิธีปฏิบัติที่เป็นเลิศสำหรับการปฏิบัติงานให้บริการตรวจสอบภายใน เอกสารนี้จะช่วยสนับสนุน*มาตรฐาน* โดยได้ระบุประเด็นต่างๆ ตามหัวข้อ และประเด็นของแต่ละธุรกิจเฉพาะอย่าง โดยให้รายละเอียดมากกว่าแนวทางการนำมาตรฐานไปใช้ปฏิบัติและได้รับการรับรองโดย IIA โดยผ่านกระบวนการการทบทวนและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวปฏิบัติ (Practice Guides)

แนวปฏิบัติเป็นรูปแบบหนึ่งของแนวทางเสริม ซึ่งจะให้วิถีทางโดยละเอียด กระบวนการแต่ละขั้นตอน พร้อมทั้งตัวอย่างที่จะช่วยสนับสนุนผู้ตรวจสอบภายในทุกคน บางแนวปฏิบัติจะเน้นไปที่:

- การให้บริการทางการเงิน
- ภาครัฐ
- เทคโนโลยีสารสนเทศ (GTAG®)

สำหรับภาพรวมข้อมูลเกี่ยวกับเอกสารของแนวปฏิบัติที่จัดทำโดย IIA โปรดดูได้ที่ www.globaliia.org/standards-guidance.

เกี่ยวกับ GTAGs

ภายในแนวทางเสริมของ IPPF แนวการตรวจสอบเทคโนโลยีในระดับสากล (GTAGs) ให้ความรู้แก่ผู้ตรวจสอบภายในในการให้บริการให้ความเชื่อมั่นและให้คำปรึกษาที่เกี่ยวข้องกับความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ (IT) ขององค์กรและความปลอดภัยของสารสนเทศ (IS) มาตรฐานซึ่งเป็นที่มาของ GTAGs มีดังต่อไปนี้

- 1210.A3 – ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและวิธีการควบคุมหลักของ เทคโนโลยีสารสนเทศ รวมทั้งเทคนิคการตรวจสอบด้วยเทคโนโลยีสารสนเทศเพื่อให้ปฏิบัติงานที่ได้รับมอบหมายได้ อย่างไรก็ตาม ใช่ว่าผู้ตรวจสอบภายในทุกคนที่จำเป็นต้องมีความเชี่ยวชาญเทียบเท่ากับผู้ตรวจสอบภายในที่รับผิดชอบงานตรวจสอบเทคโนโลยีสารสนเทศโดยตรง
- 2110.A2 – หน่วยงานตรวจสอบภายในต้องประเมินว่าการกำกับดูแลด้านเทคโนโลยีสารสนเทศของ องค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่
- 2130.A1 – หน่วยงานตรวจสอบภายในต้องประเมินความเพียงพอและประสิทธิผลของวิธีการควบคุม ในการตอบสนองต่อความเสี่ยงที่มีอยู่ในการกำกับดูแล การปฏิบัติงาน และระบบสารสนเทศขององค์กร เกี่ยวกับ:
    - การบรรลุวัตถุประสงค์เชิงกลยุทธ์ขององค์กร
    - ความเชื่อถือได้และความถูกต้องของสารสนเทศทางการเงินและการปฏิบัติงาน
    - ความมีประสิทธิผลและประสิทธิภาพของการปฏิบัติงานและโครงการต่างๆ (Programs)
    - ความปลอดภัยของสินทรัพย์และ
    - การปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ นโยบาย วิธีการปฏิบัติงาน (Procedures) และ สัญญา
- 2220.A1 – ขอบเขตของงานที่ได้รับมอบหมายต้องรวมถึงการคำนึงถึงสิ่งต่างๆ ที่เกี่ยวข้อง ได้แก่ ระบบงาน การบันทึกข้อมูล บุคลากร และทรัพย์สินที่จับต้องได้รวมทั้งทรัพย์สินที่อยู่ในความควบคุมดูแลของกลุ่มบุคคลที่สาม

สารบัญ

บทสรุปสำหรับผู้บริหาร

การบริหารการระบุตัวตนและการเข้าถึง (IAM) จะครอบคลุมนโยบาย กระบวนการ และเครื่องมือเพื่อให้แน่ใจว่าผู้ใช้สามารถเข้าถึงทรัพยากรเทคโนโลยีสารสนเทศ (IT) ได้อย่างเหมาะสม วิธีการควบคุม IAM จำเป็นต้องมีอยู่ในทุกที่ ที่มีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ซึ่งกำหนดให้มีการอนุญาตสิทธิที่แตกต่างกันหรือความสามารถในการติดตามการกระทำต่างๆ ที่ได้ทำไป กระบวนการ IAM อาจต้องมีการประสานงานระหว่างบุคลากรและระบบต่างๆ ในฝ่ายทรัพยากรบุคคล หน่วยธุรกิจอื่นๆ และไอที

โดยพื้นฐานแล้ว IAM ประกอบด้วยวัตถุประสงค์ทางการ**ควบคุม** 3 ประการ:

1. ***อัตลักษณ์/ตัวตน (Identity)*** – *คุณเป็นใคร?* **ตัวระบุตัวตน** (identifiers) ที่เป็นดิจิทัล (IDs) อาจถูกสร้างขึ้นสำหรับบุคคล กลุ่ม และกระบวนการที่กำหนดโดยระบบ แต่ละ ID ควรสามารถตรวจสอบย้อนกลับได้หรือมีพนักงานเพียงคนเดียวเป็นเจ้าของเพื่อให้มั่นใจได้ในเรื่องความรับผิดชอบ (accountability)
2. ***การอนุมัติ (Authorization)*** – *คุณสามารถทำอะไรในระบบนี้ได้บ้าง?* วัตถุประสงค์นี้กำหนดให้ต้องมีการประสานงานระหว่าง**ผู้ดูแลระบบ** (โดยปกติคือไอที) หน่วยธุรกิจหลักที่ได้รับประโยชน์ (มักเรียกว่า**เจ้าของธุรกิจ**) รวมทั้งผู้ใช้ขั้นปลายและหัวหน้างาน ซึ่งจะเกี่ยวข้องกับการกำหนดสิทธิที่เหมาะสมสำหรับหน้าที่ในงานต่างๆ และทำให้แน่ใจได้ว่าแต่ละ ID ที่กำลัง**ขอสิทธิการเข้าถึง**ได้รับการตอบสนองที่เหมาะสม กระบวนการอนุมัติซ้ำและปิดการใช้งานบัญชีผู้ใช้อาจต้องมีการประสานงานระหว่างฝ่ายทรัพยากรบุคคล หน่วยธุรกิจ และไอที
3. ***การยืนยันตัวตน (Authentication)*** – *คุณใช่คนที่คุณอ้างว่าเป็นหรือไม่?* กลไกการควบคุม เช่น รหัสผ่าน รหัสเข้าใช้ชั่วคราว หรือข้อมูลไบโอเมตริกซ์อาจถูกใช้เพื่อยืนยันตัวตนของบุคคลหรือกระบวนการที่กำลังพยายามเข้าถึงสิทธิที่กี่ยวข้องกับ ID หนึ่ง ปัจจัยการยืนยันตัวตนมักถูกกำหนดให้เป็นสิ่งที่คุณรู้ (เช่น รหัสผ่าน) สิ่งที่คุณมี (เช่น โทรศัพท์มือถือ) หรือสิ่งที่คุณเป็น (ข้อมูลไบโอเมตริกซ์ เช่น ลายนิ้วมือ)

วัตถุประสงค์การควบคุมที่สำคัญอื่นๆ ที่เกี่ยวข้องกับ IAM ได้แก่:

4. ***การบริหารความเสี่ยง*** *(Risk management) – มีการปรับใช้โซลูชัน IAM ที่เหมาะสมกับความสำคัญของแต่ละระบบหรือไม่?*

5. ***การบันทึกเหตุการณ์*** *(Event logging)– ระบบกำลังบันทึกเหตุการณ์ที่เกี่ยวข้องกับด้านความปลอดภัย เช่น การเปิดใช้งานหรือปิดใช้งานบัญชีผู้ใช้ ความพยายามเข้าสู่ระบบ และการเปลี่ยนแปลงการอนุญาตหรือไม่?*

6. ***การเฝ้าติดตามเหตุการณ์ในบันทึก*** *(Log monitoring)– บันทึกเหตุการณ์ที่เกี่ยวกับความปลอดภัยมีความปลอดภัยและมีการเฝ้าติดตามดูเพื่อตรวจจับกิจกรรมที่ผิดปกติหรือไม่?*

หมายเหตุ: ในขณะที่การจัดการการเข้าถึงทางกายภาพคือวัตถุประสงค์หลัก แนวทางฉบับนี้จะเน้นที่การเข้าถึงของ**ผู้ใช้งาน**ในการเข้าถึงทรัพยากรและเทคโนโลยีสารสนเทศ ซึ่งบางครั้งเรียกว่าการเข้าถึงเชิงตรรกะ สำหรับวัตถุประสงค์ของแนวปฏิบัติฉบับนี้ “การเข้าถึง” จะมีความหมายเหมือนกับการเข้าถึงเชิงตรรกะสำหรับกลุ่มผู้ใช้

ผู้มีส่วนได้ส่วนเสีย เช่น ผู้บริหารระดับสูงและ**คณะกรรมการ** ต้องการ**ความเชื่อมั่น**ว่า**วิธีการควบคุมทางเทคโนโลยีสารสนเทศ** รวมถึงการบริหารจัดการการเข้าถึงทรัพยากรไอที ได้รับการออกแบบมาเป็นอย่างดีและมีการนำไปใช้ปฏิบัติได้อย่างมีประสิทธิภาพ

บทนำ

มีกรอบโครงสร้างที่ใช้กันอย่างแพร่หลายมากมายที่ให้คำอธิบายเกี่ยวกับวิธีการควบคุม IAM ได้แก่ COBIT 2019 ของ ISACA การตีพิมพ์พิเศษจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The National Institute of Standards and Technology หรือ NIST) และ " Center for Internet Security Top 20 Controls & Resources " สำหรับการรักษาความปลอดภัยในโลกไซเบอร์

หมายเหตุ: ภาคผนวก ก. แสดงรายการแหล่งทรัพยากรอื่นๆ ของ IIA ที่เกี่ยวข้องกับแนวทางฉบับนี้ คำที่เป็นตัวหนาได้มีคำอธิบายไว้แล้วในภาคผนวก ข.

แนวปฏิบัติฉบับนี้จะอ้างอิงถึงวิธีการควบคุมบางอย่างที่ได้บรรยายไว้ในกรอบโครงสร้างเหล่านี้ เพื่อช่วยให้ผู้อ่านเข้าใจแนวคิด แต่จะไม่อธิบายถึงการควบคุมและวิธีการควบคุมย่อยซ้ำอีกทั้งหมด ผู้อ่านแนวปฏิบัติฉบับนี้จะถูกถือว่ามีความรู้โดยทั่วไปเกี่ยวกับ**ความเสี่ยง**และวิธีการควบคุมด้านไอทีและด้านความปลอดภัยของข้อมูล (information security--IS) ตามที่ได้อธิบายไว้ในแนวการตรวจสอบเทคโนโลยีสารสนเทศระดับโลก (Global Technology Audit Guide หรือ GTAG) เรื่อง "ไอทีที่จำเป็นสำหรับผู้ตรวจสอบภายใน (IT Essentials for Internal Auditors)" และควรรวมเอาการทบทวนข้อความฉบับเต็มของกรอบการควบคุมด้านไอที (IT-IS control frameworks) ตั้งแต่หนึ่งกรอบขึ้นไปเข้าไปในการวางแผนการตรวจสอบและแนวการทดสอบด้วย

กระบวนการ IAM จะสร้างตัวระบุผู้ใช้งาน (user IDs) ที่เป็นดิจิทัลและการอนุญาตใช้ทรัพยากรไอทีที่เกี่ยวข้อง และสอบทานว่าคำขอเข้าถึงและการดำเนินการภายในระบบนั้นกระทำโดยเจ้าของบัญชีผู้ใช้งานและไม่ใช่ผู้แอบอ้างIDs อาจถูกสร้างให้แก่ พนักงาน คู่สัญญา บุคลากรของผู้ขาย ลูกค้า เครื่องจักร และโปรแกรมต่างๆ ซึ่งโดยพื้นฐานแล้วก็จะเป็นหน่วยงานที่ต้องการเข้าถึงระบบเพื่อการดำเนินการทางธุรกิจเครื่องมือที่องค์กรอำนวยความสะดวกในการเข้าถึงของผู้ใช้ (แต่ก็จำกัดไว้เฉพาะสิ่งที่จำเป็นในการปฏิบัติหน้าที่ ที่ได้รับอนุญาตเท่านั้น)ทำให้เกิดพื้นฐานของ IAM

ประเภทของ Ids

แนวคิดการควบคุม IAM ถูกนำมาใช้กับบัญชีที่มนุษย์เป็นผู้ใช้ รวมทั้งฟังก์ชันหรือบริการที่ตั้งโปรแกรมไว้ที่อาจกำหนด IDs โดยระบบ (mechanized ID)เพื่อเข้าถึงทรัพยากรไอที ในแนวปฏิบัติฉบับนี้ คำว่า ID ใช้กับ IDs ทุกประเภทประเภท เว้นแต่จะระบุไว้เป็นอย่างอื่น

วิธีการควบคุมการบริหารจัดการการระบุตัวตนและการเข้าถึงเป็นการควบคุมขั้นพื้นฐานมากๆ สำหรับ**การกำกับดูแลด้านไอที**และการบรรลุผลสำเร็จของกลยุทธ์และวัตถุประสงค์ด้านไอทีขององค์กรซึ่งหน่วยงาน

ตรวจสอบภายในจะต้องตรวจสอบว่าองค์กรมีการควบคุมการเข้าถึงอย่างไร ทำความเข้าใจว่ากระบวนการอาจถูกนำไปใช้ทั่วทั้งองค์กรหรือเฉพาะกับบางทรัพยากรหรือในบางสภาพแวดล้อมไม่ใช่ทรัพยากรทางไอทีทั้งหมดที่ต้องการการปกป้องในระดับเดียวกัน ดังนั้นวิธีการควบคุม IAM จึงได้รับการออกแบบมาเป็นอย่างดีเพื่อให้เหมาะสมกับแต่ละชั้นความปลอดภัยของแต่ละระบบ ตลอดจน**ความเสี่ยง**ที่เกี่ยวข้องกับการทุจริตหรือ**การปฏิบัติตาม**กฎระเบียบทางการ

การควบคุม IAM ถูกนำมาใช้ในทุกๆ ชั้นของทรัพยากรไอที ซึ่งรวมถึงอุปกรณ์โครงสร้างพื้นฐานด้านเครือข่าย (เช่น สวิตช์ เราเตอร์ และระบบการจัดการเครือข่าย) เซิร์ฟเวอร์ ฐานข้อมูล บริการ**มิดเดิลแวร์** และ**แอปพลิเคชัน**องค์กรทุกขนาดต้องเผชิญกับความท้าทายของ IAM ส่วนใหญ่ก็มาจากการขยายจำนวนและความหลากหลายของทรัพยากรไอที รวมทั้งกระบวนวิธีในเข้าถึงด้วย ในการออกแบบการนำไปใช้งาน และดำเนินวิธีการควบคุม IAM ที่มีประสิทธิผลนั้น ผู้ดูแลระบบ หน่วยธุรกิจ และผู้ใช้ขั้นปลายต้องร่วมมือและยึดมั่นในหลักการของการให้สิทธิน้อยที่สุด (least privilege) ซึ่งระบุว่าการเข้าถึงระบบจะจำกัดให้เฉพาะเท่าที่จำเป็นต่อการปฏิบัติหน้าที่ในทางธุรกิจที่ได้รับอนุมัติเท่านั้น

ในการเริ่มต้นการประเมินวิธีการควบคุม IAM ผู้ตรวจสอบภายในมักจะระบุทรัพยากรไอทีบางอย่าง หรือชั้นหรือกลุ่มของทรัพยากรที่จะตรวจสอบ แล้วจึงทำความเข้าใจในบริบททางธุรกิจสำหรับสินทรัพย์นั้น จากนั้นอาจดำเนินการประเมินความเสี่ยงในระบบที่อยู่ในขอบเขตเพื่อปรับแต่งแนวการตรวจสอบสำหรับงานที่ได้รับมอบหมาย ในระหว่างขั้นตอนการวางแผนและการปฏิบัติงานภาคสนาม ผู้ตรวจสอบภายในอาจแนะนำว่าองค์กรจะสามารถเพิ่มประสิทธิผลของวิธีการควบคุม IAM ได้อย่างไร ซึ่งจะเป็นการช่วยลดความเสี่ยงด้านความปลอดภัยและการปฏิบัติกฎระเบียบได้ ตามแนวทางนี้ ผู้ตรวจสอบภายในจะแสดงให้เห็นได้ถึงการปฏิบัติตาม **มาตรฐาน** 1220 – ความระมัดระวังในทางวิชาชีพ

มาตรฐาน 1220 – ความระมัดระวังในทางวิชาชีพ

ผู้ตรวจสอบภายในต้องปฏิบัติหน้าที่ด้วยความระมัดระวัง และใช้ทักษะเยี่ยงผู้ตรวจสอบภายในที่มีความรู้ความสามารถและความสุขุมรอบคอบอย่างพอเหมาะพอควร อย่างไรก็ตาม ความระมัดระวังในทางวิชาชีพไม่ได้หมายความถึงการกระทำที่ปราศจากข้อผิดพลาดใดๆ เลย

วัตถุประสงค์

แนวปฏิบัติฉบับนี้จะช่วยให้ผู้อ่าน:

- เข้าใจความหมายของ IAM และพัฒนาความรู้เพื่อใช้ในการทำงานของกระบวนการที่เกี่ยวข้อง ซึ่งรวมถึง**การกำกับดูแล**และวิธีการควบคุมความปลอดภัยที่เกี่ยวข้อง

- เข้าใจความเสี่ยงและโอกาสที่เกี่ยวข้องกับ IAM
- เข้าใจองค์ประกอบของกระบวนการ IAM ซึ่งประกอบด้วย การสร้างIDs การจัดการและการอนุมัติให้สิทธิการเข้าถึง และการคงไว้ซึ่งการบังคับใช้โดยผ่านทางการยืนยันตัวตน (authentication) การสอบทานการอนุมัติซ้ำ และกระบวนการปิดใช้งานบัญชีโดยอัตโนมัติ
- เข้าใจข้อควรคำนึงและกลยุทธ์บางประการสำหรับการนำการควบคุม IAM ไปใช้
- เข้าใจพื้นฐานของการตรวจสอบ IAM ซึ่งรวมถึงวิธีการควบคุมเฉพาะอย่างที่จะต้องประเมิน

องค์ประกอบของ IAM

ในส่วนนี้จะให้คำอธิบายสั้นๆ เกี่ยวกับ วิธีการควบคุมอัตลักษณ์/ตัวตน การอนุมัติ และการยืนยันตัวตน โดยอ้างอิงถึงกรอบการควบคุมของ IAM ตามความเหมาะสม คำจำกัดความโดยละเอียดของวิธีการควบคุมมีอยู่ในเอกสารซึ่งเป็นแหล่งที่ใช้อ้างอิง

อัตลักษณ์/ตัวตน (Identity)

หนึ่งในเอกสารที่ดีสำหรับการทำความเข้าใจความเสี่ยงและวัตถุประสงค์ในการควบคุมที่เกี่ยวข้องกับการสร้าง IDs ของระบบคือ *NIST Special Publication (SP) 800-63 Digital Identity Guidelines* (PDF) เอกสารดังกล่าวระบุว่า “อัตลักษณ์ที่เป็นดิจิทัลเป็นตัวแทนเฉพาะของสิ่งใดสิ่งหนึ่ง” และ “กระบวนการและเทคโนโลยีในการสร้างและใช้อัตลักษณ์ที่เป็นแบบดิจิทัลทำให้เกิดโอกาสมากมายสำหรับการปลอมตัวบุคคลอื่นและการโจมตีอื่นๆ”[1] ดังนั้น การสร้าง การบริหารจัดการ และความปลอดภัยของ IDs จึงเป็นวัตถุประสงค์ในการควบคุมหลักสำหรับทรัพยากรไอทีทุกรายการที่ต้องการการอนุญาตที่แตกต่างกันไป กลุ่มเอกสารที่เกี่ยวข้องกับ NIST SP 800-63 ยอมรับว่าไม่ใช่ IDs ของระบบทุกระบบที่อาจต้องติดตามย้อนกลับไปยังบุคคลที่ได้รับการยืนยันได้ อย่างไรก็ตาม สำหรับงานตรวจสอบที่ได้รับมอบหมายส่วนใหญ่ที่เกี่ยวกับ IAM จะกำหนดขอบเขตตามความเสี่ยง ซึ่งจะเน้นที่กระบวนการและวิธีการควบคุมที่จำเป็นต้องมีการสอบยัน IDs เป็นรายบุคคลหรือ IDs ที่สร้างโดยระบบ (mechanized IDs) เทียบกับเจ้าของตามเอกสารเพื่อให้แน่ใจได้ถึงความรับผิดชอบสำหรับการกระทำต่างๆ ภายในระบบ

ผู้ออกแบบระบบจะกำหนดประเภทของ IDs ที่จำเป็นสำหรับทรัพยากรไอทีแต่ละรายการเพื่อให้เป็นไปตามวัตถุประสงค์ทางธุรกิจ ในขณะที่ผู้ดูแลระบบจะสร้างและจัดการ IDs ระบบให้เป็นไปตามความต้องการที่ได้กำหนดไว้ โดยปกติแล้ว ผู้ดูแลระบบมักจะทำงานร่วมกับเจ้าของทรัพยากรซึ่งเป็นหน่วยธุรกิจเพื่อนำกระบวนการที่บันทึกการระบุตัวตนของบุคคลหรือบุคคลที่รับผิดชอบ IDs ที่สร้างโดยระบบไปใช้ปฏิบัติ

1. Paul Grassi, Michael Garcia, James Fenton, NIST SP 800-63-3 Digital Identity Guidelines, NIST, iv, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

IDs เครือข่าย (Network Identity)

ในสภาพแวดล้อมที่ใช้ไอทีทั่วทั้งองค์กร การสร้าง IDs เครือข่าย (ซึ่งจำเป็นสำหรับการเข้าถึงเครือข่ายข้อมูลขององค์กร) เป็นการควบคุมขั้นพื้นฐาน ซึ่งโดยทั่วไปแล้วจะดำเนินการสำหรับบุคคลในระหว่างกระบวนการต้อนรับพนักงานใหม่ ผู้ดูแลระบบเครือข่ายอาจสร้าง IDs ที่สร้างโดยระบบหรือ IDs เพื่อวัตถุประสงค์พิเศษ (เช่น IDs ของผู้ดูแลระบบที่จะใช้เฉพาะเมื่อบุคคลนั้นทำหน้าที่เป็นผู้ดูแลระบบที่ได้รับอนุมัติเท่านั้น)

ID เครือข่ายมักถูกใช้โดยแอปพลิเคชันที่ทำงานบนเครือข่ายข้อมูลในกระบวนการที่เรียกว่า**การรวมศูนย์**หรือ federation (บางครั้งเรียกว่า การลงชื่อเข้าใช้เพียงครั้งเดียว หรือ single sign-on) วิธีนี้จะยอมให้แอปพลิเคชันพึ่งพาวิธีการควบคุมที่ใช้ในการสร้างและจัดการ IDs เครือข่าย แอปพลิเคชันทางธุรกิจที่ไม่ได้กำหนดให้ผู้ใช้ขั้นปลาย (ที่ Log-in เข้าสู่ระบบเครือข่ายข้อมูลขององค์กร) ต้องป้อน**ข้อมูลประจำตัว**ด้วยเพื่อล็อกอินเข้าสู่แอปพลิเคชันนั้น--หรือแอปพลิเคชันที่ต้องใส่ IDs เครือข่ายและรหัสผ่านของผู้ใช้เพื่อล็อกอินเข้าสู่ระบบ--จะถูกรวมเข้ากับ (federated with) IDs เครือข่ายและกระบวนการยืนยันตัวตนได้ในระดับหนึ่ง

การรวม IDs เข้าด้วยกัน (Federation of IDs) มีประโยชน์โดยเฉพาะสำหรับการเปิดใช้งานและปิดใช้งานบัญชีผู้ใช้โดยอัตโนมัติ เนื่องจาก IDs เครือข่ายมักจะเชื่อมโยงกับฐานข้อมูลทรัพยากรบุคคลของตัวตนที่สอบยัน (พนักงานและคู่สัญญา) และสถานะปัจจุบันของพวกเขา ตัวอย่างเช่น เมื่อใดก็ตามที่พนักงานหรือคู่สัญญาได้ถูกบอกเลิกสัญญาอย่างเป็นทางการ (และสถานะการจ้างงานของพวกเขาถูกเปลี่ยนในฐานข้อมูลเป็นเลิกจ้าง) สถานะ ID เครือข่ายก็จะระงับการใช้งานเช่นกัน และสถานะของ ID ก็จะไม่สามารถใช้งานได้ในทันทีสำหรับแอปพลิเคชันทั้งหมดที่เชื่อมต่อกับภายนอก (federated applications)

การระบุตัวตนเฉพาะอุปกรณ์หรือแอปพลิเคชัน (Device- or Application-specific Identity)

ทรัพยากรไอทีที่ไม่ได้ใช้ ID ร่วมกับ ID เครือข่ายจะต้องมีการสร้าง ID ผู้ใช้ที่โดยปกติมักจะมีความเสี่ยงและวัตถุประสงค์ในการควบคุมเดียวกันกับของ ID เครือข่าย ที่สำคัญคือ ถ้าความรับผิดชอบ (accountability) ต่อการกระทำที่ทำในระบบเป็นหนึ่งในวัตถุประสงค์การควบคุม ดังนั้น จะต้องมีการสร้าง ID ที่ไม่ซ้ำกันและไม่แบ่งกันใช้ และเชื่อมโยงกับหรือมีบุคคลซึ่งได้รับการยืนยันเป็นเจ้าของระบบที่ไม่เชื่อมต่อกับภายนอกต้องมีการกำหนดให้ผู้ใช้เข้าสู่ระบบด้วย ID และรหัสผ่านที่ไม่ผูกติดอยู่กับ ID เครือข่ายแอปพลิเคชันที่อยู่บนคลาวด์อาจจะมี ID รวมศูนย์หรือไม่ก็ได้

แอปพลิเคชันที่ไม่เชื่อมต่อกับภายนอก (Nonfederated applications) มีวิธีการควบคุม IAM ที่มีความเสี่ยงโดยธรรมชาติมากกว่าที่เชื่อมต่อ เนื่องจากโดยทั่วไปแล้วผู้ดูแลระบบและผู้บังคับบัญชาของผู้ใช้ขั้นปลายมักจะไม่ตรวจสอบหรือจัดการ IDs อย่างเข้มข้นดังเช่นที่กระบวนการด้านทรัพยากรมนุษย์ทำ นอกจากนี้ข้อมูลอภิพันธุ์ (metadata) [หมายเหตุผู้ทบทวน: หมายถึง ข้อมูลหรือสารสนเทศที่ถูกจัดทำขึ้นอย่างมี

โครงสร้างเพื่อใช้ในการบรรยายทรัพยากรสารสนเทศ ในด้านลักษณะเนื้อหา และบริบทที่เกี่ยวข้อง] ของผู้ใช้ (เช่น สถานะการจ้างงานและหน้าที่งานในปัจจุบัน) จำเป็นต้องมีการอัปเดตด้วยมือในระบบที่ไม่ติดต่อกับภายนอก (nonfederated system) ในการตรวจสอบ IAM สำหรับอุปกรณ์หรือแอปพลิเคชันที่ไม่ติดต่อกับภายนอก ผู้ตรวจสอบภายในจะประเมินความแข็งแกร่งของกระบวนการที่ใช้ตรวจสอบข้อมูลเฉพาะบุคคลที่เกี่ยวข้องกับแต่ละ ID ของระบบ (รวมถึง IDs ที่สร้างโดยระบบ) และตรวจสอบว่ากระบวนการสอบยันสถานะปัจจุบันของพนักงานและผู้ใช้ที่ไม่ใช่พนักงานมีความเพียงพอหรือไม่

การอนุมัติและการยืนยันความถูกต้อง (Approval and Validation)

คำร้องขอสร้างข้อมูลเพื่อระบุตัวตน มักจะต้องผ่านกระบวนการอนุมัติและการยืนยันความถูกต้อง ซึ่งใน NIST SP 800-63[2] เรียกว่า "การตรวจพิสูจน์(proofing)" คำขอมี ID จะได้รับการอนุมัติโดยหัวหน้าของผู้ขอหรือพนักงานผู้รับผิดชอบที่ได้รับมอบหมาย การยึดถือและปฏิบัติตามข้อกำหนดในเรื่องการตรวจพิสูจน์ตามที่กำหนดไว้อาจได้รับการสอบยันความถูกต้องโดยอัตโนมัติ เช่น ทันทีที่กรอกแบบฟอร์ม I-9 ตรวจสอบสิทธิในการหางาน (I-9 employment eligibility verification[3]) เสร็จสิ้นหรือดำเนินการด้วยมือโดยบุคคลอื่นที่ไม่ใช่หัวหน้างานของผู้ขอ เพื่อให้แน่ใจว่ามี**การแบ่งแยกหน้าที่**อย่างเพียงพอ

การอนุมัติ (Authorization)

กระบวนการในการกำหนดว่าระบบใดที่ ID หนึ่ง จะสามารถเข้าถึงได้และระดับสิทธิใดที่ ID นั้นมีอยู่ในแต่ละระบบซึ่งเป็นที่รู้จักกันว่าเป็นการอนุมัติ กระบวนการอนุมัติจะถูกกำหนดโดย**กฎเกณฑ์ทางธุรกิจ (business rules)** และอาจเป็นแบบอัตโนมัติในกระบวนการรับพนักงานใหม่ หรืออาจต้องมีการแทรกด้วยการทำด้วยมือในระดับหนึ่ง ตัวอย่างเช่น การให้บัญชีอีเมลสำหรับทุก ID เครือข่ายที่เกี่ยวข้องกับมนุษย์ในระหว่างการรับพนักงานใหม่เป็นตัวอย่างของกระบวนการอนุมัติโดยอัตโนมัติ ตามกรอบโครงสร้าง COBIT ฉบับปี 2019 เรื่อง การกำกับดูแลและวัตถุประสงค์ทางการบริหาร *(Framework: Governance and Management Objectives)* ได้อธิบายกิจกรรมการอนุมัติไว้ที่ภายใต้หัวข้อ DSS06.03 – หัวข้อ จัดการบทบาท ภาระหน้าที่ สิทธิการเข้า และระดับของอำนาจอนุมัติ (Manage Roles, Responsibilities, Access Privileges, and Levels of Authority)

2. Grassi, Garcia, and Fenton, NIST SP 800-63-3, iv
3. "I-9, Employment Eligibility Verification," U.S. Citizenship and Immigration Services, accessed January-February 2021, https://www.uscis.gov/i-9

การกำหนดแอปพลิเคชันของผู้ใช้ (Determining a User's Applications)

โดยทั่วไปแล้ว แต่ละบุคคลมักจำเป็นต้องเข้าถึงแอปพลิเคชันทางธุรกิจตั้งแต่หนึ่งรายการขึ้นไปเพื่อปฏิบัติหน้าที่ ดังนั้นจึงจำเป็นต้องมีกระบวนการในการกำหนดกลุ่มแอปพลิเคชันใดซึ่งแต่ละบุคคลจำเป็นต้องใช้ วิธีง่ายๆ ที่ทำด้วยมือเป็นหลักคือ หัวหน้างานของบุคคลนั้นมักจะรับหน้าที่ในการกำหนดแอปพลิเคชันที่จำเป็นและอนุมัติคำขอเข้าถึงตั้งแต่แรกโดยทั่วไปแล้ว แอปพลิเคชันที่จำเป็นสำหรับแต่ละงานจะได้รับการบันทึกไว้ และหากมีแอปพลิเคชันใดรวมเข้ากับ IDs เครือข่าย การตั้งค่าผู้ใช้ใหม่ด้วยแอปพลิเคชันจะเป็นแบบอัตโนมัติ

การกำหนดบทบาทในระบบ (Defining System Roles)

เจ้าของธุรกิจที่เป็นเจ้าของทรัพยากรไอทีจะทำงานร่วมกับผู้ดูแลระบบเพื่อสร้างการอนุญาตให้สิทธิที่สัมพันธ์กับความต้องการของหน้าที่งานหรือตำแหน่งงาน ตัวอย่างเช่น บุคลากรที่ได้รับมอบหมายจากฝ่าย ดูแลลูกค้าจะทำงานร่วมกับผู้ดูแลระบบการจัดการลูกค้าสัมพันธ์เพื่อกำหนดบทบาทภายในระบบที่ตรงกับความต้องการของตัวแทนฝ่ายบริการลูกค้า หัวหน้าทีม ผู้จัดการ และกรรมการ โดยเพิ่มสิทธิพิเศษที่สอดคล้องกับหน้าที่งานตามลำดับชั้นขององค์กร ระบบจำนวนมาก เช่น แพลตฟอร์มระบบทรัพยากรขององค์กรอาจมีชุดตั้งต้นของบทบาทที่เป็นมาตรฐานโดยมีพื้นฐานมาจากวิธีปฏิบัติในทางธุรกิจทั่วไป

การกำหนด **ผู้ใช้งานที่มีสิทธิสูง** (superusers) **ผู้ดูแลระบบฐานข้อมูล** (database administrators) และบทบาทผู้ดูแลระบบหรือบทบาทของสิทธิพิเศษอื่นๆ อาจต้องได้รับการอนุมัติจากสองฝ่าย (dual authorization) ตัวอย่างเช่น จากทั้งเจ้าของธุรกิจและผู้ดูแลระบบ การกำหนดให้ใช้วิธีการอนุมัติสองฝ่ายจะห้ามผู้ดูแลระบบสร้างบทบาทใหม่แต่เพียงฝ่ายเดียว และกำหนดให้การอนุมัติสำหรับแต่ละบทบาทต้องมาจากเจ้าของธุรกิจหรือหัวหน้างานของผู้ดูแลระบบบทบาทของระบบ

หมายเหตุ: แอปพลิเคชันที่ไม่ได้ใช้การกำหนดบทบาทในระบบ จำเป็นต้องทำการอนุญาตด้วยมือให้แก่แต่ละบัญชีผู้ใช้ ซึ่งวิธีนี้มีความเสี่ยงมากกว่าปกติ เนื่องจากมีโอกาสที่จะเกิดข้อผิดพลาดได้ หรือมีการให้สิทธิที่มากเกินไปโดยเจตนา

การอนุญาตที่เกี่ยวข้อง และหน้าที่หรือตำแหน่งงานที่เกี่ยวข้องอาจบันทึกไว้เป็นเอกสาร เพื่อทำให้เกิดเป็นข้อตกลงระหว่างเจ้าของธุรกิจและผู้ดูแลระบบอย่างเป็นทางการ และเพื่อช่วยในกระบวนการกำหนดบัญชีผู้ใช้ ซึ่งรวมถึงระบบอัตโนมัติด้วย

ขั้นตอนเพิ่มเติมอีกขั้นหนึ่งที่มักจะกระทำเมื่อทำการกำหนดบทบาทของระบบคือ ให้เจ้าของธุรกิจระบุการอนุญาตที่แสดงถึงการแบ่งแยกหน้าที่ไม่เพียงพอ เป็นต้นว่า ความสามารถในการส่งและอนุมัติใบคำขอซื้อหรือบัตรลงเวลาของผู้หนึ่งผู้ใดด้วยตนเอง

มีแอปพลิเคชันหลายๆ แอปพลิเคชัน ฐานข้อมูลและเครื่องมือเป็นจำนวนมากที่มีการกำหนดให้ต้องใช้ IDs ที่ถูกสร้างโดยระบบ (mechanized IDs) เพื่อทำงานเฉพาะบางอย่างหรือเพื่อสื่อสารกับส่วนประกอบระบบที่แตกต่างกัน ตัวอย่างเช่น ระบบการจัดการฐานข้อมูลอาจกำหนดให้เซิร์ฟเวอร์ที่เป็นโฮสต์ของระบบให้มีบัญชีผู้ใช้เฉพาะที่สร้างขึ้นและใช้งานอยู่เพื่อให้ระบบฐานข้อมูลนั้นทำงานได้ ดังนั้น เจ้าของธุรกิจหรือหัวหน้างานของผู้ดูแลระบบควรบันทึกและอนุมัติบทบาทในระบบที่กำหนดขึ้นเพื่อ IDs ที่สร้างโดยระบบด้วย

การกำหนดบทบาทในระบบ (Assigning System Roles)

แนวทางหนึ่งซึ่งใช้กันทั่วไปในการให้สิทธิการเข้าถึงแก่ผู้ใช้เรียกว่า **การควบคุมการเข้าถึงตามบทบาท (role-based access control)** โดยที่ผู้เชี่ยวชาญเฉพาะด้านจะพิจารณาว่าแอปพลิเคชันใดและบทบาทใดในระบบที่จำเป็นสำหรับแต่ละตำแหน่งงานหรือหน้าที่การงานในองค์กร แล้วทำงานร่วมกับผู้ดูแลระบบเครือข่ายและเพื่อดำเนินการกระบวนการให้สิทธิ ซึ่งอาจทำด้วยมือหรือโดยอัตโนมัติในระดับหนึ่ง หรืออีกแนวทางหนึ่ง การกำหนดบทบาทสามารถกำหนดได้ด้วยมือเป็นรายบุคคลหากมีความต้องการการเข้าถึงที่แตกต่างกันในหมู่สมาชิกของหน้าที่งานเดียวกัน

คำขอมีบทบาทในระบบบางคำขอ โดยเฉพาะอย่างยิ่งคำขอที่เพิ่มสิทธิในระดับที่ค่อนข้างสูง อาจต้องมีการอนุมัติแบบสองฝ่าย (dual authorization) โดยที่ผู้บังคับบัญชาและผู้ที่ได้รับมอบหมายจากเจ้าของธุรกิจต้องทำการอนุมัติให้ผู้ใช้เข้าถึงบทบาทนั้นได้มีการนำเอาวิธีการควบคุมเพื่อป้องกันการฝ่าฝืนหลักการแบ่งแยกหน้าที่ไปใช้ปฏิบัติ ณ ที่ระดับ IDsเพื่อให้แน่ใจว่าผู้ใช้ไม่มีสิทธิที่มากจนเกินไป การเช็คสอบการฝ่าฝืนหลักการแบ่งแยกหน้าที่อาจจะทำโดยอัตโนมัติหรือผู้ที่ได้รับมอบหมายจากเจ้าของธุรกิจเป็นผู้ทำการเช็คสอบด้วยตนเอง

การจัดการบัญชีที่มีสิทธิพิเศษ (Privileged Account Management)

บัญชีที่มีสิทธิพิเศษในระดับผู้ดูแลระบบ เช่น ความสามารถในการสร้างบทบาทใหม่หรือบัญชีผู้ใช้ใหม่ หรือการแก้ไขสิทธิของบัญชีผู้ใช้ที่มีอยู่เดิมแล้ว โดยปกติ มักจะถูกกำหนดให้แก่บุคลากรด้านไอทีที่มอบหมายไว้หรือผู้ใช้ขั้นสูงที่ไม่ใช่ผู้ใช้ไอที (non-IT superusers) บ่อยครั้ง **ผู้ใช้ที่มีสิทธิพิเศษ**จะได้รับ IDs แยกไปต่างหากเพื่อใช้เฉพาะสำหรับฟังก์ชันการดูแลระบบเท่านั้น บัญชีที่มีสิทธิพิเศษเป็นเป้าหมายหลักของอาชญากรไซเบอร์ เนื่องมาจากความสามารถในการสร้าง IDs และบัญชีผู้ใช้ระบบ การยกระดับสิทธิ และการเข้าถึงฐานข้อมูล เพื่อป้องกันการสร้างหรือการเข้าถึงบัญชีที่มีสิทธิพิเศษเหล่านี้อย่างไม่เหมาะสม หลายองค์กรจึงใช้เครื่องมือการจัดการบัญชีที่มีสิทธิพิเศษเพื่ออำนวยความสะดวกในการให้สิทธิการดูแลระบบ การเฝ้าติดตาม และการบังคับใช้

กระบวนการอนุมัติซ้ำ (Reauthorization Processes)

ผู้บังคับบัญชาอาจถูกกำหนดให้ต้องอนุมัติการเข้าถึงระบบของผู้ที่รายงานตรงต่อพวกเขาเป็นระยะ เพื่อบรรเทาความเสี่ยงจากการอนุญาตที่ไม่จำเป็น ความถี่ของการอนุมัติซ้ำควรสัมพันธ์กับการจัดประเภทข้อมูลของระบบ ซึ่งหมายความว่าระบบที่มีความละเอียดอ่อนมากขึ้นก็ควรมีการอนุญาตบัญชีผู้ใช้ซ้ำบ่อยขึ้น โดยทั่วไปแล้วผู้ดูแลระบบโดยทั่วไปควรออกแบบกระบวนการและนำกระบวนการไปใช้ปฏิบัติเพื่อให้ข้อมูลแก่หัวหน้างานของผู้ใช้อย่างเพียงพอที่จะทำการตัดสินใจอนุมัติใหม่ได้อย่างมีข้อมูล ข้อมูลดังกล่าวอาจรวมถึงคำอธิบายรายละเอียดของแอปพลิเคชัน บทบาทที่เกี่ยวข้องกับผู้ใช้ และตำแหน่งงานที่คาดว่าจะรับบทบาทแต่ละบทบาท

เมื่อมีคนเปลี่ยนหน้าที่งาน ข้อกำหนดในการเข้าถึงระบบก็มักจะต้องเปลี่ยนแปลงตามไปด้วย ดังนั้น วิธีปฏิบัติที่ดีที่สุดคือต้องมีกระบวนการที่กำหนดให้หัวหน้างานคนเดิมต้องปิดการเข้าถึงที่ไม่จำเป็น และหัวหน้างานคนใหม่ก็ต้องอนุมัติการเข้าถึงสำหรับบทบาทใหม่ ตามหลักการแล้ว กระบวนการนี้ควรเป็นแบบอัตโนมัติโดยการอาศัยเครื่องมือ IAM บูรณาการเข้ากับระบบบริหารทรัพยากรบุคคล และใช้วิธีการควบคุมการเข้าถึงโดยอิงตามบทบาทให้มากที่สุดเท่าที่จะทำได้ อย่างไรก็ตาม แม้จะไม่มีเครื่องมือในการบูรณาการหรือเครื่องช่วยอำนวยความสะดวก ก็ควรบังคับใช้หลักของการให้สิทธิที่น้อยที่สุด

องค์กรหนึ่งอาจใช้เครื่องมือ IAM อย่างน้อยหนึ่งเครื่องมือเพื่ออำนวยความสะดวกหรือทำให้กระบวนการอนุญาตซ้ำเป็นแบบอัตโนมัติ ถึงแม้แอปพลิเคชันที่ไม่ได้บูรณาการเข้ากับเครื่องมือต่างๆ ก็อาจต้องใช้แนวทางการอนุญาตซ้ำด้วยมือการตรวจสอบวิธีการควบคุม IAM มักจะสอบยันว่าบัญชีที่ไม่ได้รับอนุญาตให้อนุมัติซ้ำได้ถูกปิดการใช้งานหรือไม่ นอกจากนี้ ผู้ตรวจสอบอาจมองหาความผิดปกติในตำแหน่งงานหรือฝ่ายงานในรายการบัญชีผู้ใช้และบทบาทของระบบเพื่อระบุความเสี่ยงของการอนุมัติซ้ำโดยอัตโนมัติของผู้บังคับบัญชาโดยไม่มีการพิจารณาไตร่ตรองอย่างเหมาะสม การสอบทาน ดังกล่าว อาจจำเป็นต้องมีการเปรียบเทียบรายการเข้าถึงของผู้ใช้กับข้อมูลจากฝ่ายทรัพยากรบุคคล

ข้อดีอย่างหนึ่งของกระบวนการ IAM แบบอัตโนมัติคือแอปพลิเคชันแบบบูรณาการ จะรับเอาจุดแข็งของการควบคุม (เรียกว่า**การสืบทอดการควบคุม**) ดังนั้น หากกระบวนการอัตโนมัติได้รับการตรวจสอบและพบว่าสอดคล้องกับนโยบายและขั้นตอนขององค์กรแล้ว ก็อาจไม่จำเป็นต้องทดสอบกระบวนการนั้นซ้ำอีกครั้งเมื่อได้ทำการตรวจสอบทรัพยากรที่เชื่อมต่อกับภายนอก (federated resource) แล้ว

การปิดบัญชีผู้ใช้ (Account Deactivation)

บางครั้ง จำเป็นต้องมีการปิดบัญชีผู้ใช้บางราย เนื่องมาจากการเลิกจ้าง การเปลี่ยนแปลงในหน้าที่งาน หรือเป็นเพราะไม่มีการใช้งานมาระยะหนึ่งแล้ว กฎสำหรับการปิดบัญชีที่ไม่ได้ใช้งานควรสอดคล้องกับการจำแนกข้อมูลของระบบผู้ดูแลระบบจะตั้งค่าพารามิเตอร์ควบคุมเพื่อปิดบัญชีที่ไม่มีการเข้าถึงภายในระยะเวลาที่กำหนดโดยอัตโนมัติตามความเหมาะสม หากจำเป็น ผู้ใช้สามารถขอให้บัญชีของตนเปิดใช้งานได้อีกครั้ง ทั้งนี้ ขึ้นอยู่กับการอนุมัติของหัวหน้างาน

แอปพลิเคชันที่เชื่อมต่อกับภายนอกสามารถมีหรือรับการแจ้งเตือนอัตโนมัติเมื่อมีการเปลี่ยนแปลงสถานะของ IDs ในขณะที่แอปพลิเคชันที่ไม่เชื่อมต่อกับภายนอกจะต้องอาศัยกระบวนการแจ้งเตือนแบบที่ต้องทำด้วยมือซึ่งโดยธรรมชาติแล้วจะช้ากว่าและมีความเสี่ยงมากกว่า

การยืนยันตัวตน (Authentication)

วิธีการควบคุมที่สอบยันคำขอเข้าระบบ ว่ามาจากหน่วยงานที่ได้รับอนุญาตให้ใช้บัญชีหนึ่งๆ นั้นเรียกว่าการยืนยันตัวตน (authentication) รหัสผ่านเป็นปัจจัยการยืนยันตัวตนที่คนส่วนใหญ่คุ้นเคย และในขณะที่มีแนวทางในการเพิ่มความปลอดภัยที่รหัสผ่านมีให้ ข้อบกพร่องของการใช้รหัสผ่านก็เป็นที่รู้จักอย่างกว้างขวางเช่นกัน การออกแบบการควบคุมการยืนยันตัวตนที่เพียงพอได้อธิบายไว้อย่างละเอียดใน NIST SP 800-53 Revision 5 (PDF) ในหัวข้อการระบุและการยืนยันตัวตน (identification and authentication)

ปัจจัยสำหรับการยืนยันตัวตน (Authentication Factors)

ตามที่ได้กล่าวไว้ก่อนหน้านี้ ปัจจัยการยืนยันตัวตนมักถูกกำหนดเป็นสิ่งที่คุณรู้ (เช่น รหัสผ่าน) สิ่งที่คุณมี (เช่น โทรศัพท์มือถือ) หรือสิ่งที่คุณเป็น (ข้อมูลไบโอเมตริก เช่น ลายนิ้วมือ) ผู้ออกแบบระบบและผู้ดูแลระบบจะกำหนดวิธีการยืนยันตัวตนที่เหมาะสมกับประเภทข้อมูลของทรัพยากรและความสามารถทางเทคนิค ระบบที่มีความเสี่ยงต่ำกว่าบางระบบอาจใช้การยืนยันความถูกต้องของเครือข่ายเพียงอย่างเดียวซึ่งมีการสืบทอดจุดแข็งของวิธีการควบคุมการเข้าถึงเครือข่ายอยู่แล้ว ในขณะที่ทรัพยากรหรือกระบวนการที่มีความเสี่ยงสูงกว่า (เช่น ฐานข้อมูลที่มีข้อมูลส่วนบุคคลที่สามารถใช้ระบุตัวตนได้หรือฟังก์ชันผู้ดูแลระบบ) อาจต้องใช้ขั้นตอนการยืนยันตัวตนเพิ่มขึ้นในการเข้าถึง

กระบวนการยืนยันตัวตนแบบหลายปัจจัย ต้องการเพียงหนึ่ง ID เพื่อใช้ยืนยันตัวตนมากกว่าหนึ่งประเภท ตัวอย่างเช่น หลังจากตรวจสอบ ID หนึ่งไอดีและรหัสผ่านแล้ว ระบบอาจส่งรหัสการเข้าถึงแบบชั่วคราวไปยังบัญชีอีเมลหรือโทรศัพท์มือถือที่ลงทะเบียนของผู้ใช้ซึ่งผู้ใช้ต้องป้อนรหัสนั้นก่อนจึงจะสามารถเข้าถึงระบบได้ บ่อยครั้งที่ผู้ดูแลระบบมักจะบูรณาการเครื่องมือที่มีจำหน่ายทั่วไปในการให้บริการยืนยัน

ตัวตนแบบหลายปัจจัย การจำแนกประเภทข้อมูลขององค์กรและนโยบายการปกป้องข้อมูลที่เกี่ยวข้องนั้น ตามหลักการแล้วจะก่อให้เกิดเกณฑ์สำหรับตัดสินว่าเมื่อใดที่จำเป็นต้องมีการยืนยันตัวตนแบบหลายปัจจัย และวิธีการใดบ้างที่ยอมรับได้

วิธีการควบคุมด้วยรหัสผ่าน (Password Controls)

ในแอปพลิเคชันที่มีจำหน่ายทั่วไปส่วนใหญ่ วิธีการควบคุมเพื่อเพิ่มความปลอดภัยของรหัสผ่านรวมถึง:

- *ความยาว* – องค์กรจะกำหนดจำนวนอักขระขั้นต่ำสำหรับรหัสผ่าน หลายๆ เจ้าแนะนำให้ใช้รหัสผ่านที่เป็นข้อความสั้นๆ หรือวลีเพื่อสามารถทำให้จำได้ง่ายขึ้น
- *ความซับซ้อน* – การใช้อักษรตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ต่างๆ (เช่น !, #, $, * ฯลฯ) จะเพิ่มจำนวนของค่าที่เป็นไปได้ ดังนั้น จึงยากแก่การถอดรหัสผ่าน
- *การหมดอายุและการนำกลับมาใช้ใหม่* – รหัสผ่านจะหมดอายุลงหลังจากผ่านไประยะหนึ่งตามการจำแนกประเภทข้อมูลของทรัพยากร และจะต้องแตกต่างจากรหัสผ่านเดิมมากพอสมควรเพื่อลดความเสี่ยงของการทำให้ข้อมูลส่วนตัวเสื่อมเสียได้
- *การออกจากระบบ* – IDs สามารถถูกล็อคให้ออกจากระบบชั่วคราวได้ หากมีการพยายามเข้าสู่ระบบไม่สำเร็จเกินจำนวนครั้งที่ระบุภายในระยะเวลาที่กำหนด วิธีการควบคุมนี้ช่วยลดความเสี่ยงของการพยายามถอดรหัสผ่านได้
- *การจัดเก็บและการเข้าถึง* – รหัสผ่านจะถูกเก็บไว้ในไฟล์ที่เข้ารหัสซึ่งผู้ดูแลระบบสามารถทำได้แค่การรีเซ็ตเท่านั้น แต่ไม่สามารถถอดรหัส (decrypt) ออกมาได้

เนื่องจากบ่อยครั้งที่ผู้ใช้งานอาจมีรหัสผ่านหมดอายุอยู่หลายสิบรหัสผ่าน การดูแลรักษาข้อมูลประจำตัวจึงกลายเป็นเรื่องท้าทาย ดังนั้นองค์กรอาจมีเครื่องมือสำหรับการจัดเก็บรหัสผ่านที่ปลอดภัยและดึงข้อมูลโดยผู้ใช้ หรือมีนโยบายเกี่ยวกับการใช้เครื่องมือการจัดการรหัสผ่านจากภายนอก

ปัจจัยทางกายภาพ (Physical Factors)

ในการยืนยันตัวตนแบบใช้หลายปัจจัย ปัจจัยทางกายภาพ (บางอย่างที่ผู้ใช้มี) มักจะใช้เพิ่มเติมจากรหัสผ่าน เพื่อเพิ่มระดับความปลอดภัยให้มากขึ้นเป็นพิเศษอาจมีการลงทะเบียนตัวระบุอุปกรณ์ (Device identifiers) เช่น รหัสการเข้าถึงสื่อ เพื่อให้ผู้ใช้สามารถล็อกอินเข้าสู่บัญชีในเครื่องใดเครื่องหนึ่งเท่านั้น หรืออาจติดตั้งโทเค็นของซอฟต์แวร์ (software token) เพื่อให้บริการยืนยันตัวตนและระบุอุปกรณ์ได้โดยไม่ซ้ำกัน ผู้ใช้อาจพกอุปกรณ์แยกต่างหาก เช่น โทเค็นที่เป็นกายภาพ (physical token) ที่ซิงโครไนซ์กับเครื่องสร้างโค้ดกลางหรือกับโทรศัพท์มือถือที่มีหมายเลขที่ผู้ใช้ลงทะเบียนไว้ก่อนหน้านี้

ใบรับรองดิจิทัลเป็นปัจจัยกึ่งกายภาพซึ่งใช้โดยบริการหรือโปรแกรมอัตโนมัติในกระบวนวิธีการระบุตัวตนภายใต้โครงสร้างพื้นฐานกุญแจสาธารณะ ในแง่ที่ว่าใบรับรองดิจิทัลเป็นสิ่งที่โปรแกรมนั้นมีความถูกต้องของใบรับรองดิจิทัลต้องได้รับการสอบยันกับผู้ออกใบรับรองที่เชื่อถือได้หรือกับผู้ให้บริการสอบยันใบรับรองนั้น

ชีวมิติ หรือ ไบโอเมตริกซ์ (Biometrics)

ปัจจัยทางกายภาพชนิดพิเศษคือข้อมูลที่ได้มาจากลักษณะทางกายภาพเฉพาะของบุคคล เช่น รูปแบบของลายนิ้วมือ เรตินา หรือเสียง ปัจจัยเหล่านี้จะต้องลงทะเบียนกับบริการสอบยันซึ่งอาจอยู่ในอุปกรณ์ เช่น ในกรณีของเครื่องสแกนลายนิ้วมือบนโทรศัพท์มือถือหรือบนคอมพิวเตอร์แล็ปท็อป

กลุ่มความเสี่ยงและการควบคุมที่เกี่ยวข้อง

วัตถุประสงค์ในการควบคุม IT-IS บางข้อที่เกี่ยวข้องเป็นอย่างมากกับความเสี่ยงของ IAM กล่าวโดยสรุปได้ดังต่อไปนี้

การบริหารความเสี่ยง

อาจมีผลกระทบที่สำคัญจากวิธีการควบคุม IAM ที่ไม่เพียงพอจากบุคคลภายใน แฮกเกอร์ และ "บอท (bot)" อัตโนมัติที่พยายามเข้าถึงทรัพยากรไอที กระบวนการจัดการความเสี่ยงขององค์กรตามหลักแล้วควรจะระบุระบบและข้อมูล(data) ที่มีความเสี่ยงสูงไว้โดยเป็นส่วนหนึ่งของโปรแกรมการจำแนกประเภทข้อมูลและโปรแกรมป้องกัน และกำหนดมาตรการป้องกันที่จำเป็น เช่น การควบคุมการเข้าถึงโดยอิงตามบทบาทการยืนยันตัวตนแบบหลายปัจจัย หรือการบริหารจัดการบัญชีที่มีสิทธิพิเศษ สำหรับแต่ละหมวดหมู่ กระบวนการประเมินความเสี่ยงควรระบุบริเวณที่โซลูชัน IAM มีความปลอดภัยไม่เพียงพอและจัดทำเอกสารแผนการแก้ไขหรือเหตุผลของผู้บริหารที่ยอมรับความเสี่ยงนั้น

การบันทึกเหตุการณ์

วิธีปฏิบัติที่เป็นเลิศคือ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยซึ่งรวมถึงความพยายามในการเข้าถึงทรัพยากรต่างๆ การสร้าง IDs และบัญชีผู้ใช้ระบบ (system accounts) การยกระดับบทบาทหรือสิทธิ และกิจกรรมอื่นๆ ของผู้ดูแลระบบบันทึกของเหตุการณ์ดังกล่าวมักมีข้อมูลเพียงพอ เพื่อการกำหนดความรับผิดชอบและ**การห้ามปฏิเสธความรับผิด** (nonrepudiation) ซึ่งอำนวยความสะดวกในการเฝ้าระวังและกระบวนการทางนิติเวช

การเฝ้าติดตามเหตุการณ์

การเฝ้าติดตามดูบันทึกเหตุการณ์การรักษาความปลอดภัยในเชิงรุก อาจทำให้ตรวจพบภัยคุกคามจากภายในหรือภายนอกที่พยายามเข้าถึงทรัพยากรไอทีได้ ตัวบ่งชี้อาจรวมถึงการพยายามเข้าสู่ระบบที่ไม่สำเร็จซ้ำแล้วซ้ำอีก การสร้าง IDs ที่อนุมัติด้วยตนเองหรือการยกระดับสิทธิ หรือการเปิดใช้งานและการปิดใช้งานบัญชีซ้ำๆ วิธีการควบคุมโดยการเฝ้าติดตามเหตุการณ์ในบันทึกมักจะถูกนำไปใช้โดยองค์กรรักษาความปลอดภัยข้อมูล ในระหว่างการวางแผนการตรวจสอบ IAM ผู้ตรวจสอบภายในอาจระบุว่ามีวิธีการควบคุมโดยการติดตามดูบันทึกสำหรับระบบที่มีความเสี่ยงสูงทั้งหมดอยู่หรือไม่ และวิธีการควบคุมนี้ได้รับการออกแบบมาเพื่อตรวจหารูปแบบความเสี่ยงของ IAM ที่น่าจะเป็นไปได้หรือไม่

บทสรุป

วิธีการควบคุม IAM จะปกป้องความลับและความสมบูรณ์ของระบบและข้อมูลโดยการจำกัดผู้ใช้ให้ใช้สิทธิเพียงเท่าที่จำเป็นในการดำเนินการตามที่ได้รับอนุมัติเท่านั้น ผู้ออกแบบระบบและผู้ดูแลระบบมีหน้าที่ในการวางแผนและนำเอาวิธีการควบคุม IAM ที่แข็งแกร่งพอที่จะตอบสนองความต้องการด้านความปลอดภัยของแต่ละระบบไปใช้ปฏิบัติ IDs ผู้ใช้และสิทธิที่ได้รับอนุญาตให้เข้าระบบที่เกี่ยวข้องจะได้รับการสอบทานเป็นระยะ และดำเนินการโดยอัตโนมัติเท่าที่จะเป็นไปได้ เพื่อให้แน่ใจได้ว่าสิทธิจะยังคงสอดคล้องกับความต้องการของผู้ใช้ในปัจจุบัน การบันทึกและเฝ้าติดตามดูเหตุการณ์ของ IAM และความพยายามในการเข้าถึงที่ไม่สำเร็จอาจช่วยให้วิศวกรความปลอดภัยสามารถตรวจพบการโจมตีทางไซเบอร์หรือภัยคุกคามจากภายในได้

ภาคผนวก ก. มาตรฐานและแนวปฏิบัติที่เกี่ยวข้องของ IIA

แหล่งข้อมูลของ IIA ต่อไปนี้ ได้ถูกใช้อ้างอิงตลอดแนวปฏิบัติฉบับนี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน* โปรดดูที่**แนวทางการนำมาตรฐานไปใช้ปฏิบัติ** (Implementation Guidance) ของ IIA

ประมวลจรรยาบรรณ
หลักการที่ 1: ความซื่อสัตย์ (Integrity)
หลักการที่ 2: ความเที่ยงธรรม (Objectivity)
หลักการที่ 3: การรักษาความลับ (Confidentiality)
หลักการที่ 4: ความสามารถในหน้าที่ (Competency)
มาตรฐาน
มาตรฐาน 1210 – ความเชี่ยวชาญ
มาตรฐาน 1220 – ความระมัดระวังในทางวิชาชีพ
มาตรฐาน 2110 – การกำกับดูแล
มาตรฐาน 2130 – การควบคุม
มาตรฐาน 2220 – ขอบเขตของงานที่ได้รับมอบหมาย
แนวปฏิบัติ
“GTAG: สิ่งสำคัญด้านไอทีที่จำเป็นสำหรับผู้ตรวจสอบภายใน (IT Essentials for Internal Auditors),” 2563

ภาคผนวก ข. อภิธานศัพท์

คำจำกัดความของคำศัพท์ที่มีเครื่องหมายดอกจัน ได้นำมาจากภาค "อภิธานศัพท์" ของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากลของ IIA (IIA's International Professional Practices Framework®) ฉบับปี 2560 (2017) คำจำกัดความอื่นๆ ได้ถูกกำหนดขึ้นเพื่อวัตถุประสงค์ของเอกสารนี้หรือได้มาจากแหล่งต่อไปนี้:

- Paul A. Grassi, Michael E. Garcia, and James L. Fenton,NIST SP 800-63-3: Digital Identity Guidelines, Glossary (Gaithersburg, MD: NIST,June2017),https://doi.org/10.6028/NIST.SP.800-63-3
- ISACA,Glossary, information technology terms, and definitions,accessed March 15, 2021, https://www.isaca.org/resources/glossary
- Joint Task Force, NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5, Glossary (Gaithersburg, MD: NIST, September 2020), https://doi.org/10.6028/NIST.SP.800-53r5.
- NIST Computer Security Resource Center, Glossary,accessed April 8, 2021, https://csrc.nist.gov/glossary.

สิทธิการเข้าถึง - **access rights**: การอนุญาตหรือสิทธิพิเศษที่มอบให้กับผู้ใช้ โปรแกรม หรือเวิร์กสเตชันเพื่อสร้าง เปลี่ยนแปลง ลบ หรือดูข้อมูลและไฟล์ต่าง ๆ ภายในระบบ ตามกฎที่กำหนดโดยเจ้าของข้อมูลและนโยบายการรักษาความปลอดภัยของข้อมูล [อภิธานศัพท์ของ ISACA]

แอปพลิเคชัน - **application**: โปรแกรมคอมพิวเตอร์หรือชุดโปรแกรมที่ดำเนินการประมวลผลระเบียนข้อมูลต่างๆ สำหรับฟังก์ชันเฉพาะ ซึ่งตรงกันข้ามกับโปรแกรมระบบ เช่น ระบบปฏิบัติการหรือโปรแกรมควบคุมเครือข่าย และโปรแกรมอรรถประโยชน์ เช่น คัดลอกและจัดเรียงข้อมูล [อภิธานศัพท์ของISACA]

การให้ความเชื่อมั่น - **assurance [services]***: การตรวจสอบหลักฐานอย่างเที่ยงธรรมเพื่อให้ได้มาซึ่งการประเมินกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร อย่างเป็นอิสระตัวอย่างได้แก่ การตรวจสอบทางด้านการเงิน การตรวจสอบผลการปฏิบัติงาน การตรวจสอบการปฏิบัติตามกฎระเบียบ การตรวจสอบความมั่นคงปลอดภัยของระบบต่างๆ และการตรวจสอบสถานะกิจการ (Due Diligence Engagement)

การยืนยันตัวตน - authentication: การยืนยันตัวตนของผู้ใช้ กระบวนการ หรืออุปกรณ์ ซึ่งมักเป็นข้อกำหนดเบื้องต้นในการอนุญาตให้เข้าถึงทรัพยากรในระบบ [อภิธานศัพท์ของ NIST SP 800-53, Revision5]

การอนุมัติ - authorization*:* สิทธิการเข้าถึงที่มอบให้กับผู้ใช้ โปรแกรม หรือกระบวนการ หรือการกระทำในการให้สิทธิพิเศษเหล่านั้น [อภิธานศัพท์ของ NIST SP *800-53*, Revision 5]

คณะกรรมการ – board*: คณะบุคคลในระดับสูงสุดที่ทำหน้าที่ในการกำกับดูแลองค์กร (ตัวอย่าง เช่น คณะกรรมการองค์กร (Board of Directors) คณะกรรมการกำกับดูแล (Supervisory Board) หรือ คณะกรรมการนโยบาย หรือทรัสตี (Board of Governors or Trustees) ซึ่งมีหน้าที่ในการสั่งการและ/หรือสอดส่องดูแลกิจกรรมขององค์กร และพิจารณาความรับผิดชอบในผลงานการบริหารของผู้บริหารระดับสูงถึงแม้การจัดระบบการกำกับดูแลอาจแตกต่างกันไปตามแต่ละขอบเขตอำนาจของแต่ละรัฐหรือในแต่ละภาคส่วน โดยมากแล้ว คณะกรรมการจะรวมถึงสมาชิกที่ไม่ได้มีส่วนในการบริหารหากในองค์กรไม่มีคณะกรรมการแล้ว คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้จะหมายถึง กลุ่ม คนหรือบุคคลที่ทำหน้าที่กำกับดูแลองค์กรนอกจากนั้น คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้ อาจหมายถึงคณะหรือองค์คณะอื่นใดที่ทางองค์คณะซึ่งมีหน้าที่กำกับดูแลได้มอบหมายหน้าที่บางอย่างให้ (เช่น คณะกรรมการตรวจสอบ

เจ้าของธุรกิจ - business owner: ผู้นำหน่วยธุรกิจที่ได้รับผลประโยชน์หลักจากทรัพยากรไอที เจ้าของธุรกิจจะเป็นผู้กำหนดข้อกำหนดทางธุรกิจและอนุมัติการยอมรับทรัพยากร (ดู "การอนุมัติอย่างเป็นทางการ *(*authorizing official)" ใน NIST SP 800-53, Rev. 5)

กฎเกณฑ์ทางธุรกิจ - business rules*:* การแสดงกระบวนการทางธุรกิจและข้อจำกัดที่เข้ารหัสในแอปพลิเคชันเพื่อตอบสนองความต้องการของผู้ใช้

การปฏิบัติตามกฎระเบียบ – compliance*: การยึดถือและปฏิบัติตามนโยบาย แผนงาน วิธีการปฏิบัติงาน กฎหมาย ระเบียบข้อบังคับ สัญญา ตลอดจนข้อกำหนดอื่นๆ

การควบคุม – control*: การกระทำใดๆ โดยฝ่ายบริหาร คณะกรรมการ และกลุ่มบุคคลอื่นๆ เพื่อจัดการกับความเสี่ยงและเพิ่มความเป็นไปได้ ในอันที่จะบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ ผู้บริหารจะวางแผน จัดระบบรวมทั้งกำกับและสั่งการให้เกิดการปฏิบัติอย่างเพียงพอเพื่อก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่าจะบรรลุวัตถุประสงค์และเป้าหมายได้

การสืบทอดการควบคุม – control inheritance*:* สถานการณ์ที่ระบบหรือแอปพลิเคชันได้รับการปกป้องจากวิธีการควบคุมความปลอดภัยหรือความเป็นส่วนตัว (หรือจากบางส่วนของวิธีการควบคุม) ที่ได้พัฒนา นำไปใช้ ประเมิน อนุมัติ และเฝ้าติดตามโดยหน่วยงานอื่นที่ไม่ได้เป็นผู้รับผิดชอบระบบหรือแอปพลิเคชันนั้นๆ หน่วยงานภายในหรือภายนอกองค์กรที่ระบบหรือแอปพลิเคชันนั้นตั้งอยู่ [อภิธานศัพท์ของ NIST SP 800-53 Revision 5]

ข้อมูลประจำตัว – credential*:* อ็อบเจ็กต์หรือโครงสร้างข้อมูลที่ได้รับอนุมัติให้ผูกอัตลักษณ์โดยผ่านตัวระบุตัวตน (identifier) ตั้งแต่หนึ่งตัวขึ้นไป และ (อีกทางเลือกหนึ่ง) สมาชิกอาจจะเพิ่มคุณลักษณะบางอย่างที่สมาชิกมีและควบคุมเองไปเป็นตัวยืนยันตัวตน (authenticator) อย่างน้อยหนึ่งตัวเพื่อใช้ยืนยันตัวตนของสมาชิก [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

ผู้ดูแลระบบฐานข้อมูล – database administrator: บุคคลหรือฝ่ายงานที่รับผิดชอบด้านความปลอดภัยและการจำแนกประเภทข้อมูลของข้อมูลที่ใช้ร่วมกันซึ่งจัดเก็บไว้ในระบบฐานข้อมูล หน้าที่นี้รวมถึงการออกแบบ คำจำกัดความ และการบำรุงรักษาฐานข้อมูล [อภิธานศัพท์ของ ISACA]

การบันทึกเหตุการณ์ – event logging: การบันทึกกิจกรรมของระบบตามลำดับเวลาที่เกิด เช่น ความพยายามในการเข้าถึง การสร้างบทบาท การสร้างหรือปิดใช้งานบัญชีผู้ใช้ ฯลฯ (ดู “บันทึกการตรวจสอบ” ใน NIST SP 800-53, Rev. 5)

การรวมกัน – federation: กระบวนการที่ช่วยให้สามารถถ่ายทอดข้อมูลประจำตัวและการยืนยันตัวตนผ่านชุดของระบบเครือข่าย [อภิธานศัพท์ของ NIST SP 800-63]

การทุจริต – Fraud*:* การกระทำผิดกฎหมายของบุคคลหรือองค์กรในลักษณะของการฉ้อฉลหลอกลวง ปกปิด หรือทำลายความเชื่อมั่น การกระทำเหล่านี้ไม่จำเป็นต้องเป็นการคุกคามโดยใช้ความรุนแรงหรือการใช้กำลังบังคับ การทุจริตอาจกระทำโดยกลุ่มบุคคลและองค์กร เพื่อให้ได้มาซึ่งเงินทองทรัพย์สินหรือบริการ เพื่อเลี่ยงการจ่ายเงินหรือ การสูญเสียบริการ หรือเพื่อปกป้องผลประโยชน์ของ บุคคลหรือผลประโยชน์ทางธุรกิจ

การกำกับดูแล – Governance*:* การผสมผสานของกระบวนการและโครงสร้างต่างๆ ที่คณะกรรมการนำมาใช้เพื่อบอกกล่าว สั่งการ บริหาร และ เฝ้าติดตามกิจกรรมต่างๆ ภายในองค์กรเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

อัตลักษณ์/ตัวตน (หรือตัวระบุ) – identity (or identifier): ป้ายกำกับเฉพาะที่ระบบใช้เพื่อระบุหน่วยงาน วัตถุ หรือกลุ่ม [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

การควบคุมด้านเทคโนโลยีสารสนเทศ – Information Technology Controls*: วิธีการควบคุมที่สนับสนุนการบริหารและการกำกับดูแลธุรกิจรวมทั้งก่อให้เกิด วิธีการควบคุมทั่วไป (general controls) และการควบคุมทางเทคนิค (technical controls) สำหรับโครงสร้างพื้นฐานของเทคโนโลยีสารสนเทศ (Information technology infrastructures) อันได้แก่ ระบบงาน ข้อมูล โครงสร้าง และบุคลากร

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ – Information Technology Governance*: ประกอบด้วยภาวะความเป็นผู้นำ โครงสร้างขององค์กร และกระบวนการที่สร้างความมั่นใจได้ว่า เทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กร

สิทธิพิเศษน้อยที่สุด – least privilege: คือหลักการที่ว่าสถาปัตยกรรมการรักษาความปลอดภัยได้รับการออกแบบมาเพื่อให้แต่ละหน่วยงานได้รับทรัพยากรระบบและการอนุมัติให้น้อยที่สุด เท่าที่หน่วยงานจำเป็นต้องใช้ในการดำเนินการตามหน้าที่ [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

การเฝ้าติดตามเหตุการณ์ – log monitoring: การใช้ซอฟต์แวร์พิเศษเพื่อติดตามดูเหตุการณ์ในบันทึกแบบผ่านๆ เพื่อหารูปแบบหรือความผิดปกติที่อาจบ่งบอกถึงบัญชีผู้ใช้ การเข้าถึง หรือกิจกรรมที่ไม่ได้รับอนุมัติ

ID ที่สร้างโดยระบบ – Mechanized ID: ID ระบบที่สร้างขึ้นสำหรับโปรแกรมหรือบริการอัตโนมัติ ID ที่สร้างโดยระบบ หรือ "mech ID" ควรมีบุคคลที่ได้รับการระบุว่าเป็นผู้รับผิดชอบในการตั้งค่าและการใช้งาน

มิดเดิลแวร์ – middleware: เป็นอีกคำหนึ่งสำหรับโปรแกรมที่ใช้เชื่อมต่อจากระบบหนึ่งไปอีกระบบหนึ่ง (API) ซึ่งหมายถึงการเชื่อมต่อที่อนุญาตให้โปรแกรมเมอร์เข้าถึงบริการในระดับล่างหรือสูงกว่าโดยมีการให้ชั้นตัวกลางซึ่งรวมถึงฟังก์ชันที่เรียกใช้บริการต่างๆ [อภิธานศัพท์ของ ISACA]

การยืนยันตัวตนแบบหลายปัจจัย – multi-factor authentication: ระบบการยืนยันตัวตนที่ต้องการมากกว่าหนึ่งปัจจัยสำหรับการยืนยันตัวตนที่สำเร็จ ปัจจัยการยืนยันความถูกต้องสามประการคือสิ่งที่คุณรู้ สิ่งที่คุณมี และสิ่งที่คุณเป็น [NIST SP 800-53, Revision 5, Glossary]

การห้ามปฏิเสธความรับผิด – nonrepudiation: การป้องกันบุคคลที่ปฏิเสธการกระทำบางอย่างอย่างไม่ถูกต้องและให้ความสามารถในการตัดสินได้ว่าบุคคลได้ดำเนินการบางอย่างไปแล้วหรือไม่ เป็นต้นว่า การสร้างข้อมูล การส่งข้อความ การอนุมัติข้อมูล หรือการรับข้อความ [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

ผู้ใช้ที่มีสิทธิพิเศษ – privileged user: ผู้ใช้ที่ได้รับอนุมัติ (และดังนั้น จึงเชื่อถือได้) ให้ทำหน้าที่ที่เกี่ยวข้องกับความปลอดภัยซึ่งผู้ใช้โดยทั่วไปจะไม่ได้รับอนุมัติให้ดำเนินการ [อภิธานศัพท์ของ NIST SP 800-53, Revision]

ความเสี่ยง – *Risk*:* ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่จะส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบจากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น

การบริหารความเสี่ยง – Risk Management*: กระบวนการในการระบุ ประเมิน จัดการและควบคุมเหตุการณ์หรือสถานการณ์ไม่พึงประสงค์ที่อาจจะเกิดขึ้น เพื่อก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

การควบคุมการเข้าถึงตามบทบาท – role-based access control: การควบคุมการเข้าถึงตามบทบาทของผู้ใช้ (ซึ่งก็คือ การรวบรวมสิทธิการเข้าถึงที่ผู้ใช้ได้รับตามสมมติฐานที่ชัดเจนหรือโดยปริยายของบทบาทที่กำหนด) สิทธิในบทบาทอาจสืบทอดผ่านลำดับชั้นของบทบาท และโดยทั่วไปจะสะท้อนถึงสิทธิที่จำเป็นในการทำหน้าที่ที่กำหนดไว้ภายในองค์กร บทบาทที่กำหนดอาจนำไปใช้กับบุคคลคนเดียวหรือหลายคนก็ได้ [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

หมวดหมู่ความปลอดภัย – security category: การกำหนดลักษณะของข้อมูลหรือระบบสารสนเทศโดยอิงตามการประเมินผลกระทบที่อาจเกิดขึ้นซึ่งผลกระทบจากการสูญเสียความลับ ความสมบูรณ์ หรือความพร้อมใช้ของข้อมูลหรือระบบสารสนเทศดังกล่าวจะมีผลต่อการดำเนินงานขององค์กร สินทรัพย์ขององค์กร หรือบุคคล [อภิธานศัพท์ของ NIST CSRC]

การแบ่งแยก/การแบ่งหน้าที่ – segregation/separation of duties: การควบคุมภายในขั้นพื้นฐานที่ป้องกันหรือตรวจจับข้อผิดพลาดและความผิดปกติโดยมอบหมายให้บุคคลมีการแบ่งแยกหน้าที่ในการเริ่มต้นและบันทึกธุรกรรม และสำหรับการพิทักษ์รักษาสินทรัพย์ [อภิธานศัพท์ของ ISACA]

ควร – Should*: มาตรฐานใช้คำว่า "ควร" ในที่ที่คาดว่าจะมีความสอดคล้อง เว้นแต่เมื่อใช้วิจารณญาณอย่างมืออาชีพ สถานการณ์จะแสดงให้เห็นถึงความเบี่ยงเบน

มาตรฐาน – Standard*: มาตรฐานการปฏิบัติงานวิชาชีพการตรวจสอบภายในที่ทางคณะกรรมการมาตรฐานการตรวจสอบภายในสากล ได้ประกาศใช้เป็นบรรทัดฐานสำหรับการดำเนินกิจกรรมการตรวจสอบภายในและสำหรับการประเมินผลงานการตรวจสอบภายใน

ผู้ใช้ที่มีสิทธิขั้นสูง – Superuser: ประเภทของบทบาทผู้ดูแลระบบที่มีสิทธิทั้งหมด ซึ่งรวมถึงการเข้าถึงราก (root) ของระบบปฏิบัติการ

ผู้ดูแลระบบ – system administrators: บุคลากรที่ได้รับอนุมัติให้ตั้งค่าและสนับสนุนการทำงานของทรัพยากรด้านไอที

ผู้ออกแบบระบบ – system architects: บุคลากรที่รับผิดชอบในการออกแบบหรืออนุมัติระบบที่ตรงตามความต้องการภายในและผนวกรวมเข้ากับโครงสร้างพื้นฐานในปัจจุบันหรือที่วางแผนไว้

ผู้ใช้ – user :บุคคล หรือ(ระบบ) กระบวนการที่ดำเนินการในนามของบุคคล ซึ่งได้รับอนุมัติให้เข้าถึงระบบ [อภิธานศัพท์ของ NIST SP 800-53, Revision 5]

ภาคผนวก ค เอกสารอ้างอิง

Center for Internet Security. “The 20 CIS Controls & Resources.” Interactive guide to CIS controls. Version 7.1. Accessed May 3, 2021, https://www.cisecurity.org/controls/cis-controls-list/

Grassi, Paul A., Michael E. Garcia, and James L. Fenton. *NIST SP 800-63-3: Digital Identity Guidelines*. Gaithersburg, MD: NIST, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3

ISACA. Control Objectives for Information Technologies (COBIT) 2019. Online framework and guidance. https://www.isaca.org/resources/cobit

ISACA.Glossary. Information technology terms and definitions. Accessed May3, 2021, https://www.isaca.org/resources/glossary

Joint Task Force. *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5*. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

NIST Computer Security Resource Center. Glossary. Accessed May 3, 2021, https://csrc.nist.gov/glossary

กิตติกรรมประกาศ

ทีมพัฒนาแนวปฏิบัติเกี่ยวกับไอที

Susan Haseley, CIA, United States (Chairman)

Terence Washington, CIA, CRMA United States (Project Lead)

Brad Ames, CISA, CPA, United States

Anand Balakrishnan, CIA, United States

Ruth Mueni Kioko, CIA, Kenya

Sajay Rai, CISM, CISSP,CPA, United States

มาตรฐานสากลของ IIA และแนวปฏิบัติทางวิชาชีพ

David Petrisky, CIA, CRMA, CISA, CPA, Director (Project Lead)

Jim Pelletier, CIA, CGAP, Vice President

Harold Silverman, CIA, QIAL, CRMA, Managing Director

Anne Mercer, CIA, CFSA,CFE, Director

Pam Stroebel Powers, CIA, CRMA,Director

Daniel Walker,CIA,CISA, CISSP, CPA, Director

Tammy Wyche, Director

Shelli Browning, Manager

Logan Wamsley, Manager

Lauressa Nelson, Senior Editor

Christine Janesko, Content Writer and Technical Editor

IIA ขอขอบคุณหน่วยงานกำกับดูแลต่างๆ สำหรับการสนับสนุนต่างๆ อันได้แก่ คณะกรรมการกำหนดแนวเทคโนโลยีสารสนเทศคณะกรรมการมาตรฐานการตรวจสอบภายในสากลสภากำกับดูแลกรอบการปฏิบัติวิชาชีพระหว่างประเทศ และสภาที่ปรึกษาแนวปฏิบัติในทางวิชาชีพ

เกี่ยวกับสมาคม

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นหน่วยงานด้านการตรวจสอบภายในที่ได้รับการยอมรับอย่างกว้างขวางในการเป็นผู้ให้การสนับสนุน ผู้ให้ความรู้ และผู้กำหนดมาตรฐาน แนวทางปฏิบัติต่างๆ และวุฒิบัตรรับรองคุณวุฒิต่างๆ ที่เกี่ยวข้องกับวิชาชีพตรวจสอบภายใน สมาคมก่อตั้งขึ้นในปี พ.ศ. 2484 ในปัจจุบัน IIA ได้ให้บริการสมาชิกมากกว่า 200,000 คน จากเกือบ 200 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี่ (Lake Mary) มลรัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม www.theiia.org หรือ www.globaliia.org

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

พิมพ์ครั้งแรก พ.ศ. 2552
พิมพ์ครั้งที่ 2 มิถุนายน พ.ศ. 2564

The Institute of Internal Auditors | Global
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