ISO/IEC 27001:2022

Start your transition

การควบคุมใหม่

LRQA

การเปลี่ยนแปลงที่สำคัญ

ในเดือนกุมภาพันธ์ 2022 ISO 27002:2022 ซึ่งเป็นมาตรฐานที่ให้การควบคุมแนวทางปฏิบัติที่ดีที่สุดที่องค์กรสามารถนำไปใช้เพื่อปรับปรุงความปลอดภัยได้รับการอัปเดต ด้วยเหตุนี้จึงคาดว่าจะมีการเผยแพร่ ISO 27001 เวอร์ชันใหม่ซึ่งเป็นมาตรฐานสากลที่ระบุข้อกำหนดของระบบการจัดการความปลอดภัยของข้อมูล (ISMS) ในไตรมาสสุดท้ายของปี 2022 ด้วย

มาตรฐานเวอร์ชันใหม่จะมีการควบคุมตามที่ระบุไว้ใน ISO 27002:2022 และองค์กรจะต้องทบทวนการประเมินความเสี่ยงอีกครั้งเพื่อพิจารณาว่าจำเป็นต้องปรับปรุงหรือใช้วิธีใหม่ในการดูแลความเสี่ยงหรือไม่

องค์กรที่มีใบรับรอง ISO 27001:2013 อยู่แล้วจะมีเวลาสามปีในการเปลี่ยนผ่านไปสู่มาตรฐานใหม่

93
การควบคุม
แทนที่จะเป็น
114

มีทั้งหมด
11
การควบคุมใหม่

56
รวมการควบคุมจาก ISO 27001:2013 ให้เป็น 24 รายการใน ISO 27001:2022

โดยส่วนใหญ่แล้ว
อาจมีการเปลี่ยนแปลงข้อความบางรูปแบบในการควบคุม ซึ่งอาจส่งผลต่อวิธีการตีความ และใช้มาตรฐาน

ตอนนี้การควบคุมแบ่งออกเป็นสี่ ธีม “ใหม่”

องค์กร	บุคคล	ทางกายภาพ	ทางเทคนิค
- รวมกัน 28 รายการ	- รวมกัน 2 รายการ	- รวมกัน 5 รายการ	- รวมกัน 21 รายการ
- ใหม่ 3 รายการ	- ใหม่ 0 รายการ	- ใหม่ 1 รายการ	- ใหม่ 7 รายการ

การควบคุม ISO 27001:2022

การควบคุมที่ระบุไว้ใน ISO 27002:2022 จะอยู่ใน ISO 27001:2022 ภาคผนวก A โดยแสดงถึงการเปลี่ยนแปลงที่สำคัญที่สุดในมาตรฐานใหม่

ISO 27001:2022 ฉบับใหม่		
ธีม	**การควบคุม (ใหม่)**	**หัวข้อ**
นโยบายความปลอดภัยของข้อมูล		
A.5.1	การควบคุมองค์กร	นโยบายสำหรับความปลอดภัยของข้อมูล
A.5.1.2	**รวมไว้เป็น A.5.1**	
การจัดระเบียบข้อมูล		
A.5.2	การควบคุมองค์กร	บทบาทและความรับผิดชอบด้านความปลอดภัยของข้อมูล
A.5.3	การควบคุมองค์กร	การแบ่งแยกหน้าที่
A.5.5	การควบคุมองค์กร	การติดต่อกับเจ้าหน้าที่
A.5.6	การควบคุมองค์กร	การติดต่อกับกลุ่มผลประโยชน์พิเศษ
ใหม่ A.5.7	การควบคุมองค์กร	ข่าวกรองภัยคุกคาม LRQA NETTITUDE คลิกเพื่อดูข้อมูลเพิ่มเติม
A.5.8	การควบคุมองค์กร	ความปลอดภัยของข้อมูลในการจัดการโครงการ
A.8.1	ทางเทคนิค	อุปกรณ์ปลายทางของผู้ใช้
A.6.7	บุคคล	การทำงานระยะไกล

ความมั่นคงด้านทรัพยากรบุคคล		
A.6.1	บุคคล	การคัดกรอง
A.6.2	บุคคล	ข้อกำหนดและเงื่อนไขการจ้างงาน
A.5.4	การควบคุมองค์กร	ความรับผิดชอบของฝ่ายบริหาร
A.6.3	บุคคล	ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความปลอดภัยของข้อมูล
A.6.4	บุคคล	กระบวนการทางวินัย
A.6.5	บุคคล	ความรับผิดชอบหลังการเลิกจ้างหรือการเปลี่ยนแปลงการจ้างงาน
การบริหารสินทรัพย์		
A.5.9	การควบคุมองค์กร	รายการข้อมูลและสินทรัพย์อื่นที่เกี่ยวข้อง
A.8.1.2	**รวมไว้เป็น A.5.9**	
A.5.10	การควบคุมองค์กร	การใช้ข้อมูลและทรัพย์สินอื่น ๆ ที่เกี่ยวข้องที่ยอมรับได้
A.5.11	การควบคุมองค์กร	การคืนสินทรัพย์
A.5.12	การควบคุมองค์กร	การจำแนกประเภทของข้อมูล
A.5.13	การควบคุมองค์กร	การระบุประเภทข้อมูล
A.8.2.3	**รวมไว้เป็น A.5.10**	
A.7.10	ทางกายภาพ	สื่อจัดเก็บข้อมูล
A.8.3.2	**รวมไว้เป็น A.7.10**	
A.8.3.3	**รวมไว้เป็น A.7.10**	

การควบคุมการเข้าถึง		
A.5.15	การควบคุมองค์กร	การควบคุมการเข้าถึง
A.9.1.2	**รวมไว้เป็น A.5.15**	
A.5.16	การควบคุมองค์กร	การจัดการข้อมูลประจำตัว
A.5.18	การควบคุมองค์กร	สิทธิ์ในการเข้าถึง
A.8.2	ทางเทคนิค	สิทธิ์การเข้าถึงพิเศษ
A.5.17	การควบคุมองค์กร	ข้อมูลการตรวจสอบตัวตน
A.9.2.5	**รวมไว้เป็น A.5.18**	
A.9.2.6	**รวมไว้เป็น A.5.18**	
A.9.3.1	**รวมไว้เป็น A.5.17**	
A.8.3	ทางเทคนิค	การจำกัดการเข้าถึงข้อมูล
A.8.5	ทางเทคนิค	การตรวจสอบตัวตนอย่างปลอดภัย
A.9.4.3	**รวมไว้เป็น A.5.17**	
A.8.18	ทางเทคนิค	การใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษ
A.8.4	ทางเทคนิค	การเข้าถึงซอร์สโค้ด
การเข้ารหัส		
A.8.24	ทางเทคนิค	การใช้การเข้ารหัส
รวมไว้เป็น A.8.24 กับ A.10.1.1		

ความปลอดภัยทางกายภาพและสิ่งแวดล้อม			
	A.7.1	ทางกายภาพ	ขอบเขตการรักษาความปลอดภัยทางกายภาพ
	A.7.2	ทางกายภาพ	การเข้าสู่พื้นที่ทางกายภาพ
	A.7.3	ทางกายภาพ	การรักษาความปลอดภัยสำนักงาน ห้องพัก และสิ่งอำนวยความสะดวก
ใหม่	A.7.4	ทางกายภาพ	การตรวจสอบความปลอดภัยทางกายภาพ
	A.7.5	ทางกายภาพ	การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม
	A.7.6	ทางกายภาพ	การทำงานในพื้นที่ที่ปลอดภัย
A.11.1.6		**รวมไว้เป็น A.7.2 กับ A.11.1.2**	
	A.7.8	ทางกายภาพ	การจัดตั้งและการป้องกันอุปกรณ์
	A.7.11	ทางกายภาพ	สาธารณูปโภคเสริม
	A.7.12	ทางกายภาพ	การรักษาความปลอดภัยของสายเคเบิล
	A.7.13	ทางกายภาพ	การบำรุงรักษาอุปกรณ์
A.11.2.5		**รวมไว้เป็น A.7.10**	
	A.7.9	ทางกายภาพ	ความปลอดภัยของทรัพย์สินนอกสถานที่
	A.7.14	ทางกายภาพ	การทิ้งหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย
A.11.2.8		**รวมไว้เป็น A.8.1 กับ A.6.2.1**	
	A.7.7	ทางกายภาพ	โต๊ะทำงานปลอดเอกสารสำคัญและหน้าจอคอมพิวเตอร์ที่สะอาด

ความปลอดภัยในการดำเนินงาน			
	A.5.37	การควบคุมองค์กร	ขั้นตอนการปฏิบัติงานที่บันทึกเป็นเอกสาร
	A.8.32	ทางเทคนิค	การจัดการความเปลี่ยนแปลง
	A.8.6	ทางเทคนิค	การจัดการสมรรถภาพ
	A.8.31	ทางเทคนิค	การแยกสภาพแวดล้อมการพัฒนา การทดสอบ และการผลิต
	A.8.7	ทางเทคนิค	การป้องกันมัลแวร์
	A.8.13	ทางเทคนิค	การสำรองข้อมูล
	A.8.15	ทางเทคนิค	การบันทึก
	A.12.4.2	**รวมไว้เป็น A.8.1.5**	
	A.12.4.3	**รวมไว้เป็น A.8.1.5**	
ใหม่	A.8.16	ทางเทคนิค	กิจกรรมการตรวจสอบ
ใหม่	A.8.17	ทางเทคนิค	การซิงโครไนซ์นาฬิกา
ใหม่	A.8.19	ทางเทคนิค	การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ
ใหม่	A.8.8	ทางเทคนิค	การจัดการช่องโหว่ทางเทคนิค
ใหม่	A.8.9	ทางเทคนิค	การจัดการการกำหนดค่า
ใหม่	A.8.10	ทางเทคนิค	การลบข้อมูล
ใหม่	A.8.11	ทางเทคนิค	การปิดบังข้อมูล
ใหม่	A.8.12	ทางเทคนิค	การป้องกันการรั่วไหลของข้อมูล
	A.12.6.2	**รวมไว้เป็น A.8.19 กับ A.12.5.1**	
	A.12.7.1 A.8.34	ทางเทคนิค	การปกป้องระบบข้อมูลระหว่างการทดสอบการตรวจสอบ

ความปลอดภัยของการสื่อสาร			
	A.8.20	ทางเทคนิค	ความปลอดภัยของเครือข่าย
	A.8.21	ทางเทคนิค	ความปลอดภัยของบริการในเครือข่าย
	A.8.22	ทางเทคนิค	การแยกส่วนเครือข่าย
ใหม่	A.8.23	ทางเทคนิค	การกรองเว็บ
	A.5.14	การควบคุมองค์กร	การถ่ายโอนข้อมูล
	A.13.2.2	**รวมไว้เป็น A.5.14**	
	A.13.2.3	**รวมไว้เป็น A.5.14**	
	A.6.6	บุคคล	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูล
การจัดหา การพัฒนา และการบำรุงรักษาระบบ			
	A.14.1.1	**รวมไว้เป็น A.5.8 กับ A.6.1.5**	
	A.8.26	ทางเทคนิค	ข้อกำหนดด้านความปลอดภัยของแอปพลิเคชัน
	A.14.1.3	**รวมกับ A.8.26**	
	A.8.2.5	ทางเทคนิค	วงจรชีวิตของการพัฒนาอย่างปลอดภัย
	A.14.2.2	**รวมไว้เป็น A.8.32 กับ A.12.1.2**	
	A.14.2.3	**รวมไว้เป็น A.8.32 กับ A.12.1.2, A.14.2.2 และ A.14.2.4**	
	A.14.2.4	**รวมไว้เป็น A.8.32 กับ A.12.1.2, A.14.2.2 และ A.14.2.3**	
	A.14.2.5 A.8.27	ทางเทคนิค	หลักการทางสถาปัตยกรรมและวิศวกรรมสำหรับระบบรักษาความปลอดภัย
	A.14.2.6	**รวมไว้เป็น A.8.31 กับ A.12.1.4**	
ใหม่	A.8.28	ทางเทคนิค	การเข้ารหัสอย่างปลอดภัย
	A.8.30	ทางเทคนิค	การพัฒนาที่ว่าจ้างบุคคลภายนอก
	A.8.29	ทางเทคนิค	การทดสอบความปลอดภัยในการพัฒนาและการยอมรับ
	A.14.2.9	**รวมไว้เป็น A.8.29 กับ A.14.2.8**	
	A.8.33	ทางเทคนิค	ข้อมูลการทดสอบ

ความสัมพันธ์กับซัพพลายเออร์			
	A.5.19	การควบคุมองค์กร	ความปลอดภัยของข้อมูลในความสัมพันธ์กับซัพพลายเออร์
	A.5.20	การควบคุมองค์กร	การจัดการความปลอดภัยของข้อมูลภายในข้อตกลงสำหรับซัพพลายเออร์
	A.5.21	การควบคุมองค์กร	การจัดการความปลอดภัยของข้อมูลในห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)
	A.5.22	การควบคุมองค์กร	การตรวจสอบ ทบทวน และจัดการการเปลี่ยนแปลงบริการของซัพพลายเออร์
	A.15.2.2	**รวมไว้กับ A.5.22 กับ A.15.2.1**	
ใหม่	A.5.23	การควบคุมองค์กร	ความปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์
การจัดการเหตุการณ์ด้านความปลอดภัยของข้อมูล			
	A.5.24	การควบคุมองค์กร	การวางแผนและการเตรียมการจัดการเหตุการณ์ด้านความปลอดภัยของข้อมูล
	A.6.8	บุคคล	การรายงานเหตุการณ์ด้านความปลอดภัยของข้อมูล
	A.16.1.3	**รวมไว้เป็น A.6.8 กับ A.16.1.2**	
	A.16.1.4 A.5.25	การควบคุมองค์กร	การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความปลอดภัยของข้อมูล
	A.16.1.5 A.5.26	การควบคุมองค์กร	การตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของข้อมูล
	A.16.1.6 A.5.27	การควบคุมองค์กร	การเรียนรู้จากเหตุการณ์ด้านความปลอดภัยของข้อมูล
	A.16.1.7 A.5.28	การควบคุมองค์กร	การรวบรวมหลักฐาน
แง่มุมด้านความมั่นคงปลอดภัยของข้อมูลในการบริหารความต่อเนื่องทางธุรกิจ			
	A.17.1.1 A.5.29	การควบคุมองค์กร	ความปลอดภัยของข้อมูลในช่วงที่เกิดการหยุดชะงัก
	A.17.1.2	**รวมไว้เป็น A.5.29 กับ A.17.1.1, A.17.1.3**	
	A.17.1.3	**รวมไว้เป็น A.5.29 กับ A.17.1.1, A.17.1.2**	
ใหม่	A.5.30	การควบคุมองค์กร	ความพร้อมด้านไอซีทีเพื่อความต่อเนื่องทางธุรกิจ
	A.8.14	ทางเทคนิค	ความซ้ำซ้อนของสิ่งอำนวยความสะดวกสำหรับการประมวลผลข้อมูล

การปฏิบัติตามกฎ		
A.5.31	การควบคุมองค์กร	ข้อกำหนดตามกฎหมาย ที่กฎหมายกำหนด ข้อบังคับ และสัญญา
A.5.32	การควบคุมองค์กร	สิทธิ์ในทรัพย์สินทางปัญญา
A.5.33	การควบคุมองค์กร	การป้องกันระเบียน
A.5.34	การควบคุมองค์กร	ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII)
A.18.1.5	**รวมไว้เป็น A.5.31 กับ A.18.1.1**	
การทบทวนความปลอดภัยของข้อมูล		
A.5.35	การควบคุมองค์กร	การทบทวนความปลอดภัยของข้อมูลอย่างเป็นอิสระ
A.5.36	การควบคุมองค์กร	การปฏิบัติตามนโยบาย กฎ และมาตรฐานสำหรับความปลอดภัยของข้อมูล
A.18.2.3	**รวมไว้เป็น A.5.36 กับ A.18.2.2**	

บริการฝึกอบรมและตรวจสอบ ISO 27001:2022 ของเรา

การฝึกอบรม

เสริมสร้างความรู้ของคุณเกี่ยวกับ ISO 27001:2022 กับหลักสูตรมากมายที่ออกแบบมาสำหรับ ระดับประสบการณ์ที่แตกต่างกัน - ผ่านวิธีการเรียนรู้หลายรูปแบบ

การวิเคราะห์ช่องว่าง

บริการเสริมที่หนึ่งในผู้ตรวจสอบที่เชี่ยวชาญของเราจะช่วยคุณระบุประเด็นวิกฤต มีความเสี่ยงสูง หรือเป็นจุดอ่อนใน ระบบของคุณก่อน ตรวจสอบการเปลี่ยนผ่าน

การตรวจสอบการเปลี่ยนผ่าน

เราจะประเมิน ISMS ของคุณตามข้อกำหนด ISO 27001:2022 โดยมุ่งเน้นที่ การควบคุมในภาคผนวก A และ ผลกระทบต่อระบบของคุณโดยเฉพาะ

การตรวจสอบแบบบูรณาการ

หากคุณใช้ระบบการจัดการหลายระบบคุณจะได้รับประโยชน์จากโปรแกรมการตรวจสอบและการเฝ้าระวังแบบบูรณาการ ซึ่งมีประสิทธิภาพและคุ้มค่ากว่า

ทำงานร่วมกับคุณเพื่อมุ่งเป้ารักษาความปลอดภัยทางไซเบอร์ทุกแง่มุม

ประสบการณ์เชิงลึกของเราในการประกัน รวมกับบริการรักษาความปลอดภัยทางไซเบอร์ที่ได้รับรางวัลและระบบอัจฉริยะที่ปรับตามภัยคุกคามช่วยให้เราสามารถส่งมอบข้อมูลเชิงลึกตามความต้องการและมอบการป้องกันภัยคุกคามที่ไม่เหมือนใครซึ่งธุรกิจของคุณกำลังเผชิญอยู่ได้ ทำให้คุณก้าวนำหน้าความเสี่ยงทางไซเบอร์หนึ่งก้าวในวันนี้ พรุ่งนี้ และในอนาคต

เราให้บริการตรวจสอบ ฝึกอบรม และรับรองตามมาตรฐานและแนวทางระหว่างประเทศชั้นนำ พร้อมบริการรักษาความปลอดภัยทางไซเบอร์ขั้นสูงที่หลากหลาย ซึ่งจัดทำโดย Nettitude ผู้เชี่ยวชาญของเรา

เราทำงานร่วมกับธุรกิจของคุณ - ช่วยให้คุณระบุภัยคุกคามเฉพาะที่คุณเผชิญ และพัฒนากลยุทธ์เพื่อบรรเทาภัยคุกคามเหล่านั้น เราจะทำงานร่วมกับคุณเพื่อรับรองระบบของคุณ ระบุช่องโหว่ และช่วยป้องกันการโจมตีและเหตุการณ์ที่อาจส่งผลกระทบต่อความสมบูรณ์ของแบรนด์ การเงิน และการดำเนินงานของคุณ

ความปลอดภัยของข้อมูล

บริการด้านการปฏิบัติตามข้อกำหนดและการรับรองของเราช่วยคุณปกป้องข้อมูลที่สำคัญต่อธุรกิจและแสดงให้เห็นแนวทางปฏิบัติที่ดีที่สุดที่ได้รับการยอมรับในระดับสากล

อ่านเพิ่มเติม >

ความยืดหยุ่นในการดำเนินงาน

เตรียมพร้อมที่จะป้องกัน ตอบสนอง และฟื้นฟูจากการหยุดชะงักด้วยบริการการรับรอง การฝึกอบรมและการกำกับดูแลความเสี่ยงและการปฏิบัติตามข้อกำหนดของเรา

อ่านเพิ่มเติม >

การป้องกันภัยคุกคามทางไซเบอร์

ก้าวนำหน้าภัยคุกคามทางไซเบอร์ไปหนึ่งก้าวด้วยโซลูชันที่ปรับแต่งมาโดยเฉพาะ ซึ่งให้การป้องกันและตอบสนองต่อการโจมตีทางไซเบอร์ทุกประเภท

อ่านเพิ่มเติม >

รู้จัก ThreatWatcher

บริการ ThreatWatcher ของ LRQA Nettitude ให้การประเมินพร้อมการจัดการโดยใช้ระบบลาดตระเวนและวิเคราะห์ขั้นสูงเพื่อระบุภัยคุกคามที่ไม่รู้จักมาก่อน ซึ่งสามารถใช้ในการโจมตีทางไซเบอร์ได้ ความปลอดภัยข่าวกรองจาก ThreatWatcher สามารถชี้ให้เห็นจุดอ่อนในการให้ข้อมูลผู้ใช้และช่วยระบุ พื้นที่การโจมตีแบบดิจิทัลอย่างที่ไม่เคยทำได้มาก่อน Threat Watcher จาก Nettitude ให้บริการโดยทีม นักวิเคราะห์ข่าวกรองภัยคุกคามที่มีทักษะและประสบการณ์สูง ดูแลระบบโดยแพลตฟอร์ม Recorded Future

ThreatWatcher และ ISO 27001:2022

ระบบข่าวกรองภัยคุกคาม A.5.7 ซึ่งเป็นระบบควบคุมองค์กรแบบใหม่ กำหนดให้องค์กรต้องรวบรวม วิเคราะห์ และสร้างข่าวกรองภัยคุกคามเกี่ยวกับภัยคุกคามด้านความปลอดภัยของข้อมูล

เป้าหมายของการควบคุมแบบใหม่นี้คือการทำให้องค์กรมีความเข้าใจอย่างลึกซึ้งยิ่งขึ้นเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยการรวบรวม วิเคราะห์ และกำหนดบริบทข้อมูลเกี่ยวกับการโจมตีทางไซเบอร์ทั้งในปัจจุบันและอนาคตนอกจากนี้ยังออกแบบมาเพื่อช่วยให้องค์กรเข้าใจว่าแฮ็กเกอร์จะเจาะระบบของพวกเขาได้อย่างไร และแจ้งให้บริษัททราบเกี่ยวกับประเภทของข้อมูลที่ผู้โจมตีต้องการ

ThreatWatcher นำเสนอโซลูชันที่แน่นอนเหล่านี้ ช่วยให้องค์กรแสดงให้เห็นการปฏิบัติตามระบบควบคุมข่าวกรองภัยคุกคามแบบใหม่

ติดต่อผู้เชี่ยวชาญของเราเพื่อรับข้อมูลเพิ่มเติมเกี่ยวกับ ThreatWatcher และบริการอื่น ๆ จาก LRQA Nettitude ที่สามารถช่วยสาธิตการปฏิบัติตามข้อกำหนด และระบบควบคุมใหม่ที่ใช้ใน ISO 27001:2022

อ่านเพิ่มเติม →

อนาคตของคุณ คือสิ่งที่เราให้ความสำคัญ

เกี่ยวกับ LRQA:

ด้วยการรวบรวมความเชี่ยวชาญที่ไม่มีใครเทียบได้ในด้านการรับรอง การรับประกันแบรนด์ และการฝึกอบรม LRQA จึงเป็นหนึ่งในผู้ให้บริการชั้นนำระดับโลกด้านความปลอดภัยด้านอาหารและโซลูชันการรับประกัน เราทำงานร่วมกับฟาร์ม กิจการประมง ผู้ผลิตอาหาร ร้านอาหาร โรงแรม และผู้ค้าปลีกทั่วโลกเพื่อช่วยจัดการความเสี่ยงด้านความปลอดภัยและความยั่งยืนของอาหารตลอดห่วงโซ่อุปทาน และก้าวมาเป็นผู้ให้บริการด้านประกันชั้นนำระดับโลก

เราภูมิใจในมรดกของเรา แต่สิ่งที่สำคัญจริง ๆ ก็คือตัวตนของเราในปัจจุบัน เพราะนั่นคือสิ่งที่หล่อหลอมการสร้างความเป็นพันธมิตรกับลูกค้าของเราในอนาคต ด้วยการผสมผสานค่านิยมที่แข็งแกร่ง ประสบการณ์หลายสิบปีในการบริหารความเสี่ยงและการบรรเทาผลกระทบ และความใส่ใจในอนาคต เราพร้อมสนับสนุนลูกค้าของเราในขณะที่พวกเขาสร้างธุรกิจที่ปลอดภัย มั่นคงและยั่งยืนมากขึ้น

ตั้งแต่การตรวจสอบแบบอิสระ การรับรอง และการฝึกอบรม ไปจนถึงบริการให้คำปรึกษาด้านเทคนิค เทคโนโลยีการประกันแบบเรียลไทม์ และการเปลี่ยนแปลงห่วงโซ่อุปทานที่ขับเคลื่อนด้วยข้อมูล โซลูชันแบบครบวงจรที่เป็นนวัตกรรมใหม่ของเราจะช่วยให้ลูกค้าของเราสามารถรับมือกับภูมิทัศน์ของความเสี่ยงที่เปลี่ยนแปลงอย่างรวดเร็ว เพื่อให้แน่ใจว่าพวกเขาเป็นผู้กำหนดอนาคตของตนเอง แทนที่จะถูกอนาคตกำหนด

ติดต่ อเรา

เย ยี มชม www.lrqa.com/th หากต้ องการข้ อมูลเพ่มิ เติม ติดต่ อท่ อีเมล enquiries.th@lrqa.com หรือโทร +66 24590252

LRQA

Muang Thai - Phatra Complex Tower B,
Rachadaphisek Road, Huaykwang 10310
Bangkok, Thailand