

Generative AI

คืออะไร และทำไมฝ่ายตรวจสอบ
ต้องให้ความสำคัญ?

“อนาคตของ AI ไม่ใช่การเข้ามาแทนที่มนุษย์ แต่เป็นการเพิ่มขีดความสามารถของมนุษย์ Generative AI เป็นเครื่องมืออันทรงพลังในการปลดปล่อยความคิดสร้างสรรค์และประสิทธิภาพของมนุษย์ ขณะเดียวกันก็ควรมีการกำกับดูแลที่แข็งแกร่งและการพิจารณาด้านจริยธรรมควบคู่กันไปด้วย”

Gen AI คืออะไร?

Gen AI เป็นคำที่ครอบคลุมเทคนิคปัญญาประดิษฐ์ (AI) ที่เรียนรู้จากการแสดงผลของสิ่งประดิษฐ์ในโมเดล และสามารถสร้างสิ่งประดิษฐ์ใหม่ๆ ที่มีลักษณะคล้ายกันได้ โมเดล Gen AI สามารถผลิตผลลัพธ์ได้หลากหลายรูปแบบ เช่น เสียง, ข้อความ, รูปภาพ, ข้อความ และวิดีโอจำลอง โดยการเรียนรู้จากคลังเนื้อหาต้นฉบับขนาดใหญ่ ลองนึกภาพว่าคุณสอน Gen AI ให้รู้จักภาพวาดจำนวนมาก มันก็จะสามารถสร้างภาพวาดใหม่ที่ไม่เคยมีมาก่อนได้เอง ซึ่งไม่ใช่แค่การคัดลอก แต่เป็นการสร้างสรรค์จากสิ่งที่มันได้เรียนรู้ ตัวอย่างของ Gen AI ที่เรารู้จักกันดีคือ ChatGPT ที่สามารถสนทนาและเขียนข้อความได้อย่างเป็นธรรมชาติ

Gen AI จะเข้ามาเปลี่ยนโลกธุรกิจอย่างไร?

เครื่องมือ Gen AI มีความสามารถโดดเด่นในการทำงานอัตโนมัติและเพิ่มประสิทธิภาพในหลากหลายงาน เช่น การเขียนอีเมล, สรุปรายงาน, และการเขียนโค้ดโปรแกรม ซึ่งช่วยให้พนักงานทำงานได้เร็วและมีประสิทธิภาพมากขึ้น Gen AI ยังสามารถปรับปรุงกระบวนการทำงานให้ดีขึ้นได้ ซึ่งอาจส่งผลกระทบอย่างมากต่อการดำเนินธุรกิจต่อไปในอนาคต

แล้วทำไมผู้ตรวจสอบภายในต้องสนใจ Gen AI ด้วย?

แม้ Gen AI จะมีประโยชน์มากมาย แต่ก็มาพร้อมกับความเสี่ยงใหม่ๆ ที่ฝ่ายตรวจสอบจำเป็นต้องเข้าใจและจัดการ ความเสี่ยงเหล่านี้ไม่ได้จำกัดอยู่แค่ภายในองค์กรของเราเท่านั้น แต่ยังรวมถึงความเสี่ยงที่มาจากภายนอกด้วย ซึ่ง Gartner ชี้ให้เห็นว่า Gen AI สร้างความเสี่ยงที่สำคัญที่ฝ่ายตรวจสอบต้องระบุและจัดการ ซึ่งหัวหน้าหน่วยงานตรวจสอบภายใน (CAEs) ควรกำหนดขั้นตอนเพื่อทำความเข้าใจความสามารถและกรณีการใช้งานของ Gen AI เพื่อเตรียมพร้อมสำหรับการจัดการความเสี่ยง

ความเสี่ยงหลักๆ ที่ผู้ตรวจสอบภายในควรให้ความสำคัญ ประกอบด้วย:

- **ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Risk):** Gen AI สามารถถูกนำไปใช้สร้างข้อมูลที่บิดเบือนที่ซับซ้อนขึ้น, การโจมตีแบบฟิชชิ่ง (Phishing attacks) หรือมัลแวร์ (Malware) ที่ซับซ้อนมากขึ้น ซึ่งอาจทำให้การโจมตีเหล่านี้ยากต่อการตรวจจับและป้องกัน นอกจากนี้ ยังมีความเสี่ยงที่ข้อมูลที่เรารับเข้า Gen AI อาจถูกปนเปื้อน หรือถูกใช้ในทางที่ผิด หากไม่สามารถป้องกันการโจมตีเหล่านี้ได้เพียงพอ อาจนำไปสู่การรั่วไหลของข้อมูล, การสูญเสียทางการเงิน หรือชื่อเสียงขององค์กร
- **ความเสี่ยงด้านชื่อเสียง (Reputational Risk):** Gen AI ช่วยให้สามารถสร้างเนื้อหาปลอม (counterfeit content) ที่มีความน่าเชื่อถือสูง ไม่ว่าจะเป็นเสียง, วิดีโอ, รูปภาพ หรือข้อความ ที่ดูเหมือนจริงมาก เนื้อหาปลอมเหล่านี้อาจถูกนำไปใช้เพื่อเผยแพร่ข้อมูลเท็จเกี่ยวกับบริษัทโดยเจตนา ซึ่งจะส่งผลเสียต่อชื่อเสียงและทำให้บริษัทสูญเสียเงินได้
- **ความเสี่ยงจากการเปิดเผยข้อมูลต่อบุคคลภายนอก (Increased Third-party Exposure):** เนื่องจากผู้ขายที่เป็นบุคคลภายนอกนำความสามารถของ Gen AI ไปรวมไว้ในข้อเสนอและการดำเนินงานภายในของพวกเขามากขึ้น ข้อมูลขององค์กรเราอาจถูกเปิดเผยได้โดยไม่ตั้งใจ นี่อาจสร้างความเสี่ยงเพิ่มเติมด้านการป้องกันข้อมูลสำหรับทั้งองค์กรของเราและองค์กรที่เป็นพันธมิตร
- **ความเสี่ยงข้อมูลรั่วไหล (Data Leakage Risk):** ความล้มเหลวในการสร้างการควบคุมที่เพียงพอสำหรับ Input และ Output ของ Gen AI อาจทำให้ข้อมูลที่เป็นความลับหรือทรัพย์สินทางปัญญาขององค์กรถูกเปิดเผย สิ่งนี้อาจนำไปสู่ผลทางกฎหมายจากการละเมิดกฎหมายความเป็นส่วนตัวของข้อมูล และอาจส่งผลให้ชื่อเสียงเสียหายในหมู่พนักงาน และสูญเสียความไว้วางใจของลูกค้าเนื่องจากการใช้ข้อมูลในทางที่ผิดโดยผู้ไม่หวังดี
- **ความรับผิดชอบทางกฎหมายต่อเนื้อหาที่ Gen AI สร้างขึ้น (Legal liability for Generated Content):** องค์กรอาจต้องรับผิดชอบทางกฎหมายสำหรับเนื้อหาที่สร้างโดยโมเดล Gen AI โดยเฉพาะอย่างยิ่งหากเนื้อหานั้นก่อให้เกิดความเสียหาย (เช่น ข้อมูลที่บิดเบือนและการหมิ่นประมาท) หรือละเมิดกฎหมาย รวมถึงลิขสิทธิ์
- **การเลือกปฏิบัติและอคติ (Discrimination and Biases):** โมเดล Gen AI มีแนวโน้มที่จะสร้างผลลัพธ์ที่ไม่ถูกต้อง (Hallucination) และอาจสร้างอคติที่มีอยู่ในข้อมูลการฝึกอบรมขึ้นมาใหม่ การพึ่งพาผลลัพธ์ของ Gen AI จึงอาจนำไปสู่การตัดสินใจที่ด้อยประสิทธิภาพ ซึ่งอาจส่งผลให้เกิดผลลัพธ์ที่มีค่าใช้จ่ายสูง (หรือแม้แต่อันตราย) เช่น การดำเนินการทางกฎหมาย, การลงโทษทางกฎหมาย และรายได้ที่ลดลงสำหรับองค์กร

ฝ่ายตรวจสอบควรดำเนินการอย่างไรกับ Gen AI?

- **สำรวจการใช้ Gen AI ทั่วทั้งองค์กร (Review enterprise wide Gen AI usage):** สิ่งแรกที่ต้องระบุว่าเป็นงานใดบ้างในองค์กรที่กำลังใช้หรือมีแผนจะใช้ Gen AI และมีส่วนร่วมในการประเมินความเสี่ยงกับพวกเขา การทำเช่นนี้จะช่วยให้เราเข้าใจภาพรวมของการใช้ Gen AI, ความเชื่อมโยงระหว่างส่วนงานต่างๆ และแหล่งที่มาของความเสี่ยงทั้งหมด
- **จัดทำแผนที่ความเสี่ยง Gen AI (Map Gen AI risks):** หลังจากทราบการใช้งานแล้ว ให้รวบรวมและจัดหมวดหมู่ความเสี่ยงใหม่ๆ ที่เกี่ยวข้องกับ Gen AI โดยเฉพาะสำหรับองค์กรของเรา รวมถึงความเสี่ยงชนิดใหม่และการเปลี่ยนแปลงความเสี่ยงที่มีอยู่ ขั้นตอนนี้จะช่วยให้ฝ่ายตรวจสอบสามารถวางแผนการตรวจสอบที่เหมาะสม

ฝ่ายตรวจสอบควรดำเนินการอย่างไรกับ Gen AI?

- **ให้คำแนะนำผู้มีส่วนได้ส่วนเสียเกี่ยวกับความเสี่ยง Gen AI (Advise stakeholders on Gen AI risks):** ฝ่ายตรวจสอบควรมีส่วนร่วมหรือให้คำแนะนำกับคณะกรรมการและคณะทำงานที่เกี่ยวข้องกับ Gen AI เพื่อเน้นย้ำถึงความเสี่ยงต่างๆ สื่อสารความเสี่ยงเหล่านี้ให้คณะกรรมการบริษัทและผู้บริหารระดับสูงทราบอย่างชัดเจน และชี้ให้เห็นว่าความเสี่ยงเหล่านี้อาจส่งผลกระทบต่อเป้าหมายเชิงกลยุทธ์ขององค์กรอย่างไร
- **ทบทวนกระบวนการอนุมัติสำหรับกรณีการใช้งาน Gen AI (Review approval process for Gen AI use cases):** ตรวจสอบกระบวนการและระบบที่ใช้ในการอนุมัติการใช้งาน Gen AI ขององค์กร รวมถึงการเปลี่ยนแปลงนโยบายการใช้งาน ประเมินว่าการใช้งานจริงนั้นสอดคล้องกับสิ่งที่ได้รับอนุมัติหรือไม่ และแจ้งให้ผู้บริหารทราบถึงกรณีที่ไม่ปฏิบัติตาม เพื่อให้มีการแก้ไข
- **ประเมินการสื่อสารขององค์กรเกี่ยวกับนโยบาย Gen AI (Evaluate organizational communication on Gen AI policies):** ประเมินว่าพนักงานในองค์กรรับทราบนโยบาย Gen AI มากน้อยเพียงใด ประเมินความถี่และประสิทธิภาพของการฝึกอบรมและการสื่อสารนโยบาย Gen AI

นอกเหนือจากนี้ ฝ่ายตรวจสอบภายในควรให้ความสำคัญกับการเสริมสร้างความสามารถของผู้ตรวจสอบใน ซึ่งทำได้โดย:

- **ประเมินความจำเป็นในการฝึกอบรมเจ้าหน้าที่ตรวจสอบเกี่ยวกับ Gen AI (Assess the need for training audit staff on Gen AI):** ตรวจสอบทักษะของเจ้าหน้าที่ตรวจสอบในปัจจุบัน เทียบกับทักษะที่จำเป็นในการตรวจสอบเครื่องมือ Gen AI ได้อย่างมีประสิทธิภาพ เริ่มการฝึกอบรมและพัฒนาทักษะเพื่อให้มั่นใจว่าความสามารถของแผนกจะทันกับการนำเทคโนโลยีมาใช้ขององค์กร
- **ทำงานร่วมกับผู้เชี่ยวชาญ Gen AI ในธุรกิจ (Collaborate with Gen AI experts in the business):** ระบุนักวิชาการหรือหน่วยงานที่มีความเชี่ยวชาญเฉพาะด้านใน Gen AI หรือ AI โดยรวมภายในองค์กร ใช้โอกาสนี้ในการนำผู้เชี่ยวชาญเหล่านี้มาช่วยปรับปรุงผลลัพธ์ของการประกันคุณภาพ และถ่ายทอดความรู้ให้กับเจ้าหน้าที่ตรวจสอบ
- **ประสานงานกับผู้ให้บริการประกันคุณภาพรายอื่น (Coordinate with other assurance providers):** สื่อสารเชิงรุกกับฝ่ายอื่นๆ ที่เกี่ยวข้อง เช่น ฝ่ายกฎหมาย, ฝ่ายกำกับการปฏิบัติตามกฎหมาย (Compliance), ฝ่ายบริหารความเสี่ยงองค์กร (ERM), ฝ่ายความปลอดภัยของข้อมูล โดยมีเป้าหมายคือเพื่อประสานงานกิจกรรมด้านธรรมาภิบาลและการบริหารความเสี่ยงสำหรับ Gen AI และกำหนดบทบาทและความรับผิดชอบที่ชัดเจน

บทสรุป

Gen AI ขับเคลื่อนนวัตกรรมและประสิทธิภาพให้องค์กร แต่ก็มาพร้อมความเสี่ยงใหม่ๆ ที่ซับซ้อน ผู้ตรวจสอบภายในจึงมีบทบาทสำคัญในการเข้าใจความสามารถของ Gen AI, ประเมินความเสี่ยง, และให้คำแนะนำผู้บริหารในการกำกับดูแลและควบคุม การเตรียมพร้อมบุคลากรและการทำงานร่วมกับผู้เชี่ยวชาญ จะช่วยให้องค์กรใช้ประโยชน์จาก Gen AI ได้เต็มที่ พร้อมลดผลกระทบจากความเสี่ยง เพื่อการเติบโตที่ยั่งยืนในยุคดิจิทัล

แปลจาก Gartner: Quick Answer: What Should Audit Know and Do About Generative AI?

ณัฐวัฒน์ วาจาบุตร

CIA, CPA, CPIAT