

บทความชุด “Internal Auditing 4.0 (IA 4.0)”

ตอนที่ 2 : "คำเปลี่ยนโลก (Words to Change the World) : โอกาสและความเสี่ยงที่ Internal Auditor 4.0 (IA4.0) ต้องรู้!" (ตอนที่ 1)

นายสิริชัย สกกุลแพรวพาณิชย์ (โค้ชเมิ่ง)

ผู้ก่อตั้ง และกรรมการผู้จัดการ CIA Coach Consulting Co., Ltd.

CIA, CRMA, C-PA, CPIAT, IAEP, EIAP, ISMS Lead Auditor

ปริญญาตรี บัญชี จุฬาฯ (Shi 58) และปริญญาโท หลักสูตร MSCG จุฬาฯ (รุ่นที่ 1)

ตามที่ผมได้ให้ความเห็นในบทความตอนที่แล้ว (ตอนที่ 1 : “AI” มาแทนที่ “IA” จริงหรือ???) ไว้ว่า แนวโน้มทางเทคโนโลยี (IT Trend) ต่างๆ สะท้อนแนวโน้มของการตรวจสอบภายใน (IA Trend) ในแง่มุมหนึ่งว่า ความรู้ความสามารถของผู้ตรวจสอบภายใน ยุคใหม่ หรือยุค 4.0 นั้น ต้องพัฒนาและปรับปรุงให้สามารถตรวจสอบเทคโนโลยีใหม่ๆ เหล่านั้น ได้อย่างมีประสิทธิภาพและมีประสิทธิผล ซึ่งผู้ตรวจสอบภายในจำเป็นต้องศึกษาและมีความรู้เกี่ยวกับเทคโนโลยีใหม่ๆ เหล่านั้น เพื่อให้สามารถระบุได้ถึงสิ่งต่างๆ เช่น โอกาสและความเสี่ยงในการนำเทคโนโลยีใหม่ๆ เหล่านั้นมาใช้ในองค์กร ทั้งนี้ เพื่อให้ผู้ตรวจสอบภายใน สามารถให้ความเห็นหรือข้อเสนอแนะที่มีประโยชน์และมีคุณค่าต่อองค์กรได้

บทความตอนนี้ จึงขอนำเสนอรายละเอียดของโอกาสและความเสี่ยงของเทคโนโลยีต่างๆ ที่ผู้ตรวจสอบภายในยุคใหม่ ที่ผมเรียกว่า Internal Auditor 4.0 (IA4.0) ต้องรู้ตามที่กล่าวข้างต้น โดยเรียบเรียงและจัดเรียงเป็นคำศัพท์ของเทคโนโลยีต่างๆ ตามลำดับของตัวอักษรในภาษาอังกฤษ จาก A ถึง Z ซึ่งผมเรียกว่า “คำเปลี่ยนโลก (Words to Change the World)” มีรายละเอียดดังนี้

A = Artificial Intelligence : AI (ปัญญาประดิษฐ์)

Artificial Intelligence : AI (ปัญญาประดิษฐ์) ตามความหมายที่ระบุอยู่ในวิกิพีเดีย สารานุกรมเสรี หมายถึง “ความฉลาดเทียมที่สร้างขึ้นให้กับสิ่งที่ไม่มีชีวิต ปัญญาประดิษฐ์เป็นสาขาหนึ่งในด้านวิทยาการคอมพิวเตอร์ และวิศวกรรมเป็นหลัก แต่ยังรวมถึงศาสตร์ในด้านอื่น ๆ อย่างจิตวิทยา ปรัชญา หรือชีววิทยา ซึ่งสาขาปัญญาประดิษฐ์เป็นการเรียนรู้เกี่ยวกับกระบวนการการคิด การกระทำ การให้เหตุผล การปรับตัว หรือการอนุมาน และการทำงานของสมอง...”

หากจะกล่าวถึงโอกาสหรือประโยชน์ของ AI ที่นำมาใช้งานในภาคธุรกิจนั้น มีมากมายหลายประการ ซึ่งจากการสำรวจของ eMarketer นั้น ผู้บริหารในองค์กรใหญ่ ได้ให้ความเห็นถึงงานที่ AI จะเข้ามา

ช่วยในธุรกิจได้ ได้แก่ AI ใช้วิเคราะห์ข้อมูลซับซ้อนได้แม่นยำมากกว่า เช่น ในด้านการรักษาความปลอดภัยของข้อมูล ซึ่งปัจจุบันมีมัลแวร์เกิดขึ้นใหม่กว่า 3 แสนไฟล์ทุกวัน โดยมีความแตกต่างกันไม่เกิน 10% ทำให้การตรวจสอบติดตามทำได้ยากมาก แต่ระบบ AI สามารถแยกแยะได้ทันทีว่าไฟล์ไหนเป็นมัลแวร์คุกคาม โดยเฉพาะปัจจุบันนี้มีการใช้ระบบคลาวด์ ระบบ AI จึงยิ่งมีความสำคัญในการตรวจสอบข้อมูล เป็นต้น **AI ยังเปิดโอกาสในการสร้างสรรค์บริการและความประทับใจให้ลูกค้าได้มากกว่าเดิม** โดยการสร้างสรรค์รูปแบบบริการใหม่ๆ ที่ได้จากการสนับสนุนการทำงานของ AI ตัวอย่างเช่น Chatbot ที่เราสามารถเพิ่มลูกเล่นในการรับมือกับลูกค้าและบริการได้จากข้อมูลการถามตอบกับลูกค้า นอกจากนี้ AI ยังสามารถช่วยเจ้าของธุรกิจให้ตัดสินใจได้ดีขึ้น โดย AI สามารถทำงานประมวลผลซึ่งว่ากันด้วยข้อมูลล้วนๆ มาวิเคราะห์ และตัดสินใจโดยอิงจากข้อมูลที่เคยมีมาก่อน เพื่อหาทางเลือกที่คุ้มค่าที่สุด มีความเสี่ยงน้อยที่สุด หรือใช้เวลาน้อยที่สุดได้ โดยเรียกว่าการค้นหาทางเลือกที่ Optimize ที่สุดบนข้อมูลที่มีอยู่ เพื่อช่วยให้เราตัดสินใจเรื่องต่างๆ จากข้อมูลที่ต้องใช้ประกอบการตัดสินใจจำนวนมหาศาล แตกต่างกันไปโดยสิ้นเชิงกับของมนุษย์ เพราะ AI ไม่ได้นำเรื่องของ Sense อารมณ์ ความชอบ รสนิยม ความคิดเห็น และความสัมพันธ์ส่วนตัวมาพิจารณา

AI มีประโยชน์อนันต์ ก็มีโทษมหันต์เช่นกัน ความเสี่ยงหรือความกังวลของ AI ในอนาคต มีมากมาย เช่น AI จะเข้ามาแทนที่แรงงานคน ทำให้มนุษย์อย่างเราอาจตกงานได้ หรือ หาก AI ฉลาดกว่าเรา ที่เป็นมนุษย์จะคุมไม่อยู่ แต่ที่ส่งผลกระทบต่อรุนแรงและน่ากังวลมากกว่านั้นมาก คือ หากการพัฒนา AI ทำอย่างรวดเร็วจนเกินไป ประกอบกับอาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ก็มีการปรับเปลี่ยนวิธีการมมาตลอด จึงมีความกังวลว่า AI อาจถูกนำมาใช้เป็นเครื่องมือในการก่อการร้าย เช่น การรวมเทคโนโลยี AI เข้ากับวิธีการโจมตีแบบหลายทางเพื่อตรวจหาและใช้ประโยชน์จากจุดอ่อนในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์ การสร้างมัลแวร์จาก AI เพื่อสร้างการโจมตีแบบใหม่ เจ้าของธุรกิจมีโอกาสโดนโจมตีในระดับรุนแรงหากถูกบุกรุกหรือหยุดทำงาน การแทรกแซงบังคับควบคุมสิ่งต่างๆ ที่เกิดขึ้นจาก AI ทั้งรถยนต์ไร้คนขับ โดรนส่งของ โดรนทำงานของรัฐบาล ฯลฯ การบิดเบือนข่าวสาร วิดีโอ การสื่อสาร หรือการแอบอ้างบุคคลสำคัญเพื่อส่งสารที่สร้างความเข้าใจผิด และการจัดการเหตุการณ์ ไปจนถึงการขโมยและแบ่งปันข้อมูลลับ และอาจนำไปสู่การคุกคามมนุษย์ด้วยกัน เป็นต้น

B = Blockchain (บล็อกเชน)

Blockchain (บล็อกเชน) เป็นบัญชีแยกประเภทระบบอิเล็กทรอนิกส์ที่มีความปลอดภัย โดยเชื่อมต่อกับหลายภาคส่วนบนเครือข่ายที่มีความน่าเชื่อถือและไว้วางใจได้ ทั้งยังช่วยอำนวยความสะดวกในการถ่ายโอนสินทรัพย์และข้อมูลที่เกี่ยวข้องกับสินทรัพย์ดังกล่าวด้วย โดยเบื้องต้นแล้ว เทคโนโลยีนี้ถูกสร้างขึ้นเพื่อใช้

เป็นเครื่องมือของบิทคอยน์ในการรับรองความถูกต้องของสกุลเงินอิเล็กทรอนิกส์หลังจากที่เกิดเหตุการณ์ครั้งใหญ่ในโลกการเงินจนนำไปสู่วิกฤตการณ์ทางการเงินระดับโลกเมื่อปี พ.ศ. 2551

ทุกธุรกรรมในระบบดิจิทัลจะได้รับการเก็บบันทึกอย่างปลอดภัยในห่วงโซ่ (เชน) ที่เชื่อมต่อกันด้วยคีย์ดิจิทัลที่มีการเข้ารหัสไว้สำหรับใช้แสดงความถูกต้องเมื่อได้รับการตรวจสอบจากเครือข่าย การสร้างสำเนา การแก้ไข หรือการลบธุรกรรมจะได้รับการป้องกันโดยเชนซึ่งมีอยู่ในคอมพิวเตอร์ของแต่ละคนบนเครือข่าย ยิ่งบล็อกเชนยาวมากเท่าไรและเครือข่ายกว้างไกลมากเพียงใด คีย์ดิจิทัลก็ยิ่งมีความซับซ้อนมากขึ้น ดังนั้นบล็อกเชนจึงมีความปลอดภัยมากยิ่งขึ้นไปอีก

การใช้ระบบค้าขายแลกเปลี่ยนแบบใหม่สามารถสร้างโอกาสหรือประโยชน์ให้กับธุรกิจได้อย่างมากมาย แต่ส่วนใหญ่แล้วจะมุ่งเน้นไปที่ความสามารถอย่างน้อย 1 ใน 6 อย่าง ได้แก่ ประสิทธิภาพ : การทำธุรกรรมระหว่างบุคคลหรือกลุ่มที่เกี่ยวข้องสามารถเสร็จสมบูรณ์ได้โดยตรงและไม่ต้องมีคนกลาง ทั้งยังสามารถใช้ข้อมูลในรูปแบบดิจิทัล จึงทำให้การดำเนินธุรกรรมเป็นไปอย่างรวดเร็ว **ความพร้อมที่จะให้ตรวจสอบบัญชี :** เนื่องจากธุรกรรมแต่ละรายการได้รับการเก็บบันทึกอย่างต่อเนื่องและไม่มีกำหนด ดังนั้นจึงสามารถดำเนินการตรวจสอบได้ตลอดทั้งวงจรชีวิตของสินทรัพย์ สิ่งนี้จะยิ่งมีความสำคัญอย่างมากหากข้อมูลต้นฉบับเป็นสิ่งจำเป็นที่ต้องใช้ในการตรวจสอบความถูกต้องของสินทรัพย์ **ความสามารถด้านการติดตาม :** การติดตามสินค้าในซัพพลายเชนจะได้รับประโยชน์หากต้องการติดตามตรวจสอบว่าตอนนี้ชิ้นส่วนต่างๆ อยู่ที่ใดบ้าง โดยข้อมูลที่เกี่ยวข้องกับชิ้นส่วนดังกล่าวจะถูกส่งไปยังหรือได้รับจากเจ้าของใหม่เพื่อดำเนินการในด้านอื่นๆ ต่อไป

ความโปร่งใส : ในบางครั้งการขาดความโปร่งใสทางการค้าอาจนำไปสู่ความล่าช้าในการดำเนินธุรกิจและสามารถทำลายความสัมพันธ์ระหว่างกันได้ ซึ่งการให้รายละเอียดของการทำธุรกรรมอย่างชัดเจนจะช่วยเพิ่มความน่าเชื่อถือให้กับกระบวนการค้าขาย ทั้งยังช่วยเสริมสร้างความสัมพันธ์ให้มั่นคงยิ่งขึ้นตามระดับความโปร่งใสที่มีอยู่ด้วย **ความปลอดภัย :** ธุรกรรมแต่ละรายการจะได้รับการตรวจสอบภายในเครือข่ายโดยใช้การเข้ารหัสลับที่ซับซ้อนและได้รับการตรวจสอบอย่างอิสระ ดังนั้นจึงสามารถมั่นใจในความถูกต้องของข้อมูลได้ และ **ความเห็น :** ด้วยความสามารถในการติดตามสินทรัพย์ครอบคลุมทั้งวงจรชีวิต ผู้ออกแบบและผู้ผลิตสินทรัพย์จึงสามารถปรับรูปแบบการบริหารจัดการสินทรัพย์ตลอดวงจรชีวิตได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น โดยอาศัยข้อมูลในด้านต่างๆ ไม่ว่าจะเป็นการจัดส่ง การติดตั้ง การบำรุงรักษา และการรีดถอน

สำหรับ **ความเสี่ยงหรือข้อจำกัดของ Blockchain** ก็มีอยู่ไม่น้อย ได้แก่ **ความคุ้มค่าทางเศรษฐศาสตร์ :** การกระจายข้อมูลให้เครื่องจำนวนมากเก็บซ้ำซ้อนกัน ย่อมใช้ต้นทุนมากกว่าระบบ ธรรมดาแบบเก่าที่เก็บข้อมูลอยู่ที่เครื่องแน่นอน โจทย์ที่จะประยุกต์ใช้ Blockchain จึงต้องตั้งคำถามว่า จุดเด่นของ

Blockchain มีค่ามากพอให้คุ้มกับการลงทุนมีเครื่องจำนวนมากหรือไม่? คุ้มค่าแค่ไหนเมื่อเทียบกับเทคโนโลยีทางเลือกอื่น ๆ **ความเร็วในการประมวลผล** : การตรวจสอบความถูกต้องของ transaction ในระบบ Blockchain ต้องอาศัยความเห็นจากเครื่องจำนวนมากใน network การติดต่อกับเครื่องจำนวนมาก ย่อมต้องใช้เวลามากกว่า เช่น Bitcoin ใช้เวลาประมวลผลเพื่อยืนยัน transaction ทางทฤษฎีอยู่ที่ 10 นาที แต่ทางปฏิบัติ อาจใช้เวลาประมวลผลสูงถึง 2-3 ชั่วโมงหรือมากกว่านั้น **สิทธิในการแก้ไขข้อมูล** : สิทธิควรเป็นแบบเปิดกว้างหรือไม่? ถ้าคุณไม่ได้ต้องการให้คน/องค์กรจำนวนมากมีสิทธิแก้ไขฐานข้อมูล คุณก็ไม่จำเป็นต้องใช้ Blockchain และคุณเชื่อใจคนที่มิสิทธิได้แค่ไหน? ถ้าคุณเชื่อใจ หรือมีเหตุให้ต้องเชื่อคนในระบบอยู่แล้ว คุณก็ไม่จำเป็นต้องใช้ Blockchain ก็ได้ เช่น ถ้าของที่เก็บไม่ได้มีผลประโยชน์มาเกี่ยวข้องที่จะเป็นแรงจูงใจให้คนอยากโกงระบบ เป็นต้น

ข้อมูลเหมาะกับการเก็บแบบ Ledger/Immutable หรือไม่ : จุดแข็งของ Blockchain เมื่อเทียบกับ Database ปกติ คือ การเก็บข้อมูลแบบ Ledger ซึ่งหมายถึงการเก็บข้อมูลที่ ข้อมูลปัจจุบันจะถูกต้อง ต้องดูข้อมูลย้อนหลัง หรือ ข้อมูลของคนอื่น ๆ ประกอบ เช่น ยอดเงินล่าสุดในบัญชี ต้องมาจากการสรุปมาจากยอดฝากถอนโอนก่อนหน้านั้น สิทธิความเป็นเจ้าของรถ ต้องดูว่า การโอนสิทธิของเจ้าของคนก่อนหน้านั้นทั้งหมดเป็นไปอย่างถูกต้องหรือไม่ ถ้าข้อมูลของคุณไม่มีลักษณะแบบนี้ คุณก็จะไม่ได้ใช้จุดแข็งของ Blockchain คุณจะใช้ Blockchain ก็ไม่ผิด แต่วิธีแบบเดิม ๆ มันยุ่งน้อยกว่า และต้นทุนถูกกว่า และ **ความรับผิดชอบต่อสิ่งที่อยู่ใน Blockchain** : Blockchain ยังใหม่เกินไป ช่องโหว่และปัญหาที่รอให้อุดยังมีอีกมาก อีกเหตุผลหนึ่งคือ ระบบ Blockchain อยู่บนพื้นฐานของการโหวตแบบประชาธิปไตย ระบบประชาธิปไตยทำให้การแก้ไขปัญหามองแบบล่าช้ามาก เพราะต้องรอการโหวต ต่างกับระบบ Database แบบเดิมที่รับผิดชอบโดยองค์กรใดองค์กรหนึ่ง ที่พร้อมตัดสินใจเองได้เลย

C = Cloud Computing (คลาวด์คอมพิวติ้ง)

Cloud Computing (คลาวด์คอมพิวติ้ง) คือ การที่เราใช้ซอฟต์แวร์ ระบบ และทรัพยากรของเครื่องคอมพิวเตอร์ของผู้ให้บริการ ผ่านอินเทอร์เน็ต โดยสามารถเลือกกำลังการประมวลผล เลือกจำนวนทรัพยากร ได้ตามความต้องการในการใช้งาน และให้เราสามารถเข้าถึงข้อมูลบน Cloud จากที่ไหนก็ได้

Cloud Computing สามารถสร้างโอกาสหรือประโยชน์ให้กับบริษัทได้หลายวิธีขึ้นอยู่กับขนาด **สเกล เซกเตอร์ รวมทั้งเป้าหมายด้านกลยุทธ์ของบริษัทเหล่านั้น และนี่คือข้อได้เปรียบ 5 ประการของการย้ายบริการด้านไอทีไปที่คลาวด์** ได้แก่ **ลดค่าใช้จ่ายด้านเงินทุน** : ความสามารถในการใช้แหล่งบริการด้านไอทีแบบออนดีมานด์ ตามความต้องการ เมื่อใดที่ต้องการ ช่วยให้ธุรกิจย้ายไปยังรูปแบบการลงทุนที่ขึ้นอยู่กับค่าใช้จ่ายในการดำเนินงาน **การบำรุงรักษาและการอัปเดตที่ง่ายขึ้น** : ผู้ให้บริการคอมพิวเตอร์ระบบคลาวด์เป็น

ผู้รับผิดชอบสำหรับเซิร์ฟเวอร์ ซอฟต์แวร์และการจัดการเครือข่าย ทำให้ผู้เชี่ยวชาญด้านไอทีในองค์กรสามารถเปลี่ยนไปจัดการกับงานอื่นๆ ที่สำคัญ เพิ่มความยืดหยุ่นและอิสระในการทำงานได้จากสถานที่ต่าง ๆ : ด้วยบริการคลาวด์ที่ปลายนิ้วสัมผัส พนักงานสามารถทำงานได้จากสถานที่ต่าง ๆ เกือบทุกสถานที่ พวกเขาสามารถเข้าถึงไฟล์ที่สำคัญ ข้อมูล เอกสารและเครื่องมือไอทีจากอุปกรณ์ทุกรูปแบบจากเกือบทุกสถานที่ที่มีการเชื่อมต่อ

ความต่อเนื่องของธุรกิจ : ประโยชน์ที่ได้รับจากการทำงานระยะไกลคือในกรณีที่เกิดภัยพิบัติ ลูกค้าไม่ต้องสงสัยว่าจะสามารถทำงานอย่างต่อเนื่องได้หรือไม่ หากมีไฟไหม้ น้ำท่วม โจรกรรม เทคโนโลยีใช้งานไม่ได้ หรือหิมะตก หรือน้ำแข็ง ที่ขัดขวางไม่ให้พนักงานเข้ามาทำงานในสำนักงาน พวกเขาก็มีตัวเลือกในการทำงานจากสถานที่ต่าง ๆ และ **การรักษาความปลอดภัยด้านไอทีที่ดีขึ้น :** แทนที่จะทำให้การรักษาความปลอดภัยด้านไอทีอ่อนแอลง กลับมีกรณีที่แสดงให้เห็นว่าคลาวด์คอมพิวเตอร์ช่วยเสริมสร้างการป้องกันให้กับองค์กร นี่เป็นเพราะผู้ให้บริการคลาวด์ใช้จ่ายเงินจำนวนมาก ไปในการรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานของศูนย์ข้อมูล และการเก็บรักษาข้อมูลลูกค้าของพวกเขาให้ปลอดภัย

แม้ว่า **Cloud Computing** จะให้ประโยชน์แก่ผู้ใช้อย่างมากมาย แต่ทั้งนี้เหรียญย่อมมีสองด้านเสมอ การใช้ **Cloud Computing** นั้นก็มีความเสี่ยงจากภัยคุกคามเช่นเดียวกับการใช้เทคโนโลยีอื่นๆ โดยทาง **CSA หรือ Cloud Security Alliance** ได้ทำการสรุปประเภทของภัยคุกคามที่จะเกิดกับ **Cloud Computing** เอาไว้ 7 ประเภท ได้แก่ **Abuse and nefarious use of cloud computing :** การใช้ cloud computing ในทางที่ผิด อย่างเช่น hacker ที่จะใช้ทรัพยากรที่มีอยู่อย่างไม่จำกัดของ cloud เช่น แบนด์วิธ,สตอเรจ เป็นฐานในการโจมตีผู้อื่น การส่งสแปมเมลล์ และการ crack encryption ต่างๆ เป็นต้น **Insecure interfaces and APIs :** ความน่าเชื่อถือในด้าน security และ availability เนื่องจากผู้ใช้บริการจะอาศัย API ในการติดต่อกับ Backend software และเซอร์วิสต่างๆที่อยู่ใน cloud จึงอาจเป็นช่องทางที่ผู้ไม่หวังดีสามารถใช้เข้าโจมตีและเข้าถึงเซอร์วิสต่างๆได้โดยตรง ซึ่งสิ่งเหล่านี้จะมีผลต่อความน่าเชื่อถือของข้อมูลและการรักษาความลับของข้อมูลใน cloud **Malicious insiders :** ภัยคุกคามที่เกิดจากคนใน จากฝั่งผู้ให้บริการเอง เช่น พนักงานสามารถเข้าถึงข้อมูลที่เกินกว่าสิทธิของตนเองที่จะเข้าถึงได้

Shared technology issues : เป็นปัญหาเกี่ยวกับ Software ที่ใช้ในการจัดการการแชร์ระบบ และทรัพยากรต่างๆแก่ผู้ใช้เกิดความผิดพลาด หรือมี bug ทำให้เป็นช่องโหว่ที่ทำให้ hacker สวมรอยเข้ามาเป็นผู้ให้บริการ cloud แล้วทำการเจาะระบบของผู้ใช้รายอื่นผ่านทางระบบที่ตนเองใช้งานอยู่ได้ **Data loss or leakage :** การรั่วไหลของข้อมูล เนื่องจากอาจมีผู้อื่นมาใช้งานบน cloud ดดยไม่ได้รับอนุญาต **Account or service hijacking :** การถูกขโมยใช้งานเซอร์วิสต่างๆ,การ Phishing,การถูกโจมตีตามช่องโหว่ของ software ที่ไม่ได้มีการ patch ซึ่งสาเหตุส่วนหนึ่งก็มาจากการที่ผู้ใช้ใช้ password เดิมซ้ำๆอยู่นาน หรือ ไม่มีการเปลี่ยน password ในเวลาที่เหมาะสม และ **Unknown risk profile :** เนื่องจากบริการของ cloud นั้น ทางผู้ให้บริการ

ไม่ได้เปิดเผยถึงรายละเอียดของการดำเนินการภายใน เช่น การ config ระบบ,กระบวนการด้าน security,การเก็บ log file ต่างๆ ทำให้ผู้ใช้บริการมีความเสี่ยงเพราะไม่รู้ว่าคุณเสี่ยงคืออะไรทำให้ไม่สามารถเตรียมการรองรับได้

โปรดติดตามรายละเอียดของโอกาสและความเสี่ยงของเทคโนโลยีต่างๆ ที่ผมเรียบเรียงเป็น คำศัพท์ทางเทคโนโลยี ซึ่งผมเรียกว่า “คำเปลี่ยนโลก (Words to Change the World)” ได้ในตอนต่อไปนะครับ

ข้อมูลอ้างอิง :

- “ปัญญาประดิษฐ์”,<https://th.wikipedia.org/wiki/ปัญญาประดิษฐ์>
- บทความชื่อ “ประโยชน์ของ AI กับการใช้งานในภาคธุรกิจ”, <https://www.aware.co.th>
- บทความชื่อ “ประโยชน์ 6 ข้อ สำหรับธุรกิจที่จะได้รับจากบล็อกเชน”, <https://www.techtalkthai.com/6-business-benefits-of-blockchain/>
- บทความชื่อ “ข้อจำกัดของ Blockchain”, <https://jirasukhanon.com/blockchain-limitation-f96677ea04eb>
- บทความชื่อ “Cloud Computing คืออะไร ? Cloud Computing คืออย่างไร?”, <https://www.it24hrs.com/2015/cloud-computing-and-cloud-definition/>
- บทความชื่อ “5 ประโยชน์สูงสุดของคลาวด์คอมพิวติ้ง”, <https://blogs.business.microsoft.com/th-th/2016/10/05/top-5-benefits-cloud-computing/>
- บทความชื่อ “ภัยคุกคาม 7 อย่างสำหรับ Cloud computing”, <https://suntos.wordpress.com>