การประเมินและการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ [Risk Assessment and Risk Treatment (Threat & Vulner.) of Cybersecurity Act.]

ผู้พิจารณาประเมิน : สมาชิกคณะกรรมการพิจารณาความเสี่ยง
ผู้บันทึก : นาย สุรศักดิ์ มั่นคง, สมาชิกคณะกรรมการพิจารณาความเสี่ยง
วันที่ทำการประชุมความเสี่ยงพร้อมบันทึก : 6 ก.ย. 67
สถานที่ : Data Center of HQ
ที่อยู่ : 89/999 ถนนสุรวงศ์ ปทุมวัน กทม 10320
ระบบบริการที่สำคัญ : All critical application

มาตรการควบคุมไซเบอร์ขั้นต่ำ	
ผลการประเมินความเสี่ยง (เฉลี่ย) โดยรวมขององค์กร (16 Clusters, 160 Risk Id.)	7.5

	Risk Score
แดง (สูง) = 17 เอกสาร เป็นอย่างน้อย	7.0 - 25
เหลือง (ปานกลาง) = 13 เอกสาร เป็นอย่างน้อย	5.1- 6.9
เขียว (ต่ำ) = 10 เอกสาร เป็นอย่างน้อย	1 - 5.0

ผลการประเมินความเสี่ยง(เฉลี่ย) โดยรวมขององค์กร หลังจัดการความเสี่ยง	5.00
Residual Risk Level	

	Risk Score
เป็นความเสี่ยงขั้นวิกฤติ ต้องมีการดำเนินการโดยทันที	12.50 - 25.00
เป็นความเสี่ยงสูง ต้องมีการดำเนินการบางอย่างเพื่อลดความเสี่ยง	9.50 - 12.49
เป็นความเสี่ยงปานกลาง ต้องมีการติดตามและอาจมีมาตรการป้องกัน	5.01 - 9.49
ต้องมีการติดตามเป็นระยะ แต่ยังไม่ต้องมีการดำเนินการใดๆเพิ่มเติม	1 - 5.0

PART 1 : RISK ASSESSMENT

No.	หมวดหมู่ความเสี่ยง (Risk Cluster)	ระบุความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ (Risk Identification)		มาตรการควบคุมในปัจจุบัน	มีผลกระทบต่อ			มีผลต่อความรุนแรงแต่ละด้าน						Risk Analysis A	B	C = A*B	เจ้าของความเสี่ยง (Risk Owner)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk Level) - ของแต่ละ Cluster
		ภัยคุกคาม (Threat)	ช่องโหว่ (Vulner.)		C	I	A	B/F	S	R	I	L	O	โอกาสเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)		
	กรอบมาตรฐาน																	
1	การโจมตีด้วยมัลแวร์ (Malware Attacks)	1. มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงด้วยมัลแวร์	1. ไม่มีระบบหรือมาตรการควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ในองค์กร	รพ มีระบบป้องกันการดาวน์โหลด	-	-	x	x	x	x	x	-	-	1	5	5	CSMR	11.0
		2. มีการติดมัลแวร์ที่มาจากการใช้อุปกรณ์ USB Storage หรือสื่อเก็บข้อมูลภายนอก	2. ไม่มีการติดตั้งหรืออัปเดตโปรแกรมป้องกันไวรัสเมื่อใช้อุปกรณ์ USB Storage	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	3	5	15	CSMR	
		3. ไฟล์แนบในอีเมล์มีฟิชชิงและแฝงด้วยมัลแวร์	3. ขาดระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งาน อีเมล์ที่มีไฟล์แนบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	2	5	10	CSMR	
		4. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ฝังด้วยมัลแวร์	4. พนักงานขาดความรู้ในการติดตั้งไฟล์หรือเว็บไซต์ที่มีความเสี่ยงไซเบอร์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	3	3	9	CSMR	
		5. พนักงานเข้าถึงโฆษณาออนไลน์ (Malvertising) ตามเว็บต่างๆ ที่พาไปยังเว็บไซต์ที่มีมัลแวร์	5. ไม่มีระบบกรองเว็บไซต์ ที่ป้องกันมัลแวร์และอัพเดทเป็นประจำ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	4	4	16	CSMR	
2	การโจมตีด้วยฟิชชิง (Phishing Attacks)	1. การรับอีเมล์ที่มีฟิชชิงหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน	1. ขาดการฝึกอบรมพนักงาน เช่น พนักงานไม่สามารถแยกแยะอีเมล์หรือเว็บไซต์ปลอมได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	14.4
		2. Spear Phishing ที่กำหนดเป้าหมายเจาะจงบุคคลหรือหน่วยงานหลุดเข้ามาในระบบ	2. ไม่มีระบบตรวจจับอีเมล์ฟิชชิง เช่น ไม่มีการใช้ตัวกรองอีเมล์เพื่อบล็อกอีเมล์ที่เป็นอันตราย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	
		3. มีการรับส่งลิงก์ที่มีฟิชชิงผ่าน SMS หรือโซเชียลมีเดีย	3. การใช้รหัสผ่านซ้ำหรือไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้ซ้ำในหลายระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	5	4	20	CSMR	
		4. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าล็อกอินขององค์กรหรือบริการออนไลน์	4. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	4	4	16	CSMR	
		5. ถูกระบบโทรศัพท์ปลอม (Call center) หลอกขอข้อมูลส่วนตัว	5. ไม่มีกระบวนการยืนยันการสื่อสารที่ปลอดภัย เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมล์หรือข้อความ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	
3	ภัยคุกคามจากบุคคลภายใน (Insider Threats)	1. การใช้งานข้อมูลโดยใช้อำนาจมิชอบ เช่น พนักงานที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	1. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น พนักงานบางคนได้รับสิทธิ์เข้าถึงข้อมูลมากเกินความจำเป็น	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	4	12	CSMR	8.0
		2. การรั่วไหลของข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจองค์กรส่งข้อมูลสำคัญให้คู่แข่งหรือบุคคลภายนอก	2. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ผิดปกติในระบบของพนักงาน	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	3	6	CSMR	
		3. กระทำผิดพลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญหรือแชร์ข้อมูลให้บุคคลที่ไม่เกี่ยวข้อง	3. ขาดการฝึกอบรมเกี่ยวกับการปกป้องข้อมูล เช่น พนักงานไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR	
		4. การใช้บัญชีที่ถูกยึดหรือถูกแฮ็ก (Inactive users) เช่น บัญชีของพนักงานที่ถูกยึดหรือแฮ็กมีการนำไปใช้ในการกระทำที่ไม่เหมาะสม	4. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากองค์กร เช่น บัญชีของพนักงานที่ลาออกยังคงสามารถเข้าถึงระบบได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR	
		5. มีการปลอมตัวเป็นบุคคลภายใน เช่น บุคคลภายนอกแฝงตัวเข้ามาในองค์กรผ่านการร่วมมือของพนักงานภายใน	5. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการคัดลอกหรือส่งออก	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	3	3	9	CSMR	
4	การละเมิดข้อมูล (Data Breaches)	1. มีการแฮ็กระบบเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้า หรือข้อมูลทางการเงิน	1. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	4	8	CSMR	9.4
		2. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่อ่อนแอ	2. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นผลเปิดช่องโหว่ให้ถูกโจมตี	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	5	10	CSMR	
		3. มีการรั่วไหลของข้อมูลผ่านพนักงาน (โดยเจตนาหรือไม่เจตนา)	3. การตั้งรหัสผ่านที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้รหัสผ่านซ้ำกันในหลายระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR	
		4. มีการส่งข้อมูลสำคัญผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมล์ที่ไม่มีการเข้ารหัส	4. ขาดระบบตรวจสอบการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	3	5	15	CSMR	
		5. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	5. ขาดการตรวจสอบกิจกรรมในระบบ เช่น ไม่มีการตรวจสอบกิจกรรมที่น่าสงสัยในระบบหรือการแจ้งเตือน	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	3	6	CSMR	
5	การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS)	1. พบว่ามีการส่งคำขอแปลกปลอมจำนวนมหาศาลเพื่อทำให้ระบบหยุดชะงัก	1. ไม่มีการกำหนดขีดจำกัดคำขอหรือกรองคำขอ เช่น ระบบไม่สามารถจำกัดจำนวนคำขอที่ส่งเข้ามาภายในช่วงเวลาที่กำหนดได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	1	5	5	CSMR	8.6
		2. ถูกการโจมตีแบบ DNS Amplification ที่เพิ่มปริมาณคำขอเพื่อให้ระบบของเรา (จุดเป้าหมาย) รับภาระเกินกำลัง	2. ระบบตรวจจับการโจมตีที่ไม่เพียงพอ เช่น ไม่มีเครื่องมือในการตรวจจับและตอบสนองต่อพฤติกรรมที่ผิดปกติ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	3	4	12	CSMR	
		3. ถูกการใช้ Botnet เพื่อกระจายการโจมตีจากหลายแหล่งไปยังเป้าหมาย	3. ไม่มีการใช้ Load Balancer เช่น ระบบไม่สามารถกระจายโหลดภาระของการประมวลผลคำขอไปยังเซิร์ฟเวอร์อื่นๆได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	2	4	8	CSMR	
		4. ถูกการโจมตีในระดับแอปพลิเคชัน เช่น การทำให้เว็บเซิร์ฟเวอร์ไม่สามารถรองรับคำขอที่ถูกต้องได้	4. ความปลอดภัยของ DNS และโปรโตคอลอยู่ในระดับต่ำ เช่น DNS Server ไม่มีการกำหนดค่าเพื่อป้องกันการโจมตี อาทิ DNS Spoofing หรือ Amplification	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	2	4	8	CSMR	
		5. ถูกการโจมตีโปรโตคอล เช่น SYN Flood, Ping of Death	5. มีการจัดการทรัพยากรระบบไม่เหมาะสม เช่น ระบบเซิร์ฟเวอร์ไม่มีแบนด์วิดท์หรือทรัพยากรเพียงพอที่จะรองรับการโจมตี	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	2	5	10	CSMR	
6	การโจมตีแบบ Man-in-the-Middle (MitM)	1. มีการดักฟังการสื่อสาร (Eavesdropping) เช่น แฮ็กเกอร์ดักจับข้อมูลระหว่างผู้ใช้และเซิร์ฟเวอร์ อาทิ รหัสผ่านหรือข้อมูลสำคัญ	1. การสื่อสารที่ไม่มีการเข้ารหัส เช่น การส่งข้อมูลผ่าน HTTP แทน HTTPS	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	x	-	x	x	x	x	x	-	2	3	6	CSMR	4.2
		2. ถูกการปลอมแปลงเว็บไซต์ (Spoofing) เช่น สร้างเว็บไซต์หรือเครือข่าย Wi-Fi ปลอมเพื่อหลอกให้ผู้ใช้ป้อนข้อมูล	2. เครือข่าย Wi-Fi สาธารณะ เช่น ไม่มีการตั้งค่าความปลอดภัย อาทิ WPA2/WPA3	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	x	-	x	x	x	x	x	-	2	3	6	CSMR	
		3. ถูกการโจมตีผ่าน Wi-Fi ที่ไม่ปลอดภัย เช่น การโจมตีในเครือข่าย Wi-Fi สาธารณะที่ไม่มีการเข้ารหัส	3. การไม่ตรวจสอบใบรับรอง SSL/TLS เช่น ผู้ใช้ไม่สามารถแยกแยะใบรับรองปลอมจากใบรับรองจริงได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	x	-	x	x	x	x	-	-	1	2	2	CSMR	
		4. มีการ Hijack เซสชัน (Session Hijacking) เช่น การเข้าควบคุมเซสชันของผู้ใช้งานที่เข้าสู่ระบบแล้ว	4. การขาดการยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ไม่มีการป้องกันเมื่อเซสชันของผู้ใช้ถูกแฮ็ก	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	x	-	x	x	x	x	-	-	1	2	2	CSMR	
		5. มีการปลอมใบรับรอง (Certificate Spoofing) เช่น การใช้ใบรับรอง SSL/TLS ปลอมเพื่อลวงผู้ใช้	5. การตั้งค่าอุปกรณ์ที่ไม่ปลอดภัย เช่น อุปกรณ์ IoT หรือเครือข่ายในองค์กรไม่มีการตั้งค่าความปลอดภัยที่เหมาะสม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	x	-	x	x	x	x	-	-	1	5	5	CSMR	
7	การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	1. มีการดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่แฝงแรนซัมแวร์ผ่านอีเมล์ฟิชชิง	1. การขาดการฝึกอบรมพนักงาน เช่น พนักงานเปิดไฟล์แนบที่เป็นอันตรายจากอีเมล์ฟิชชิง	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	4	5	20	CSMR	15.0
		2. ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	2. ซอฟต์แวร์และระบบปฏิบัติการที่ไม่ได้อัปเดต เช่น ระบบหรือซอฟต์แวร์ มีช่องโหว่ที่เปิดให้แรนซัมแวร์เข้าถึงได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	3	5	15	CSMR	
		3. มีการใช้ Remote Desktop Protocol (RDP) ที่ไม่ได้ตั้งค่าความปลอดภัย	3. การขาดการสำรองข้อมูล (Backup) เช่น ไม่มีระบบสำรองข้อมูลที่สามารถกู้คืนได้เมื่อถูกโจมตี	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	2	5	10	CSMR	
		4. มีการแอบแฝงแรนซัมแวร์ในอุปกรณ์ USB Storage หรืออุปกรณ์พกพาอื่นๆ	4. การตั้งค่าความปลอดภัยของ RDP ที่ไม่เหมาะสม เช่น เปิดใช้งาน RDP โดยไม่มีการควบคุมการเข้าถึงที่เข้มงวด	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	3	5	15	CSMR	
		5. มีการกระจายแรนซัมแวร์ผ่านเครือข่ายที่เชื่อมโยงกับองค์กร	5. การขาดระบบป้องกันมัลแวร์ที่มีประสิทธิภาพ เช่น ไม่มีซอฟต์แวร์ป้องกันแรนซัมแวร์ที่สามารถตรวจจับและบล็อกการโจมตี	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	3	5	15	CSMR	
8	การโจมตีด้วยวิศวกรรมสังคม (Social Engineering)	1. Phishing - มีการส่งอีเมล์หรือข้อความที่ดูน่าเชื่อถือเพื่อหลอกให้ผู้ใช้งาน ให้ข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลส่วนตัว	1. การขาดความตระหนักของพนักงาน เช่น พนักงานไม่เข้าใจความเสี่ยงจาก Social Engineering	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR	
		2. Spear Phishing - ถูกการโจมตีที่ใช้การกำหนดเป้าหมายเฉพาะบุคคลหรือหน่วยงานเฉพาะ โดยใช้ข้อมูลส่วนตัวของผู้ใช้งาน เพื่อเพิ่มความน่าเชื่อถือ	2. ไม่มีการตรวจสอบตัวตนของผู้ขอข้อมูล เช่น ขาดกระบวนการยืนยันตัวตนก่อนให้ข้อมูลสำคัญ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR	

PART 2 : RISK TREATMENT

Cluster	ตัวเลือกการตอบสนอง (Risk Treatment)	No.	แผนจัดการความเสี่ยง (Risk Treatment Plan) หัวข้อ	รายละเอียด	คาดว่าดำเนินการแล้วเสร็จ (Expected finish date)
1	Continue Monitoring	1			
	Mitigate Risk	2	**ควบคุมการใช้งาน USB และอุปกรณ์พกพา**	ออกนโยบาย BYOD (Bring Your Own Device) พร้อมกำหนดข้อบังคับในการใช้งานอุปกรณ์ส่วนตัว	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**การให้ความรู้และฝึกอบรมพนักงาน**	จัดอบรมเกี่ยวกับการหลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**สร้างระบบสำรองข้อมูล (Backup)**	กำหนดการสำรองข้อมูลอัตโนมัติเป็นระยะ ๆ	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**ใช้เครื่องมือความปลอดภัยแบบครบวงจร (Security Suites)**	ติดตั้งแพลตฟอร์ม SIEM (Security Information and Event Management) เพื่อตรวจสอบกิจกรรมที่น่าสงสัย	ภายใน 30 ก.ย. 67
2	Mitigate Risk	1	**ให้ความรู้และฝึกอบรมพนักงาน**	จัดอบรมพนักงานเกี่ยวกับวิธีการระบุอีเมลและลิงก์ฟิชชิง เช่น การตรวจสอบ URL และหัวข้ออีเมล	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)**	เปิดใช้งาน MFA สำหรับทุกบัญชี โดยเฉพาะบัญชีที่เกี่ยวข้องกับข้อมูลสำคัญ	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**ตรวจสอบและควบคุมการเข้าถึงเว็บไซต์**	ใช้ระบบ Web Filtering เพื่อบล็อกการเข้าถึงเว็บไซต์ฟิชชิง	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**ใช้เครื่องมือ SIEM (Security Information and Event Management)**	ติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**นโยบายการรายงานเหตุการณ์ (Incident Reporting)**	จัดทำนโยบายสำหรับพนักงานในการรายงานอีเมลหรือกิจกรรมที่น่าสงสัย	ภายใน 30 ก.ย. 67
3	Mitigate Risk	1	**การกำหนดสิทธิ์การเข้าถึง (Access Control)**	ใช้หลักการ Least Privilege เพื่อให้พนักงานเข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการทำงาน	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**การฝึกอบรมพนักงาน**	ให้ความรู้เกี่ยวกับการป้องกันการรั่วไหลของข้อมูลและผลกระทบของการกระทำโดยมิชอบ	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**การเข้ารหัสข้อมูลสำคัญ**	ใช้การเข้ารหัสข้อมูลที่สำคัญในทุกขั้นตอน รวมถึงการจัดเก็บและการส่งข้อมูล	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**นโยบายและกระบวนการตรวจสอบความปลอดภัย**	สร้างกระบวนการตรวจสอบกิจกรรมของผู้ใช้งาน เช่น Log Review และ Audit Trail	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**สร้างโปรแกรม Insider Threat Program (ITP)**	ตั้งทีมเฉพาะกิจเพื่อตรวจสอบและจัดการภัยคุกคามจากบุคคลภายใน	ภายใน 30 ก.ย. 67
4	Mitigate Risk	1	**การเข้ารหัสข้อมูล (Encryption)**	ใช้การเข้ารหัสข้อมูลทั้งในระหว่างการส่ง (In Transit) และขณะจัดเก็บ (At Rest)	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**กำหนดนโยบายรหัสผ่านที่เข้มงวด**	กำหนดให้ใช้รหัสผ่านที่ซับซ้อนและเปลี่ยนรหัสผ่านเป็นระยะ	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**ระบบตรวจสอบและแจ้งเตือนภัยคุกคาม**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อตรวจสอบและแจ้งเตือนกิจกรรมที่ผิดปกติ	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**ใช้ระบบสำรองข้อมูล (Backup)**	กำหนดให้มีการสำรองข้อมูลอัตโนมัติ และเก็บข้อมูลสำรองไว้ในระบบที่แยกออกจากระบบหลัก	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)**	สร้างกระบวนการตอบสนองเมื่อเกิดเหตุการณ์ Data Breach	ภายใน 30 ก.ย. 67
5	Mitigate Risk	1	**การติดตั้งระบบตรวจจับและป้องกัน DDoS (DDoS Protection Solutions)**	ใช้เครื่องมือ DDoS Mitigation เช่น Cloudflare, AWS Shield, หรือ Akamai เพื่อกรองคำขอที่เป็นอันตราย	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**กำหนดขีดจำกัดคำขอ (Rate Limiting)**	กำหนดจำนวนคำขอที่ระบบสามารถรับได้ต่อวินาทีต่อ IP Address	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**การเฝ้าระวังและแจ้งเตือนแบบเรียลไทม์**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อแจ้งเตือนพฤติกรรมที่น่าสงสัย	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**สร้างนโยบาย Incident Response Plan**	กำหนดขั้นตอนการตอบสนองต่อการโจมตี DoS/DDoS	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**การอัปเดตและป้องกันโปรโตคอล**	ปรับแต่ง TCP/IP Stack เพื่อป้องกันการโจมตี เช่น SYN Cookies	ภายใน 30 ก.ย. 67
6	Mitigate Risk	1	**ใช้โปรโตคอล HTTPS และ TLS**	บังคับให้ทุกการสื่อสารระหว่างผู้ใช้และเซิร์ฟเวอร์ใช้ HTTPS	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**หลีกเลี่ยงการใช้งาน Wi-Fi สาธารณะที่ไม่มีความปลอดภัย**	ใช้ VPN เพื่อเข้ารหัสข้อมูลขณะใช้งาน Wi-Fi สาธารณะ	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**การเฝ้าระวังและตรวจสอบการโจมตี**	ติดตั้งระบบ IDS/IPS (Intrusion Detection and Prevention Systems) เพื่อตรวจจับกิจกรรมที่ผิดปกติ	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**อัปเดตซอฟต์แวร์และเฟิร์มแวร์**	อัปเดตเบราว์เซอร์และระบบปฏิบัติการเพื่อป้องกันช่องโหว่ใหม่	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**การกำหนดค่าเครือข่ายที่ปลอดภัย**	ใช้ WPA3 สำหรับเครือข่าย Wi-Fi ในองค์กรและบ้าน	ภายใน 30 ก.ย. 67
7	Mitigate Risk	1	**การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันแรนซัมแวร์**	ใช้โปรแกรม Antivirus และ Antimalware ที่มีการตรวจจับแรนซัมแวร์โดยเฉพาะ	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**การสำรองข้อมูลอย่างสม่ำเสมอ**	ใช้กลยุทธ์ 3-2-1 Backup (สำรองข้อมูล 3 ชุด ใน 2 สื่อที่ต่างกัน และเก็บ 1 ชุดนอกสถานที่)	ภายใน 30 ก.ย. 67
	Mitigate Risk	3	**การฝึกอบรมพนักงาน**	ให้ความรู้เกี่ยวกับการตรวจสอบอีเมลฟิชชิงและไฟล์แนบที่น่าสงสัย	ภายใน 30 ก.ย. 67
	Mitigate Risk	4	**การใช้เทคโนโลยีการจำกัดสิทธิ์ (Access Control)**	ใช้หลักการ Least Privilege เพื่อให้สิทธิ์การเข้าถึงเฉพาะที่จำเป็น	ภายใน 30 ก.ย. 67
	Mitigate Risk	5	**ใช้การเข้ารหัสข้อมูล**	เข้ารหัสข้อมูลที่สำคัญเพื่อป้องกันไม่ให้ผู้โจมตีเข้าถึงได้ง่าย	ภายใน 30 ก.ย. 67
8	Mitigate Risk	1	**การฝึกอบรมและสร้างความตระหนัก**	จัดอบรมพนักงานให้เข้าใจรูปแบบการโจมตี Social Engineering เช่น Phishing, Pretexting	ภายใน 30 ก.ย. 67
	Mitigate Risk	2	**การใช้เทคโนโลยีกรองและป้องกัน**	ติดตั้งระบบ Email Filtering เพื่อลดโอกาสที่อีเมลฟิชชิงจะเข้าสู่ระบบ	ภายใน 30 ก.ย. 67

PART 3 : PROGRESS

Cluster	No.	สถานะความคืบหน้า (Progress Status)	ผู้รับผิดชอบในการดำเนินการ
1	1	100%	
	2	80%	
	3	100%	
	4	50%	
	5	100%	
2	1	77%	
	2	100%	
	3	88%	
	4	33%	
	5	22%	
3	1	100%	
	2	33%	
	3	100%	
	4	100%	
	5	66%	
4	1	23%	
	2	100%	
	3	100%	
	4	2%	
	5	100%	
5	1	67%	
	2	100%	
	3	65%	
	4	43%	
	5	100%	
6	1	100%	
	2	100%	
	3	34%	
	4	100%	
	5	55%	
7	1	100%	
	2	100%	
	3	55%	
	4	100%	
	5	66%	
8	1	100%	
	2	100%	

PART 4 : RISK EVALUATION AFTER RESOLVED 100 %

ความเสี่ยงที่คงเหลืออยู่ (Risk Residual)

Cluster	No.	กระทบต่อ C	I	A	ความรุนแรงแต่ละด้าน B/F	S	R	I	L	O	โอกาสเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยงที่คงเหลือ (Risk Residual Level)	ดำเนินการเพิ่มเติมเพื่อลดความเสี่ยงให้น้อยลงอีก (Further actions to be taken to further minimize risk)
1	1	x	x	x	x	-	-	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
2	1	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
3	1	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
4	1	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
5	1	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
6	1	x	x	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	x	x	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	x	x	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
7	1	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	3	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	4	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	5	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
8	1	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
	2	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ

		3. Pretexting - มีการสร้างสถานการณ์หลอกลวง เช่น แอบอ้างเป็นฝ่าย IT เพื่อขอข้อมูลสำคัญ	3. ไม่มีการควบคุมการเข้าถึงพื้นที่ทางกายภาพ เช่น การเข้า-ออกพื้นที่สำคัญไม่ได้รับการควบคุมอย่างเข้มงวด	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR	7.6	Mitigate Risk	3	**การควบคุมการเผยแพร่ข้อมูลในโซเชียลมีเดีย**	ให้คำแนะนำพนักงานในการป้องกันการเผยแพร่ข้อมูลที่อาจถูกนำไปใช้โจมตี	ภายใน 30 ก.ย. 67	22%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. Baiting - มีการหลอกล่อ วางเหยื่อเพื่อให้ผู้ใช้งานนำไปใช้ เช่น อุปกรณ์ USB Storage ที่แฝงมัลแวร์เพื่อให้เป้าหมายหยิบไปใช้งาน	4. ขาดการป้องกันระบบสารสนเทศ เช่น ระบบไม่มีการกรองอีเมล์หรือเว็บไซต์ที่น่าสงสัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การจำกัดสิทธิ์การเข้าถึง (Access Control)**	ใช้หลักการ Least Privilege เพื่อให้พนักงานเข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการทำงาน	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. Tailgating - มีการเข้าถึงพื้นที่ที่มีการจำกัดการเข้าถึงพื้นที่ที่สำคัญ โดยติดตามผู้มีสิทธิ์เข้าไปในพื้นที่	5. การใช้โซเชียลมีเดียที่ไม่มีการควบคุม เช่น ข้อมูลสำคัญขององค์กรหรือพนักงานถูกเผยแพร่ในโซเชียลมีเดีย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)**	เพิ่มระดับการป้องกันเมื่อเข้าสู่ระบบสำคัญ เช่น การใช้รหัส OTP หรือแอปพลิเคชัน Authenticator	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
9	**ความเสี่ยงด้านความปลอดภัยของคลาวด์ (Cloud Security Risks)**	1. การตั้งค่าคลาวด์ที่ไม่ปลอดภัย (Misconfiguration) เช่น การเปิดเผยข้อมูลที่สำคัญบางอย่างบนอินเทอร์เน็ตเนื่องจากการตั้งค่าที่ผิดพลาด จึงต้องยอมเปิดเผย	1. ขาดการตรวจสอบการตั้งค่าที่รัดกุม เช่น ไม่มีการตรวจสอบหรือปรับปรุงการตั้งค่าความปลอดภัยในระบบคลาวด์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	1	**การตั้งค่าคความปลอดภัยที่เหมาะสม**	ใช้ Security Tools เช่น AWS Config, Azure Security Center หรือ Google Cloud Security Command Center เพื่อตรวจสอบการตั้งค่า	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. ถูกการโจมตี API เช่น แฮ็กเกอร์โจมตี API ที่ไม่ได้รับการป้องกัน อาทิ API Key หรือ Token ที่ไม่ได้รับการเข้ารหัส	2. การควบคุมการเข้าถึงที่ไม่เหมาะสม เช่น สิทธิ์การเข้าถึงคลาวด์ถูกกำหนดอย่างไม่รัดกุม เช่น ทุกคนสามารถเข้าถึงได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR		Mitigate Risk	2	**การเข้ารหัสข้อมูล**	เข้ารหัสข้อมูลทั้งในขณะจัดเก็บ (At Rest) และขณะส่ง (In Transit) ด้วยโปรโตคอล TLS หรือ AES-256	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการขโมยข้อมูลในระหว่างการส่งข้อมูล เช่น การดักฟังข้อมูลที่ไม่ได้เข้ารหัสระหว่างการส่งข้อมูล	3. การขาดการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บหรือส่งผ่านคลาวด์ไม่ได้รับการเข้ารหัส	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR	5.6	Mitigate Risk	3	**การเฝ้าระวังและแจ้งเตือนแบบเรียลไทม์**	ใช้ SIEM (Security Information and Event Management) เพื่อตรวจสอบและแจ้งเตือนเมื่อมีเหตุการณ์ผิดปกติ	ภายใน 30 ก.ย. 67	88%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. มีการแฮ็กบัญชีผู้ใช้คลาวด์ เช่น ผู้โจมตีเข้าควบคุมบัญชีผ่านช่องโหว่ของรหัสผ่านหรือการฟิชชิง	4. การไม่ปฏิบัติตามกฎระเบียบหรือมาตรฐานความปลอดภัยของระบบคลาวด์ เช่น ระบบคลาวด์ไม่ได้รับการปรับให้สอดคล้องกับมาตรฐาน เช่น ISO 27001, 27018, 27701	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	1	4	4	CSMR		Mitigate Risk	4	**การตรวจสอบผู้ให้บริการคลาวด์**	ตรวจสอบว่าผู้ให้บริการคลาวด์ปฏิบัติตามมาตรฐานความปลอดภัย เช่น SOC 2, ISO 27001	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. ถูกมัลแวร์ในคลาวด์ เช่น การอัปโหลดไฟล์ที่แฝงมัลแวร์ขึ้นสู่ระบบคลาวด์และกระจายไปยังผู้ใช้รายอื่นๆ	5. การพึ่งพาผู้ให้บริการคลาวด์โดยไม่มีการตรวจสอบมาตรฐาน เช่น ขาดการตรวจสอบนโยบายความปลอดภัยของผู้ให้บริการคลาวด์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	4	4	CSMR		Mitigate Risk	5	**การตรวจสอบช่องโหว่ (Vulnerability Scanning)**	ใช้เครื่องมือสแกน เช่น Qualys หรือ Tenable เพื่อตรวจหาช่องโหว่ในระบบคลาวด์	ภายใน 30 ก.ย. 67	54%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
10	**ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)**	1. มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้จำหน่าย (3rd Party/Suppliers) ที่ไม่ได้มีการควบคุมความปลอดภัยอาจทำให้ข้อมูลขององค์กรรั่วไหล	1. การขาดกระบวนการตรวจสอบผู้จำหน่าย (3rd Party/Suppliers) เช่น ไม่มีการตรวจสอบความปลอดภัยของผู้จำหน่าย (3rd Party/Suppliers) ก่อนเซ็นต์สัญญา	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	1	**การตรวจสอบความปลอดภัยก่อนเลือกผู้จำหน่าย**	ใช้ Vendor Security Assessment Questionnaire เพื่อตรวจสอบมาตรการความปลอดภัย	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มีการโจมตีผ่านซัพพลายเชน (Supply Chain Attacks) เช่น ผู้โจมตีใช้ช่องโหว่ของซัพพลายเออร์เพื่อเข้าถึงระบบองค์กร	2. ไม่มีข้อตกลงด้านความปลอดภัย (Security SLA) เช่น ขาดข้อตกลงที่กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	2	**การจัดการสิทธิ์การเข้าถึง (Access Control)**	ให้สิทธิ์เข้าถึงข้อมูลหรือระบบแก่ผู้จำหน่ายเฉพาะที่จำเป็นเท่านั้น (Principle of Least Privilege)	ภายใน 30 ก.ย. 67	65%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. พบว่าผู้จำหน่ายขาดการปฏิบัติตามกฎระเบียบ เช่น ผู้จำหน่ายไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดด้านความปลอดภัย เช่น ISO 27001, 27018, 27701	3. การเข้าถึงระบบที่ไม่เหมาะสม: ผู้จำหน่ายได้รับสิทธิ์เข้าถึงระบบมากเกินความจำเป็น	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR	5.6	Mitigate Risk	3	**การแบ่งชั้นข้อมูลที่แชร์กับผู้จำหน่าย**	จัดประเภทข้อมูลและแชร์เฉพาะข้อมูลที่จำเป็นเท่านั้น	ภายใน 30 ก.ย. 67	23%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. การพึ่งพาผู้จำหน่ายที่ไม่มีความมั่นคงในการบริการ เช่น ความล้มเหลวของผู้จำหน่าย อาทิ การหยุดให้บริการ อาจส่งผลกระทบต่อธุรกิจ	4. ขาดการเฝ้าระวังความปลอดภัยของผู้จำหน่าย เช่น ไม่มีการติดตามการปฏิบัติงานของผู้จำหน่ายในด้านความปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	4	**การประเมินความเสี่ยงของซัพพลายเชน**	ประเมินความเสี่ยงด้านความปลอดภัยของผู้จำหน่ายก่อนเริ่มโครงการ	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. การแชร์ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้มีการป้องกัน เช่น การส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีการเข้ารหัส	5. การแชร์ข้อมูลกับผู้จำหน่ายหลายๆ ราย ทำให้ยิ่งแชร์ข้อมูลกับผู้จำหน่ายมากๆ ความเสี่ยงที่ข้อมูลจะรั่วไหลก็ยิ่งสูง	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การจัดทำแผนรับมือเหตุการณ์ร่วมกับผู้จำหน่าย**	สร้าง Incident Response Plan ที่ครอบคลุมผู้จำหน่าย	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
11	**ความเสี่ยงของอุปกรณ์มือถือ (Mobile Device Risks) ขององค์กร**	1. มีการสูญหายหรือถูกขโมย เช่น อุปกรณ์ที่เก็บข้อมูลสำคัญถูกขโมยหรือสูญหายโดยไม่มีการป้องกัน	1. ไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลในอุปกรณ์ไม่ได้รับการเข้ารหัส ทำให้ง่ายต่อการเข้าถึงเมื่ออุปกรณ์สูญหาย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	1	**การเข้ารหัสข้อมูลในอุปกรณ์ (Encryption)**	เปิดใช้งานการเข้ารหัสข้อมูลในอุปกรณ์มือถือทั้งหมด	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มัลแวร์ในมือถือขององค์กร เช่น การติดตั้งแอปพลิเคชันที่มีมัลแวร์ซึ่งสามารถเข้าถึงข้อมูลในอุปกรณ์	2. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น อุปกรณ์ไม่มีการตั้งรหัสผ่านหรือการล็อกหน้าจอ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	2	**การใช้เครื่องมือจัดการอุปกรณ์มือถือ (Mobile Device Management - MDM)**	ใช้ MDM เพื่อติดตาม ควบคุม และจัดการอุปกรณ์ที่เชื่อมต่อกับเครือข่ายองค์กร	ภายใน 30 ก.ย. 67	44%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการโจมตีผ่าน Wi-Fi สาธารณะ เช่น การดักจับข้อมูลจากอุปกรณ์ที่เชื่อมต่อเครือข่าย Wi-Fi ที่ไม่มีการป้องกัน	3. การดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ เช่น การติดตั้งแอปพลิเคชั่นจากร้านค้าที่ไม่ได้รับการรับรอง	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR	3.6	Mitigate Risk	3	**การอัปเดตซอฟต์แวร์และระบบปฏิบัติการ**	บังคับให้อุปกรณ์ติดตั้งอัปเดตซอฟต์แวร์และแพตช์ความปลอดภัยล่าสุด	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. Phishing ผ่านอุปกรณ์มือถือ เช่น การส่งข้อความหรืออีเมล์ ฟิชชิง เพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูล	4. การขาดการควบคุมการใช้งาน BYODในองค์กร เช่น ไม่มีนโยบาย BYOD (Bring Your Own Device) ที่ชัดเจน	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	4	**การกำหนดนโยบาย BYOD (Bring Your Own Device)**	สร้างนโยบาย BYOD ที่ระบุข้อกำหนดการใช้งานอุปกรณ์ส่วนตัวในเครือข่ายองค์กร	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การใช้ข้อมูลหรือแอปพลิเคชันในอุปกรณ์โดยผู้ไม่ได้รับอนุญาต	5. ไม่มีการอัปเดตระบบ เช่น อุปกรณ์ไม่ได้รับการอัปเดตซอฟต์แวร์และแพตช์ความปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	5	**การสำรองข้อมูล (Backup)**	ตั้งค่าให้มีการสำรองข้อมูลอัตโนมัติของอุปกรณ์มือถือไปยังระบบคลาวด์ที่ปลอดภัย	ภายใน 30 ก.ย. 67	45%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
12	**ซอฟต์แวร์และระบบที่มีช่องโหว่ (Vulnerable Software and Systems)**	1. พบว่ามีการใช้ช่องโหว่ของซอฟต์แวร์ที่ไม่ได้อัปเดตเพื่อเข้าควบคุมระบบ (Exploitation of Unpatched Software)	1. ซอฟต์แวร์และระบบที่ไม่ได้อัปเดต เช่น การใช้เวอร์ชันที่ล้าสมัยของซอฟต์แวร์และระบบปฏิบัติการ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	1	**การอัปเดตและติดตั้งแพตช์ (Patch Management)**	ใช้ระบบ Patch Management Tools เช่น WSUS หรือ SCCM เพื่อจัดการและติดตั้งแพตช์ความปลอดภัย	ภายใน 30 ก.ย. 67	100%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มีการโจมตีผ่านช่องโหว่ของระบบปฏิบัติการ เช่น การโจมตีแบบ Zero-Day	2. การตั้งค่าที่ไม่ปลอดภัย (Misconfiguration) เช่น การตั้งค่าซอฟต์แวร์หรือเซิร์ฟเวอร์ที่เปิดเผยข้อมูลสำคัญ ทำให้เปิดช่องโหว่	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	2	**การตั้งค่าความปลอดภัยของระบบ (Secure Configuration)**	ใช้ Security Hardening Guides เช่น CIS Benchmarks หรือ NIST เพื่อปรับแต่งการตั้งค่าให้ปลอดภัย	ภายใน 30 ก.ย. 67	100%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการโจมตีผ่านแอปพลิเคชันเว็บ เช่น SQL Injection, Cross-Site Scripting (XSS)	3. การใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ เช่น ซอฟต์แวร์ที่ไม่มีการรับประกันความปลอดภัย หรือไม่มีแพตช์อัปเดตหรือผ่านการถอดระหัสที่ไม่สมบรูณ์	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR	7.6	Mitigate Risk	3	**การตรวจสอบซัพพลายเชนของซอฟต์แวร์ (Software Supply Chain Security)**	เลือกใช้ซอฟต์แวร์จากผู้จัดจำหน่ายที่น่าเชื่อถือและมีประวัติการสนับสนุนที่ดี	ภายใน 30 ก.ย. 67	55%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. มีการแฝงมัลแวร์ในส่วนของปลั๊กอินหรือส่วนเสริมของซอฟต์แวร์	4. ไม่มีระบบจัดการช่องโหว่ เช่น ขาดเครื่องมือและกระบวนการในการค้นหาและแก้ไขช่องโหว่ในระบบ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การเฝ้าระวังและแจ้งเตือนแบบเรียลไทม์**	ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อเฝ้าระวังเหตุการณ์ที่ผิดปกติ	ภายใน 30 ก.ย. 67	100%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการใช้บริการหรือโปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet	5. ขาดการตรวจสอบซัพพลายเชนของซอฟต์แวร์ (Software Supply Chain) เช่น ไม่มีการตรวจสอบความน่าเชื่อถือของซอฟต์แวร์จากผู้จัดจำหน่าย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การทดสอบความปลอดภัย (Penetration Testing)**	ทำการทดสอบช่องโหว่ในระบบโดยผู้เชี่ยวชาญเพื่อค้นหาความเสี่ยงที่อาจเกิดขึ้น	ภายใน 30 ก.ย. 67	23%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
13	**ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)**	1. ถูกการโจมตีแบบ DDoS (Distributed Denial of Service) เช่น การส่งคำขอจำนวนมากเพื่อทำให้เครือข่ายหยุดทำงาน	1. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น การตั้งค่าเราเตอร์หรือไฟร์วอลล์ที่ไม่ปลอดภัย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	1	**การติดตั้งไฟร์วอลล์ (Firewall)**	ใช้ไฟร์วอลล์เพื่อควบคุมการเข้าถึงเครือข่ายและบล็อกการเข้าถึงที่ไม่ได้รับอนุญาต	ภายใน 30 ก.ย. 67	100%	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. ถูกการโจมตีแบบ Man-in-the-Middle (MitM) เช่น การดักฟังข้อมูลระหว่างการสื่อสารผ่านเครือข่าย	2. ไม่มีการแยกเครือข่าย (Network Segmentation) เช่น ขาดการแยกเครือข่ายสำคัญออกจากเครือข่ายทั่วไป (VLAN)	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	2	**การใช้ระบบตรวจจับและป้องกันภัยคุกคาม (IDS/IPS)**	ติดตั้งระบบ IDS/IPS เพื่อตรวจจับและป้องกันกิจกรรมที่เป็นอันตรายในเครือข่าย	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. ถูกการโจมตีแบบ Phishing ผ่านเครือข่าย เช่น การส่งลิงก์ฟิชชิงหรือไฟล์ที่เป็นอันตรายผ่านอีเมล์หรือเครือข่าย	3. ขาดระบบตรวจจับและป้องกันภัยคุกคาม เช่น ไม่มีการติดตั้ง IDS/IPS (Intrusion Detection/Prevention Systems)	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	4	8	CSMR	6.8	Mitigate Risk	3	**การควบคุมการเข้าถึง (Access Control)**	ใช้ NAC (Network Access Control) เพื่อตรวจสอบและอนุญาตการเข้าถึงเครือข่าย	ภายใน 30 ก.ย. 67	34%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. มีการใช้ช่องโหว่ของโปรโตคอลเครือข่าย เช่น การโจมตีผ่านโปรโตคอล อาทิ DNS Spoofing หรือ ARP Poisoning	4. การใช้โปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet ที่ไม่มีการเข้ารหัส	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	4	**การอัปเดตอุปกรณ์เครือข่ายและระบบปฏิบัติการ**	อัปเดตเราเตอร์ สวิตช์ และไฟร์วอลล์เป็นประจำเพื่อลดความเสี่ยงจากช่องโหว่	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรืออุปกรณ์ที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายขององค์กร	5. ไม่มีการควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการตรวจสอบอุปกรณ์หรือผู้ใช้ที่เชื่อมต่อกับเครือข่ายขององค์กร	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	5	10	CSMR		Mitigate Risk	5	**การป้องกันการโจมตี DDoS**	ใช้บริการ DDoS Mitigation เช่น Cloudflare หรือ AWS Shield เพื่อป้องกันการโจมตี DDoS	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
14	**ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)**	1. มีการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรือผู้ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่สำคัญได้ อาทิ ศูนย์ข้อมูลหรือเซิร์ฟเวอร์รูมหรือดาต้าเซ็นต์เตอร์	1. การขาดระบบควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการกำหนดสิทธิ์หรือการยืนยันตัวตนก่อนเข้าถึงพื้นที่สำคัญ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	1	**การติดตั้งระบบควบคุมการเข้าถึงทางกายภาพ (Access Control)**	ใช้ระบบ Keycard, Biometric Authentication หรือ PIN เพื่อควบคุมการเข้าถึงพื้นที่สำคัญ	ภายใน 30 ก.ย. 67	100%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		2. มีการขโมยหรือสูญหายของอุปกรณ์ เช่น อุปกรณ์สำคัญต่างๆ อาทิ เซิร์ฟเวอร์ ฮาร์ดไดรฟ์ แล็ปท็อป ถูกขโมยหรือสูญหาย	2. ไม่มีการเฝ้าระวังด้วยกล้องวงจรปิด (CCTV) เช่น ขาดระบบเฝ้าระวังหรือการตรวจสอบเหตุการณ์ที่เกิดขึ้นในพื้นที่สำคัญ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	1	3	3	CSMR		Mitigate Risk	2	**การป้องกันภัยธรรมชาติ**	ออกแบบสถานที่ให้มีการป้องกันน้ำท่วม เช่น การยกพื้นศูนย์ข้อมูลหรือใช้ระบบกันน้ำ	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการก่อวินาศกรรม (Sabotage) เช่น การทำลายทรัพย์สินหรือระบบโดยบุคคลภายในหรือบุคคลภายนอก	3. ไม่มีระบบป้องกันการก่อวินาศกรรม เช่น ขาดการออกแบบหรือมาตรการป้องกันการก่อวินาศกรรม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	x	-	1	3	3	CSMR	4.2	Mitigate Risk	3	**การกำหนดนโยบายการเข้าถึงพื้นที่สำคัญ**	จัดทำรายการผู้มีสิทธิ์เข้าถึงพื้นที่สำคัญและตรวจสอบสิทธิ์เป็นระยะ	ภายใน 30 ก.ย. 67	65%	-	-	x	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
		4. เกิดภัยธรรมชาติ (Natural Disasters) เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหวที่ส่งผลกระทบต่ออุปกรณ์และข้อมูลสำคัญ	3. ไม่มีระบบป้องกันภัยธรรมชาติ เช่น ขาดการออกแบบหรือมาตรการป้องกันภัยธรรมชาติ อาทิ การป้องกันน้ำท่วม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	-	-	x	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	4	**การฝึกอบรมพนักงานด้านความปลอดภัย**	ฝึกอบรมพนักงานให้เข้าใจวิธีป้องกันและรับมือกับภัยคุกคามทางกายภาพ	ภายใน 30 ก.ย. 67	100%	-	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		5. มีการขโมยข้อมูลผ่านการเข้าถึงทางกายภาพ เช่น การเชื่อมต่อกับพอร์ต USB หรือเครือข่ายโดยตรงในองค์กร เพื่อขโมยข้อมูล	5. การเก็บรักษาอุปกรณ์สำคัญในที่ไม่ปลอดภัย เช่น อุปกรณ์สำคัญถูกเก็บไว้ในพื้นที่ที่เข้าถึงได้ง่าย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	2	3	6	CSMR		Mitigate Risk	5	**การตรวจสอบความปลอดภัยทางกายภาพเป็นระยะ**	ตรวจสอบระบบล็อก กล้องวงจรปิด และระบบป้องกันภัยธรรมชาติอย่างสม่ำเสมอ	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
15	**ความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบและข้อบังคับ (Regulatory and Compliance Risks)**	1. บทลงโทษทางกฎหมาย เช่น การถูกปรับหรือฟ้องร้องจากการไม่ปฏิบัติตามกฎหมาย เช่น พรบ คอมพิวเตอร์, พรบ ข้อมูลส่วนบุคคล หรือ พรบ ไซเบอร์	1. การขาดความรู้เกี่ยวกับกฎหมายและข้อบังคับที่เกี่ยวข้อง เช่น พนักงานและผู้บริหารไม่ทราบถึงข้อกำหนดและกฎหมายที่ต้องปฏิบัติตาม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	2	3	6	CSMR		Mitigate Risk	1	**การติดตามและวิเคราะห์กฎหมายและข้อบังคับ**	แต่งตั้งทีม Compliance หรือใช้ที่ปรึกษาเพื่อให้คำแนะนำเกี่ยวกับข้อกำหนดที่เกี่ยวข้อง	ภายใน 30 ก.ย. 67	100%	x	-	-	x	x	x	x	x	-	1	5	5	เฝ้าติดตามเป็นระยะ
	(Non-Compliance Activity)	2. การเสียชื่อเสียง เช่น ความน่าเชื่อถือขององค์กรลดลงเนื่องจากการละเมิดกฎระเบียบข้อบังคับด้านความมั่นคงปลอดภัยของข้อมูล	2. ไม่มีระบบติดตามและตรวจสอบการปฏิบัติตามข้อกำหนด เช่น ขาดเครื่องมือหรือกระบวนการในการประเมินสถานะความสอดคล้อง	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	1	3	3	CSMR		Mitigate Risk	2	**การฝึกอบรมพนักงาน (Employee Training)**	อบรมพนักงานเกี่ยวกับข้อกำหนดและความสำคัญของการปฏิบัติตามกฎหมาย	ภายใน 30 ก.ย. 67	33%	x	-	-	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ
		3. มีการหยุดชะงักของธุรกิจ เช่น การปิดระบบหรือบริการชั่วคราวเนื่องจากการตรวจสอบจากหน่วยงานกำกับดูแล	3. ขาดนโยบายและกระบวนการที่ชัดเจน เช่น ไม่มีแนวทางปฏิบัติที่ช่วยให้พนักงานรวมถึงหน่วยงานกำกับดูแลปฏิบัติตามข้อบังคับได้ง่าย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	1	3	3	CSMR	4.2	Mitigate Risk	3	**การตรวจสอบและประเมินสถานะการปฏิบัติตามข้อกำหนด**	ดำเนินการ Internal Audit เป็นระยะเพื่อประเมินความสอดคล้องกับข้อกำหนด	ภายใน 30 ก.ย. 67	100%	x	-	x	x	x	x	x	-	-	1	5	5	เฝ้าติดตามเป็นระยะ

		4.มีความเสียหายทางการเงิน เช่น การสูญเสียลูกค้าหรือโอกาสทางธุรกิจเนื่องจากการละเมิดข้อบังคับ	4. การจัดการเอกสารและข้อมูลที่ไม่เหมาะสม เช่น การจัดเก็บเอกสารหรือการตีความหมายของข้อมูลไม่ตรงตามข้อกำหนดของกฎหมาย	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	**1**	**3**	**3**	CSMR		Mitigate Risk	**4**	**การจัดทำแผนและกระบวนการจัดการเหตุการณ์**	สร้าง Incident Response Plan ที่รวมข้อกำหนดด้านการรายงานเหตุการณ์ให้กับหน่วยงานกำกับดูแล	ภายใน 30 ก.ย. 67	**100%**		x	-	x	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
		5. มีความเสี่ยงต่อความปลอดภัยของข้อมูล เช่น การจัดการข้อมูลไม่ตรงตามกฎหมาย อาจนำไปสู่การละเมิดข้อมูล	5. การไม่ทำการประเมินความเสี่ยงด้านข้อกำหนด เช่น ไม่ได้ตรวจสอบว่ากระบวนการใดอาจละเมิดข้อบังคับ	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	**2**	**3**	**6**	CSMR		Mitigate Risk	**5**	**การทำแผนการปฏิบัติตามข้อกำหนดอย่างต่อเนื่อง (Compliance Roadmap)**	จัดทำแผนการปฏิบัติตามข้อบังคับในระยะยาว พร้อมตรวจสอบความก้าวหน้า	ภายใน 30 ก.ย. 67	**55%**		x	-	-	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
16	**การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)**	1. มีการส่งข้อมูลโดยไม่ได้ตั้งใจ เช่น การส่งข้อมูลสำคัญไปยังผู้รับผิดคน หรือแพลตฟอร์มที่ไม่ปลอดภัย	1. การขาดการควบคุมการเข้าถึงข้อมูล เช่น ไม่มีการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	**2**	**3**	**6**	CSMR		Mitigate Risk	**1**	**การเข้ารหัสข้อมูล (Data Encryption)**	เข้ารหัสข้อมูลสำคัญทั้งในขณะจัดเก็บ (At Rest) และระหว่างส่งผ่านเครือข่าย (In Transit)	ภายใน 30 ก.ย. 67	**100%**		x	-	-	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
		2. มีการขโมยข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจหรือบุคคลภายนอกขโมยข้อมูลเพื่อผลประโยชน์ส่วนตัว	2. การไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บหรือรับส่งกัน ไม่มีการเข้ารหัส	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	x	-	**2**	**3**	**6**	CSMR		Mitigate Risk	**2**	**การใช้ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP)**	ใช้ DLP เพื่อตรวจสอบและบล็อกการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	ภายใน 30 ก.ย. 67	**100%**		x	-	-	x	x	x	x	x	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
		3. มีการละเมิดข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัย เช่น การรั่วไหลของข้อมูลที่ส่งผ่าน Wi-Fi หรือเครือข่ายที่ไม่มีการเข้ารหัส	3. ขาดนโยบายและกระบวนการจัดการข้อมูล เช่น ไม่มีการกำหนดนโยบายในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคล	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	**1**	**3**	**3**	CSMR	**4.2**	Mitigate Risk	**3**	**การสำรองข้อมูล (Backup)**	ตั้งค่าการสำรองข้อมูลอัตโนมัติในสถานที่ที่ปลอดภัยและแยกจากระบบหลัก	ภายใน 30 ก.ย. 67	**56%**		x	-	-	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
		4. ถูกการโจมตีแบบ Phishing เช่น ผู้โจมตีใช้ฟิชชิงเพื่อเข้าถึงข้อมูลสำคัญผ่านอีเมล์หรือข้อความ	4. การขาดระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention - DLP) เช่น ไม่มีการใช้ระบบเพื่อตรวจจับและป้องกันการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	-	x	x	x	x	-	-	**1**	**3**	**3**	CSMR		Mitigate Risk	**4**	**การควบคุมการใช้งานอุปกรณ์พกพา (Mobile Device Management - MDM)**	ใช้ MDM เพื่อติดตามและจัดการอุปกรณ์ที่เชื่อมต่อกับข้อมูลสำคัญ	ภายใน 30 ก.ย. 67	**100%**		x	-	-	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ
		5. มีการติดมัลแวร์หรือแรนซัมแวร์ เช่น มีการใช้มัลแวร์เพื่อดึงข้อมูลหรือขัดขวางการเข้าถึงข้อมูล	5. อุปกรณ์และบัญชีทรัพย์สินที่ไม่ได้รับการควบคุม เช่น อุปกรณ์พกพาหรือบัญชีผู้ใช้งานที่ไม่ได้ใช้งานยังสามารถเข้าถึงข้อมูลได้	ยังไม่มีมาตรการควบคุมที่เข้มแข็งและเพียงพอ	x	-	x	x	x	x	x	-	-	**1**	**3**	**3**	CSMR		Mitigate Risk	**5**	**การตั้งค่าความปลอดภัยของเครือข่าย**	ใช้ Virtual Private Network (VPN) สำหรับการเข้าถึงข้อมูลผ่านเครือข่ายสาธารณะ	ภายใน 30 ก.ย. 67	**66%**		x	-	x	x	x	x	x	-	-	**1**	**5**	**5**	เฝ้าติดตามเป็นระยะ