

การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST

นายวุฒิพงศ์ ศรีภูมั่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2569

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST

นายวุฒิพงศ์ ศรีภูมั่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร

สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2569
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองโครงร่างวิทยานิพนธ์

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST

โดย นายวุฒิพงศ์ ศรีภูมั่น

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

.....

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบวิทยานิพนธ์

.....

ประธาน

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

.....

อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

.....

กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

มหาวิทยาลัยเทคโนโลยี
พระจอมเกล้าพระนครเหนือ

ชื่อ : นายวุฒิพงศ์ ศรีภูมั่น

ชื่อวิทยานิพนธ์ : การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST

สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์

ปีการศึกษา : 2569

บทคัดย่อ

การค้นคว้าอิสระนี้มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ ให้สอดคล้องกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework 2.0 โดยมุ่งเน้นการประเมินความเสี่ยงในด้านการควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การบริหารจัดการเหตุการณ์ที่ไม่คาดคิด การกู้คืนระบบ และการติดตามตรวจสอบการทำงานของระบบ การศึกษานี้ใช้วิธีการวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อเปรียบเทียบการดำเนินงานปัจจุบันของศูนย์ข้อมูลกับแนวทางตามกรอบ NIST พร้อมทั้งกำหนดตัวชี้วัดผลการประเมิน (KPI) เพื่อวัดระดับความสอดคล้องและจัดลำดับความสำคัญของความเสี่ยง ผลการศึกษาคาดว่าจะช่วยให้หน่วยงานสามารถระบุจุดอ่อน ประเมินระดับความพร้อม และจัดทำข้อเสนอแนะในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบและเหมาะสมกับบริบทของหน่วยงานภาครัฐ

(มีจำนวนทั้งสิ้น 73 หน้า)

คำสำคัญ : การประเมินความเสี่ยง, ศูนย์ข้อมูลภาครัฐ, ความมั่นคงปลอดภัยไซเบอร์, NIST Cybersecurity Framework 2.0, การวิเคราะห์ช่องว่าง, ตัวชี้วัดผลการประเมิน

_____ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Name : Mr. Wuttipong Sripoomun

Thesis Title : Improving government network infrastructure to align with NIST Cybersecurity frameworks.

Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok

Thesis Advisor : Assistant Professor Dr. Nawaporn Wisitpongphan

Academic Year : 2026

ABSTRACT

This independent study aims to analyze and assess risks related to the infrastructure of a government agency's data center in alignment with the NIST Cybersecurity Framework 2.0. The study focuses on key risk areas, including access control, physical security, incident management, system recovery and system monitoring and auditing.

The study applies Gap Analysis to compare the current operations of the data center with the guidelines of the NIST Cybersecurity Framework 2.0. In addition, Key Performance Indicators (KPIs) are defined to measure the level of alignment and support the prioritization of risks in a systematic manner.

The expected outcome of this study is to enable the organization to identify weaknesses, assess its cybersecurity readiness, and develop recommendations for reducing cybersecurity risks in a structured and appropriate manner within the context of a government agency.

(Total 73 Pages)

Keywords: Risk Assessment, Government Data Center, Cybersecurity, NIST Cybersecurity Framework 2.0, Gap Analysis, Key Performance Indicators

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาและความอนุเคราะห์จากบุคคลหลายฝ่าย ผู้ศึกษาขอกราบขอบพระคุณอาจารย์ที่ปรึกษาการค้นคว้าอิสระเป็นอย่างสูง ที่ได้กรุณาให้คำแนะนำ ข้อคิดเห็น และข้อเสนอแนะที่เป็นประโยชน์ ตลอดจนช่วยตรวจสอบและปรับปรุงเนื้อหาของการศึกษาครั้งนี้ให้มีความถูกต้อง สมบูรณ์ และเป็นไปตามหลักวิชาการ

ขอขอบพระคุณผู้บริหารและเจ้าหน้าที่ของหน่วยงานภาครัฐที่เกี่ยวข้อง ที่ได้ให้ความอนุเคราะห์ข้อมูล คำแนะนำ และความร่วมมือในการศึกษาเกี่ยวกับโครงสร้างพื้นฐานของศูนย์ข้อมูล การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และแนวทางการดำเนินงานที่เกี่ยวข้องกับกรอบการทำงานของ NIST Cybersecurity Framework 2.0 ซึ่งเป็นประโยชน์อย่างยิ่งต่อการวิเคราะห์และจัดทำการค้นคว้าอิสระฉบับนี้

ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ แนวคิด และประสบการณ์อันมีคุณค่า ตลอดระยะเวลาการศึกษา รวมถึงเจ้าหน้าที่ประจำหลักสูตรที่ให้ความช่วยเหลือและอำนวยความสะดวกในด้านต่าง ๆ เป็นอย่างดี

ท้ายที่สุดนี้ ผู้ศึกษาขอกราบขอบพระคุณครอบครัว เพื่อนร่วมงาน และผู้มีส่วนเกี่ยวข้องทุกท่านที่ให้กำลังใจ ความช่วยเหลือ และการสนับสนุนมาโดยตลอด จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี ผู้ศึกษาหวังเป็นอย่างยิ่งว่าการค้นคว้าอิสระฉบับนี้จะเป็นประโยชน์ต่อหน่วยงานภาครัฐและผู้ที่สนใจด้านการประเมินความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ต่อไป

ขอขอบคุณทุกท่านอีกครั้งมา ณ โอกาสนี้

วุฒิพงศ์ ศรีภูมั่น

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง (ถ้ามี) ..... ฌ

สารบัญรูปภาพ (ถ้ามี) ..... ญ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์ของการวิจัย 2

1.3 ขอบเขตของการวิจัย 2

1.4 ประโยชน์ที่คาดว่าจะได้รับ 3

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง 5

2.1 มาตรฐานและกรอบการทำงานที่เกี่ยวข้อง 5

2.2 การประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูล 11

2.3 งานวิจัยที่เกี่ยวข้อง 17

บทที่ 3 วิธีการดำเนินการวิจัย 21

3.1 ขั้นตอนการดำเนินการวิจัย 21

3.2 เครื่องมือที่ใช้ในการวิจัย 22

3.3 การเก็บรวบรวมข้อมูล 24

3.4 การวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 26
3.5 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 28
3.6 เกณฑ์การประเมินและการจัดระดับความเสี่ยง 30
3.7 การกำหนดตัวชี้วัดผลการประเมิน 33
บทที่ 4 ผลการดำเนินการวิจัย 36
4.1 ผลการศึกษาข้อมูลพื้นฐานและกระบวนการประเมินความเสี่ยงของหน่วยงาน 36
4.2 ผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้ 38
4.3 ผลการจัดระดับสถานการณ์ความเสี่ยง 39
4.4 ผลการจัดกลุ่มประเด็นความเสี่ยง 43
4.5 ผลการวิเคราะห์ความเสี่ยงตามกรอบ NIST Cybersecurity Framework 2.0 45
4.6 แนวทางการจัดการความเสี่ยง 46
4.7 สรุปผลการวิเคราะห์ความเสี่ยง 48
บทที่ 5 สรุป อภิปรายผล และข้อเสนอแนะ 49
5.1 อภิปรายผล 49
5.2 สรุปผลการวิจัย 50
5.3 ข้อเสนอแนะ 52
บรรณานุกรม 55
ภาคผนวก 58
ประวัติผู้เขียน 62

สารบัญตาราง

หน้า

ตารางที่ 3-1 เครื่องมือที่ใช้ในการวิจัย 24
ตารางที่ 3-2 แหล่งข้อมูลที่ใช้ในการวิจัย..... 26
ตารางที่ 3-3 แนวทางการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0..... 27
ตารางที่ 3-4 ขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 29
ตารางที่ 3-5 เกณฑ์การประเมินโอกาสเกิดเหตุการณ์(Likelihood)..... 30
ตารางที่ 3-6 เกณฑ์การประเมินผลกระทบ (Impact)..... 31
ตารางที่ 3-7 เมทริกซ์จัดระดับความเสี่ยง..... 31
ตารางที่ 3-8 เกณฑ์การยอมรับความเสี่ยง..... 32
ตารางที่ 3-9 ตัวชี้วัดผลการประเมิน..... 34
ตารางที่ 4-1 กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน..... 37
ตารางที่ 4-2 สรุปจำนวนรายการความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้ 39
ตารางที่ 4-3 ผลการประเมินความเสี่ยง ณ ท่าอากาศยานอุบลราชธานี..... 40
ตารางที่ 4-4 ผลการประเมินความเสี่ยง ณ ท่าอากาศยานอุดรธานี..... 41
ตารางที่ 4-5 การเปรียบเทียบภาพรวมผลการประเมินความเสี่ยงของพื้นที่เดิมและพื้นที่ที่ศึกษาในครั้งนี้ .. 42
ตารางที่ 4-6 การจัดกลุ่มประเด็นความเสี่ยงที่พบจากการประเมิน 44
ตารางที่ 4-7 การเชื่อมโยงสถานการณ์ความเสี่ยงกับ NIST Cybersecurity Framework 2.0..... 45
ตารางที่ 4-8 แนวทางการจัดการความเสี่ยงตามสถานการณ์ความเสี่ยง..... 46
ตารางที่ ก-1 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานอุบลราชธานี.....58
ตารางที่ ก-2 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานอุดรธานี.....59
ตารางที่ ก-3 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานนครพนม.....60
ตารางที่ ก-4 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานกระบี่.....61

สารบัญรูปภาพ

หน้า

ภาพที่ 2-1 กรอบการทำงาน NIST Cybersecurity Framework 2.0 6
ภาพที่ 2-2 ระดับการนำ NIST Cybersecurity Framework ไปปฏิบัติ 8
ภาพที่ 2-3 ความเชื่อมโยงระหว่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับ NIST Cybersecurity Framework 2.0 11
ภาพที่ 2-4 องค์ประกอบศูนย์ข้อมูลภาครัฐ 12
ภาพที่ 2-5 กระบวนการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 16
ภาพที่ 3-1 ขั้นตอนการดำเนินงานวิจัย 21
ภาพที่ 4-1 กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน 37

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

NIST Cybersecurity Framework 2.0 เป็นกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ถูกพัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา เพื่อช่วยให้หน่วยงานและองค์กรต่าง ๆ สามารถบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ โดยกรอบการทำงานดังกล่าวครอบคลุมหน้าที่หลัก 6 ด้าน ได้แก่ การกำกับดูแล (Govern), การระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond) และการกู้คืน (Recover) ทำให้องค์กรสามารถวางแผนและป้องกันความเสี่ยงใน Data Center ได้อย่างครอบคลุม

ในปัจจุบัน หน่วยงานภาครัฐที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) จำเป็นต้องดำเนินงานให้สอดคล้องกับนโยบาย กฎหมาย และแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นต่อระบบสารสนเทศ ข้อมูลสำคัญ และการให้บริการประชาชน ศูนย์ข้อมูลจึงถือเป็นองค์ประกอบสำคัญของหน่วยงานภาครัฐ เนื่องจากเป็นโครงสร้างพื้นฐานที่ใช้จัดเก็บ ประมวลผล และให้บริการข้อมูลที่เกี่ยวข้องกับภารกิจของหน่วยงาน

ศูนย์ข้อมูล เป็นโครงสร้างพื้นฐานที่ใช้จัดเก็บและประมวลผลข้อมูลขององค์กรต่างๆ จึงมีความสำคัญเป็นอย่างมาก ดังนั้น การปรับปรุงโครงสร้างพื้นฐานของศูนย์ข้อมูล ของหน่วยงานรัฐจะต้องมีการปฏิบัติตามกรอบมาตรฐานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Framework) หรือ นโยบายของหน่วยงานที่กำกับดูแล เพื่อป้องกันการละเมิดหรือการถูกโจมตีจากภายนอก และให้คงไว้ซึ่ง การรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้งานของข้อมูล (Availability) รวมถึงช่วยเสริมสร้างความมั่นใจในด้านการป้องกันภัยคุกคาม ตลอดจนเพิ่มความน่าเชื่อถือให้กับประชาชน

จากสถานการณ์ข้างต้น การศึกษานี้จึงนำกรอบการทำงาน NIST Cybersecurity Framework 2.0 มาประยุกต์ใช้ในการวิเคราะห์และประเมินความเสี่ยงของศูนย์ข้อมูลของหน่วยงาน เพื่อให้สามารถระบุจุดอ่อน ช่องว่าง และประเด็นที่ควรได้รับการปรับปรุง รวมทั้งจัดทำข้อเสนอแนะในการลดความเสี่ยงให้สอดคล้องกับแนวทางด้านความมั่นคงปลอดภัยไซเบอร์และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อวิเคราะห์กระบวนการและปรับปรุงโครงสร้างพื้นฐานของศูนย์ข้อมูล ให้มีความสอดคล้องกับ NIST Cybersecurity Framework 2.0

1.2.2 เพื่อศึกษากรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ

1.2.3 เพื่อวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยครอบคลุมด้านการควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การติดตามตรวจสอบระบบ และการบริหารจัดการเหตุการณ์ที่ไม่คาดคิด

1.2.4 เพื่อวิเคราะห์ช่องว่างระหว่างการดำเนินงานปัจจุบันของศูนย์ข้อมูลกับแนวทางตาม NIST Cybersecurity Framework 2.0 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.2.5 เพื่อจัดทำข้อเสนอแนะในการลดความเสี่ยงและยกระดับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลให้เหมาะสมกับหน่วยงานภาครัฐ

1.3 ขอบเขตของการวิจัย

1.3.1 ศึกษาและวิเคราะห์ กรอบการทำงานด้านการบริหารจัดการความเสี่ยงทางไซเบอร์ 2.0 (NIST Framework 2.0)

1.3.2 วิเคราะห์โครงสร้างพื้นฐานศูนย์ข้อมูล ของหน่วยงานเพื่อตรวจสอบว่าเป็นไปตามกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ 2.0 โดยจะต้องมีส่วนที่ครอบคลุม ดังนี้

1.3.2.1 การประเมินความเสี่ยง (Risk Assessment and Management)

1.3.2.2 การควบคุมการเข้าถึง (Access Control)

1.3.2.3 การรักษาความปลอดภัยทางกายภาพ(Physical Security)

1.3.2.4 การบริหารจัดการกับเหตุการณ์ที่ไม่คาดคิดและการกู้คืนระบบ (Incident Management and Recovery)

1.3.2.5 การติดตามและตรวจสอบการทำงานของระบบ (Monitoring and Auditing)

1.3.2.6 การฝึกอบรมและสร้างความตระหนักต่อภัยคุกคามทางไซเบอร์ (Security Awareness Training)

1.3.2.7 การปฏิบัติตามกฎหมาย พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อบังคับของหน่วยงานที่มีหน้าที่กำกับดูแล

1.3.3 วิเคราะห์และประเมินความเสี่ยงที่เกี่ยวข้องกับการจัดการข้อมูลในศูนย์ข้อมูล

1.3.4 ออกแบบและเสนอแนวทางการปรับปรุงโครงสร้างพื้นฐานเพื่อให้เป็นไปตามกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ 2.0 (NIST Framework 2.0)

1.3.5 ตรวจสอบประสิทธิภาพของการนำกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Framework 2.0) โดยผู้ตรวจสอบภายนอก (External Audit) หรือ ผู้ตรวจสอบภายใน (Internal Audit) มาปรับใช้ในศูนย์ข้อมูลของหน่วยงาน และ ประเมินผลโดยการนำ KPI มาเป็นตัวใช้ในการชี้วัด

1.3.6 การศึกษานี้ใช้ข้อมูลผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่นำร่องจำนวน 2 แห่ง ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี ซึ่งเป็นพื้นที่ภายใต้การกำกับดูแลของกรมท่าอากาศยาน โดยนำผลการประเมินดังกล่าวมาใช้วิเคราะห์เปรียบเทียบ และจัดทำข้อเสนอแนะเพื่อยกระดับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานศูนย์ข้อมูลและระบบสนับสนุนที่เกี่ยวข้อง

ทั้งนี้ ผู้วิจัยได้นำผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้มาเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ ซึ่งเป็นพื้นที่ที่เคยมีการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์มาก่อน เพื่อวิเคราะห์ความเหมือน ความแตกต่าง และแนวทางการบริหารจัดการความเสี่ยงในระดับหน่วยงาน รายละเอียดผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้และพื้นที่เปรียบเทียบเดิม แสดงไว้ในภาคผนวก

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 หน่วยงานสามารถทราบถึงระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานศูนย์ข้อมูล โดยเฉพาะในด้านการควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การติดตามตรวจสอบระบบ และการบริหารจัดการเหตุการณ์ที่ไม่คาดคิด

1.4.2 หน่วยงานสามารถระบุจุดอ่อน ช่องว่าง และข้อบกพร่องของการดำเนินงานปัจจุบัน เมื่อเปรียบเทียบกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework 2.0

1.4.3 หน่วยงานได้รับแนวทางในการลดความเสี่ยงและปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลให้มีความเหมาะสมกับบริบทของหน่วยงานภาครัฐ

1.4.4 ผลการศึกษาสามารถใช้เป็นข้อมูลประกอบการวางแผน การกำหนดนโยบาย และการจัดลำดับความสำคัญของการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลได้อย่างเป็นระบบ

1.4.5 หน่วยงานสามารถนำผลการประเมินไปใช้เป็นแนวทางในการเตรียมความพร้อมให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.4.6 ช่วยสนับสนุนให้ศูนย์ข้อมูลของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยมากขึ้น ลดโอกาสการเกิดเหตุการณ์ด้านไซเบอร์ และเสริมสร้างความเชื่อมั่นต่อการให้บริการของหน่วยงานภาครัฐแก่ประชาชนและผู้มีส่วนเกี่ยวข้อง

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การค้นคว้าอิสระเรื่อง การปรับปรุงโครงสร้าง พื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยอ้างอิงกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework 2.0 รวมถึงแนวคิดด้านการบริหารจัดการความเสี่ยง การวิเคราะห์ช่องว่าง การกำหนดมาตรการควบคุม และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

เนื่องจากศูนย์ข้อมูลเป็นโครงสร้างพื้นฐานสำคัญที่ใช้ในการจัดเก็บ ประมวลผล และให้บริการข้อมูลของหน่วยงานภาครัฐ หากขาดมาตรการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสม อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูล การเข้าถึงโดยไม่ได้รับอนุญาต การหยุดชะงักของระบบ และส่งผลกระทบต่อความต่อเนื่องในการให้บริการประชาชน ดังนั้น ผู้วิจัยจึงได้ศึกษาเอกสารมาตรฐาน แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง เพื่อนำมาใช้เป็นกรอบในการดำเนินการวิจัยดังต่อไปนี้

2.1 มาตรฐานและกรอบการทำงานที่เกี่ยวข้อง

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลจำเป็นต้องอาศัยมาตรฐานและกรอบการทำงานที่ได้รับการยอมรับ เพื่อให้การวิเคราะห์มีความเป็นระบบ สามารถตรวจสอบได้ และสามารถนำผลการประเมินไปใช้ในการกำหนดแนวทางลดความเสี่ยงได้อย่างเหมาะสม ในการศึกษานี้ ผู้วิจัยได้พิจารณามาตรฐานและกรอบการทำงานที่เกี่ยวข้อง ได้แก่ NIST Cybersecurity Framework 2.0, NIST SP 800-30, NIST SP 800-53, CIS Controls และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.1.1 NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework หรือ NIST CSF เป็นกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาโดย National Institute of Standards and Technology ของสหรัฐอเมริกา โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างเป็นระบบ กรอบการทำงานดังกล่าวสามารถนำไปประยุกต์ใช้ได้กับองค์กรหลากหลาย

ประเภท ทั้งภาครัฐ ภาคเอกชน และหน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ (Pascoe et al., 2024)

NIST Cybersecurity Framework 2.0 มีจุดเด่นสำคัญ คือ การเพิ่มหน้าที่ด้านการกำกับดูแล หรือ Govern เข้ามาเป็นหนึ่งในองค์ประกอบหลัก เพื่อเน้นให้การบริหารจัดการความเสี่ยงด้านไซเบอร์ไม่ได้เป็นเพียงหน้าที่ของฝ่ายเทคนิคเท่านั้น แต่ต้องเชื่อมโยงกับนโยบาย บทบาท ความรับผิดชอบ การตัดสินใจ และเป้าหมายขององค์กรโดยรวม ส่งผลให้ NIST CSF 2.0 ประกอบด้วยหน้าที่หลัก 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover ดังที่แสดงในภาพที่ 2-1



ภาพที่ 2-1 กรอบการทำงาน NIST Cybersecurity Framework 2.0

2.1.1.1 ด้าน Govern เป็นการกำหนดนโยบาย บทบาท หน้าที่ ความรับผิดชอบ และแนวทางการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร เพื่อให้การดำเนินงานด้านความปลอดภัยมีทิศทางชัดเจน สอดคล้องกับเป้าหมายของหน่วยงาน และสามารถบริหารจัดการความเสี่ยงได้อย่างเป็นระบบ

2.1.1.2 ด้าน Identify เป็นการระบุทรัพย์สิน ระบบ ข้อมูล บุคลากร กระบวนการ และความเสี่ยงที่เกี่ยวข้องกับองค์กร เพื่อให้องค์กรเข้าใจบริบทของตนเอง ทราบว่าสินทรัพย์ใดมีความสำคัญต่อการดำเนินงาน และสามารถจัดลำดับความสำคัญของการป้องกันได้อย่างเหมาะสม

2.1.1.3 ด้าน Protect เป็นการกำหนดมาตรการป้องกันเพื่อลดโอกาสการเกิดเหตุการณ์ด้านไซเบอร์ เช่น การควบคุมการเข้าถึง การฝึกอบรมบุคลากร การป้องกันข้อมูล การบำรุงรักษา

ระบบ และการใช้เทคโนโลยีด้านความมั่นคงปลอดภัย เพื่อจำกัดผลกระทบที่อาจเกิดขึ้นกับระบบและข้อมูล

2.1.1.4 ด้าน Detect เป็นการตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่อาจเกิดขึ้นกับระบบ โดยอาศัยการเฝ้าระวัง การบันทึกเหตุการณ์ การตรวจสอบ Log และการวิเคราะห์พฤติกรรมที่ผิดปกติ เพื่อให้องค์กรสามารถรับรู้เหตุการณ์ได้อย่างทันท่วงที

2.1.1.5 ด้าน Respond เป็นการกำหนดกระบวนการตอบสนองต่อเหตุการณ์ด้านไซเบอร์ เช่น การแจ้งเหตุ การวิเคราะห์เหตุการณ์ การจำกัดผลกระทบ การสื่อสารกับผู้เกี่ยวข้อง และการดำเนินการแก้ไขปัญหา เพื่อควบคุมสถานการณ์ไม่ให้ขยายผลกระทบต่อระบบและการให้บริการ

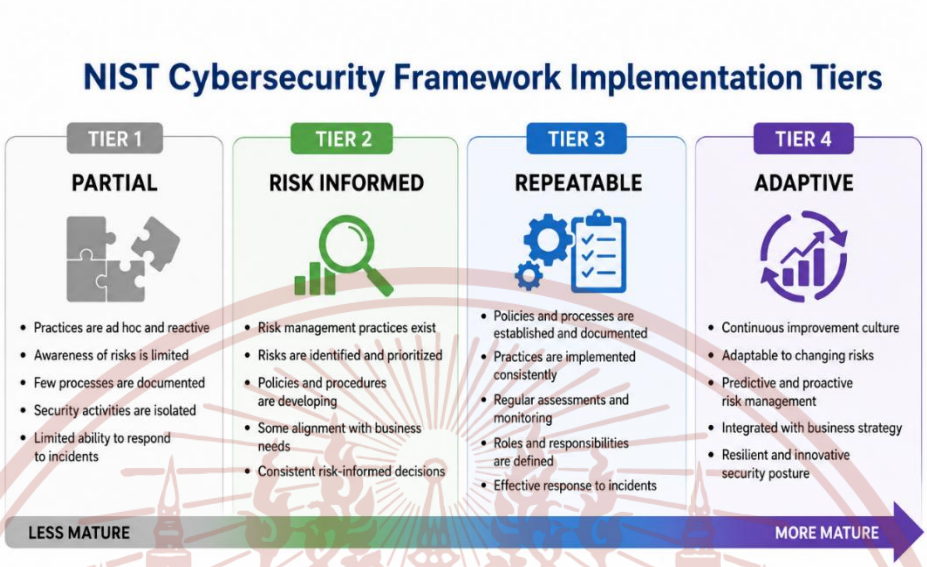
2.1.1.6 ด้าน Recover เป็นการกำหนดแนวทางในการกู้คืนระบบและบริการให้กลับมาใช้งานได้ตามปกติ รวมถึงการปรับปรุงกระบวนการหลังเกิดเหตุการณ์ เพื่อให้หน่วยงานสามารถดำเนินงานได้อย่างต่อเนื่องและลดผลกระทบจากเหตุการณ์ที่ไม่คาดคิด

จากองค์ประกอบดังกล่าว NIST Cybersecurity Framework 2.0 จึงมีความเหมาะสมต่อการนำมาใช้เป็นกรอบในการวิเคราะห์และประเมินความเสี่ยงของศูนย์ข้อมูลของหน่วยงานภาครัฐ เนื่องจากครอบคลุมตั้งแต่ระดับการกำกับดูแล การระบุความเสี่ยง การป้องกัน การตรวจจับ การตอบสนอง และการกู้คืนระบบ ซึ่งสอดคล้องกับวัตถุประสงค์ของงานวิจัยที่มุ่งประเมินความพร้อมและจัดทำข้อเสนอแนะในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.1.2 ระดับการนำ NIST Cybersecurity Framework ไปปฏิบัติ

นอกจากหน้าที่หลักของ NIST Cybersecurity Framework แล้ว กรอบการทำงานดังกล่าวยังมีแนวคิดเรื่อง ระดับการนำไปปฏิบัติ หรือ Implementation Tiers ซึ่งใช้สะท้อนระดับความพร้อมและลักษณะการบริหารจัดการความเสี่ยงด้านไซเบอร์ขององค์กร โดยสามารถแบ่งออกเป็น 4 ระดับ ได้แก่ Tier 1 Partial, Tier 2 Risk Informed, Tier 3 Repeatable และ Tier 4 Adaptive (Dedeke, 2017)

ทั้งนี้ ระดับดังกล่าวสามารถใช้แสดงให้เห็นถึงพัฒนาการขององค์กรในการบริหารจัดการความเสี่ยงด้านไซเบอร์ ตั้งแต่การดำเนินงานแบบเฉพาะหน้าไปจนถึงการปรับตัวเชิงรุกต่อภัยคุกคาม ดังแสดงในรูปที่ 2-2



ภาพที่ 2-2 ระดับการนำ NIST Cybersecurity Framework ไปปฏิบัติ

2.1.2.1 Tier 1 Partial หมายถึง องค์กรมีการบริหารจัดการความเสี่ยงแบบเฉพาะหน้า ยังไม่มีแนวทางที่เป็นระบบหรือมีการดำเนินงานที่สม่ำเสมอ การตัดสินใจด้านความมั่นคงปลอดภัยไซเบอร์มักขึ้นอยู่กับสถานการณ์เฉพาะหรือประสบการณ์ของผู้ปฏิบัติงาน

2.1.2.2 Tier 2 Risk Informed หมายถึง องค์กรเริ่มตระหนักถึงความเสี่ยงด้านไซเบอร์ และมีการนำความเสี่ยงมาประกอบการตัดสินใจบางส่วน แต่อาจยังไม่มีนโยบายหรือกระบวนการที่เป็นมาตรฐานทั่วทั้งองค์กร

2.1.2.3 Tier 3 Repeatable หมายถึง องค์กรมีนโยบาย กระบวนการ และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน สามารถดำเนินการซ้ำได้ และมีการสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบ

2.1.2.4 Tier 4 Adaptive หมายถึง องค์กรมีความสามารถในการปรับตัวต่อภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่อง มีการเรียนรู้จากเหตุการณ์ที่ผ่านมา และนำข้อมูลภัยคุกคามมาใช้ปรับปรุงมาตรการด้านความปลอดภัยอย่างต่อเนื่อง

ในการศึกษานี้ แนวคิด Implementation Tiers สามารถนำมาใช้ประกอบการพิจารณาระดับความพร้อมของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยเฉพาะการประเมินว่านโยบาย กระบวนการ และมาตรการควบคุมที่มีอยู่ในปัจจุบันอยู่ในระดับใด และควรได้รับการปรับปรุงไปสู่ระดับที่เหมาะสมอย่างไร

2.1.3 NIST SP 800-30 แนวทางการประเมินความเสี่ยงด้านสารสนเทศ

NIST SP 800-30 เป็นแนวทางที่เกี่ยวข้องกับการประเมินความเสี่ยงด้านระบบสารสนเทศ โดยมุ่งเน้นกระบวนการระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจส่งผลกระทบต่อระบบ ข้อมูล ทรัพย์สินสารสนเทศ และการดำเนินงานขององค์กร (Joint Task Force Transformation Initiative, 2012) แนวทางดังกล่าวสามารถนำมาใช้ในการประเมินความเสี่ยงของศูนย์ข้อมูลได้ เนื่องจากศูนย์ข้อมูลเป็นแหล่งรวมทรัพย์สินสารสนเทศที่มีความสำคัญต่อการให้บริการของหน่วยงาน

กระบวนการประเมินความเสี่ยงโดยทั่วไปประกอบด้วย การระบุทรัพย์สินสารสนเทศ การระบุภัยคุกคาม การระบุช่องโหว่ การวิเคราะห์โอกาสเกิดเหตุการณ์ การวิเคราะห์ผลกระทบ การจัดระดับความเสี่ยง และการกำหนดแนวทางในการจัดการความเสี่ยง ผลจากการประเมินดังกล่าวจะช่วยให้หน่วยงานทราบถึงระดับความเสี่ยงของระบบ และสามารถจัดลำดับความสำคัญของมาตรการควบคุมได้อย่างเหมาะสม

ในการศึกษานี้ แนวทางของ NIST SP 800-30 ถูกนำมาใช้เป็นแนวคิดประกอบการประเมินความเสี่ยงของศูนย์ข้อมูล โดยพิจารณาประเด็นสำคัญ ได้แก่ การควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การติดตามตรวจสอบระบบ การบริหารจัดการเหตุการณ์ และการกู้คืนระบบ เพื่อให้สามารถระบุความเสี่ยงและจัดทำข้อเสนอแนะในการลดความเสี่ยงได้อย่างเป็นระบบ

2.1.4 NIST SP 800-53 มาตรการควบคุมด้านความมั่นคงปลอดภัยและความเป็นส่วนตัว

NIST SP 800-53 เป็นเอกสารแนวทางที่กำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวสำหรับระบบสารสนเทศและองค์กร โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถเลือก นำไปใช้ ประเมิน และติดตามมาตรการควบคุมได้อย่างเหมาะสมกับระดับความเสี่ยงและบริบทขององค์กร (Joint Task Force, 2020)

มาตรการควบคุมที่เกี่ยวข้องกับการประเมินศูนย์ข้อมูล ได้แก่ การควบคุมการเข้าถึง การจัดการบัญชีผู้ใช้งาน การตรวจสอบและบันทึกเหตุการณ์ การรักษาความปลอดภัยทางกายภาพ การสำรองข้อมูล การตอบสนองต่อเหตุการณ์ การบริหารความต่อเนื่องของระบบ และการกู้คืนระบบหลังเกิดเหตุการณ์ มาตรการเหล่านี้สามารถนำมาใช้เป็นเกณฑ์ประกอบการวิเคราะห์ช่องว่างระหว่างสถานะปัจจุบันของศูนย์ข้อมูลกับแนวทางที่ควรดำเนินการตามกรอบ NIST นอกจากนี้ แนวคิดของ NIST SP 800-53 ยังช่วยให้องค์กรสามารถเลือกใช้มาตรการควบคุมตามความเหมาะสม ไม่จำเป็นต้องนำทุกมาตรการมาใช้ทั้งหมด แต่ควรพิจารณาตามระดับความเสี่ยง ความสำคัญ

ของระบบ ผลกระทบที่อาจเกิดขึ้น และทรัพยากรที่องค์กรมีอยู่ ดังนั้น NIST SP 800-53 จึงมีบทบาทสำคัญในการช่วยระบุว่าศูนย์ข้อมูลควรมีมาตรการควบคุมใดบ้าง และมาตรการที่มีอยู่ในปัจจุบันมีความเพียงพอหรือยังต้องได้รับการปรับปรุงเพิ่มเติม

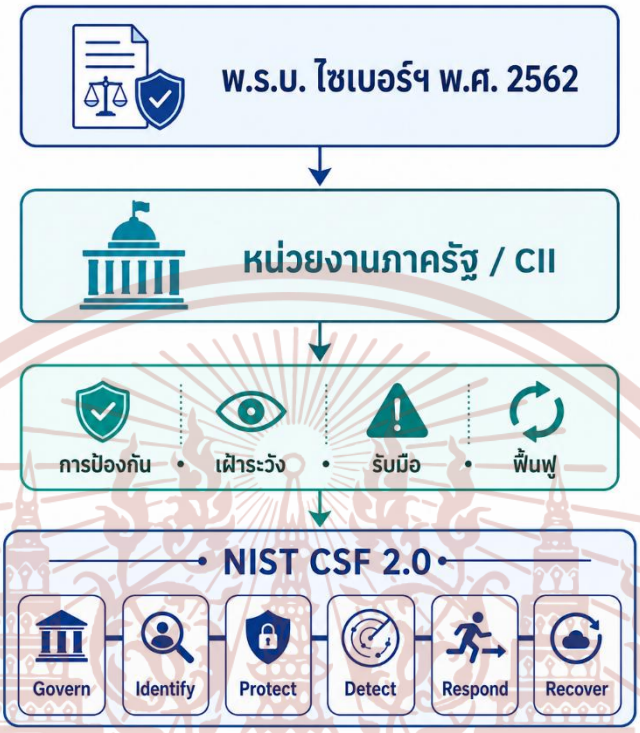
2.1.5 CIS Controls และมาตรการควบคุมเชิงเทคนิค

CIS Controls เป็นชุดแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่มุ่งเน้นมาตรการควบคุมเชิงปฏิบัติและเชิงเทคนิค ซึ่งสามารถช่วยให้องค์กรกำหนดมาตรการพื้นฐานในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเป็นรูปธรรม (Center for Internet Security, 2024) ตัวอย่างมาตรการที่เกี่ยวข้อง ได้แก่ การจัดทำบัญชีทรัพย์สิน การบริหารจัดการช่องโหว่ การควบคุมสิทธิ์ผู้ดูแลระบบ การบันทึกและตรวจสอบเหตุการณ์ การป้องกันมัลแวร์ การสำรองข้อมูล และการควบคุมการเข้าถึงเครือข่าย ซึ่งเมื่อนำ CIS Controls มาใช้ร่วมกับ NIST Cybersecurity Framework 2.0 จะช่วยเติมเต็มรายละเอียดเชิงเทคนิคให้กับกรอบ NIST โดยเฉพาะในกรณีที่หน่วยงานต้องการนำผลการประเมินความเสี่ยงไปจัดทำเป็นข้อเสนอแนะหรือมาตรการปฏิบัติที่ชัดเจนสำหรับผู้ดูแลระบบ เช่น การกำหนดแนวทางควบคุมสิทธิ์การเข้าถึง การตรวจสอบบันทึกเหตุการณ์ การสำรองข้อมูล และการจัดการช่องโหว่ของระบบอย่างเป็นระบบ

ในบริบทของงานวิจัยนี้ CIS Controls สามารถนำมาใช้เป็นแนวคิดประกอบการจัดทำข้อเสนอแนะในการลดความเสี่ยงของศูนย์ข้อมูล เช่น การปรับปรุงการจัดการบัญชีผู้ใช้งาน การตรวจสอบ Log การสำรองข้อมูล การควบคุมอุปกรณ์เครือข่าย และการเฝ้าระวังเหตุการณ์ผิดปกติ

2.1.6 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายสำคัญของประเทศไทยที่กำหนดแนวทางในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการให้บริการที่จำเป็นของประเทศ (ราชกิจจานุเบกษา, 2562) กฎหมายฉบับนี้ให้ความสำคัญกับหน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ Critical Information Infrastructure: CII ซึ่งจำเป็นต้องมีมาตรการในการป้องกัน เฝ้าระวัง รับมือ และฟื้นฟูระบบจากภัยคุกคามทางไซเบอร์เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่องและลดผลกระทบต่อประชาชน พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกรอบทางกฎหมายที่กำหนดให้หน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีมาตรการด้านการป้องกัน เฝ้าระวัง รับมือ และฟื้นฟูระบบ ซึ่งสามารถเชื่อมโยงกับหน้าที่หลักของ NIST Cybersecurity Framework 2.0 ได้ ดังแสดงในภาพที่ 2-3



ภาพที่ 2-3 ความเชื่อมโยงระหว่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับ NIST Cybersecurity Framework 2.0

ในบริบทของหน่วยงานภาครัฐ ศูนย์ข้อมูลถือเป็นส่วนสำคัญในการจัดเก็บ ประมวลผล และให้บริการข้อมูล หากศูนย์ข้อมูลไม่มีมาตรการควบคุมที่เหมาะสม อาจส่งผลกระทบต่อความปลอดภัยของข้อมูล ความต่อเนื่องของบริการ และความเชื่อมั่นของประชาชน ดังนั้น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงถูกนำมาใช้เป็นบริบททางกฎหมายประกอบการวิเคราะห์ความเสี่ยงและการจัดทำข้อเสนอแนะในการยกระดับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลภาครัฐ

2.2 การประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูล

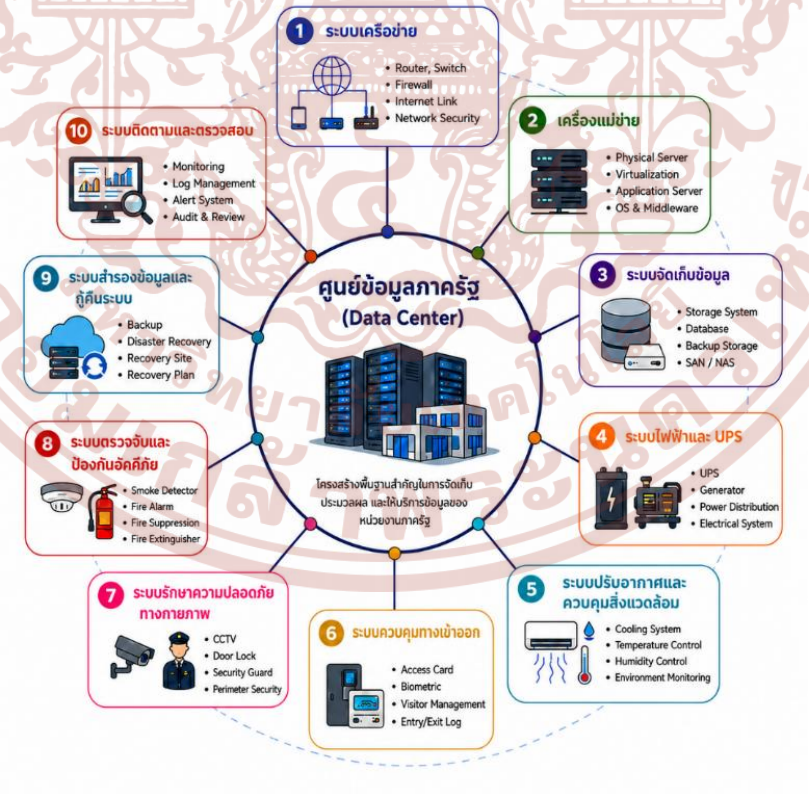
ศูนย์ข้อมูล หรือ Data Center เป็นโครงสร้างพื้นฐานสำคัญที่ใช้ในการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูลขององค์กร โดยประกอบด้วยเครื่องแม่ข่าย ระบบเครือข่าย อุปกรณ์จัดเก็บข้อมูล ระบบไฟฟ้า ระบบปรับอากาศ ระบบสำรองไฟ ระบบรักษาความปลอดภัยทางกายภาพ และระบบควบคุมการเข้าถึง ศูนย์ข้อมูลจึงมีความสำคัญต่อความต่อเนื่องในการให้บริการของหน่วยงานภาครัฐ การประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลเป็นกระบวนการที่ช่วยให้หน่วยงานสามารถระบุจุดอ่อน ภัยคุกคาม ช่องโหว่ และผลกระทบที่อาจเกิดขึ้นกับระบบและข้อมูลได้อย่างเป็นระบบ โดยการประเมินควรครอบคลุมทั้งด้านเทคนิค ด้านกระบวนการ

ด้านกายภาพ และด้านบุคลากร เพื่อให้สามารถกำหนดมาตรการลดความเสี่ยงได้อย่างเหมาะสมกับบริบทของหน่วยงาน

2.2.1 แนวคิดเกี่ยวกับศูนย์ข้อมูลภาครัฐ

ศูนย์ข้อมูลภาครัฐเป็นโครงสร้างพื้นฐานที่มีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานรัฐ เนื่องจากเป็นแหล่งรวมของระบบสารสนเทศ ข้อมูลสำคัญ และบริการดิจิทัลที่เกี่ยวข้องกับภารกิจของหน่วยงาน หากศูนย์ข้อมูลเกิดความเสียหายหรือไม่สามารถให้บริการได้ อาจส่งผลกระทบต่อการทำงานของหน่วยงาน การให้บริการประชาชน และความเชื่อมั่นต่อภาครัฐ

ศูนย์ข้อมูลภาครัฐประกอบด้วยระบบเครือข่าย เครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล ระบบไฟฟ้า ระบบสำรองไฟ ระบบปรับอากาศ ระบบควบคุมการเข้าออก ระบบตรวจจับและป้องกันอัคคีภัย ตลอดจนกระบวนการบริหารจัดการและบุคลากรที่เกี่ยวข้อง ซึ่งองค์ประกอบเหล่านี้ล้วนส่งผลต่อระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น การประเมินความเสี่ยงของศูนย์ข้อมูลจึงจำเป็นต้องพิจารณาทั้งด้านเทคโนโลยีสารสนเทศและด้านกายภาพควบคู่กัน ดังแสดงในภาพที่ 2-4



ภาพที่ 2-4 องค์ประกอบศูนย์ข้อมูลภาครัฐ

2.2.2 การประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการสำคัญที่ช่วยให้หน่วยงานสามารถทำความเข้าใจภัยคุกคามและช่องโหว่ที่อาจส่งผลกระทบต่อศูนย์ข้อมูล โดยพิจารณาจากทรัพย์สินสารสนเทศ โอกาสการเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้นกับศูนย์ข้อมูล หากหน่วยงานไม่มีการประเมินความเสี่ยงอย่างต่อเนื่อง อาจทำให้ไม่สามารถระบุจุดอ่อนของระบบและไม่สามารถจัดลำดับความสำคัญของมาตรการควบคุมได้อย่างเหมาะสม (Joint Task Force Transformation Initiative, 2012)

กระบวนการประเมินความเสี่ยงควรเริ่มจากการระบุทรัพย์สินที่เกี่ยวข้องกับ ศูนย์ข้อมูล เช่น เครื่องแม่ข่าย ระบบเครือข่าย ฐานข้อมูล ระบบสำรองข้อมูล และระบบสนับสนุนต่าง ๆ จากนั้นจึงวิเคราะห์ภัยคุกคามที่อาจเกิดขึ้น เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์ อุปกรณ์ขัดข้อง ไฟฟ้าดับ อัคคีภัย หรือภัยพิบัติทางธรรมชาติ แล้วนำมาพิจารณาร่วมกับช่องโหว่ที่มีอยู่เพื่อประเมินระดับความเสี่ยงและกำหนดแนวทางควบคุมที่เหมาะสม

ในการศึกษานี้ การประเมินความเสี่ยงถูกนำมาใช้เพื่อวิเคราะห์ระดับความพร้อมของศูนย์ข้อมูลและระบุประเด็นที่ควรได้รับการปรับปรุง โดยเชื่อมโยงกับหน้าที่หลักของ NIST Cybersecurity Framework 2.0 ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover

2.2.3 การควบคุมการเข้าถึง

การควบคุมการเข้าถึงเป็นมาตรการสำคัญในการป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบ ข้อมูล หรือพื้นที่สำคัญภายในศูนย์ข้อมูล โดยการควบคุมการเข้าถึงควรครอบคลุมทั้งการเข้าถึงเชิงกายภาพและการเข้าถึงเชิงตรรกะ

การควบคุมการเข้าถึงเชิงกายภาพ ได้แก่ การกำหนดสิทธิ์เข้าออกพื้นที่ศูนย์ข้อมูล การใช้บัตรผ่าน ระบบยืนยันตัวตน กล้องวงจรปิด ระบบบันทึกการเข้าออก และการกำหนดผู้มีอำนาจในการอนุมัติการเข้าถึงพื้นที่ ส่วนการควบคุมการเข้าถึงเชิงตรรกะประกอบด้วย การกำหนดสิทธิ์ผู้ใช้งาน การใช้รหัสผ่านที่ปลอดภัย การพิสูจน์ตัวตนหลายปัจจัย การจำกัดสิทธิ์ตามหน้าที่งาน และการทบทวนสิทธิ์อย่างสม่ำเสมอ หากมาตรการดังกล่าวไม่มีประสิทธิภาพเพียงพอ อาจก่อให้เกิดความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต การแก้ไขข้อมูลโดยมิชอบ การใช้สิทธิ์เกินความจำเป็น หรือการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต ดังนั้น การประเมินความพร้อมด้านการควบคุมการเข้าถึงจึงเป็นองค์ประกอบสำคัญในการรักษาความมั่นคงปลอดภัยของศูนย์ข้อมูล

2.2.4 การรักษาความปลอดภัยทางกายภาพ

การรักษาความปลอดภัยทางกายภาพเป็นมาตรการที่ใช้ป้องกันการเข้าถึงพื้นที่ศูนย์ข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการป้องกันความเสียหายจากเหตุการณ์ทางกายภาพ เช่น อัคคีภัย น้ำท่วม ความเสียหายจากระบบไฟฟ้า ความร้อน ความชื้น หรือการบุกรุกพื้นที่

มาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางกายภาพอาจประกอบด้วยระบบควบคุมประตู ระบบกล้องวงจรปิด ระบบบันทึกการเข้าออก ระบบตรวจจับควันไฟ ระบบดับเพลิง ระบบสำรองไฟ เครื่องกำเนิดไฟฟ้าสำรอง ระบบปรับอากาศ และการควบคุมสภาพแวดล้อมภายในศูนย์ข้อมูล เนื่องจากความเสียหายทางกายภาพสามารถส่งผลกระทบโดยตรงต่อความพร้อมใช้งานของระบบและข้อมูล การประเมินมาตรการด้านนี้จึงช่วยให้หน่วยงานสามารถระบุจุดอ่อนของระบบสนับสนุนและกำหนดแนวทางป้องกันได้อย่างเหมาะสม

2.2.5 การติดตามและตรวจสอบการทำงานของระบบ

การติดตามและตรวจสอบการทำงานของระบบเป็นกระบวนการสำคัญในการเฝ้าระวัง ตรวจจับ และวิเคราะห์ความผิดปกติหรือความเสี่ยงที่อาจส่งผลกระทบต่อศูนย์ข้อมูล โดยอาศัยข้อมูลจากบันทึกเหตุการณ์ (Log) การแจ้งเตือนจากระบบรักษาความปลอดภัย การเฝ้าระวังเครือข่าย และการวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถรับรู้สถานการณ์และดำเนินการตอบสนองได้อย่างทันท่วงที หากหน่วยงานขาดกลไกการเฝ้าระวังติดตามที่มีประสิทธิภาพ อาจไม่สามารถตรวจพบปัญหาหรือภัยคุกคามได้ในระยะเริ่มต้น ส่งผลให้ความเสียหายขยายวงกว้างและกระทบต่อระบบสารสนเทศรวมถึงข้อมูลสำคัญขององค์กร ดังนั้น ความพร้อมด้านการเฝ้าระวังและการตรวจสอบจึงถือเป็นองค์ประกอบสำคัญในการประเมินความเสี่ยงของศูนย์ข้อมูล โดยการติดตามควรครอบคลุมระบบเครือข่าย เครื่องแม่ข่าย ระบบฐานข้อมูล ระบบสำรองข้อมูล อุปกรณ์รักษาความปลอดภัย และระบบสนับสนุนอื่น ๆ ที่เกี่ยวข้อง พร้อมกำหนดผู้รับผิดชอบ ขั้นตอนการแจ้งเตือน และแนวทางการจัดการเมื่อเกิดความผิดปกติอย่างชัดเจน เพื่อเพิ่มประสิทธิภาพในการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยและลดผลกระทบต่อการดำเนินงานของศูนย์ข้อมูล

2.2.6 การบริหารจัดการเหตุการณ์ที่ไม่คาดคิดและการกู้คืนระบบ

การบริหารจัดการเหตุการณ์ที่ไม่คาดคิดเป็นกระบวนการที่ช่วยให้หน่วยงานสามารถตอบสนองต่อภัยคุกคามทางไซเบอร์หรือสถานการณ์ที่ส่งผลกระทบต่อศูนย์ข้อมูลได้อย่างเป็นระบบ เช่น การโจมตีทางไซเบอร์ ระบบขัดข้อง อุปกรณ์เสียหาย ไฟฟ้าดับ หรือภัยพิบัติทางกายภาพ โดยควรมีขั้นตอนในการแจ้งเหตุ วิเคราะห์สาเหตุ จำกัดผลกระทบ ดำเนินการแก้ไข และรายงานผลการ

ดำเนินงานอย่างชัดเจน นอกจากนี้ การกู้คืนระบบเป็นกลไกสำคัญที่ช่วยให้หน่วยงานสามารถกลับมาให้บริการได้อย่างต่อเนื่องภายหลังเกิดเหตุขัดข้อง โดยควรจัดทำแผนสำรองข้อมูล แผนฟื้นฟูระบบ การทดสอบแผนอย่างสม่ำเสมอ และการปรับปรุงแนวทางปฏิบัติจากบทเรียนที่ได้รับ เพื่อเพิ่มประสิทธิภาพในการรับมือกับเหตุการณ์ในอนาคต แนวคิดดังกล่าวสอดคล้องกับหน้าที่ Respond และ Recover ของ NIST Cybersecurity Framework 2.0

สำหรับศูนย์ข้อมูลภาครัฐ การบริหารจัดการเหตุการณ์และการกู้คืนระบบมีความสำคัญอย่างยิ่ง เนื่องจากระบบและข้อมูลที่อยู่ภายในศูนย์ข้อมูลอาจเกี่ยวข้องกับการให้บริการประชาชนหรือภารกิจสำคัญของหน่วยงาน หากไม่มีแผนรับมือและแผนกู้คืนระบบที่ชัดเจน อาจส่งผลให้การให้บริการหยุดชะงักเป็นระยะเวลานานและกระทบต่อความเชื่อมั่นของผู้ใช้บริการ

2.2.7 การวิเคราะห์ช่องว่าง

การวิเคราะห์ช่องว่าง หรือ Gap Analysis เป็นกระบวนการเปรียบเทียบสถานะปัจจุบันของศูนย์ข้อมูลกับแนวทางหรือมาตรฐานที่ควรเป็น เพื่อระบุประเด็นที่มีความสอดคล้องกับแนวทางที่กำหนด และประเด็นที่ยังต้องได้รับการปรับปรุงหรือพัฒนาเพิ่มเติม

ในการศึกษานี้ การวิเคราะห์ช่องว่างถูกนำมาใช้เพื่อเปรียบเทียบการดำเนินงานปัจจุบันของศูนย์ข้อมูลกับแนวทางตาม NIST Cybersecurity Framework 2.0 (Pascoe et al., 2024) โดยพิจารณาประเด็นด้านการกำกับดูแล การระบุความเสี่ยง การควบคุมการเข้าถึง การรักษาความปลอดภัยทางกายภาพ การตรวจจับเหตุการณ์ การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบ

การวิเคราะห์ช่องว่างช่วยให้เห็นลำดับขั้นตอนตั้งแต่การสำรวจสถานะปัจจุบันของศูนย์ข้อมูล การเปรียบเทียบกับแนวทางตามกรอบ NIST Cybersecurity Framework 2.0 การระบุช่องว่างของมาตรการควบคุม การประเมินระดับความเสี่ยง การจัดลำดับความสำคัญของความเสี่ยง และการจัดทำข้อเสนอแนะในการลดความเสี่ยง ดังแสดงในภาพที่ 2-5



ภาพที่ 2-5 กระบวนการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework

การวิเคราะห์ช่องว่างช่วยให้หน่วยงานสามารถประเมินระดับความพร้อมของศูนย์ข้อมูลระบุประเด็นที่ควรได้รับการปรับปรุง และจัดลำดับความสำคัญของความเสี่ยงได้อย่างเป็นระบบ เพื่อนำไปสู่การจัดทำข้อเสนอแนะในการลดความเสี่ยงที่เหมาะสมกับบริบทของหน่วยงานภาครัฐ

2.2.8 ตัวชี้วัดผลการประเมิน

ตัวชี้วัดผลการประเมิน (Key Performance Indicators: KPI) เป็นเครื่องมือที่ใช้ในการวัดผลการดำเนินงานและระดับความสำเร็จของกิจกรรมต่าง ๆ ตามเป้าหมายที่กำหนด ในบริบทของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ KPI สามารถนำมาใช้เพื่อวัดระดับความสอดคล้องของมาตรการควบคุมกับกรอบมาตรฐานที่เกี่ยวข้อง รวมถึงใช้ในการติดตามความก้าวหน้าของการปรับปรุงมาตรการด้านความมั่นคงปลอดภัย ตัวอย่างดัชนีชี้วัดที่สามารถนำมาใช้กับศูนย์ข้อมูล ได้แก่ ระดับความครบถ้วนของบัญชีทรัพย์สินสารสนเทศ ระดับความสอดคล้องของสิทธิ์การเข้าถึงกับหน้าที่งาน จำนวนเหตุการณ์ด้านความปลอดภัยที่ได้รับการตรวจพบ ระยะเวลาในการตอบสนองต่อเหตุการณ์ ความถี่ในการสำรองข้อมูล ความสำเร็จของการทดสอบแผนกู้คืนระบบ และระดับการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์การกำหนด KPI ที่เหมาะสมจะช่วยให้หน่วยงานสามารถวัดผลการดำเนินงานได้อย่างเป็นรูปธรรม และสามารถนำผลการประเมินไปใช้ประกอบการตัดสินใจในการลดความเสี่ยงและปรับปรุงมาตรการควบคุมได้อย่างมีประสิทธิภาพ

2.3 งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้อง ทั้งในประเทศและต่างประเทศ พบว่ามีการประยุกต์ใช้ NIST Cybersecurity Framework ในการประเมินความเสี่ยง การจัดลำดับความสำคัญของมาตรการควบคุม การบริหารจัดการความเสี่ยง และการยกระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรในหลากหลายบริบท โดยมีรายละเอียดดังต่อไปนี้

Amiruddin และคณะ (2021) ได้ศึกษาการวางแผนบริหารจัดการความเสี่ยงทางไซเบอร์โดยใช้ NIST Cybersecurity Framework, NIST SP 800-53 และ CIS Controls ผลการศึกษาชี้ให้เห็นว่าการบูรณาการกรอบมาตรฐานหลายแหล่งช่วยให้องค์กรสามารถเชื่อมโยงความเสี่ยงกับมาตรการควบคุมได้ชัดเจนขึ้น และสามารถกำหนดแผนลดความเสี่ยงที่เหมาะสมกับระบบสารสนเทศขององค์กรได้อย่างเป็นระบบ แนวคิดดังกล่าวมีความเกี่ยวข้องกับงานวิจัยนี้ เนื่องจากการประเมินศูนย์ข้อมูลภาครัฐจำเป็นต้องแปลงผลการวิเคราะห์ความเสี่ยงให้เป็นมาตรการควบคุมที่สามารถนำไปปฏิบัติได้จริง

Bakalynskyi และ Korobeynikov (2023) ได้ศึกษาแนวทางการกำหนดเป้าหมายในการสร้างระบบที่มีความยืดหยุ่นทางไซเบอร์ตามแนวทางของ NIST โดยเน้นความสามารถของระบบในการคาดการณ์ ทนทาน กู้คืน และปรับตัวต่อเหตุการณ์ที่ไม่พึงประสงค์ แนวคิดนี้มีความสอดคล้องกับการประเมินศูนย์ข้อมูลภาครัฐที่ต้องสามารถให้บริการได้อย่างต่อเนื่องแม้เกิดเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์

Dedeke (2017) ได้ศึกษาการนำ NIST Cybersecurity Framework ไปใช้โดยอ้างอิง Capability Levels, Implementation Tiers และ Profiles ผลการศึกษาชี้ให้เห็นว่าแนวทางดังกล่าวช่วยให้องค์กรสามารถประเมินระดับความพร้อมของตนเอง กำหนดเป้าหมายด้านความปลอดภัย และวางแผนปรับปรุงตามลำดับความสำคัญได้อย่างเป็นระบบ แนวคิดนี้สามารถนำมาใช้ประกอบการประเมินระดับความพร้อมของศูนย์ข้อมูลภาครัฐในงานวิจัยนี้

Dutta และ Al-Shaer (2019) ได้ศึกษาการเลือกมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์เพื่อการลดความเสี่ยงอย่างเหมาะสม โดยพิจารณาจากปัจจัยหลายด้าน เช่น ทรัพย์สิน ภัยคุกคาม ประสิทธิภาพของมาตรการควบคุม และข้อจำกัดด้านทรัพยากร แนวคิดดังกล่าวสอดคล้องกับงานวิจัยนี้ ซึ่งมุ่งจัดลำดับความสำคัญของความเสี่ยงและเสนอแนวทางลดความเสี่ยงให้เหมาะสมกับบริบทของหน่วยงานภาครัฐ

Freas และคณะ (2022) ได้ศึกษากรอบกระบวนการวิศวกรรมสำหรับการประเมินการตอบสนองต่อเหตุการณ์ด้านไซเบอร์ โดยชี้ให้เห็นว่าการตอบสนองต่อเหตุการณ์ควรถูกออกแบบให้เป็นกระบวนการที่มีขั้นตอนชัดเจน สามารถประเมินระดับความพร้อมขององค์กร และสามารถนำไปใช้ในการปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ได้ งานวิจัยนี้มีความเกี่ยวข้องกับการศึกษานี้ในส่วนของการประเมินความพร้อมด้านการบริหารจัดการเหตุการณ์และการกู้คืนระบบของศูนย์ข้อมูล

Handri และคณะ (2023) ได้ศึกษาการจัดลำดับความสำคัญด้านบุคลากร กระบวนการและเทคโนโลยีสำหรับการนำ NIST Cybersecurity Framework ไปใช้ในระบบรัฐบาลอิเล็กทรอนิกส์ ผลการศึกษาพบว่าการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ไม่ควรเน้นเฉพาะเทคโนโลยีเท่านั้น แต่ต้องพิจารณาความพร้อมของบุคลากร กระบวนการทำงาน และเครื่องมือที่เกี่ยวข้องร่วมกัน ซึ่งสอดคล้องกับบริบทของศูนย์ข้อมูลภาครัฐที่ต้องอาศัยทั้งผู้ดูแลระบบ นโยบาย กระบวนการปฏิบัติงาน และเทคโนโลยีในการบริหารจัดการความเสี่ยง

Khou และคณะ (2017) ได้ศึกษากรอบการจัดลำดับความสำคัญของกระบวนการ กิจกรรมและงานด้าน Systems Security Engineering ตามแนวทางของ NIST SP 800-160 ผลการศึกษาชี้ให้เห็นว่าการออกแบบระบบที่ปลอดภัยควรคำนึงถึงความปลอดภัยตั้งแต่ระดับกระบวนการและโครงสร้างระบบ ไม่ใช่เพียงการเพิ่มมาตรการควบคุมภายหลัง แนวคิดนี้มีความเกี่ยวข้องกับการวิเคราะห์โครงสร้างพื้นฐานของศูนย์ข้อมูลที่ต้องพิจารณาความมั่นคงปลอดภัยตั้งแต่ระดับการออกแบบการดำเนินงาน และการบำรุงรักษา

Monev (2024) ได้ศึกษาความเหมาะสมของกรอบงานด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่เน้นด้านไอที ผลการศึกษาชี้ให้เห็นว่าองค์กรควรเลือกใช้กรอบงานให้เหมาะสมกับวัตถุประสงค์ ขอบเขต ทรัพยากร และข้อจำกัดขององค์กร ไม่จำเป็นต้องใช้ทุกมาตรฐานอย่างครบถ้วน แต่ควรเลือกเฉพาะส่วนที่เหมาะสมกับบริบทและความเสี่ยงขององค์กร แนวคิดนี้สนับสนุนการศึกษานี้ที่เลือกใช้ NIST Cybersecurity Framework 2.0 เป็นกรอบหลัก และใช้มาตรฐานอื่นเป็นแนวทางประกอบเฉพาะส่วนที่เกี่ยวข้อง

Moreira และคณะ (2021) ได้ศึกษาการประเมินประสิทธิภาพของมาตรการควบคุมตาม NIST Framework ด้วยวิธีการตัดสินใจหลายเกณฑ์ ผลการศึกษาชี้ให้เห็นว่าการประเมินมาตรการควบคุมไม่ควรพิจารณาเพียงว่ามีหรือไม่มีมาตรการเท่านั้น แต่ควรพิจารณาระดับความสำคัญ ประสิทธิผลและความเหมาะสมของมาตรการในบริบทขององค์กรด้วย แนวคิดดังกล่าวมีความเกี่ยวข้องกับการกำหนดตัวชี้วัดผลการประเมินและการจัดลำดับความสำคัญของความเสี่ยงในงานวิจัยนี้

Mylrea และคณะ (2017) ได้ศึกษา Buildings Cybersecurity Framework ซึ่งเป็นกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์สำหรับอาคารและระบบที่เกี่ยวข้อง โดยอ้างอิงหน้าที่หลักของ NIST Cybersecurity Framework ได้แก่ Identify, Protect, Detect, Respond และ Recover งานวิจัยดังกล่าวชี้ให้เห็นว่าอาคารสมัยใหม่และระบบโครงสร้างพื้นฐานที่มีการเชื่อมโยงระหว่างเทคโนโลยีสารสนเทศและระบบควบคุมทางกายภาพมีความเสี่ยงจากภัยคุกคามทางไซเบอร์เพิ่มขึ้น จึงจำเป็นต้องมีแนวทางในการประเมินและจัดการความเสี่ยงอย่างเป็นระบบ แนวคิดดังกล่าวมีความเกี่ยวข้องกับการประเมินความเสี่ยงของศูนย์ข้อมูล เนื่องจากศูนย์ข้อมูลมีทั้งองค์ประกอบด้านระบบดิจิทัล ระบบเครือข่าย และระบบกายภาพที่สนับสนุนการดำเนินงาน

Perdana และคณะ (2022) ได้ศึกษาการประเมินความมั่นคงปลอดภัยและความเสี่ยงของระบบสารสนเทศทางวิชาการโดยใช้ NIST Framework ผลการศึกษาพบว่าการใช้กรอบ NIST ช่วยให้องค์กรสามารถประเมินสถานะความปลอดภัยของระบบสารสนเทศได้อย่างเป็นระบบ และสามารถระบุประเด็นความเสี่ยงที่ควรได้รับการปรับปรุง เช่น การควบคุมการเข้าถึง การจัดการช่องโหว่ และการกำหนดมาตรการลดความเสี่ยง

Safitri และ Kabetta (2023) ได้ศึกษาการวางแผนบริหารจัดการความเสี่ยงทางไซเบอร์โดยใช้ NIST Cybersecurity Framework, ISO/IEC 27005 และ NIST SP 800-53 ในองค์กรกรณีศึกษา ผลการศึกษาพบว่าการวางแผนบริหารจัดการความเสี่ยงควรเริ่มจากการระบุทรัพย์สินที่สำคัญ วิเคราะห์ภัยคุกคาม ประเมินผลกระทบ และเลือกมาตรการควบคุมที่สัมพันธ์กับระดับความเสี่ยง แนวคิดดังกล่าวสามารถนำมาปรับใช้กับการประเมินความเสี่ยงของศูนย์ข้อมูลภาครัฐได้ เนื่องจากศูนย์ข้อมูลประกอบด้วยทรัพย์สินสารสนเทศหลายประเภทและมีผลกระทบต่อความต่อเนื่องของบริการ

Saritac และคณะ (2022) ได้ศึกษาการประเมิน Cybersecurity Framework ในบริบทของโครงสร้างพื้นฐานสำคัญ ผลการศึกษาพบว่า NIST Cybersecurity Framework สามารถนำมาใช้เป็นแนวทางในการจัดการความเสี่ยงของระบบที่มีความซับซ้อน เช่น ระบบเทคโนโลยีสารสนเทศ ระบบควบคุมอุตสาหกรรม ระบบไซเบอร์กายภาพ และ Internet of Things ได้อย่างเหมาะสม งานวิจัยนี้สนับสนุนแนวคิดที่ว่าหน่วยงานที่มีระบบสำคัญควรมีกรอบการประเมินความเสี่ยงที่ครอบคลุมทั้งการป้องกัน การตรวจจับ การตอบสนอง และการกู้คืนระบบ

Supriyadi และ Hardani (2018) ได้ศึกษาการสร้างสถานการณ์ความเสี่ยงของระบบสารสนเทศโดยใช้ COBIT 5 for Risk ร่วมกับ NIST SP 800-30 ผลการศึกษาชี้ให้เห็นว่าการประเมินความเสี่ยงควรเริ่มจากการระบุสถานการณ์ความเสี่ยง วิเคราะห์ภัยคุกคามและช่องโหว่ ประเมินระดับโอกาสเกิดและผลกระทบ จากนั้นจึงกำหนดมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยง งานวิจัยนี้สอดคล้องกับการศึกษาของผู้วิจัยที่มุ่งประเมินความเสี่ยงของศูนย์ข้อมูลอย่างเป็นระบบ

Werthwein และ Annighoefer (2024) ได้ศึกษากรอบการประเมินความเสี่ยงด้านไซเบอร์สำหรับระบบอากาศยาน ซึ่งแม้จะเป็นบริบทเฉพาะด้าน แต่สะท้อนให้เห็นว่าการประเมินความเสี่ยงมีความสำคัญต่อระบบที่มีความซับซ้อนและมีผลกระทบสูง แนวคิดดังกล่าวสามารถนำมาเทียบเคียงกับศูนย์ข้อมูลภาครัฐ ซึ่งเป็นระบบสำคัญที่ต้องมีมาตรการควบคุมที่รัดกุมและสามารถตรวจสอบได้

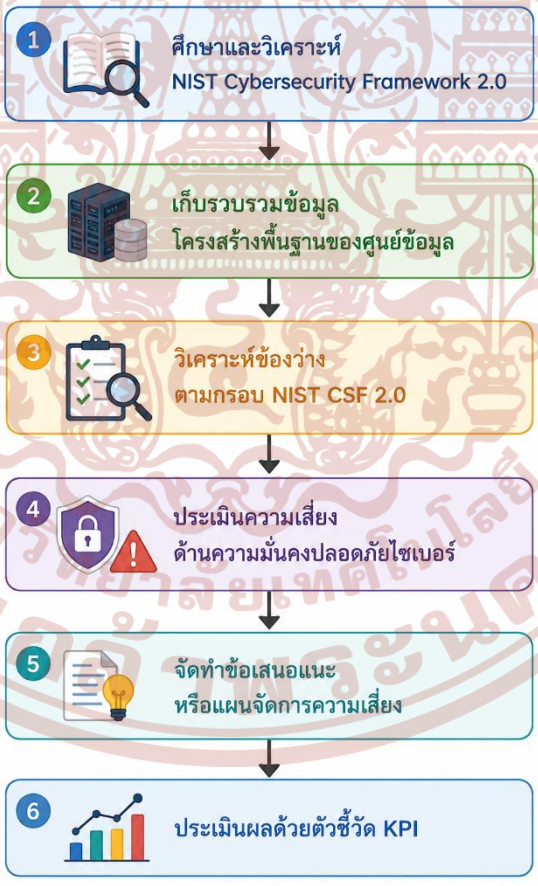
จากงานวิจัยที่เกี่ยวข้องข้างต้น สามารถสรุปได้ว่า NIST Cybersecurity Framework เป็นกรอบการทำงานที่สามารถนำไปใช้ในการประเมินความเสี่ยงและปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ได้ในหลายบริบท โดยเฉพาะระบบที่มีความสำคัญต่อการดำเนินงานขององค์กร เช่น ศูนย์ข้อมูล ระบบสารสนเทศภาครัฐ และโครงสร้างพื้นฐานสำคัญ ผู้วิจัยจึงนำแนวคิดจาก NIST Cybersecurity Framework 2.0 การประเมินความเสี่ยง การวิเคราะห์ช่องว่าง และแนวทางการจัดลำดับความสำคัญของมาตรการควบคุม มาใช้เป็นกรอบในการวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ

บทที่ 3

วิธีการดำเนินการวิจัย

การค้นคว้าอิสระนี้ มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยอ้างอิงกรอบการทำงาน NIST Cybersecurity Framework 2.0 เป็นแนวทางหลักในการศึกษา การดำเนินการวิจัยประกอบด้วยการศึกษากรอบมาตรฐานที่เกี่ยวข้อง การเก็บรวบรวมข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล การวิเคราะห์ช่องว่าง การประเมินความเสี่ยง การจัดทำข้อเสนอแนะในการลดความเสี่ยง และการกำหนดตัวชี้วัดผลการประเมิน โดยมีรายละเอียดวิธีการดำเนินการวิจัยดังต่อไปนี้

3.1 ขั้นตอนการดำเนินการวิจัย



ภาพที่ 3-1 ขั้นตอนการดำเนินงานวิจัย

จากภาพที่ 3-1 มีขั้นตอนในการดำเนินงานวิจัยดังนี้

3.1.1 ศึกษากรอบการทำงาน NIST Cybersecurity Framework 2.0 รวมถึงมาตรฐานและแนวคิดที่เกี่ยวข้อง เพื่อนำมาใช้เป็นกรอบอ้างอิงในการวิเคราะห์ความเสี่ยงของศูนย์ข้อมูล โดยพิจารณาหน้าที่หลักของ NIST CSF 2.0 ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover

3.1.2 เก็บรวบรวมข้อมูลเกี่ยวกับองค์ประกอบของศูนย์ข้อมูล เช่น ระบบเครือข่าย เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล ระบบไฟฟ้า ระบบสำรองไฟ ระบบปรับอากาศ ระบบควบคุมทางเข้าออกระบบรักษาความปลอดภัยทางกายภาพ ระบบติดตามตรวจสอบ และกระบวนการบริหารจัดการที่เกี่ยวข้อง

3.1.3 นำข้อมูลสถานะปัจจุบันของศูนย์ข้อมูลมาเปรียบเทียบกับแนวทางตามกรอบ NIST CSF 2.0 เพื่อประเมินความสอดคล้องของมาตรการและกระบวนการที่มีอยู่ในปัจจุบัน รวมถึงระบุข้อจำกัดและประเด็นที่ควรได้รับการปรับปรุงเพิ่มเติม เพื่อนำไปใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

3.1.4 นำประเด็นที่ได้จากการวิเคราะห์ช่องว่างมาประกอบการประเมินความเสี่ยง โดยพิจารณาจากทรัพย์สินที่เกี่ยวข้อง ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ โอกาสเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดระดับความเสี่ยงของแต่ละประเด็น

3.1.5 หลังจากประเมินระดับความเสี่ยง ผู้วิจัยจัดลำดับความสำคัญของความเสี่ยง และจัดทำข้อเสนอแนะในการลดความเสี่ยงหรือแผนจัดการความเสี่ยง เพื่อให้หน่วยงานสามารถนำไปใช้เป็นแนวทางในการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูล

3.1.6 กำหนดตัวชี้วัดผลการประเมิน หรือ Key Performance Indicators (KPI) เพื่อใช้วัดระดับความสอดคล้องของมาตรการควบคุมกับกรอบ NIST CSF 2.0 ประเมินระดับความพร้อมของศูนย์ข้อมูล และสนับสนุนการจัดลำดับความสำคัญของประเด็นที่ควรได้รับการปรับปรุง

3.2 เครื่องมือที่ใช้ในการวิจัย

การดำเนินการวิจัยครั้งนี้ใช้เครื่องมือและเอกสารประกอบการวิเคราะห์ เพื่อสนับสนุนการเก็บรวบรวมข้อมูล การวิเคราะห์ช่องว่าง การประเมินความเสี่ยง และการจัดทำข้อเสนอแนะในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูล โดยเครื่องมือที่ใช้ในการวิจัยประกอบด้วยเครื่องมือสำคัญ ดังนี้

3.2.1 กรอบการทำงาน NIST Cybersecurity Framework 2.0

ผู้วิจัยใช้ NIST Cybersecurity Framework 2.0 เป็นกรอบหลักในการวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูล โดยพิจารณาตามหน้าที่หลัก 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover เพื่อใช้เป็นแนวทางในการเปรียบเทียบสถานะปัจจุบันของศูนย์ข้อมูลกับแนวทางที่ควรดำเนินการ

3.2.2 ตารางวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0

ตารางวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 ใช้สำหรับเปรียบเทียบสถานะการดำเนินงานปัจจุบันของศูนย์ข้อมูลกับแนวทางที่กำหนดไว้ในกรอบดังกล่าว โดยพิจารณามาตรการควบคุม กระบวนการปฏิบัติงาน และข้อจำกัดที่เกี่ยวข้องกับการดำเนินงานของศูนย์ข้อมูล ผลจากการวิเคราะห์จะถูกนำไปใช้เพื่อระบุประเด็นที่ควรได้รับการปรับปรุงเพิ่มเติม และใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

3.2.3 แบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

แบบประเมินความเสี่ยงใช้สำหรับวิเคราะห์ระดับความเสี่ยงของประเด็นที่เกี่ยวข้องกับโครงสร้างพื้นฐานศูนย์ข้อมูล โดยพิจารณาจากทรัพย์สินที่เกี่ยวข้อง ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ โอกาสเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้น เพื่อนำไปสู่การจัดระดับความเสี่ยงและการจัดลำดับความสำคัญของความเสี่ยง

3.2.4 เอกสารแผนการตรวจสอบและประเมินความเสี่ยง

ผู้วิจัยใช้เอกสารแผนการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นแนวทางประกอบการกำหนดขั้นตอนและเกณฑ์ในการประเมินความเสี่ยง โดยครอบคลุมกระบวนการกำหนดบริบทความเสี่ยง การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยง และการติดตามทบทวนความเสี่ยง

3.2.5 เกณฑ์การประเมินโอกาสเกิดและผลกระทบ

เกณฑ์การประเมินโอกาสเกิดและผลกระทบใช้สำหรับกำหนดระดับความเสี่ยงของแต่ละประเด็น โดยพิจารณาความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้นร่วมกับระดับผลกระทบที่อาจเกิดขึ้นต่อศูนย์ข้อมูล ระบบสารสนเทศ ข้อมูลสำคัญ การให้บริการของหน่วยงาน และความเชื่อมั่นของผู้มีส่วนเกี่ยวข้อง

3.2.6 ตัวชี้วัดผลการประเมิน

ตัวชี้วัดผลการประเมิน หรือ Key Performance Indicators (KPI) ใช้สำหรับวัดระดับความสอดคล้องของมาตรการควบคุมกับกรอบ NIST CSF 2.0 รวมถึงใช้ประกอบการประเมินระดับความพร้อมของศูนย์ข้อมูล การจัดลำดับความสำคัญของความเสี่ยง และการพิจารณาประเด็นที่ควรได้รับการปรับปรุง ดังตารางที่ 3-1

ตารางที่ 3-1 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือ	วัตถุประสงค์การใช้งาน
NIST Cybersecurity Framework 2.0	ใช้เป็นกรอบหลักในการประเมิน
ตารางวิเคราะห์ช่องว่างตามกรอบ NIST CSF 2.0	ใช้เปรียบเทียบสถานะปัจจุบันของศูนย์ข้อมูลกับแนวทางตามกรอบ NIST CSF 2.0 และระบุประเด็นที่ควรได้รับการปรับปรุง
แบบประเมินความเสี่ยง	ใช้ประเมินระดับความเสี่ยง
เอกสารแผนการตรวจสอบและประเมินความเสี่ยง	ใช้กำหนดขั้นตอนและเกณฑ์การประเมิน
เกณฑ์โอกาสเกิดและผลกระทบ	ใช้คำนวณระดับความเสี่ยง
KPI	ใช้วัดผลการประเมินและจัดลำดับความสำคัญ

3.3 การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลในการศึกษานี้มีวัตถุประสงค์เพื่อให้ได้ข้อมูลที่เพียงพอและเหมาะสมสำหรับการวิเคราะห์ช่องว่างและการประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยได้มีการรวบรวมข้อมูลจากเอกสารที่เกี่ยวข้อง ข้อมูลด้านโครงสร้างพื้นฐานของศูนย์ข้อมูล ตารางวิเคราะห์ช่องว่าง แบบประเมินความเสี่ยง และข้อมูลจากผู้ที่เกี่ยวข้องกับการดูแลระบบเทคโนโลยีสารสนเทศของหน่วยงาน

3.3.1 ข้อมูลจากเอกสารและมาตรฐานที่เกี่ยวข้อง

การศึกษานี้ใช้ข้อมูลจากเอกสาร มาตรฐาน และกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง ได้แก่ NIST Cybersecurity Framework 2.0, NIST SP 800-30, NIST SP 800-53 , CIS Controls, ITIL, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, แผนดิจิทัล, สถาปัตยกรรมองค์กร, แผนประเมินความเสี่ยง และแผนรับมือภัยคุกคามไซเบอร์ เพื่อใช้เป็นกรอบอ้างอิงในการกำหนดประเด็นการประเมิน การวิเคราะห์ช่องว่าง และการจัดทำข้อเสนอแนะในการลดความเสี่ยง

3.3.2 ข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล

ข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูลที่อยู่ในขอบเขตการศึกษาประกอบด้วย ระบบเครือข่าย เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล ระบบไฟฟ้า ระบบสำรองไฟ ระบบปรับอากาศ ระบบควบคุมทางเข้าออก ระบบรักษาความปลอดภัยทางกายภาพ ระบบตรวจจับและป้องกันอัคคีภัย ระบบติดตามตรวจสอบ และกระบวนการบริหารจัดการเหตุการณ์ที่เกี่ยวข้อง ข้อมูลดังกล่าวใช้สำหรับพิจารณาสถานะปัจจุบันของศูนย์ข้อมูลและระบุประเด็นที่อาจก่อให้เกิดความเสี่ยง

3.3.3 ข้อมูลจากตารางวิเคราะห์ช่องว่างและแบบประเมินความเสี่ยง

ตารางวิเคราะห์ช่องว่างและแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ใช้สำหรับรวบรวมข้อมูลเกี่ยวกับมาตรการควบคุมที่มีอยู่ในปัจจุบัน ช่องว่างของมาตรการควบคุม ภัยคุกคาม ช่องโหว่ โอกาสเกิดเหตุการณ์ ผลกระทบที่อาจเกิดขึ้น และระดับความเสี่ยงของแต่ละประเด็น ข้อมูลที่ได้จะถูกนำไปใช้ในการสรุปผลการประเมินความเสี่ยง การจัดระดับสถานการณ์ความเสี่ยง การจัดกลุ่มประเด็นความเสี่ยง และการกำหนดแนวทางในการลดความเสี่ยง

3.3.4 ข้อมูลจากผู้ที่เกี่ยวข้องกับการดูแลศูนย์ข้อมูล

ข้อมูลเพิ่มเติมได้จากผู้ที่เกี่ยวข้องกับการดูแลระบบเทคโนโลยีสารสนเทศและศูนย์ข้อมูลของหน่วยงาน เช่น เจ้าหน้าที่ผู้ดูแลระบบเครือข่าย เจ้าหน้าที่ผู้ดูแลเครื่องแม่ข่าย เจ้าหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศ และผู้รับผิดชอบระบบที่เกี่ยวข้อง เพื่อให้ได้ข้อมูลเกี่ยวกับการดำเนินงานจริง ปัญหา ข้อจำกัด และมาตรการควบคุมที่ใช้อยู่ในปัจจุบัน

ข้อมูลที่รวบรวมได้ทั้งหมดจะถูกนำไปใช้ประกอบการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อระบุจุดอ่อน ประเมินระดับความพร้อม และจัดทำข้อเสนอแนะในการลดความเสี่ยงให้เหมาะสมกับบริบทของหน่วยงานภาครัฐ ทั้งนี้ แหล่งข้อมูล รายละเอียดข้อมูล และการนำข้อมูลไปใช้ในการวิจัยสามารถสรุปได้ดังตารางที่ 3-2

ตารางที่ 3-2 แหล่งข้อมูลที่ใช้ในการวิจัย

แหล่งข้อมูล	รายละเอียดข้อมูล	การนำข้อมูลไปใช้
เอกสารและมาตรฐานที่เกี่ยวข้อง	มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ กฎหมายที่เกี่ยวข้อง แผนดิจิทัล สถาปัตยกรรมองค์กร แผนประเมินความเสี่ยง และแผนรับมือภัยคุกคามไซเบอร์ของหน่วยงาน	ใช้เป็นกรอบอ้างอิงในการวิเคราะห์และประเมิน
ข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล	ระบบเครือข่าย เครื่องแม่ข่าย ระบบปรับอากาศ และระบบรักษาความปลอดภัย	ใช้ประเมินสถานะปัจจุบันของศูนย์ข้อมูล
ตารางวิเคราะห์ช่องว่างและแบบประเมินความเสี่ยง	ข้อมูลมาตรการควบคุม ช่องว่าง ภัยคุกคาม ช่องโหว่ โอกาสเกิด และผลกระทบ	ใช้วิเคราะห์ช่องว่างและจัดระดับความเสี่ยง
ผู้ที่เกี่ยวข้องกับการดูแลศูนย์ข้อมูล	ข้อมูลจากเจ้าหน้าที่หรือผู้รับผิดชอบระบบที่เกี่ยวข้อง	ใช้ยืนยันข้อมูลการดำเนินงานจริงและข้อจำกัด

3.4 การวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0

การวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 เป็นขั้นตอนที่ใช้ในการเปรียบเทียบสถานะการดำเนินงานปัจจุบันของศูนย์ข้อมูลกับแนวทางที่ควรดำเนินการตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อระบุประเด็นที่มีความสอดคล้องกับแนวทางที่กำหนด ประเด็นที่ยังมีข้อจำกัด และประเด็นที่จำเป็นต้องได้รับการปรับปรุงเพิ่มเติม

การศึกษานี้ใช้กรอบ NIST Cybersecurity Framework 2.0 เป็นแนวทางหลักในการวิเคราะห์ โดยพิจารณาตามหน้าที่หลัก 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover ซึ่งครอบคลุมกระบวนการกำกับดูแล การระบุทรัพย์สินและความเสี่ยง การป้องกัน การตรวจจับเหตุการณ์ การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบ ทั้งนี้การวิเคราะห์ดังกล่าวช่วยให้สามารถประเมินระดับความพร้อมของศูนย์ข้อมูล และระบุจุดอ่อนของมาตรการควบคุมที่มีอยู่ในปัจจุบันได้อย่างเป็นระบบ

การวิเคราะห์ช่องว่างดำเนินการโดยนำข้อมูลที่ได้จากการเก็บรวบรวมข้อมูลในหัวข้อก่อนหน้า เช่น ข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล เอกสารมาตรฐานที่เกี่ยวข้อง ตารางวิเคราะห์ช่องว่างแบบประเมินความเสี่ยง และข้อมูลจากผู้ที่เกี่ยวข้องกับการดูแลศูนย์ข้อมูล มาเปรียบเทียบกับ

แนวทางตามกรอบ NIST CSF 2.0 เพื่อประเมินความสอดคล้องของมาตรการและกระบวนการที่มีอยู่ในปัจจุบัน รวมถึงระบุข้อจำกัดและประเด็นที่ควรได้รับการปรับปรุงเพิ่มเติม

ผลจากการวิเคราะห์ช่องว่างจะถูกนำไปใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยประเด็นที่พบว่ายังมีข้อจำกัดหรือยังไม่สอดคล้องกับแนวทางที่กำหนด จะถูกนำไปพิจารณาร่วมกับปัจจัยด้านทรัพย์สินที่เกี่ยวข้อง สถานการณ์ความเสี่ยง ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ โอกาสเกิดเหตุการณ์ และผลกระทบที่อาจเกิดขึ้น เพื่อใช้ในการจัดระดับความเสี่ยง จัดลำดับความสำคัญของความเสี่ยง และกำหนดแนวทางในการลดความเสี่ยงต่อไป

ทั้งนี้ กระบวนการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 สามารถสรุปขั้นตอนการดำเนินการ รายละเอียด และผลลัพธ์ที่ได้ ดังแสดงในตารางที่ 3-3

ตารางที่ 3-3 แนวทางการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0

ขั้นตอนการวิเคราะห์	รายละเอียดการดำเนินการ	ผลลัพธ์ที่ได้
ศึกษากรอบ NIST CSF 2.0	ศึกษาหน้าที่หลักของกรอบ NIST CSF 2.0 เพื่อนำมาใช้เป็นกรอบอ้างอิงในการวิเคราะห์	ได้กรอบแนวทางสำหรับใช้เปรียบเทียบกับสถานะปัจจุบันของศูนย์ข้อมูล
รวบรวมสถานะปัจจุบัน	รวบรวมข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล มาตรการควบคุมที่มีอยู่ กระบวนการปฏิบัติงาน เอกสารที่เกี่ยวข้อง และข้อมูลจากผู้รับผิดชอบระบบ	ได้ข้อมูลสถานะปัจจุบันของศูนย์ข้อมูลและมาตรการควบคุมที่มีอยู่
เปรียบเทียบกับแนวทางตาม NIST CSF 2.0	นำข้อมูลสถานะปัจจุบันมาเปรียบเทียบกับแนวทางตามกรอบ NIST CSF 2.0 เพื่อพิจารณาความสอดคล้องและข้อจำกัดของการดำเนินงาน	ทราบประเด็นที่มีความสอดคล้อง ประเด็นที่ยังมีข้อจำกัด และประเด็นที่ควรได้รับการปรับปรุง
ระบุช่องว่าง	วิเคราะห์ประเด็นที่ยังมีข้อจำกัดหรือยังไม่สอดคล้องกับแนวทางที่กำหนด เพื่อระบุช่องว่างของมาตรการควบคุมที่เกี่ยวข้องกับศูนย์ข้อมูล	ได้รายการช่องว่างหรือจุดอ่อนที่อาจก่อให้เกิดความเสี่ยง

ขั้นตอนการวิเคราะห์	รายละเอียดการดำเนินการ	ผลลัพธ์ที่ได้
เชื่อมโยงช่องว่างกับประเด็นความเสี่ยง	นำช่องว่างที่พบไปเชื่อมโยงกับทรัพย์สิน สถานการณ์ความเสี่ยง ภัยคุกคาม ช่องโหว่ และมาตรการควบคุมที่มีอยู่	ได้ข้อมูลตั้งต้นสำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
นำผลไปใช้ประเมินความเสี่ยง	นำประเด็นความเสี่ยงไปพิจารณาร่วมกับโอกาสเกิดเหตุการณ์และผลกระทบที่อาจเกิดขึ้น	ได้ข้อมูลสำหรับจัดระดับความเสี่ยง จัดลำดับความสำคัญ และกำหนดแนวทางลดความเสี่ยง

3.5 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นขั้นตอนที่ใช้ในการวิเคราะห์ประเด็นความเสี่ยงที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานของศูนย์ข้อมูล โดยนำผลจากการวิเคราะห์ช่องว่างตามกรอบ NIST Cybersecurity Framework 2.0 มาใช้ประกอบการพิจารณา เพื่อระบุสถานการณ์ความเสี่ยง ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ โอกาสเกิดเหตุการณ์ ผลกระทบ และระดับความเสี่ยงของแต่ละประเด็น

การศึกษานี้ดำเนินการประเมินความเสี่ยงตามแนวทางของแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วยขั้นตอนสำคัญ ได้แก่ การกำหนดบริบทความเสี่ยง การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยง และการติดตามทบทวนความเสี่ยง เพื่อให้การประเมินเป็นระบบและสามารถนำผลที่ได้ไปใช้กำหนดแนวทางลดความเสี่ยงได้อย่างเหมาะสม

การประเมินเริ่มจากการกำหนดขอบเขตและบริบทของความเสี่ยง โดยพิจารณาทรัพย์สินหรือองค์ประกอบของศูนย์ข้อมูลที่เกี่ยวข้อง เช่น ระบบเครือข่าย เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล ระบบไฟฟ้า ระบบสำรองไฟ ระบบปรับอากาศ ระบบควบคุมทางเข้าออก ระบบรักษาความปลอดภัยทางกายภาพ และระบบติดตามตรวจสอบ จากนั้นจึงระบุสถานการณ์ความเสี่ยง ภัยคุกคาม ช่องโหว่ และมาตรการควบคุมที่มีอยู่ในปัจจุบัน

เมื่อระบุความเสี่ยงแล้ว จะดำเนินการวิเคราะห์โอกาสเกิดเหตุการณ์และผลกระทบที่อาจเกิดขึ้นต่อระบบ ข้อมูล การให้บริการ และการดำเนินงานของหน่วยงาน เพื่อนำไปสู่การจัดระดับความเสี่ยง การจัดลำดับความสำคัญ และการกำหนดแนวทางลดความเสี่ยงหรือข้อเสนอแนะในการปรับปรุงมาตรการควบคุมให้เหมาะสมกับบริบทของศูนย์ข้อมูลภาครัฐ ทั้งนี้ ขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สามารถสรุปได้ดังตารางที่ 3-4

ตารางที่ 3-4 ขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอนการประเมิน	รายละเอียดการดำเนินการ	ผลลัพธ์ที่ได้
กำหนดบริบทความเสี่ยง	กำหนดขอบเขตการประเมิน ทรัพย์สินหรือองค์ประกอบของศูนย์ข้อมูล และบริบทของการดำเนินงาน	ขอบเขตและบริบทของความเสี่ยง
ระบุความเสี่ยง	ระบุสถานการณ์ความเสี่ยงที่อาจส่งผลกระทบต่อศูนย์ข้อมูล	รายการสถานการณ์ความเสี่ยง
วิเคราะห์ภัยคุกคามและช่องโหว่	พิจารณาภัยคุกคาม ช่องโหว่ แหล่งที่มาของความเสี่ยง และข้อจำกัดของมาตรการควบคุม	รายการภัยคุกคาม ช่องโหว่ และแหล่งที่มาของความเสี่ยง
พิจารณามาตรการควบคุมที่มีอยู่	ตรวจสอบมาตรการควบคุมด้านเทคนิค ด้านกายภาพ และด้านกระบวนการปฏิบัติงาน	ข้อมูลมาตรการควบคุมปัจจุบัน
วิเคราะห์ความเสี่ยง	ประเมินโอกาสเกิดเหตุการณ์และผลกระทบที่อาจเกิดขึ้น	ระดับโอกาสเกิดและระดับผลกระทบ
ประเมินระดับความเสี่ยง	นำโอกาสเกิดและผลกระทบมาประกอบการกำหนดระดับความเสี่ยง	ระดับความเสี่ยงของแต่ละประเด็น
จัดการความเสี่ยง	กำหนดแนวทางลดความเสี่ยงหรือข้อเสนอแนะในการปรับปรุงมาตรการควบคุม	แนวทางการจัดการความเสี่ยง
ติดตามและทบทวนความเสี่ยง	ติดตามผลการดำเนินงานและทบทวนความเสี่ยงเมื่อมีการเปลี่ยนแปลง	ข้อมูลสำหรับการปรับปรุงมาตรการอย่างต่อเนื่อง

จากขั้นตอนการประเมินความเสี่ยงตามตารางที่ 3-4 ผลลัพธ์ที่ได้จากการประเมินจะถูกนำไปใช้เป็นข้อมูลสำหรับการวิเคราะห์ผลในบทถัดไป โดยผู้วิจัยนำผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้มาเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ ซึ่งเป็นพื้นที่ที่เคยมีการดำเนินการประเมินความเสี่ยงด้านความมั่นคง

ปลอดภัยไซเบอร์มาก่อน เพื่อพิจารณาความเหมือนและความแตกต่างของสถานการณ์ความเสี่ยง ระดับความเสี่ยง กลุ่มประเด็นความเสี่ยง และมาตรการควบคุมที่เกี่ยวข้อง รวมทั้งใช้ประกอบการกำหนดข้อเสนอแนะด้านการบริหารจัดการความเสี่ยงในระดับหน่วยงาน

3.6 เกณฑ์การประเมินและการจัดระดับความเสี่ยง

เกณฑ์การประเมินและการจัดระดับความเสี่ยงในการศึกษานี้ใช้สำหรับกำหนดระดับความรุนแรงของประเด็นความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐานของศูนย์ข้อมูล โดยพิจารณาจาก 2 ปัจจัยหลัก ได้แก่ โอกาสเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นต่อระบบ ข้อมูล การให้บริการ และการดำเนินงานของหน่วยงาน

การกำหนดระดับความเสี่ยงดำเนินการโดยนำค่าระดับผลกระทบและค่าระดับโอกาสเกิดเหตุการณ์มาประกอบกัน เพื่อคำนวณค่าความเสี่ยงของแต่ละสถานการณ์ความเสี่ยง โดยใช้สมการ ดังนี้

$$\text{Risk Level} = \text{Impact} \times \text{Likelihood} \quad (3\text{-}1)$$

โดยที่ Risk Level คือ ระดับความเสี่ยง

Impact คือ ผลกระทบ

Likelihood คือ โอกาสเกิดเหตุการณ์

การประเมินโอกาสเกิดเหตุการณ์กำหนดเป็น 5 ระดับ ตั้งแต่ระดับต่ำมากถึงสูงมาก โดยพิจารณาจากความเป็นไปได้และความถี่ที่เหตุการณ์ความเสี่ยงอาจเกิดขึ้น ดังแสดงในตารางที่ 3-5

ตารางที่ 3-5 เกณฑ์การประเมินโอกาสเกิดเหตุการณ์(Likelihood)

ระดับ	โอกาสเกิด	คำอธิบาย
1	ต่ำมาก	โอกาสเกิดน้อยมาก เกิดขึ้น 1 ครั้งในช่วง 5 ปี หรือมากกว่า 5 ปี หรือไม่เคยเกิดขึ้น
2	ต่ำ	เป็นไปได้น้อยที่จะเกิดขึ้น หรือเกิดขึ้น 1 ครั้งในช่วง 3 ปี
3	ปานกลาง	เป็นไปได้ที่จะเกิดขึ้น หรือเกิดขึ้น 1 ครั้งในรอบ 1 ปี
4	สูง	มีโอกาสเกิดสูง หรือเกิดขึ้นอย่างน้อย 1 ครั้งในรอบ 6 เดือน
5	สูงมาก	คาดว่าจะเกิดขึ้นแน่นอน หรือเกิดขึ้นเฉลี่ยเป็นประจำทุกเดือน

การประเมินผลกระทบกำหนดเป็น 5 ระดับเช่นเดียวกัน โดยพิจารณาจากระดับความเสียหายหรือผลกระทบที่อาจเกิดขึ้นต่อเป้าหมาย ผลการดำเนินงาน ระบบสารสนเทศ ข้อมูลสำคัญ และการให้บริการของหน่วยงาน ดังแสดงในตารางที่ 3-6

ตารางที่ 3-6 เกณฑ์การประเมินผลกระทบ (Impact)

ระดับ	ผลกระทบ	คำอธิบาย
1	ต่ำมาก	มีผลกระทบเพียงเล็กน้อยหรือไม่ส่งผลกระทบต่อเป้าหมายและผลการดำเนินงาน
2	ต่ำ	มีผลกระทบเล็กน้อยต่อเป้าหมาย แต่สามารถจัดการได้ง่าย
3	ปานกลาง	มีผลกระทบพอสมควรต่อเป้าหมาย และอาจต้องใช้ทรัพยากรเพิ่มเติมเพื่อแก้ไขความเสี่ยง
4	สูง	มีผลกระทบอย่างมีนัยสำคัญต่อเป้าหมาย อาจต้องมีการวางแผนหรือปรับปรุงกระบวนการ
5	สูงมาก	มีผลกระทบอย่างรุนแรงที่อาจทำให้ล้มเหลวต่อเป้าหมายหรือต่อองค์กร

เมื่อนำค่าระดับโอกาสเกิดเหตุการณ์และค่าระดับผลกระทบมาคำนวณร่วมกันตามสมการ 3-1 จะได้ค่าคะแนนความเสี่ยงเบื้องต้นสำหรับใช้ประกอบการจัดระดับความเสี่ยง ทั้งนี้ การจัดระดับความเสี่ยงไม่ได้พิจารณาจากค่าคะแนนรวมเพียงอย่างเดียว แต่พิจารณาจากตำแหน่งของค่าผลกระทบและโอกาสเกิดเหตุการณ์ในเมทริกซ์ความเสี่ยง เพื่อให้การจัดระดับความเสี่ยงสอดคล้องกับระดับความรุนแรงและความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น ดังแสดงในตารางที่ 3-7

ตารางที่ 3-7 เมทริกซ์จัดระดับความเสี่ยง

ระดับความเสี่ยง		โอกาสเกิด (Likelihood)				
		1 (ต่ำมาก)	2 (ต่ำ)	3 (ปานกลาง)	4 (สูง)	5 (สูงมาก)
ผลกระทบ (Impact)	5 (สูงมาก)	5 High	10 High	15 High	20 Extreme	25 Extreme
	4 (สูง)	4 Medium	8 Medium	12 High	16 High	20 Extreme

ระดับความเสี่ยง		โอกาสเกิด (Likelihood)				
		1 (ต่ำมาก)	2 (ต่ำ)	3 (ปานกลาง)	4 (สูง)	5 (สูงมาก)
	3 (ปานกลาง)	3 Low	6 Medium	9 High	12 High	15 High
	2 (ต่ำ)	2 Low	4 Medium	6 Medium	8 Medium	10 High
	1 (ต่ำมาก)	1 Low	2 Low	3 Low	4 Medium	5 Medium

ระดับความเสี่ยงที่ได้จากเมทริกซ์ดังกล่าวจะถูกนำไปใช้ประกอบการพิจารณาระดับการยอมรับความเสี่ยง และกำหนดแนวทางในการจัดการความเสี่ยงให้เหมาะสมกับระดับความรุนแรงของแต่ละประเด็น โดยสามารถสรุปเกณฑ์การยอมรับความเสี่ยงได้ดังตารางที่ 3-8

ตารางที่ 3-8 เกณฑ์การยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
สูงมาก (Extreme)	ความเสี่ยงระดับนี้ **ไม่สามารถยอมรับได้** และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ซึ่งสามารถเลือกกลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนได้ จำเป็นต้องดำเนินการทันที โดยแผนจัดการความเสี่ยงควรได้รับอนุมัติและเริ่มต้นดำเนินการภายใน 1 เดือน
เสี่ยงสูง (High)	ความเสี่ยงระดับนี้ **ไม่สามารถยอมรับได้** ซึ่งสามารถเลือกกลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยง โดยแผนจัดการความเสี่ยงควรได้รับอนุมัติและเริ่มต้นดำเนินการภายใน 3–6 เดือน

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
ปานกลาง (Medium)	ความเสี่ยงระดับนี้สามารถ **ยอมรับได้** ได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด แต่ควรมีการติดตามและควบคุมความเสี่ยงอย่างเข้มงวด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม โดยแผนจัดการความเสี่ยงควรได้รับการพิจารณาระยะเวลาดำเนินการตามความเหมาะสม
ต่ำ (Low)	ความเสี่ยงระดับนี้สามารถ **ยอมรับ** โดยไม่ต้องดำเนินการเพิ่มเติม แต่ควรมีการติดตามและควบคุมความเสี่ยงอย่างเข้มงวด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

จากเกณฑ์ดังกล่าว ประเด็นความเสี่ยงที่อยู่ในระดับสูงและสูงมากจะได้รับการพิจารณาเป็นลำดับแรกในการกำหนดแนวทางลดความเสี่ยงหรือแผนจัดการความเสี่ยง เพื่อให้ระดับความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานสามารถยอมรับได้

3.7 การกำหนดตัวชี้วัดผลการประเมิน

การกำหนดตัวชี้วัดผลการประเมิน หรือ Key Performance Indicators (KPI) เป็นขั้นตอนที่ใช้สำหรับติดตามและประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูล ภายหลังจากการวิเคราะห์ช่องว่างและการประเมินความเสี่ยง โดยตัวชี้วัดดังกล่าวมีวัตถุประสงค์เพื่อใช้วัดระดับความสอดคล้องของมาตรการควบคุมกับกรอบ NIST Cybersecurity Framework 2.0 ประเมินระดับความพร้อมของศูนย์ข้อมูล และสนับสนุนการจัดลำดับความสำคัญของประเด็นที่ควรได้รับการปรับปรุง

การกำหนดตัวชี้วัดในการศึกษานี้พิจารณาจากผลการวิเคราะห์ช่องว่าง ผลการประเมินความเสี่ยง ระดับความเสี่ยงที่พบ และแนวทางการจัดการความเสี่ยงที่เหมาะสม โดยมุ่งเน้นตัวชี้วัดที่สามารถสะท้อนสถานะการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างชัดเจน เช่น ระดับความสอดคล้องกับกรอบ NIST CSF 2.0 จำนวนประเด็นความเสี่ยงที่ได้รับการจัดการ ระยะเวลาในการดำเนินการตามแผนจัดการความเสี่ยง และระดับความพร้อมในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดผลการประเมินจะถูกนำไปใช้ประกอบการติดตามความก้าวหน้าในการปรับปรุงมาตรการควบคุม การทบทวนระดับความเสี่ยง และการประเมินผลการดำเนินงานตามข้อเสนอแนะในการลดความเสี่ยง เพื่อให้หน่วยงานสามารถบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบและต่อเนื่อง

ทั้งนี้ ตัวชี้วัดผลการประเมินที่ใช้ในการศึกษาสามารถสรุปได้ดังตารางที่ 3-9

ตารางที่ 3-9 ตัวชี้วัดผลการประเมิน

ตัวชี้วัด	รายละเอียดการประเมิน	การนำผลไปใช้
ระดับความสอดคล้องกับกรอบ NIST CSF 2.0	ประเมินว่ามาตรการควบคุมและกระบวนการดำเนินงานของศูนย์ข้อมูลมีความสอดคล้องกับแนวทางตามกรอบ NIST CSF 2.0 มากน้อยเพียงใด	ใช้ระบุจุดแข็ง ช่องว่าง และประเด็นที่ควรได้รับการปรับปรุง
จำนวนประเด็นความเสี่ยงที่ได้รับการระบุ	พิจารณาจำนวนสถานการณ์ความเสี่ยง ภัยคุกคาม ช่องโหว่ และข้อจำกัดที่พบจากการประเมิน	ใช้ประกอบการจัดลำดับความสำคัญของความเสี่ยง
ระดับความเสี่ยงของแต่ละประเด็น	ประเมินระดับความเสี่ยงจากโอกาสเกิดเหตุการณ์และผลกระทบตามเมทริกซ์ความเสี่ยง	ใช้กำหนดความเร่งด่วนในการจัดการความเสี่ยง

ตัวชี้วัด	รายละเอียดการประเมิน	การนำผลไปใช้
จำนวนประเด็นความเสี่ยงที่ต้องได้รับการจัดการ	พิจารณาประเด็นความเสี่ยงที่อยู่ในระดับสูงและสูงมาก หรือประเด็นที่ไม่สามารถยอมรับได้	ใช้กำหนดแผนจัดการความเสี่ยงและข้อเสนอแนะในการลดความเสี่ยง
ความคืบหน้าในการดำเนินการตามแผนจัดการความเสี่ยง	ติดตามสถานะการดำเนินการตามข้อเสนอแนะหรือแผนจัดการความเสี่ยง	ใช้ประเมินผลการปรับปรุงมาตรการควบคุม
ระดับความพร้อมในการรับมือเหตุการณ์ด้านไซเบอร์	พิจารณาความพร้อมด้านกระบวนการ บุคลากร บทบาทหน้าที่ และแผนรับมือเหตุการณ์	ใช้ประเมินความพร้อมของศูนย์ข้อมูลในการตอบสนองและกู้คืนจากเหตุการณ์ด้านไซเบอร์

จากตัวชี้วัดดังกล่าว ผลการประเมินจะช่วยให้หน่วยงานสามารถติดตามสถานะความพร้อมของศูนย์ข้อมูล เห็นความคืบหน้าในการจัดการความเสี่ยง และนำข้อมูลไปใช้ประกอบการวางแผนปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมกับบริบทของหน่วยงานภาครัฐ

จากวิธีการดำเนินการวิจัยที่กล่าวมาข้างต้น การศึกษานี้ได้กำหนดขั้นตอนการดำเนินงานให้สอดคล้องกับวัตถุประสงค์ของการศึกษา โดยเริ่มจากการศึกษากรอบ NIST Cybersecurity Framework 2.0 การเก็บรวบรวมข้อมูลโครงสร้างพื้นฐานของศูนย์ข้อมูล การวิเคราะห์ช่องว่างการประเมินความเสี่ยง การกำหนดเกณฑ์การจัดระดับความเสี่ยง และการกำหนดตัวชี้วัดผลการประเมิน

กระบวนการดังกล่าวช่วยให้สามารถวิเคราะห์สถานะปัจจุบันของศูนย์ข้อมูล ระบุข้อจำกัดและประเด็นที่ควรได้รับการปรับปรุง ประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และจัดลำดับความสำคัญของความเสี่ยงได้อย่างเป็นระบบ ทั้งนี้ ผลจากการดำเนินการตามวิธีวิจัยดังกล่าวจะถูกนำเสนอในบทถัดไป เพื่อแสดงผลการวิเคราะห์ช่องว่าง ผลการประเมินความเสี่ยงและข้อเสนอแนะในการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลภาครัฐ

บทที่ 4
ผลการดำเนินการวิจัย

จากการดำเนินการวิจัยเรื่อง “การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST” ผู้วิจัยได้นำผลจากรายงานการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์มาวิเคราะห์ร่วมกับกรอบ NIST Cybersecurity Framework 2.0 เพื่อพิจารณาประเด็นความเสี่ยง ระดับความเสี่ยง มาตรการควบคุมที่มีอยู่ และแนวทางในการจัดการความเสี่ยงให้เหมาะสมกับบริบทของหน่วยงานภาครัฐ

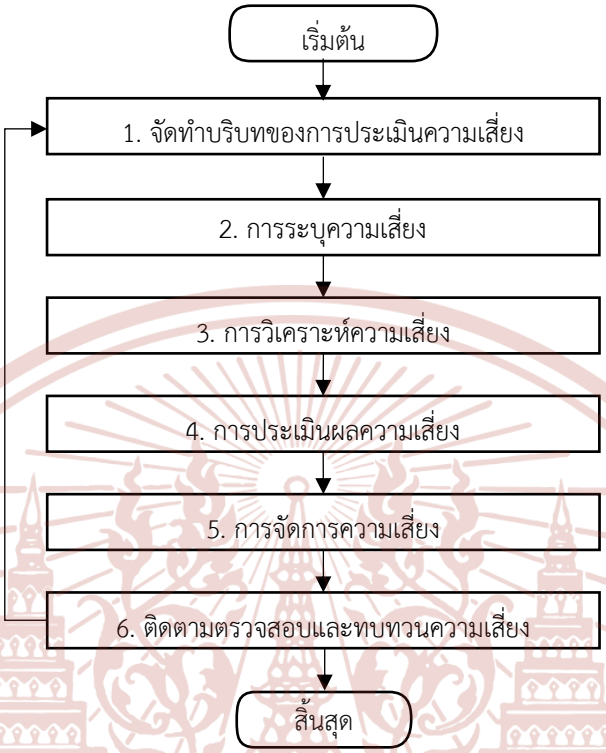
การนำเสนอผลการดำเนินการวิจัยในบทนี้แบ่งออกเป็น 7 ส่วน ได้แก่ ผลการศึกษากระบวนการประเมินความเสี่ยงของหน่วยงาน ผลการประเมินความเสี่ยงของพื้นที่นำร่อง ผลการจัดระดับสถานการณ์ความเสี่ยง ผลการจัดกลุ่มประเด็นความเสี่ยง ผลการวิเคราะห์ความเสี่ยงตามกรอบ NIST Cybersecurity Framework 2.0 แนวทางการจัดการความเสี่ยง และสรุปผลการดำเนินการวิจัย

4.1 ผลการศึกษาข้อมูลพื้นฐานและกระบวนการประเมินความเสี่ยงของหน่วยงาน

จากการศึกษาข้อมูลผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน พบว่า หน่วยงานเคยดำเนินการประเมินความเสี่ยงในพื้นที่นำร่องจำนวน 2 แห่ง ได้แก่ ท่าอากาศยานนครพนม และท่าอากาศยานกระบี่ ซึ่งเป็นพื้นที่ที่เคยมีการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์มาก่อน ผลการประเมินดังกล่าวใช้เป็นข้อมูลพื้นฐานในการพิจารณาลักษณะของความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐาน ระบบสนับสนุน การควบคุมการเข้าถึง และความปลอดภัยทางกายภาพของพื้นที่ที่ติดตั้งอุปกรณ์สารสนเทศ

ในการศึกษาครั้งนี้ ผู้วิจัยได้นำผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษา ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี มาใช้เป็นข้อมูลหลักในการวิเคราะห์ โดยพิจารณารายการความเสี่ยงที่พบ ระดับความเสี่ยงของแต่ละพื้นที่ ความเหมือนและความแตกต่างของประเด็นความเสี่ยง ตลอดจนแนวทางการจัดการความเสี่ยงที่เหมาะสมกับบริบทของหน่วยงานภาครัฐ

ทั้งนี้ การวิเคราะห์ดังกล่าวดำเนินการภายใต้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ซึ่งประกอบด้วยขั้นตอนสำคัญ 6 ขั้นตอน ได้แก่ การจัดทำบริบทของการประเมินความเสี่ยง การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินผลความเสี่ยง การจัดการความเสี่ยง และการติดตามตรวจสอบและทบทวนความเสี่ยง ดังแสดงในภาพที่ 4-1



ภาพที่ 4-1 กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

กระบวนการดังกล่าวสะท้อนให้เห็นว่า การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานไม่ได้พิจารณาเฉพาะผลลัพธ์ของระดับความเสี่ยงเท่านั้น แต่ครอบคลุมตั้งแต่การกำหนดขอบเขตและบริบทของการประเมิน การระบุทรัพย์สิน ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ โอกาสเกิดเหตุการณ์ ผลกระทบที่อาจเกิดขึ้น ตลอดจนการกำหนดแนวทางจัดการความเสี่ยงและการติดตามทบทวนผลการดำเนินงาน ซึ่งเป็นพื้นฐานสำคัญในการนำผลการประเมินของแต่ละพื้นที่มาเปรียบเทียบและวิเคราะห์ร่วมกัน

ตารางที่ 4-1 กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ขั้นตอน	รายละเอียดโดยสรุป
การจัดทำบริบทของการประเมินความเสี่ยง	กำหนดขอบเขต วิธีการ เกณฑ์ความเสี่ยง และผู้เกี่ยวข้องในการประเมิน
การระบุความเสี่ยง	ระบุทรัพย์สิน ภัยคุกคาม ช่องโหว่ มาตรการควบคุมที่มีอยู่ และผลกระทบที่อาจเกิดขึ้น
การวิเคราะห์ความเสี่ยง	วิเคราะห์ระดับโอกาสเกิดเหตุการณ์และระดับผลกระทบของแต่ละสถานการณ์ความเสี่ยง

ขั้นตอน	รายละเอียดโดยสรุป
การประเมินผลความเสี่ยง	นำผลการวิเคราะห์มาจัดระดับความเสี่ยงและจัดลำดับความสำคัญ
การจัดการความเสี่ยง	กำหนดแนวทางลด ยอมรับ โอน หรือหลีกเลี่ยงความเสี่ยง
การติดตามตรวจสอบและทบทวนความเสี่ยง	ติดตามผลการดำเนินงานและทบทวนความเหมาะสมของแผนจัดการความเสี่ยง

จากตารางที่ 4-1 พบว่า กระบวนการประเมินความเสี่ยงของหน่วยงานมีลักษณะเป็นกระบวนการต่อเนื่อง ตั้งแต่การกำหนดบริบทของการประเมิน การระบุและวิเคราะห์ความเสี่ยง การประเมินผลความเสี่ยง การกำหนดแนวทางจัดการความเสี่ยง ตลอดจนการติดตามตรวจสอบและทบทวนความเสี่ยง ซึ่งเป็นพื้นฐานสำคัญในการนำผลการประเมินไปใช้วิเคราะห์ร่วมกับกรอบ NIST Cybersecurity Framework 2.0 และนำไปสู่การเปรียบเทียบผลการประเมินของพื้นที่นำร่องในหัวข้อถัดไป

4.2 ผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้

ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้ พบว่า มีการประเมินความเสี่ยงในพื้นที่ท่าอากาศยานจำนวน 2 แห่ง ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี โดยแต่ละพื้นที่มีการระบุสถานการณ์ความเสี่ยงจำนวน 6 รายการ รวมทั้งสิ้น 12 รายการ

เมื่อพิจารณาระดับความเสี่ยง พบว่า ท่าอากาศยานอุบลราชธานีมีความเสี่ยงระดับปานกลาง จำนวน 2 รายการ และระดับต่ำ จำนวน 4 รายการ ส่วนท่าอากาศยานอุดรธานีมีความเสี่ยงระดับปานกลาง จำนวน 4 รายการ และระดับต่ำ จำนวน 2 รายการ โดยไม่พบความเสี่ยงระดับสูงและระดับสูงมากในพื้นที่ที่ศึกษาในครั้งนี้ ดังแสดงในตารางที่ 4-2

ตารางที่ 4-2 สรุปจำนวนรายการความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้

พื้นที่ประเมิน	จำนวนรายการความเสี่ยงทั้งหมด	ต่ำ (Low)	ปานกลาง (Medium)	สูง (High)	สูงมาก (Extreme)
ท่าอากาศยานอุบลราชธานี	6	4	2	0	0
ท่าอากาศยานอุดรธานี	6	2	4	0	0
รวม	**12**	**6**	**6**	**0**	**0**

จากตารางที่ 4-2 พบว่า ความเสี่ยงที่ได้รับการประเมินในพื้นที่ที่ศึกษาในครั้งนี้อยู่ในระดับต่ำและระดับปานกลางทั้งหมด โดยไม่พบความเสี่ยงในระดับสูงหรือระดับสูงมาก แสดงให้เห็นว่าความเสี่ยงที่พบยังอยู่ในระดับที่สามารถบริหารจัดการได้ อย่างไรก็ตาม ประเด็นความเสี่ยงในระดับปานกลางยังควรได้รับการติดตามและกำหนดมาตรการควบคุมเพิ่มเติม เพื่อป้องกันไม่ให้ระดับความเสี่ยงเพิ่มสูงขึ้นในอนาคต

4.3 ผลการจัดระดับสถานการณ์ความเสี่ยง

เมื่อพิจารณารายละเอียดของสถานการณ์ความเสี่ยงที่พบในพื้นที่ที่ศึกษาในครั้งนี้ พบว่าทั้งสองพื้นที่มีลักษณะของประเด็นความเสี่ยงที่ใกล้เคียงกัน โดยเกี่ยวข้องกับความพร้อมใช้งานของระบบเครือข่าย การเชื่อมต่อ Internet ระบบเครื่องแม่ข่าย CCTV การควบคุมการเข้าถึง ระบบไฟฟ้าและความปลอดภัยทางกายภาพของพื้นที่ที่ติดตั้งอุปกรณ์สารสนเทศ รายละเอียดผลการจัดระดับสถานการณ์ความเสี่ยงของแต่ละพื้นที่แสดงในตารางที่ 4-3 และตารางที่ 4-4

ตารางที่ 4-3 ผลการประเมินความเสี่ยง ณ ท่าอากาศยานอุบลราชธานี

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงานส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	ต่ำ
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	ต่ำ
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้	ต่ำ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ตารางที่ 4-4 ผลการประเมินความเสี่ยง ณ ท่าอากาศยานอุดรธานี

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงานส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	ต่ำ
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	ปานกลาง
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้	ปานกลาง

จากตารางที่ 4-3 และตารางที่ 4-4 พบว่า สถานการณ์ความเสี่ยงที่พบในพื้นที่ที่ศึกษาในครั้งนี้ทั้งสองแห่งมีประเด็นหลักที่สอดคล้องกัน ได้แก่ ความเสี่ยงจากอุปกรณ์เครือข่ายเสียหายพร้อมกัน ความเสี่ยงจากการไม่สามารถใช้งาน Internet ได้ ความเสี่ยงจากอุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย ความเสี่ยงจากการตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย ความเสี่ยงจากเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย และความเสี่ยงจากเหตุขัดข้องด้านระบบไฟฟ้า

เมื่อเปรียบเทียบระดับความเสี่ยงของทั้งสองพื้นที่ พบว่าท่าอากาศยานอุดรธานีมีจำนวนประเด็นความเสี่ยงระดับปานกลางมากกว่าท่าอากาศยานอุบลราชธานี โดยเฉพาะประเด็นด้านความปลอดภัยทางกายภาพและระบบไฟฟ้า ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการให้ความสำคัญกับมาตรการป้องกันเหตุขัดข้องและการเตรียมความพร้อมด้านความต่อเนื่องของบริการในพื้นที่ดังกล่าว

ทั้งนี้ เพื่อให้เห็นภาพรวมของระดับความเสี่ยงในบริบทที่กว้างขึ้น ผู้วิจัยจึงนำผลการประเมินของพื้นที่ที่ศึกษาในครั้งนี้มาเปรียบเทียบกับผลการประเมินเดิมของท่าอากาศยานนครพนม และท่าอากาศยานกระบี่ ดังแสดงในตารางที่ 4-5

ตารางที่ 4-5 การเปรียบเทียบภาพรวมผลการประเมินความเสี่ยงของพื้นที่เดิมและพื้นที่ที่ศึกษาในครั้งนี้

พื้นที่ประเมิน	ประเภทข้อมูล	จำนวนรายการความเสี่ยงทั้งหมด	ระดับความเสี่ยงที่พบ	ข้อสังเกต
ท่าอากาศยานนครพนม	ผลการประเมินเดิม	6 รายการ	(High) 3, (Medium) 2, (Low) 1	พบความเสี่ยงระดับสูงหลายรายการ สะท้อนว่ามีประเด็นที่ต้องให้ความสำคัญด้านระบบสนับสนุนความปลอดภัยทางกายภาพ และความต่อเนื่องของบริการ
ท่าอากาศยานกระบี่	ผลการประเมินเดิม	6 รายการ	(High) 1, (Medium) 2, (Low) 3	พบความเสี่ยงระดับสูง 1 รายการ ระดับปานกลาง 2 รายการ และระดับต่ำ 3 รายการ โดยประเด็นระดับสูงเกี่ยวข้องกับเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย
ท่าอากาศยานอุบลราชธานี	ผลการศึกษาครั้งนี้	6 รายการ	(Medium) 2, (Low) 4	ไม่พบความเสี่ยงระดับสูงหรือสูงมาก โดยประเด็นระดับปานกลางควรได้รับการติดตามและควบคุมเพิ่มเติม
ท่าอากาศยานอุดรธานี	ผลการศึกษาครั้งนี้	6 รายการ	(Medium) 4, (Low) 2	มีจำนวนความเสี่ยงระดับปานกลางมากกว่าอุบลราชธานี จึงควรให้ความสำคัญกับการติดตามและจัดการประเด็นที่เกี่ยวข้องกับระบบสนับสนุนและความต่อเนื่องของบริการ

จากตารางที่ 4-5 พบว่า พื้นที่ทั้ง 4 แห่งมีจำนวนรายการความเสี่ยงที่ได้รับการประเมินเท่ากัน คือ พื้นที่ละ 6 รายการ อย่างไรก็ตาม ระดับความเสี่ยงที่พบมีความแตกต่างกัน โดยผลการประเมินเดิมของท่าอากาศยานครพนม พบความเสี่ยงระดับสูง จำนวน 3 รายการ ระดับปานกลาง 2 รายการ และระดับต่ำ 1 รายการ

ส่วนท่าอากาศยานกระบี่พบความเสี่ยงระดับสูง จำนวน 1 รายการ ระดับปานกลาง 2 รายการ และระดับต่ำ 3 รายการ ขณะที่ผลการศึกษาครั้งนี้ของท่าอากาศยานอุบลราชธานีและท่าอากาศยานอุดรธานีไม่พบความเสี่ยงระดับสูงหรือสูงมาก แต่พบความเสี่ยงระดับปานกลางและระดับต่ำเท่านั้น

เมื่อพิจารณาลักษณะของประเด็นความเสี่ยง พบว่าพื้นที่ทั้งผลการประเมินเดิมและผลการศึกษาครั้งนี้มีประเด็นความเสี่ยงที่คล้ายคลึงกันในหลายด้าน ได้แก่ ความเสี่ยงจากอุปกรณ์เครือข่ายเสียหาย การไม่สามารถใช้งาน Internet ได้ ความเสียหายของเครื่องแม่ข่าย CCTV การตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย เหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย และเหตุขัดข้องด้านระบบไฟฟ้า อย่างไรก็ตาม ระดับความเสี่ยงของแต่ละพื้นที่แตกต่างกันตามบริบทของพื้นที่ สภาพแวดล้อม ระบบสนับสนุน มาตรการควบคุมที่มีอยู่ และความพร้อมในการตอบสนองต่อเหตุการณ์

ผลการเปรียบเทียบดังกล่าวสะท้อนให้เห็นว่า หน่วยงานควรกำหนดแนวทางบริหารจัดการความเสี่ยงใน 2 ระดับ ได้แก่ มาตรการกลางสำหรับประเด็นความเสี่ยงที่พบร่วมกันในหลายพื้นที่ และมาตรการเฉพาะพื้นที่สำหรับประเด็นที่มีระดับความเสี่ยงสูงหรือมีความสำคัญต่อความต่อเนื่องของบริการ เพื่อให้การบริหารจัดการความเสี่ยงสามารถตอบสนองต่อบริบทของแต่ละสนามบินได้อย่างเหมาะสม ทั้งนี้ รายละเอียดผลการประเมินความเสี่ยงของแต่ละพื้นที่ แสดงไว้ในภาคผนวก ก

4.4 ผลการจัดกลุ่มประเด็นความเสี่ยง

จากผลการจัดระดับสถานการณ์ความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้ และผลการเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ พบว่าประเด็นความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐานศูนย์ข้อมูลและระบบสนับสนุนสามารถจัดกลุ่มตามลักษณะของความเสี่ยงได้เป็น 4 กลุ่มหลัก ได้แก่ ความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่าย ความเสี่ยงด้านระบบสนับสนุนและความต่อเนื่องของบริการ ความเสี่ยงด้านความปลอดภัยทางกายภาพ และความเสี่ยงด้านการควบคุมการเข้าถึง

การจัดกลุ่มประเด็นความเสี่ยงดังกล่าวช่วยให้สามารถมองเห็นลักษณะของความเสี่ยงที่เกี่ยวข้องกับศูนย์ข้อมูลได้ชัดเจนมากขึ้น โดยไม่ได้พิจารณาเฉพาะสถานการณ์ความเสี่ยงแต่ละรายการแยกจากกันเท่านั้น แต่ยังช่วยให้สามารถวิเคราะห์ความสัมพันธ์ระหว่างความเสี่ยง สาเหตุ ผลกระทบ และมาตรการควบคุมที่ควรกำหนดให้เหมาะสมกับแต่ละกลุ่มประเด็น ดังแสดงในตารางที่ 4-6

ตารางที่ 4-6 การจัดกลุ่มประเด็นความเสี่ยงที่พบจากการประเมิน

กลุ่มประเด็นความเสี่ยง	ตัวอย่างสถานการณ์ความเสี่ยง	ความเกี่ยวข้องกับศูนย์ข้อมูล
ด้านโครงสร้างพื้นฐานระบบเครือข่าย	อุปกรณ์เครือข่ายเสียหายพร้อมกัน, ไม่สามารถใช้งาน Internet ได้	ส่งผลต่อการเชื่อมต่อระบบ การเข้าถึงระบบสารสนเทศ และความพร้อมใช้งานของบริการ
ด้านระบบสนับสนุนและความต่อเนื่องของบริการ	ไฟฟ้าดับ, ระบบไฟฟ้าใช้งานไม่ได้	ส่งผลต่อความพร้อมใช้งานของระบบ อุปกรณ์สารสนเทศ และความต่อเนื่องในการปฏิบัติงาน
ด้านความปลอดภัยทางกายภาพ	ไฟไหม้ภายในห้อง Server CCTV หรือห้องเครือข่าย	ส่งผลต่อพื้นที่ติดตั้งอุปกรณ์สารสนเทศ ระบบสนับสนุน และความปลอดภัยของทรัพย์สินสารสนเทศ
ด้านการควบคุมการเข้าถึง	การตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย	เพิ่มโอกาสการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต และอาจส่งผลให้ข้อมูลรั่วไหล

จากตารางที่ 4-6 พบว่า ประเด็นความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐานศูนย์ข้อมูลสามารถจัดกลุ่มได้เป็น 4 กลุ่มหลัก โดยกลุ่มความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่ายและกลุ่มความเสี่ยงด้านระบบสนับสนุนและความต่อเนื่องของบริการ เป็นกลุ่มที่ส่งผลโดยตรงต่อความพร้อมใช้งานของระบบและการให้บริการของหน่วยงาน ขณะที่กลุ่มความเสี่ยงด้านความปลอดภัยทางกายภาพและการควบคุมการเข้าถึง มีความเกี่ยวข้องกับการป้องกันความเสียหายต่ออุปกรณ์ สถานที่ปฏิบัติงาน และข้อมูลสำคัญของหน่วยงาน

ผลการจัดกลุ่มดังกล่าวช่วยให้หน่วยงานสามารถกำหนดแนวทางจัดการความเสี่ยงได้เป็นระบบมากขึ้น โดยสามารถแยกมาตรการควบคุมตามลักษณะของความเสี่ยง เช่น มาตรการด้านระบบเครือข่าย มาตรการด้านระบบไฟฟ้าและระบบสนับสนุน มาตรการด้านความปลอดภัยทางกายภาพ และมาตรการด้านการควบคุมสิทธิ์การเข้าถึง ซึ่งจะนำไปใช้ประกอบการวิเคราะห์ความสอดคล้องกับกรอบ NIST Cybersecurity Framework 2.0 ในหัวข้อถัดไป

4.5 ผลการวิเคราะห์ความเสี่ยงตามกรอบ NIST Cybersecurity Framework 2.0

จากผลการจัดระดับสถานการณ์ความเสี่ยงและการจัดกลุ่มประเด็นความเสี่ยงในหัวข้อก่อนหน้า ผู้วิจัยนำสถานการณ์ความเสี่ยงที่พบมาวิเคราะห์เชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 ซึ่งประกอบด้วยหน้าที่หลัก 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover เพื่อพิจารณาว่าแต่ละสถานการณ์เกี่ยวข้องกับหน้าที่หลักด้านใดของกรอบ NIST และสามารถนำไปใช้ประกอบการกำหนดแนวทางจัดการประเด็นความเสี่ยงได้อย่างเหมาะสม ดังแสดงในตารางที่ 4-7

ตารางที่ 4-7 การเชื่อมโยงสถานการณ์ความเสี่ยงกับ NIST Cybersecurity Framework 2.0

สถานการณ์ความเสี่ยง	หน้าที่หลักของ NIST CSF 2.0	เหตุผลในการเชื่อมโยง
อุปกรณ์เครือข่ายเสียหายพร้อมกัน	Identify, Protect, Respond, Recover	เกี่ยวข้องกับการระบุทรัพย์สินสำคัญ การป้องกันความขัดข้องของระบบเครือข่าย และการกู้คืนบริการเมื่อเกิดเหตุ
ไม่สามารถใช้งาน Internet ได้	Protect, Respond, Recover	เกี่ยวข้องกับการป้องกันความต่อเนื่องของบริการ การตอบสนองเมื่อการเชื่อมต่อขัดข้อง และการกู้คืนการเชื่อมต่อให้กลับมาใช้งานได้
เครื่องแม่ข่าย CCTV เสียหาย	Identify, Protect, Respond, Recover	เกี่ยวข้องกับการระบุระบบสนับสนุนที่สำคัญ การป้องกันความเสียหายของอุปกรณ์ และการจัดเตรียมแนวทางสำรองหรือกู้คืนระบบ
รหัสผ่านคาดเดาได้ง่าย	Govern, Protect, Detect	เกี่ยวข้องกับการกำหนดนโยบายควบคุมสิทธิ์ การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการตรวจจับพฤติกรรมการใช้งานที่ผิดปกติ
ไฟไหม้ในห้อง Server CCTV หรือห้องเครือข่าย	Protect, Respond, Recover	เกี่ยวข้องกับมาตรการป้องกันทางกายภาพ การตอบสนองต่อเหตุฉุกเฉิน และการกู้คืนระบบหรืออุปกรณ์ที่ได้รับผลกระทบ
ไฟฟ้าดับหรือระบบไฟฟ้าใช้งานไม่ได้	Protect, Respond, Recover	เกี่ยวข้องกับระบบสนับสนุนความต่อเนื่องของบริการ การตอบสนองต่อเหตุขัดข้อง และการกู้คืนการดำเนินงานของระบบ

จากตารางที่ 4-7 พบว่า สถานการณ์ความเสี่ยงส่วนใหญ่มีความเชื่อมโยงกับหน้าที่ด้าน Protect, Respond และ Recover เป็นหลัก เนื่องจากความเสี่ยงที่พบเกี่ยวข้องกับความพร้อมใช้งานของระบบ การป้องกันเหตุขัดข้อง การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบเมื่อเกิดปัญหา นอกจากนี้ สถานการณ์ความเสี่ยงด้านการตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย ยังสะท้อนถึงความสำคัญของหน้าที่ด้าน Govern และ Detect ซึ่งเกี่ยวข้องกับการกำหนดนโยบายควบคุมการเข้าถึงและการตรวจจับพฤติกรรมผิดปกติของผู้ใช้งาน

ดังนั้น การนำกรอบ NIST Cybersecurity Framework 2.0 มาใช้วิเคราะห์ผลการประเมินความเสี่ยง จึงช่วยให้สามารถมองเห็นความสัมพันธ์ระหว่างสถานการณ์ความเสี่ยงกับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ได้ชัดเจนมากขึ้น และสามารถนำไปใช้ประกอบการกำหนดแนวทางจัดการความเสี่ยงให้เหมาะสมกับบริบทของศูนย์ข้อมูลภาครัฐ

4.6 แนวทางการจัดการความเสี่ยง

จากผลการจัดระดับสถานการณ์ความเสี่ยง การจัดกลุ่มประเด็นความเสี่ยง และการวิเคราะห์ความเชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 ผู้วิจัยได้นำผลการวิเคราะห์ดังกล่าวมาใช้กำหนดแนวทางการจัดการความเสี่ยง เพื่อให้หน่วยงานสามารถลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และสามารถกำหนดมาตรการควบคุมที่เหมาะสมกับลักษณะของความเสี่ยงที่พบในแต่ละกลุ่มประเด็น ดังแสดงในตารางที่ 4-8

ตารางที่ 4-8 แนวทางการจัดการความเสี่ยงตามสถานการณ์ความเสี่ยง

สถานการณ์ความเสี่ยง	แนวทางการจัดการความเสี่ยง
อุปกรณ์เครือข่ายเสียหายพร้อมกัน	จัดทำแผนบำรุงรักษาและตรวจสอบสถานะอุปกรณ์เครือข่ายอย่างสม่ำเสมอ จัดเตรียมอุปกรณ์สำรองหรืออะไหล่ที่จำเป็น และกำหนดแนวทางกู้คืนระบบเครือข่ายเมื่อเกิดเหตุขัดข้อง
ไม่สามารถใช้งาน Internet ได้	จัดหา Link Internet สำรอง กำหนดแนวทางการสลับใช้งานเมื่อ Link หลักขัดข้อง และติดตามสถานะการเชื่อมต่ออย่างต่อเนื่อง
เครื่องแม่ข่าย CCTV เสียหาย	จัดเตรียมอะไหล่หรืออุปกรณ์สำรองสำหรับระบบ CCTV Server กำหนดแนวทางสำรองข้อมูล และจัดทำขั้นตอนการกู้คืนระบบให้สามารถกลับมาใช้งานได้

สถานการณ์ความเสี่ยง	แนวทางการจัดการความเสี่ยง
รหัสผ่านคาดเดาได้ง่าย	กำหนดนโยบายรหัสผ่านที่เหมาะสม เช่น ความยาวและความซับซ้อนของรหัสผ่าน การเปลี่ยนรหัสผ่านตามรอบระยะเวลา และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างสม่ำเสมอ
ไฟไหม้ในห้อง Server CCTV หรือห้องเครือข่าย	ตรวจสอบและบำรุงรักษาระบบป้องกันอัคคีภัย ระบบแจ้งเตือน และอุปกรณ์ดับเพลิงในพื้นที่สำคัญ รวมถึงจัดทำแนวทางรับมือเหตุฉุกเฉินและแผนฟื้นฟูระบบหลังเกิดเหตุ
ไฟฟ้าดับหรือระบบไฟฟ้าใช้งานไม่ได้	ตรวจสอบและบำรุงรักษาระบบไฟฟ้า ระบบ UPS และอุปกรณ์สำรองไฟอย่างสม่ำเสมอ พร้อมกำหนดแผนรองรับกรณีไฟฟ้าขัดข้องเพื่อให้ระบบสำคัญสามารถให้บริการได้อย่างต่อเนื่อง

จากตารางที่ 4-8 พบว่า แนวทางการจัดการความเสี่ยงที่เหมาะสมกับสถานการณ์ความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้ ควรมุ่งเน้นการป้องกันเหตุขัดข้อง การเตรียมความพร้อมของอุปกรณ์และระบบสนับสนุน การกำหนดมาตรการควบคุมการเข้าถึง และการจัดทำแนวทางตอบสนองและกู้คืนระบบเมื่อเกิดเหตุการณ์ โดยแนวทางดังกล่าวสอดคล้องกับหน้าที่หลักของ NIST Cybersecurity Framework 2.0 โดยเฉพาะด้าน Protect, Respond และ Recover

การนำแนวทางการจัดการความเสี่ยงไปใช้ควรกำหนดผู้รับผิดชอบ ระยะเวลาดำเนินการ และวิธีติดตามผลอย่างชัดเจน เพื่อให้สามารถประเมินได้ว่ามาตรการที่ดำเนินการสามารถลดความเสี่ยงคงเหลือให้อยู่ในระดับที่หน่วยงานยอมรับได้หรือไม่ และสามารถใช้เป็นข้อมูลประกอบการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลภาครัฐได้อย่างต่อเนื่อง

ในระดับหน่วยงานส่วนกลางหรือระดับกรม ควรกำหนดแนวทางบริหารจัดการความเสี่ยงด้านโครงสร้างพื้นฐานศูนย์ข้อมูลและระบบสนับสนุนในลักษณะมาตรฐานกลาง เพื่อให้พื้นที่ในสังกัดสามารถนำไปใช้เป็นแนวทางเดียวกัน โดยเฉพาะประเด็นความเสี่ยงที่พบร่วมกันในหลายพื้นที่ เช่น ความพร้อมใช้งานของระบบเครือข่าย การเชื่อมต่อ Internet ระบบไฟฟ้า ระบบสำรองไฟ ความปลอดภัยทางกายภาพ การควบคุมการเข้าถึง และการกู้คืนระบบเมื่อเกิดเหตุการณ์

นอกจากนี้ หน่วยงานควรกำหนดมาตรการบริหารจัดการความเสี่ยงเป็น 2 ระดับ ได้แก่ มาตรการกลางที่ใช้กับทุกพื้นที่ในสังกัด และมาตรการเฉพาะพื้นที่สำหรับประเด็นที่มีระดับความเสี่ยง

สูงหรือมีลักษณะเฉพาะตามบริบทของแต่ละสนามบิน เพื่อให้การบริหารจัดการความเสี่ยงมีความเหมาะสมกับสภาพแวดล้อม ทรัพยากร และระดับความพร้อมของแต่ละพื้นที่

4.7 สรุปผลการวิเคราะห์ความเสี่ยง

จากผลการวิเคราะห์ในบทนี้ พบว่า การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้ ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี มีรายการความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐานของศูนย์ข้อมูลและระบบสนับสนุนจำนวนรวม 12 รายการ โดยระดับความเสี่ยงที่พบอยู่ในระดับต่ำและระดับปานกลางทั้งหมด และไม่พบความเสี่ยงในระดับสูงหรือสูงมาก

เมื่อเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ พบว่า พื้นที่ทั้งผลการประเมินเดิมและผลการศึกษาครั้งนี้มีลักษณะของสถานการณ์ความเสี่ยงที่คล้ายคลึงกันในหลายด้าน ได้แก่ ความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่าย ความเสี่ยงด้านระบบสนับสนุนและความต่อเนื่องของบริการ ความเสี่ยงด้านความปลอดภัยทางกายภาพ และความเสี่ยงด้านการควบคุมการเข้าถึง อย่างไรก็ตาม ระดับความเสี่ยงของแต่ละพื้นที่มีความแตกต่างกันตามบริบทของพื้นที่ สภาพแวดล้อม ระบบสนับสนุน มาตรการควบคุมที่มีอยู่ และความพร้อมในการตอบสนองต่อเหตุการณ์

สำหรับการเชื่อมโยงสถานการณ์ความเสี่ยงที่พบกับกรอบ NIST Cybersecurity Framework 2.0 พบว่า ความเสี่ยงส่วนใหญ่มีความเกี่ยวข้องกับหน้าที่หลักด้าน Protect, Respond และ Recover เป็นสำคัญ เนื่องจากเกี่ยวข้องกับการป้องกันเหตุขัดข้อง การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบหรือบริการให้กลับมาใช้งานได้ตามปกติ นอกจากนี้ ความเสี่ยงด้านการควบคุมการเข้าถึงยังมีความเกี่ยวข้องกับหน้าที่ด้าน Govern และ Detect ซึ่งเกี่ยวข้องกับการกำหนดนโยบายควบคุมการเข้าถึงและการตรวจจับพฤติกรรมผิดปกติของผู้ใช้งาน

ผลการวิเคราะห์ดังกล่าวแสดงให้เห็นว่า การจัดการความเสี่ยงของหน่วยงานควรดำเนินการทั้งในระดับมาตรการกลางที่ใช้กับทุกพื้นที่ในสังกัด และมาตรการเฉพาะพื้นที่ที่สอดคล้องกับบริบทของแต่ละสนามบิน เพื่อให้สามารถลดความเสี่ยงด้านโครงสร้างพื้นฐานศูนย์ข้อมูลและระบบสนับสนุนได้อย่างเหมาะสม และสามารถนำผลการวิเคราะห์ไปใช้ประกอบการสรุปผล อภิปรายผล และจัดทำข้อเสนอแนะในบทถัดไป

บทที่ 5

สรุป อภิปรายผล และข้อเสนอแนะ

การค้นคว้าอิสระเรื่อง “การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST” มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลของหน่วยงานภาครัฐ โดยอ้างอิงกรอบ NIST Cybersecurity Framework 2.0 เป็นแนวทางหลักในการศึกษา

การดำเนินการวิจัยประกอบด้วยการศึกษากระบวนการประเมินความเสี่ยงของหน่วยงาน การรวบรวมข้อมูลจากรายงานผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้ และการเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของพื้นที่ที่เคยมีการประเมินมาก่อน การจัดระดับสถานการณ์ความเสี่ยง การจัดกลุ่มประเด็นความเสี่ยง การเชื่อมโยงประเด็นความเสี่ยงกับหน้าที่หลักของ NIST Cybersecurity Framework 2.0 และการสรุปแนวทางการจัดการความเสี่ยงที่เหมาะสมกับบริบทของศูนย์ข้อมูลภาครัฐ

บทนี้นำเสนอการอภิปรายผล สรุปผลการวิจัย และข้อเสนอแนะจากการศึกษาโดยมีรายละเอียดดังต่อไปนี้

5.1 อภิปรายผล

จากผลการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้ พบว่าประเด็นความเสี่ยงที่เกี่ยวข้องกับโครงสร้างพื้นฐานของศูนย์ข้อมูลอยู่ในระดับต่ำถึงระดับปานกลาง โดยไม่พบความเสี่ยงระดับสูงหรือสูงมาก อย่างไรก็ตาม ประเด็นความเสี่ยงในระดับปานกลางยังเป็นประเด็นที่ควรได้รับการติดตามและบริหารจัดการอย่างต่อเนื่อง เนื่องจากอาจส่งผลกระทบต่อความพร้อมใช้งานของระบบ การให้บริการ และการดำเนินงานของหน่วยงานหากไม่มีมาตรการควบคุมหรือแนวทางจัดการความเสี่ยงที่เหมาะสม

เมื่อเปรียบเทียบผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ พบว่า พื้นที่ที่ศึกษาในครั้งนี้มีลักษณะของสถานการณ์ความเสี่ยงที่คล้ายคลึงกับผลการประเมินเดิมในหลายด้าน ได้แก่ ความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่าย ความเสี่ยงด้านระบบสนับสนุนและความต่อเนื่องของบริการ ความเสี่ยงด้านความปลอดภัยทางกายภาพ และความเสี่ยงด้านการควบคุมการเข้าถึง อย่างไรก็ตาม ระดับความเสี่ยงของแต่ละดื้นที่มีความแตกต่างกัน โดยผลการประเมินเดิมบางพื้นที่พบความเสี่ยงระดับสูง ขณะที่พื้นที่ที่ศึกษาในครั้งนี้ไม่พบความเสี่ยงระดับสูง

สะท้อนให้เห็นว่าการบริหารจัดการความเสี่ยงควรพิจารณรทั้งประเด็นความเสี่ยงที่พบร่วมกันและบริบทเฉพาะของแต่ละพื้นที่

เมื่อพิจารณาประเด็นความเสี่ยงที่พบ จะเห็นได้ว่าความเสี่ยงไม่ได้จำกัดอยู่เฉพาะด้านเทคนิคของระบบสารสนเทศเท่านั้น แต่ยังครอบคลุมถึงระบบสนับสนุนทางกายภาพ กระบวนการควบคุมการเข้าถึง และความต่อเนื่องของบริการ เช่น ความเสี่ยงจากอุปกรณ์เครือข่ายเสียหายพร้อมกัน การไม่สามารถใช้งาน Internet ได้ ความเสียหายของเครื่องแม่ข่าย CCTV การตั้งรหัสผ่านที่สามารถคาดเดาได้ง่าย เหตุไฟไหม้ภายในห้อง Server CCTV หรือห้องเครือข่าย และเหตุขัดข้องด้านระบบไฟฟ้า ประเด็นดังกล่าวสะท้อนให้เห็นว่าการรักษาความมั่นคงปลอดภัยของศูนย์ข้อมูลภาครัฐจำเป็นต้องพิจารณาทั้งด้านเทคโนโลยี กระบวนการปฏิบัติงาน บุคลากร และมาตรการควบคุมทางกายภาพควบคู่กัน

เมื่อนำสถานการณ์ความเสี่ยงที่พบมาเชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 พบว่าความเสี่ยงส่วนใหญ่มีความเกี่ยวข้องกับหน้าที่หลักด้าน Protect, Respond และ Recover เป็นสำคัญ เนื่องจากความเสี่ยงที่พบส่วนใหญ่เกี่ยวข้องกับการป้องกันเหตุขัดข้อง การตอบสนองเมื่อเกิดเหตุการณ์ และการกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามปกติ ขณะเดียวกันประเด็นด้านการตั้งรหัสผ่านที่สามารถคาดเดาได้ง่ายยังสะท้อนถึงความสำคัญของหน้าที่ด้าน Govern และ Detect ซึ่งเกี่ยวข้องกับการกำหนดนโยบายควบคุมการเข้าถึงและการตรวจจับพฤติกรรมผิดปกติของผู้ใช้งาน

ผลการศึกษาดังกล่าวแสดงให้เห็นว่า การปรับปรุงโครงสร้างพื้นฐานของศูนย์ข้อมูลภาครัฐให้สอดคล้องกับกรอบ NIST Cybersecurity Framework 2.0 ไม่ควรมุ่งเน้นเฉพาะการจัดหาอุปกรณ์หรือเทคโนโลยีเพิ่มเติมเท่านั้น แต่ควรให้ความสำคัญกับการกำหนดนโยบาย การจัดทำกระบวนการปฏิบัติงาน การติดตามตรวจสอบ การเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ และการกู้คืนระบบอย่างเป็นระบบ เพื่อให้หน่วยงานสามารถบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างต่อเนื่องและเหมาะสมกับบริบทของหน่วยงานภาครัฐ

5.2 สรุปผลการวิจัย

จากการศึกษากระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน พบว่า หน่วยงานมีการกำหนดกระบวนการประเมินความเสี่ยงไว้อย่างเป็นระบบ โดยประกอบด้วยขั้นตอนสำคัญ ได้แก่ การจัดทำบริบทของการประเมินความเสี่ยง การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินผลความเสี่ยง การจัดการความเสี่ยง และการติดตามตรวจสอบและทบทวนความเสี่ยง ซึ่งสามารถนำมาใช้เป็นกรอบในการวิเคราะห์ความเสี่ยงด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลได้อย่างเหมาะสม

ผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้ จำนวน 2 แห่ง ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี พบว่ามีรายการความเสี่ยงรวมทั้งสิ้น 12 รายการ โดยท่าอากาศยานอุบลราชธานีมีรายการความเสี่ยงจำนวน 6 รายการ แบ่งเป็นความเสี่ยงระดับปานกลาง 2 รายการ และระดับต่ำ 4 รายการ ส่วนท่าอากาศยานอุดรธานีมีรายการความเสี่ยงจำนวน 6 รายการ แบ่งเป็นความเสี่ยงระดับปานกลาง 4 รายการ และระดับต่ำ 2 รายการ โดยไม่พบความเสี่ยงระดับสูงและสูงมากในพื้นที่ที่ศึกษาในครั้งนี้

เมื่อนำผลการประเมินความเสี่ยงของพื้นที่ที่ศึกษาในครั้งนี้มาเปรียบเทียบกับผลการประเมินความเสี่ยงเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่ พบว่า พื้นที่ทั้ง 4 แห่งมีจำนวนรายการความเสี่ยงที่ได้รับการประเมินเท่ากัน คือ พื้นที่ละ 6 รายการ แต่ระดับความเสี่ยงที่พบมีความแตกต่างกัน โดยผลการประเมินเดิมของท่าอากาศยานนครพนมและท่าอากาศยานกระบี่พบความเสี่ยงระดับสูงบางรายการ ขณะที่ท่าอากาศยานอุบลราชธานีและท่าอากาศยานอุดรธานีไม่พบความเสี่ยงระดับสูงหรือสูงมาก ทั้งนี้ สถานการณ์ความเสี่ยงที่พบมีลักษณะคล้ายคลึงกันในหลายด้าน โดยเฉพาะความเสี่ยงที่เกี่ยวข้องกับระบบเครือข่าย การเชื่อมต่อ Internet ระบบ CCTV การควบคุมการเข้าถึง ความปลอดภัยทางกายภาพ และระบบไฟฟ้า

เมื่อพิจารณาสถานการณ์ความเสี่ยงที่พบ สามารถจัดกลุ่มประเด็นความเสี่ยงได้เป็น 4 กลุ่มหลัก ได้แก่ ความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่าย ความเสี่ยงด้านระบบสนับสนุนและความต่อเนื่องของบริการ ความเสี่ยงด้านความปลอดภัยทางกายภาพ และความเสี่ยงด้านการควบคุมการเข้าถึง ซึ่งประเด็นเหล่านี้ล้วนมีความเกี่ยวข้องกับความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์ข้อมูลภาครัฐ

เมื่อนำสถานการณ์ความเสี่ยงดังกล่าวมาเชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 พบว่าความเสี่ยงส่วนใหญ่มีความเกี่ยวข้องกับหน้าที่หลักด้าน Protect, Respond และ Recover เป็นสำคัญ เนื่องจากประเด็นความเสี่ยงที่พบส่วนใหญ่เกี่ยวข้องกับการป้องกันเหตุขัดข้อง การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบให้กลับมาใช้งานได้ตามปกติ นอกจากนี้ ประเด็นด้านการตั้งรหัสผ่านที่สามารถคาดเดาได้ง่ายยังมีความเกี่ยวข้องกับหน้าที่ด้าน Govern และ Detect ซึ่งสะท้อนถึงความสำคัญของการกำหนดนโยบายควบคุมการเข้าถึงและการตรวจจับพฤติกรรมผิดปกติของผู้ใช้งาน

จากผลการศึกษา สามารถสรุปได้ว่า แม้ความเสี่ยงที่พบในพื้นที่ที่ศึกษาในครั้งนี้จะอยู่ในระดับต่ำถึงปานกลาง และยังอยู่ในระดับที่สามารถบริหารจัดการได้ แต่ยังมีความจำเป็นต้องกำหนดแนวทางในการลดความเสี่ยงและปรับปรุงมาตรการควบคุมที่เกี่ยวข้องกับระบบเครือข่าย ระบบไฟฟ้า ระบบสนับสนุนความต่อเนื่องของบริการ การควบคุมการเข้าถึง และการเตรียมความพร้อมในการตอบสนองและกู้คืนระบบ นอกจากนี้ ผลการเปรียบเทียบกับพื้นที่ที่เคยมีการประเมินมาก่อนยัง

สะท้อนให้เห็นว่า หน่วยงานควรกำหนดมาตรการบริหารจัดการความเสี่ยงทั้งในระดับมาตรฐานกลางของกรม และมาตรการเฉพาะพื้นที่ที่เหมาะสมกับบริบทของแต่ละสนามบิน เพื่อให้ศูนย์ข้อมูลของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่อง

5.3 ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยได้จัดทำข้อเสนอแนะเพื่อใช้เป็นแนวทางในการลดความเสี่ยงและยกระดับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลภาครัฐ โดยแบ่งข้อเสนอแนะออกเป็น 2 ส่วน ได้แก่ ข้อเสนอแนะจากผลการวิจัย และข้อเสนอแนะสำหรับการศึกษาครั้งต่อไป

5.3.1 ข้อเสนอแนะจากผลการวิจัย

จากผลการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้ พบว่าศูนย์ข้อมูลของหน่วยงานภาครัฐควรให้ความสำคัญกับการปรับปรุงมาตรการควบคุมที่เกี่ยวข้องกับระบบเครือข่าย ระบบสนับสนุนความต่อเนื่องของบริการ การควบคุมการเข้าถึง ความปลอดภัยทางกายภาพ และการเตรียมความพร้อมในการตอบสนองและกู้คืนระบบ โดยมีข้อเสนอแนะดังนี้

1. หน่วยงานควรจัดทำและปรับปรุงข้อมูลทรัพย์สินสารสนเทศที่เกี่ยวข้องกับศูนย์ข้อมูลให้มีความครบถ้วนและเป็นปัจจุบัน เช่น อุปกรณ์เครือข่าย เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล ระบบไฟฟ้า ระบบสำรองไฟ ระบบควบคุมการเข้าถึง และระบบสนับสนุนอื่น ๆ เพื่อใช้เป็นข้อมูลพื้นฐานในการประเมินความเสี่ยงและจัดลำดับความสำคัญของมาตรการควบคุม

2. หน่วยงานควรกำหนดมาตรการป้องกันความเสี่ยงด้านโครงสร้างพื้นฐานระบบเครือข่ายและการเชื่อมต่อ Internet เช่น การตรวจสอบสถานะอุปกรณ์อย่างสม่ำเสมอ การจัดเตรียมอุปกรณ์สำรอง การจัดหา Link Internet สำรอง และการกำหนดแนวทางการสลับใช้งานเมื่อเกิดเหตุขัดข้อง เพื่อรักษาความต่อเนื่องของการให้บริการ

3. หน่วยงานควรปรับปรุงมาตรการด้านการควบคุมการเข้าถึง โดยกำหนดนโยบายรหัสผ่านที่เหมาะสม ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างสม่ำเสมอ และพิจารณาใช้มาตรการยืนยันตัวตนเพิ่มเติมสำหรับระบบหรือพื้นที่ที่มีความสำคัญ เพื่อลดโอกาสการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต

4. หน่วยงานควรตรวจสอบและบำรุงรักษาระบบสนับสนุนทางกายภาพที่เกี่ยวข้องกับศูนย์ข้อมูลอย่างต่อเนื่อง เช่น ระบบไฟฟ้า ระบบสำรองไฟ ระบบป้องกันอัคคีภัย ระบบแจ้งเตือน และระบบควบคุมสภาพแวดล้อม เพื่อป้องกันเหตุขัดข้องที่อาจส่งผลกระทบต่อความพร้อมใช้งานของระบบ

5. หน่วยงานควรจัดทำหรือทบทวนแผนรับมือเหตุการณ์และแผนกู้คืนระบบให้มีความชัดเจน โดยกำหนดขั้นตอนการแจ้งเหตุ ผู้รับผิดชอบ แนวทางการตอบสนอง การกู้คืนระบบ และการทดสอบแผนอย่างสม่ำเสมอ เพื่อให้สามารถลดผลกระทบและกลับมาให้บริการได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ที่ไม่คาดคิด

6. หน่วยงานควรนำตัวชี้วัดผลการประเมินมาใช้ติดตามความก้าวหน้าในการลดความเสี่ยง เช่น จำนวนประเด็นความเสี่ยงที่ได้รับการจัดการ ระยะเวลาในการดำเนินการตามแผนจัดการความเสี่ยง ระดับความพร้อมในการตอบสนองต่อเหตุการณ์ และระดับความสอดคล้องกับกรอบ NIST Cybersecurity Framework 2.0 เพื่อให้การปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์สามารถดำเนินการได้อย่างต่อเนื่องและตรวจสอบได้

7. หน่วยงานควรกำหนดมาตรการบริหารจัดการความเสี่ยงในระดับกรม โดยจัดทำมาตรฐานกลางสำหรับประเด็นความเสี่ยงที่พบร่วมกันในหลายพื้นที่ เช่น ระบบเครือข่าย การเชื่อมต่อ Internet ระบบไฟฟ้า ระบบสำรองไฟ การควบคุมการเข้าถึง ความปลอดภัยทางกายภาพ และการกู้คืนระบบ พร้อมทั้งกำหนดแนวทางให้แต่ละพื้นที่สามารถปรับใช้มาตรการเพิ่มเติมตามระดับความเสี่ยงและบริบทเฉพาะของตนเอง เพื่อให้การบริหารจัดการความเสี่ยงมีความเหมาะสมและสามารถลดผลกระทบต่อความต่อเนื่องของบริการได้อย่างเป็นระบบ

5.3.2 ข้อเสนอแนะสำหรับการศึกษาครั้งต่อไป

สำหรับการศึกษาครั้งต่อไป ผู้วิจัยมีข้อเสนอแนะเพื่อพัฒนาการศึกษาเกี่ยวกับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ข้อมูลภาครัฐให้มีความครอบคลุมและสมบูรณ์มากยิ่งขึ้น ดังนี้

1. ควรขยายขอบเขตการศึกษาไปยังศูนย์ข้อมูลหรือพื้นที่ปฏิบัติงานอื่นของหน่วยงาน เพื่อให้สามารถเปรียบเทียบระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างพื้นที่ได้ครอบคลุมมากยิ่งขึ้น

2. ควรเก็บรวบรวมข้อมูลเพิ่มเติมจากผู้ที่เกี่ยวข้องหลายกลุ่ม เช่น ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องแม่ข่าย ผู้รับผิดชอบระบบความปลอดภัย ผู้บริหารด้านเทคโนโลยีสารสนเทศ และ

ผู้ใช้งานระบบ เพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับปัญหา ข้อจำกัด และความต้องการในการปรับปรุงมาตรการควบคุม

3. ควรศึกษาการประยุกต์ใช้กรอบมาตรฐานอื่นร่วมกับ NIST Cybersecurity Framework 2.0 เช่น ISO/IEC 27001, CIS Controls หรือ NIST SP 800-53 เพื่อให้สามารถกำหนดมาตรการควบคุมที่มีความละเอียดและเหมาะสมกับบริบทของหน่วยงานมากยิ่งขึ้น

4. ควรศึกษาความพร้อมด้านทรัพยากรของหน่วยงาน เช่น งบประมาณ บุคลากร เครื่องมือ เทคโนโลยี และระยะเวลาดำเนินการ เพื่อประกอบการจัดลำดับความสำคัญของแผนจัดการความเสี่ยงให้สามารถนำไปปฏิบัติได้จริง

5. ควรมีการติดตามผลหลังจากหน่วยงานนำข้อเสนอแนะหรือมาตรการลดความเสี่ยงไปดำเนินการ เพื่อประเมินว่ามาตรการดังกล่าวสามารถลดระดับความเสี่ยง เพิ่มความพร้อมในการตอบสนองต่อเหตุการณ์ และยกระดับความสอดคล้องกับกรอบ NIST Cybersecurity Framework 2.0 ได้มากน้อยเพียงใด

บรรณานุกรม

ราชกิจจานุเบกษา. (2562). "พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.

Amiruddin, A., H. G. Afiansyah and H. A. Nugroho (2021). Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8, IEEE.

Bakalynskyi, O. and F. Korobeynikov (2023). Establishing Goals in the Creation of Cyber-Resilient Systems per NIST. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE.

Center for Internet Security (2024). CIS Critical Security Controls Version 8.1, Center for Internet Security.

Dedeke, A. (2017). "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles." IEEE Security & Privacy 15(5): 47-54.

Dutta, A. and E. Al-Shaer (2019). “What”, “Where”, and “Why” Cybersecurity Controls to Enforce for Optimal Risk Mitigation. 2019 IEEE Conference on Communications and Network Security (CNS), IEEE.

Freas, R. L., H. F. Adair and E. Hammad (2022). An Engineering Process Framework for Cybersecurity Incident Response Assessment. 2022 IEEE Conference on Dependable and Secure Computing (DSC).

Handri, E. Y., P. A. W. Putro and D. I. Sensuse (2023). Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs).

Joint Task Force (2020). Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology.

Joint Task Force Transformation Initiative (2012). Guide for Conducting Risk Assessments, National Institute of Standards and Technology.

Khou, S., L. O. Mailloux, J. M. Pecarina and M. Mcevilley (2017). "A Customizable Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks." IEEE Access 5: 12878-12894.

Monev, V. (2024). Suitability of Information Security Frameworks for an IT-Centric ISMS. 2024 International Conference on Information Technologies (InfoTech).

Moreira, F. R., D. A. D. S. Filho, G. D. A. Nze, R. T. d. S. Júnior and R. R. Nunes (2021). "Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology." IEEE Access 9: 129605-129618.

Mylrea, M., S. N. G. Gourisetti and A. Nicholls (2017). An introduction to buildings cybersecurity framework. 2017 IEEE Symposium Series on Computational Intelligence (SSCI).

Pascoe, C., S. Quinn and K. Scarfone (2024). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD, National Institute of Standards and Technology.

Perdana, R. S., A. Effendy, H. Garnida, A. Fidayan, F. Nazar and D. Saepudin (2022). Security and Risk Assessment of Academic Information System By Using NIST Framework (A Case Study Approach). 2022 16th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

Safitri, E. H. N. and H. Kabetta (2023). Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs).

Saritac, U., X. Liu and R. Wang (2022). Assessment of Cybersecurity Framework in Critical Infrastructures. 2022 IEEE Delhi Section Conference (DELCON).

Supriyadi, Y. and C. W. Hardani (2018). Information System Risk Scenario Using COBIT 5 for Risk And NIST SP 800-30 Rev. 1 A Case Study. 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE).

Werthwein, M. and B. Annighoefer (2024). Model-Based Avionics Cybersecurity Framework for Identification of Risk and Evaluation. 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC).



ภาคผนวก

รายละเอียดผลการประเมินความเสี่ยงของพื้นที่ศึกษาและพื้นที่เปรียบเทียบ

ภาคผนวกนี้แสดงรายละเอียดผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของพื้นที่ที่ศึกษาในครั้งนี้และพื้นที่เปรียบเทียบเดิม เพื่อใช้ประกอบการวิเคราะห์ความเหมือน ความแตกต่าง และแนวทางการบริหารจัดการความเสี่ยงในระดับหน่วยงาน โดยพื้นที่ที่ศึกษาในครั้งนี้ได้แก่ ท่าอากาศยานอุบลราชธานี และท่าอากาศยานอุดรธานี ส่วนพื้นที่เปรียบเทียบเดิม ได้แก่ ท่าอากาศยานนครพนม และท่าอากาศยานกระบี่

ตารางที่ ก-1 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานอุบลราชธานี

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงาน ส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	ต่ำ
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	ต่ำ
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้	ต่ำ

จากตารางที่ ก-1 พบว่าท่าอากาศยานอุบลราชธานีมีสถานการณ์ความเสี่ยงจำนวน 6 รายการ โดยมีความเสี่ยงระดับปานกลาง 2 รายการ และระดับต่ำ 4 รายการ ประเด็นความเสี่ยง

ที่อยู่ในระดับปานกลางเกี่ยวข้องกับอุปกรณ์เครือข่ายเสียหายพร้อมกัน และการไม่สามารถใช้งาน Internet ได้ ซึ่งควรได้รับการติดตามและกำหนดมาตรการควบคุมเพิ่มเติมเพื่อรักษาความต่อเนื่องของการให้บริการ

ตารางที่ ก-2 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานอุดรธานี

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงาน ส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	ต่ำ
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	ปานกลาง
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้	ปานกลาง

จากตารางที่ ก-2 พบว่าท่าอากาศยานอุดรธานีมีสถานการณ์ความเสี่ยงจำนวน 6 รายการ โดยมีความเสี่ยงระดับปานกลาง 4 รายการ และระดับต่ำ 2 รายการ ประเด็นความเสี่ยงที่อยู่ในระดับปานกลางเกี่ยวข้องกับอุปกรณ์เครือข่าย การใช้งาน Internet เหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย และเหตุขัดข้องด้านระบบไฟฟ้า ซึ่งควรได้รับการติดตามและกำหนดมาตรการควบคุมเพิ่มเติมเพื่อรักษาความต่อเนื่องของการให้บริการ

ตารางที่ ก-3 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานนครพนม

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงาน ส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	สูง
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	สูง
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้ พนักงานไม่สามารถปฏิบัติงานได้	สูง

จากตารางที่ ก-3 พบว่าท่าอากาศยานนครพนมมีสถานการณ์ความเสี่ยงจำนวน 6 รายการ โดยมีความเสี่ยงระดับสูง 3 รายการ ระดับปานกลาง 2 รายการ และระดับต่ำ 1 รายการ ประเด็นความเสี่ยงระดับสูงเกี่ยวข้องกับอุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย เหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย และเหตุขัดข้องด้านระบบไฟฟ้า ซึ่งควรได้รับการจัดลำดับความสำคัญในการกำหนดมาตรการลดความเสี่ยงและแผนจัดการความเสี่ยงของพื้นที่

ตารางที่ ก-4 รายละเอียดผลการประเมินความเสี่ยงของท่าอากาศยานกระบี่

ลำดับ	สถานการณ์ความเสี่ยง	ระดับความเสี่ยง
1	อุปกรณ์เครือข่ายเสียหายพร้อมกัน ทำให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้	ปานกลาง
2	ไม่สามารถใช้งาน Internet ได้ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบได้	ปานกลาง
3	อุปกรณ์เครื่องแม่ข่าย CCTV เสียหาย หรือมีการซ่อมแซมพื้นที่ปฏิบัติงาน ส่งผลต่อระบบ ทำให้ผู้ใช้งานไม่สามารถนำข้อมูลมาใช้งานได้	ต่ำ
4	ผู้ใช้งานตั้งรหัสผ่านในการเข้าถึงระบบที่สามารถคาดเดาได้ง่าย ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และทำให้ข้อมูลรั่วไหล	ต่ำ
5	เกิดเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ทำให้พนักงานไม่สามารถเข้าปฏิบัติงาน หรืออุปกรณ์สารสนเทศได้รับความเสียหาย	สูง
6	เกิดเหตุขัดข้อง เช่น ไฟฟ้าดับ และไม่สามารถใช้ระบบไฟฟ้าได้ ส่งผลให้ระบบไฟฟ้าของอาคารหรือสำนักงานไม่สามารถใช้งานได้ พนักงานไม่สามารถปฏิบัติงานได้	ต่ำ

จากตารางที่ ก-4 พบว่าท่าอากาศยานกระบี่มีสถานการณ์ความเสี่ยงจำนวน 6 รายการ โดยมีความเสี่ยงระดับสูง 1 รายการ ระดับปานกลาง 2 รายการ และระดับต่ำ 3 รายการ ประเด็นความเสี่ยงระดับสูงเกี่ยวข้องกับเหตุไฟไหม้ภายในพื้นที่ห้องจัดเก็บ Server CCTV หรือห้องเครือข่าย ซึ่งอาจส่งผลต่อการปฏิบัติงานและความเสียหายของอุปกรณ์สารสนเทศ จึงควรได้รับการติดตามและกำหนดมาตรการควบคุมเพิ่มเติมอย่างเหมาะสม

ประวัติผู้เขียน

ชื่อ	นายวุฒิพงศ์ ศรีภูมั่น
ชื่อวิทยานิพนธ์	การปรับปรุงโครงสร้างพื้นฐานระบบเครือข่ายภาครัฐเพื่อให้สอดคล้องกับกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST
สาขาวิชา	การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ประวัติ	ประวัติการศึกษา : สำเร็จการศึกษาระดับปริญญาตรี คณะวิศวกรรมศาสตร์ สาขาวิชา วิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ประวัติการทำงาน พ.ศ. 2559 – 2565 บริษัท จัสเทล เน็ตเวิร์ค จำกัด ตำแหน่ง System Engineer พ.ศ. 2565 - ปัจจุบัน กรมท่าอากาศยาน ตำแหน่ง นักวิชาการคอมพิวเตอร์