



ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ๗/๒๕๖๙

เรื่อง หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแล ตามแนวทางพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

.....

ด้วยประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๘ และที่แก้ไขเพิ่มเติม ซึ่งออกตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านบริการภาครัฐที่สำคัญซึ่งมีภารกิจหรือให้บริการโดยตรง ได้แก่ บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล และบริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์ วิธีการ และแนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของ สพร. เพื่อให้การกำกับดูแล และการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ มีมาตรฐาน และสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง จึงอาศัยอำนาจตามความในมาตรา ๘ (๙) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ ประกอบกับมาตรา ๕๓ และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ รวมทั้งประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ จึงออกประกาศเรื่อง หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลตามแนวทางพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนด เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลดังกล่าว ได้ถือปฏิบัติ โดยมีหลักเกณฑ์ วิธีการ และแนวทางการตรวจประเมินปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศ
เปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๒ กันยายน พ.ศ. ๒๕๖๙

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการ รักษาการแทน

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประกาศแนบท้าย
เรื่อง หลักเกณฑ์การตรวจประเมิน
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ภายใต้การควบคุมหรือกำกับดูแล ตามแนวทาง
พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

สารบัญ

บทที่ 1 บทนำ	11
1.1 ความเป็นมา.....	11
1.2 วัตถุประสงค์	11
1.3 ขอบเขตการศึกษา	12
1.4 ประโยชน์ที่คาดว่าจะได้รับ	12
1.5 วิธีดำเนินการศึกษา.....	13
บทที่ 2 ผลการศึกษามาตรฐานและกฎหมายที่เกี่ยวข้อง	15
2.1 บทวิเคราะห์เชิงเปรียบเทียบระหว่างมาตรฐานสากล กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.....	15
2.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	16
2.1.2 บทวิเคราะห์เชิงเปรียบเทียบกรอบแนวทาง NIST Cybersecurity Framework กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	28
2.1.3 บทวิเคราะห์เชิงเปรียบเทียบกลุ่มมาตรฐาน ISO/IEC 27000 family กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.....	36
2.2 บทวิเคราะห์เชิงเปรียบเทียบ ระหว่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	49
2.2.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.....	49
2.2.2 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของ ผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565.....	50
2.3 เอกสารต้นแบบที่สำคัญสำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	57
บทที่ 3 หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลตามแนวทาง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	63
3.1 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อกำหนดหลักที่ต้องปฏิบัติ (Mandatory Requirements).....	63
ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ	64
องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์.....	64
3.1.1 การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์.....	64
3.1.2 การรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์.....	66
3.1.3 การแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด	68
3.1.4 การปรับปรุงแผนการดำเนินงานการแก้ไข.....	69
3.1.5 การดำเนินการแก้ไขข้อบกพร่อง.....	70
องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	72
3.1.6 การประเมินความเสี่ยง	72
3.1.7 การจัดการความเสี่ยง	74
3.1.8 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review).....	76

3.1.9 การรายงานความเสี่ยง (Risk Reporting)	77
องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์	79
3.1.10 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	79
3.1.11 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ (Communication of Cybersecurity Incident Response Plan) (ข้อ 19.2)	81
3.1.12 การทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Review of Cybersecurity Incident Response Plan)	83
3.1.13 การทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (Review of Cybersecurity Incident Response Plan upon Significant Change)	84
ส่วนที่ 2 : แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์	86
1. การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)	86
3.1.14 การจัดการทะเบียนทรัพย์สินสำหรับบริการที่สำคัญ (Asset Management Inventory)	86
3.1.15 การระบุขอบเขตเครือข่ายและระบบคอมพิวเตอร์ที่เชื่อมต่อ (Network Boundary and Interfaces)	88
3.1.16 การตรวจสอบและปรับปรุงทะเบียนทรัพย์สิน (Review and Update of Inventory)	89
3.1.17 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์รายปี (Annual Cybersecurity Risk Assessment)	90
3.1.18 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	92
3.1.19 ทะเบียนความเสี่ยง (Risk Register)	93
3.1.20 การประเมินช่องโหว่ของบริการที่สำคัญ (Vulnerability Assessment)	95
3.1.21 ขอบเขตของการประเมินช่องโหว่ (Scope of Vulnerability Assessment)	97
3.1.22 การประเมินช่องโหว่ก่อนเริ่มระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ (Vulnerability Assessment for New Systems or Significant Changes)	99
3.1.23 การทดสอบเจาะระบบ (Penetration Testing)	101
3.1.24 ขอบเขตของการทดสอบเจาะระบบ (Scope of Penetration Testing)	103
3.1.25 ความถี่และความจำเป็นในการทดสอบเจาะระบบ (Frequency and Necessity of Penetration Testing)	104
3.1.26 คุณสมบัติและความเป็นอิสระของผู้ทดสอบเจาะระบบ (Qualifications and Independence of Penetration Testers)	106
3.1.27 การกำกับดูแลการทดสอบเจาะระบบโดยผู้ให้บริการภายนอก (Supervision of Penetration Testing)	108
3.1.28 กระบวนการติดตามและจัดการช่องโหว่ (Vulnerability Tracking and Remediation Process)	110
3.1.29 การส่งรายงานสรุปผลการทดสอบเจาะระบบต่อสำนักงาน (Submission of Penetration Test Summary Report)	112
3.1.30 ภาระรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ในการใช้บริการจากภายนอก (Accountability in Third Party Management)	113

3.1.31 ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญาจ้างผู้ให้บริการภายนอก (Cybersecurity Requirements in Service Agreements)	115
3.1.32 การตรวจสอบความถูกต้องและความสอดคล้องของผู้ให้บริการภายนอก (Verification of Third Party Compliance).....	117
3.1.33 การปรับปรุงเงื่อนไขสัญญาจ้างตามกฎหมายหรือข้อบังคับใหม่ (Negotiation of Contract Terms for New Legal Requirements).....	119
2. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)	122
3.1.34 การจำกัดการเข้าถึงบริการที่สำคัญ (Restriction of Access to Critical Services).....	122
3.1.35 เทคนิคการตรวจสอบสิทธิ์การเข้าถึง (Authentication Techniques for Access).....	124
3.1.36 การเก็บรักษาและตรวจสอบบันทึกการเข้าถึง (Access Logging and Monitoring).....	126
3.1.37 การกำกับดูแลการเข้าถึงอินเทอร์เน็ตและการเข้าถึงทางลอจิคอล (Supervision of Interface and Logical Access)	128
3.1.38 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards).....	129
3.1.39 หลักการรักษาความมั่นคงปลอดภัยในมาตรฐานการกำหนดค่า (Principles for Security Baseline Configuration).....	131
3.1.40 การตรวจสอบความสอดคล้องของมาตรฐานการกำหนดค่าก่อนเริ่มใช้งาน (Security Baseline Enforcement before Connection or Change).....	133
3.1.41 การทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยรายปี (Annual Review of Security Baseline Configuration Standards).....	135
3.1.42 กระบวนการจัดการการเปลี่ยนแปลง (Change Management Process).....	136
การเชื่อมต่อระยะไกล (Remote Connection).....	138
3.1.43 การรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล (Security of Remote Connection).....	138
3.1.44 แนวทางปฏิบัติเฉพาะสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ (Specific Practices for Remote Connection to Critical Services)	139
3.1.45 การควบคุมสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (Control of Removable Storage Media and Portable Computing Devices).....	141
3.1.46 การเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้ (Encryption of Data on Removable Storage Media)	143
3.1.47 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness).....	144
3.1.48 การทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Review of Cybersecurity Awareness Program).....	146
3.1.49 การแบ่งปันข้อมูล (Information Sharing)	147
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect).....	150
3.1.50 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring).....	150

3.1.51 การทบทวนกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Review of Cyber Threat Detection and Monitoring Mechanisms and Processes)	151
4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	154
3.1.52 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	154
3.1.53 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	155
3.1.54 รายละเอียดของแผนการสื่อสารในภาวะวิกฤต (Details of Crisis Communication Plan)	156
3.1.55 การประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบในแผนการสื่อสารในภาวะวิกฤต (Coordination among Affected Parties in Crisis Communication Plan)	158
3.1.56 การฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต (Cybersecurity Crisis Communication Exercise)	159
3.1.57 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	160
3.1.58 การให้ข้อมูลเพื่อการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ (Provision of Information for Cyber Exercise Planning and Execution)	162
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	164
3.1.59 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	164
3.1.60 การฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan Exercise)	166
3.2 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามแนวทางปฏิบัติที่ดี (Best Practices)	168
ส่วนที่ 1 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติ	168
องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	168
3.2.1 ความรับผิดชอบของผู้นำองค์กรและการส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์	168
3.2.2 การกำกับดูแล การทบทวน และการปรับปรุงกลยุทธ์และผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์	170
ส่วนที่ 2 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	173
1. การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)	173
3.2.3 การจัดทำนโยบายและกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์ของห่วงโซ่อุปทาน	173
2. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)	175
3.2.4 การจัดการบัญชีผู้ใช้	175
3.2.5 การรักษาความมั่นคงปลอดภัยของข้อมูล	177
3.2.6 การจัดการแพตช์	180
3.2.7 การจัดการซอฟต์แวร์	182
3.2.8 การจัดการฮาร์ดแวร์	185
3.2.9 การจัดการบันทึกเหตุการณ์	186

3.2.10 การพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย.....	188
3.2.11 การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี.....	192
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect).....	194
3.2.12 การวิเคราะห์เหตุการณ์ไม่พึงประสงค์	194
4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond).....	197
3.2.13 การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์.....	197
3.2.14 การบรรเทาเหตุภัยคุกคามทางไซเบอร์.....	199
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover).....	201
3.2.15 การจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์.....	201
3.2.16 การทดสอบ ทบทวน และปรับปรุงแผน	203
3.2.17 การดำเนินการตามแผนฟื้นฟูจากเหตุจริง	205
3.2.18 แผนการสำรองข้อมูล.....	208
3.2.19 การสื่อสารระหว่างการฟื้นฟูเหตุภัยคุกคามทางไซเบอร์	211
บทที่ 4 การพัฒนาระบบการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ	213
4.1 แบบฟอร์มคำรับรองการนำข้อความไปใช้ (Statement of Applicability : SOA)	213
4.2 โปรแกรมการตรวจประเมิน (Audit Program).....	215
4.3 แผนการตรวจประเมิน (Audit Plan).....	216
4.4 รายงานการตรวจประเมิน (Audit Report)	219
4.5 แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR).....	221
4.6 แผนการแก้ไข (Corrective Action Plan)	222
4.7 รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)	223
4.8 ข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องตามประมวลแนวทางปฏิบัติฯ สำหรับ บริการทั้ง 4 บริการ	226
4.9 คู่มือขั้นตอนการปฏิบัติงานของกระบวนการตรวจประเมิน (Audit Manual)	228
บรรณานุกรม.....	232
ภาคผนวก	234

สารบัญตาราง

ตารางที่ 1 กลไกการตรวจสอบ (Audit).....	20
ตารางที่ 2 สรุปหัวข้อการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ	24
ตารางที่ 3 ประเภทและลำดับชั้นของเอกสาร.....	27
ตารางที่ 4 สรุปความสัมพันธ์ของกฎหมายฉบับรอง ของ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	30
ตารางที่ 5 ความสอดคล้องของ NIST CSF 1.1 และประมวลแนวทางปฏิบัติ พ.ศ. 2564	34
ตารางที่ 6 ความสอดคล้องของ NIST CSF 2.0 และประมวลแนวทางปฏิบัติ พ.ศ. 2564	36
ตารางที่ 7 Subcategory ใน NIST CSF 2.0 ที่แตกต่างกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	37
ตารางที่ 8 ข้อเสนอแนะในการจัดทำหัวข้อการตรวจประเมินเพิ่มเติม อ้างอิงตาม NIST CSF 2.0	40
ตารางที่ 9 สรุปมาตรการควบคุมตามมาตรฐาน ISO/IEC 27001:2022.....	43
ตารางที่ 10 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27001:2022 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	47
ตารางที่ 11 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27701:2025 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	48
ตารางที่ 12 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27017:2015 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	49
ตารางที่ 13 สรุปความแตกต่างของมาตรฐาน ISO/IEC 27001:2022 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	52
ตารางที่ 14 ข้อเสนอแนะในการจัดทำหัวข้อการตรวจประเมินเพิ่มเติม อ้างอิงตาม NIST CSF 2.0 และ ISO/IEC 27001:2022	54
ตารางที่ 15 สรุปความสอดคล้องของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	60
ตารางที่ 16 โครงสร้างแบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)	254

สารบัญภาพ

รูปที่ 1	แบบจำลองกรอบแนวคิดที่ใช้ในการศึกษา วิเคราะห์ และกำหนดแนวทางการตรวจประเมิน	16
รูปที่ 2	โครงสร้างหลักของกรอบการทำงาน NIST Cybersecurity Framework 2.0	34
รูปที่ 3	ต้นแบบเอกสาร (ร่าง) หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศฯ..	66
รูปที่ 4	ต้นแบบแบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ (Statement of Applicability : SOA).....	67
รูปที่ 5	ต้นแบบโปรแกรมการตรวจประเมิน (Audit Program)	67
รูปที่ 6	ต้นแบบแผนการตรวจประเมิน (Audit Plan)	68
รูปที่ 7	ต้นแบบรายงานการตรวจประเมิน (Audit Report)	68
รูปที่ 8	ต้นแบบแบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR).....	69
รูปที่ 9	ต้นแบบแผนการแก้ไข (Corrective Action Plan)	69
รูปที่ 10	ต้นแบบรายงานการทบทวนโดยฝ่ายบริหาร (Management Review)	69
รูปที่ 11	ต้นแบบข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ	70

บทที่ 1 บทนำ

1.1 ความเป็นมา

ด้วยพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีการกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568 และที่แก้ไขเพิ่มเติม มอบหมายให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมวด 2 ด้านบริการภาครัฐที่สำคัญ ข้อ 2 ที่มีการให้บริการโดยตรงแก่ประชาชน รวม 4 บริการ ได้แก่

- 1) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- 2) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ
- 3) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง
- 4) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน

ในการนี้เพื่อให้บรรลุวัตถุประสงค์ข้างต้นอย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น และให้เป็นไปตามมาตรา 53 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สพร. จึงเห็นสมควรดำเนินการศึกษามาตรฐานและกฎหมายที่เกี่ยวข้อง เช่น ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017 และ NIST Cybersecurity Framework ที่ประกาศเป็นปัจจุบัน และศึกษากฎหมาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อเปรียบเทียบกับพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้เห็นถึงความสอดคล้องและไม่สอดคล้อง จากนั้น นำเสนอ ออกแบบ จัดทำแผนดำเนินการและกระบวนการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่อยู่ภายใต้การกำกับดูแลของ สพร. ให้ปฏิบัติตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งนี้ เพื่อให้การตรวจประเมินระบบเทคโนโลยีสารสนเทศของหน่วยงานภายใต้การกำกับดูแลของ สพร. เป็นไปอย่างมีประสิทธิภาพ สอดคล้องตามประกาศที่เกี่ยวข้อง และอ้างอิงตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

1.2 วัตถุประสงค์

การศึกษารั้วนี้ มีวัตถุประสงค์หลักดังต่อไปนี้

1. เพื่อวิเคราะห์เชิงเปรียบเทียบและระบุความสอดคล้อง/ความแตกต่าง ระหว่าง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับมาตรฐานสากลที่ได้รับการยอมรับ ได้แก่ กรอบแนวทาง NIST Cybersecurity Framework 2.0 และ กลุ่มมาตรฐาน ISO/IEC 27000 Families
2. เพื่อวิเคราะห์เชิงเปรียบเทียบ ระหว่าง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. เพื่อนำผลการวิเคราะห์ที่ได้ ไปใช้ในการออกแบบ จัดทำแผนดำเนินการ กระบวนการตรวจประเมิน และจัดทำเอกสารต้นแบบ สำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่อยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

1.3 ขอบเขตการศึกษา

การศึกษานี้ ครอบคลุมการวิเคราะห์กฎหมายและมาตรฐานสากลที่เกี่ยวข้อง ดังนี้

1. กลุ่มกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์
 - พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
 - ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564
 - ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำฯ พ.ศ. 2566
 - ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติฯ พ.ศ. 2568
2. กลุ่มมาตรฐานสากล (International Standards)
 - NIST Cybersecurity Framework 2.0
 - ISO/IEC 27001:2022 (การรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองความเป็นส่วนตัว — ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ)
 - ISO/IEC 27701:2025 (การรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองความเป็นส่วนตัว — ระบบการจัดการข้อมูลส่วนบุคคล)
 - ISO/IEC 27017:2015 และ ISO/IEC 27017:2025 (DIS) (การรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองความเป็นส่วนตัว — การควบคุมความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ตามมาตรฐาน ISO/IEC 27002)
3. กลุ่มกฎหมายคุ้มครองข้อมูลส่วนบุคคล
 - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
4. ขอบเขตหน่วยงานเป้าหมาย ได้แก่ หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ (CII) จำนวน 4 บริการ ภายใต้การกำกับดูแลของ สพร.

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ผลการศึกษานี้ คาดว่าจะเกิดประโยชน์ในมิติต่าง ๆ ดังนี้

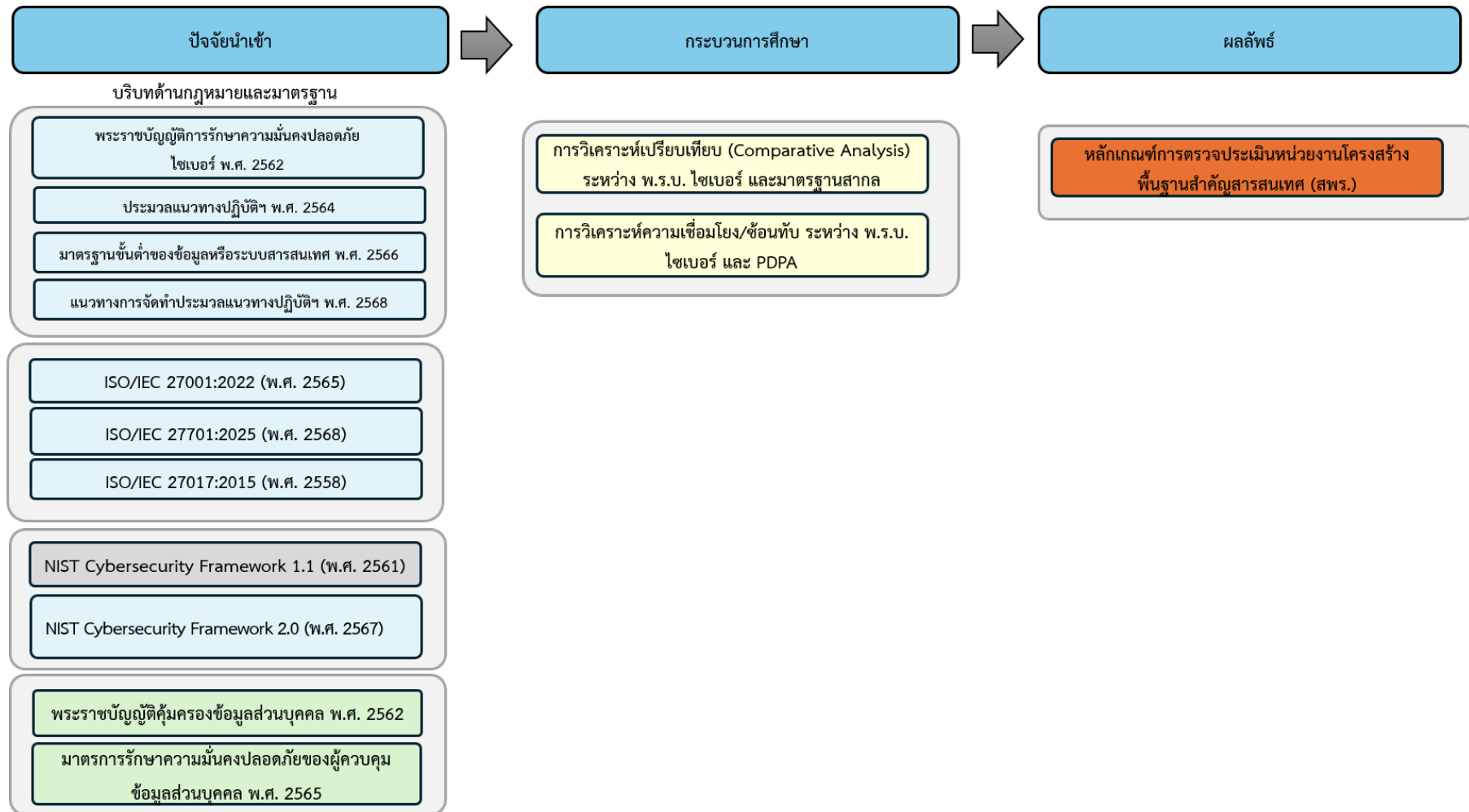
1. ได้เอกสารต้นแบบและเครื่องมือมาตรฐาน เช่น แนวทางการตรวจประเมิน แบบฟอร์มการตรวจประเมิน ที่มีประสิทธิภาพ ครบคลุม และสอดคล้องกับมาตรฐานสากล สำหรับใช้ในการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ภายใต้การกำกับดูแลของ สพร.
2. องค์กรและหน่วยงานที่เกี่ยวข้องมีความเข้าใจที่ชัดเจนถึงจุดเชื่อมโยงระหว่างข้อกำหนดทางกฎหมายของไทยและมาตรฐานสากล (เช่น NIST CSF และ ISO/IEC) ทำให้สามารถวางแผนในการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ
3. หน่วยงาน CII จำนวน 4 บริการภายใต้การกำกับดูแลของ สพร. สามารถยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างบูรณาการ เป็นระบบ และถูกต้องตามข้อกำหนดของกฎหมาย รวมถึงสอดคล้องกับมาตรฐานสากล

1.5 วิธีดำเนินการศึกษา

กรอบแนวคิดที่ใช้ในการศึกษา วิเคราะห์ และกำหนดแนวทางการตรวจประเมิน จะประกอบไปด้วย การศึกษาข้อมูลกฎหมายและมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่

- **บริบททางกฎหมายและเกณฑ์มาตรฐานภายในประเทศ:** ศึกษากลุ่มกฎหมายแม่บท ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง อาทิ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำฯ พ.ศ. 2566 ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติฯ พ.ศ. 2568
- **กรอบมาตรฐาน NIST Cybersecurity Framework:** การนำแนวทางจาก NIST ทั้งฉบับ 1.1 และ 2.0 (พ.ศ. 2567) มาใช้เป็นต้นแบบในการวิเคราะห์มิติการรักษาความมั่นคงปลอดภัยเชิงระบบ
- **มาตรฐานสากลด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ:** อ้างอิงเกณฑ์มาตรฐาน ISO/IEC เวอร์ชันล่าสุด ได้แก่ ISO/IEC 27001:2022 (ISMS), ISO/IEC 27701:2025 (PIMS), ISO/IEC 27017:2015 และ ISO/IEC 27017:2025
- **กฎหมายคุ้มครองข้อมูลส่วนบุคคล:** การบูรณาการร่วมกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

จากนั้นดำเนินการเปรียบเทียบข้อกำหนดระหว่างกฎหมายของไทยและมาตรฐานสากล (NIST CSF และ ISO/IEC) เพื่อระบุช่องว่าง (Gap Analysis) และระดับความเข้มงวดของมาตรการที่จำเป็น โดยผลลัพธ์จากการศึกษา จะเป็นต้นแบบในการกำหนดหลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) สำหรับ สพร. เพื่อใช้เป็นเครื่องมือมาตรฐานในการตรวจประเมินและยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยสารสนเทศภาครัฐในระดับประเทศ



รูปที่ 1 แบบจำลองกรอบแนวคิดที่ใช้ในการศึกษา วิเคราะห์ และกำหนดแนวทางการตรวจประเมิน

บทที่ 2 ผลการศึกษามาตรฐานและกฎหมายที่เกี่ยวข้อง

รายละเอียดในบทที่ 2 นี้ จะเป็นการนำเสนอผลการศึกษามาตรฐานและกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้เป็นพื้นฐานในการวิเคราะห์ความสอดคล้องและความแตกต่างระหว่างข้อกำหนดตามกฎหมายไทยกับมาตรฐานสากลที่ได้รับการยอมรับโดยครอบคลุมการศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตลอดจนกรอบแนวทางและมาตรฐานสำคัญ เช่น NIST Cybersecurity Framework และกลุ่มมาตรฐาน ISO/IEC 27000 family ผลการศึกษาดังกล่าวจะนำไปใช้ประกอบการออกแบบแนวทาง แผนดำเนินการ กระบวนการตรวจประเมิน และเอกสารต้นแบบสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ให้มีความครบถ้วน สอดคล้องกับกฎหมาย และอ้างอิงมาตรฐานสากลอย่างเป็นระบบ ดังนี้

ศึกษามาตรฐานและกฎหมายที่เกี่ยวข้อง เช่น ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017 และ NIST Cybersecurity Framework ที่ประกาศเป็นปัจจุบัน และศึกษากฎหมาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อเปรียบเทียบกับพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้เห็นถึงความสอดคล้องและไม่สอดคล้องในด้านใดบ้าง โดยจัดทำเป็น

(1) รายงานบทวิเคราะห์เชิงเปรียบเทียบมาตรฐาน กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(2) รายงานบทวิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(3) เอกสารต้นแบบที่สำคัญสำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.1 บทวิเคราะห์เชิงเปรียบเทียบระหว่างมาตรฐานสากล กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ในสภาวะการณปัจจุบันที่ภัยคุกคามทางไซเบอร์มีความซับซ้อนและส่งผลกระทบในวงกว้าง การสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นสากล รวมถึงการดำเนินการตรวจสอบอย่างต่อเนื่องจึงเป็นกลไกสำคัญในการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การศึกษานี้จึงจัดทำขึ้นเพื่อวิเคราะห์เชิงเปรียบเทียบ ระหว่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งเป็นกฎหมายหลักของประเทศไทย กับมาตรฐานสากลที่ได้รับการยอมรับในระดับนานาชาติ โดยมีวัตถุประสงค์หลักเพื่อระบุความสอดคล้องและไม่สอดคล้อง โดยครอบคลุมชุดมาตรฐานสำคัญ ดังนี้

- 1) กรอบแนวทาง NIST Cybersecurity Framework 2.0
- 2) กลุ่มมาตรฐาน ISO/IEC ได้แก่ ISO/IEC 27001:2022, ISO/IEC 27701:2025, ISO/IEC 27017:2015, ISO/IEC 27017:2015 และ ISO/IEC 27017:2025 (DIS)

ทั้งนี้ ผลการศึกษาจะถูกนำไปใช้ในการออกแบบและจัดทำแผนดำเนินการและกระบวนการตรวจประเมิน
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การ
มหาชน) (สพร.) ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ต่อไป โดยมีรายละเอียดผลการ
วิเคราะห์ ดังต่อไปนี้

2.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีวัตถุประสงค์เพื่อให้การรักษาความมั่นคง
ปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทาง
ไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยมีสาเหตุจากปัจจุบันการ
ให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการของ
ดาวเทียม มีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อย
ภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควร
กำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงาน
ของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการ
ปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่าง
ร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมี
เอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

สาระสำคัญ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 แบ่งออกเป็น 4 หมวดด้วยกัน ได้แก่

หมวด 1 คณะกรรมการ แบ่งโครงสร้างการบริหารจัดการออกเป็น 2 คณะกรรมการหลัก ได้แก่

- คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีนายกรัฐมนตรีเป็น
ประธานกรรมการ มีหน้าที่กำหนดนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคง
ปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี รวมถึงสร้างมาตรฐานขั้นต่ำและกำหนดกรอบการ
ประสานความร่วมมือทั้งในและต่างประเทศ (ม.5 - ม.11)
- คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีรัฐมนตรีว่าการกระทรวง
ดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน มีหน้าที่ติดตามนโยบาย รับมือภัยคุกคามทาง
ไซเบอร์ระดับร้ายแรง และเป็นผู้กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้าน
การรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นข้อกำหนดขั้นต่ำให้หน่วยงานปฏิบัติตาม (ม.12 -
ม.19)

หมวด 2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (ม.20 -
ม.40)

- จัดตั้งสำนักงาน (สกมช.) ให้เป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล โดยไม่เป็นส่วนราชการ
หรือรัฐวิสาหกิจ
- ทำหน้าที่รับผิดชอบงานธุรการและวิชาการให้คณะกรรมการ เป็นศูนย์กลางรวบรวม วิเคราะห์
และเฝ้าระวังข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ของประเทศ รวมถึงประสานงานตอบสนอง
เหตุการณ์ภัยคุกคามร่วมกับหน่วยงานทั้งภาครัฐและเอกชน

- ให้มีคณะกรรมการบริหารสำนักงาน (กบส.) ดูแลการบริหารทั่วไป และมีเลขาธิการเป็นผู้รับผิดชอบการปฏิบัติงานและเป็นผู้บังคับบัญชาพนักงานในสำนักงาน

หมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นหมวดที่สำคัญที่สุดซึ่งครอบคลุมกลไกการปฏิบัติงาน โดยแบ่งย่อยเป็น 4 ส่วน คือ

ส่วนที่ 1 นโยบายและแผน มุ่งเน้นการบูรณาการและการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยบังคับให้หน่วยงานจัดทำประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งต้องมีแผนตรวจสอบความเสี่ยงและแผนรับมือภัยคุกคาม (ม.41 - ม.44)

ส่วนที่ 2 การบริหารจัดการ หน่วยงานของรัฐ หน่วยงานกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ต้องแจ้งรายชื่อเจ้าหน้าที่เพื่อใช้เป็นช่องทางประสานงานด้านไซเบอร์ไปยังสำนักงาน (ม.45 - ม.47)

ส่วนที่ 3 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) (ม.48 - ม.57)

กำหนดกลุ่มหน่วยงานที่มีภารกิจหรือบริการเป็น CII ไว้ 7 ด้าน ได้แก่

- 1) ด้านความมั่นคงของรัฐ
- 2) ด้านบริการภาครัฐที่สำคัญ
- 3) ด้านการเงินการธนาคาร
- 4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- 5) ด้านการขนส่งและโลจิสติกส์
- 6) ด้านพลังงานและสาธารณูปโภค
- 7) ด้านสาธารณสุข

ทั้งนี้ อาจมีด้านอื่น ตามที่คณะกรรมการประกาศกำหนดเพิ่มเติมในอนาคตได้

หน่วยงาน CII จะต้องจัดให้มีการประเมินความเสี่ยงและมีผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศเข้าตรวจสอบระบบอย่างน้อยปีละ 1 ครั้ง และหากเกิดภัยคุกคามอย่างมีนัยสำคัญต้องรายงานต่อสำนักงานทันที

ส่วนที่ 4 การรับมือกับภัยคุกคามทางไซเบอร์ แบ่งระดับความรุนแรงของภัยคุกคามออกเป็น 3 ระดับ ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ กฎหมายให้อำนาจ กกม. และพนักงานเจ้าหน้าที่ในการขอข้อมูล เข้าตรวจสอบสถานที่ เข้าถึงระบบคอมพิวเตอร์ หรือยึดอายัดอุปกรณ์เพื่อระงับและตรวจสอบภัยคุกคามได้ (โดยบางกรณีต้องขออำนาจศาลพิจารณาไต่สวนฉุกเฉิน) ทั้งนี้ หากเป็นภัยคุกคามระดับวิกฤติจะเป็นอำนาจของสภาความมั่นคงแห่งชาติในการเข้ามามีอำนาจจัดการ (ม.58 - ม.69)

หมวด 4 บทกำหนดโทษ (ม.70 - ม.77)

- กำหนดโทษสำหรับเจ้าหน้าที่หากมีการนำข้อมูลความลับ ข้อมูลจราจร หรือข้อมูลคอมพิวเตอร์ไปเปิดเผยโดยมิชอบ จะมีโทษจำคุกและโทษปรับ
- หากหน่วยงาน CII เกิดภัยคุกคามแล้วไม่รายงานเหตุโดยไม่มีเหตุอันสมควร มีโทษปรับไม่เกินสองแสนบาท
- กำหนดโทษปรับและจำคุกสำหรับผู้ฝ่าฝืน ขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. พนักงานเจ้าหน้าที่ หรือคำสั่งศาลในการรับมือกับภัยคุกคาม รวมถึงกำหนดให้กรรมการหรือผู้จัดการนิติบุคคลต้องรับโทษด้วยหากการกระทำผิดเกิดจากการสั่งการหรือละเว้นการปฏิบัติหน้าที่ของบุคคลนั้น

ผลการศึกษาและวิเคราะห์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในด้าน กลไกการตรวจสอบ (Audit)

จากการวิเคราะห์กฎหมายในด้านกลไกการตรวจสอบ (Audit) หน่วยงานที่มีสถานะเป็น CII ต้อง
ดำเนินการ ดังนี้

ตารางที่ 1 กลไกการตรวจสอบ (Audit)

ลำดับ	หัวข้อ	รายละเอียด	มาตราที่เกี่ยวข้อง
1	จัดทำแผนการตรวจสอบ	ต้องบรรจุแผนการตรวจสอบและประเมินความ เสี่ยงไว้ในประมวลแนวทางปฏิบัติของหน่วยงาน	มาตรา 44
2	ดำเนินการตรวจสอบ ประจำปี	ต้องจัดหาผู้ตรวจสอบด้านความมั่นคงปลอดภัย สารสนเทศที่มีความเชี่ยวชาญมาดำเนินการ ประเมินความเสี่ยงและ Audit ระบบอย่างน้อย ปีละครั้ง	มาตรา 44 และ มาตรา 54
3	จัดส่งรายงาน	ต้องบริหารจัดการเอกสารและส่งสรุปรายงานผล การดำเนินการให้แก่ สกมช. ภายใน 30 วัน นับแต่วันที่ดำเนินการเสร็จสิ้น	มาตรา 54
4	แก้ไขตามคำสั่ง	หากตรวจสอบพบว่าไม่ได้มาตรฐาน หรือ รายงานการตรวจสอบไม่เป็นไปตามมาตรฐานที่ กำหนด หน่วยงานต้องมีความพร้อมในการ ดำเนินการแก้ไขโดยเร็ว หรือดำเนินการ ตรวจสอบใหม่ตามคำสั่งของหน่วยงานกำกับ ดูแลหรือ กกม.	มาตรา 53 และ มาตรา 55

อย่างไรก็ดี พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นั้น มิได้กำหนด
รายละเอียดและหลักเกณฑ์การตรวจสอบ การศึกษารั้ครั้งนี้ จึงได้พิจารณาครอบคลุมถึงกฎหมายลำดับรองที่สำคัญ
และเป็นแนวทางอยู่ในขอบเขตการศึกษา ได้แก่

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ
และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 (ประมวลแนวทางปฏิบัติฯ พ.ศ.
2564) เป็นข้อกำหนดขั้นต่ำที่บังคับใช้กับหน่วยงาน CII ประกอบด้วย 3 องค์ประกอบหลัก (แผน
ตรวจสอบ, ประเมินความเสี่ยง, แผนรับมือ) และกรอบมาตรฐาน 5 ด้าน (Identify, Protect,
Detect, Respond, Recover)
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของ
ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (มาตรฐานขั้นต่ำฯ พ.ศ. 2566) เป็นการนำประมวล
แนวทางปฏิบัติฯ พ.ศ. 2564 มาบังคับใช้โดยจัดระดับความสำคัญของข้อมูลหรือระบบสารสนเทศ
ออกเป็น 3 ระดับ คือ ต่ำ กลาง และสูง เพื่อให้องค์กรเลือกใช้มาตรการได้อย่างเหมาะสมกับ
ความเสี่ยง

- ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2568 (แนวทางการจัดทำประมวลฯ พ.ศ. 2568) ทำหน้าที่เป็นคู่มือและแนวทางปฏิบัติเชิงลึก (Guidelines) เพื่อให้หน่วยงานใช้เป็นต้นแบบในการจัดทำเอกสารของตนเอง โดยมีเอกสารแนบเพื่อให้ปฏิบัติตามได้ง่ายขึ้น

2.1.1.1 ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

ประกาศฉบับนี้กำหนดขึ้นภายใต้อำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (มาตรา 13 ววรรคหนึ่ง (4) และวรรคสอง และมาตรา 54) มีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา (ประกาศ ณ วันที่ 2 สิงหาคม พ.ศ. 2564) โดยมีวัตถุประสงค์เพื่อเป็นแนวทางในการกำหนดข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

สาระสำคัญ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มีสาระสำคัญดังนี้

1. ขอบเขตการบังคับใช้

มาตรการนี้มีผลบังคับใช้ครอบคลุมองค์กรในภาคส่วนที่มีความสำคัญเชิงโครงสร้างและเสถียรภาพของประเทศ ได้แก่

- หน่วยงานภาครัฐ ที่มีหน้าที่ในการให้บริการสาธารณะหรือจัดการข้อมูลภาครัฐ
- หน่วยงานกำกับดูแล (Regulator) ที่มีหน้าที่ควบคุมกำกับดูแลเฉพาะภาคส่วน
- หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ทั้งในภาครัฐและเอกชนที่หากเกิดเหตุขัดข้องเมื่อมีภัยคุกคามทางไซเบอร์ แล้วจะส่งผลกระทบในวงกว้าง

2. โครงสร้างหลักของประกาศ

การขับเคลื่อนระบบรักษาความมั่นคงปลอดภัยไซเบอร์ถูกแบ่งออกเป็น 2 กลไกหลักที่เกี่ยวเนื่องกัน ได้แก่

- ประมวลแนวทางปฏิบัติ (Code of Practice) เน้นในด้านการบริหารจัดการเชิงปฏิบัติการ ได้แก่ การตรวจสอบความมั่นคงปลอดภัย (Audit), การประเมินความเสี่ยง (Risk Assessment) และการตอบสนองต่ออุบัติการณ์ (Incident Response)
- กรอบมาตรฐาน 5 องค์ประกอบ (Core Functions) ซึ่งยึดโยงตามมาตรฐานสากลประกอบด้วย:

- การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)
- มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)
- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

3. กลไกการตรวจสอบ (Audit)

ประกาศฉบับนี้ ได้กล่าวถึงกลไกการตรวจสอบ (Audit) อ้างอิงแนวปฏิบัติของข้อ 17. องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไว้ดังนี้

1. ผู้ตรวจสอบและความถี่ในการตรวจสอบ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง โดยผู้ที่เข้ามตรวจสอบสามารถเป็นได้ทั้ง ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบอิสระภายนอก ที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ

2. ขอบเขตของการตรวจสอบ (Audit Scope) การตรวจสอบจะต้องครอบคลุมหัวข้ออย่างน้อย ดังนี้:

- กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
- บริการที่สำคัญที่หน่วยงาน CII เป็นเจ้าของหรือใช้บริการอยู่ ตามผลวิเคราะห์ได้จาก BIA
- การประเมินความสอดคล้องในการปฏิบัติตาม พ.ร.บ. ไซเบอร์ฯ, ประมวลแนวทางปฏิบัติฯ, และหลักปฏิบัติหรือมาตรฐานอื่นๆ ที่คณะกรรมการประกาศกำหนด

3. การรายงานผล (Reporting) เมื่อดำเนินการตรวจสอบแล้วเสร็จ หน่วยงาน CII จะต้องจัดส่งผลสรุปรายงานการตรวจสอบให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใน 30 วัน นับแต่วันที่ดำเนินการเสร็จสิ้น ตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งต้องส่งสำเนารายงานนั้นให้หน่วยงานควบคุมหรือกำกับดูแลของตนด้วย

4. การจัดการความไม่สอดคล้อง (Corrective Actions) ในกรณีที่การตรวจสอบภายใต้มาตรา 54 พบว่าหน่วยงานมีการไม่ปฏิบัติตามข้อกำหนด (เว้นแต่คณะกรรมการ กกม. จะมีคำสั่งเป็นอย่างอื่น) หน่วยงานจะต้องจัดทำ แผนการดำเนินการแก้ไข ส่งไปยัง สกมช. ภายใน 30 วัน นับจากวันที่ได้รับรายงานการตรวจสอบ โดยแผนดังกล่าวจะต้องระบุรายละเอียดของการดำเนินการเพื่อแก้ไขปัญหา พร้อมทั้งกำหนดกรอบระยะเวลาที่ชัดเจน และหากคณะกรรมการ กกม. ให้ความเห็นชอบหรือสั่งให้ปรับปรุงแผน หน่วยงานก็จะต้องดำเนินการแก้ไขให้แล้วเสร็จตามระยะเวลาที่ระบุไว้ในแผนนั้น

2.1.1.2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

ประกาศฉบับนี้กำหนดขึ้นภายใต้อำนาจของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (มาตรา 9 (4)) มีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา (ประกาศ ณ วันที่

18 มกราคม พ.ศ. 2567) โดยมีวัตถุประสงค์หลักเพื่อกำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลหรือระบบสารสนเทศของหน่วยงานต่าง ๆ ให้มีระดับความมั่นคงปลอดภัยที่เหมาะสม มุ่งเน้นไปที่การสร้างบรรทัดฐานในการคุ้มครองมิติด้านสารสนเทศโดยยึดถือหลักการพื้นฐาน 3 ประการ ได้แก่ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) และการดำรงไว้ซึ่งสภาพพร้อมใช้งานของระบบ (Availability) เพื่อให้โครงสร้างพื้นฐานดิจิทัลมีความมั่นคงและน่าเชื่อถือในทุกสถานการณ์

กลยุทธ์การบังคับใช้มาตรการควบคุมนั้น ถูกออกแบบภายใต้หลักการบริหารจัดการความเสี่ยง โดยมีการจำแนกมาตรการออกตามระดับความสำคัญของข้อมูลหรือระบบสารสนเทศเป็น 3 ระดับ ประกอบด้วย ระดับต่ำ ระดับกลาง และระดับสูง เพื่อให้หน่วยงานสามารถประยุกต์ใช้ข้อกำหนดทางเทคนิคและแนวทางปฏิบัติได้อย่างเหมาะสมกับบริบทและความเสี่ยงของตนเอง นอกจากนี้ กรอบการดำเนินงานดังกล่าวยังครอบคลุมวงจรการบริหารจัดการภัยคุกคามไซเบอร์อย่างเป็นระบบ เริ่มตั้งแต่กระบวนการระบุความเสี่ยงและสินทรัพย์ (Identify) การวางมาตรการป้องกันเชิงรุก (Protect) การจัดให้มีกลไกตรวจสอบและเฝ้าระวัง (Detect) การกำหนดขั้นตอนการเผชิญเหตุเมื่อเกิดภัยคุกคาม (Respond) ตลอดจนการวางแผนทางฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างมีประสิทธิภาพ (Recover) อันเป็นการสร้างภูมิคุ้มกันทางไซเบอร์ที่ครบวงจร

ตารางที่ 2 สรุปหัวข้อการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

หัวข้อมาตรการควบคุม	ระดับต่ำ	ระดับกลาง	ระดับสูง
องค์ประกอบที่ 1: แผนการตรวจสอบ (Audit Plan)		●	●
องค์ประกอบที่ 2: การประเมินความเสี่ยง (Risk Assessment)	●	●	●
องค์ประกอบที่ 3: แผนการรับมือภัยคุกคาม (Incident Response Plan)	●	●	●
1. การระบุความเสี่ยง (Identify)			
1.1 การจัดการทรัพย์สิน (Asset Management)	●	●	●
1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	●	●	●
1.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			●
1.4 การจัดการผู้ให้บริการภายนอก (Third Party)			●
2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)			
2.1 การควบคุมการเข้าถึง (Access Control)	●	●	●
2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	●	●	●
2.3 การเชื่อมต่อระยะไกล (Remote Connection)		●	●
2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		●	●
2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	●	●	●
2.6 การแบ่งปันข้อมูล (Information Sharing)			●

หัวข้อมาตรการควบคุม	ระดับต่ำ	ระดับกลาง	ระดับสูง
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)			
3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	●	●	●
4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)			
4.1 แผนการรับมือภัยคุกคาม (Cybersecurity Incident Response Plan)	●	●	●
4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	●	●	●
4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	●	●	●
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)			
5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	●	●	●

ความสอดคล้องและความแตกต่างกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 และประกาศฉบับนี้ มีความเชื่อมโยงกันดังนี้

ความสอดคล้อง

- 1) เอกสารทั้ง 2 ฉบับจัดทำขึ้นภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และบังคับใช้กับกลุ่มเป้าหมายเดียวกัน คือ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
- 2) เอกสารฉบับนี้ได้ดึงหัวข้อมาตรการทั้งหมดมาจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยอ้างอิงโครงสร้างหลักเดียวกันอย่างสมบูรณ์ ประกอบด้วย
 - ประมวลแนวทางปฏิบัติ 3 องค์ประกอบ ได้แก่ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์, การประเมินความเสี่ยง และแผนการรับมือภัยคุกคามทางไซเบอร์
 - กรอบมาตรฐาน 5 หัวข้อหลัก: การระบุความเสี่ยง (Identify), มาตรการป้องกัน (Protect), มาตรการตรวจสอบและเฝ้าระวัง (Detect), มาตรการเผชิญเหตุ (Respond) และมาตรการรักษาและฟื้นฟู (Recover)

ความแตกต่าง

- 1) เอกสารฉบับนี้ ออกโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ซึ่งเป็นคณะกรรมการระดับสูงกว่า ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ซึ่งออกโดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กม.)
- 2) เอกสารทั้ง 2 ฉบับมีบทบาทและกลไกการนำไปใช้งานที่แตกต่างกัน โดย ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มุ่งเน้นการกำหนดเนื้อหาและวิธีการปฏิบัติเชิงลึก โดยทำหน้าที่เป็นเสมือนคู่มือมาตรฐานที่ขยายความมาตรการต่าง ๆ ให้เป็นรูปธรรมผ่านการอธิบายรายละเอียดเชิงเทคนิคและกระบวนการบริหารจัดการที่หน่วยงานต้องยึดถือเป็นแนวทางปฏิบัติ แต่ประกาศฉบับนี้ จะมุ่งเน้นการแบ่งระดับความเข้มข้นของการบังคับใช้ ซึ่งนำกรอบของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มาจัดระดับความสำคัญ โดยแบ่งออกเป็น 3 ระดับ คือ ต่ำ กลาง และ สูง จากนั้นกฎหมายจะบังคับว่าระบบแต่ละระดับ ต้องเลือกใช้มาตรการข้อใดจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 บ้างได้แก่
 - ระดับต่ำ: บังคับใช้มาตรการพื้นฐาน เช่น การจัดการทรัพย์สิน, การประเมินความเสี่ยง, การควบคุมการเข้าถึง, การสร้างความตระหนักรู้ ฯลฯ
 - ระดับกลาง: ต้องทำทุกข้อของระดับต่ำ และเพิ่มมาตรการ เช่น แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์, การควบคุมการเชื่อมต่อระยะไกล (Remote Connection) และการควบคุมสื่อเก็บข้อมูลแบบถอดได้
 - ระดับสูง: ต้องทำทุกข้อของระดับกลาง และเพิ่มมาตรการขั้นสูง เช่น การทดสอบเจาะระบบ (Penetration Testing), การจัดการผู้ให้บริการภายนอก, การแบ่งปันข้อมูล และการฟื้นฟูความเสียหาย

2.1.1.3 ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2568

ประกาศฉบับนี้กำหนดขึ้นภายใต้อำนาจตามความข้อ 5 ของประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ลงนามโดยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 3 กรกฎาคม พ.ศ. 2568 โดยให้มีผลบังคับใช้ตั้งแต่วันที่ถัดจากวันประกาศเป็นต้นไป จัดทำขึ้นเพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) มีกรอบการดำเนินงานที่ชัดเจนและสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

สาระสำคัญ

สาระสำคัญของประกาศฉบับนี้ แบ่งออกเป็นห้าส่วน ได้แก่

ส่วนที่ 1 : ประเภทและลำดับชั้นของเอกสารความมั่นคงปลอดภัย

เพื่อให้การดำเนินงานมีประสิทธิภาพ สกมช. ได้กำหนดโครงสร้างลำดับชั้นของเอกสารที่หน่วยงานควรจัดทำ โดยแบ่งออกเป็น 6 ประเภทหลัก ดังนี้

ตารางที่ 3 ประเภทและลำดับชั้นของเอกสาร

ประเภทเอกสาร	คำอธิบาย/ตัวอย่าง
1. นโยบาย (Policy)	กำหนดทิศทางและเป้าหมายในภาพรวมจากผู้บริหารระดับสูง
2. ขั้นตอนปฏิบัติ (Procedure)	รายละเอียดวิธีการทำงาน มักอยู่ในรูปของ Flow Chart
3. แนวทาง (Guideline)	คำแนะนำทั่วไปหรือทางเลือกในการปฏิบัติ (เป็นไปตามความสมัครใจ)
4. มาตรฐาน (Standard)	หลักเกณฑ์หรือข้อบังคับที่ต้องปฏิบัติตามเพื่อให้ได้ผลลัพธ์ตามที่กำหนด
5. แผน (Plan)	การกำหนดกิจกรรม ช่วงเวลา และทรัพยากรเพื่อให้บรรลุเป้าหมาย
6. เอกสารสนับสนุน	แบบฟอร์ม สัญญา หรือเอกสารอ้างอิงภายนอก (เช่น กฎหมาย)

ส่วนที่ 2 : แนวทางการจัดทำประมวลแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกาศนี้กำหนดแนวทางการจัดทำประมวลแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นแนวทางในแต่ละด้าน ดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ 3 : แนวทางการจัดทำกรอบมาตรฐานการรักษาความมั่นคงปลอดภัย 5 ด้านหลัก

ประกาศนี้กำหนดแนวทางปฏิบัติที่ครอบคลุมวงจรการบริหารจัดการภัยคุกคามทางไซเบอร์ เพื่อเป็นแนวทางในแต่ละด้าน ดังนี้

2.1 การระบุความเสี่ยง (Identify)

- การจัดการทรัพย์สิน (Asset Management): การระบุและจัดทำทะเบียนทรัพย์สินสารสนเทศ
- การประเมินความเสี่ยง (Risk Assessment): การวิเคราะห์โอกาสและผลกระทบของภัยคุกคาม
- การประเมินช่องโหว่ (VA/PT): การทดสอบเจาะระบบเพื่อหาจุดอ่อนด้านเทคนิค
- การจัดการผู้ให้บริการภายนอก (Third Party Management): การควบคุมความปลอดภัยของคู่สัญญา

2.2 มาตรการป้องกัน (Protect)

- การควบคุมการเข้าถึง (Access Control): การจัดการสิทธิ์ผู้ใช้งาน
- การทำให้ระบบมีความแข็งแกร่ง (System Hardening): การปรับแต่งค่าความปลอดภัยของระบบ
- การเชื่อมต่อระยะไกล (Remote Connection): การเชื่อมต่อผ่านช่องทางที่ปลอดภัยและมีการเข้ารหัสข้อมูล
- สื่อเก็บข้อมูลแบบถอดได้ (Removable Media): การจำกัดสิทธิ์การเขียนข้อมูล หรือการเข้ารหัสข้อมูลในสื่อเก็บข้อมูลแบบถอดได้
- การแบ่งปันข้อมูล (Information Sharing): แนวทางปฏิบัติในการแลกเปลี่ยนข้อมูลอย่างปลอดภัย

2.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

2.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

- แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan): การจัดทำ Cybersecurity Incident Response Plan
- แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) : ขั้นตอนการแจ้งเหตุต่อสาธารณะหรือผู้มีส่วนได้ส่วนเสีย
- การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

2.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

ส่วนที่ 4 : กระบวนการจัดทำเอกสาร

หน่วยงานควรดำเนินการจัดทำประมวลแนวทางปฏิบัติผ่านขั้นตอนที่เป็นระบบ ดังนี้

1. การศึกษาเบื้องต้น: ศึกษากฎหมายและระเบียบที่เกี่ยวข้อง
2. การสนับสนุนจากผู้บริหาร: ขอความเห็นชอบเชิงนโยบายและงบประมาณ
3. การค้นคว้าและเขียนร่าง: จัดทำเนื้อหาให้สอดคล้องกับบริบทเฉพาะของหน่วยงาน
4. การทบทวนโดยผู้มีส่วนได้ส่วนเสีย: เพื่อให้เกิดความเข้าใจและความพร้อมในการปฏิบัติ
5. การอนุมัติเอกสาร: ดำเนินการตามขั้นตอนการอนุมัติภายในหน่วยงาน
6. การสร้างความรู้ความเข้าใจ: สื่อสารและฝึกอบรมบุคลากร
7. การเผยแพร่เอกสาร: แจกจ่ายตามระดับชั้นความลับของข้อมูล (เช่น ชั้นลับที่สุด, ชั้นลับ, ชั้นเปิดเผย)
8. การติดตามประสิทธิผล: ตรวจสอบว่ามีการนำนโยบายไปปฏิบัติจริงหรือไม่
9. การทบทวนและปรับปรุง: พัฒนาเอกสารให้ทันสมัยตามสถานการณ์ที่เปลี่ยนแปลง

ส่วนที่ 5 : การทบทวนและปรับปรุงตามความจำเป็น

หน่วยงานต้องทบทวนประมวลแนวทางปฏิบัติอย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น มีการเปลี่ยนเทคโนโลยีใหม่ เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลหรือภัยคุกคามทางไซเบอร์ที่รุนแรง เมื่อมีการเปลี่ยนแปลงกฎหมาย กฎระเบียบ มาตรฐานและข้อบังคับใหม่ที่เกี่ยวข้องกับหน่วยงาน เป็นต้น

ความสอดคล้องและความแตกต่างกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 และประกาศฉบับนี้ มีความเชื่อมโยงกันดังนี้

ความสอดคล้อง

- 1) เอกสารทั้ง 2 ฉบับจัดทำขึ้นภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และบังคับใช้กับกลุ่มเป้าหมายเดียวกัน คือ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI)
- 2) เอกสารฉบับนี้ได้ดึงหัวข้อมาตรการทั้งหมดมาจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยอ้างอิงโครงสร้างหลักเดียวกันอย่างสมบูรณ์ ประกอบด้วย
 - ประมวลแนวทางปฏิบัติ 3 องค์ประกอบ ได้แก่ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์, การประเมินความเสี่ยง และแผนการรับมือภัยคุกคามทางไซเบอร์
 - กรอบมาตรฐาน 5 หัวข้อหลัก ได้แก่ การระบุความเสี่ยง (Identify), มาตรการป้องกัน (Protect), มาตรการตรวจสอบและเฝ้าระวัง (Detect), มาตรการเผชิญเหตุ (Respond) และมาตรการรักษาและฟื้นฟู (Recover)

ความแตกต่าง

- 1) เอกสารฉบับนี้ ออกโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยอาศัยอำนาจจาก ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ซึ่งออกโดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)
- 2) เอกสารทั้ง 2 ฉบับมีบทบาทและกลไกการนำไปใช้งานที่แตกต่างกัน โดย ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มุ่งเน้นการกำหนดเนื้อหาและวิธีการปฏิบัติ โดยทำหน้าที่เป็นเสมือนคู่มือมาตรฐานที่ขยายความมาตรการต่าง ๆ ให้เป็นรูปธรรมผ่านการอธิบายรายละเอียดเชิงเทคนิคและกระบวนการบริหารจัดการที่หน่วยงานต้องยึดถือเป็นแนวทางปฏิบัติ แต่ประกาศฉบับนี้ จะมุ่งเน้นการลงลึกถึงระดับเทคนิคและวิธีปฏิบัติงานจริง โดยแบ่งเป็นเอกสารแนบถึง 15 ฉบับ (Annex 1-15) ซึ่งมีทั้งตัวอย่างแบบฟอร์ม (เช่น ทะเบียนทรัพย์สิน, แบบฟอร์ม BIA, แบบฟอร์มรายงานการตรวจสอบ), ขั้นตอนการเจาะระบบ (Penetration Testing), การจัดการผู้ให้บริการภายนอก, ไปจนถึงการตั้งค่าความปลอดภัย (System Hardening)

ตารางที่ 4 สรุปความสัมพันธ์ของกฎหมายฉบับรอง ของ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หัวข้อ	ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานขั้นต่ำฯ พ.ศ. 2566	แนวทางการจัดทำประมวลฯ พ.ศ. 2568
หน่วยงานที่ประกาศ	กกม. (คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์)	กมช. (คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)	สกมช. (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)
อาศัยอำนาจจากประกาศ/มาตรา	มาตรา 13 วรรคหนึ่ง (4) และวรรคสอง และมาตรา 54 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	มาตรา 9 (4) แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	ข้อ 5 ของประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564
วันที่ประกาศบังคับใช้	มีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา (ประกาศเมื่อ 6 ก.ย. 2564)	มีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา (ประกาศเมื่อ 18 ม.ค. 2567)	มีผลบังคับใช้ตั้งแต่วันที่ถัดจากวันประกาศเป็นต้นไป (ประกาศ 3 ก.ค. 2568)
วัตถุประสงค์	เพื่อจัดให้มีข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การ	เพื่อกำหนดมาตรฐานขั้นต่ำในการควบคุมความมั่นคงปลอดภัยไซเบอร์ โดยจัดระดับคุณลักษณะของข้อมูล	เพื่อกำหนดแนวทางและอธิบายรายละเอียดให้หน่วยงานเข้าใจกระบวนการ และสามารถจัดทำประมวล

หัวข้อ	ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานขั้นต่ำฯ พ.ศ. 2566	แนวทางการจัดทำประมวลฯ พ.ศ. 2568
	ปฏิบัติงานเป็นไปอย่างรวดเร็ว มีประสิทธิภาพ ทิศทางเดียวกัน และ สอดคล้องกับมาตรฐานสากล	หรือระบบสารสนเทศ ออกเป็น 3 ระดับ (ต่ำ, กลาง, สูง)	แนวทางปฏิบัติและกรอบ มาตรฐานของตนเองได้อย่างมีประสิทธิภาพ
สาระสำคัญ	กำหนดประมวลแนวทางปฏิบัติ (แผนตรวจสอบ, ประเมินความเสี่ยง, แผนรับมือ) และกรอบมาตรฐานหลัก 5 ด้าน (Identify, Protect, Detect, Respond, Recover) เพื่อใช้เป็นเกณฑ์ในการดำเนินงาน	นำกรอบมาตรฐานจากปี 2564 มาใช้บังคับตามระดับ ความสำคัญของข้อมูลหรือระบบสารสนเทศ (เช่น ระดับต่ำต้องทำมาตรการใดบ้าง ระดับกลางและระดับสูงต้องทำมาตรการขั้นสูงใดเพิ่มขึ้นมา)	เป็นคู่มือเชิงปฏิบัติที่มีเอกสารแนบ 15 ฉบับ อธิบายวิธีการทำงานแบบฟอร์ม และข้อกำหนดทางเทคนิค หากหน่วยงานยังไม่มีเอกสารของตนเองสามารถนำประมวลแนวทางฯ ฉบับนี้ไปใช้พลางก่อนได้
หน่วยงานที่ต้องปฏิบัติตาม	หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
อื่น ๆ	สกมช. ได้กำหนดแบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยอ้างอิงหัวข้อตามประกาศฉบับนี้	-	-

2.1.1.4 สรุปผลการศึกษาและกำหนดแนวทางในการตรวจสอบ (Audit)

จากการศึกษาความสัมพันธ์ของกฎหมายลำดับรองทั้ง 3 ฉบับพบว่า **ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564** มีความเหมาะสมในการใช้เป็นหลักเกณฑ์การตรวจสอบ (Audit Criteria) ด้วยเหตุผลดังนี้

- 1) ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เป็นฉบับที่กำหนด กรอบมาตรฐานหลัก 5 ด้าน (Identify, Protect, Detect, Respond, Recover) ตามมาตรฐานสากล NIST CSF 1.1 ไว้อย่างชัดเจน ซึ่งถือเป็นหัวใจสำคัญของการตรวจสอบความปลอดภัยทางไซเบอร์ ในขณะที่มาตรฐานขั้นต่ำฯ 2566 เน้นการแบ่งระดับความสำคัญ และแนวทางการจัดทำประมวลฯ พ.ศ. 2568 เน้นคู่มือเชิงปฏิบัติ

- 2) ประกาศฉบับนี้อาศัยอำนาจตามมาตรา 54 แห่ง พ.ร.บ. ไซเบอร์ฯ 2562 ซึ่งเป็นมาตราหลักที่บังคับให้หน่วยงาน CII ต้องจัดให้มีการตรวจสอบประจำปี ดังนั้น การใช้หลักเกณฑ์จากประกาศที่ออกตามมาตรานี้โดยตรงจึงมีความสอดคล้องทางกฎหมายสูงสุด
- 3) วัตถุประสงค์ของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 คือการจัดให้มีข้อกำหนดขั้นต่ำ เพื่อให้การปฏิบัติงานเป็นไปในทิศทางเดียวกันและสอดคล้องกับมาตรฐานสากล ทำให้ผู้ตรวจประเมินสามารถใช้เป็นตัววัดมาตรฐานในการวัดผลหน่วยงาน CII ทุกแห่งได้อย่างเป็นธรรมและเป็นมาตรฐานเดียวกัน
- 4) สกมช. ได้พัฒนาแบบประเมินสถานภาพการดำเนินงาน (Cyber Readiness) โดยอ้างอิงหัวข้อตามประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 นี้เป็นหลัก ทำให้การตรวจประเมินโดยใช้แนวทางนี้มีความสอดคล้องกับแนวทางการกำกับดูแลของหน่วยงานรัฐที่เป็นปัจจุบัน
- 5) มาตรฐานขั้นต่ำฯ 2566 และแนวทางการจัดทำประมวลฯ พ.ศ. 2568 ต่างพัฒนาขึ้นโดยอ้างอิงฐานข้อมูลจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 (เช่น การนำระดับความสำคัญในมาตรฐานขั้นต่ำฯ 2566 มาบังคับใช้ตามมาตรการที่กำหนดไว้ในประมวลแนวทางปฏิบัติฯ พ.ศ. 2564) ดังนั้น การเข้าใจและใช้ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เป็นแกนกลาง จึงทำให้ครอบคลุมเนื้อหาสำคัญของกฎหมายฉบับอื่นไปในตัว

2.1.2 บทวิเคราะห์เชิงเปรียบเทียบกรอบแนวทาง NIST Cybersecurity Framework กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

NIST Cybersecurity Framework คือ กรอบการทำงานที่แนะนำแนวทางปฏิบัติ (Practices) ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร เป็นกรอบการทำงานที่ออกโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (National Institute of Standards and Technology) หรือ NIST โดยกรอบการทำงานนี้ได้เริ่มต้นประกาศใช้เวอร์ชัน 1.0 ในสหรัฐอเมริกามาตั้งแต่ปี พ.ศ. 2557 และ มีการปรับปรุงเป็นเวอร์ชัน 1.1 เมื่อ 16 เมษายน 2561 กลายเป็นที่นิยมระดับสากลในเวลาต่อมา

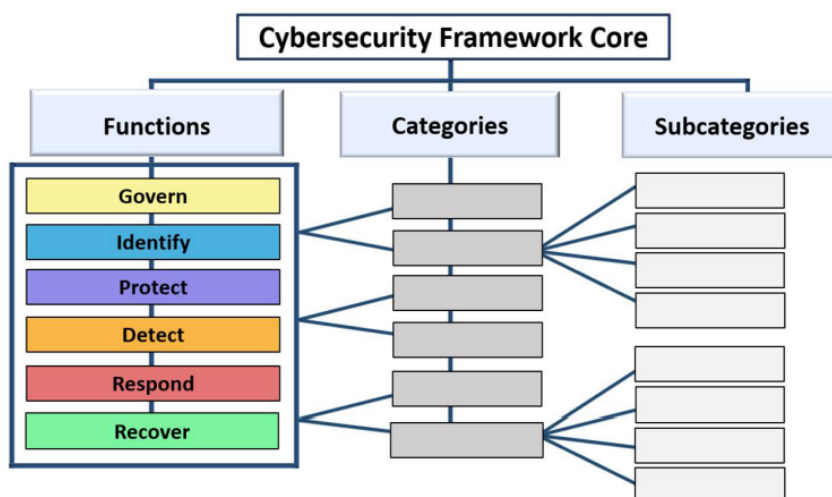
เป้าหมายของ NIST Cybersecurity Framework คือ ต้องการให้องค์กรสามารถตอบสนองและสร้างความยืดหยุ่น (Resilience) ในการรับมือต่อภัยคุกคามที่อาจเกิดขึ้น และที่สำคัญองค์กรต้องทำอย่างต่อเนื่อง โดยกรอบการดำเนินงานนี้จะนำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุด (Best Practice) ของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจสอบ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างต่อเนื่อง ซึ่งแบ่งออกได้เป็น 5 ปัจจัยหลัก ได้แก่ การระบุความเสี่ยง (Identify) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) โดยจะมุ่งเน้นไปที่การวิเคราะห์การดำเนินธุรกิจขององค์กร เพื่อสร้างแนวทางของกิจกรรมและพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยงโดยรวมขององค์กร

ไม่เพียงแต่องค์กรในสหรัฐอเมริกาเท่านั้น กรอบการทำงานที่แนะนำแนวทางปฏิบัติดังกล่าว ยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลก รวมถึงประเทศไทย ที่ได้นำหลักการมาประยุกต์ใช้กับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เพื่อรับมือกับภัยคุกคามไซเบอร์ รวมถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ก็มีกรอบการพัฒนาและเขียนมาจากการยกกรอบการทำงานของ NIST มาใช้อ้างอิง

ปัจจุบัน NIST Cybersecurity Framework เวอร์ชันล่าสุด ได้แก่ เวอร์ชัน 2.0 โดยเผยแพร่ออกมาเมื่อ 24 กุมภาพันธ์ 2567 สำคัญของการปรับปรุงของเวอร์ชัน 2.0 จากเวอร์ชัน 1.1 มีการยกระดับความสำคัญของธรรมาภิบาลผ่านการเพิ่มหน้าที่งานการกำกับดูแล (Govern) ขึ้นเป็นหน้าที่งานหลักลำดับแรก ซึ่งเดิมที่ประเด็นด้านการกำกับดูแลเป็นเพียงส่วนหนึ่งภายใต้ฟังก์ชัน Identify เท่านั้น การเปลี่ยนแปลงนี้มุ่งเน้นให้การจัดการความเสี่ยงด้านไซเบอร์ได้รับความเห็นชอบและการสนับสนุนโดยตรงจากระดับบริหาร รวมถึงมีการบูรณาการการจัดการความเสี่ยงในห่วงโซ่อุปทานเข้าไว้ภายใต้หน้าที่งานการกำกับดูแล เพื่อให้เกิดการบริหารจัดการความเสี่ยงจากคู่ค้าและซัพพลายเออร์เชิงรุกตลอดวงจรชีวิตของผลิตภัณฑ์และบริการ

แกนหลักของกรอบการทำงาน (Framework Core) คือการจัดเตรียมชุดกิจกรรมเพื่อที่จะช่วยในการทำให้ได้ผลลัพธ์ที่เฉพาะเจาะจงทางความมั่นคงปลอดภัยทางไซเบอร์ และอ้างอิงตัวอย่างแนวทางปฏิบัติเพื่อให้ได้ผลลัพธ์ที่ต้องการ องค์ประกอบหลักของแกนหลักของกรอบการทำงานนี้ ประกอบไปด้วย 4 ข้อ ได้แก่

- หน้าที่งาน (Functions) เป็นกลุ่มของกิจกรรมหรือแนวทางที่ต้องปฏิบัติเพื่อให้การจัดการความเสี่ยงด้านความปลอดภัยข้อมูลเป็นไปอย่างมีประสิทธิภาพ
- หมวดหมู่ (Categories) เป็นหน่วยย่อยของหน้าที่งาน ซึ่งจะแบ่งออกเป็นกลุ่มตามประเภทของผลลัพธ์ทางความมั่นคงปลอดภัยทางไซเบอร์ ตัวอย่าง เช่น การบริหารจัดการสินทรัพย์ (Asset Management) และการจัดการตัวตน การยืนยันตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control) โดยจะมีทั้งหมด 22 หมวดหมู่
- หมวดย่อย (Subcategories) เป็นการแบ่งหมวดหมู่ย่อยที่เฉพาะเจาะจงยิ่งขึ้นไม่ว่าจะเป็นการกล่าวถึงกิจกรรมทางเทคนิคหรือการบริหารอย่างละเอียด ตัวอย่างเช่น การป้องกันข้อมูลที่ถูกจัดเก็บ (Data-at-Rest are Protected) และมีการจัดทำ สื่อสาร และบำรุงรักษาการยอมรับความเสี่ยงและความทนทานต่อความเสี่ยง (Risk Appetite and Risk Tolerance Statements are Established, Communicated and Maintained) โดยจะมีทั้งหมด 106 หมวดย่อย
- ข้อมูลอ้างอิง (Informative References) คือส่วนที่ทำการอ้างอิงถึงมาตรฐาน แนวปฏิบัติ และคำแนะนำด้านความมั่นคงปลอดภัยไซเบอร์อื่น ๆ ที่สัมพันธ์กับผลลัพธ์ที่เกี่ยวข้องกับแต่ละหมวดย่อย



รูปที่ 2 โครงสร้างหลักของกรอบการทำงาน NIST Cybersecurity Framework 2.0¹

¹ NIST Cybersecurity Framework version 2.0, 2567

2.1.2.1 ความสอดคล้องของ NIST CSF 1.1 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มีกรอบการพัฒนาและอ้างอิงมาจากแนวทางของ NIST Cybersecurity Framework เวอร์ชัน 1.1 โดยโครงสร้างหลัก 5 ด้านของไทย (Identify, Protect, Detect, Respond, Recover) ตรงกับหน้าที่งาน (Functions) ของกรอบ NIST จากการศึกษาพบว่าข้อกำหนดในประมวลแนวทางปฏิบัติฯ มีความสอดคล้องกับหน้าที่งานของ NIST CSF 1.1 อย่างชัดเจน เพื่อใช้เป็นเกณฑ์ขั้นต่ำในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ โดยสามารถสรุปความสอดคล้องของ NIST CSF 1.1 และประมวลแนวทางปฏิบัติ พ.ศ. 2564 ได้ดังนี้

ตารางที่ 5 ความสอดคล้องของ NIST CSF 1.1 และประมวลแนวทางปฏิบัติ พ.ศ. 2564

NIST CSF 1.1 Functions	ประมวลแนวทางปฏิบัติ พ.ศ. 2564
Identify	17.1, 17.2, 17.3, 17.4, 17.5, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 21.1.1, 21.1.2, 21.1.3, 21.1.4, 21.2.1, 21.2.2, 21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.7, 21.3.8, 21.3.10, 21.4.1, 21.4.2, 21.4.3, 21.4.4, 22.5.1, 22.6, 24.2.2
Protect	18.1, 19.1, 19.2, 19.3, 19.4, 21.1.3, 21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.6, 21.3.9, 22.1.1, 22.1.2, 22.1.4, 22.2.1, 22.2.2, 22.2.3, 22.2.4, 22.2.5, 22.3.1, 22.3.2, 22.4.1, 22.4.2, 22.5.1, 23.1.1, 23.1.2, 24.1.1, 24.2.1, 24.3.1, 24.3.2, 25.1.1, 25.1.2
Detect	18.1, 19.1, 19.2, 21.1.2, 21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.6, 21.3.7, 21.3.8, 21.3.9, 21.4.2, 21.4.3, 22.1.3, 23.1.1, 24.1.1, 24.2.4, 24.3.1, 24.3.2, 25.1.2
Response	17.3, 17.5, 18.2, 19.1, 19.2, 19.3, 19.4, 21.2.2, 21.3.9, 22.5.1, 22.6, 23.1.2, 24.1.1, 24.2.1, 24.2.2, 24.2.3, 25.1.1
Recover	19.1, 19.2, 19.3, 19.4, 23.1.2, 24.1.1, 24.2.1, 25.1.1

ทั้งนี้ รายละเอียดของความเชื่อมโยงระหว่าง NIST CSF 1.1 และประมวลแนวทางปฏิบัติ พ.ศ. 2564 แสดงใน ภาคผนวก ง. การเปรียบเทียบประมวลแนวทางปฏิบัติ พ.ศ. 2564 และมาตรฐานสากล

2.1.2.2 ความสอดคล้องของ NIST CSF 2.0 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ในภาพรวม ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 มีรากฐานการพัฒนาที่สอดคล้องกับ NIST CSF 2.0 ในระดับสูงมาก ทั้งในเชิงเทคนิคและการบริหารจัดการ โดยพบมาตรการที่มีความเชื่อมโยงกันอย่างชัดเจน อาทิ การป้องกัน (Protect) ผ่านกลไกการพิสูจน์ตัวตนและการบริหารจัดการสิทธิ์การใช้งานที่มีความเข้มงวด ควบคู่ไปกับการยกระดับความมั่นคงปลอดภัยของระบบและข้อมูล การตรวจจับ (Detect) ภัยคุกคามผ่านระบบเฝ้าระวัง และการวิเคราะห์เหตุการณ์ที่ผิดปกติอย่างต่อเนื่อง ซึ่งถือเป็นหัวใจสำคัญในการตอบสนองต่อภัยไซเบอร์ได้อย่างทันท่วงที นอกจากนี้ ในด้านการบริหารจัดการความต่อเนื่อง ประมวลแนวทางปฏิบัติฯ ยังครอบคลุมถึงการจัดทำแผนเผชิญเหตุและแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ซึ่งบูรณาการหลักการในหมวด Respond (RS) และ Recover (RC) ของ NIST CSF 2.0 ไว้อย่างครบถ้วน

จากการศึกษาพบว่า ทุกข้อกำหนดในประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 สามารถเชื่อมโยงย้อนกลับไปยังหมวดหมู่ของ NIST CSF 2.0 ได้ครบทุกหัวข้อ ซึ่งเป็นการยืนยันว่าการปฏิบัติตามกฎหมายของประเทศ เป็นการดำเนินงานบนมาตรฐานความมั่นคงปลอดภัยระดับสากล อย่างไรก็ตาม แม้จะมีความสอดคล้องในเชิงหลักการ แต่ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ได้มีการขยายรายละเอียดข้อกำหนดเชิงเทคนิคและบริบทเฉพาะทางเพื่อให้เหมาะสมกับสถานะแวดล้อมและการบังคับใช้กฎหมายภายในประเทศ ดังนั้น หน่วยงานที่ยึดถือการปฏิบัติตามมาตรฐาน NIST CSF 2.0 เป็นหลัก จึงยังคงมีความจำเป็นต้องพิจารณารายละเอียดส่วนเพิ่มและปรับปรุงการดำเนินงานให้เป็นไปตามเกณฑ์เฉพาะที่ระบุไว้ในประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เพื่อให้เกิดความสอดคล้องทางกฎหมายและมาตรฐานความมั่นคงปลอดภัยในระดับสากลไปพร้อมกัน

ตารางที่ 6 ความสอดคล้องของ NIST CSF 2.0 และประมวลแนวทางปฏิบัติ พ.ศ. 2564

NIST CSF 2.0 Functions	ประมวลแนวทางปฏิบัติ พ.ศ. 2564
Govern	17.1, 17.2, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 21.2.1, 21.3.7, 21.3.8, 21.3.10, 21.4.1, 21.4.2, 21.4.3, 21.4.4, 22.5.1, 24.2.2, 24.3.2, 25.1.1
Identify	17.3, 17.5, 18.1, 18.2, 19.1, 19.2, 19.3, 19.4, 22.6, 21.1.1, 21.1.2, 21.1.3, 21.1.4, 21.2.1, 21.2.2, 21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.6, 21.3.9, 21.4.2, 21.4.3, 22.2.3, 22.2.4, 22.2.5, 22.5.2, 23.1.2, 24.1.1, 24.2.1, 24.2.4, 24.3.1, 24.3.2, 25.1.1, 25.1.2
Protect	22.1.1, 22.1.2, 22.1.4, 22.2.1, 22.2.2, 22.2.3, 22.2.4, 22.3.1, 22.3.2, 22.4.1, 22.4.2, 22.5.1, 24.3.1
Detect	21.4.3, 22.1.3, 23.1.1
Response	19.1, 22.6, 24.2.2, 24.2.3
Recover	25.1.1

ทั้งนี้ รายละเอียดของความเชื่อมโยงระหว่าง NIST CSF 2.0 และประมวลแนวทางปฏิบัติ พ.ศ. 2564 แสดงใน ภาคผนวก ง. การเปรียบเทียบประมวลแนวทางปฏิบัติ พ.ศ. 2564 และมาตรฐานสากล

2.1.2.3 ความแตกต่างของ NIST CSF 2.0 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

จุดแตกต่างที่พบส่วนใหญ่เกิดจากลักษณะของเอกสารที่ต่างกัน โดยประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ของไทยมีสถานะเป็นข้อกำหนดทางกฎหมายที่มีสภาพบังคับ (Mandatory) ในขณะที่ NIST CSF เป็นเพียงกรอบแนวทางปฏิบัติแบบสมัครใจ (Voluntary) ส่งผลให้มีความแตกต่างในรายละเอียดบางประการ เช่น หน้าที่ในการรายงานอุบัติการณ์ต่อหน่วยงานกำกับดูแลของรัฐซึ่งเป็นข้อบังคับตามกฎหมายไทย แต่ไม่มีระบุเฉพาะเจาะจงใน NIST โดยต้องมีการรายงานดังนี้

- หน่วยงานต้องส่งรายงานผลการตรวจสอบ (Audit Report) ให้กับ สกมช. และหน่วยงานกำกับดูแลภายใน 30 วัน
- หน่วยงานต้องกำหนดโครงสร้างการรายงานเหตุการณ์ให้เป็นไปตามภาระหน้าที่ภายใต้ พ.ร.บ. ไซเบอร์ฯ
- หน่วยงานต้องส่งสำเนารายงานผลการทดสอบเจาะระบบ (Penetration Testing) และการให้ข้อมูลตามคำขอใด ๆ แก่คณะกรรมการหรือ สกมช. เมื่อได้รับการร้องขอ

นอกจากนี้ ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ยังได้มีการขยายความรายละเอียดเชิงเทคนิคมากกว่า NIST CSF เพื่อให้เหมาะสมกับสภาวะแวดล้อมทางเทคโนโลยีและระดับความพร้อมของหน่วยงานในประเทศ โดยมีการกำหนดเกณฑ์เฉพาะเจาะจงที่ NIST CSF อาจจะละไว้ในฐานะแนวทางปฏิบัติทั่วไป ทั้งนี้ เพื่อยกระดับการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับมาตรฐานสากลยุคใหม่ จึงควรพิจารณาปรับปรุงและเพิ่มมาตรการจาก NIST CSF 2.0 เข้าไปในรายการตรวจประเมิน ดังนี้

ตารางที่ 7 Subcategory ใน NIST CSF 2.0 ที่แตกต่างกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ฟังก์ชัน	Subcategory ใน NIST CSF 2.0
Governance (GV) – การกำกับดูแล	- GV.RR-01: ผู้นำองค์กรมีหน้าที่รับผิดชอบและพร้อมรับผิดชอบต่อความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงส่งเสริมวัฒนธรรมที่ตระหนักถึงความเสี่ยง มีจริยธรรม และมีการปรับปรุงอย่างต่อเนื่อง - GV.OV-01: ผลลัพธ์ของกลยุทธ์การบริหารจัดการความเสี่ยงไซเบอร์จะได้รับการทบทวน เพื่อใช้เป็นข้อมูลในการแจ้งและปรับเปลี่ยนกลยุทธ์ รวมถึงทิศทางขององค์กร - GV.OV-02: กลยุทธ์การบริหารจัดการความเสี่ยงไซเบอร์ได้รับการทบทวนและปรับปรุง เพื่อให้มั่นใจว่าครอบคลุมข้อกำหนดและความเสี่ยงขององค์กร - GV.OV-03: ผลการดำเนินงานด้านการบริหารจัดการความเสี่ยงไซเบอร์ขององค์กรได้รับการประเมินและทบทวน เพื่อพิจารณาการปรับเปลี่ยนที่จำเป็น - GV.RM-07: โอกาสในเชิงกลยุทธ์ (นั่นคือ ความเสี่ยงในเชิงบวก) ได้รับการระบุลักษณะและถูกรวมเข้าไว้ในการหารือด้านความเสี่ยงไซเบอร์ขององค์กร - GV.SC-01: มีการจัดตั้งและได้รับความเห็นชอบจากผู้มีส่วนได้ส่วนเสียในองค์กร สำหรับโปรแกรม กลยุทธ์ วัตถุประสงค์ นโยบาย และกระบวนการบริหารจัดการความเสี่ยงในห่วงโซ่อุปทานด้านความมั่นคงปลอดภัยไซเบอร์
Protect (PR) – การป้องกัน	- PR.AA-01: องค์กรมีการจัดการอัตลักษณ์ (Identities) และข้อมูลประจำตัว (Credentials) สำหรับผู้ใช้งาน บริการ และฮาร์ดแวร์ที่ได้รับอนุญาต - PR.AA-02: อัตลักษณ์ได้รับการพิสูจน์และเชื่อมโยงกับข้อมูลประจำตัวโดยพิจารณาตามบริบทของการปฏิสัมพันธ์ - PR.DS-01: ข้อมูลที่จัดเก็บอยู่กับที่ (Data-at-rest) ได้รับการคุ้มครองทั้งในด้านความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) - PR.DS-02: ข้อมูลที่อยู่ระหว่างการส่ง (Data-in-transit) ได้รับการคุ้มครองทั้งในด้านความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน - PR.DS-10: ข้อมูลที่กำลังถูกใช้งาน (Data-in-use) ได้รับการคุ้มครองทั้งในด้านความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน - PR.DS-11: ข้อมูลสำรองได้รับการสร้างขึ้น คุ้มครอง ดูแลรักษา และทดสอบการใช้งาน - PR.PS-02: ซอฟต์แวร์ได้รับการบำรุงรักษา เปลี่ยนแทน และลบทิ้งตามระดับความเสี่ยง

ฟังก์ชัน	Subcategory ใน NIST CSF 2.0
	- PR.PS-03: ฮาร์ดแวร์ได้รับการบำรุงรักษา เปลี่ยนแทน และลบทิ้งตามระดับความเสี่ยง - PR.PS-04: บันทึกเหตุการณ์ (Log records) ถูกสร้างขึ้นและพร้อมใช้งานสำหรับการตรวจสอบอย่างต่อเนื่อง - PR.PS-05: ป้องกันการติดตั้งและการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาต - PR.PS-06: แนวปฏิบัติการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development) ถูกรวมเข้าเป็นส่วนหนึ่งของกระบวนการ และมีการตรวจสอบประสิทธิภาพตลอดวงจรชีวิตการพัฒนาซอฟต์แวร์ - PR.IR-02: ทรัพย์สินทางเทคโนโลยีขององค์กรได้รับการปกป้องจากภัยคุกคามทางสภาพแวดล้อม - PR.IR-03: กลไกต่าง ๆ ถูกนำมาใช้เพื่อให้บรรลุข้อกำหนดด้านความยืดหยุ่น (Resilience) ทั้งในสถานการณ์ปกติและสถานการณ์ที่เลวร้าย - PR.IR-04: มีการรักษาขีดความสามารถของทรัพยากรที่เพียงพอเพื่อให้มั่นใจในความพร้อมใช้งาน
Detect (DE) – การตรวจจับ	- DE.AE-02: เหตุการณ์ที่อาจส่งผลเสียได้รับการวิเคราะห์เพื่อให้เข้าใจกิจกรรมที่เกี่ยวข้องได้ดียิ่งขึ้น - DE.AE-03: ข้อมูลจากหลายแหล่งได้รับการวิเคราะห์ความสัมพันธ์ (Correlated) ร่วมกัน - DE.AE-04: มีความเข้าใจถึงผลกระทบและขอบเขตที่คาดการณ์ไว้ของเหตุการณ์ที่ส่งผลเสีย - DE.AE-06: ข้อมูลเกี่ยวกับเหตุการณ์ที่ส่งผลเสียถูกส่งต่อไปยังเจ้าหน้าที่และเครื่องมือที่ได้รับอนุญาต - DE.AE-07: ข้อมูลข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) และข้อมูลบริบทอื่น ๆ ถูกนำมาบูรณาการในการวิเคราะห์ - DE.AE-08: การประกาศว่าเป็น "อุบัติการณ์" (Incidents) จะทำเมื่อเหตุการณ์ที่ส่งผลเสียนั้นตรงตามเกณฑ์อุบัติการณ์ที่กำหนดไว้
Respond (RS) – การตอบสนอง	- RS.AN-03: ดำเนินการวิเคราะห์เพื่อระบุว่ามีอะไรเกิดขึ้นบ้างในระหว่างเกิดอุบัติการณ์ และหาสาเหตุที่แท้จริง (Root cause) ของอุบัติการณ์นั้น - RS.AN-06: กิจกรรมที่ดำเนินการระหว่างการสืบสวนจะถูกบันทึกไว้ และมีการรักษาความถูกต้องครบถ้วนรวมถึงแหล่งที่มาของบันทึกเหล่านั้น - RS.AN-07: ข้อมูลอุบัติการณ์และข้อมูลอธิบายข้อมูล (Metadata) ถูกรวบรวมไว้ โดยมีการรักษาความถูกต้องครบถ้วนและแหล่งที่มา - RS.AN-08: มีการประเมินและตรวจสอบยืนยันขนาดความรุนแรงของอุบัติการณ์ - RS.MI-01: อุบัติการณ์ได้รับการควบคุมขอบเขต (Contained) - RS.MI-02: อุบัติการณ์ได้รับการกำจัดให้หมดไป (Eradicated)

ฟังก์ชัน	Subcategory ใน NIST CSF 2.0
Recover (RC) – การฟื้นฟู	• RC.RP-01: ส่วนการฟื้นฟูของแผนตอบสนองต่ออุบัติการณ์ได้รับการปฏิบัติเมื่อมีการเริ่มกระบวนการตอบสนองต่ออุบัติการณ์ • RC.RP-02: การดำเนินการฟื้นฟูได้รับการเลือก กำหนดขอบเขต จัดลำดับความสำคัญ และลงมือปฏิบัติ • RC.RP-03: ความถูกต้องครบถ้วนของข้อมูลสำรองและทรัพย์สินเพื่อการคืนสภาพอื่น ๆ ได้รับการตรวจสอบยืนยันก่อนนำไปใช้ในการฟื้นฟู • RC.RP-04: มีการนำหน้าที่ทางพันธกิจที่สำคัญและการบริหารความเสี่ยงไซเบอร์มาพิจารณาเพื่อกำหนดบรรทัดฐานการดำเนินงานหลังเกิดอุบัติการณ์ • RC.RP-05: ตรวจสอบยืนยันความถูกต้องครบถ้วนของทรัพย์สินที่ได้รับการฟื้นฟู ระบบและบริการต่าง ๆ กลับมาใช้งานได้ และยืนยันสถานะการดำเนินงานที่ปกติ • RC.RP-06: มีการประกาศสิ้นสุดการฟื้นฟูอุบัติการณ์ตามเกณฑ์ที่กำหนด และจัดทำเอกสารที่เกี่ยวข้องกับอุบัติการณ์ให้ครบถ้วน • RC.CO-03: กิจกรรมการฟื้นฟูและความคืบหน้าในการกู้คืนขีดความสามารถในการดำเนินงานได้รับการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่ได้รับมอบหมาย • RC.CO-04: ข้อมูลอัปเดตสาธารณะเกี่ยวกับการฟื้นฟูอุบัติการณ์ได้รับการเผยแพร่โดยใช้วิธีการและข้อความที่ได้รับอนุมัติ

2.1.2.4 ข้อเสนอแนะในการจัดทำหลักเกณฑ์การตรวจประเมินฯ

เพื่อให้การจัดทำหลักเกณฑ์การตรวจประเมินฯ มีความสมบูรณ์ ทั้งในแง่ของการปฏิบัติตามกฎหมาย และการรักษาความมั่นคงปลอดภัยในระดับสากล หน่วยงานควรพิจารณากำหนดหัวข้อการตรวจประเมินเพิ่มเติมจากฐานเดิมของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยอ้างอิงองค์ประกอบใหม่จาก NIST CSF 2.0 ดังนี้

ตารางที่ 8 ข้อเสนอแนะในการจัดทำหัวข้อการตรวจประเมินเพิ่มเติม อ้างอิงตาม NIST CSF 2.0

ลำดับ	รายละเอียด	NIST CSF 2.0	ข้ออ้างอิง (หลักเกณฑ์ฯ)
ข้อที่ 1	ความรับผิดชอบของผู้นำองค์กรและการส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์	GV.RR-01	3.2.1
ข้อที่ 2	การกำกับดูแล การทบทวน และการปรับปรุงกลยุทธ์และผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์	GV.OV-01 GV.OV-02 GV.OV-03 GV.RM-07	3.2.2

ลำดับ	รายละเอียด	NIST CSF 2.0	ข้ออ้างอิง (หลักเกณฑ์ฯ)
ข้อที่ 3	การจัดทำนโยบายและกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์ของห่วงโซ่อุปทาน	GV.SC-01	3.2.3
ข้อที่ 4	การจัดการบัญชีผู้ใช้	PR.AA-01 PR.AA-02	3.2.4
ข้อที่ 5	การรักษาความมั่นคงปลอดภัยของข้อมูล	PR.DS-01 PR.DS-02 PR.DS-10 PR.DS-11	3.2.5
ข้อที่ 6	1. การจัดการแพตช์	PR.PS-02	3.2.6
	2. การจัดการซอฟต์แวร์	PR.PS-02 PR.PS-05	3.2.7
	3. การจัดการฮาร์ดแวร์	PR.PS-03	3.2.8
	4. การจัดการบันทึกเหตุการณ์	PR.PS-04	3.2.9
	5. การพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย	PR.PS-06	3.2.10
ข้อที่ 7	การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี	PR.IR-02 PR.IR-03 PR.IR-04	3.2.11
ข้อที่ 8	การวิเคราะห์เหตุการณ์ไม่พึงประสงค์	DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-07 DE.AE-08	3.2.12
ข้อที่ 9	การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์	RS.AN-03 RS.AN-06 RS.AN-07 RS.AN-08	3.2.13
ข้อที่ 10	การบรรเทาเหตุภัยคุกคามทางไซเบอร์	RS.MI-01 RS.MI-02	3.2.14
ข้อที่ 11	1. การจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์	RC.RP-02	3.2.15
	2. การทดสอบ ทบทวน และปรับปรุงแผน	RC.RP-04	3.2.16
	3. การดำเนินการตามแผนฟื้นฟูจากเหตุจริง	RC.RP-01 RC.RP-03	3.2.17

ลำดับ	รายละเอียด	NIST CSF 2.0	ข้ออ้างอิง (หลักเกณฑ์ฯ)
ข้อที่ 12		RC.RP-05 RC.RP-06	
	4. แผนการสำรองข้อมูล	PR.DS-11	3.2.18
	การสื่อสารระหว่างหน่วยงานที่เผชิญเหตุภัยคุกคามทางไซเบอร์	RC.CO-03 RC.CO-04	3.2.19

2.1.3 บทวิเคราะห์เชิงเปรียบเทียบกลุ่มมาตรฐาน ISO/IEC 27000 family กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มาตรฐานกลุ่ม ISO/IEC 27000 ถือเป็นบรรทัดฐานสากลที่สำคัญในการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งเกิดจากความร่วมมือของสององค์กรระดับโลก คือ ISO และ IEC โดยมีการจัดตั้งคณะกรรมการวิชาการร่วมคือ ISO/IEC JTC 1 และคณะอนุกรรมการ SC 27 ที่รับผิดชอบในการร่างและพัฒนามาตรฐานด้าน Information Security, Cybersecurity และ Privacy Protection โดยเฉพาะ

มาตรฐาน ISO/IEC 27001 พัฒนามาจากมาตรฐานแห่งชาติของสหราชอาณาจักร คือ BS 7799 ซึ่งสถาบันมาตรฐานอังกฤษ (BSI) ได้เริ่มพัฒนาขึ้นในปี ค.ศ.1995 เพื่อคุ้มครองข้อมูลที่สำคัญ ต่อมาในปี ค.ศ. 2000 องค์กร ISO ได้รับเอาเนื้อหาในส่วนของแนวทางปฏิบัติ (Code of Practice) มาประกาศเป็น ISO/IEC 17799 และท้ายที่สุดได้พัฒนาส่วนของข้อกำหนดระบบการจัดการ (Requirements) เป็นมาตรฐานสากลในชื่อ ISO/IEC 27001:2005 อันเป็นรากฐานสำคัญให้แก่มาตรฐานเฉพาะด้านอื่น ๆ ในเวลาต่อมา

ปัจจุบัน มาตรฐานในตระกูลนี้ได้ขยายขอบเขตเพื่อให้ครอบคลุมบริบทดิจิทัลสมัยใหม่ อาทิ ISO/IEC 27701 ซึ่งเป็นส่วนขยายด้านการจัดการข้อมูลส่วนบุคคล (PIMS) เพื่อสนับสนุนการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น GDPR หรือ PDPA ของไทย และ ISO/IEC 27017 ที่ให้แนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยบนระบบคลาวด์ (Cloud Security) โดยเฉพาะ ซึ่งมาตรฐานเหล่านี้ล้วนเป็นองค์ประกอบสำคัญที่องค์กรสามารถนำมาประยุกต์ใช้เพื่อให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดไว้

1) ISO/IEC 27001

มาตรฐาน ISO/IEC 27001 ประกาศใช้ครั้งแรกในปี ค.ศ. 2005 และได้มีการปรับปรุงมาโดยตลอด โดยแบ่งออกเป็น 3 ระยะ ได้แก่

1. **ISO/IEC 27001:2005** มาตรฐานจะมุ่งเน้นการสร้างระบบการจัดการตามวงจร PDCA (Plan-Do-Check-Act) โดยให้ความสำคัญกับการควบคุมเชิงกระบวนการที่ชัดเจนและต่อเนื่อง เพื่อสร้างความเชื่อมั่นว่าองค์กรมีระบบการตรวจสอบที่เข้มงวด
2. **ISO/IEC 27001:2013** เกิดการปฏิรูปโครงสร้างเข้าสู่ Annex SL (High-Level Structure) เพื่อให้มาตรฐานนี้สามารถบูรณาการร่วมกับมาตรฐานการจัดการอื่นได้ ในเวอร์ชันนี้ได้เปลี่ยนจุดเน้นจากการบังคับตามขั้นตอน (Prescriptive) ไปสู่การบริหารความเสี่ยง (Risk-based) โดยให้องค์กรประเมินความเสี่ยงตามบริบทเฉพาะของตนเอง
3. **ISO/IEC 27001:2022** เป็นเวอร์ชันปัจจุบันที่ปรับปรุงเพื่อรับมือกับภัยคุกคามในยุค Digital Transformation มีการปรับโครงสร้างมาตรการควบคุม (Annex A) ใหม่ทั้งหมด โดยรวมการจัดการด้าน Cybersecurity และ Data Privacy เข้ามาเป็นเนื้อเดียวกัน พร้อมทั้งนำระบบ Attributes

(Tagging) มาใช้เพื่อให้ผู้ปฏิบัติงานสามารถเลือกใช้มาตรการควบคุมได้อย่างยืดหยุ่นและสอดคล้อง
กับภัยคุกคามสมัยใหม่ เช่น Cloud Services, Threat Intelligence และ Data Masking

ข้อกำหนดหลัก (Main Clauses 0-10)

มาตรฐาน ISO/IEC 27001:2022 จะมีข้อกำหนดหลักเป็นส่วนที่ระบุว่าเป็นข้อบังคับ (Mandatory Requirements) ที่องค์กรต้องปฏิบัติตามเพื่อขอรับการรับรอง ประกอบด้วย 11 ข้อหลัก ได้แก่

- **Clause 0-3** บทนำ ขอบข่าย การอ้างอิง และคำนิยาม (Introductory sections)
- **Clause 4 Context of the Organization** การวิเคราะห์บริบทองค์กรและความต้องการของผู้มีส่วนได้ส่วนเสีย
- **Clause 5 Leadership** บทบาทและความมุ่งมั่นของผู้บริหารระดับสูง และการกำหนดนโยบาย
- **Clause 6 Planning** การประเมินความเสี่ยง (Risk Assessment) และการวางแผนจัดการความเสี่ยง (Risk Treatment)
- **Clause 7 Support** การจัดการทรัพยากร สมรรถนะ ความตระหนัก และการจัดการเอกสารสารสนเทศ
- **Clause 8 Operation** การนำแผนไปปฏิบัติจริงและการควบคุมกระบวนการ
- **Clause 9 Performance Evaluation** การเฝ้าระวัง การวัดผล การตรวจประเมินภายใน (Internal Audit) และการทบทวนโดยฝ่ายบริหาร
- **Clause 10 Improvement** การจัดการข้อบกพร่อง (Non-conformity) และการปรับปรุงอย่างต่อเนื่อง

ภาคผนวก (Annexes)

มาตรฐาน ISO/IEC 27001:2022 มีมาตรการควบคุมในภาคผนวก (Annex A Controls) โดยในเวอร์ชัน 2022 มีการเปลี่ยนแปลงโครงสร้างจากเดิมที่แบ่งตามโดเมน และมีจำนวน 114 ข้อ มาเป็นการแบ่งตามกลุ่ม (Themes) และมีจำนวนทั้งหมด 93 ข้อ เพื่อให้เกิดความคล่องตัวและลดความซ้ำซ้อน โดยสรุปสาระสำคัญหลักได้ดังนี้

ตารางที่ 9 สรุปมาตรการควบคุมตามมาตรฐาน ISO/IEC 27001:2022

กลุ่ม (Theme)	จำนวนมาตรการ	ตัวอย่างมาตรการควบคุม
A.5 Organizational Controls	37 ข้อ	นโยบายความมั่นคงปลอดภัย, การจัดลำดับความสำคัญของสินทรัพย์, Cloud Services
A.6 People Controls	8 ข้อ	การตรวจสอบประวัติ, ข้อตกลงการรักษาความลับ, การอบรมความตระหนัก
A.7 Physical Controls	14 ข้อ	การรักษาความปลอดภัยพื้นที่, การป้องกันอุปกรณ์, การกำจัดทำลายสื่อ
A.8 Technological Controls	34 ข้อ	การเข้ารหัส (Encryption), การสำรองข้อมูล, การป้องกันมัลแวร์

หน่วยงานที่ต้องการขอรับรองมาตรฐาน ISO/IEC 27001:2022 หากได้มีการดำเนินการตามข้อกำหนดหลัก 4 – 10 แล้ว แล้วนั้น ยังคงจำเป็นต้องพัฒนามาตรการควบคุมในส่วนของ Annex A เพื่อให้ครบถ้วนและเพียงพอสำหรับการขอการรับรอง

2) ISO/IEC 27701

มาตรฐาน ISO/IEC 27701 ประกาศใช้ครั้งแรกในปี ค.ศ. 2019 ในฐานะมาตรฐานส่วนขยาย (Extension) ของ ISO/IEC 27001 และ 27002 โดยมีหัวใจสำคัญในการยกระดับระบบ ISMS (Information Security Management System) ให้กลายเป็น PIMS (Privacy Information Management System) ISO/IEC 27701 เวอร์ชัน 2019 ถูกออกแบบมาภายใต้โครงสร้าง Annex SL เช่นเดียวกับ ISO/IEC 27001:2013 ทำให้องค์กรสามารถผนวกข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล เข้ากับระบบบริหารจัดการเดิมที่มีอยู่ได้ทันที โดยมี การเพิ่มข้อกำหนดเฉพาะใน Clause 4 ถึง Clause 10 เพื่อให้ครอบคลุมมิติของความเป็นส่วนตัว (Privacy) เพิ่มเติมจากมิติความมั่นคงปลอดภัย (Security)

มาตรฐานนี้ได้กำหนดบทบาทที่ชัดเจนตามบริบทขององค์กร โดยแบ่งข้อกำหนดออกเป็น 2 ส่วนหลัก เพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น GDPR หรือ PDPA) ได้แก่

- **ผู้ควบคุมข้อมูล (PII Controllers)** เน้นเรื่องสิทธิของเจ้าของข้อมูล (Data Subject Rights), การแจ้ง วัตถุประสงค์ (Privacy Notice), และความยินยอม (Consent)
- **ผู้ประมวลผลข้อมูล (PII Processors)** เน้นเรื่องการปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล, การจำกัดการ ส่งต่อข้อมูล, และความปลอดภัยในการประมวลผล

ปัจจุบันมาตรฐาน ISO/IEC 27701 เวอร์ชันล่าสุด ได้แก่ ISO/IEC 27701:2025 ซึ่งมีการปรับปรุง โครงสร้าง (Mapping) ให้เข้ากับ ISO/IEC 27001:2022 โดยเปลี่ยนจากการอ้างอิง 14 โดเมนมาเป็นการอ้างอิง ผ่าน 4 กลุ่ม (Organizational, People, Physical, Technological) และลดจำนวนมาตรการควบคุมเหลือ 93 ข้อตามมาตรฐาน ISO/IEC 27001:2022

ข้อกำหนดหลัก (Main Clauses 0-10)

มาตรฐาน ISO/IEC 27701:2025 จะมีข้อกำหนดหลักเป็นส่วนที่ระบุว่าเป็นข้อบังคับ (Mandatory Requirements) ที่องค์กรต้องปฏิบัติตามเพื่อขอรับการรับรอง ประกอบด้วย 11 ข้อหลัก ได้แก่

- **Clause 0-3** บทนำ, ขอบข่าย, การอ้างอิง และคำนิยาม (Introductory sections)
- **Clause 4 Context of the Organization** การทำความเข้าใจองค์กรและบริบท, การระบุ ความต้องการของผู้มีส่วนได้ส่วนเสีย, และการกำหนดขอบเขตของ PIMS รวมถึงบทบาทของ องค์กรว่าเป็นผู้ควบคุมข้อมูล (PII Controller) หรือผู้ประมวลผลข้อมูล (PII Processor)
- **Clause 5 Leadership** ความมุ่งมั่นของผู้บริหารระดับสูง, การกำหนดนโยบายความเป็นส่วนตัว (Privacy policy), และการกำหนดบทบาท ความรับผิดชอบ และอำนาจหน้าที่
- **Clause 6 Planning** การจัดการความเสี่ยงและโอกาส, กระบวนการประเมินความเสี่ยงด้าน ความเป็นส่วนตัว (Privacy risk assessment), กระบวนการจัดการความเสี่ยง, และการกำหนด วัตถุประสงค์ด้านความเป็นส่วนตัว
- **Clause 7 Support** การจัดการทรัพยากร สมรรถนะ ความตระหนัก และการจัดการเอกสาร สารสนเทศ
- **Clause 8 Operation** การนำแผนไปปฏิบัติจริงและการควบคุมกระบวนการ

- **Clause 9 Performance Evaluation** การเฝ้าระวัง การวัดผล การตรวจประเมินภายใน (Internal Audit) และการทบทวนโดยฝ่ายบริหาร
- **Clause 10 Improvement** การจัดการข้อบกพร่อง (Non-conformity) และการปรับปรุงอย่างต่อเนื่อง

ภาคผนวก (Annexes)

ภาคผนวกที่เป็นข้อกำหนดบังคับ (Normative) ของมาตรฐาน ISO/IEC 27701 มีดังนี้

- **Annex A (ข้อบังคับ - Normative)** สรุปลักษณะประสงค์และมาตรการควบคุมอ้างอิงของ PIMS (Reference control objectives and controls) โดยแบ่งออกเป็น 3 ส่วน ได้แก่
 - A.1 มาตรการสำหรับผู้ควบคุมข้อมูล (PII controllers) 31 ข้อ
 - A.2 มาตรการสำหรับผู้ประมวลผลข้อมูล (PII processors) 18 ข้อ
 - A.3 มาตรการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับทั้งสองบทบาท 29 ข้อมาตรฐาน ISO/IEC 27701:2025 จะมีเฉพาะข้อกำหนด 78 ข้อที่เจาะจงกับข้อมูลส่วนบุคคล (Privacy/PII) เท่านั้น ส่วนเรื่องความปลอดภัยพื้นฐานขององค์กรในมิติอื่น ๆ ตามมาตรการควบคุมของ ISO/IEC 27001:2022 ได้ถูกจัดเป็นมาตรฐานตามโปรแกรมความมั่นคงปลอดภัยสารสนเทศที่องค์กรต้องดำเนินการควบคุมอยู่แล้ว โดยเป็นไปตามข้อกำหนด CL.6.1.3
- **Annex B (ข้อบังคับ - Normative)** แนวทางในการนำมาตรการควบคุมไปปฏิบัติ (Implementation guidance) โดยให้รายละเอียดเชิงลึกของแต่ละมาตรการใน Annex A แยกเป็นแนวทางสำหรับ PII controllers, PII processors และแนวทางด้านความปลอดภัยสารสนเทศที่ใช้ร่วมกัน

หน่วยงานที่ต้องการขอรับรองมาตรฐาน ISO/IEC 27701:2025 หากได้มีการดำเนินการตามมาตรฐาน ISO/IEC 27001:2022 แล้วนั้น ยังคงจำเป็นต้องพิจารณามาตรการควบคุมเพิ่มเติมในส่วนของ Annex A.1, Annex A.2 และ Annex A.3 เพิ่มเติม เพื่อให้ครบถ้วนและเพียงพอสำหรับการขอการรับรอง

3) ISO/IEC 27017

มาตรฐาน ISO/IEC 27017 ประกาศใช้ครั้งแรกในปี ค.ศ. 2015 โดยมีฐานะเป็น Code of Practice หรือแนวทางปฏิบัติที่ขยายความจาก ISO/IEC 27002 เพื่อให้การประยุกต์ใช้มาตรการควบคุมความปลอดภัย (Controls) ในสภาพแวดล้อมคลาวด์มีความชัดเจนและเป็นรูปธรรมมากขึ้น โดยได้เพิ่มรายละเอียดวิธีการปฏิบัติ (Implementation Guidance) ให้กับมาตรการเดิมใน Annex A อีก 37 ข้อ เพื่อให้ตอบโจทย์ความเสี่ยงเฉพาะของคลาวด์ เช่น การจัดการสิทธิ์การเข้าถึงของผู้ให้บริการ (Provider) และการสำรองข้อมูลข้ามภูมิภาค และมีการกำหนดเพิ่มเข้ามาใหม่เพื่อใช้กับระบบคลาวด์โดยเฉพาะ ซึ่งเป็นข้อกำหนดที่ไม่มีอยู่ในมาตรฐาน ISO/IEC 27002 อีก 7 ข้อ ได้แก่

- CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment (การแบ่งปันบทบาทและความรับผิดชอบร่วมกันในสภาพแวดล้อมการประมวลผลคลาวด์)
- CLD.8.1.5 Removal of cloud service customer assets (การลบทรัพย์สินของผู้ใช้บริการคลาวด์)
- CLD.9.5.1 Segregation in virtual computing environments (การแยกส่วนในสภาพแวดล้อมการประมวลผลแบบเสมือน)

- CLD.9.5.2 Virtual machine hardening (การปรับแต่งความปลอดภัยระดับเข้มงวดให้กับเครื่องเสมือน)
- CLD.12.1.5 Administrator's operational security (ความมั่นคงปลอดภัยในการปฏิบัติงานของผู้ดูแลระบบ)
- CLD.12.4.5 Monitoring of Cloud Services (การตรวจสอบเฝ้าระวังการบริการคลาวด์)
- CLD.13.1.4 Alignment of security management for virtual and physical networks (การจัดแนวทางการบริหารจัดการความมั่นคงปลอดภัยสำหรับเครือข่ายเสมือนและเครือข่ายกายภาพ)

มาตรฐานนี้ได้กำหนดบทบาทความรับผิดชอบระหว่าง Cloud Service Provider (CSP) และ Cloud Service Customer (CSC) ซึ่งสอดคล้องกับแนวคิด Risk-based Approach ใน ISO/IEC 27001:2013 โดยระบุชัดเจนว่าความเสี่ยงใดที่ลูกค้าต้องดูแล เช่น ข้อมูลและแอปพลิเคชัน และความเสี่ยงใดที่ผู้ให้บริการต้องรับผิดชอบ เช่น โครงสร้างพื้นฐานทางกายภาพ

ISO/IEC 27017:2025 ปัจจุบันอยู่ในขั้นตอน Draft International Standard (DIS) ซึ่งเป็นขั้นตอนสุดท้ายก่อนที่จะประกาศเป็นมาตรฐานฉบับสมบูรณ์ (FDIS และ Publication) โดยจะยกเลิกเวอร์ชันเก่า (2015) และให้คำแนะนำเพิ่มเติมสำหรับการควบคุมที่ระบุไว้ในมาตรฐาน ISO/IEC 27002:2022 มาตรฐานฉบับนี้ มุ่งเน้นการควบคุมที่เกี่ยวข้องกับบริการคลาวด์โดยเฉพาะ โดยได้เพิ่มรายละเอียดวิธีการปฏิบัติ (Implementation Guidance) ให้กับมาตรการเดิมใน Annex A อีก 39 ข้อ และมีกำหนดเพิ่มเข้ามาใหม่เพื่อใช้กับระบบคลาวด์โดยเฉพาะ ซึ่งเป็นมาตรการที่ไม่มีอยู่ในมาตรฐาน ISO/IEC 27002 อีก 4 ข้อ ได้แก่

- CLD.5.38 Shared roles and responsibilities within a cloud computing environment (การแบ่งปันบทบาทและความรับผิดชอบร่วมกันในสภาพแวดล้อมการประมวลผลคลาวด์)
- CLD.5.39 Agreement on the roles and responsibilities of the cloud service partner (ข้อตกลงเกี่ยวกับบทบาทและความรับผิดชอบของพันธมิตรบริการคลาวด์)
- CLD.8.35 Segregation in virtual computing environments (การแบ่งแยกในสภาพแวดล้อมการประมวลผลเสมือน)
- CLD.8.36 Detection and prevention of unauthorized use of cloud services (การตรวจจับและป้องกันการใช้บริการคลาวด์โดยไม่ได้รับอนุญาต)

หน่วยงานที่ต้องการขอรับรองมาตรฐาน ISO/IEC 27017:2015 หากได้มีการดำเนินการตามมาตรฐาน ISO/IEC 27001:2022 และวิธีการปฏิบัติ (Implementation Guidance) ของ ISO/IEC 27017:2015 ให้กับมาตรการเดิมใน Annex A อีก 37 ข้อ แล้วนั้น ยังคงจำเป็นต้องพิจารณามาตรการควบคุมเพิ่มเติมในส่วนของมาตรการเพิ่มเติมจำนวน 7 ข้อ เพื่อให้ครบถ้วนและเพียงพอสำหรับการขอการรับรอง

2.1.3.1 ความสอดคล้องของกลุ่มมาตรฐาน ISO/IEC 27000 family และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ในภาพรวม มาตรฐาน ISO/IEC 27000 family มีความสอดคล้องของมาตรการควบคุมกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยเฉพาะ ISO/IEC 27001:2022 จะมีความสอดคล้องในระดับสูงมาก โดยสามารถจำแนกความเชื่อมโยงตามโครงสร้างใหม่ของ ISO/IEC 27001:2022 ได้ดังนี้

ตารางที่ 10 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27001:2022 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ISO/IEC 27001:2022	ประมวลแนวทางปฏิบัติ พ.ศ. 2564
Clause 4 - 10	17.1, 17.2, 17.3, 17.4, 17.5, 18.1, 18.2, 18.3, 18.4, 19.1, 19.4, 21.1.2, 21.2.1, 21.2.2, 21.3.7, 22.5.1, 22.5.2, 23.1.2, 24.2.1, 24.2.4
A.5 Organizational Controls	17.1, 17.2, 19.1, 19.2, 19.3, 19.4, 21.1.1, 21.1.3, 21.1.4, 21.3.10, 21.3.3, 21.4.1, 21.4.2, 21.4.3, 21.4.4, 22.1.1, 22.1.2, 22.1.3, 22.2.2, 22.3.1, 22.3.2, 22.5.1, 22.6, 23.1.1, 23.1.2, 24.1.1, 24.2.1, 24.2.2, 24.2.3, 24.2.4, 24.3.1, 24.3.2, 25.1.1, 25.1.2
A.6 People Controls	19.1, 22.1.1, 22.3.1, 22.5.1, 22.5.2
A.7 Physical Controls	21.1.1, 22.1.1, 22.1.4, 22.2.1, 22.4.1, 22.4.2, 23.1.1, 25.1.1
A.8 Technological Controls	21.1.1, 21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.6, 21.3.7, 21.3.8, 21.3.9, 21.4.2, 22.1.1, 22.1.2, 22.1.3, 22.2.1, 22.2.2, 22.2.3, 22.2.4, 22.2.5, 22.3.2, 22.4.1, 22.4.2, 23.1.1, 25.1.1

มาตรฐาน ISO/IEC 27701:2025 มีความสอดคล้องเชิงโครงสร้างกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ในหลายมิติ โดยเฉพาะในส่วนของการบริหารจัดการข้อมูลส่วนบุคคล (PII) ทั้งในบทบาทของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ซึ่งสามารถสรุปความเชื่อมโยงของข้อกำหนดและมาตรการควบคุมได้ดังนี้

ตารางที่ 11 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27701:2025 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ISO/IEC 27701:2025	ประมวลแนวทางปฏิบัติ พ.ศ. 2564	หมายเหตุ / ข้อเสนอแนะในการตรวจประเมินเพิ่มเติม
Clause 4 - 10	17.1, 17.2, 17.3, 17.4, 17.5, 18.1, 18.2, 18.3, 18.4, 19.1, 19.4, 21.1.2, 21.2.1, 21.2.2, 21.3.7, 22.5.1, 22.5.2, 23.1.2, 24.2.1, 24.2.4	ตรวจสอบเพิ่มเติมในกรณีที่มีการพัฒนาระบบบริหารจัดการความเป็นส่วนตัว (PIMS)
A.1 — Control objectives and controls for PII controllers	-	ควรตรวจสอบให้ครอบคลุมในส่วนหน้าที่ของผู้ควบคุมข้อมูลตามกฎหมาย PDPA
A.2 — Control objectives and	-	ควรตรวจสอบให้ครอบคลุมหน้าที่ของผู้ประมวลผลข้อมูลตามกฎหมาย

ISO/IEC 27701:2025	ประมวลแนวทางปฏิบัติ พ.ศ. 2564	หมายเหตุ / ข้อเสนอแนะ ในการตรวจประเมินเพิ่มเติม
controls for PII processors		PDPA และข้อตกลงการประมวลผลข้อมูล (DPA)
A.3 — Control objectives and controls for PII controllers and PII processors	17.1, 19.1, 21.1.1, 21.4.2, 21.4.3, 21.4.4, 22.1.2, 22.1.3, 22.2.1, 22.2.2, 22.3.1, 22.3.2, 22.4.1, 22.4.2, 22.5.1, 22.5.2, 22.6, 23.1.1, 23.1.2, 24.2.2, 24.2.3, 25.1.1	ควรตรวจสอบให้ครอบคลุมว่า มาตรการควบคุมเหล่านี้ครอบคลุมถึงข้อมูลส่วนบุคคล

แม้มาตรการควบคุมของ ISO/IEC 27017:2015 ส่วนใหญ่จะสามารถเชื่อมโยงย้อนกลับไปยังตามประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 แต่เนื่องจากมาตรฐาน ISO/IEC 27017:2015 มุ่งเน้นไปที่ความมั่นคงปลอดภัยบนบริการคลาวด์โดยเฉพาะ หน่วยงานจึงจำเป็นต้องพิจารณามาตรการควบคุมเพิ่มเติมในส่วนที่เป็นบริบทเฉพาะของ Cloud Service Provider (CSP) และ Cloud Service Customer (CSC) ด้วย หน่วยงานที่ใช้งานระบบคลาวด์ ไม่สามารถยึดถือเพียงประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ได้เพียงอย่างเดียว แต่ต้องใช้มาตรการใน ISO/IEC 27017 เป็นเกณฑ์เสริมเพื่อให้ครอบคลุมความเสี่ยงที่เกิดจากการใช้ทรัพยากรร่วมกัน (Shared Resources) ในสภาพแวดล้อมคลาวด์

สำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ในหัวข้อที่ระบุว่ามี **มาตรการเฉพาะสำหรับคลาวด์** ผู้ตรวจประเมินจำเป็นต้องประยุกต์ใช้ข้อกำหนดจาก ISO/IEC 27017:2015 เป็นเกณฑ์การตรวจประเมินเพิ่มเติม เพื่อให้ครอบคลุมการควบคุมความมั่นคงปลอดภัยในสภาพแวดล้อมคลาวด์อย่างครบถ้วน

ตารางที่ 12 สรุปความสอดคล้องของมาตรฐาน ISO/IEC 27017:2015 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ISO/IEC 27017:2015	ประมวลแนวทางปฏิบัติ พ.ศ. 2564		หมายเหตุ / ข้อเสนอแนะ ในการตรวจประเมินเพิ่มเติม
	ใช้เป็นมาตรการพื้นฐาน	ต้องมีมาตรการเฉพาะสำหรับคลาวด์เพิ่ม	
5 Information security policies	-	-	ควรตรวจสอบนโยบายที่ระบุถึงการใช้งานคลาวด์ โดยเฉพาะ รวมถึงเกณฑ์การเลือกผู้ให้บริการและการยกเลิกบริการ
6 Organization of information security	22.2.2, 22.6	17.2, 19.1, 21.3.3, 21.3.10, 22.2.2, 22.3.1, 22.6, 24.3.1, 24.3.2	ควรตรวจสอบให้ครอบคลุมการกำหนดบทบาท แต่ควรระบุความรับผิดชอบร่วมกัน (Shared Responsibility)

ISO/IEC 27017:2015	ประมวลแนวทางปฏิบัติ พ.ศ. 2564		หมายเหตุ / ข้อเสนอแนะ ในการตรวจประเมิน เพิ่มเติม
	ใช้เป็นมาตรการพื้นฐาน	ต้องมีมาตรการเฉพาะ สำหรับคลาวด์เพิ่ม	
			ระหว่างหน่วยงานและ CSP
7 Human resource security	22.1.1, 22.5.1	22.1.1, 22.5.1, 22.5.1	ควรตรวจสอบให้ ครอบคลุมการให้ความรู้ แก่พนักงานเรื่องความ ปลอดภัยคลาวด์ และ หน้าที่รับผิดชอบหลังพ้น สภาพพนักงานที่ เกี่ยวข้องกับระบบ คลาวด์
8 Asset management	21.1.1, 22.4.1, 22.4.2, 22.5.1, 23.1.2	21.1.1, 21.1.3, 21.1.4, 22.4.1, 22.4.2	ควรตรวจสอบให้ ครอบคลุมการจัดการ สินทรัพย์บนคลาวด์ (Virtual Assets) และ การทำลายข้อมูลเมื่อเลิก ใช้งานคลาวด์
9 Access control	22.3.2	21.1.1, 22.1.1, 22.1.2, 22.2.2	ควรตรวจสอบให้ ครอบคลุมการบริหาร จัดการสิทธิ์ของผู้ ให้บริการ (CSP Admin) และการเข้าถึง Console ของระบบคลาวด์
10 Cryptography	-	22.3.2, 22.4.2	ควรตรวจสอบให้ ครอบคลุมการจัดการ กุญแจรหัส (Key Management) และ การเข้ารหัสข้อมูลทั้ง ขณะจัดเก็บ (At Rest) และรับส่ง (In Transit)
11 Physical and environmental security	22.1.1, 22.1.4, 22.2.1, 22.4.1, 22.4.2, 25.1.1	21.1.1	ควรตรวจสอบให้ ครอบคลุมบทบาทความ รับผิดชอบของ CSP ใน การดูแล Data Center

ISO/IEC 27017:2015	ประมวลแนวทางปฏิบัติ พ.ศ. 2564		หมายเหตุ / ข้อเสนอแนะ ในการตรวจประเมิน เพิ่มเติม
	ใช้เป็นมาตรการพื้นฐาน	ต้องมีมาตรการเฉพาะ สำหรับคลาวด์เพิ่ม	
12 Operations security	22.4.2	21.3.1, 21.3.2, 21.3.3, 21.3.4, 21.3.5, 21.3.6, 21.3.7, 21.3.8, 21.3.9, 22.1.3, 22.2.2, 22.2.5, 25.1.1	ควรตรวจสอบให้ครอบคลุมการตรวจสอบ Log ในส่วนที่ CSP เป็นผู้ดูแลและส่วนที่หน่วยงานต้องดูแลเอง
13 Communications security	22.3.1, 22.3.2, 22.5.1	21.1.1	ควรตรวจสอบให้ครอบคลุมความมั่นคงปลอดภัยของการเชื่อมต่อระหว่างองค์กรและระบบคลาวด์ (เช่น VPN, Direct Connect)
14 System acquisition, development and maintenance	21.3.1, 21.3.2, 21.3.4, 21.3.5, 21.3.6, 21.3.7, 21.3.8, 21.3.9, 21.4.2, 22.2.1, 22.2.2	21.3.3, 22.2.5	ควรตรวจสอบให้ครอบคลุมความปลอดภัยในกระบวนการพัฒนาแอปพลิเคชันบนสภาพแวดล้อมคลาวด์ (DevSecOps)
15 Supplier relationships	21.4.3	21.4.1, 21.4.2, 21.4.4, 25.1.1	ควรตรวจสอบให้ครอบคลุมสัญญา (SLA) และข้อกำหนดด้านความปลอดภัยที่ทำร่วมกับ CSP
16 Information security incident management	22.6, 24.2.3	19.1, 19.2, 19.3, 19.4, 23.1.1, 24.1.1, 24.2.1, 24.2.2, 24.2.4, 24.3.1	ควรตรวจสอบให้ครอบคลุมการประสานงานแจ้งเหตุระหว่าง CSP และหน่วยงาน เมื่อเกิดภัยคุกคามบนระบบคลาวด์
17 Information security aspects of business continuity management	25.1.1, 25.1.2	-	ควรตรวจสอบให้ครอบคลุมการแผนสำรองกรณีระบบคลาวด์ขัดข้องเป็นเวลานาน (Cloud Outage) หรือ

ISO/IEC 27017:2015	ประมวลแนวทางปฏิบัติ พ.ศ. 2564		หมายเหตุ / ข้อเสนอแนะ ในการตรวจประเมิน เพิ่มเติม
	ใช้เป็นมาตรการพื้นฐาน	ต้องมีมาตรการเฉพาะ สำหรับคลาวด์เพิ่ม	
			แผนการย้ายระบบ (Migration/Exit Plan)
18 Compliance	22.5.1, 23.1.2	17.1, 21.1.1, 21.4.4, 22.1.3	ควรตรวจสอบให้ ครอบคลุมการปฏิบัติ ตามกฎหมายคุ้มครอง ข้อมูลส่วนบุคคล (PDPA) ในกรณีที่มีการ เก็บข้อมูลใน ต่างประเทศ (Cross- border)
Annex A – Cloud service extended control set	-	-	ควรตรวจสอบมาตรการ เฉพาะสำหรับคลาวด์ เช่น การแยก Virtual Network และการ ป้องกันข้อมูลที่ใช้ ทรัพยากรร่วมกัน

2.1.3.2 ความแตกต่างของกลุ่มมาตรฐาน ISO/IEC 27000 family และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

เนื่องจาก Annex A ของมาตรฐาน ISO/IEC 27001 เป็นโครงสร้างมาตรการควบคุมหลักที่มาตรฐาน
ความมั่นคงปลอดภัยสารสนเทศฉบับอื่น ทั้ง ISO/IEC 27017 และ ISO/IEC 27701 ใช้เป็นเกณฑ์อ้างอิง
(Baseline) การศึกษานี้จึงมุ่งเน้นการวิเคราะห์เปรียบเทียบส่วนต่าง (Gap Analysis) ระหว่าง ประมวลแนวทาง
ปฏิบัติฯ พ.ศ. 2564 และ ISO/IEC 27001 Annex A เพื่อระบุความสอดคล้องและมาตรการเพิ่มเติมที่สำคัญ
โดยสามารถสรุปสาระสำคัญได้ดังนี้

ตารางที่ 13 สรุปความแตกต่างของมาตรฐาน ISO/IEC 27001:2022 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ISO/IEC 27001:2022	ข้อกำหนดที่แตกต่างจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564
Clause 4 - 10	Clause 4.4 Information security management system Clause 7.5.1 Documented information (General) Clause 7.5.2 Documented information (Creating and updating) Clause 7.5.3 Documented information (Control of documented information)
A.5 Organizational Controls	Annex A 5.1 Policies for information security Annex A 5.4 Management responsibilities

ISO/IEC 27001:2022	ข้อกำหนดที่แตกต่างจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564
	Annex A 5.16 Identity management Annex A 5.37 Documented operating procedures
A.6 People Controls	-
A.7 Physical Controls	-
A.8 Technological Controls	Annex A 8.10 Information deletion Annex A 8.13 Information backup Annex A 8.15 Logging Annex A 8.19 Installation of software on operational systems Annex A 8.25 Secure development life cycle Annex A 8.26 Application security requirements Annex A 8.28 Secure coding Annex A 8.31 Separation of development, test and production environments Annex A 8.33 Test information

เนื่องจากหน่วยงานไม่ได้มุ่งเน้นการขอรับรองมาตรฐาน (Certification) จึงไม่จำเป็นต้องนำข้อกำหนดในกลุ่ม Clause 4 - 10 มาจัดทำเป็นแนวทางการตรวจประเมินหลัก เนื่องจากข้อกำหนดเหล่านี้เน้นไปที่กระบวนการรักษาระบบมาตรฐานในระยะยาว ซึ่งประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ไม่ได้ระบุเป็นข้อบังคับโดยตรง อย่างไรก็ตาม ควรนำมาตรการควบคุมใน Annex A มาพิจารณาจัดทำเป็นแนวทางการตรวจประเมินเพิ่มเติม เพื่อใช้เป็นเกณฑ์เสริมในการยกระดับความมั่นคงปลอดภัย ซึ่งมาตรการเหล่านี้จะช่วยปิดช่องว่างความเสี่ยงทางเทคนิคและทำให้ระบบการป้องกันของหน่วยงานมีความเข้มแข็งสอดคล้องกับมาตรฐานสากล

2.1.3.3 ข้อเสนอแนะในการจัดทำหลักเกณฑ์การตรวจประเมินฯ

จากการวิเคราะห์ในหัวข้อ 2.2.3 ซึ่งเสนอให้มีการยกระดับหัวข้อการตรวจประเมินเพิ่มเติมจากฐานของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยอ้างอิงองค์ประกอบใหม่จาก NIST CSF 2.0 ในการขยายขอบเขตการตรวจประเมินเพิ่มเติมจากฐานเดิมของ ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เพื่อให้ครอบคลุมมิติการบริหารจัดการความเสี่ยงสมัยใหม่ อย่างไรก็ตาม เนื่องจากการศึกษาพบว่ามาตรการควบคุมใน ISO/IEC 27001:2022 (Annex A) ยังคงมีรายละเอียดและข้อกำหนดที่แตกต่างจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ในการศึกษาครั้งนี้ จึงได้นำข้อแตกต่างที่พบมาเปรียบเทียบและรวบรวมกับแนวทางของ NIST CSF เพื่อจัดทำเป็นเกณฑ์การตรวจประเมินที่สมบูรณ์ โดยมุ่งเน้นไปที่มาตรการเชิงปฏิบัติที่นำไปใช้ได้จริง โดยแสดงไว้ในตารางดังต่อไปนี้

ตารางที่ 14 ข้อเสนอแนะในการจัดทำหัวข้อการตรวจประเมินเพิ่มเติม อ้างอิงตาม NIST CSF 2.0 และ ISO/IEC 27001:2022

ลำดับ	รายละเอียด	NIST CSF 2.0	ISO/IEC 27001:2022	ข้ออ้างอิง (หลักเกณฑ์ฯ)
ข้อที่ 1	ความรับผิดชอบของผู้นาองค์กร และการส่งเสริมวัฒนธรรมด้าน ความมั่นคงปลอดภัยไซเบอร์	GV.RR-01	Clause 7.2, Annex A 5.4	3.2.1
ข้อที่ 2	การกำกับดูแล การทบทวน และ การปรับปรุงกลยุทธ์และผลการ ดำเนินงานด้านความมั่นคง ปลอดภัยไซเบอร์	GV.OV-01 GV.OV-02 GV.OV-03 GV.RM-07	Clause 9.1, Annex A 5.1, Annex A 5.4, Annex A 5.19, Annex A 5.20	3.2.2
ข้อที่ 3	การจัดทำนโยบายและกระบวนการ บริหารจัดการความเสี่ยงด้าน ไซเบอร์ของห่วงโซ่อุปทาน	GV.SC-01	Clause 8.1, Annex A 5.1, Annex A 5.19, Annex A 5.20, Annex A 5.21, Annex A 5.22	3.2.3
ข้อที่ 4	การจัดการบัญชีผู้ใช้	PR.AA-01 PR.AA-02	Annex A 5.16, Annex A 8.2, Annex A 8.3, Annex A 8.5	3.2.4
ข้อที่ 5	การรักษาความมั่นคงปลอดภัยของ ข้อมูล	PR.DS-01 PR.DS-02 PR.DS-10 PR.DS-11	Clause 4.2, Clause 5.2, Annex A 5.1, Annex A 5.3, Annex A 5.10, Annex A 5.13, Annex A 5.14, Annex A 5.15, Annex A 6.1, Annex A 6.2, Annex A 6.5, Annex A 7.7, Annex A 7.10, Annex A 8.2, Annex A 8.3, Annex A 8.4, Annex A 8.7, Annex A 8.8,	3.2.5

ลำดับ	รายละเอียด	NIST CSF 2.0	ISO/IEC 27001:2022	ข้ออ้างอิง (หลักเกณฑ์ฯ)
			Annex A 8.10, Annex A 8.13, Annex A 8.17, Annex A 8.19, Annex A 8.20, Annex A 8.22, Annex A 8.26	
ข้อที่ 6	1. การจัดการแพตช์	PR.PS-02	Annex A 5.9	3.2.6
	2. การจัดการซอฟต์แวร์	PR.PS-02 PR.PS-05	Annex A 5.9, Annex A 8.19	3.2.7
	3. การจัดการฮาร์ดแวร์	PR.PS-03	Annex A 5.9	3.2.8
	4. การจัดการบันทึกเหตุการณ์	PR.PS-04	Annex A 8.15, Annex A 8.17	3.2.9
	5. การพัฒนาซอฟต์แวร์ที่มีความ มั่นคงปลอดภัย	PR.PS-06	Annex A 8.25, Annex A 8.28, Annex A 8.31, Annex A 8.33	3.2.10
ข้อที่ 7	การเสริมสร้างความพร้อมรับมือ ของโครงสร้างพื้นฐานทาง เทคโนโลยี	PR.IR-02 PR.IR-03 PR.IR-04	Clause 4.2, Clause 6.1.1, Annex A 5.29, Annex A 7.5, Annex A 8.6, Annex A 8.14	3.2.11
ข้อที่ 8	การวิเคราะห์เหตุการณ์ไม่พึง ประสงค์	DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-07 DE.AE-08	Annex A 5.7, Annex A 5.24, Annex A 5.25, Annex A 5.26, Annex A 8.15, Annex A 8.16	3.2.12
ข้อที่ 9	การวิเคราะห์เหตุภัยคุกคามทาง ไซเบอร์	RS.AN-03 RS.AN-06 RS.AN-07 RS.AN-08	Annex A 5.25, Annex A 5.27, Annex A 5.28	3.2.13
ข้อที่ 10	การบรรเทาเหตุภัยคุกคามทาง ไซเบอร์	RS.MI-01 RS.MI-02	Annex A 5.26	3.2.14

ลำดับ	รายละเอียด	NIST CSF 2.0	ISO/IEC 27001:2022	ข้ออ้างอิง (หลักเกณฑ์ฯ)
ข้อที่ 11	1. การจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์	RC.RP-02	Annex A 5.26	3.2.15
	2. การทดสอบ ทบทวน และปรับปรุงแผน	RC.RP-04	Annex 5.30	3.2.16
	3. การดำเนินการตามแผนฟื้นฟูจากเหตุจริง	RC.RP-01 RC.RP-03 RC.RP-05 RC.RP-06	Annex 5.26, Annex 5.27, Annex 8.13	3.2.17
	4. แผนการสำรองข้อมูล	PR.DS-11	Annex A 8.13	3.2.18
ข้อที่ 12	การสื่อสารระหว่างกันฟื้นฟูเหตุภัยคุกคามทางไซเบอร์	RC.CO-03 RC.CO-04	Clause 7.4	3.2.19

2.2 บทวิเคราะห์เชิงเปรียบเทียบ ระหว่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

การเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลนำมาซึ่งความท้าทายสำคัญสองประการ คือ การคุ้มครองสิทธิในข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ การศึกษานี้จึงจัดทำขึ้นเพื่อวิเคราะห์เชิงเปรียบเทียบระหว่าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์หลักเพื่อระบุความสอดคล้องและไม่สอดคล้อง และนำผลการวิเคราะห์นี้ไปใช้ในการออกแบบ และจัดทำแผนดำเนินการและกระบวนการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่อยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ต่อไป โดยมีรายละเอียดผลการวิเคราะห์ ดังต่อไปนี้

2.2.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในประเทศไทยมีการประกาศใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีวัตถุประสงค์เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เป็นทั้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และมีการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคล จำเป็นต้องพิจารณาและปฏิบัติตามกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ร่วมด้วย
การปฏิบัติตามมาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในบริบทของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งมีการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล หน่วยงานมีความจำเป็นที่ต้องปฏิบัติตามทั้งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะในมิติของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Data Security) เพื่อคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ มาตรการดังกล่าวต้องได้รับการทบทวนอย่างสม่ำเสมอเมื่อเกิดการเปลี่ยนแปลงทางเทคโนโลยี เพื่อธำรงไว้ซึ่งประสิทธิภาพในการคุ้มครองข้อมูลตามมาตรฐานขั้นต่ำที่คณะกรรมการกำหนด

เพื่อให้เกิดรูปธรรมในการปฏิบัติ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (ซึ่งอาศัยอำนาจตามมาตรา 16 (4) และ 37 (1)) ได้กำหนดมาตรฐานขั้นต่ำที่ครอบคลุมหลักการพื้นฐาน 3 ประการ (CIA Triad) ดังนี้

- การรักษาความลับ (Confidentiality): การจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่มีอำนาจหน้าที่
- ความถูกต้องครบถ้วน (Integrity): การป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลโดยมิชอบ
- สภาพพร้อมใช้งาน (Availability): การสร้างหลักประกันว่าข้อมูลสามารถเรียกใช้ได้เมื่อต้องการ

โดยมาตรการเหล่านี้ต้องประกอบด้วย มาตรการเชิงองค์กร (Organizational Measures) และ มาตรการเชิงเทคนิค (Technical Measures) รวมถึงมาตรการทางกายภาพที่สอดคล้องกับระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

2.2.2 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ถูกกำหนดขึ้นตามมาตรา 16 (4) และมาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศฉบับนี้ระบุถึงมาตรฐานขั้นต่ำในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยครอบคลุมทั้งในด้านการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งต้องคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบ มีรายละเอียดโดยสังเขป ดังนี้

- 1) (ข้อ 4) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยมาตรการรักษาความมั่นคงปลอดภัยอย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้
 - (1) ต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม
 - (2) ต้องประกอบด้วยมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (Physical Measures) ที่จำเป็น

- (3) ต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) การป้องกันความเสี่ยงที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง
- (4) มาตรการรักษาความมั่นคงปลอดภัยต้องคำนึงถึงความสามารถในการดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน และความเป็นไปได้ในการดำเนินการประกอบกัน
- (5) มาตรการรักษาความมั่นคงปลอดภัยจะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple Layers of Security Controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์
- (6) มาตรการรักษาความมั่นคงปลอดภัยในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย การดำเนินการ ดังต่อไปนี้
 - (ก) การควบคุมการเข้าถึง (Access Control) ที่มีการพิสูจน์และยืนยันตัวตน (Identity Proofing and Authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (Authorization) ที่เหมาะสม ด้วยหลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know Basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege)
 - (ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่เหมาะสมซึ่งรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (User Registration and De-Registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of Privileged Access Rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)
 - (ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
 - (ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit Trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

- (7) ต้องมีการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) เกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย รวมถึงมีการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสมให้ผู้เกี่ยวข้องทั้งหมดรับทราบและปฏิบัติ
- 2) (ข้อ 5) ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป ครอบคลุมถึงกรณีมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- 3) (ข้อ 6) ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมรวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ตารางที่ 15 สรุปความสอดคล้องของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประมวลแนวทางปฏิบัติ พ.ศ. 2564	ประกาศคณะกรรมการ เรื่องมาตรการรักษาความ มั่นคงปลอดภัยฯ 2565
ส่วนที่ 1: ประมวลแนวทางปฏิบัติ (Code of Practice)	
องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
18.1 การประเมินความเสี่ยง (Risk Assessment)	
18.1 (ก) การระบุความเสี่ยง (Risk Identification) ระบุความเสี่ยงจากภัยคุกคามและช่องโหว่ ที่มาจากกระบวนการ ระบบงาน บุคลากร หรือปัจจัยภายนอก	ข้อ 4 (3)
18.1 (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ทำความเข้าใจและวิเคราะห์ความเสี่ยงเพื่อหาแนวทางจัดการที่เหมาะสม	ข้อ 4 (3)
18.1 (ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ประเมินโอกาสเกิดผลกระทบ และกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ข้อ 4 (3)
18.2 การจัดการความเสี่ยง (Risk Treatment) มีแนวทางจัดการ ควบคุม ป้องกันความเสี่ยง เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงความคุ้มค่า และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ข้อ 4 (3)
18.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) มีกระบวนการติดตามและทบทวนความเสี่ยง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้	ข้อ 5
องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์	

ประมวลแนวทางปฏิบัติ พ.ศ. 2564	ประกาศคณะกรรมการฯ เรื่องมาตรการรักษาความ มั่นคงปลอดภัยฯ 2565
19.1 การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	
19.1 (ก) โครงสร้างทีมรับมือเหตุการณ์ (CIRT) ระบุบทบาท และความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ	ข้อ 4 (3)
19.1 (ข) โครงสร้างการรายงานเหตุการณ์ ให้เป็นไปตามการรายงานตามภาระหน้าที่ภายใต้ พ.ร.บ. และกฎหมายที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ	ข้อ 4 (3)
19.1 (ค), (ง), (จ), (ฉ) ขั้นตอนการเผชิญเหตุ ต้องมีการกำหนดเกณฑ์การเรียกใช้งาน (Activate), การจำกัดขอบเขต (Containment), กระบวนการกู้คืน (Recovery) และการสอบสวน (Investigate) สาเหตุและผลกระทบ	ข้อ 4 (3)
19.1 (ซ) การเก็บรักษาหลักฐาน (Preservation of Evidence) ขั้นตอนการเก็บรักษาหลักฐานก่อนเริ่มกระบวนการกู้คืน รวมถึงหลักฐานทางคอมพิวเตอร์เพื่อสนับสนุนการสอบสวน	ข้อ 4 (3)
19.1 (ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review) การทบทวนหลังการดำเนินการเพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อ 5
19.2 การสื่อสารแผนการรับมือ ต้องสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมด	ข้อ 4 (7)
19.3 การทบทวนแผนตามรอบเวลา ทำการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ	ข้อ 5
19.4 การทบทวนแผนเมื่อมีการเปลี่ยนแปลง	ข้อ 5
ส่วนที่ 2: กรอบมาตรฐาน (Standard Framework)	
หัวข้อหลักที่ 1 Identify	
21.1 การจัดการทรัพย์สิน (Asset Management)	
21.1.1 จัดทำและปรับปรุงทะเบียนทรัพย์สิน (Inventory) ให้เป็นปัจจุบัน ระบุชื่อ ฟังก์ชัน ความสำคัญ เจ้าของ ที่ตั้ง และการพึ่งพากันของทรัพย์สิน	ข้อ 4 (1), 4 (2), 4 (3), 4 (5)
21.1.2 ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง (Network scope & interface)	ข้อ 4 (5)
21.1.4 ประเมินความเสี่ยงด้านไซเบอร์ของทรัพย์สินที่อยู่ในทะเบียน อย่างน้อยปีละ 1 ครั้ง	ข้อ 4 (3)
21.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง	
21.2.1 ประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	ข้อ 5
21.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)	

ประมวลแนวทางปฏิบัติ พ.ศ. 2564	ประกาศคณะกรรมการ เรื่องมาตรการรักษาความ มั่นคงปลอดภัยฯ 2565
21.4.1 องค์กรต้องรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ แม้จะใช้ผู้ให้บริการภายนอก	ข้อ 6
21.4.2 กำหนดข้อกำหนดด้านไซเบอร์ในข้อตกลง SLA หรือเงื่อนไขสัญญากับผู้ให้บริการภายนอก ครอบคลุมภาระหน้าที่, ห่วงโซ่อุปทาน (Supply chain) และสิทธิในการตรวจสอบ	ข้อ 6
21.4.4 เจรจาทอรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมาย/ข้อบังคับใหม่	ข้อ 6
หัวข้อหลักที่ 2 Protect	
22.1 การควบคุมการเข้าถึง (Access Control)	
22.1.1 จำกัดการเข้าถึงบริการสำคัญ เฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เน็ตที่ได้รับอนุญาตเท่านั้น	ข้อ 4 (6)
22.1.2 ใช้เทคนิคการตรวจสอบสิทธิ์ (Authentication) ที่สอดคล้องกับโปรไฟล์ความเสี่ยง	ข้อ 4 (6) (ก)
22.1.3 เก็บบันทึกการเข้าถึงทั้งหมด (Logs) และตรวจสอบบันทึกเพื่อหากิจกรรมที่ผิดปกติอย่างสม่ำเสมอ	ข้อ 4 (6) (ง)
22.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	
22.2.1 จัดทำมาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้ครอบคลุมทุกระบบและอุปกรณ์โดยสอดคล้องกับโปรไฟล์ความเสี่ยงของบริการสำคัญ	ข้อ 4 (5)
22.2.2 มาตรฐานต้องมี: สิทธิเข้าถึงน้อยสุด (Least Privilege), แบ่งแยกหน้าที่ (Separation of Duties), รหัสผ่านซับซ้อน, ลบบัญชี/แอป/พอร์ตที่ไม่ใช้, ป้องกันมัลแวร์, และอัปเดตแพตช์	ข้อ 4 (5), 4 (6) (ก), 4 (6) (ข)
22.2.3 หน่วยงานรัฐและ CII ต้องบังคับใช้มาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้เรียบร้อยก่อนเริ่มเชื่อมต่ออุปกรณ์หรือปรับปรุงระบบทุกครั้ง	ข้อ 4 (5)
22.2.4 หน่วยงานรัฐและ CII ต้องทบทวนมาตรฐาน Security Baseline อย่างน้อยปีละครั้งเพื่อให้มั่นใจว่ายังรับมือกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ	ข้อ 5
22.2.5 จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบการเปลี่ยนแปลงระบบ	ข้อ 4 (6) (ข)
22.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	
22.4.1 ควบคุมการใช้สื่อแบบถอดได้ (เช่น ปิดพอร์ต USB และเปิดเมื่อจำเป็น), ใช้เฉพาะที่ได้รับอนุญาต, และตรวจสอบมัลแวร์ก่อนเชื่อมต่อ	ข้อ 4 (1), ข้อ 4 (5)
22.4.2 เข้ารหัสข้อมูลที่ละเอียดอ่อนบนสื่อบันทึกข้อมูลแบบถอดได้	ข้อ 4 (1)

ประมวลแนวทางปฏิบัติ พ.ศ. 2564	ประกาศคณะกรรมการฯ เรื่องมาตรการรักษาความ มั่นคงปลอดภัยฯ 2565
22.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	
22.5.1 หน่วยงานรัฐและ CII ต้องสร้างความตระหนักรู้ด้านไซเบอร์ให้บุคลากรทุกระดับและบุคคลภายนอกอย่างทั่วถึง โดยครอบคลุมทั้งหน้าที่ความรับผิดชอบ ความรู้ด้านกฎหมาย และการแจ้งเตือนภัยคุกคามอย่างสม่ำเสมอเพื่อให้เกิดความปลอดภัยในการปฏิบัติงานอย่างเป็นรูปธรรม	ข้อ 4 (6) (ค), 4 (7)
22.5.2 ต้องทบทวนแผนสร้างความตระหนักรู้ไซเบอร์อย่างน้อยปีละครั้งเพื่อให้เนื้อหาทันสมัยและเหมาะสมกับสถานการณ์ปัจจุบัน	ข้อ 5
หัวข้อหลักที่ 3 Detect	
23.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
23.1.1 (ก) สร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน	ข้อ 4 (3)
23.1.1 (ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ	ข้อ 4 (3)
23.1.1 (ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญหรือไม่	ข้อ 4 (3)
23.1.2 ดำเนินการทบทวนกลไกและกระบวนการ (ตามข้อ 23.1.1) อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ	ข้อ 5
หัวข้อหลักที่ 4 Respond	
24.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	
24.1.1 จัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้การรับมือดำเนินการได้อย่างมีประสิทธิภาพ	ข้อ 4 (3)
หัวข้อหลักที่ 5 Recover	
25.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	
25.1.1 จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการสำคัญสามารถดำเนินการต่อไปได้เมื่อเกิดการหยุดชะงักจากเหตุการณ์ด้านไซเบอร์กำหนดระยะเวลาและเกณฑ์ที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective	ข้อ 4 (3), 4 (4)

ประมวลแนวทางปฏิบัติ พ.ศ. 2564	ประกาศคณะกรรมการฯ เรื่องมาตรการรักษาความ มั่นคงปลอดภัยฯ 2565
(RTO) และ Recovery Point Objective (RPO) สอบทานแผนของผู้ให้บริการ ภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน	

2.3 เอกสารต้นแบบที่สำคัญสำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เพื่อให้การนำไปปฏิบัติเป็นไปอย่างมีรูปธรรมและครอบคลุมทุกมิติ ผลการศึกษาในครั้งนี้ ได้ถูกนำมาใช้ในการออกแบบเอกสารต้นแบบที่สำคัญสำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีรายการเอกสารต้นแบบที่สำคัญ ดังนี้

1. (ร่าง) หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศฯ

(ร่าง) หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีเป้าหมายเพื่อใช้เป็นกลไกสำคัญในการกำกับดูแล ตรวจสอบ และยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญ (CII) ให้สอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐานในระดับสากลอย่างมีประสิทธิภาพ โดยจะมีการกำหนดโครงสร้างเนื้อหาออกเป็นส่วนสำคัญ ดังต่อไปนี้

1) บทนำ เป็นส่วนอธิบายภาพรวมของเอกสาร ประกอบด้วย

- หลักการ ความจำเป็น และวัตถุประสงค์ของการจัดทำเกณฑ์การตรวจประเมิน
- คำจำกัดความ และการควบคุมที่พึงมี
- แนวทางการประเมิน กำหนดกติกาเบื้องต้น เช่น ความถี่ในการประเมิน (อย่างน้อยปีละ 1 ครั้ง) และเกณฑ์การให้คะแนนระดับความไม่สอดคล้อง (Major NC, Minor NC, C, OBS, OFI)
- รายการกฎหมายและมาตรฐานสากลที่เกี่ยวข้อง

2) มาตรฐาน กรอบปฏิบัติงานที่ใช้อ้างอิงสำหรับการตรวจประเมิน เป็นส่วนที่แสดงให้เห็นถึงที่มา และรากฐานของเกณฑ์การประเมิน ประกอบด้วย

- กรอบแนวคิดในการวิเคราะห์และจัดทำแนวทางการตรวจประเมิน
- ผลการศึกษาและวิเคราะห์เชิงเปรียบเทียบระหว่าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับข้อกำหนดอื่นๆ ได้แก่ กฎหมายลำดับรอง, กรอบแนวทาง NIST Cybersecurity Framework, มาตรฐานกลุ่ม ISO/IEC และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

3) แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นส่วนเนื้อหาหลักที่ใช้ในการลงพื้นที่ตรวจประเมินจริง โดยแบ่งหมวดหมู่ตามกฎหมายคือ "ประมวลแนวทางปฏิบัติ" และ "กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์" (ครอบคลุมกรอบ Identify, Protect, Detect, Respond, Recover)

ทุกหัวข้อย่อยของการตรวจประเมิน จะถูกจัดรูปแบบโครงสร้างให้เป็นมาตรฐานเดียวกันทั้งหมด เพื่อให้ผู้ตรวจ (Auditor) ทำงานได้ง่าย โดยแต่ละข้อจะประกอบด้วยตารางที่มีหัวข้อดังนี้

- วัตถุประสงค์ - เป้าหมายของการตรวจข้อนี้
- การควบคุมที่พึงมี - สิ่งที่หน่วยงานต้องปฏิบัติตามกฎหมาย
- แนวทางการประเมิน - สิ่งที่ผู้ตรวจต้องมองหาหรือตรวจสอบ
- มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิง - การอ้างอิง (Mapping) ไปยัง ISO/IEC หรือ NIST CSF
- ขั้นตอนการตรวจสอบ - วิธีการปฏิบัติงานตรวจจริง ซึ่งแบ่งย่อยเป็น การสัมภาษณ์ผู้ที่เกี่ยวข้อง, การสอบถามเอกสาร, รายการเอกสารที่เกี่ยวข้อง และเทคนิคในการตรวจสอบเชิงเทคนิค

4) ภาคผนวก เป็นส่วนที่รวบรวมเครื่องมือที่ต้องนำไปใช้งานจริง อาทิ

- แบบฟอร์มการตรวจประเมิน
- แบบฟอร์มรายงานผลการประเมิน

ทั้งนี้ รายละเอียดและเนื้อหาของ (ร่าง) หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) DGA Community Standard มสพร. x-xxxx DGA x-xxxx	ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ข้อ 17 3.1.1 การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ข้อ 17.1 วัตถุประสงค์ เพื่อให้มั่นใจว่า หน่วยงานมีการปฏิบัติตามกฎหมายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดอย่างต่อเนื่อง ความเสี่ยง มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ของหน่วยงานไม่สอดคล้องกับข้อกำหนดตามกฎหมายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงไม่สามารถรับมือกับรูปแบบภัยคุกคามที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ การควบคุมที่พึงมี ต้องจัดทำแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ที่เป็นผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยมิชอบเบี่ยงเบนการตรวจสอบ ดังนี้ (ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) (ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าอาณและใช้บริการ ตามเอกสารวิเคราะห์ข้อ (ก) (ค) การปฏิบัติตามพระราชบัญญัติฯ และประมวลแนวทางปฏิบัติฯ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับการประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด แนวทางการประเมิน 1. ตรวจสอบการแต่งตั้งผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ว่าได้รับอนุมัติอย่างเป็นทางการ มีความเป็นอิสระ และมีความสามารถตรงตามเกณฑ์ 2. ตรวจสอบแผนการตรวจสอบประจำปีให้ครอบคลุมการดำเนินการอย่างน้อยปีละ 1 ครั้ง 3. ตรวจสอบขอบเขตการตรวจสอบว่าครอบคลุมกระบวนการ BIA บริการที่สำคัญ (CI) และการปฏิบัติตามกฎหมายประมวลแนวทางปฏิบัติฯ อย่างครบถ้วน 4. ตรวจสอบว่าวิธีการประเมินมีการดำเนินการให้การตรวจสอบตามข้อกำหนด (Compliance) และการตรวจสอบตามความเสี่ยง (Risk-based) มาตรฐานหรือกรอบปฏิบัติงานที่ใช้ใช้ในการตรวจสอบ ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ข้อ 17.1 แนวทางการจัดทำประมวลฯ พ.ศ. 2568 เอกสารแนบ 1 NIST CSF 2.0 GV/OC-03
--	---

รูปที่ 3 ต้นแบบเอกสาร (ร่าง) หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศฯ

2. ต้นแบบเครื่องมือสำหรับการตรวจประเมิน

เครื่องมือสำหรับการตรวจประเมินฯ ถือเป็นองค์ประกอบสำคัญในการขับเคลื่อนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายฉบับรองที่เกี่ยวข้อง โดยในการศึกษาครั้งนี้ จะออกแบบเครื่องมือสำหรับการใช้งาน ดังนี้

- (1) แบบฟอร์มคำรับรองการนำข้อความคุ้มครองไปใช้ (Statement of Applicability : SOA)
- (2) โปรแกรมการตรวจประเมิน (Audit Program)
- (3) แผนการตรวจประเมิน (Audit Plan)
- (4) รายงานการตรวจประเมิน (Audit Report)
- (5) แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)
- (6) แผนการแก้ไข (Corrective Action Plan)
- (7) รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)
- (8) ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศที่สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน สำหรับ 4 บริการ

ชื่อเอกสาร	แบบฟอร์มสำหรับรายงานการตรวจควบคุมไปใช้ (Statement of Applicability : SOA)							
เวอร์ชัน	1.0							
สพท.	ตัวชี้วัด	ข้อมูลประกอบ แบบทางปฏิบัติ (ตัวชี้วัด)	สาระสำคัญ (ประมวลแนวทางปฏิบัติของพท.)	ตัวอย่างเอกสารที่เกี่ยวข้อง	การนำมาตรการควบคุมมาใช้	รายละเอียดของมาตรการควบคุมปัจจุบัน (ระบุถึงตำแหน่งงานจริง เช่น มีการกำหนด กระบวนการการนำเทคโนโลยีเข้ามาใช้)	เอกสารจริงของหน่วยงาน	หมายเหตุ
3.1 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคบังคับ(Mandatory)								
ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ								
3.1.1	การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์	17.1	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง	1.มีผู้รับผิดชอบตรวจสอบภายใน หรือผู้เกี่ยวข้อง ผู้ตรวจสอบภายนอก 2.ไม่มีการตรวจสอบการบริหารความมั่นคงปลอดภัยไซเบอร์ 3.มีรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 4.มีกระบวนการบริหารที่สำคัญ	นำมาใช้			
3.1.2	การรายงานการตรวจสอบด้านความมั่นคง ปลอดภัยไซเบอร์	17.2	ต้องจัดส่งสรุปรายงานการตรวจสอบ ต่อสำนักงานภายใน กำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ได้ดำเนินการแล้วเสร็จ	1. รายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 2. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ ตรวจสอบที่เกี่ยวข้อง และหน่วยงานกำกับดูแล 3. กระบวนการใช้ข้อมูลหรือการนำไปใช้ตาม ข้อกำหนด 4. แนวทางการปรับปรุงแก้ไขข้อบกพร่องหรือการไม่ ปฏิบัติตามข้อกำหนด 5. แผนการดำเนินการตามข้อกำหนด 6. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล	ไม่นำมาใช้			
3.1.3	การแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตาม ข้อกำหนด	17.3	ในกรณีที่ไม่ปฏิบัติตามข้อ ๓๓.๔ ต้องส่งผลการดำเนินการ แก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วัน	1.เอกสารที่พิจารณาและดำเนินการปรับปรุงแผนจาก กรม หรือ สถาน 2. แผนการดำเนินการแก้ไขข้อบกพร่อง 3. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล				
3.1.4	การปรับปรุงแผนการดำเนินการตามการ	17.4	ในกรณี กทม. เห็นสมควรให้ปรับปรุงแผน ต้องดำเนินการ เพื่อส่งผลการดำเนินการแก้ไขถึงการปรับปรุงแล้วเสร็จ สำนักงาน	1.เอกสารที่พิจารณาและดำเนินการปรับปรุงแผนจาก กรม หรือ สถาน 2. แผนการดำเนินการแก้ไขข้อบกพร่อง 3. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล				

รูปที่ 4 ต้นแบบแบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ (Statement of Applicability : SOA)

แนวทางการตรวจสอบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคบังคับ (Mandatory) (Audit Program)									
ลำดับ	ตัวชี้วัด เชิงปริมาณ	ตัวชี้วัด	วัตถุประสงค์	รายการข้อค้นพบ	แนวทางการประเมิน	ตัวชี้วัด เชิงปริมาณ	ผลการประเมิน	ผลการตรวจสอบและหลักฐานการตรวจสอบ	รายละเอียดการปฏิบัติตามข้อกำหนด
ส่วนที่ 1 : แนวทางการตรวจสอบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคบังคับ(Mandatory)									
		การตรวจสอบด้านความ มั่นคงปลอดภัยไซเบอร์	ต้องจัดให้มีการ ตรวจสอบด้านความ มั่นคงปลอดภัยไซเบอร์	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ ตรวจสอบภายใน หรือผู้เกี่ยวข้องผู้ตรวจสอบภายนอก อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยต้องส่งผลการตรวจสอบ สรุป รายงานการดำเนินการแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด 30 (สามสิบ) วันนับแต่วันที่ได้ดำเนินการแล้วเสร็จ 30 (สามสิบ) วัน 4. การปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการปรับปรุงแผนจากกรม หรือ สถาน	1.มีผู้รับผิดชอบตรวจสอบภายใน หรือผู้เกี่ยวข้อง ผู้ตรวจสอบภายนอก 2.ไม่มีการตรวจสอบการบริหารความมั่นคงปลอดภัยไซเบอร์ 3.มีรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 4.มีกระบวนการบริหารที่สำคัญ	17.1	WA		
		การรายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์	ต้องจัดให้มีการ รายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์	ต้องจัดส่งสรุปรายงานการตรวจสอบ ต่อสำนักงานภายใน กำหนด 30 (สามสิบ) วันนับแต่วันที่ได้ดำเนินการแล้วเสร็จ 30 (สามสิบ) วัน 3. แผนการดำเนินการปรับปรุงแก้ไขข้อบกพร่องหรือการไม่ ปฏิบัติตามข้อกำหนด 4. แผนการดำเนินการตามข้อกำหนด	1. รายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 2. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ ตรวจสอบที่เกี่ยวข้อง และหน่วยงานกำกับดูแล 3. กระบวนการใช้ข้อมูลหรือการนำไปใช้ตาม ข้อกำหนด 4. แนวทางการปรับปรุงแก้ไขข้อบกพร่องหรือการไม่ ปฏิบัติตามข้อกำหนด 5. แผนการดำเนินการตามข้อกำหนด 6. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล	17.2	CRS		
		การแก้ไขข้อบกพร่องหรือ การไม่ปฏิบัติตาม ข้อกำหนด	ต้องจัดให้มีการ ดำเนินการแก้ไขข้อบกพร่อง หรือการไม่ปฏิบัติตาม ข้อกำหนด	ในกรณีที่ไม่ปฏิบัติตามข้อ 33.4 ต้องส่งผลการดำเนินการ แก้ไขไปยังสำนักงานภายในกำหนด 30 (สามสิบ) วัน 30 (สามสิบ) วัน 3. แผนการดำเนินการปรับปรุงแก้ไขข้อบกพร่องหรือการไม่ ปฏิบัติตามข้อกำหนด 4. แผนการดำเนินการตามข้อกำหนด	1.เอกสารที่พิจารณาและดำเนินการปรับปรุงแผนจาก กรม หรือ สถาน 2. แผนการดำเนินการแก้ไขข้อบกพร่อง 3. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล	17.3	WA		
		การปรับปรุงแผนการ ดำเนินการตามการ	ต้องจัดให้มีการ ปรับปรุงแผนการ ดำเนินการตามการ	ในกรณี กทม. เห็นสมควรให้ปรับปรุงแผน ต้องดำเนินการ เพื่อส่งผลการดำเนินการแก้ไขถึงการปรับปรุงแล้วเสร็จ สำนักงาน	1.เอกสารที่พิจารณาและดำเนินการปรับปรุงแผนจาก กรม หรือ สถาน 2. แผนการดำเนินการแก้ไขข้อบกพร่อง 3. หลักฐานการส่งมอบข้อมูลไปยังหน่วยงานการ กำกับดูแล	17.4	Minor NC		

รูปที่ 5 ต้นแบบโปรแกรมการตรวจประเมิน (Audit Program)

รูปที่ 6 ต้นแบบแผนการตรวจประเมิน (Audit Plan)

รูปที่ 7 ต้นแบบรายงานการตรวจประเมิน (Audit Report)

ส่วนที่ 1 : สิ่งที่พบจากการตรวจสอบ (Audit Finding) (สำหรับผู้ตรวจสอบ)					
(1)ข้อ	(2)เลขอ้างอิงจาก หลักเกณฑ์ฯ	(3)หัวข้อ	(4)เลขอ้างอิงจาก ประมวลฯ	(5)รายละเอียดความไม่สอดคล้องประเด็นที่พบ	(6)ระดับความไม่สอดคล้อง
1					Major NC
2					Minor NC
3					C
4					OBS
5					OFI
6					
7					
8					
9					
10					

รูปที่ 8 ต้นแบบแบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)

ส่วนที่ 2 : แผนการแก้ไข (Corrective Action Plan) (สำหรับคณะทำงานหน่วยงานรัฐ หรือ CII)						
(1)วิเคราะห์สาเหตุ (Root Cause) (กรณีที่เป็น Major NC หรือ Minor NC)	(2) แผนการแก้ไข (Corrective Action Plan)	(3)สถานะการแก้ไข	(4)วันที่เริ่มต้น	(5)วันที่คาดว่าจะ แล้วเสร็จ	(6)วันที่แก้ไขแล้วเสร็จ	(7)หมายเหตุ/คำอธิบายเพิ่มเติม (ถ้ามี)
		รอดำเนินการ				
		อยู่ระหว่างดำเนินการ				
		เสร็จสิ้น				
		ล่าช้า				

รูปที่ 9 ต้นแบบแผนการแก้ไข (Corrective Action Plan)

ลับ
(Confidential)



รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)

ประจำปี

[ชื่อหน่วยงาน]

[วันที่จัดทำ]

รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)		รหัสเอกสาร: เลขที่:
สารบัญ หน้า		
1. บทนำ	4	
2. สถานะการดำเนินการจากงานครั้งก่อน (ถ้ามี)	4	
3. สรุปผลการตรวจสอบภายใน	5	
4. สรุปประเด็นประชุมชี้แจงการจากฝ่ายบริหาร (เพิ่มข้อมูลถึงการประชุม)	6	
5. ประเมินความเสี่ยงและผลกระทบ	7	
6. การเปลี่ยนแปลงภายในที่มีผลกระทบ	7	
7. ข้อเสนอแนะต่อทิศทางการพัฒนา	7	
8. การดำเนินการตามกฎหมาย	8	

ลับ (Confidential)

หน้า 3 จาก 8

รูปที่ 10 ต้นแบบรายงานการทบทวนโดยฝ่ายบริหาร (Management Review)

ชื่อเอกสาร	ชื่อผู้ประกอบการด้านความมั่นคงปลอดภัยไซเบอร์หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สอดคล้องตาม ประมวลกฎหมายปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน สำหรับ 4 บริการ							
เวอร์ชัน	1.0							
ทพว.	หัวข้อ	อ้างอิง ประมวล แนวทางปฏิบัติ ไซบี	สาระสำคัญ (ประมวลแนวทางปฏิบัติ/ทพว.)	CSF 1.1	NIST CSF 2.0	ISO/IEC27001:2022	ISO/IEC27701:2025	ISO/IEC27017:2015
3.1 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคบังคับ (Mandatory)								
ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ								
3.1.1	การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์	17.1	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง	ID.GV-3	GV/OC-03	Clause 9.2.1, Clause 9.2.2, Annex A 5.35, Annex A 5.36	Clause 9.2.1, Clause 9.2.2, A.3.15, A.3.16	18.2.1
3.1.2	การรายงานการตรวจสอบด้านความมั่นคง ปลอดภัยไซเบอร์	17.2	ต้องจัดส่งสรุปรายงานการตรวจสอบ ต่อสำนักงานภายใน กำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ได้รับผลการตรวจสอบ	ID.GV-3	GV/OC-03	Clause 7.4, Annex A 5.5	Clause 7.4	-
3.1.3	การแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตาม ข้อกำหนด	17.3	ในกรณีที่ไม่ปฏิบัติตามข้อ ๑๗.๑ ต้องส่งผลการดำเนินการ แก้ไขไปสำนักงานภายในกำหนด ๓๐ (สามสิบ) วัน	ID.RA-6, RS.MI-3	ID.IM-01, ID.RA-06	Clause 10.2	Clause 10.2	-
3.1.4	การปรับปรุงแผนการดำเนินงานการแก้ไข	17.4	ในกรณีที่มี กม. เห็นสมควรให้ปรับปรุงแผน ต้องดำเนินการ และเสนอผลการดำเนินการแก้ไขที่ได้รับการปรับปรุงแก้ไขให้ สำนักงาน	ID.GV-3	GV/OC-03	Clause 10.2	Clause 10.2	-
3.1.5	การดำเนินการแก้ไขข้อบกพร่อง	17.5	เมื่อแผนได้รับการเห็นชอบ ต้องดำเนินการตามแผนการ ดำเนินการแก้ไขข้อบกพร่อง แล้วเสร็จภายในกำหนดระยะเวลา	ID.RA-6, RS.MI-3	ID.IM-01, ID.RA-06	Clause 10.2	Clause 10.2	-

รูปที่ 11 ต้นแบบข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ

ทั้งนี้ เอกสารต้นแบบและชุดเครื่องมือสำหรับการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทาง
สารสนเทศฉบับสมบูรณ์ จะถูกนำไปใช้เป็นเนื้อหาหลักในการจัดอบรมเชิงปฏิบัติการ เพื่อถ่ายทอด
ผลการศึกษา และทดสอบการใช้งาน ในลำดับต่อไป

บทที่ 3 หลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลตามแนวทาง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เอกสารฉบับนี้กำหนดแนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจำแนกออกเป็น 2 ส่วนหลัก ดังนี้

แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อกำหนดหลักที่ต้องปฏิบัติ (Mandatory Requirements) ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด โดยอ้างอิงตามประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 และมาตรฐานขั้นต่ำ พ.ศ. 2566 เพื่อรักษามาตรฐานความปลอดภัยพื้นฐานในระดับประเทศ ทั้งนี้ จำนวนหัวข้อที่หน่วยงานต้องรับการตรวจประเมินจะแปรผันตามผลการประเมินและการจัดระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศ ตามหลักเกณฑ์ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 โดยแบ่งเกณฑ์การตรวจประเมินออกเป็น 3 ระดับ ดังนี้ ระดับต่ำ จำนวน 34 ข้อ ระดับกลาง จำนวน 43 ข้อ และระดับสูง จำนวน 60 ข้อ

แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามแนวทางปฏิบัติที่ดี (Best Practices) ชุดข้อเสนอแนะในการตรวจประเมินเพิ่มเติมที่มุ่งเน้นการยกระดับขีดความสามารถในการบริหารจัดการความเสี่ยงทางไซเบอร์ โดยประยุกต์ใช้มาตรฐานสากลที่เกี่ยวข้อง เพื่อให้หน่วยงานสามารถตอบสนองต่อภัยคุกคามที่มีความซับซ้อนได้อย่างมีประสิทธิภาพและยั่งยืน จำนวน 19 ข้อ

3.1 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อกำหนดหลักที่ต้องปฏิบัติ (Mandatory Requirements)

แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อกำหนดหลักที่ต้องปฏิบัติ (Mandatory Requirements) จะประกอบไปด้วย 2 ส่วน ได้แก่ แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ (ข้อ 17 – 19) และ แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (ข้อ 21 - 25) แห่งประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 รวมทั้งหมด 60 ข้อ ซึ่งครอบคลุมเนื้อหา 2 ส่วน ได้แก่

ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ

แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ มีทั้งหมด 13 ข้อ โดยครอบคลุมการตรวจสอบตามประมวลแนวทางปฏิบัติ (ข้อ 17 – 19) แห่งประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ดังนี้

- องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน 5 ข้อ
- องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน 4 ข้อ
- องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์ จำนวน 4 ข้อ

ส่วนที่ 2 : แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ มีทั้งหมด 47 ข้อ โดยครอบคลุมการตรวจสอบตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (ข้อ 21 - 25) แห่งประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ดังนี้

- การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) จำนวน 20 ข้อ
- มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) จำนวน 16 ข้อ
- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) จำนวน 2 ข้อ
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) จำนวน 7 ข้อ
- มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) จำนวน 2 ข้อ

การตรวจประเมินตามแนวทางภาคบังคับทั้งสองส่วน มีรายละเอียดของข้อกำหนดที่ต้องดำเนินการตรวจสอบและประเมินผล ดังนี้

ส่วนที่ 1 : แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ

องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
3.1.1 การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการปฏิบัติตามกฎหมายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดอย่างต่อเนื่อง
ความเสี่ยง
มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ของหน่วยงานไม่สอดคล้องกับข้อกำหนดตามกฎหมาย และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงไม่สามารถรับมือกับรูปแบบภัยคุกคามที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ
การควบคุมที่พึงมี
ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้ (ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) (ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและให้บริการ ตามผลการวิเคราะห์ในข้อ (ก) (ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้อง กับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด
แนวทางการประเมิน
1. ตรวจสอบการแต่งตั้งผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ว่าได้รับอนุมัติอย่างเป็นทางการ มีความเป็นอิสระ และมีความสามารถตรงตามเกณฑ์ 2. ตรวจสอบแผนการตรวจสอบประจำปีให้ครอบคลุมการดำเนินการอย่างน้อยปีละ 1 ครั้ง

3. ตรวจสอบขอบเขตการตรวจสอบว่าครอบคลุมกระบวนการ BIA บริการที่สำคัญ (CII) และการปฏิบัติตามกฎหมาย/ประมวลแนวทางปฏิบัติฯ อย่างครบถ้วน
4. ตรวจสอบว่าวิธีการประเมินมีการดำเนินการทั้งการตรวจสอบตามข้อกำหนด (Compliance) และการตรวจสอบตามความเสี่ยง (Risk-based)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 17.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 1
NIST CSF 2.0	GV.OC-03
ISO/IEC27001:2022	Clause 9.2.1, Clause 9.2.2, Annex A 5.35, Annex A 5.36
ISO/IEC27701:2025	Clause 9.2.1, Clause 9.2.2, A.3.15, A.3.16
ISO/IEC27017:2015	18.2.1
ISO/IEC27007:2020	A.6.1, A.6.2
ISO/IEC TS 27008:2019	18.2.1, 18.2.2, 18.2.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีหลักเกณฑ์การพิจารณาคุณสมบัติ ความเชี่ยวชาญ และความเป็นอิสระของผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างไร
2. หน่วยงานมีการกำหนดขอบเขตการตรวจสอบอย่างไร ครอบคลุมบริการที่สำคัญตามกระบวนการ BIA บริการที่สำคัญ (CII) และการปฏิบัติตามกฎหมาย/ประมวลแนวทางปฏิบัติฯ หรือไม่
3. หน่วยงานมีการกำหนดวิธีการตรวจสอบหรือไม่ ครอบคลุมทั้งการตรวจสอบตามข้อกำหนด (Compliance) และการตรวจสอบตามความเสี่ยง (Risk-based) หรือไม่

■ การสอบทานเอกสาร

1. สอบทานคำสั่งแต่งตั้งหรือสัญญาจ้างผู้ตรวจสอบเทียบกับคุณสมบัติและใบรับรอง
2. สอบทานแผนการตรวจสอบประจำปีเพื่อยืนยันรอบระยะเวลาและขอบเขต
3. สอบทานความสอดคล้องของรายงาน BIA กับขอบเขตบริการที่นำมาตรวจสอบ
4. สอบทานผลการปฏิบัติตามกฎหมาย มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด อย่างน้อย ดังนี้
 - ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 (มีผลบังคับใช้ 10 พฤษภาคม 66) – กำหนดให้หน่วยงานเมื่อเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ต้องแจ้งหรือรายงานเหตุกับ สกมช. หรือ หน่วยงานกำกับดูแลโดยใช้เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ และเอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

- ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (มีผลบังคับใช้ 10 กันยายน 69) - ดำเนินการตรวจรับรองฯ (ขึ้นอยู่กับประเภทการดำเนินงานด้านคลาวด์ของหน่วยงาน และระดับผลกระทบของข้อมูล) และส่งผลการตรวจรับรองต่อ สกมช. อย่างน้อยปีละ 1 ครั้ง - ประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ พ.ศ. 2568 (มีผลบังคับใช้ 16 กันยายน 69) - ประเมินตนเอง (Self-Assessment) ตามแบบฟอร์ม คด อย่างน้อยปีละครั้ง (จัดเก็บที่หน่วยงาน กรณีผลกระทบระดับต่ำหรือกลาง และสำเนาถึง กมช. กรณีผลกระทบระดับสูง) - กรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล (มติ ครม. วันที่ 2 กันยายน 2568 คณะรัฐมนตรีมีมติเห็นชอบ และอนุมัติให้ทุกหน่วยงานนำไปดำเนินการ) - การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ทุกระบบงาน เพื่อป้องกันการเข้าถึงโดยผู้ไม่หวังดี และลดความเสี่ยงจากการถูกเจาะระบบ (โดยที่ประชุม กมช. ครั้งที่ 2/2569 เมื่อวันที่ 15 พฤษภาคม 2569 มีมติให้ สกมช. เสนอเรื่องต่อคณะรัฐมนตรีเพื่อพิจารณากำหนดให้หน่วยงานของรัฐทุกแห่งบังคับใช้มาตรการดังกล่าว)
■ เอกสารที่เกี่ยวข้อง 1. คำสั่งแต่งตั้งผู้ตรวจสอบภายใน หรือสัญญาจ้างผู้ตรวจสอบภายนอก 2. แผนการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ 3. รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 4. ทะเบียนรายการบริการที่สำคัญ ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

3.1.2 การรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานปฏิบัติตามเงื่อนไขระยะเวลาที่กฎหมายกำหนดในการรายงานผลการตรวจประเมินต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแล
ความเสี่ยง
หน่วยงานอาจถูกดำเนินการลงโทษทางปกครองหรือได้รับโทษปรับตามกฎหมายเนื่องจากส่งรายงานล่าช้า
การควบคุมที่พึงมี
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด 30 (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานประกาศกำหนด
แนวทางการประเมิน

1. ตรวจสอบวันที่ดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์แล้วเสร็จ (วันที่ผู้บริหารสูงสุดของหน่วยงานรับทราบรายงานการตรวจสอบเป็นลายลักษณ์อักษร) 2. ตรวจสอบหลักฐานและกระบวนการจัดส่งรายงานผลการตรวจสอบให้ สกมช. 3. ตรวจสอบเทียบระยะเวลาการส่งว่าอยู่ภายใน 30 วันนับแต่วันที่แล้วเสร็จ (และต้องไม่เกินวันที่ 30 มกราคม ของปีถัดไป) 4. ตรวจสอบการส่งสำเนารายงานให้แก่หน่วยงานควบคุมหรือกำกับดูแล	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 17.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 1
NIST CSF 2.0	GV.OC-03
ISO/IEC27001:2022	Clause 7.4, Annex A 5.5
ISO/IEC27701:2025	Clause 7.4
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.4.4
ISO/IEC TS 27008:2019	6.1.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. กระบวนการนำเสนอรายงานผลการตรวจสอบต่อผู้บริหารสูงสุดเพื่อลงนามรับทราบ มีขั้นตอนและกรอบเวลาอย่างไร 2. หน่วยงานมีการลงบันทึกรับ-ส่ง หรือติดตามอย่างไร เพื่อยืนยันว่าการส่งรายงานต่อ สกมช. เกิดขึ้นภายใน 30 วัน 3. หน่วยงานมีกระบวนการนำเสนอให้แก่หน่วยงานควบคุมหรือกำกับดูแลอย่างไร ■ การสอบทานเอกสาร 1. สอบทานรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารสูงสุด ว่ามีการลงนามรับทราบ 2. สอบทานบันทึกรับ-ส่งรายงานผลการตรวจสอบ เพื่อยืนยันว่าการส่งรายงานต่อ สกมช. เกิดขึ้นภายใน 30 วัน 3. สอบทานบันทึกรับ-ส่งสำเนาให้แก่หน่วยงานควบคุมหรือกำกับดูแล ■ เอกสารที่เกี่ยวข้อง 1. รายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 2. หลักฐานการส่งมอบ/หนังสือนำเสนอรายงานการตรวจสอบให้แก่ สกมช. และหน่วยงานกำกับดูแล ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	

3.1.3 การแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการแก้ไขข้อบกพร่อง หรือการไม่ปฏิบัติตามข้อกำหนดที่ตรวจพบจากการตรวจสอบอย่างเป็นระบบ

ความเสี่ยง

ข้อบกพร่องที่ตรวจสอบพบ ไม่ได้รับการปรับปรุงอย่างเหมาะสมและทันเวลา

การควบคุมที่พึงมี

ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ระบุการไม่ปฏิบัติตามข้อ 17.1 เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด 30 (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

- (ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ
- (ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ (ก)

แนวทางการประเมิน

1. ตรวจสอบรายการข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด ที่ระบุในรายงานการตรวจสอบ
2. ตรวจสอบแผนการดำเนินการแก้ไข (Corrective Action Plan) ว่ามีการวิเคราะห์สาเหตุ (Root Cause) และระบุรายละเอียดวิธีการจัดการอย่างครบถ้วน
3. ตรวจสอบการกำหนดระยะเวลา (Expected Due Date) สำหรับการดำเนินการแก้ไขในแต่ละกิจกรรม
4. ตรวจสอบหลักฐานการจัดส่งแผนการดำเนินการแก้ไขให้ สกมช. ภายใน 30 วันนับจากวันที่ได้รับรายงานการตรวจสอบ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 17.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 1
NIST CSF 2.0	ID.IM-01, ID.RA-06
ISO/IEC27001:2022	Clause 10.2
ISO/IEC27701:2025	Clause 10.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.7.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนดอย่างไร

- เมื่อพบข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด หน่วยงานมีกระบวนการวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause Analysis) อย่างไร - หน่วยงานมีการพิจารณาและอนุมัติแผนการแก้ไขพร้อมกำหนดกรอบเวลาให้เสร็จสิ้นภายใน 30 วันอย่างไร
■ การสอบทานเอกสาร - สอบทานแผนการดำเนินการแก้ไข ว่ามีการระบุสาเหตุ กิจกรรมการแก้ไข กำหนดเวลา ผู้รับผิดชอบ และได้รับการอนุมัติจากผู้มีอำนาจ - สอบทานหลักฐานและวันที่ในการส่งแผนดังกล่าวไปยัง สกมช. ■ เอกสารที่เกี่ยวข้อง - กระบวนการแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด - แบบฟอร์มการร้องขอให้แก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด - แผนการดำเนินการแก้ไข - หลักฐานการส่งหนังสือนำส่งแผนการดำเนินการแก้ไขให้ สกมช. ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

3.1.4 การปรับปรุงแผนการดำเนินงานการแก้ไข	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีการปรับปรุงและแก้ไขรายละเอียดในแผนการดำเนินการแก้ไข ให้มีความครบถ้วน สอดคล้องตามคำแนะนำหรือข้อสังเกตของ กกม. และมีการประสานงานร่วมกับหน่วยงานกำกับดูแลอย่างเป็นระบบ	
ความเสี่ยง	
มาตรการแก้ไขไม่เพียงพอต่อการรับมือกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	
การควบคุมที่พึงมี	
ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย	
แนวทางการประเมิน	
- ตรวจสอบข้อสั่งการหรือหนังสือแจ้งผลพิจารณาจาก กกม. ในกรณีที่ไม่เห็นชอบและให้ปรับปรุงแผนการแก้ไข - ตรวจสอบการปรับปรุงรายละเอียดในแผนการดำเนินการแก้ไขของหน่วยงาน ว่าสอดคล้องกับคำแนะนำของ กกม. หรือไม่ - ตรวจสอบหลักฐานการจัดส่งแผนฉบับปรับปรุงไปยัง สกมช. ภายในระยะเวลาที่กำหนดใหม่ - ตรวจสอบการจัดส่งสำเนาแผนฉบับปรับปรุงให้หน่วยงานควบคุมหรือกำกับดูแล	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 17.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 1

NIST CSF 2.0	GV.OC-03
ISO/IEC27001:2022	Clause 10.2
ISO/IEC27701:2025	Clause 10.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.7.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีกลไกในการตอบสนองและปรับปรุงแผนการดำเนินการแก้ไขอย่างไร เมื่อได้รับข้อสั่งการให้ปรับปรุงแผนจาก กกม. 2. ผู้บริหารมีการติดตามการปรับปรุงแผนการดำเนินการแก้ไขอย่างไร เพื่อให้ทันต่อรอบเวลาใหม่ ■ การสอบทานเอกสาร 1. สอบทานหนังสือแจ้งผลการพิจารณาหรือข้อสั่งการจาก กกม./สกมช. 2. สอบทานแผนดำเนินการแก้ไขฉบับปรับปรุง เทียบกับข้อเสนอแนะของ กกม. 3. สอบทานหลักฐานการนำส่งแผนฉบับปรับปรุงไปยัง สกมช. 4. สอบทานการจัดส่งสำเนาแผนฉบับปรับปรุงให้หน่วยงานควบคุมหรือกำกับดูแล ■ เอกสารที่เกี่ยวข้อง 1. เอกสารแจ้งข้อเสนอแนะ/คำสั่งให้ปรับปรุงแผนจาก กกม. หรือ สกมช. 2. แผนการดำเนินการแก้ไขฉบับปรับปรุง 3. หลักฐานการส่งหนังสือนำส่งแผนฉบับปรับปรุง 4. หลักฐานการจัดส่งสำเนาแผนฉบับปรับปรุง ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

3.1.5 การดำเนินการแก้ไขข้อบกพร่อง
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานได้ปฏิบัติตามแผนการดำเนินงานการแก้ไขที่ได้รับความเห็นชอบจาก กกม. ให้แล้วเสร็จครบถ้วนภายในระยะเวลาที่กำหนด
ความเสี่ยง
ข้อบกพร่องที่ตรวจสอบพบ ไม่ได้รับการปรับปรุงอย่างเหมาะสมและทันเวลา
การควบคุมที่พึงมี

เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

แนวทางการประเมิน

1. ตรวจสอบหนังสือหรือหลักฐานการให้ความเห็นชอบแผนดำเนินการแก้ไขจาก กกม.
2. ตรวจสอบสถานะความคืบหน้าของการดำเนินการแก้ไขข้อบกพร่องจริงเทียบกับแผนที่กำหนดไว้
3. ตรวจสอบผลการดำเนินการว่ามีการแก้ไขข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนดทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุ
4. ตรวจสอบผลการตรวจติดตาม (Follow-up) จากผู้ตรวจสอบ เพื่อยืนยันการปิดข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 17.5
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 1
NIST CSF 2.0	ID.IM-01, ID.RA-06
ISO/IEC27001:2022	Clause 10.2
ISO/IEC27701:2025	Clause 10.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.7.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีการบันทึกหนังสือหรือหลักฐานการให้ความเห็นชอบแผนดำเนินการแก้ไขจาก กกม. อย่างไร
2. หน่วยงานมีการติดตามสถานะความคืบหน้าของการดำเนินการแก้ไขข้อบกพร่องจริงเทียบกับแผนที่กำหนดไว้อย่างไร
3. หากพบว่ากิจกรรมใดมีความเสี่ยงที่จะแก้ไขล่าช้ากว่าแผนดำเนินการแก้ไข หน่วยงานมีกระบวนการรายงานต่อผู้บริหาร หรือขอขยายเวลาอย่างไร
4. ผู้ตรวจสอบมีเกณฑ์พิจารณาอย่างไร เพื่อให้มั่นใจว่าข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด ถูกแก้ไขโดยสมบูรณ์แล้ว

■ การสอบทานเอกสาร

1. สอบทานหนังสือหรือหลักฐานการให้ความเห็นชอบแผนดำเนินการแก้ไขจาก กกม.
2. สอบทานความคืบหน้าในการแก้ไขเทียบกับแผนดำเนินการแก้ไขที่กำหนดไว้
3. สอบทานกระบวนการรายงานต่อผู้บริหาร หรือการขอขยายเวลา ในกรณีที่มีการแก้ไขล่าช้ากว่าแผนดำเนินการแก้ไข

- เอกสารที่เกี่ยวข้อง
 1. หนังสือหรือหลักฐานการให้ความเห็นชอบแผนดำเนินการแก้ไขจาก กกม.
 2. แบบฟอร์มการดำเนินการแก้ไขที่ระบุวันที่เสร็จจริงและสถานะดำเนินการ
 3. บันทึก/หลักฐานการดำเนินการแก้ไขทางเทคนิค (เช่น System Logs, Patch Reports)
 4. บันทึกการประชุม/รายงานในกรณีที่มีการแก้ไขล่าช้ากว่าแผนดำเนินการแก้ไข
- เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.1.6 การประเมินความเสี่ยง

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานได้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม

ความเสี่ยง

ไม่สามารถระบุและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสม

การควบคุมที่พึงมี

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องมีการดำเนินการด้านการประเมินความเสี่ยง (Risk Assessment) ครอบคลุมหัวข้อดังต่อไปนี้

- (ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก
- (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม
- (ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการทำงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

แนวทางการประเมิน

1. ตรวจสอบกระบวนการประเมินความเสี่ยง (Risk Assessment) ของหน่วยงาน ว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ค)
2. ตรวจสอบความสอดคล้องของการดำเนินการประเมินความเสี่ยง (Risk Assessment) กับกระบวนการประเมินความเสี่ยง (Risk Assessment) ที่กำหนด
3. ตรวจสอบการระบุความเสี่ยง (Risk Identification) ว่าครอบคลุมภัยคุกคามทางไซเบอร์และช่องโหว่จากกระบวนการ ระบบงาน บุคลากร และปัจจัยภายนอกอย่างครบถ้วน

4. ตรวจสอบเกณฑ์การวิเคราะห์ความเสี่ยง (Risk Analysis) เช่น ประเมินโอกาสเกิด (Likelihood) และผลกระทบ (Impact) และเกณฑ์การประเมินค่าความเสี่ยง (Risk Evaluation)
5. ตรวจสอบการกำหนดระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 18.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2
NIST CSF 2.0	GV.RM-02, ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05
ISO/IEC27001:2022	Clause 4.1, Clause 6.1.2
ISO/IEC27701:2025	Clause 4.1, Clause 6.1.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.1.1, A.3.1.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการประเมินความเสี่ยง (Risk Assessment) อย่างไร
2. หน่วยงานกำหนดรอบในการประเมินความเสี่ยง (Risk Assessment) อย่างไร
3. หน่วยงานมีเกณฑ์หรือวิธีการระบุภัยคุกคามและช่องโหว่อย่างไรให้ครอบคลุมทรัพย์สินและบริการที่สำคัญทั้งหมด
4. หน่วยงานมีการประเมินโอกาสเกิด (Likelihood) และผลกระทบ (Impact) โดยอ้างอิงจากข้อมูลหรือสถิติใดบ้าง
5. การกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) มีการพิจารณาอย่างไร ได้รับการอนุมัติจากผู้บริหารสูงสุดหรือไม่

■ การสอบทานเอกสาร

1. สอบทานกระบวนการประเมินความเสี่ยง (Risk Assessment) ของหน่วยงาน ว่าครอบคลุมการระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินค่าความเสี่ยง (Risk Evaluation) ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ค)
2. สอบทานทะเบียนความเสี่ยง (Risk Register) เพื่อยืนยันว่ามีการระบุภัยคุกคาม (Threats) และช่องโหว่ (Vulnerabilities) ที่เป็นปัจจุบัน รายการความเสี่ยงที่ระบุไว้สอดคล้องกับบริบทของหน่วยงานโครงสร้างพื้นฐานสำคัญ (CII) และมีการกำหนดเจ้าของความเสี่ยง (Risk Owner) ที่ชัดเจนเพื่อรับผิดชอบต่อความเสี่ยงนั้น ๆ

3. สอบทานเกณฑ์การประเมินความเสี่ยง ว่าเกณฑ์การให้คะแนนโอกาสเกิด (Likelihood) และผลกระทบ (Impact) มีค่านิยามที่ชัดเจน และมีการคำนวณระดับความเสี่ยงสอดคล้องตลอดทั้งทะเบียนความเสี่ยง 4. ตรวจสอบเอกสารการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ว่าได้รับการอนุมัติจากผู้บริหารระดับสูง ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure) 2. ทะเบียนความเสี่ยง (Risk Register) 3. รายงานการประเมินความเสี่ยง (Risk Assessment Report) 4. เอกสารกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.1.7 การจัดการความเสี่ยง
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม
ความเสี่ยง
การจัดการความเสี่ยงไม่เหมาะสม ส่งผลให้ระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) สูงกว่าระดับที่หน่วยงานยอมรับได้
การควบคุมที่พึงมี
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องมีการดำเนินการด้านการจัดการความเสี่ยง (Risk Treatment) ครอบคลุมหัวข้อดังต่อไปนี้ 1. ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ใน ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึง ความสมดุลระหว่าง ต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ 2. ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำเร็จของ ความมั่นคง ปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง
แนวทางการประเมิน
1. ตรวจสอบการกำหนดแนวทางการจัดการความเสี่ยง (Risk Treatment) เช่น การลด โอนย้าย หลีกเลี่ยง หรือยอมรับความเสี่ยง ว่ามีความเหมาะสม 2. ตรวจสอบมาตรการควบคุมและป้องกันความเสี่ยงที่เลือกใช้ ว่าสามารถลดความเสี่ยงที่เหลืออยู่ (Residual Risk) ให้อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงความสมดุลด้านต้นทุนและผลประโยชน์ 3. ตรวจสอบการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ให้สอดคล้องกับ ความสำคัญของการดำเนินธุรกิจ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 18.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2
NIST CSF 2.0	GV.RM-04, ID.RA-06
ISO/IEC27001:2022	Clause 6.1.3, Clause 6.2, Clause 8.3, Clause 9.1
ISO/IEC27701:2025	Clause 6.1.3, Clause 6.2, Clause 8.3, Clause 9.1
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A3.1.3, A3.2, A.5.2, A.5.3
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีหลักเกณฑ์การพิจารณาเลือกแนวทางการจัดการความเสี่ยง (การลด โอนย้าย หลีกเลี่ยง หรือยอมรับความเสี่ยง) อย่างไร
2. ในกรณีที่เป็นที่ยอมรับความเสี่ยง มีการขออนุมัติจากผู้บริหารหรือไม่ และมีขั้นตอนอย่างไร
3. หน่วยงานมีการกำหนด KRI อย่างไร และ KRI ที่กำหนด มีความเชื่อมโยงและสามารถใช้เป็นสัญญาณเตือนภัยล่วงหน้า (Early Warning) ได้อย่างไร

■ การสอบทานเอกสาร

1. สอบทานแผนการจัดการความเสี่ยง ว่าได้ระบุกิจกรรม กำหนดเวลา ผู้รับผิดชอบ และแนวทางการจัดการความเสี่ยง ประเมินการคะแนนความเสี่ยงคงเหลือหลังจากจัดการ
2. สอบทานหลักฐานการพิจารณาและลงนามอนุมัติยอมรับความเสี่ยงโดยผู้บริหารระดับสูง ว่ารับทราบและยอมรับผลที่อาจเกิดขึ้น
3. สอบทานเอกสารกำหนดรายการตัวชี้วัด KRI ว่ามีความสอดคล้องกับเป้าหมายทางธุรกิจและภัยคุกคามสำคัญ (เช่น จำนวนครั้งที่พบความพยายามเจาะระบบ, ระยะเวลาที่ระบบล่ม)

■ เอกสารที่เกี่ยวข้อง

1. แผนการจัดการความเสี่ยง
2. เอกสารขออนุมัติยอมรับความเสี่ยง
3. รายการตัวชี้วัด KRI

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.8 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการเฝ้าระวังและปรับปรุงสถานะความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

ความเสี่ยง

มาตรการในการจัดการความเสี่ยงไม่เหมาะสมต่อสถานะความเสี่ยงด้านไซเบอร์ที่เปลี่ยนแปลงไป

การควบคุมที่พึงมี

การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ ที่กำหนดไว้

แนวทางการประเมิน

1. ตรวจสอบกระบวนการติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ว่ามีการดำเนินการอย่างต่อเนื่องและมีประสิทธิภาพ
2. ตรวจสอบกระบวนการติดตามระดับความเสี่ยง เพื่อให้มั่นใจว่าความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ยังคงอยู่ภายใต้ระดับที่ยอมรับได้

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 18.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2
NIST CSF 2.0	GV.RM-06
ISO/IEC27001:2022	Clause 9.1, Clause 9.3.2
ISO/IEC27701:2025	Clause 9.1, Clause 9.3.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.5.3, A.6.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. สถานะความคืบหน้าของแผนจัดการความเสี่ยงของหน่วยงานในปัจจุบันเป็นอย่างไร
2. หน่วยงานมีกลไกในการเฝ้าระวังและติดตามสถานะความเสี่ยงตามรอบระยะเวลาอย่างไร
3. มีการเปลี่ยนแปลงในองค์กรที่ส่งผลกระทบต่อความเสี่ยงหรือไม่ เช่น การเปลี่ยนโครงสร้างบริหาร การนำเทคโนโลยีใหม่มาใช้ หรือการปรับเปลี่ยนกระบวนการทำงาน
4. หน่วยงานมีการติดตามสถานการณ์ภายนอก เช่น กฎหมาย/ระเบียบข้อบังคับใหม่จากหน่วยงานกำกับดูแล (เช่น สคส. หรือ สกมช.), แนวโน้มภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่ส่งผลกระทบต่อความเสี่ยงหรือไม่
5. หากพบว่าความเสี่ยงเริ่มเกินระดับที่ยอมรับได้ หน่วยงานมีกระบวนการตอบสนองต่อความเสี่ยงนั้นอย่างไร

■ การสอบทานเอกสาร 1. สอบทานความคืบหน้าของกิจกรรมการจัดการความเสี่ยงตามที่กำหนดไว้ในแผน เช่น สถานะของแต่ละกิจกรรม, วันที่ดำเนินการแล้วเสร็จ หากกิจกรรมใดล่าช้ากว่าแผน ต้องมีการระบุสาเหตุและมีการปรับเปลี่ยนแนวทางเพื่อให้ความเสี่ยงยังอยู่ภายใต้การควบคุม และได้รับการอนุมัติ 2. สอบทานบันทึกการประชุมหรือรายงานผลการทบทวนความเสี่ยงประจำรอบ (เช่น รายไตรมาส/รายเดือน) เพื่อยืนยันว่าหน่วยงานมีการทบทวนความเสี่ยงตามรอบเวลาที่กำหนด ■ เอกสารที่เกี่ยวข้อง 1. แผนการจัดการความเสี่ยง 2. บันทึกการประชุม/รายงานผลการทบทวนความเสี่ยงประจำรอบ ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.1.9 การรายงานความเสี่ยง (Risk Reporting)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานได้สื่อสารระดับความเสี่ยงและสถานะการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ไปยังคณะกรรมการหรือผู้บริหารระดับสูงอย่างสม่ำเสมอ	
ความเสี่ยง	
คณะกรรมการหรือผู้บริหารระดับสูงไม่สามารถตัดสินใจและสั่งการในการจัดการความเสี่ยงได้อย่างทันท่วงที	
การควบคุมที่พึงมี	
การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ ของหน่วยงานที่ได้รับมอบหมาย ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น	
แนวทางการประเมิน	
1. ตรวจสอบการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยง เสนอต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย 2. ตรวจสอบความถี่ในการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยง โดยดำเนินการอย่างน้อยปีละ 1 ครั้ง 3. ตรวจสอบการทบทวนนโยบายและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 18.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2

NIST CSF 2.0	GV.RM-03, GV.RM-05
ISO/IEC27001:2022	Clause 5.1, Clause 5.2, Clause 8.2, Clause 9.3.1, Clause 9.3.3, Clause 10.1
ISO/IEC27701:2025	Clause 5.1, Clause 5.2, Clause 8.2, Clause 9.3.1, Clause 9.3.3, Clause 10.1
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.2.1, A.2.2, A.5.1, A.6.2, A.6.3, A.7.1
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. รวบรวมรายงานระดับความเสี่ยงต่อคณะกรรมการหรือผู้บริหารของหน่วยงานเป็นอย่างไร และมีการนำข้อเสนอแนะมาปรับปรุงอย่างไร 2. หน่วยงานมีการกำหนดกรอบการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างไร 3. หน่วยงานมีการพิจารณาการเปลี่ยนแปลงอย่างมีนัยสำคัญอย่างไร เพื่อกระตุ้นให้เกิดการทบทวนกระบวนการบริหารความเสี่ยงก่อนถึงรอบ 1 ปี ■ การสอบทานเอกสาร 1. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) ที่นำเสนอต่อคณะกรรมการหรือผู้บริหารของหน่วยงาน 2. สอบทานรายงานการประชุมเพื่อยืนยันการรับทราบและข้อสั่งการจากคณะกรรมการหรือผู้บริหารของหน่วยงาน 3. สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของเอกสารที่เกี่ยวข้อง เช่น นโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure) ระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง 4. สอบทานรายงานการประชุมและผลการพิจารณาการเปลี่ยนแปลงอย่างมีนัยสำคัญ ■ เอกสารที่เกี่ยวข้อง 1. รายงานการประเมินความเสี่ยง (Risk Assessment Report) 2. รายงานการประชุมความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการหรือผู้บริหารของหน่วยงาน 3. นโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์
3.1.10 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการจัดทำแผนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ครอบคลุมและชัดเจน สามารถตอบสนองต่อเหตุการณ์ได้อย่างเป็นระบบ
ความเสี่ยง
การจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์ล่าช้า ส่งผลให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของหน่วยงาน
การควบคุมที่พึงมี
หน่วยงานต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้ (ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ (ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่า หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ (ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT (ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process) (ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ (ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติ การบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี (ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ
แนวทางการประเมิน
1. ตรวจสอบการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) มีเนื้อหาครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ณ) และมีการอนุมัติโดยผู้บริหาร รวมถึงการทบทวนแผนให้เป็นปัจจุบัน

2. ตรวจสอบว่ามีการกำหนดบทบาท ความรับผิดชอบ และรายละเอียดการติดต่อของทีมงานไว้อย่างชัดเจน
3. ตรวจสอบโครงสร้างการรายงานเหตุการณ์ ยืนยันว่าในแผนมีการระบุขั้นตอนและกำหนดเวลาการรายงานเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (Regulator) ตามที่กฎหมายกำหนด
4. ตรวจสอบว่าแผนการรับมือภัยคุกคามทางไซเบอร์ มีขั้นตอนการจำกัดขอบเขต (Containment) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process) และการสอบสวน (Investigation)
5. ตรวจสอบการบริหารจัดการพยานหลักฐาน (Digital Forensics) ว่ามีขั้นตอนการเก็บรักษาพยานหลักฐาน (Preservation) และบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) เพื่อรองรับการดำเนินคดีตามกฎหมาย
6. ตรวจสอบความถูกต้องของข้อมูลการติดต่อบุคคลภายนอก (Engagement Protocols) เช่นผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ หรือหน่วยงานบังคับใช้กฎหมาย

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 19.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 3
NIST CSF 2.0	GV.RR-02, GV.RR-03, ID.IM-04, RS.CO-02, RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05
ISO/IEC27001:2022	Clause 4.2, Clause 5.3, Clause 7.1, Annex A 5.2, Annex A 5.24, Annex A 5.25, Annex A 5.26, Annex A 5.27, Annex A 5.28, Annex A 6.8
ISO/IEC27701:2025	Clause 4.2, Clause 5.3, Clause 7.1, A.3.4, A.3.11, A.3.12
ISO/IEC27017:2015	6.1.1, 16.1.1, 16.1.2, 16.1.7
ISO/IEC27007:2020	A.1.2, A.2.3, A.4.1
ISO/IEC TS 27008:2019	6.1.1, 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6, 16.1.7
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3), ข้อ 5

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีเกณฑ์การแบ่งระดับความรุนแรงของเหตุการณ์อย่างไรเพื่อให้สอดคล้องกับระยะเวลาการรายงานต่อ สกมช. และใครคือผู้รับผิดชอบในการรายงานให้ทันตามกรอบเวลา 24 ชม.

2. ใครคือผู้มีอำนาจสั่งการให้เรียกใช้งานแผนการรับมือภัยคุกคามทางไซเบอร์ มีเกณฑ์การตัดสินใจ อย่างไร
3. ในขั้นตอนการจำกัดขอบเขต (Containment) ทีมงานมีวิธีการตรวจสอบอย่างไรเพื่อให้มั่นใจว่าพยานหลักฐานดิจิทัลจะไม่ถูกทำลายหรือเปลี่ยนแปลงก่อนที่จะทำการกู้คืนระบบ

■ **การสอบทานเอกสาร**

1. สอบทานแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อยืนยันความครบถ้วนของการควบคุมที่พึงมีข้อ (ก) - (ณ) และยืนยันการลงนามอนุมัติโดยผู้บริหาร
2. สอบทานเกณฑ์การรายงานเหตุการณ์ โดยพิจารณาความสอดคล้องตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ 2564 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 37(4))
3. สอบทานตารางการรายงานเหตุการณ์ว่ามีการระบุชื่อหน่วยงาน (เช่น สกมช., สคส.) ข้อมูลการติดต่อ และกรอบเวลาการรายงานที่สอดคล้องกับ พ.ร.บ.ไซเบอร์ฯ และกฎหมายเฉพาะ
4. สอบทานแบบฟอร์มบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody Form) ว่ามีการระบุรายละเอียดครบถ้วนของการได้มาของคอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ ที่ได้ยึดไว้เป็นหลักฐาน
5. สอบทานรายงานทบทวนหลังการปฏิบัติงาน (After-Action Review - AAR) หรือสรุปบทเรียนจากเหตุการณ์จริงครั้งล่าสุด หรือจากการซ้อมแผน เพื่อดูข้อเสนอแนะในการปรับปรุงแผน

■ **เอกสารที่เกี่ยวข้อง**

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) / คู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง
2. คำสั่งแต่งตั้งทีม CIRT พร้อมรายชื่อและช่องทางติดต่อ
3. ตารางสรุปเกณฑ์การรายงานเหตุการณ์ตามกฎหมาย
4. แบบฟอร์มบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody Form)
5. ทะเบียนการติดต่อผู้เชี่ยวชาญหรือหน่วยงานภายนอก (External Contact List)

■ **เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค**

-

3.1.11 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ (Communication of Cybersecurity Incident Response Plan) (ข้อ 19.2)

วัตถุประสงค์

เพื่อให้มั่นใจว่า บุคลากรทุกคนที่มีส่วนเกี่ยวข้องหรือสนับสนุนบริการสำคัญของหน่วยงาน ได้รับทราบเข้าใจ และเข้าถึงแผนการรับมือภัยคุกคามทางไซเบอร์ได้อย่างทั่วถึง

ความเสี่ยง

บุคลากรขาดความเข้าใจและไม่สามารถปฏิบัติตามแผนเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ขึ้นจริง

การควบคุมที่พึงมี

หน่วยงานต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ

แนวทางการประเมิน

1. ตรวจสอบกระบวนการสื่อสารและเผยแพร่แผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงาน
2. ตรวจสอบความทั่วถึงและประสิทธิภาพของการสื่อสารไปยังบุคลากรที่เกี่ยวข้องและผู้สนับสนุนบริการสำคัญ (CII)
3. ตรวจสอบความเข้าใจของบุคลากรต่อบทบาทหน้าที่ของตนเองตามที่ระบุในแผน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 19.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 3
NIST CSF 2.0	GV.RR-02, ID.IM-04
ISO/IEC27001:2022	Annex A 5.24
ISO/IEC27701:2025	-
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (7)

ขั้นตอนการตรวจสอบ

- **การสัมภาษณ์**
 1. หน่วยงานมีช่องทางหรือวิธีการใดในการสื่อสารแผนรับมือภัยคุกคามทางไซเบอร์ให้บุคลากรที่เกี่ยวข้องรับทราบ และมีความถี่ในการสื่อสารอย่างไร
 2. เมื่อเกิดเหตุการณ์จริง บุคลากรทราบหรือไม่ว่าต้องรายงานใครและต้องปฏิบัติตามขั้นตอนอย่างไร
- **การสอบถามเอกสาร**
 1. สอบถามหลักฐานการสื่อสาร (เช่น อีเมลแจ้งเวียน, ประกาศภายใน, บันทึกการประชุม) ว่ามีการสื่อสารแผนรับมือภัยคุกคามทางไซเบอร์ให้บุคลากรที่เกี่ยวข้องรับทราบ
 2. สอบถามบันทึกการฝึกอบรมหรือการชี้แจงแผนรับมือภัยคุกคามทางไซเบอร์และรายชื่อผู้เข้ารับการอบรมหรือรับทราบแผน ว่าครอบคลุมถึงบุคลากรที่เกี่ยวข้องทั้งหมด รวมถึงบุคคลภายนอก (Outsource/Vendor) ที่สนับสนุนบริการสำคัญด้วย
- **เอกสารที่เกี่ยวข้อง**
 1. หลักฐานการส่งอีเมล/หนังสือแจ้งเวียน หรือการประกาศบน Intranet
 2. เอกสารประกอบการฝึกอบรมและชี้แจงแผนการรับมือภัยคุกคามทางไซเบอร์
 3. รายชื่อผู้เข้ารับการอบรมหรือรับทราบแผนการรับมือภัยคุกคามทางไซเบอร์
- **เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค**

-

3.1.12 การทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Review of Cybersecurity Incident Response Plan)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า แผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานมีความทันสมัยและพร้อมใช้งานอยู่เสมอ	
การควบคุมที่พึงมี	
ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ	
ความเสี่ยง	
แผนการรับมือภัยคุกคามทางไซเบอร์ไม่สอดคล้องกับสถานการณ์และรูปแบบการโจมตีในปัจจุบัน	
แนวทางการประเมิน	
1. ตรวจสอบประวัติการทบทวนและปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ 2. ยืนยันรอบระยะเวลาการทบทวน ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง โดยนับจากวันที่แผนได้รับการอนุมัติครั้งล่าสุด	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 19.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 3
NIST CSF 2.0	ID.IM-04
ISO/IEC27001:2022	Annex A 5.24
ISO/IEC27701:2025	-
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีกลไกและรอบระยะเวลาในการนำแผนรับมือภัยคุกคามทางไซเบอร์มาทบทวนเป็นประจำทุกปีอย่างไร 2. ใครคือผู้รับผิดชอบหลักในการทบทวน รวบรวมข้อเสนอแนะ และนำเสนอเพื่อขออนุมัติแผนฉบับปรับปรุงใหม่ ■ การสอบทานเอกสาร 1. สอบทานประวัติการแก้ไขเอกสาร (Revision History / Version Control) ของแผนรับมือภัยคุกคามทางไซเบอร์ เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐานที่สำคัญ หรือเมื่อสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงไป	

2. สอบทานรายงานการประชุมหรือหลักฐานการพิจารณาทบทวนแผนประจำปี เพื่อยืนยันว่ามี การทบทวนแผนเกิดขึ้นจริง ■ เอกสารที่เกี่ยวข้อง 1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) 2. รายงานการประชุมเพื่อพิจารณาทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

3.1.13 การทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (Review of Cybersecurity Incident Response Plan upon Significant Change)

วัตถุประสงค์

เพื่อให้มั่นใจว่า แผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานมีความยืดหยุ่นและสอดคล้องกับ
สถานการณ์ปัจจุบันอยู่เสมอ

ความเสี่ยง

แผนการรับมือภัยคุกคามทางไซเบอร์ไม่สอดคล้องกับสถานการณ์และรูปแบบการโจมตีในปัจจุบัน

การควบคุมที่พึงมี

ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อม
การปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

แนวทางการประเมิน

1. ตรวจสอบว่าหน่วยงานมีกระบวนการติดตามและประเมินผลกระทบเมื่อเกิดการเปลี่ยนแปลง
อย่างมีนัยสำคัญทั้งในด้านสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญ หรือ
ข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
2. ตรวจสอบว่าเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ หน่วยงานได้ดำเนินการทบทวนและแก้ไข
แผนในกรอบเวลาที่เหมาะสม
3. ตรวจสอบการปรับปรุงเนื้อหาในแผนการรับมือภัยคุกคามทางไซเบอร์ ว่าสอดคล้องกับการ
เปลี่ยนแปลงนั้น ๆ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 19.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 3
NIST CSF 2.0	ID.IM-04
ISO/IEC 27001:2022	Clause 8.1, Annex A 5.24
ISO/IEC 27701:2025	Clause 8.1
ISO/IEC 27017:2015	16.1.1
ISO/IEC 27007:2020	A.5.1
ISO/IEC TS 27008:2019	16.1.1

มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีเกณฑ์ในการพิจารณาอย่างไรว่าการเปลี่ยนแปลงใดถือเป็นการเปลี่ยนแปลงอย่างมีนัยสำคัญ (เช่น การย้ายระบบไป Cloud การเปลี่ยนผู้ให้บริการภายนอก การเปลี่ยนกฎหมายกำกับดูแล) 2. หากมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ หน่วยงานมีกระบวนการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์หรือไม่ 3. ในช่วงปีที่ผ่านมา มีการนำสถานการณ์ภัยคุกคามใหม่ ๆ มาปรับปรุงขั้นตอนการจำกัดขอบเขต (Containment) ในแผนหรือไม่ 4. กรณีที่มีเหตุการณ์ผิดปกติ (Incidents) หรือเหตุการณ์ที่เกือบจะเกิดความเสียหาย (Near-misses) หน่วยงานได้นำบทเรียนมาปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์หรือไม่ ■ การสอบทานเอกสาร 1. สอบทานประวัติการแก้ไขเอกสาร (Revision History / Version Control) ของแผนรับมือภัยคุกคามทางไซเบอร์ เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐานที่สำคัญ หรือเมื่อสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงไป 2. สอบทานรายงานการประชุมหรือหลักฐานการพิจารณาทบทวนแผนประจำปี เพื่อยืนยันว่าการทบทวนแผนเกิดขึ้นจริง 3. สอบทานรายงานการบริหารจัดการการเปลี่ยนแปลง (Change Management Logs) เพื่อดูว่ามีการปรับปรุงแผนให้สอดคล้องกันหลังจากมีการ Change ระบบสำคัญหรือไม่ 4. สอบทานรายงานการทบทวนหลังการดำเนินการ (After-Action Review Report / Lessons Learned) เพื่อดูว่ามีการปรับปรุงแผนให้สอดคล้องกันหลังจากมีเหตุการณ์ผิดปกติหรือไม่ 5. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) เพื่อดูว่ากรณีที่มีความเสี่ยงใหม่ ๆ เกิดขึ้น มีการระบุให้ต้องปรับปรุงแผนหรือไม่ 6. สอบทานประกาศหรือระเบียบจากหน่วยงานกำกับดูแล หากมีการออกข้อกำหนดใหม่จาก สก.มช. ตรวจสอบว่าแผนได้รับปรับปรุงตามข้อกำหนดนั้นหรือไม่ ■ เอกสารที่เกี่ยวข้อง 1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) 2. รายงานการประชุมเพื่อพิจารณาทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ 3. รายงานการบริหารจัดการการเปลี่ยนแปลง (Change Management Logs) 4. รายงานการทบทวนหลังการดำเนินการ (After-Action Review Report / Lessons Learned) 5. รายงานการประเมินความเสี่ยง (Risk Assessment Report) 6. ประกาศหรือระเบียบจากหน่วยงานกำกับดูแล ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

ส่วนที่ 2 : แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

1. การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)	
การจัดการทรัพย์สิน (Asset Management)	
3.1.14 การจัดการทะเบียนทรัพย์สินสำหรับบริการที่สำคัญ (Asset Management Inventory)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีการจัดทำและดูแลรักษาทะเบียนทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญอย่างเป็นระบบ ครบถ้วน และเป็นปัจจุบัน	
ความเสี่ยง	
รายการทรัพย์สินไม่ครบถ้วนและไม่เป็นปัจจุบัน ส่งผลให้การกำหนดมาตรการรักษาความมั่นคงปลอดภัยไม่ครอบคลุมทรัพย์สินที่สำคัญ	
การควบคุมที่พึงมี	
ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้ (ก) ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ข) ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละรายการ และ (ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก	
แนวทางการประเมิน	
- ตรวจสอบกระบวนการระบุทรัพย์สินของบริการที่สำคัญ โดยอย่างน้อยประกอบด้วยขั้นตอนระบุทรัพย์สิน และการดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน - ตรวจสอบความครบถ้วนของข้อมูลในทะเบียนทรัพย์สินที่มีรายละเอียดอย่างน้อยครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ฉ)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.1.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 4
NIST CSF 2.0	ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-05, ID.AM-07

ISO/IEC27001:2022	Annex A 5.9, Annex A 5.11, Annex A 5.12, Annex A 5.13, Annex A 5.32, Annex A 8.20, Annex A 8.22
ISO/IEC27701:2025	A.3.5, A.3.6
ISO/IEC27017:2015	8.1.1, 8.2.2, 11.2.7, 13.1.3, 18.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 8.1.2, 8.1.4, 8.2.1, 8.2.2, 9.1.2, 13.1.1, 13.1.3, 18.1.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (5)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีวิธีการรวบรวมและจัดทำทะเบียนทรัพย์สินที่สำคัญให้ครบถ้วนและเป็นปัจจุบันอย่างไร 2. เมื่อมีการจัดหาทรัพย์สินใหม่หรือจำหน่ายทรัพย์สินออก หน่วยงานมีกระบวนการประสานงานเพื่อปรับปรุงทะเบียนทรัพย์สินภายในกรอบเวลาเท่าใด 3. หน่วยงานมีการระบุการขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอกอย่างไร เพื่อให้ทราบถึงผลกระทบหากอุปกรณ์ใดอุปกรณ์หนึ่งหยุดทำงาน ■ การสอบทานเอกสาร 1. สอบทานนโยบาย/ขั้นตอนการปฏิบัติงานในการเพิ่ม/ลด/ปรับปรุงรายการทรัพย์สิน 2. สอบทานทะเบียนทรัพย์สิน (Inventory) ว่ามีช่องข้อมูลครบทั้ง 6 รายการ (ก - ฉ) และมีการระบุข้อมูลครบทุกช่อง 3. สอบทานประวัติการแก้ไขเอกสาร (Revision History / Version Control) เพื่อยืนยันว่าทะเบียนมีการปรับปรุงอย่างสม่ำเสมอตามรอบเวลา หรือตามเหตุการณ์ที่มีการเปลี่ยนแปลงนัยสำคัญ 4. สอบทานแผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) นำมาเปรียบเทียบกับรายการในทะเบียนทรัพย์สินเพื่อยืนยันว่ามีการระบุความสัมพันธ์ (Dependencies) ■ เอกสารที่เกี่ยวข้อง 1. นโยบาย/ขั้นตอนการปฏิบัติงานในการเพิ่ม/ลด/ปรับปรุงรายการทรัพย์สิน 2. ทะเบียนทรัพย์สิน (Asset Inventory) 3. แผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

3.1.15 การระบุขอบเขตเครือข่ายและระบบคอมพิวเตอร์ที่เชื่อมต่อ (Network Boundary and Interfaces)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีการกำหนดและระบุขอบเขตของเครือข่ายที่รองรับบริการสำคัญอย่างชัดเจน รวมถึงการระบุระบบคอมพิวเตอร์หรือจุดเชื่อมต่อโดยตรงและมีความสำคัญต่อการทำงานของระบบ

ความเสี่ยง

ขอบเขตเครือข่ายและระบบที่เชื่อมต่อโดยตรงกับบริการสำคัญไม่ถูกระบุอย่างชัดเจน ส่งผลให้เกิดช่องโหว่ในการควบคุมการเข้าถึงจุดสำคัญที่มีผลต่อการทำงานของระบบ

การควบคุมที่พึงมี

ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

แนวทางการประเมิน

1. ตรวจสอบเอกสารที่ระบุขอบเขตเครือข่าย (Network Boundary) ของบริการที่สำคัญ ว่าครอบคลุมถึงระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) อย่างครบถ้วน
2. ตรวจสอบความถูกต้องและเป็นปัจจุบันของเอกสารที่ระบุขอบเขตหรือแผนผังเครือข่าย

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.1.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 4
NIST CSF 2.0	ID.AM-03
ISO/IEC27001:2022	Clause 4.3
ISO/IEC27701:2025	Clause 4.3
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.1.3
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (5)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีเกณฑ์การพิจารณาอย่างไรว่าระบบใดถือเป็นระบบที่เชื่อมต่อโดยตรงและมีนัยสำคัญ กับบริการที่สำคัญ (Direct and Significant Interface)
2. มีการปรับปรุงขอบเขตและแผนผังเครือข่ายให้เป็นปัจจุบันหรือไม่ เมื่อมีการเปลี่ยนแปลงสถาปัตยกรรมเครือข่าย

■ การสอบทานเอกสาร

1. สอบทานแผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) ว่ามีการระบุโซนเครือข่าย (Segmentation) ที่ชัดเจน และมีการระบุรายการจุดเชื่อมต่อ

เครือข่ายทั้งหมดที่เข้า-ออกขอบเขตบริการสำคัญ เช่น ระบบบริหารจัดการ (Management Network) ระบบสำรองข้อมูล หรือระบบของคู่สัญญาที่เชื่อมต่อเข้ามา 2. สอบทานใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) ว่าเมื่อมีการเพิ่มระบบใหม่ที่มาเชื่อมต่อกับขอบเขตบริการสำคัญ ได้มีการปรับปรุงเอกสารแผนผังเครือข่ายภายในระยะเวลาที่กำหนด ■ เอกสารที่เกี่ยวข้อง 1. แผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) 2. ใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบการตั้งค่ากฎการเข้า-ออก (Inbound/Outbound Rules) ณ จุดขอบเขตเครือข่าย ว่ามีการจำกัดการเชื่อมต่อเฉพาะระบบที่ได้รับอนุญาตจริง 2. ตรวจสอบการเชื่อมต่อทางกายภาพ (Physical Port) หรือ Logical Interface (VLAN/VPN) เพื่อยืนยันว่าไม่มีการเชื่อมต่อแปลกปลอมที่อยู่นอกเหนือขอบเขตที่ระบุไว้
--

3.1.16 การตรวจสอบและปรับปรุงทะเบียนทรัพย์สิน (Review and Update of Inventory)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีข้อมูลทรัพย์สินที่ถูกต้องและเป็นปัจจุบันอยู่เสมอ	
ความเสี่ยง	
รายการทรัพย์สินไม่ครบถ้วนและไม่เป็นปัจจุบัน ส่งผลให้การกำหนดมาตรการรักษาความมั่นคงปลอดภัยไม่ครอบคลุมทรัพย์สินที่สำคัญ	
การควบคุมที่พึงมี	
ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย	
แนวทางการประเมิน	
1. ตรวจสอบผลทะเบียนทรัพย์สิน ว่าได้มีการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง 2. ตรวจสอบว่ามีการปรับปรุงทะเบียนทรัพย์สินทันทีเมื่อมีการเปลี่ยนแปลงใด ๆ (เพิ่ม/ลด/ย้าย/เปลี่ยนสถานะ) โดยไม่ต้องรอรอบปี	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.1.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 4
NIST CSF 2.0	ID.AM-01, ID.AM-02, ID.AM-08
ISO/IEC27001:2022	Annex A 5.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	8.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 8.1.2

มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีวิธีการอย่างไรในการตรวจนับหรือยืนยันความครบถ้วนของรายการทรัพย์สินตามรอบปี 2. เมื่อทรัพย์สินมีการเปลี่ยนแปลงใด ๆ (เพิ่ม/ลด/ย้าย/เปลี่ยนสถานะ) มีกลไกอย่างไรที่ทำให้ทะเบียนทรัพย์สินจะได้รับการปรับปรุงทันที ■ การสอบทานเอกสาร 1. สอบทานบันทึกประวัติการทบทวนและปรับปรุงทะเบียนทรัพย์สิน ว่ามีการบันทึกการแก้ไขข้อมูล สอดคล้องกับกิจกรรมการจัดซื้อหรือการบำรุงรักษาที่เกิดขึ้น 2. สอบทานใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) ที่เกี่ยวข้องกับทรัพย์สินในบริการสำคัญ แล้วตรวจสอบว่ามีการปรับปรุงลงในทะเบียนทรัพย์สินได้ถูกต้องตามกรอบเวลาที่กำหนด 3. เลือกอุปกรณ์จากหน้างานจริง และตรวจสอบว่าข้อมูลทรัพย์สิน เช่น Serial Number, Tag หรือ Location ตรงกับที่ระบุไว้ในทะเบียนทรัพย์สินฉบับล่าสุด ■ เอกสารที่เกี่ยวข้อง 1. ทะเบียนทรัพย์สิน (Asset Inventory) 2. บันทึกการประชุมหรือหลักฐานการทบทวนทะเบียนทรัพย์สินประจำปี 3. ใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	
-	

3.1.17 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์รายปี (Annual Cybersecurity Risk Assessment)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการตรวจสอบและประเมินสถานการณ์ของความเสี่ยงอย่างสม่ำเสมอ โดยครอบคลุมทรัพย์สินที่เกี่ยวข้องกับบริการสำคัญทั้งหมด
ความเสี่ยง
ไม่สามารถระบุและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสม
การควบคุมที่พึงมี
ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง
แนวทางการประเมิน

- ตรวจสอบว่าการประเมินความเสี่ยงได้ครอบคลุมทรัพย์สินสารสนเทศทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินของบริการสำคัญ และผลการประเมินความเสี่ยง สะท้อนถึงสภาพช่องโหว่และภัยคุกคามของทรัพย์สินแต่ละรายการ - ตรวจสอบว่าการประเมินความเสี่ยงสำหรับทรัพย์สินของบริการที่สำคัญทั้งหมด ได้ดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงนัยสำคัญ	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.1.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 4
NIST CSF 2.0	ID.RA-04, ID.RA-05
ISO/IEC27001:2022	Annex A 5.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	8.1.1
ISO/IEC27007:2020	8.1.1, 8.1.2
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - หน่วยงานมีวิธีการในการยืนยันว่าทรัพย์สินทั้งหมดในทะเบียน (Inventory) ได้ถูกนำไปประเมินความเสี่ยงด้านไซเบอร์อย่างครบถ้วนหรือไม่ อย่างไร - หน่วยงานมีวิธีการอย่างไรในการนำทะเบียนทรัพย์สิน (Inventory) มาเชื่อมโยงกับการประเมินความเสี่ยง เพื่อให้มั่นใจว่าทรัพย์สินใหม่ที่เพิ่มระหว่างปีจะถูกนำมารวมในการประเมินด้วย - หน่วยงานกำหนดรอบในการประเมินความเสี่ยงสำหรับทรัพย์สินของบริการที่สำคัญทั้งหมดอย่างไร ■ การสอบทานเอกสาร - สอบทานรายชื่อทรัพย์สินในรายงานการประเมินความเสี่ยง เทียบกับทะเบียนทรัพย์สิน - สอบทานวันที่ในรายงานการประเมินความเสี่ยง เพื่อยืนยันว่าดำเนินการภายในรอบ 1 ปี หรือเมื่อมีการเปลี่ยนแปลงนัยสำคัญ ■ เอกสารที่เกี่ยวข้อง - รายงานการประเมินความเสี่ยง (Risk Assessment Report) - ทะเบียนทรัพย์สิน (Asset Inventory) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

3.1.18 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีการระบุ วิเคราะห์ และประเมินความเสี่ยงอย่างต่อเนื่องและเท่าทันต่อสถานการณ์ รวมถึงการเปลี่ยนแปลงที่เกิดขึ้นกับระบบสารสนเทศสำคัญ	
ความเสี่ยง	
ไม่สามารถระบุและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสม	
การควบคุมที่พึงมี	
ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการและแผนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ว่ามีขั้นตอนการดำเนินงานอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง และครอบคลุมกรณีที่มีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) 2. ตรวจสอบการดำเนินงานจริงตามรอบการประเมิน โดยพิจารณาหลักฐานบันทึกการประเมินความเสี่ยง การใช้เครื่องมือที่เกี่ยวข้องกับการประเมินความเสี่ยง และการจัดทำรายงานผลการประเมินความเสี่ยงที่เกิดขึ้นจริงตามกรอบเวลาที่กำหนด 3. ตรวจสอบความสอดคล้องของเกณฑ์การประเมินความเสี่ยงกับนโยบายการบริหารจัดการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด 4. ตรวจสอบหลักฐานการประเมินความเสี่ยงย้อนหลังในกรณีที่มีการเปลี่ยนแปลงที่สำคัญ (Significant Change) เพื่อยืนยันว่ามีการระบุผลกระทบและจัดการความเสี่ยงอย่างทันทั่วทั้งที่	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.2.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2
NIST CSF 2.0	GV.RM-01, ID.RA-05
ISO/IEC27001:2022	Clause 6.1.1, Clause 6.1.2, Clause 8.2
ISO/IEC27701:2025	Clause 6.1.1, Clause 6.1.2, Clause 8.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.3.1.1, A.3.1.2, A.5.1
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์	

1. หน่วยงานมีกระบวนการและกำหนดรอบความถี่ในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร
2. เมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานมีเกณฑ์การพิจารณาอย่างไรว่าต้องทำการประเมินความเสี่ยงเพิ่มเติม และมีใครเป็นผู้รับผิดชอบ
3. เกณฑ์ที่ใช้ในการประเมินความเสี่ยงในปัจจุบัน อ้างอิงตามนโยบายหรือประกาศของ สกมช. หรือหน่วยงานกำกับดูแล อย่างไร และมีการทบทวนเกณฑ์ให้เป็นปัจจุบันหรือไม่
4. ในการดำเนินงานประเมินความเสี่ยง มีการบันทึกข้อมูล การใช้เครื่องมือ หรือการเก็บหลักฐานประกอบการประเมินอย่างไร เพื่อให้มั่นใจในความถูกต้องของข้อมูลความเสี่ยง

■ การสอบทานเอกสาร

1. สอบทานนโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure) ว่าครอบคลุมหลักเกณฑ์และรอบระยะเวลาตามที่กฎหมายกำหนด
2. สอบทานว่ามีการทบทวนและปรับปรุงเกณฑ์การประเมินความเสี่ยงให้สอดคล้องกับนโยบายของ สกมช. หรือหน่วยงานกำกับดูแล
3. สอบทานทะเบียนความเสี่ยง (Risk Register) เพื่อตรวจสอบความครบถ้วนของรายการความเสี่ยง และการวิเคราะห์ความเสี่ยงตามเกณฑ์ที่กำหนด
4. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) เพื่อยืนยันการดำเนินการจริงตามรอบปี และตรวจสอบกรณีที่มีการเปลี่ยนแปลงที่สำคัญ
5. สอบทานหลักฐานบันทึกการเปลี่ยนแปลงที่มีผลกระทบต่อนโครงสร้างพื้นฐานสำคัญ (Change Management Records/Impact Analysis) เพื่อดูความเชื่อมโยงกับการประเมินความเสี่ยง และการวิเคราะห์ผลกระทบ

เอกสารที่เกี่ยวข้อง

1. นโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure)
2. ทะเบียนความเสี่ยง (Risk Register)
3. รายงานการประเมินความเสี่ยง (Risk Assessment Report)
4. หลักฐานบันทึกการเปลี่ยนแปลงที่มีผลกระทบต่อนโครงสร้างพื้นฐานสำคัญ (Change Management Records/Impact Analysis)
5. ประวัติการทบทวนและปรับปรุงเกณฑ์การประเมินความเสี่ยง

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.19 ทะเบียนความเสี่ยง (Risk Register)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีการจัดทำฐานข้อมูลความเสี่ยงที่เป็นระบบ มีรายละเอียดที่เพียงพอต่อการตัดสินใจของผู้บริหาร และมีการติดตามสถานะการจัดการความเสี่ยงอย่างต่อเนื่อง

ความเสี่ยง

ผู้บริหารขาดฐานข้อมูลประกอบการตัดสินใจและสั่งการในการจัดการความเสี่ยงได้อย่างทันท่วงที รวมถึงไม่สามารถติดตามสถานะความเสี่ยงที่เหลืออยู่ได้

การควบคุมที่พึงมี

ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- (ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- (ข) คำอธิบายของความเสี่ยง (Description of the Risk)
- (ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- (ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- (จ) การจัดการความเสี่ยง (Risk Treatment)
- (ฉ) เจ้าของความเสี่ยง (Risk Owner)
- (ช) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ
- (ซ) ความเสี่ยงที่เหลือ (Residual Risk)

แนวทางการประเมิน

1. ตรวจสอบกระบวนการปรับปรุงทะเบียนความเสี่ยง (Risk Register) ว่ามีการกำหนดขั้นตอนการปรับปรุงข้อมูลทันทีหลังเสร็จสิ้นการประเมินความเสี่ยง และมีการกำหนดรูปแบบข้อมูลให้ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ซ)
2. ตรวจสอบการดำเนินงานจริงในการปรับปรุงทะเบียนความเสี่ยงหลังจากการประเมินความเสี่ยงครั้งล่าสุด โดยพิจารณาจากหลักฐานการบันทึกข้อมูลในทะเบียนความเสี่ยงว่ามีการระบุรายละเอียดครบถ้วนทั้ง 8 หัวข้อในทุกรายการความเสี่ยงที่ตรวจพบ
3. ตรวจสอบการบันทึกข้อมูลการจัดการความเสี่ยง (Risk Treatment) และการคำนวณความเสี่ยงที่เหลือ (Residual Risk) ว่ามีการดำเนินการจริงตามผลการวิเคราะห์ในรายงานการประเมินความเสี่ยง
4. ตรวจสอบหลักฐานการรับรองหรือการอนุมัติทะเบียนความเสี่ยงโดยเจ้าของความเสี่ยง (Risk Owner) หรือผู้บริหารที่เกี่ยวข้อง เพื่อยืนยันการรับทราบและรับผิดชอบต่อความเสี่ยง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.2.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 2
NIST CSF 2.0	ID.RA-04, ID.RA-05, ID.RA-06
ISO/IEC27001:2022	Clause 6.1.2, Clause 6.1.3, Clause 8.3
ISO/IEC27701:2025	Clause 6.1.2, Clause 6.1.3, Clause 8.3
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	A.3.1.2, A.3.1.3, A.5.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

- การสัมภาษณ์

1. หลังจากการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เสร็จสิ้น หน่วยงานมีกระบวนการนำผลการประเมินไปปรับปรุงทะเบียนความเสี่ยงอย่างไร และใครเป็นผู้รับผิดชอบหลัก
2. หน่วยงานมีวิธีตรวจสอบความครบถ้วนของข้อมูลในทะเบียนความเสี่ยงอย่างไร เพื่อให้มั่นใจว่ามีรายละเอียดครบถ้วนตามการควบคุมที่พึงมีข้อ (ก) - (ข)
3. เจ้าของความเสี่ยง (Risk Owner) มีส่วนร่วมในการระบุแนวทางการจัดการความเสี่ยง (Risk Treatment) และการประเมินความเสี่ยงที่เหลือ (Residual Risk) อย่างไร
4. ในกรณีที่มีความเสี่ยงใหม่ หน่วยงานมีขั้นตอนการติดตามสถานะการจัดการความเสี่ยง จนกว่าจะดำเนินการตามแผนแล้วเสร็จอย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure) เพื่อตรวจสอบว่ามีการกำหนดมาตรฐานการจัดทำเอกสารและองค์ประกอบของทะเบียนความเสี่ยงที่สอดคล้องกับข้อกำหนด
2. สอบทานทะเบียนความเสี่ยง (Risk Register) เพื่อยืนยันความครบถ้วนขององค์ประกอบข้อมูลอย่างน้อย 8 หัวข้อตามการควบคุมที่พึงมีข้อ (ก) - (ข)
3. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) เพื่อเทียบเคียงความสอดคล้องของรายละเอียดความเสี่ยงและวันที่ที่ถูกนำไปบันทึกในทะเบียนความเสี่ยง
4. สอบทานบันทึกประวัติการแก้ไข (Version Control) หรือบันทึกการปรับปรุงทะเบียนความเสี่ยง เพื่อยืนยันว่ามีการปรับปรุงข้อมูลทุกครั้งภายหลังการประเมินความเสี่ยงจริง

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและระเบียบปฏิบัติการบริหารความเสี่ยง (Risk Management Policy and Procedure)
2. ทะเบียนความเสี่ยง (Risk Register)
3. รายงานการประเมินความเสี่ยง (Risk Assessment Report)
4. บันทึกประวัติการแก้ไข (Version Control) หรือบันทึกการปรับปรุงทะเบียนความเสี่ยง

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

3.1.20 การประเมินช่องโหว่ของบริการที่สำคัญ (Vulnerability Assessment)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานสามารถระบุและรับทราบถึงจุดอ่อนหรือช่องโหว่ทางเทคนิคที่อาจถูกใช้เป็นช่องทางในการโจมตีระบบที่สนับสนุนบริการสำคัญ ทั้งในส่วนของระบบสำนักงาน (IT) และระบบควบคุมการผลิตหรือโครงสร้างพื้นฐาน (ICS) และดำเนินการปรับปรุงมาตรการป้องกันให้แข็งแกร่งยิ่งขึ้น

ความเสี่ยง

ช่องโหว่ไม่ถูกตรวจพบและแก้ไขได้ภายในเวลาที่เหมาะสม

การควบคุมที่พึงมี

ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็น

- (ก) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system) และ
- (ข) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

แนวทางการประเมิน

1. ตรวจสอบกระบวนการประเมินช่องโหว่ของบริการที่สำคัญ ว่ามีการกำหนดขั้นตอนการดำเนินงานที่อ้างอิงตามหลักการบริหารความเสี่ยง และครอบคลุมทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS)
2. ตรวจสอบการดำเนินงานจริงว่ามีการประเมินช่องโหว่ตามรอบระยะเวลาที่กำหนด มีการใช้เครื่องมือ (Scanning Tools) ที่เหมาะสมกับประเภทของระบบ (โดยเฉพาะความปลอดภัยในการสแกนระบบ ICS) และมีการบันทึกหลักฐานการประเมินไว้อย่างเป็นระบบ
3. ตรวจสอบเกณฑ์การคัดเลือกบริการสำคัญที่นำมาประเมินช่องโหว่ ว่ามีความสอดคล้องกับผลการประเมินความเสี่ยงและระดับความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
4. ตรวจสอบหลักฐานการบันทึกผลการประเมินและการจัดเก็บรายงาน เพื่อยืนยันว่าหน่วยงานมีการควบคุมการเข้าถึงรายงานช่องโหว่ซึ่งเป็นข้อมูลที่มีความอ่อนไหว

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.RA-01
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและเกณฑ์ในการคัดเลือกบริการที่สำคัญ (ทั้ง IT และ ICS) เพื่อนำมาประเมินช่องโหว่อย่างไร อ้างอิงจากหลักการบริหารความเสี่ยงของหน่วยงานอย่างไร
2. ในระหว่างการดำเนินงานประเมินช่องโหว่ หน่วยงานใช้เครื่องมือหรือเทคนิคใดในการตรวจสอบ และมีมาตรการป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (ICS) อย่างไร

3. กรณีที่ตรวจพบช่องโหว่ที่มีความเสี่ยงสูง (High/Critical) หน่วยงานมีกระบวนการรายงานและบันทึกหลักฐานการดำเนินงานแก้ไขอย่างไร
4. ผู้ที่เกี่ยวข้อง (เช่น System Admin หรือ ICS Engineer) มีขั้นตอนการรับบันทึกหลักฐานและการเก็บรักษาข้อมูลผลการประเมินช่องโหว่ให้มีความถูกต้องและเป็นความลับอย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบาย/ขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy/Procedure) เพื่อยืนยันว่าสอดคล้องกับหลักการบริหารความเสี่ยง และครอบคลุมทั้งระบบ IT และ ICS
2. สอบทานรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) ของระบบ IT และ ICS เพื่อตรวจสอบความครบถ้วนของรายการทรัพย์สินที่ได้รับการประเมินตามขอบเขตที่กำหนด
3. สอบทานทะเบียนทรัพย์สิน (Inventory) ของบริการที่สำคัญ เพื่อเทียบเคียงกับขอบเขตในรายงานการประเมินช่องโหว่
4. สอบทานหลักฐานการวิเคราะห์ความเสี่ยงที่ใช้ในการเลือกระบบเป้าหมาย (Risk-based Selection Evidence) เพื่อยืนยันว่าการประเมินครอบคลุมบริการที่มีความสำคัญสูงจริง

■ เอกสารที่เกี่ยวข้อง

1. นโยบาย/ขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy/Procedure)
2. รายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report)
3. ทะเบียนทรัพย์สิน (Asset Inventory)
4. หลักฐานการวิเคราะห์ความเสี่ยงที่ใช้ในการเลือกระบบเป้าหมาย (Risk-based Selection Evidence)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.21 ขอบเขตของการประเมินช่องโหว่ (Scope of Vulnerability Assessment)

วัตถุประสงค์

เพื่อให้มั่นใจว่า การประเมินช่องโหว่ของหน่วยงานครอบคลุมทั้งในระดับอุปกรณ์ (Host) การเชื่อมต่อ (Network) และการออกแบบเชิงโครงสร้าง (Architecture) เพื่อลดช่องโหว่ในทุกมิติที่อาจส่งผลกระทบต่อบริการสำคัญ

ความเสี่ยง

การตรวจสอบช่องโหว่ไม่ครอบคลุมบริการสำคัญ

การควบคุมที่พึงมี

ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

- (ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- (ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ
- (ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

แนวทางการประเมิน

1. ตรวจสอบกระบวนการกำหนดขอบเขตการประเมินช่องโหว่ (Vulnerability Assessment) ว่ามีการระบุข้อกำหนดที่ครอบคลุม (ก) - (ค)
2. ตรวจสอบการดำเนินงานจริงในการประเมินช่องโหว่ เพื่อยืนยันว่าครอบคลุมขอบเขตทั้ง 3 ด้าน (Host, Network, Architecture) โดยพิจารณาจากการเลือกใช้เครื่องมือ (Tools) และการกำหนดค่าการตรวจสอบ (Configuration)
3. ตรวจสอบการบันทึกเป็นเอกสารและหลักฐานประกอบการดำเนินงาน เช่น รายงานการประเมิน และผลลัพธ์จากการใช้เครื่องมือตรวจสอบ เพื่อยืนยันความครบถ้วนของการดำเนินงานตามที่กำหนดในขอบเขต

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.RA-01
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและเกณฑ์ในการกำหนดขอบเขตการประเมินช่องโหว่ให้ครอบคลุมทั้งระดับโฮสต์ เครือข่าย และสถาปัตยกรรมอย่างไร เพื่อให้มั่นใจว่าครอบคลุมทรัพย์สินสารสนเทศที่สำคัญ
2. ในการประเมินครั้งล่าสุด มีการใช้เครื่องมือหรือเทคนิคใดในการประเมินความมั่นคงปลอดภัยของโฮสต์และเครือข่าย และมีขั้นตอนการทำ Architecture Security Review อย่างไร
3. หน่วยงานมีการจัดเก็บหลักฐานและบันทึกผลการตรวจสอบ (Evidence/Logs) ระหว่างการประเมินอย่างไร เพื่อยืนยันความถูกต้องและใช้ในการตรวจสอบย้อนหลัง

■ การสอบทานเอกสาร

1. สอบทานนโยบาย/ขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy/Procedure) เพื่อยืนยันการกำหนดขอบเขตการประเมินที่ครอบคลุมทั้งระดับโฮสต์ เครือข่าย และสถาปัตยกรรม
2. สอบทานรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) เพื่อตรวจสอบความสอดคล้องของขอบเขตการประเมินจริงกับขอบเขตที่กำหนดไว้
3. สอบทานรายงานการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review Report) เพื่อยืนยันว่าได้มีการประเมินในระดับโครงสร้างสถาปัตยกรรมครบถ้วนตามข้อกำหนด

4. สอบทานบันทึกหลักฐานการตรวจสอบ (Assessment Evidence/Logs) เช่น ผลลัพธ์จากเครื่องมือสแกน (Raw Scan Results) เพื่อยืนยันวันเวลา และรายละเอียดการดำเนินงานเชิงเทคนิค ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy and Procedure) 2. รายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) 3. รายงานการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review Report) 4. บันทึกหลักฐานการตรวจสอบ (Assessment Evidence/Logs) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -

3.1.22 การประเมินช่องโหว่ก่อนเริ่มระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ (Vulnerability Assessment for New Systems or Significant Changes)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า ระบบใหม่หรือส่วนที่ได้รับการปรับปรุงแก้ไข จะไม่นำพาช่องโหว่หรือจุดอ่อนใหม่ ๆ เข้าสู่สภาพแวดล้อมของบริการที่สำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยโดยรวมขององค์กรหากไม่มีการตรวจสอบและแก้ไขก่อนเริ่มใช้งานจริง	
ความเสี่ยง	
ช่องโหว่ไม่ถูกตรวจพบและแก้ไขได้ภายในเวลาที่เหมาะสม	
การควบคุมที่พึงมี	
ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการการนำระบบใหม่เข้าเชื่อมต่อ หรือการเปลี่ยนแปลงระบบที่สำคัญ (เช่น การเพิ่มโมดูลแอปพลิเคชัน, การปรับปรุงระบบ, การปรับเปลี่ยนเทคโนโลยี) ว่ามีการกำหนดให้ดำเนินการประเมินช่องโหว่เพื่อระบุจุดอ่อนก่อนการดำเนินงานจริง 2. ตรวจสอบการดำเนินงานจริงว่ามีการประเมินช่องโหว่ก่อนการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ โดยมีการใช้เครื่องมือในการตรวจสอบ มีการบันทึกผล และมีการเก็บหลักฐานประกอบการประเมินอย่างครบถ้วน	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5

NIST CSF 2.0	ID.RA-01, ID.RA-07, ID.RA-09
ISO/IEC27001:2022	Annex A 5.8, Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1, 14.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.5, 12.6.1, 14.1.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ในกรณีที่มีการนำระบบใหม่มาเชื่อมต่อหรือมีการเปลี่ยนแปลงระบบที่สำคัญ หน่วยงานมีกระบวนการและขั้นตอนการประเมินช่องโหว่ก่อนเริ่มดำเนินการอย่างไรเพื่อให้มั่นใจว่าระบบมีความปลอดภัย 2. เมื่อพบจุดอ่อนหรือช่องโหว่จากการประเมิน หน่วยงานมีเกณฑ์ในการตัดสินใจและกระบวนการจัดการเพื่อควบคุมความเสี่ยงนั้นอย่างไรก่อนจะอนุญาตให้ดำเนินการต่อ 3. หน่วยงานมีการใช้เครื่องมือหรือเทคนิคใดในการตรวจสอบช่องโหว่สำหรับการเพิ่มโมดูลแอปพลิเคชันหรือการปรับปรุงเทคโนโลยีใหม่ และมีการบันทึกหลักฐานการตรวจสอบไว้อย่างไร ■ การสอบทานเอกสาร 1. สอบทานนโยบายและขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy and Procedure) ว่ามีการกำหนดขอบเขตครอบคลุมกรณีก่อนการขึ้นระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ 2. สอบทานบันทึกการขอเปลี่ยนแปลงระบบ (Change Request) เพื่อยืนยันว่ามีการระบุรายละเอียดการประเมินช่องโหว่/ผลการวิเคราะห์จุดอ่อนก่อนการอนุมัติขึ้นระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ 3. สอบทานรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) ของระบบใหม่หรือส่วนที่มีการเปลี่ยนแปลง เพื่อตรวจสอบความครบถ้วนของรายการตรวจสอบและระดับความเสี่ยงที่พบ 4. สอบทานหลักฐานการแก้ไขช่องโหว่ (Remediation Records) ในกรณีที่พบช่องโหว่จากการประเมิน เพื่อยืนยันว่าได้มีการควบคุมหรือแก้ไขก่อนการเริ่มใช้งานหรือตามแผนที่กำหนด 5. สอบทานรายงานการอนุมัติการขึ้นระบบ (Deployment Approval Report) เพื่อประเมินความสอดคล้องระหว่างผลการตรวจสอบช่องโหว่กับการตัดสินใจให้นำระบบเข้าใช้งาน ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy and Procedure) 2. บันทึกการขอเปลี่ยนแปลงระบบ (Change Request) 3. รายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) 4. หลักฐานการแก้ไขช่องโหว่ (Remediation Records) 5. รายงานการอนุมัติการขึ้นระบบ (Deployment Approval Report)	

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. สุ่มตรวจสอบผลการสแกนช่องโหว่เชิงเทคนิค (Raw Scan Results) เพื่อยืนยันว่าครอบคลุมช่องโหว่ระดับ Critical และ High รวมถึงตรวจสอบว่าไม่มีช่องโหว่ที่สำคัญ เช่น Code Injection หรือ Session Hijacking ตกค้างอยู่
2. ตรวจสอบการตั้งค่าทางเทคนิคที่เกี่ยวข้องกับการเปลี่ยนแปลงนั้น เช่น
 - ความถูกต้องและวันหมดอายุของ SSL Certificate บนระบบที่มีการเปลี่ยนแปลง หรือเชื่อมต่อใหม่
 - การตั้งค่า Application Logs ของโมดูลใหม่ เพื่อยืนยันว่าผู้ใช้งานทั่วไปไม่สามารถลบหรือแก้ไขประวัติการใช้งานของตนเองได้
 - กลไกการคัดกรองการเข้าถึงฐานข้อมูล (Database Access Control) สำหรับบริการที่เพิ่มเข้ามาใหม่ ว่ามีการยืนยันตัวตนที่ปลอดภัยและไม่สามารถเข้าถึงได้โดยตรงจากภายนอก
 - การตั้งค่าสิทธิ์การเข้าถึงและ Protocols ที่ใช้ในระบบใหม่หรือส่วนที่ปรับปรุง โดยเทียบกับมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Hardening Baseline)

3.1.23 การทดสอบเจาะระบบ (Penetration Testing)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีการจำลองการโจมตีจริงเพื่อค้นหาจุดอ่อนที่เครื่องมือสแกนช่องโหว่ทั่วไปอาจตรวจไม่พบ

ความเสี่ยง

ช่องโหว่ไม่ถูกตรวจพบและแก้ไขได้ภายในเวลาที่เหมาะสม

การควบคุมที่พึงมี

ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

แนวทางการประเมิน

1. ตรวจสอบกระบวนการการกำหนดขอบเขตการทดสอบเจาะระบบ (Penetration Testing) ว่ามีการกำหนดขั้นตอนการคัดเลือกบริการที่สำคัญ โดยเฉพาะระบบที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับความเสี่ยง และมีการกำหนดวิธีการบริหารจัดการผลกระทบที่อาจเกิดขึ้นจากการทดสอบ
2. ตรวจสอบการดำเนินงานจริงที่มีการทดสอบเจาะระบบตามขอบเขตและระยะเวลาที่กำหนด มีการใช้เครื่องมือหรือทีมงานที่มีความเชี่ยวชาญในการทดสอบ และมีการบันทึกหลักฐานรายงานผลการทดสอบไว้อย่างครบถ้วน
3. ตรวจสอบการประเมินความเสี่ยงและผลกระทบก่อนการทดสอบจริง เพื่อยืนยันว่าหน่วยงานได้พิจารณาถึงความต่อเนื่องของบริการและมีมาตรการลดความเสี่ยงจากการทดสอบเจาะระบบนั้น

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.IM-02, ID.RA-01
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29, Annex A 8.34
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.5, 12.6.1, 14.1.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีหลักเกณฑ์ในการพิจารณาคัดเลือกบริการสำคัญและระบบที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) เพื่อทำการทดสอบเจาะระบบ (Penetration Testing) ให้สอดคล้องกับระดับความเสี่ยงอย่างไร และมีกระบวนการอนุมัติอย่างไร 2. ในการดำเนินงานทดสอบครั้งล่าสุด หน่วยงานได้มีการตรวจสอบความพร้อมของระบบ การใช้เครื่องมือ และการจัดเก็บหลักฐานการทดสอบ (เช่น Screenshots, Logs) ไว้อย่างไร 3. ก่อนเริ่มดำเนินการทดสอบ หน่วยงานมีการประเมินผลกระทบที่อาจเกิดกับระบบงานจริงอย่างไร และมีข้อตกลงเรื่องช่วงเวลาหรือวิธีการทดสอบ (Rules of Engagement) เพื่อป้องกันระบบหยุดชะงักอย่างไร 4. เมื่อพบช่องโหว่จากการทดสอบเจาะระบบ หน่วยงานมีขั้นตอนการนำผลการทดสอบไปปรับปรุงความมั่นคงปลอดภัยของระบบอย่างไร ■ การสอบทานเอกสาร 1. สอบทานนโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure) เพื่อยืนยันหลักเกณฑ์การคัดเลือกเป้าหมายตามระดับความเสี่ยง 2. สอบทานแผนการทดสอบเจาะระบบ (Penetration Testing Plan) และรายชื่อระบบเป้าหมาย เพื่อตรวจสอบความสอดคล้องกับระบบที่เชื่อมต่ออินเทอร์เน็ต (Internet Facing) 3. สอบทานรายงานผลการประเมินความเสี่ยงและผลกระทบจากการทดสอบ (Impact Assessment Report) เพื่อยืนยันว่ามีการพิจารณาความเสี่ยงก่อนเริ่มงาน 4. สอบทานเอกสารข้อกำหนดและข้อตกลงในการทดสอบ (Rules of Engagement/Terms of Reference) ที่ระบุขอบเขต วิธีการ และมาตรการลดผลกระทบ 5. สอบทานรายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) เพื่อประเมินความครบถ้วนของหลักฐานและผลการตรวจสอบตามแผนที่วางไว้ 6. สอบทานเอกสารการอนุมัติการทดสอบเจาะระบบ เพื่อยืนยันว่าผู้มีอำนาจได้รับทราบถึงความเสี่ยงและผลกระทบก่อนเริ่มดำเนินการ ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure) 2. แผนการทดสอบเจาะระบบ (Penetration Testing Plan)	

3. รายงานผลการประเมินความเสี่ยงและผลกระทบจากการทดสอบ (Impact Assessment Report) 4. เอกสารข้อกำหนดและข้อตกลงในการทดสอบ (Rules of Engagement/Terms of Reference) 5. รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) 6. เอกสารการอนุมัติการทดสอบเจาะระบบ ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -

3.1.24 ขอบเขตของการทดสอบเจาะระบบ (Scope of Penetration Testing)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า การทดสอบเจาะระบบมีความครอบคลุมครบทุกมิติของเทคโนโลยีสารสนเทศที่ประกอบกันเป็นบริการสำคัญ	
ความเสี่ยง	
การตรวจสอบช่องโหว่ไม่ครอบคลุมบริการสำคัญ	
การควบคุมที่พึงมี	
ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่ง ทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการการกำหนดขอบเขตการทดสอบเจาะระบบ (Penetration Testing) ว่ามีการกำหนดขั้นตอนการระบุเป้าหมายที่ครอบคลุมทั้งระดับโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะระบบที่เชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing) 2. ตรวจสอบการดำเนินงานจริงว่ามีการดำเนินการทดสอบเจาะระบบตามขอบเขตที่กำหนด โดยมีการใช้เครื่องมือในการตรวจสอบ มีการบันทึกรายละเอียดการทดสอบ และมีการเก็บหลักฐานประกอบ (เช่น Log การทดสอบ หรือ Screenshots) เพื่อยืนยันว่าครอบคลุมทุกองค์ประกอบ (Host, Network, Application) 3. ตรวจสอบความครบถ้วนของการบันทึกหลักฐานการดำเนินงาน เพื่อยืนยันว่าระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing) ทั้งหมดถูกรวมอยู่ในขอบเขตการทดสอบจริง	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.5
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.IM-02, ID.RA-01
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-

ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีหลักเกณฑ์ในการกำหนดขอบเขตการทดสอบเจาะระบบอย่างไร เพื่อให้มั่นใจว่าครอบคลุมทั้งระดับโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ 2. หน่วยงานมีวิธีการตรวจสอบและยืนยันอย่างไรว่า ระบบที่เชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing) ทุกระบบได้ถูกนำมารวมอยู่ในขอบเขตการทดสอบเจาะระบบอย่างครบถ้วน 3. ในการทดสอบครั้งล่าสุด มีการใช้เครื่องมือหรือเทคนิคใดในการทดสอบ และมีการจัดเก็บหลักฐานการดำเนินงาน (เช่น บันทึกการปฏิบัติงาน หรือผลลัพธ์จากเครื่องมือ) ไว้อย่างไรเพื่อใช้ในการตรวจสอบ ■ การสอบทานเอกสาร 1. สอบทานนโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure) 2. เพื่อยืนยันว่ามีการระบุข้อกำหนดที่ครอบคลุมโฮสต์ เครือข่าย แอปพลิเคชัน และระบบที่เชื่อมต่ออินเทอร์เน็ต (Internet Facing) 3. สอบทานแผนการทดสอบเจาะระบบ (Penetration Testing Plan) และรายชื่อระบบเป้าหมาย เพื่อตรวจสอบความสอดคล้องกับบริการที่สำคัญและรายการสินทรัพย์ที่เชื่อมต่ออินเทอร์เน็ต 4. สอบทานรายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) เพื่อประเมินความครบถ้วนของเนื้อหาว่ามีการทดสอบครอบคลุมทั้ง 3 ระดับ (Host, Network, Application) ตามที่กำหนดไว้ 5. สอบทานรายการทรัพย์สินหรือแผนผังเครือข่าย (Asset Inventory / Network Diagram) เปรียบเทียบกับขอบเขตการทดสอบ เพื่อยืนยันว่าไม่มีระบบ Internet Facing ใดตกหล่นจากการทดสอบ ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure) 2. แผนการทดสอบเจาะระบบ (Penetration Testing Plan) 3. รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) 4. รายการทรัพย์สินหรือแผนผังเครือข่าย (Asset Inventory / Network Diagram) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

3.1.25 ความถี่และความจำเป็นในการทดสอบเจาะระบบ (Frequency and Necessity of Penetration Testing)

วัตถุประสงค์

เพื่อให้มั่นใจว่า บริการที่สำคัญของหน่วยงานได้รับการตรวจสอบความแข็งแกร่งอย่างสม่ำเสมอ และได้รับการประเมินความมั่นคงปลอดภัยทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ

ความเสี่ยง

ช่องโหว่ไม่ถูกตรวจพบและแก้ไขได้ภายในเวลาที่เหมาะสม

การควบคุมที่พึงมี

ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

แนวทางการประเมิน

1. ตรวจสอบการกำหนดรอบการทดสอบเจาะระบบประจำปี ว่ามีการกำหนดให้ดำเนินการทดสอบเจาะระบบเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ (เช่น การเพิ่มโมดูลเสริม การปรับปรุงระบบ หรือการปรับปรุงเทคโนโลยี)
2. ตรวจสอบการดำเนินงานจริงว่ามีการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง และมีการทดสอบก่อนการขึ้นระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ โดยมีการใช้เครื่องมือในการตรวจสอบ มีการบันทึกผล และมีการเก็บหลักฐานประกอบการประเมินอย่างครบถ้วน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.6
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.IM-02, ID.RA-07
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและเกณฑ์ในการกำหนดรอบการทดสอบเจาะระบบประจำปีอย่างไร และใครเป็นผู้อนุมัติแผนการดำเนินงานดังกล่าว
2. หน่วยงานมีเกณฑ์ในการตัดสินใจอย่างไรว่าการเปลี่ยนแปลงระดับใด (เช่น การเพิ่มโมดูล การปรับปรุงระบบ หรือการปรับปรุงเทคโนโลยี) ที่ถือเป็นการเปลี่ยนแปลงที่สำคัญ ซึ่งต้องผ่านการทดสอบเจาะระบบก่อนเปิดใช้งานจริง
3. ในกรณีที่มีการนำระบบใหม่มาใช้งานหรือมีการเปลี่ยนแปลงระบบที่สำคัญ หน่วยงานมีกระบวนการและขั้นตอนทดสอบเจาะระบบก่อนเริ่มดำเนินการอย่างไรเพื่อให้มั่นใจว่าระบบมีความปลอดภัย

- เมื่อพบจุดอ่อนหรือช่องโหว่จากการทดสอบ หน่วยงานมีเกณฑ์ในการตัดสินใจและกระบวนการจัดการเพื่อควบคุมความเสี่ยงนั้นอย่างไรก่อนจะอนุญาตให้ดำเนินการต่อ
- หน่วยงานมีการใช้เครื่องมือหรือเทคนิคใดในการทดสอบเจาะระบบสำหรับการเพิ่มโมดูล แอปพลิเคชัน การปรับปรุงระบบ หรือการปรับปรุงเทคโนโลยี และมีการบันทึกหลักฐานการดำเนินงาน (เช่น บันทึกการปฏิบัติงาน หรือรายงานผล) ไว้อย่างไร

■ การสอบทานเอกสาร

- สอบทานนโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure) ว่ามีการกำหนดขอบเขตครอบคลุมกรณีก่อนการขึ้นระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ
- สอบทานแผนการทดสอบเจาะระบบประจำปี (Annual Penetration Testing Plan) เพื่อยืนยันการกำหนดขอบเขต ระยะเวลา และรอบการดำเนินงานที่สม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- สอบทานใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) เพื่อยืนยันว่ามีการระบุรายละเอียดการทดสอบเจาะระบบก่อนการอนุมัติขึ้นระบบใหม่หรือการเปลี่ยนแปลงที่สำคัญ
- สอบทานรายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) เพื่อยืนยันว่ามีการทดสอบจริงตามรอบปี และครอบคลุมระบบงานที่สำคัญตามที่กำหนดไว้ในขอบเขต
- สอบทานหลักฐานประกอบการทดสอบเจาะระบบ (Penetration Testing Evidence/Logs) เช่น ภาพถ่ายหน้าจอการทดสอบ หรือบันทึกจากเครื่องมือ เพื่อประเมินความครบถ้วนของการดำเนินงานจริง
- สอบทานบันทึกการแก้ไขช่องโหว่จากการทดสอบเจาะระบบ (Remediation Records) เพื่อยืนยันว่ามีการติดตามผลและแก้ไขจุดอ่อนที่พบก่อนการเริ่มใช้งานหรือตามแผนที่กำหนด
- สอบทานรายงานการอนุมัติการขึ้นระบบ (Deployment Approval Report) เพื่อประเมินความสอดคล้องระหว่างผลทดสอบเจาะระบบ กับการตัดสินใจให้นำระบบเข้าใช้งาน

■ เอกสารที่เกี่ยวข้อง

- นโยบายและขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Policy and Procedure)
- แผนการทดสอบเจาะระบบประจำปี (Annual Penetration Testing Plan)
- ใบคำขออนุมัติการเปลี่ยนแปลง (Change Request)
- รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report)
- หลักฐานประกอบการทดสอบเจาะระบบ (Penetration Testing Evidence/Logs)
- หลักฐานการแก้ไขช่องโหว่จากการทดสอบเจาะระบบ (Remediation Records)
- รายงานการอนุมัติการขึ้นระบบ (Deployment Approval Report)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.26 คุณสมบัติและความเป็นอิสระของผู้ทดสอบเจาะระบบ (Qualifications and Independence of Penetration Testers)

วัตถุประสงค์

เพื่อให้มั่นใจว่า การทดสอบเจาะระบบดำเนินการโดยผู้เชี่ยวชาญที่มีความรู้ความสามารถตามมาตรฐานสากล และผลการทดสอบมีความน่าเชื่อถือ ปราศจากความลำเอียงหรือผลประโยชน์ทับซ้อน

ความเสี่ยง

ผลการทดสอบเจาะระบบขาดความน่าเชื่อถือ

การควบคุมที่พึงมี

ต้องตรวจสอบให้แน่ใจว่า การทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

แนวทางการประเมิน

1. ตรวจสอบกระบวนการการคัดเลือกและตรวจสอบคุณสมบัติผู้ทดสอบเจาะระบบ (Penetration Testers) ว่ามีการกำหนดหลักเกณฑ์ด้านประกาศนียบัตร (Certifications) ความเป็นอิสระ (Independence) และคุณสมบัติอื่น ๆ ให้สอดคล้องกับหลักเกณฑ์ที่หน่วยงานกำกับดูแลกำหนด
2. ตรวจสอบการดำเนินงานจริงในการตรวจสอบคุณสมบัติผู้ทดสอบก่อนเริ่มดำเนินการ โดยมีการตรวจสอบความถูกต้องของใบประกาศนียบัตร มีการบันทึกผลการตรวจสอบเป็นเอกสาร และมีการเก็บหลักฐานประกอบการพิจารณาอย่างครบถ้วน
3. ตรวจสอบหลักฐานการยืนยันความเป็นอิสระ เพื่อยืนยันว่าผู้ทดสอบไม่มีส่วนเกี่ยวข้องกับการบริหารจัดการหรือการดูแลระบบที่ทำการทดสอบ และไม่มีผลประโยชน์ทับซ้อนในการปฏิบัติงาน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.7
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	GV.RR-02
ISO/IEC27001:2022	Clause 7.2, Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	Clause 7.2
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	A.4.2
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีขั้นตอนและหลักเกณฑ์ในการคัดเลือกผู้ทดสอบเจาะระบบอย่างไร เพื่อให้มั่นใจว่าได้รับประกาศนียบัตรวิชาชีพที่เหมาะสมและเป็นที่ยอมรับ (เช่น OSCP, CISSP, GPEN)
2. หน่วยงานมีวิธีการตรวจสอบความถูกต้อง (Verification) ของใบประกาศนียบัตรที่ผู้ทดสอบนำมาแสดงอย่างไร และมีการบันทึกหลักฐานการตรวจสอบนั้นไว้อย่างไร

3. มีกลไกหรือข้อกำหนดใดในสัญญาหรือข้อตกลงการทำงานที่ใช้รับรองว่าผู้ทดสอบมีความเป็นอิสระจากระบบที่ถูกทดสอบ และไม่ได้มีส่วนได้ส่วนเสียกับทีมผู้ดูแลระบบ
4. ในกรณีที่หน่วยงานควบคุมหรือกำกับดูแลมีการกำหนดเกณฑ์เฉพาะ หน่วยงานมีขั้นตอนการตรวจสอบคุณสมบัติของผู้ทดสอบให้เป็นไปตามเกณฑ์เหล่านั้นอย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายหรือหลักเกณฑ์การคัดเลือกผู้ทดสอบเจาะระบบ เพื่อยืนยันข้อกำหนดด้านคุณสมบัติและความเป็นอิสระที่สอดคล้องกับมาตรฐาน
2. สอบทานใบประกาศนียบัตรวิชาชีพของผู้ทดสอบ (Tester Certifications) เพื่อประเมินความสอดคล้องกับมาตรฐานอุตสาหกรรมและเกณฑ์ที่หน่วยงานกำกับดูแลกำหนด
3. สอบทานสัญญาว่าจ้างหรือข้อกำหนดขอบเขตงาน (TOR) เพื่อตรวจสอบเงื่อนไขการคัดเลือกและข้อกำหนดด้านคุณสมบัติของผู้ทดสอบ
4. สอบทานเอกสารยืนยันความเป็นอิสระหรือแบบฟอร์มแสดงการไม่มีผลประโยชน์ทับซ้อน (Conflict of Interest Declaration) ของทีมผู้ทดสอบ
5. สอบทานหลักฐานการตรวจสอบความถูกต้องของใบประกาศนียบัตร (Certification Verification Records) เพื่อยืนยันว่ามีการดำเนินงานจริงตามกระบวนการ

■ เอกสารที่เกี่ยวข้อง

1. นโยบายหรือหลักเกณฑ์การคัดเลือกผู้ทดสอบเจาะระบบ
2. ใบประกาศนียบัตรวิชาชีพของผู้ทดสอบ (Tester Certifications)
3. สัญญาว่าจ้างหรือข้อกำหนดขอบเขตงานทดสอบเจาะระบบ (TOR)
4. เอกสารยืนยันความเป็นอิสระหรือแบบฟอร์มแสดงการไม่มีผลประโยชน์ทับซ้อน (Conflict of Interest Declaration)
5. หลักฐานการตรวจสอบความถูกต้องของใบประกาศนียบัตร (Certification Verification Records)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.27 การกำกับดูแลการทดสอบเจาะระบบโดยผู้ให้บริการภายนอก (Supervision of Penetration Testing)
วัตถุประสงค์
เพื่อให้มั่นใจว่า กิจกรรมการทดสอบเจาะระบบโดยบุคคลภายนอกจะอยู่ภายใต้การควบคุมและขอบเขตที่หน่วยงานกำหนด โดยไม่ก่อให้เกิดความเสี่ยงที่ไม่ได้คาดคิดต่อความพร้อมใช้งานของบริการสำคัญ
ความเสี่ยง
การทดสอบอาจนำไปสู่ความเสี่ยงที่จะทำให้บริการสำคัญหยุดชะงักลง
การควบคุมที่พึงมี
ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน
แนวทางการประเมิน

1. ตรวจสอบกระบวนการกำกับดูแลการทดสอบเจาะระบบว่ามีการกำหนดขั้นตอนการดูแลผู้ให้บริการภายนอก และการระบุข้อตกลงที่ชัดเจนก่อนเริ่มการทดสอบให้สอดคล้องกับการควบคุมที่พึงมีหรือไม่
2. ตรวจสอบการดำเนินงานจริงว่าหน่วยงานมีการกำกับดูแลผู้ให้บริการอย่างใกล้ชิดในระหว่างการทดสอบ มีการใช้เครื่องมือควบคุมการเข้าถึง มีการบันทึกกิจกรรม และมีการเก็บหลักฐานประกอบ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.8
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	GV.RR-02, GV.SC-07
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและขั้นตอนในการกำกับดูแลผู้ให้บริการภายนอกในระหว่างการทดสอบเจาะระบบอย่างไร เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตและข้อกำหนดด้านความปลอดภัย
2. ในระหว่างการดำเนินงานจริง หน่วยงานมีการควบคุมสิทธิ์การเข้าถึงระบบของผู้ให้บริการอย่างไร และมีขั้นตอนการบันทึกหลักฐานการเข้าใช้งาน (เช่น Logs) เพื่อใช้ในการตรวจสอบความถูกต้องอย่างไร
3. หน่วยงานมีช่องทางสื่อสารฉุกเฉินและกระบวนการสั่งระงับการทดสอบทันทีอย่างไร หากพบเหตุการณ์ที่ส่งผลกระทบต่อเสถียรภาพของบริการสำคัญ
4. หน่วยงานมีเกณฑ์และวิธีการจัดเก็บหลักฐานการควบคุมดูแล รวมถึงการควบคุมความลับของรายงานผลการทดสอบ (Confidentiality) เพื่อป้องกันการรั่วไหลของข้อมูลช่องโหว่สำคัญอย่างไร

■ การสอบทานเอกสาร

1. สอบทานแผนการกำกับดูแลหรือข้อกำหนดการปฏิบัติงาน (Rules of Engagement) ที่ระบุรายชื่อเจ้าหน้าที่ผู้รับผิดชอบ (Point of Contact) และช่องทางสื่อสารฉุกเฉิน
2. สอบทานบันทึกการขออนุมัติและหลักฐานการเปิด-ปิดสิทธิ์การเข้าถึงระบบชั่วคราว (Access Request and Revocation Logs) สำหรับผู้ให้บริการภายนอก
3. สอบทานบันทึกกิจกรรมการเข้าใช้งานระบบ (Audit Trails/VPN Logs) ในช่วงเวลาที่มีการทดสอบเจาะระบบ เพื่อยืนยันว่ามีการติดตามการปฏิบัติงานจริง

4. สอบทานเอกสารข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) ที่ครอบคลุมทั้งนิติบุคคลและรายบุคคลของผู้ให้บริการ 5. สอบทานหลักฐานการสื่อสารหรือบันทึกการติดตามงาน (Supervision/Meeting Logs) ในระหว่างช่วงเวลาการทดสอบ เพื่อยืนยันความต่อเนื่องของการกำกับดูแลโดยหน่วยงาน ■ เอกสารที่เกี่ยวข้อง 1. แผนการกำกับดูแลหรือข้อกำหนดการปฏิบัติงาน (Rules of Engagement) ที่ระบุรายชื่อเจ้าหน้าที่ผู้รับผิดชอบ (Point of Contact) 2. บันทึกการขออนุมัติและหลักฐานการเปิด-ปิดสิทธิ์การเข้าถึงระบบชั่วคราว (Access Request and Revocation Logs) 3. บันทึกกิจกรรมการเข้าใช้งานระบบ (Audit Trails/VPN Logs) 4. ข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) 5. หลักฐานการสื่อสารหรือบันทึกการติดตามงาน (Supervision/Meeting Logs) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.1.28 กระบวนการติดตามและจัดการช่องโหว่ (Vulnerability Tracking and Remediation Process)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า ข้อมูลช่องโหว่ที่ตรวจพบจากการตรวจสอบทางเทคนิคจะถูกนำมาดำเนินการแก้ไขอย่างเป็นรูปธรรมและทันท่วงที	
ความเสี่ยง	
ช่องโหว่ของระบบไม่ได้รับการแก้ไขอย่างเหมาะสมและทันท่วงที	
การควบคุมที่พึงมี	
ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการการติดตามและจัดการกับช่องโหว่ (Vulnerability Management Process) ที่ระบุในผลการประเมินช่องโหว่ และการทดสอบเจาะระบบ ว่ามีขั้นตอนการติดตามและจัดการกับช่องโหว่อย่างเหมาะสม 2. ตรวจสอบการดำเนินงานจริงว่ามีการดำเนินงานตามกระบวนการติดตามและจัดการกับช่องโหว่ โดยมีการบันทึกสถานะลงในทะเบียนติดตาม มีการใช้เครื่องมือในการตรวจสอบซ้ำ (Rescanning/Retesting) และมีการเก็บหลักฐานประกอบการดำเนินงานอย่างครบถ้วน 3. ตรวจสอบการบันทึกเอกสารและหลักฐาน เพื่อยืนยันว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอตามแผนการแก้ไข (Remediation Plan) และมีการยืนยันผลการปิดช่องโหว่จากผู้มีหน้าที่เกี่ยวข้อง	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.9

แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	ID.IM-02, ID.RA-06, ID.RA-08
ISO/IEC27001:2022	Annex A 8.8, Annex A 8.29
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.6.1, 14.2.8, 14.2.9
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีกระบวนการและขั้นตอนในการติดตามและจัดการกับช่องโหว่ที่พบจากการประเมินช่องโหว่และการทดสอบเจาะระบบอย่างไร และใครเป็นผู้รับผิดชอบในแต่ละขั้นตอน 2. หน่วยงานมีการใช้เครื่องมือหรือซอฟต์แวร์ใดในการติดตามความคืบหน้าของการแก้ไข และมีการบันทึกหลักฐานการแก้ไข (เช่น Patch Logs หรือภาพถ่ายหน้าจอการตั้งค่า) ไว้อย่างไร 3. ในกระบวนการตรวจสอบซ้ำ (Rescanning/Retesting) หน่วยงานมีเกณฑ์การตัดสินใจอย่างไรเพื่อให้มั่นใจว่าช่องโหว่ได้รับการแก้ไขเพียงพอและสมบูรณ์ 4. กรณีที่พบช่องโหว่ที่ไม่สามารถแก้ไขได้ภายในระยะเวลาที่กำหนด หน่วยงานมีขั้นตอนการพิจารณามาตรการควบคุมชดเชย (Compensating Controls) และกระบวนการรายงานความเสี่ยงอย่างไร ■ การสอบทานเอกสาร 1. สอบทานนโยบายและขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy and Procedure) เพื่อยืนยันว่ามีการกำหนดกรอบเวลาการแก้ไขตามระดับความรุนแรงและขั้นตอนการตรวจสอบผลการแก้ไข 2. สอบทานทะเบียนติดตามสถานะการแก้ไขช่องโหว่ (Vulnerability Tracking Register) เพื่อตรวจสอบความต่อเนื่องของการดำเนินงานจริงเทียบกับกรอบเวลาที่กำหนด 3. สอบทานรายงานผลการสแกนซ้ำหรือทดสอบซ้ำ (Rescanning/Retest Report) เพื่อยืนยันสถานะการปิดช่องโหว่เทียบกับรายงานผลการตรวจสอบรอบแรก 4. สอบทานบันทึกหลักฐานการแก้ไขช่องโหว่ (Remediation Records) เช่น Patch Logs หรือบันทึกการปรับปรุง Configuration เพื่อยืนยันการดำเนินงานจริงเชิงเทคนิค 5. สอบทานรายงานความเสี่ยงและการพิจารณามาตรการควบคุมชดเชย (Compensating Controls) ในกรณีที่ไม่สามารถแก้ไขช่องโหว่ได้ภายในระยะเวลาที่กำหนด ■ เอกสารที่เกี่ยวข้อง 1. นโยบายและขั้นตอนการบริหารจัดการช่องโหว่ (Vulnerability Management Policy and Procedure) 2. ทะเบียนติดตามสถานะการแก้ไขช่องโหว่ (Vulnerability Tracking Register) 3. รายงานผลการสแกนซ้ำหรือทดสอบซ้ำ (Rescanning/Retest Report) 4. หลักฐานการแก้ไขช่องโหว่ (Remediation Records)	

5. รายงานความเสี่ยงและการพิจารณามาตรการควบคุมชดเชย (Compensating Controls)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.29 การส่งรายงานสรุปผลการทดสอบเจาะระบบต่อสำนักงาน (Submission of Penetration Test Summary Report)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานสามารถรวบรวมข้อมูลและประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในภาพรวมได้อย่างถูกต้อง ซึ่งจะช่วยในการกำหนดแนวทางสนับสนุนหรือแจ้งเตือนภัยคุกคามที่เหมาะสมกับระดับความเสี่ยงของโครงสร้างพื้นฐานสำคัญของประเทศ

ความเสี่ยง

การแจ้งเตือนภัยคุกคามไม่เหมาะสมกับระดับความเสี่ยงของโครงสร้างพื้นฐานสำคัญของประเทศ

การควบคุมที่พึงมี

หากได้รับการร้องขอจาก กกม. หรือ สกมช. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงานภายในกำหนด 30 (สามสิบ) วันนับแต่วันที่ได้รับหนังสือ โดยรูปแบบรายงานให้เป็นไปตามที่ สกมช. ประกาศกำหนด

แนวทางการประเมิน

1. ตรวจสอบกระบวนการการจัดทำและนำส่งรายงานสรุปผลการทดสอบเจาะระบบ เมื่อได้รับการร้องขอจาก กกม. หรือ สกมช. ว่ามีการกำหนดขั้นตอนและผู้รับผิดชอบที่ชัดเจนเพื่อให้สอดคล้องกับกรอบระยะเวลา 30 วันตามที่กฎหมายกำหนดหรือไม่
2. ตรวจสอบการดำเนินงานจริงว่ามีการจัดส่งรายงานภายในระยะเวลาที่กำหนด โดยมีการตรวจสอบรูปแบบรายงานให้เป็นไปตามที่ สกมช. ประกาศ มีการบันทึกเป็นเอกสาร และมีการเก็บหลักฐานการนำส่ง (เช่น หนังสือนำส่ง หรือบันทึกการรับ-ส่งไปรษณีย์/อีเมล) อย่างครบถ้วน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.3.10
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 5
NIST CSF 2.0	GV.OC-03
ISO/IEC27001:2022	Annex A 5.5
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีขั้นตอนและกระบวนการจัดการอย่างไรเมื่อได้รับหนังสือร้องขอจาก กกม. หรือ สกมช. เพื่อให้มั่นใจว่าสามารถรวบรวมข้อมูล ตรวจสอบรูปแบบ และจัดส่งรายงานสรุปผลได้ทันภายในกำหนด 30 วัน
2. ใครเป็นผู้รับผิดชอบในการตรวจสอบความถูกต้องของเนื้อหาและรูปแบบรายงานให้เป็นไปตามประกาศของ สกมช. และมีขั้นตอนการอนุมัติก่อนนำเสนออย่างไร
3. ในกรณีที่มีการส่งรายงาน หน่วยงานมีการจัดเก็บหลักฐานการนำเสนอและบันทึกการรับ-ส่งเอกสารไว้อย่างไร เพื่อใช้ยืนยันว่าการดำเนินงานเป็นไปตามเงื่อนไขเวลาที่กำหนด

■ การสอบทานเอกสาร

1. สอบทานหนังสือร้องขอข้อมูลจาก กกม. หรือ สกมช. เพื่อระบุวันที่ได้รับเรื่องและข้อกำหนดเฉพาะในแต่ละกรณี
2. สอบทานหนังสือนำส่งรายงานหรือหลักฐานการนำเสนอเอกสาร เพื่อตรวจสอบความสอดคล้องของระยะเวลาการดำเนินการว่าอยู่ภายใน 30 วันนับแต่วันที่ได้รับหนังสือร้องขอ
3. สอบทานรายงานสรุปผลการทดสอบเจาะระบบ เพื่อตรวจสอบความถูกต้องของรูปแบบและเนื้อหาให้เป็นไปตามที่ สกมช. ประกาศกำหนด
4. สอบทานบันทึกการรับ-ส่งเอกสารหรือสมุดทะเบียนรับ-ส่ง เพื่อยืนยันการดำเนินงานจริงในขั้นตอนการนำเสนอ

■ เอกสารที่เกี่ยวข้อง

1. หนังสือร้องขอข้อมูลจาก กกม. หรือ สกมช.
2. หนังสือนำส่งรายงานหรือหลักฐานการนำเสนอเอกสาร
3. รายงานสรุปผลการทดสอบเจาะระบบ
4. บันทึกการรับ-ส่งเอกสารหรือสมุดทะเบียนรับ-ส่ง

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

การจัดการผู้ให้บริการภายนอก (Third Party Management)

3.1.30 ภาระรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ในการใช้บริการจากภายนอก (Accountability in Third Party Management)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของบริการสำคัญที่มีการใช้บริการจากภายนอกอย่างเหมาะสม

ความเสี่ยง

ระบบสำคัญไม่ได้รับการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ให้บริการภายนอกอย่างเหมาะสม

การควบคุมที่พึงมี

หน่วยงานต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของการบริการที่สำคัญของหน่วยงาน

แนวทางการประเมิน

1. ตรวจสอบโครงสร้างการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ว่ามีการระบุผู้รับผิดชอบ (Responsible) และผู้มีภาระรับผิดชอบ (Accountable) ในการดูแลระบบ CII ไว้อย่างชัดเจน แม้จะมีการใช้งานผู้ให้บริการภายนอก
2. ตรวจสอบการดำเนินงานจริงในการกำกับดูแลและติดตามการทำงานของผู้ให้บริการภายนอก ว่ามีการดำเนินงานจริงตามที่กำหนด มีการใช้เครื่องมือในการติดตาม มีการบันทึกรายงานผล และมีการเก็บหลักฐานการปฏิบัติงานอย่างสม่ำเสมอ
3. ตรวจสอบกระบวนการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอก ตั้งแต่การคัดเลือก การทำสัญญา และการยกเลิกสัญญา เพื่อยืนยันว่าหน่วยงานยังคงไว้ซึ่งอำนาจในการตัดสินใจ และภาระรับผิดชอบสูงสุด

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.4.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 6
NIST CSF 2.0	GV.SC-02, GV.SC-10
ISO/IEC27001:2022	Annex A 5.19, Annex A 5.21, Annex A 5.22, Annex A 5.23
ISO/IEC27701:2025	A.3.10
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	15.1.1, 15.1.2, 15.1.3, 15.2.1, 15.2.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 6

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกลไกและช่องทางการสื่อสารอย่างไรในการกำกับดูแลผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าภาระรับผิดชอบ (Accountability) ยังคงอยู่ที่หน่วยงาน และมีการรายงานสถานะความมั่นคงปลอดภัยต่อผู้บริหารระดับสูงอย่างต่อเนื่อง
2. ในกรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงระบบหรือกระบวนการทำงานที่สำคัญ หน่วยงานมีขั้นตอนการพิจารณาประเมินความเสี่ยงและกระบวนการอนุมัติอย่างไรเพื่อคงไว้ซึ่งการกำกับดูแลที่เหมาะสม
3. หน่วยงานมีการใช้เครื่องมือหรือเทคนิคใดในการตรวจสอบและประเมินประสิทธิภาพการทำงานของผู้ให้บริการภายนอก (เช่น การทำ Service Audit หรือ Performance Review) และมีการจัดเก็บหลักฐานเหล่านั้นไว้อย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy) เพื่อยืนยันการกำหนดการรับผิดชอบของหน่วยงาน
2. สอบทานรายงานการประเมินความเสี่ยงผู้ให้บริการภายนอก จากการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก โดยต้องคำนึงถึงความเสี่ยงด้านต่าง ๆ ที่จำเป็น เช่น ด้านกลยุทธ์ ด้านการกำกับดูแลและบริหารจัดการผู้ให้บริการภายนอกที่ไม่ครอบคลุมและรัดกุมเพียงพอ ด้านชื่อเสียง ด้านเทคโนโลยีและภัยคุกคามทางไซเบอร์ ด้านกฎหมาย ด้านที่ตั้ง หรือประกอบธุรกิจ ด้านสัญญาหรือข้อตกลงที่ไม่ครบถ้วนสมบูรณ์ ด้านการกระจุกตัว (Concentration Risk) หรือในกรณีที่มีการว่าจ้างผู้อื่นมาดำเนินการแทน/ผู้รับเหมาช่วง (Subcontractor)
3. สอบทานรายงานการประเมินศักยภาพผู้ให้บริการ (Due Diligence Report) ก่อนการเริ่มจ้างงาน
4. สอบทานทะเบียนการให้บริการและการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Third-party Access and Service Register) เพื่อตรวจสอบความครบถ้วนของข้อมูล
5. สอบทานสัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) ที่มีการระบุขอบเขตการรับผิดชอบและสิทธิในการเข้าตรวจสอบ (Right to Audit) ของหน่วยงาน
6. สอบทานรายงานผลการติดตามและประเมินการดำเนินงานของผู้ให้บริการภายนอก (Vendor Performance Monitoring Report) เพื่อยืนยันการกำกับดูแลจริงของหน่วยงาน

■ เอกสารที่เกี่ยวข้อง

1. นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy)
2. รายงานการประเมินความเสี่ยงผู้ให้บริการภายนอก (Third Party Risk Assessment Report)
3. รายงานการประเมินศักยภาพผู้ให้บริการ (Due Diligence Report)
4. ทะเบียนการให้บริการและการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Third-party Access and Service Register)
5. สัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA)
6. รายงานผลการติดตามและประเมินการดำเนินงานของผู้ให้บริการภายนอก (Vendor Performance Monitoring Report)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.31 ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญาจ้างผู้ให้บริการภายนอก (Cybersecurity Requirements in Service Agreements)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีข้อตกลงที่ชัดเจนระหว่างหน่วยงานและผู้ให้บริการภายนอก ในการรักษามาตรฐานความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะช่วยลดช่องโหว่ที่เกิดจากการเชื่อมต่อหรือการเข้าถึงโดยบุคคลที่สาม และช่วยให้หน่วยงานสามารถกำกับดูแลความเสี่ยงตลอดอายุสัญญาได้อย่างมีประสิทธิภาพ

ความเสี่ยง

ระบบสำคัญไม่ได้รับการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ให้บริการภายนอกอย่างเหมาะสม

การควบคุมที่พึงมี

ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) หรือเงื่อนไขของ สัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อยตามที่กฎหมายกำหนด

แนวทางการประเมิน

1. ตรวจสอบข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในข้อตกลงระดับการให้บริการ (SLA) หรือสัญญาจ้าง ว่ามีการระบุรายละเอียดครอบคลุมการเข้าถึง การจัดเก็บ การสื่อสาร และการ ดำเนินงานของผู้ให้บริการภายนอกให้สอดคล้องกับที่กฎหมายกำหนด
2. ตรวจสอบการดำเนินงานจริงว่ามีการนำข้อกำหนดที่ระบุในกระบวนการไปปรับใช้ในสัญญา จริง มีการใช้เครื่องมือหรือแบบฟอร์มในการตรวจสอบความสอดคล้องก่อนลงนาม และมีการ บันทึกเป็นเอกสารหลักฐานอย่างครบถ้วน
3. ตรวจสอบหลักฐานการติดตามผลตามข้อกำหนดในสัญญา เพื่อยืนยันว่าหน่วยงานได้มีการ บังคับใช้สิทธิ์ต่าง ๆ (เช่น Right to Audit) และการควบคุมผู้รับเหมาช่วง (Subcontractor) ตามที่ระบุไว้จริง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.4.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 6
NIST CSF 2.0	GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, ID.AM-04, ID.RA-10
ISO/IEC27001:2022	Annex A 5.20, Annex A 5.21, Annex A 5.23, Annex A 8.30
ISO/IEC27701:2025	A.3.30
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	14.2.7
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 6

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและเกณฑ์ในการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อระบุลงใน SLA หรือสัญญาจ้างอย่างไร เพื่อให้มั่นใจว่าครอบคลุมความเสี่ยงจากการเข้าถึง และการดำเนินงานของผู้ให้บริการ
2. ในทางปฏิบัติ หน่วยงานมีขั้นตอนการตรวจสอบความสอดคล้องของสัญญาว่าจ้างกับ ข้อกำหนดทางกฎหมายอย่างไรก่อนที่จะมีการลงนาม และมีการจัดเก็บบันทึกผลการ ตรวจสอบนั้นไว้หรือไม่

3. หน่วยงานมีกระบวนการติดตามและกำกับดูแลผู้ให้บริการภายนอกอย่างไรเพื่อให้เป็นไปตามเงื่อนไขในสัญญา และมีการใช้เครื่องมือหรือบันทึกหลักฐานใดในการยืนยันความถูกต้องของการดำเนินงาน
4. กรณีที่ผู้ให้บริการมีการว่าจ้างผู้รับเหมาช่วง (Subcontract) หน่วยงานมีกระบวนการพิจารณาอนุญาตและควบคุมความเสี่ยงในห่วงโซ่อุปทาน (Supply Chain) อย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายหรือแนวทางการบริหารจัดการผู้ให้บริการภายนอก (Third-party Management Policy) เพื่อยืนยันการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องมีในสัญญา
2. สอบทานสัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) ของระบบที่สำคัญ เพื่อตรวจสอบความครบถ้วนของข้อกำหนดด้านการปกป้องข้อมูล สิทธิในการตรวจสอบ (Right to Audit) และภาระรับผิดชอบ (Liability)
3. สอบทานข้อตกลงการรักษาความลับ (Non-Disclosure Agreement: NDA) เพื่อยืนยันขอบเขตการคุ้มครองข้อมูลของหน่วยงาน
4. สอบทานเอกสารขอบเขตการทำงาน (Terms of Reference: TOR) เพื่อตรวจสอบความสอดคล้องของข้อกำหนดทางเทคนิคและความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการจัดซื้อจัดจ้าง

■ เอกสารที่เกี่ยวข้อง

1. นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy)
2. สัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA)
3. ข้อตกลงการรักษาความลับ (Non-Disclosure Agreement: NDA)
4. เอกสารขอบเขตการทำงาน (Terms of Reference: TOR)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.32 การตรวจสอบความถูกต้องและความสอดคล้องของผู้ให้บริการภายนอก (Verification of Third Party Compliance)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีกลไกในการยืนยันว่าผู้ให้บริการภายนอกมีการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้มาตรฐานและถูกต้องตามข้อตกลงจริง
ความเสี่ยง
ระบบสำคัญไม่ได้รับการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ให้บริการภายนอกอย่างเหมาะสม
การควบคุมที่พึงมี
ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่า สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์
แนวทางการประเมิน

1. ตรวจสอบว่าหน่วยงานมีการตรวจสอบความถูกต้องของผู้ให้บริการภายนอก (Verification Process) มีการกำหนดขั้นตอน หลักเกณฑ์ และวิธีการตรวจสอบ (เช่น การตรวจโดยบุคคลที่สาม หรือการตรวจสอบผลิตภัณฑ์) เพื่อให้มั่นใจว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญา
2. ตรวจสอบการดำเนินงานจริงว่ามีการดำเนินการตรวจสอบผู้ให้บริการตามรอบเวลาที่กำหนด โดยมีการใช้เครื่องมือหรือแบบประเมิน มีการบันทึกรายละเอียดเป็นเอกสาร และมีการเก็บหลักฐานประกอบการตรวจสอบอย่างครบถ้วน
3. ตรวจสอบความต่อเนื่องของการติดตามผลการปฏิบัติงาน และการรายงานสรุปผลการตรวจสอบต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องเพื่อพิจารณาสถานะความเสี่ยง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.4.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 6
NIST CSF 2.0	GV.SC-07, GV.SC-09, ID.RA-10, DE.CM-06,
ISO/IEC27001:2022	Annex A 5.22, Annex A 5.23
ISO/IEC27701:2025	A.3.10
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	15.1.1, 15.1.2, 15.2.1, 15.2.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและหลักเกณฑ์อย่างไรในการตรวจสอบว่าผู้ให้บริการภายนอกปฏิบัติตามข้อกำหนดความมั่นคงปลอดภัยในสัญญาจริง (เช่น การขอรายงาน Third-party Audit หรือการทำ Product Verification)
2. หน่วยงานมีวิธีการรวบรวมหลักฐานและบันทึกผลการตรวจสอบอย่างไร และมีการใช้เครื่องมือใดในการประเมินความสอดคล้องดังกล่าว
3. หากผลการตรวจสอบพบว่าผู้ให้บริการไม่ปฏิบัติตามเงื่อนไขความปลอดภัย หน่วยงานมีขั้นตอนการแจ้งเตือน บทลงโทษ หรือการติดตามให้แก้ไขอย่างไร และมีการบันทึกหลักฐานการจัดการนั้นไว้อย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy) เพื่อยืนยันการกำหนดกระบวนการและรอบเวลาในการตรวจสอบความสอดคล้องกับสัญญา
2. สอบทานรายงานผลการตรวจสอบ/ประเมินผู้ให้บริการภายนอก (Vendor Audit/Assessment Report) เพื่อยืนยันกิจกรรมการตรวจสอบจริงและข้อสรุปความสอดคล้อง

3. สอบทานใบรับรองมาตรฐานสากลหรือรายงานการประเมินโดยบุคคลที่สาม (Third-party Audit Report/Certifications เช่น ISO 27001, SOC 2) เพื่อยืนยันความน่าเชื่อถือของผู้ให้บริการ 4. สอบทานบันทึกปัญหาหรือข้อร้องเรียนที่เกิดจากผู้ให้บริการภายนอก (Vendor Issue/Complaint Logs) เพื่อประเมินประวัติการปฏิบัติงานและความสอดคล้องในเชิงปฏิบัติ 5. สอบทานหลักฐานการนำเสนอผลการประเมินต่อผู้บริหาร เพื่อยืนยันว่าผู้บริหารได้รับทราบผลการตรวจสอบและสถานะความเสี่ยงของผู้ให้บริการ ■ เอกสารที่เกี่ยวข้อง 1. นโยบายการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Policy) 2. รายงานผลการตรวจสอบ/ประเมินผู้ให้บริการภายนอก (Vendor Audit/Assessment Report) 3. ใบรับรองมาตรฐานสากลหรือรายงานการประเมินโดยบุคคลที่สาม (Third-party Audit Report/Certifications) 4. บันทึกปัญหาหรือข้อร้องเรียนที่เกิดจากผู้ให้บริการภายนอก (Vendor Issue/Complaint Logs) 5. หลักฐานการนำเสนอผลการประเมินต่อผู้บริหาร ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -

3.1.33 การปรับปรุงเงื่อนไขสัญญาจ้างตามกฎหมายหรือข้อบังคับใหม่ (Negotiation of Contract Terms for New Legal Requirements) วัตถุประสงค์ เพื่อให้มั่นใจว่า เงื่อนไขสัญญาระหว่างหน่วยงานและผู้ให้บริการภายนอกมีความสอดคล้องกับกรอบกฎหมายปัจจุบันอยู่เสมอ ความเสี่ยง เงื่อนไขของสัญญาจ้างของผู้ให้บริการภายนอกไม่สอดคล้องกับข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ส่งผลให้หน่วยงานมีความผิดหากเกิดเหตุละเมิดด้านความมั่นคงปลอดภัย การควบคุมที่พึงมี ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ แนวทางการประเมิน 1. ตรวจสอบกระบวนการติดตามและทบทวนข้อกำหนดทางกฎหมาย ระเบียบ หรือมาตรฐานใหม่ ๆ ที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ เพื่อนำมาใช้เป็นฐานในการเจรจาต่อรองและปรับปรุงเงื่อนไขสัญญาจ้างให้เป็นปัจจุบัน 2. ตรวจสอบการดำเนินงานจริงว่ามีการเจรจาต่อรองเพื่อแก้ไขสัญญา หรือทำบันทึกข้อตกลงแนบท้าย (Addendum) เมื่อมีการเปลี่ยนแปลงข้อบังคับ โดยมีการบันทึกรายงานการประชุมและจัดเก็บหลักฐานการปฏิบัติงานอย่างครบถ้วน

3. ตรวจสอบความพร้อมและการดำเนินงานตามแผนการยกเลิกสัญญา (Exit Plan) เพื่อให้มั่นใจว่ามีกระบวนการส่งมอบงาน การส่งคืนหรือทำลายข้อมูล และการรักษาความต่อเนื่องของบริการที่เป็นรูปธรรม มีการใช้เครื่องมือหรือบันทึกที่เชื่อถือได้ในการเก็บหลักฐาน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 21.4.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 6
NIST CSF 2.0	GV.OC-03, GV.SC-05
ISO/IEC27001:2022	Annex A 5.20, Annex A 5.31
ISO/IEC27701:2025	A.3.13
ISO/IEC27017:2015	15.1.2, 18.1.1, 18.1.5
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 18.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 6

ขั้นตอนการตรวจสอบ

■ **การสัมภาษณ์**

1. หน่วยงานมีขั้นตอนและกระบวนการอย่างไรในการติดตามกฎหมายหรือข้อบังคับใหม่ ๆ เพื่อนำมาพิจารณาปรับปรุงเงื่อนไขในสัญญาจ้างผู้ให้บริการภายนอกให้สอดคล้องอยู่เสมอ
2. ในกรณีที่มีการเจรจาต่อรองเงื่อนไขสัญญาใหม่ หน่วยงานมีการบันทึกรายละเอียดการตกลงการใช้เครื่องมือสื่อสารหรือการจัดทำเอกสารแนบท้ายอย่างไรเพื่อให้มีผลบังคับใช้ตามกฎหมาย
3. หน่วยงานมีแนวทางและเกณฑ์ในการกำหนดแผนการยกเลิกสัญญา (Exit Plan) อย่างไรเพื่อให้มั่นใจว่าเมื่อสิ้นสุดสัญญาจะไม่มีข้อมูลค้างอยู่ที่ผู้ให้บริการ และบริการสำคัญสามารถดำเนินต่อไปได้โดยไม่หยุดชะงัก
4. เมื่อมีการทำลายหรือส่งมอบข้อมูลคืนหลังสิ้นสุดสัญญา หน่วยงานมีวิธีการตรวจสอบความถูกต้องและจัดเก็บหลักฐานยืนยันการดำเนินงาน (เช่น Certificate of Destruction) อย่างไร

■ **การสอบทานเอกสาร**

1. สอบทานนโยบายหรือแนวทางการบริหารสัญญา (Contract Management Policy) ที่กำหนดให้มีการทบทวนเงื่อนไขตามข้อบังคับทางกฎหมายที่เปลี่ยนแปลงไป
2. สอบทานบันทึกการประชุมเจรจาต่อรอง (Meeting Minutes) หรือบันทึกข้อตกลงแนบท้ายสัญญา (Contract Addendum/Memorandum of Agreement) เพื่อยืนยันการปรับปรุงเงื่อนไขตามกฎหมายใหม่
3. สอบทานกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญา (Exit Strategy and Exit Plan) เพื่อตรวจสอบความครบถ้วนของขั้นตอนการบริหารจัดการข้อมูลและความต่อเนื่องของบริการ
4. สอบทานบันทึกหลักฐานการส่งมอบหรือทำลายข้อมูล (Data Handover/Destruction Records) เพื่อยืนยันว่าผู้ให้บริการได้ดำเนินการตามแผน Exit Plan อย่างถูกต้องปลอดภัย
5. สอบทานสัญญาจ้าง (Main Contract) เพื่อตรวจสอบข้อกำหนดเกี่ยวกับการบอกเลิกสัญญา และภาระหน้าที่ของผู้ให้บริการเมื่อสิ้นสุดการจ้างงาน

■ เอกสารที่เกี่ยวข้อง

1. นโยบายหรือแนวทางการบริหารสัญญา (Contract Management Policy)
2. บันทึกการประชุมเจรจาต่อรองและบันทึกข้อตกลงแนบท้ายสัญญา (Contract Addendum/MOA)
3. กลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญา (Exit Strategy and Exit Plan)
4. บันทึกหลักฐานการส่งมอบหรือทำลายข้อมูล (Data Handover/Destruction Records)
5. สัญญาจ้าง (Contract) ที่ระบุเงื่อนไขการบอกเลิกและผลหลังสิ้นสุดสัญญา

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

2. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)	
การควบคุมการเข้าถึง (Access Control)	
3.1.34 การจำกัดการเข้าถึงบริการที่สำคัญ (Restriction of Access to Critical Services)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า บริการที่สำคัญของหน่วยงานได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งจากบุคคลที่ไม่เกี่ยวข้องและอุปกรณ์ที่ไม่มีมาตรฐานความปลอดภัย	
ความเสี่ยง	
บุคคลหรืออุปกรณ์ที่ไม่ได้รับอนุญาตสามารถเข้าถึงบริการที่สำคัญได้	
การควบคุมที่มี	
ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกจำกัดไว้เฉพาะ (ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ (ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการกำหนดและจำกัดสิทธิ์การเข้าถึงบริการที่สำคัญ ว่ามีข้อกำหนดที่ครอบคลุมถึง (ก) และ (ข) 2. ตรวจสอบการดำเนินงานจริงในการอนุญาตและจำกัดสิทธิ์การเข้าถึง ว่ามีการใช้เครื่องมือในการควบคุม (เช่น NAC, Firewall, IAM) และมีการบันทึกหลักฐานการอนุมัติสิทธิ์ที่สอดคล้องกับนโยบาย 3. ตรวจสอบหลักฐานการควบคุมอุปกรณ์และอินเทอร์เฟซ เพื่อยืนยันว่ามีการตรวจสอบและอนุญาตเฉพาะอุปกรณ์ที่มีตัวตนถูกต้อง (Authorized Devices) ก่อนเข้าถึงบริการที่สำคัญ 4. ตรวจสอบกระบวนการและบันทึกการทบทวนสิทธิ์ (User Access Review) เพื่อให้มั่นใจว่ากิจกรรมและบุคคลที่เข้าถึงระบบยังคงได้รับอนุญาตตามความจำเป็น (Least Privilege) และมีการระบุสิทธิ์ทันทีเมื่อหมดความจำเป็น	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.1.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 7
NIST CSF 2.0	PR.AA-05, PR.IR-01
ISO/IEC 27001:2022	Annex A 5.15, Annex A 6.1, Annex A 6.5, Annex A 7.1, Annex A 7.2, Annex A 7.3, Annex A 7.6, Annex A 7.8, Annex A 8.3, Annex A 8.4, Annex A 8.11
ISO/IEC 27701:2025	-
ISO/IEC 27017:2015	9.1.2, 9.4.1
ISO/IEC 27007:2020	-
ISO/IEC TS 27008:2019	7.1.1, 7.3.1, 9.1.1, 9.4.1, 9.4.5, 11.1.1, 11.1.2, 11.1.3, 11.1.5, 11.1.6, 11.2.1

มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (6)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีเกณฑ์และกระบวนการอย่างไรในการระบุและจำกัดสิทธิ์ให้เฉพาะบุคลากรและกิจกรรมที่ได้รับอนุญาตในการเข้าถึงบริการสำคัญ 2. การดำเนินการตามขั้นตอนการขออนุมัติ การระบุ และยกเลิกสิทธิ์การเข้าถึง มีการบันทึกหลักฐานและใช้เครื่องมือใดในการควบคุมให้เป็นไปตามกระบวนการที่กำหนด 3. หน่วยงานมีวิธีการทางเทคนิคหรือมาตรการควบคุมอย่างไร เพื่อตรวจสอบและอนุญาตเฉพาะอุปกรณ์และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้นก่อนให้เข้าถึงระบบ 4. ในกรณีที่มีการเข้าถึงจากอุปกรณ์ภายนอกหรืออินเทอร์เฟซใหม่ หน่วยงานมีกระบวนการตรวจสอบความปลอดภัยและลงทะเบียนอุปกรณ์นั้นอย่างไร 5. หน่วยงานมีระยะเวลาในการทบทวนสิทธิ์ผู้ใช้งานและรายการอุปกรณ์ที่ได้รับอนุญาตอย่างไร และใครเป็นผู้รับผิดชอบในการยืนยันความถูกต้อง ■ การสอบทานเอกสาร 1. สอบทานนโยบายการควบคุมการเข้าถึง (Access Control Policy) ว่ามีการระบุหลักการจำกัดสิทธิ์เฉพาะบุคคล กิจกรรม อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาต 2. สอบทานทะเบียนรายชื่อผู้ใช้งานและสิทธิ์ (User Access Matrix) เพื่อตรวจสอบความสอดคล้องของการมอบหมายสิทธิ์ตามบทบาทหน้าที่ (Role-based Access Control : RBAC) และหลักการ Least Privilege 3. สอบทานบันทึกคำขออนุมัติ/ระบุ/ยกเลิกสิทธิ์การเข้าถึงระบบ เพื่อยืนยันว่าการดำเนินงานจริงตามขั้นตอนและมีการลงนามอนุมัติโดยผู้มีอำนาจ 4. สอบทานทะเบียนรายการอุปกรณ์และอินเทอร์เฟซที่ได้รับอนุญาต ว่ามีความเป็นปัจจุบันและระบุข้อมูลระบุตัวตนอุปกรณ์ได้อย่างถูกต้อง 5. สอบทานรายงานผลการทบทวนสิทธิ์การเข้าถึง (User Access Review Report) เพื่อตรวจสอบหลักฐานการตรวจสอบสิทธิ์ประจำปีหรือตามรอบระยะเวลาที่กำหนด ■ เอกสารที่เกี่ยวข้อง 1. นโยบายการควบคุมการเข้าถึง (Access Control Policy) 2. ทะเบียนรายชื่อผู้ใช้งานและสิทธิ์ (User Access Matrix) 3. บันทึกคำขออนุมัติ/ระบุ/ยกเลิกสิทธิ์การเข้าถึงระบบ 4. ทะเบียนรายการอุปกรณ์และอินเทอร์เฟซที่ได้รับอนุญาต 5. รายงานผลการทบทวนสิทธิ์การเข้าถึง (User Access Review Report) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบการตั้งค่า (Configuration) ในระบบควบคุมสิทธิ์ เช่น การตั้งค่าสิทธิ์บน Active Directory หรือการจัดการสิทธิ์ในระดับ OS/Application/Database ว่าสอดคล้องกับทะเบียนรายชื่อผู้ใช้งานและสิทธิ์ (User Access Matrix) หรือไม่ 2. ตรวจสอบว่าผู้ใช้ที่มีสิทธิ์สูง (Privileged User เช่น Admin, Root) แยกบัญชี (User ID) ระหว่างการทำงานปกติกับการทำงานที่ต้องใช้สิทธิ์สูงหรือสิทธิ์พิเศษออกจากกันหรือไม่	

3. ตรวจสอบบันทึกเหตุการณ์การเข้าถึงระบบ (Access Logs) ว่ามีใครใช้งานระบบบ้าง ในช่วงเวลาใด สอดคล้องกับบันทึกคำขออนุมัติหรือไม่
4. ตรวจสอบบันทึกเหตุการณ์การเข้าถึงระบบ (Access Logs) ว่ามีการระบุ/ลบสิทธิ์การเข้าถึงระบบ สอดคล้องกับบันทึกคำขออนุมัติหรือไม่
5. ตรวจสอบบันทึกเหตุการณ์การเข้าถึงระบบ (Access Logs) ว่ามีการใช้งานที่ผิดปกติ (Unauthorized access attempts) หรือไม่ เช่น การเข้าสู่ระบบด้วยบัญชีผู้ใช้งานที่ถูกระงับสิทธิ์หรืออดีตพนักงาน หรือบัญชีผู้ใช้แปลกปลอม
6. ตรวจสอบการตั้งค่าบนระบบเครือข่าย (Network Access Control : NAC) เพื่อยืนยันว่ามี การจำกัดสิทธิ์เฉพาะอุปกรณ์ (Hardware ID/MAC Address) ที่ลงทะเบียนไว้ในทะเบียน อุปกรณ์เท่านั้นที่สามารถเข้าถึงบริการสำคัญได้

3.1.35 เทคนิคการตรวจสอบสิทธิ์การเข้าถึง (Authentication Techniques for Access)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า กระบวนการยืนยันตัวตนของผู้ใช้งานและระบบมีความแข็งแกร่งเพียงพอและเหมาะสมกับระดับความเสี่ยงของบริการสำคัญ	
ความเสี่ยง	
บุคคลหรืออุปกรณ์ที่ไม่ได้รับอนุญาตสามารถเข้าถึงบริการที่สำคัญได้	
การควบคุมที่พึงมี	
ต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการกำหนดเทคนิคการตรวจสอบสิทธิ์ (Authentication Techniques) ว่ามีการพิจารณาให้สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) และโหมดการเข้าถึง (Access Modes) ของแต่ละบริการที่สำคัญ 2. ตรวจสอบการดำเนินงานจริงว่าบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาต ได้ใช้เทคนิคการตรวจสอบสิทธิ์ตามที่กำหนดไว้ในแต่ละระดับความเสี่ยง (เช่น การใช้ MFA สำหรับระบบที่มีความเสี่ยงสูง หรือการเข้าถึงจากภายนอก) 3. ตรวจสอบการใช้เครื่องมือและการบันทึกหลักฐานประกอบการดำเนินงาน เช่น บันทึกการตั้งค่าระบบพิสูจน์ตัวตน (Authentication Logs)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.1.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 7
NIST CSF 2.0	PR.AA-03
ISO/IEC27001:2022	Annex A 5.17, Annex A 8.5

ISO/IEC27701:2025	A.3.23
ISO/IEC27017:2015	9.2.4
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	9.2.4, 9.3.1, 9.4.2, 9.4.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (6) (ก)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีเกณฑ์การประเมินโปรไฟล์ความเสี่ยง (Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญอย่างไร เพื่อนำมาใช้ในการกำหนดระดับความเข้มงวดของเทคนิคการตรวจสอบสิทธิ์ในแต่ละบริการที่สำคัญ 2. สำหรับโหมดการเข้าถึงที่แตกต่างกัน (เช่น Local, Remote) หน่วยงานมีการเลือกใช้เทคนิคการตรวจสอบสิทธิ์ที่แตกต่างกันเพื่อให้สอดคล้องกับความเสี่ยงอย่างไร 3. ในกรณีของกิจกรรมหรือกระบวนการที่ต้องใช้สิทธิ์ระดับสูง (เช่น Privileged Account) หน่วยงานมีการบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) หรือเทคนิคอื่นที่รัดกุมกว่าปกติอย่างไร 4. หน่วยงานมีวิธีการตรวจสอบอย่างไรว่าบุคลากรและกิจกรรมต่าง ๆ ได้รับการตรวจสอบสิทธิ์ด้วยเทคนิคที่ถูกต้องตามนโยบายที่วางไว้ ■ การสอบทานเอกสาร 1. สอบทานรายงานโปรไฟล์ความเสี่ยง (Risk Profile Report) เพื่อยืนยันว่ามีการระบุระดับความเสี่ยงที่เชื่อมโยงกับการกำหนดเทคนิคการตรวจสอบสิทธิ์ในแต่ละโหมดการเข้าถึง 2. สอบทานนโยบายรหัสผ่านและการพิสูจน์ตัวตน (Password and Authentication Policy) ว่ามีการระบุเงื่อนไขการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงและโหมดการเข้าถึงที่ได้รับอนุญาต 3. สอบทานมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับการพิสูจน์ตัวตน เพื่อตรวจสอบเกณฑ์ทางเทคนิค (เช่น MFA, Biometrics, Token) ที่ต้องใช้ในแต่ละระบบ 4. สอบทานบันทึกการตั้งค่าระบบหรือรายงานผลการตรวจสอบสิทธิ์ (System Configuration or Authentication Reports) เพื่อยืนยันหลักฐานการดำเนินงานจริงตามที่นโยบายกำหนด ■ เอกสารที่เกี่ยวข้อง 1. รายงานโปรไฟล์ความเสี่ยง (Risk Profile Report) 2. นโยบายรหัสผ่านและการพิสูจน์ตัวตน (Password and Authentication Policy) 3. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) 4. บันทึกการตั้งค่าระบบหรือรายงานผลการตรวจสอบสิทธิ์ (System Configuration or Authentication Reports) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	

1. ตรวจสอบการตั้งค่ารหัสผ่านจริงในระบบ ว่ามีการบังคับใช้กฎการตั้งรหัสผ่านให้สอดคล้องและตรงตามที่ระบุไว้ในเอกสารนโยบายหรือแนวปฏิบัติขององค์กร
2. ตรวจสอบบันทึกการเข้าถึง (Access Logs) ของระบบว่ามีการเปลี่ยนรหัสผ่านตามรอบที่กำหนด

3.1.36 การเก็บรักษาและตรวจสอบบันทึกการเข้าถึง (Access Logging and Monitoring)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีหลักฐานที่เพียงพอสำหรับการตรวจสอบย้อนหลัง (Audit Trail) ในกรณีที่เกิดเหตุการณ์ภัยคุกคาม และเพื่อให้มั่นใจว่า หน่วยงานมีกลไกในการตรวจพบพฤติกรรมการบุกรุกหรือการใช้งานที่ผิดปกติได้อย่างรวดเร็ว

ความเสี่ยง

ไม่มีหลักฐานเพื่อติดตามผู้กระทำผิด หรือไม่สามารถตรวจจับกิจกรรมที่ผิดปกติได้ทัน่วงที

การควบคุมที่พึงมี

ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และต้องตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ โดยความถี่ในการตรวจสอบต้องสอดคล้องกับระดับความสำคัญหรือกิจกรรมการเข้าถึงนั้น ๆ

แนวทางการประเมิน

1. ตรวจสอบกระบวนการการเก็บรักษาบันทึกการเข้าถึง (Access Logs) และความพยายามเข้าถึง (Access Attempts) ว่ามีการกำหนดขั้นตอนการจับเก็บที่ครบถ้วนสำหรับทุกบริการสำคัญ
2. ตรวจสอบกระบวนการเฝ้าระวังและสอบสวนบันทึก ว่ามีการระบุความถี่ในการตรวจสอบที่สอดคล้องกับระดับความสำคัญของระบบหรือความเสี่ยงของกิจกรรมการเข้าถึง
3. ตรวจสอบการดำเนินงานจริงในการจัดเก็บและเฝ้าระวังบันทึกข้อมูล ว่ามีการใช้เครื่องมือ (เช่น SIEM, Centralized Log Management) มีการบันทึกเป็นเอกสาร และมีการเก็บหลักฐานการตรวจสอบอย่างสม่ำเสมอตามรอบที่กำหนด
4. ตรวจสอบมาตรการคุ้มครองบันทึกข้อมูล เพื่อยืนยันว่ามีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย และการดัดแปลงแก้ไข (Integrity) เพื่อให้หลักฐานมีความน่าเชื่อถือ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.1.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 7
NIST CSF 2.0	DE.CM-01, DE.CM-03
ISO/IEC27001:2022	Annex A 5.33, Annex A 8.15, Annex A 8.16, Annex A 8.17
ISO/IEC27701:2025	A.3.14, A.3.25
ISO/IEC27017:2015	12.4.1, 12.4.3, 12.4.4, 18.1.3
ISO/IEC27007:2020	A4.5
ISO/IEC TS 27008:2019	12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (6) (ง)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการจัดเก็บบันทึกการเข้าถึง (Access Logs) ทั้งการเข้าถึงที่สำเร็จและไม่สำเร็จสำหรับบริการสำคัญอย่างไร และใช้เครื่องมือใดในการรวมศูนย์ข้อมูล (Centralization)
2. เกณฑ์การกำหนดความถี่ในการตรวจสอบบันทึกข้อมูล (Log Review) ของแต่ละระบบคืออะไร และมีการปรับเปลี่ยนตามระดับความสำคัญของระบบอย่างไร
3. ในทางปฏิบัติ เมื่อพบกิจกรรมที่ผิดปกติจากการตรวจสอบ Log มีขั้นตอนการบันทึก การแจ้งเตือน และการเก็บหลักฐานเพื่อดำเนินการต่ออย่างไร
4. หน่วยงานมีมาตรการควบคุมสิทธิ์การเข้าถึงระบบจัดเก็บ Log อย่างไร
5. หน่วยงานมีมาตรการเชิงเทคนิคอย่างไร (เช่น การตั้งค่า Write-once, การทำ Hashing) เพื่อรับประกันว่าบันทึกการเข้าถึงจะไม่ถูกดัดแปลงหรือลบโดยผู้ดูแลระบบหรือผู้ไม่ประสงค์ดี

■ การสอบทานเอกสาร

1. สอบทานนโยบายและขั้นตอนการบริหารจัดการ Log (Log Management Policy and Procedure) ว่าครอบคลุมรายการ Log ที่ต้องเก็บ ระยะเวลา และเกณฑ์ความถี่ในการตรวจสอบที่สอดคล้องกับสำคัญของระบบ
2. สอบทานมาตรฐานการตั้งค่าความปลอดภัยสำหรับ Log (Security Configuration Baseline for Logging) เพื่อตรวจสอบรายการข้อมูลที่จำเป็น (เช่น User ID, IP, Timestamp) และมาตรการป้องกันการแก้ไข
3. สอบทานรายงานการตรวจสอบและแจ้งเตือนเหตุการณ์ผิดปกติ (Security Incident/Event Log Report) เพื่อยืนยันว่ามีการเฝ้าระวังและบันทึกหลักฐานเมื่อพบกิจกรรมที่น่าสงสัย
4. สอบทานบันทึกการทบทวน Log ประจำงวด (Periodic Log Review Log/Report) เพื่อตรวจสอบหลักฐานการดำเนินงานจริงตามรอบความถี่ที่กำหนดไว้ในนโยบาย

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการบริหารจัดการ Log (Log Management Policy and Procedure)
2. มาตรฐานการตั้งค่าความปลอดภัยสำหรับ Log (Security Configuration Baseline for Logging)
3. รายงานการตรวจสอบและแจ้งเตือนเหตุการณ์ผิดปกติ (Security Incident/Event Log Report)
4. บันทึกการทบทวน Log ประจำงวด (Periodic Log Review Log/Report)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบการตั้งค่าในระบบจริง ว่ามีการเปิดใช้งานและตั้งค่าการบันทึกประวัติการใช้งาน (Log) ตรงตามนโยบายที่กำหนด
2. ตรวจสอบว่ามีการเก็บบันทึกข้อมูลที่จำเป็นหรือไม่ เช่น รหัสผู้ใช้งาน (User ID) วันที่และเวลา การเข้าสู่ระบบ (Log-on)/การออกจากระบบ (Log-off) หมายเลขเครื่องหรือชื่อเครื่องคอมพิวเตอร์ที่ใช้ในการเชื่อมต่อ หมายเลข IP Address และรูปแบบการสื่อสาร (เช่น HTTP, SSH, FTP) ที่ใช้
3. ตรวจสอบสิทธิ์ในการเข้าถึงระบบ Log (SIEM/Storage) ว่าถูกจำกัดเฉพาะผู้ที่ได้รับมอบหมายเท่านั้น และไม่มีสิทธิ์ในการลบหรือแก้ไข

4. ตรวจสอบการตั้งค่าระยะเวลาการเก็บรักษา (Retention Policy) ว่าสอดคล้องกับกฎหมายอื่นที่เกี่ยวข้อง (เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่กำหนดให้เก็บไม่น้อยกว่า 90 วัน)

3.1.37 การกำกับดูแลการเข้าถึงอินเทอร์เฟซและการเข้าถึงทางลอจิคอล (Supervision of Interface and Logical Access)

วัตถุประสงค์

เพื่อให้มั่นใจว่า การเข้าถึงจุดเชื่อมต่อที่สำคัญของระบบ ทั้งในทางกายภาพและทางลอจิคอล จะได้รับการเฝ้าสังเกตการณ์จากหน่วยงาน ซึ่งจะช่วยป้องกันการลักลอบติดตั้งอุปกรณ์แปลกปลอม การขโมยข้อมูล หรือการเปลี่ยนแปลงการตั้งค่าระบบโดยไม่ได้รับอนุญาต

ความเสี่ยง

มีการติดตั้งอุปกรณ์แปลกปลอมหรือเปลี่ยนแปลงค่าของระบบโดยไม่ได้รับอนุญาต

การควบคุมที่พึงมี

ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

- (ก) ทำภายใต้การดูแลของหน่วยงานเท่านั้น และ
- (ข) ดำเนินการในสถานที่ (On-site) หากเป็นไปได้

แนวทางการประเมิน

1. ตรวจสอบกระบวนการกำกับดูแลการเข้าถึงอินเทอร์เฟซ (Interface) ทั้งทางกายภาพ (เช่น USB, Serial Port) และทางลอจิคอล (Logical Access) ว่ามีข้อกำหนดให้ดำเนินการภายใต้การดูแลของหน่วยงาน และต้องปฏิบัติงานในสถานที่ (On-site) เป็นหลัก
2. ตรวจสอบการดำเนินงานจริงในการเข้าถึงอินเทอร์เฟซของบริการสำคัญ ว่ามีการควบคุมโดยเจ้าหน้าที่ของหน่วยงาน (Supervision) มีการใช้เครื่องมือในการปิดกั้นหรือจำกัดสิทธิ์ และมีการบันทึกหลักฐานการปฏิบัติงานในสถานที่จริงตามที่กำหนด
3. ตรวจสอบมาตรการควบคุมอินเทอร์เฟซ ว่ามีการใช้เทคนิคหรือเครื่องมือเพื่อจำกัดการใช้งาน (เช่น การปิด Port ใน BIOS/OS, การใช้ Endpoint Security) และมีหลักฐานการอนุญาตเป็นรายกรณี (Exception handling)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.1.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 7
NIST CSF 2.0	PR.AA-05, PR.AA-06
ISO/IEC27001:2022	Annex A 5.15, Annex A 7.12
ISO/IEC27701:2025	
ISO/IEC27017:2015	9.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	9.1.1, 11.2.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีนโยบายและขั้นตอนการควบคุมให้ปฏิบัติงานในสถานที่ (On-site) และมีเจ้าหน้าที่ควบคุมดูแล (Escort/Supervise) สำหรับการเข้าถึงอินเทอร์เฟซ (Interface) ทั้งทางกายภาพ (เช่น USB, Serial Port) และทางลอจิคอล (Logical Access) อย่างไร
2. หน่วยงานมีมาตรการกำกับดูแลอย่างไร เมื่อบุคคล (เช่น Vendor หรือเจ้าหน้าที่เทคนิค) จำเป็นต้องเข้าถึงอินเทอร์เฟซทางกายภาพ (เช่น พอร์ตอนุกรม, USB) หรือเข้าถึงทางลอจิคอล (Logical Access) ของบริการสำคัญ
3. หน่วยงานมีมาตรการหรือเครื่องมือที่ใช้ในการบล็อกหรือจำกัดการเข้าถึงพอร์ตสื่อสาร (Disable unused ports) อย่างไร
4. เมื่อมีความจำเป็นต้องเปิดใช้งานพอร์ตหรืออินเทอร์เฟซชั่วคราว มีกระบวนการขออนุมัติและใครเป็นผู้รับผิดชอบในการติดตามการกำกับดูแลจนเสร็จสิ้นกิจกรรม

■ การสอบทานเอกสาร

1. สอบทานนโยบายการควบคุมการเข้าถึง (Access Control Policy) เพื่อตรวจสอบข้อกำหนดเรื่องการปฏิบัติงานในสถานที่และการกำกับดูแลโดยหน่วยงาน
2. สอบทานบันทึกการกำกับดูแลการปฏิบัติงานของบุคคลภายนอกหรือเจ้าหน้าที่ (Supervision/Escort Logs) เพื่อยืนยันว่าการเข้าถึงอินเทอร์เฟซเกิดขึ้นภายใต้การดูแลของหน่วยงาน
3. สอบทานบันทึกการเข้า-ออกสถานที่สำคัญ (Data Center Access Log) เพื่อเทียบเคียงกับการเข้าถึงอินเทอร์เฟซทางกายภาพว่าเป็นการปฏิบัติงานแบบ On-site จริง
4. สอบทานบันทึกคำขอเปิดใช้งานพอร์ตหรือการใช้งานอินเทอร์เฟซเป็นกรณีพิเศษ (Port/Interface Access Request Form) เพื่อตรวจสอบความครบถ้วนของรายละเอียดการอนุญาตและระยะเวลาที่ใช้

■ เอกสารที่เกี่ยวข้อง

1. นโยบายการควบคุมการเข้าถึง (Access Control Policy)
2. บันทึกการกำกับดูแลการปฏิบัติงานของบุคคลภายนอกหรือเจ้าหน้าที่ (Supervision/Escort Logs)
3. บันทึกการเข้า-ออกสถานที่สำคัญ (Data Center Access Log)
4. บันทึกคำขอเปิดใช้งานพอร์ตหรือการใช้งานอินเทอร์เฟซเป็นกรณีพิเศษ (Port/Interface Access Request Form)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

3.1.38 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

วัตถุประสงค์

เพื่อให้มั่นใจว่า ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่สนับสนุนบริการสำคัญ มีการตั้งค่าความมั่นคงปลอดภัยที่แข็งแกร่ง (System Hardening) และเป็นมาตรฐานเดียวกันทั้งองค์กร

ความเสี่ยง

บริการสำคัญมีความเสี่ยงจากการที่ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่สนับสนุนบริการสำคัญ ไม่ได้รับการตั้งค่าความมั่นคงปลอดภัยที่เหมาะสมและเพียงพอ

การควบคุมที่พึงมี

ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของหน่วยงาน

แนวทางการประเมิน

1. ตรวจสอบกระบวนการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ว่ามีการครอบคลุมทั้งระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของบริการที่สำคัญ และมีการนำโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) มาเป็นปัจจัยในการกำหนดความเข้มงวด
2. ตรวจสอบการดำเนินงานจริงว่ามีการนำมาตรฐานดังกล่าวไปบังคับใช้กับระบบที่เกี่ยวข้อง การนำเครื่องมือมาใช้ในการตรวจสอบความสอดคล้อง (Configuration Audit Tool) และมีการบันทึกหลักฐานการปรับปรุงค่าความมั่นคงปลอดภัย (Hardening) เป็นเอกสาร
3. ตรวจสอบหลักฐานการทบทวนและปรับปรุงมาตรฐาน เพื่อให้มั่นใจว่ามาตรฐานที่กำหนดขึ้น ยังคงสอดคล้องกับสถานะความเสี่ยงล่าสุดและเทคโนโลยีที่เปลี่ยนแปลงไป

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.2.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 8
NIST CSF 2.0	PR.PS-01
ISO/IEC27001:2022	Annex A 7.7, Annex A 8.9, Annex A 8.23, Annex A 8.27
ISO/IEC27701:2025	A.3.19, A.3.29
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	11.2.9, 14.2.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (5)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีหลักเกณฑ์อย่างไรในการเลือกอ้างอิงมาตรฐานสากล (เช่น CIS Benchmarks, NIST) มาพัฒนาเป็น Security Baseline ขององค์กรให้เหมาะสมกับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่มีอยู่

2. กระบวนการปรับแต่ง (Fine-tune) มาตรฐานการกำหนดค่าให้สอดคล้องกับโปรไฟล์ความเสี่ยง (Risk Profile) ของแต่ละบริการสำคัญมีขั้นตอนอย่างไร และใครเป็นผู้รับผิดชอบในการอนุมัติมาตรฐานดังกล่าว
3. เมื่อมีการติดตั้งระบบใหม่ หน่วยงานมีกระบวนการบังคับใช้มาตรฐานอย่างไร และมีการใช้เครื่องมือหรือระบบอัตโนมัติในการตรวจสอบความสอดคล้องก่อนนำระบบขึ้นใช้งานจริง
4. ในกรณีที่ระบบไม่สามารถตั้งค่าตามมาตรฐานได้ (Exception) หน่วยงานมีกระบวนการประเมินความเสี่ยงชดเชยและบันทึกหลักฐานไว้อย่างไร

■ การสอบทานเอกสาร

1. สอบทานมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) เพื่อยืนยันความครบถ้วนของเนื้อหาที่ครอบคลุมทั้งระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของบริการที่สำคัญ
2. สอบทานรายงานโปรไฟล์ความเสี่ยง (Risk Profile) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเทียบเคียงความสอดคล้องกับข้อกำหนดในมาตรฐาน ว่าระบบที่มีความสำคัญสูงมีการกำหนดค่าที่เข้มงวดกว่าปกติ
3. สอบทานบันทึกหรือรายงานการตรวจประเมินความสอดคล้อง (Configuration Compliance Audit Report/Hardening Logs) เพื่อยืนยันว่ามีการดำเนินงานจริงตามมาตรฐานที่กำหนดไว้
4. สอบทานทะเบียนบันทึกรายการข้อยกเว้น (Security Exception Log) การปฏิบัติตามมาตรฐาน ในกรณีที่ระบบมีข้อจำกัดทางเทคนิค เพื่อตรวจสอบการประเมินความเสี่ยงและการอนุมัติ

■ เอกสารที่เกี่ยวข้อง

1. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)
2. รายงานโปรไฟล์ความเสี่ยง (Risk Profile Report)
3. บันทึกหรือรายงานการตรวจประเมินความสอดคล้อง (Configuration Compliance Audit Report/Hardening Logs)
4. ทะเบียนบันทึกรายการข้อยกเว้น (Security Exception Log)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.39 หลักการรักษาความมั่นคงปลอดภัยในมาตรฐานการกำหนดค่า (Principles for Security Baseline Configuration)

วัตถุประสงค์

เพื่อให้มั่นใจว่า มาตรฐานการตั้งค่าระบบของหน่วยงานมีความสมบูรณ์และครอบคลุมหลักการรักษาความมั่นคงปลอดภัยเชิงลึก

ความเสี่ยง

บริการสำคัญมีความเสี่ยงจากการที่ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่สนับสนุนบริการสำคัญ ไม่ได้รับการตั้งค่าความมั่นคงปลอดภัยที่เหมาะสมและเพียงพอ

การควบคุมที่พึงมี

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องประกอบด้วยหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย 8 ประการ ได้แก่

- (ก) สิทธิพิเศษน้อยที่สุด
- (ข) การแบ่งแยกหน้าที่
- (ค) ความซับซ้อนของรหัสผ่าน
- (ง) การลบบัญชีที่ไม่ได้ใช้
- (จ) การลบบริการที่ไม่จำเป็น
- (ฉ) การปิดพอร์ตที่ไม่ใช้
- (ช) การป้องกันมัลแวร์ และ
- (ซ) การปรับปรุงซอฟต์แวร์และแพตช์

แนวทางการประเมิน

1. ตรวจสอบกระบวนการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ว่ามีเนื้อหาครอบคลุมหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย 8 ประการ (ก) – (ซ) ตามที่กำหนด

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.2.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 8
NIST CSF 2.0	PR.AA-05, PR.PS-01
ISO/IEC27001:2022	Annex A 5.3, Annex A 5.17, Annex A 5.18, Annex A 8.2, Annex A 8.7, Annex A 8.8, Annex A 8.9, Annex A 8.18, Annex A 8.23, Annex A 8.27
ISO/IEC27701:2025	A.3.9, A.3.29
ISO/IEC27017:2015	9.2.2, 9.2.3, 9.2.4, 9.4.4, 12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.2, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.3, 9.4.4, 12.2.1, 12.6.1, 14.2.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (5), 4 (6) (ก), 4 (6) (ข)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการและเครื่องมือใดที่ใช้ในการบังคับใช้มาตรฐาน (Enforcement) ครอบคลุมหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย 8 ประการ (ก) – (ซ)
2. หน่วยงานมีการใช้เครื่องมือใดในการตรวจสอบการป้องกันมัลแวร์และการปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันตามมาตรฐานที่กำหนดไว้

■ การสอบทานเอกสาร

1. สอบทานเอกสารมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) เพื่อยืนยันว่ามีเนื้อหาครอบคลุมหลักการตามการควบคุมที่พึงมี ข้อ (ก) - (ข) ครบถ้วนทุกระบบสำคัญ ■ เอกสารที่เกี่ยวข้อง 1. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) 2. รายการตรวจสอบการกำหนดค่าความมั่นคงปลอดภัย (Security Configuration Checklist) 3. รายงานการทดสอบหรือผลสแกนช่องโหว่ 4. ทะเบียนบันทึกรายการข้อยกเว้น (Security Exception Log) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.1.40 การตรวจสอบความสอดคล้องของมาตรฐานการกำหนดค่าก่อนเริ่มใช้งาน (Security Baseline Enforcement before Connection or Change)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า มาตรการรักษาความมั่นคงปลอดภัยทางเทคนิคได้ถูกนำมาใช้อย่างถูกต้องและครบถ้วน	
ความเสี่ยง	
บริการสำคัญมีความเสี่ยงจากการที่ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่สนับสนุนบริการสำคัญ ไม่ได้รับการตั้งค่าความมั่นคงปลอดภัยที่เหมาะสมและเพียงพอ	
การควบคุมที่พึงมี	
ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการที่ต้องดำเนินการเมื่อนำทรัพย์สินใหม่เชื่อมต่อเข้ากับบริการที่สำคัญ ว่าครอบคลุมการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ 2. ตรวจสอบการดำเนินงานจริงว่ามีการนำมาตรฐานไปบังคับใช้กับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย การนำเครื่องมือมาใช้ (เช่น GPO, Configuration Management, Patch Management) และมีการบันทึกหลักฐานการดำเนินงาน 3. ตรวจสอบหลักฐานและบันทึกที่แสดงถึงการตรวจสอบความสอดคล้องกับมาตรฐาน ก่อนที่จะอนุญาตให้เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน 4. ตรวจสอบหลักฐานและบันทึกที่แสดงถึงการตรวจสอบความสอดคล้องกับมาตรฐาน เพื่อยืนยันว่าการตั้งค่าในระบบจริงยังคงเป็นไปตามมาตรฐานที่กำหนดไว้	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.2.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 8

NIST CSF 2.0	ID.RA-07, ID.RA-09, PR.PS-01
ISO/IEC27001:2022	Annex A 8.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (5)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ผู้ดูแลระบบมีการใช้รายการตรวจสอบ (Checklist) เพื่อทวนสอบการตั้งค่าตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ให้ครบถ้วนก่อนเริ่มใช้งานหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงานหรือไม่ และมีใครเป็นผู้สอบทานความถูกต้อง 2. ในกรณีที่ระบบงานบางประเภทมีข้อจำกัดทางเทคนิคจนไม่สามารถตั้งค่าตามมาตรฐานได้ หน่วยงานมีกระบวนการขอยกเว้น (Exception Process) อย่างไร และมีมาตรการชดเชย (Compensating Controls) เพื่อลดความเสี่ยงในส่วนนั้นอย่างไร ■ การสอบทานเอกสาร 1. สอบทานรายการตรวจสอบ (Checklist) ที่ผ่านการบันทึกแล้ว เพื่อยืนยันว่ามีการตั้งค่าตามมาตรฐานจริงก่อนการใช้งาน โดยอย่างน้อยต้องประกอบด้วย (ก) สิทธิ์พิเศษน้อยที่สุด (ข) การแบ่งแยกหน้าที่ (ค) ความซับซ้อนของรหัสผ่าน (ง) การลบบัญชีที่ไม่ได้ใช้ (จ) การลบบริการที่ไม่จำเป็น (ฉ) การปิดพอร์ตที่ไม่ใช้ (ช) การป้องกันมัลแวร์ และ (ซ) การปรับปรุงซอฟต์แวร์และแพตช์ 2. สอบทานรายงานการทดสอบหรือผลสแกนช่องโหว่ก่อนอนุญาตให้เชื่อมต่อบริษัท 3. สอบทานทะเบียนบันทึกการขอยกเว้น (Security Exception Log) ที่มีการกำหนดระยะเวลาสิ้นสุด และเจ้าของความเสี่ยง ■ เอกสารที่เกี่ยวข้อง 1. รายการตรวจสอบการกำหนดค่าความมั่นคงปลอดภัย (Security Configuration Checklist) 2. รายงานการทดสอบหรือผลสแกนช่องโหว่ 3. ทะเบียนบันทึกการขอยกเว้น (Security Exception Log) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบการตั้งค่าระบบจริง เทียบกับรายการตรวจสอบ (Checklist) ที่ผ่านการบันทึกแล้ว	

- ตรวจสอบรายชื่อกลุ่มผู้ใช้ที่มีสิทธิ์สูงในระบบจริง (เช่น Administrators, sudoers, dba) ว่ามีเฉพาะบุคคลที่จำเป็นต้องใช้งานหรือไม่ - ใช้คำสั่งตรวจสอบการตั้งค่านโยบายรหัสผ่านเพื่อยืนยันค่า เช่น Minimum Length, Complexity และ History - ตรวจสอบว่าบัญชีเริ่มต้น (เช่น guest, admin, test) ถูกปิดใช้งานหรือเปลี่ยนชื่อไปแล้ว และไม่มีบัญชีที่ไม่ได้ใช้งานนานเกินระยะเวลาที่กำหนด (เช่น 90 วัน) คงเหลืออยู่ - ใช้เครื่องมือ (เช่น Nmap) เพื่อตรวจสอบว่ามี Service หรือ Port แปลกปลอมที่ไม่ได้ระบุไว้ในมาตรฐานเปิดทิ้งไว้หรือไม่ - ตรวจสอบรายชื่อโปรแกรมที่ติดตั้งในเครื่องว่าไม่มีโปรแกรมหรือซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการทำงานของบริการสำคัญ - ตรวจสอบจากหน้าจอ Dashboard หรือคำสั่งว่ามีโปรแกรมป้องกันมัลแวร์มีการทำงานอยู่ (Running) และมีฐานข้อมูลไวรัสที่เป็นปัจจุบัน (Up-to-date Definition) - สุ่มตรวจสอบรายการปรับปรุงซอฟต์แวร์และแพตช์ล่าสุด เพื่อยืนยันว่ามีการลง Security Patch ล่าสุดตามรอบที่นโยบายกำหนด
--

3.1.41 การทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยรายปี (Annual Review of Security Baseline Configuration Standards)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีการปรับปรุงให้เท่าทันกับเทคนิคการโจมตีและเทคโนโลยีที่เปลี่ยนแปลงไปอย่างสม่ำเสมอ	
ความเสี่ยง	
มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยไม่ทันสมัย ส่งผลให้ไม่สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ได้	
การควบคุมที่พึงมี	
ต้องทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์	
แนวทางการประเมิน	
- ตรวจสอบรอบระยะเวลาการทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) - ตรวจสอบว่ามีการปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) อย่างน้อยปีละ 1 ครั้ง - ตรวจสอบว่ามีการทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) เมื่อมีภัยคุกคามทางไซเบอร์แบบใหม่	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.2.4

แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 8
NIST CSF 2.0	ID.IM-01, PR.PS-01
ISO/IEC27001:2022	Annex A 8.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีเกณฑ์การกำหนดรอบระยะเวลาในการทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ไว้อย่างไร 2. เมื่อตรวจพบภัยคุกคามรูปแบบใหม่ หรือช่องโหว่ระดับร้ายแรง หน่วยงานมีกระบวนการพิจารณาปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) เป็นกรณีพิเศษก่อนรอบการทบทวนประจำปีอย่างไร ■ การสอบทานเอกสาร 1. สอบทานประวัติการแก้ไขเอกสาร (Revision History / Version Control) ของมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือสอดคล้องกับภัยคุกคามทางไซเบอร์แบบใหม่ที่เกิดขึ้น 2. สอบทานบันทึกการประชุมหรือผลการทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ประจำปี ■ เอกสารที่เกี่ยวข้อง 1. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) 2. รายงานการประชุมหรือบันทึกข้อความอนุมัติ ผลการทบทวน/ปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ประจำปี ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

3.1.42 กระบวนการจัดการการเปลี่ยนแปลง (Change Management Process)

วัตถุประสงค์

เพื่อให้มั่นใจว่า การปรับปรุง แก้ไข หรือเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับระบบสารสนเทศที่สนับสนุนบริการสำคัญ จะถูกดำเนินการอย่างเป็นระบบ มีการควบคุมและตรวจสอบอย่างรอบคอบ

ความเสี่ยง

ระบบสารสนเทศที่สนับสนุนบริการสำคัญอาจทำงานผิดพลาดหรือหยุดชะงักเมื่อมีการปรับปรุง แก้ไข หรือเปลี่ยนแปลงใด ๆ

การควบคุมที่พึงมี

ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

แนวทางการประเมิน

1. ตรวจสอบกระบวนการจัดการการเปลี่ยนแปลง (Change Management Process) ว่าครอบคลุมการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
2. ตรวจสอบการเปลี่ยนแปลงระบบที่มีต่อบริการที่สำคัญ ว่าถูกต้องและเป็นไปตามขั้นตอนที่กำหนดไว้

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.2.5
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 8
NIST CSF 2.0	ID.RA-07
ISO/IEC27001:2022	Annex A 8.32
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.1.2, 14.2.2, 14.2.3, 14.2.4
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (6) (ข)

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. เมื่อมีความจำเป็นต้องเปลี่ยนแปลงระบบที่กระทบบริการสำคัญ (CII) หน่วยงานมีขั้นตอนการขออนุมัติ (Change Request) อย่างไร และมีกระบวนการวิเคราะห์ความเสี่ยงและผลกระทบอย่างไร
2. ในกรณีเกิดเหตุการณ์ฉุกเฉินที่ต้องแก้ไขระบบทันที (Emergency Change) มีขั้นตอนปฏิบัติที่แตกต่างจากกรณีปกติอย่างไร และมีการอนุมัติย้อนหลังอย่างไรเพื่อให้ยังคงมีการควบคุมที่เหมาะสม

■ การสอบทานเอกสาร

1. สอบทานนโยบายและขั้นตอนการจัดการการเปลี่ยนแปลง (Change Management Policy and Procedure) ว่ามีที่ระบุขั้นตอนขออนุมัติและบทบาทหน้าที่ชัดเจน
2. สอบทานแบบฟอร์มคำขออนุมัติเปลี่ยนแปลง (Change Request) ที่ระบุรายละเอียดของแผนการเปลี่ยนแปลง การวิเคราะห์ผลกระทบ ผลการอนุมัติ แผนการย้อนกลับ (Roll-back Plan) และ บันทึกผลการทดสอบ (UAT/Testing Report) ก่อนการนำขึ้นใช้งานจริง

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการจัดการการเปลี่ยนแปลง (Change Management Policy and Procedure) 2. ใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) 3. บันทึกผลการทดสอบ (UAT/Testing Report) 4. บันทึกการประชุม Change Advisory Board (CAB) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค
--

การเชื่อมต่อระยะไกล (Remote Connection)	
3.1.43 การรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล (Security of Remote Connection)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่าการเชื่อมต่อระยะไกลเข้าสู่ระบบหรือบริการที่สำคัญของหน่วยงาน มีมาตรการควบคุมที่เข้มงวดและมีประสิทธิภาพเพียงพอในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และสามารถตรวจพบความพยายามในการบุกรุกได้อย่างทันท่วงที	
ความเสี่ยง	
ผู้ไม่ประสงค์ดีมีโอกาสดำเนินการเข้าถึงระบบหรือบริการที่สำคัญผ่านการเชื่อมต่อระยะไกลได้	
การควบคุมที่พึงมี	
ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	
แนวทางการประเมิน	
1. ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกลว่าครอบคลุมป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต 2. ตรวจสอบเครื่องมือหรือระบบเฝ้าระวังที่ใช้สำหรับตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาตผ่านการเชื่อมต่อระยะไกล (Remote Connection)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.3.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 9
NIST CSF 2.0	PR.IR-01
ISO/IEC27001:2022	Annex A 5.14, Annex A 6.7
ISO/IEC27701:2025	A.3.7
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.2.2, 13.2.1, 13.2.2, 13.2.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์	

1. หน่วยงานมีการออกแบบสถาปัตยกรรมในการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกลหรือไม่ อย่างไร
2. หน่วยงานมีนโยบายและขั้นตอนในการควบคุมการเข้าถึงจากระยะไกลอย่างไร
3. หน่วยงานมีเกณฑ์การตัดสินใจอย่างไรว่ากิจกรรมใดคือความผิดปกติ (Anomaly) เช่น การ Login นอกเวลาทำการ หรือจากพิกัดที่ไม่เคยพบ (Geolocation) และมีขั้นตอนการระงับสิทธิ์ชั่วคราวทันทีอย่างไรเมื่อพบเหตุต้องสงสัย

■ การสอบทานเอกสาร

1. สอบทานแผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) เพื่อยืนยันสถาปัตยกรรมในการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกล
2. สอบทานนโยบายและขั้นตอนควบคุมการเชื่อมต่อระยะไกล (Remote Access Policy and Procedure) เพื่อดูว่ามีการจำกัดสิทธิ์การเชื่อมต่อเฉพาะบุคคลที่จำเป็น และมีการระบุเงื่อนไขความปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security)
3. สอบทานบันทึกการเฝ้าระวัง (Monitoring Logs) และตัวอย่างการแจ้งเตือน (Alerts) เพื่อยืนยันว่าระบบมีการตรวจจับและรายงานเหตุการณ์ที่ผิดปกติได้จริงตามที่กำหนดไว้ในนโยบาย

■ เอกสารที่เกี่ยวข้อง

1. แผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram)
2. นโยบายและขั้นตอนการเชื่อมต่อระยะไกล (Remote Access Policy and Procedure)
3. รายงานการเฝ้าระวังความปลอดภัยและ Log การเชื่อมต่อ VPN/Remote Access

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบการตั้งค่าบนอุปกรณ์ที่ควบคุมการเชื่อมต่อระยะไกล ว่ามีการตั้งค่าไว้สอดคล้องกับที่ออกแบบ เช่น การจำกัดการเข้าถึงจากการเชื่อมต่อระยะไกล ให้เข้าถึงได้เฉพาะบุคคลที่จำเป็น
2. ตรวจสอบการตั้งค่าบนอุปกรณ์ที่ควบคุมการเชื่อมต่อระยะไกล ว่ามีการตั้งค่าเกี่ยวกับการรายงานเหตุการณ์ที่ผิดปกติ

3.1.44 แนวทางปฏิบัติเฉพาะสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ (Specific Practices for Remote Connection to Critical Services)

วัตถุประสงค์

เพื่อให้มั่นใจว่า มีการเชื่อมต่อระยะไกลเฉพาะที่จำเป็นและได้รับอนุญาตเท่านั้น และผ่านการพิสูจน์ตัวตนที่ปลอดภัย

ความเสี่ยง

ผู้ไม่ประสงค์ดีมีโอกาสดำเนินการเข้าถึงระบบหรือบริการที่สำคัญผ่านการเชื่อมต่อระยะไกลได้

การควบคุมที่พึงมี

สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไคลเอนต์ระยะไกล เมื่อจำเป็นเท่านั้น

- (ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัย ในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
- (ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
- (ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการทำงานของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ
- (จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

แนวทางการประเมิน

1. ตรวจสอบแนวทางปฏิบัติสำหรับการเชื่อมต่อระยะไกล เพื่อให้แน่ใจว่า ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (จ)
2. ตรวจสอบการตั้งค่าการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ได้แก่ การพิสูจน์ตัวตนที่แข็งแกร่ง (เช่น MFA) มาตรการเข้ารหัส (เช่น HTTPS, SSH)
3. ตรวจสอบการตั้งค่าเพื่อจำกัดการใช้คำสั่งระบบ (Issuing System Commands) และการจำกัดการไหลของข้อมูลของบริการที่สำคัญ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.3.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 9
NIST CSF 2.0	PR.AA-03, PR.AA-04, PR.AA-05, PR.IR-01
ISO/IEC27001:2022	Annex A 5.14, Annex A 6.7, Annex A 8.5, Annex A 8.21, Annex A 8.24
ISO/IEC27701:2025	A.3.7, A.3.23, A.3.26
ISO/IEC27017:2015	10.1.1, 10.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.2.2, 10.1.1, 10.1.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีขั้นตอนในการขออนุญาตเชื่อมต่อระยะไกลอย่างไร
2. หน่วยงานมีการใช้เทคนิคการพิสูจน์ตัวตนอย่างไรสำหรับการเชื่อมต่อระยะไกล (เช่น Multi-Factor Authentication: MFA)
3. หน่วยงานมีกระบวนการจำกัดและอนุมัติการใช้ System Commands ผ่านการ Remote อย่างไร เพื่อป้องกันผลกระทบต่อระบบสำคัญ (เช่น การใช้ Jump Host หรือระบบ Privileged Access Management : PAM)

■ การสอบทานเอกสาร

1. สอบทานแนวทางปฏิบัติเฉพาะสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ (Specific Practices for Remote Connection to Critical Services Guideline) ว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (จ)
2. สอบทานใบคำขอเชื่อมต่อระยะไกล เพื่อดูการระบุเหตุผลความจำเป็นและระยะเวลาสิ้นสุดของสิทธิ์
3. สอบทานบันทึกการทบทวนสิทธิ์การเชื่อมต่อระยะไกล ว่าได้มีการทบทวนสิทธิ์ตามรอบที่กำหนด และได้มีการระงับสิทธิ์ทันทีที่พนักงานลาออกหรือเปลี่ยนหน้าที่
4. สอบทานแผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) ที่แสดงตำแหน่งโซนเครือข่าย และจุดติดตั้งระบบรักษาความความมั่นคงปลอดภัย (เช่น VPN Gateway, Firewall) ที่ใช้ในการจำกัดการไหลของข้อมูล

■ เอกสารที่เกี่ยวข้อง

1. แนวทางปฏิบัติเฉพาะสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ (Specific Practices for Remote Connection to Critical Services Guideline)
2. ทะเบียนรายชื่อและสิทธิ์ผู้ใช้งานการเชื่อมต่อระยะไกล
3. ใบคำขอเชื่อมต่อระยะไกล
4. บันทึกการทบทวนสิทธิ์การเชื่อมต่อระยะไกล
5. บันทึกการเข้าถึงผ่านระบบ Jump Host หรือระบบ PAM
6. แผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ดึงรายชื่อบัญชี (User IDs) ทั้งหมดที่มีสิทธิ์เข้าใช้งานผ่าน VPN Gateway หรือระบบ Remote เทียบกับใบคำขอที่ได้รับการอนุมัติว่า สิทธิ์ที่เปิดไว้นั้นมีการขออนุมัติครบถ้วน และมีกำหนดระยะเวลาสิ้นสุดการขอใช้งาน
2. ตรวจสอบไฟล์บันทึกการทำงาน (Log) ของระบบเครือข่าย ว่ามีการบันทึกประวัติการยืนยันตัวตนสอดคล้องกับใบคำขอเชื่อมต่อระยะไกล
3. ตรวจสอบการเชื่อมต่อระยะไกลว่ามีการใช้โปรโตคอลที่ปลอดภัย (เช่น TLS 1.2+, SSH v2) และ Algorithms การเข้ารหัสที่แข็งแกร่ง (เช่น AES-256 ขึ้นไป) ไม่ใช่ SHA-1 หรือ MD5
4. ตรวจสอบการตั้งค่าบน Firewall ว่าอนุญาตเฉพาะ IP/Port ที่จำเป็นตามฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ
5. ตรวจสอบการตั้งค่าระยะเวลาการตัดการเชื่อมต่ออัตโนมัติ (Session Timeout) เมื่อไม่มีการใช้งาน เพื่อป้องกันการสวมสิทธิ์จากเซสชันที่ค้างไว้

สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

3.1.45 การควบคุมสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (Control of Removable Storage Media and Portable Computing Devices)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีมาตรการควบคุมการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์พกพาอย่างเข้มงวด

ความเสี่ยง	
มัลแวร์กระจายเข้าสู่บริการที่สำคัญผ่านการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์พกพา	
การควบคุมที่พึงมี	
ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยใช้มาตรการอย่างน้อย ดังนี้ (ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น (ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๒๒.๑.๑ (ข) ของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 เท่านั้น และ (ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	
แนวทางการประเมิน	
1. ตรวจสอบมาตรการควบคุมทางกายภาพและการป้องกันเชิงเทคนิคสำหรับการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ เพื่อให้แน่ใจว่า ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ค)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.4.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 10
NIST CSF 2.0	PR.IR-01
ISO/IEC27001:2022	Annex A 7.10, Annex A 7.14, Annex A 8.1
ISO/IEC27701:2025	A.3.20, A.3.21, A.3.22
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.2.1, 8.3.1, 8.3.2, 8.3.3, 11.2.5, 11.2.7, 11.2.8
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (1), ข้อ 4 (5)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - หากพนักงานมีความจำเป็นต้องใช้แฟลชไดรฟ์ (USB) มีขั้นตอนการขออนุญาตเปิดพอร์ตอย่างไร - หน่วยงานมีเกณฑ์การเลือกใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตอย่างไร เช่น ต้องเป็นของหน่วยงานจัดหาให้เท่านั้น หรือต้องมีการลงทะเบียนอุปกรณ์ก่อนหรือไม่ - ระบบมีกลไกบังคับการตรวจสอบมัลแวร์อัตโนมัติทันทีที่เชื่อมต่อสื่อบันทึกข้อมูลหรือไม่ ■ การสอบถามเอกสาร - สอบถามนโยบายการกำกับดูแลสื่อบันทึกข้อมูลและอุปกรณ์พกพาว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ค) และมีการระบุข้อห้ามและบทลงโทษ	

2. สอบทานบันทึกการขออนุญาตใช้งานพอร์ต USB ว่ามีการระบุข้อ เหตุผล และระยะเวลาที่ใช้ งาน 3. สอบทานทะเบียนคุมสื่อบันทึกข้อมูลและอุปกรณ์พกพา (เช่น รายการ USB Flash Drive ที่ ได้รับอนุญาต) ว่ามีสถานะเป็นปัจจุบัน ■ เอกสารที่เกี่ยวข้อง 1. นโยบายการกำกับดูแลสื่อบันทึกข้อมูลและอุปกรณ์พกพา (Removable Storage Media and Portable Computing Devices) 2. แบบฟอร์มขออนุญาตใช้งานสื่อบันทึกข้อมูลและอุปกรณ์พกพา 3. ทะเบียนคุมสื่อบันทึกข้อมูลและอุปกรณ์พกพา ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบเครื่องคอมพิวเตอร์ในโซนบริการสำคัญ เพื่อยืนยันว่าพอร์ต USB ถูกปิดกั้นในระดับ OS หรือใช้ระบบ DLP (Data Loss Prevention) ในการควบคุม 2. ตรวจสอบ Log จากโปรแกรม Antivirus หรือระบบ Endpoint Security เพื่อยืนยันว่ามีการ ตรวจจับมัลแวร์บนอุปกรณ์พกพาโดยอัตโนมัติเมื่อมีการเชื่อมต่อ
--

3.1.46 การเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้ (Encryption of Data on Removable Storage Media)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า ข้อมูลที่มีความละเอียดอ่อนหรือข้อมูลสำคัญของบริการที่สำคัญ จะได้รับการคุ้มครองด้วย เทคโนโลยีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูงเมื่อมีการจัดเก็บในสื่อบันทึกข้อมูลแบบถอดได้	
ความเสี่ยง	
ข้อมูลที่มีความละเอียดอ่อนหรือข้อมูลสำคัญของบริการที่สำคัญรั่วไหล	
การควบคุมที่พึงมี	
ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศบนสื่อบันทึกข้อมูลแบบถอดได้	
แนวทางการประเมิน	
1. ตรวจสอบว่ามีมาตรการการป้องกันข้อมูลที่ละเอียดอ่อน (Sensitive Data) ของบริการที่ สำคัญ 2. ตรวจสอบว่ามีการบังคับใช้การเข้ารหัสข้อมูล (Encryption) ทุกครั้งที่มีการคัดลอกหรือจัดเก็บ ข้อมูลลงบนสื่อบันทึกข้อมูลแบบถอดได้ ตามนโยบายที่กำหนด	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.4.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 10
NIST CSF 2.0	PR.DS-01
ISO/IEC27001:2022	Annex A 7.9, Annex A 7.10, Annex A 8.7, Annex A 8.12, Annex A 8.24
ISO/IEC27701:2025	A.3.20, A.3.26

ISO/IEC27017:2015	10.1.1, 10.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.3.1, 8.3.2, 8.3.3, 10.1.1, 10.1.2, 11.2.5, 11.2.6, 12.2.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (1)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีการบังคับใช้เทคโนโลยีหรือซอฟต์แวร์ใดเพื่อทำการเข้ารหัสบนสื่อบันทึกข้อมูลแบบถอดได้หรือไม่ (เช่น BitLocker To Go, DLP Endpoint) ■ การสอบถามเอกสาร 1. สอบทานนโยบาย/แนวปฏิบัติ/คู่มือในการเข้ารหัสข้อมูล (Encryption) เพื่อยืนยันว่ามีการระบุมาตรฐาน Algorithm (เช่น AES-256) และขั้นตอนการเข้ารหัสก่อนคัดลอกข้อมูลออกจากระบบ 2. สอบทานบันทึกการขออนุญาตนำข้อมูลออกนอกหน่วยงาน เพื่อตรวจสอบว่ามีการระบุความจำเป็น ระดับความลับของข้อมูล และการยืนยันว่าข้อมูลนั้นได้รับการเข้ารหัสแล้ว ■ เอกสารที่เกี่ยวข้อง 1. นโยบาย/แนวปฏิบัติ/คู่มือในการเข้ารหัสข้อมูล (Encryption) 2. บันทึกการขออนุญาตนำข้อมูลออกนอกหน่วยงาน 3. ทะเบียนคุมการรับ-ส่งสื่อบันทึกข้อมูลที่ละเอียดอ่อนออกนอกหน่วยงาน ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบการเข้ารหัสบนสื่อบันทึกข้อมูลแบบถอดได้ (Removable media) ว่ามีการเข้ารหัสข้อมูลด้วยวิธีการที่แข็งแกร่งและความยาวของกุญแจเข้ารหัสที่ปลอดภัยตามนโยบายที่กำหนด 2. ตรวจสอบให้แน่ใจว่ากุญแจ (Keys) ที่ใช้สำหรับการเข้ารหัสและถอดรหัสข้อมูลทั้งหมด ถูกจัดเก็บในที่ปลอดภัย (เช่น HSM หรือ Secure Vault) และมีการจำกัดสิทธิ์เข้าถึงอย่างเข้มงวด	

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
3.1.47 การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการจัดทำและดำเนินแผนงานสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ครอบคลุมบุคลากรทุกกลุ่มที่เกี่ยวข้องอย่างเหมาะสม
ความเสี่ยง
บุคลากรขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมและทันต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นใหม่ ส่งผลให้ข้อมูลหรือระบบสำคัญมีความเสี่ยง
การควบคุมที่พึงมี

หน่วยงานต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สาม ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- พนักงานใหม่ (New Employees)
- ผู้ใช้และระดับบริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS และ
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ

(ง) การสื่อสารอย่างสม่ำเสมอและทันทั่วถึง ครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

แนวทางการประเมิน

1. ตรวจสอบแผนงานการสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ว่าครอบคลุมบุคลากรทุกประเภท (พนักงานใหม่, ระดับบริหาร, ฝ่าย IT/ICS, ผู้รับเหมา และผู้ให้บริการภายนอก)
2. ตรวจสอบเนื้อหาการอบรมที่มีการเผยแพร่ความรับผิดชอบของกลุ่มหรือบุคคลอย่างชัดเจน
3. ตรวจสอบเนื้อหาการอบรมว่าครอบคลุมกฎหมาย กฎ ระเบียบ นโยบาย และมาตรฐานที่เกี่ยวข้องกับการใช้งานและเข้าถึงบริการสำคัญ (CII)
4. ตรวจสอบการสื่อสารข้อมูลภัยคุกคาม ผลกระทบ และการบรรเทาผลกระทบ ว่ามีความสม่ำเสมอและทันทั่วถึง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.5.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	ข้อ 5 ของประกาศ
NIST CSF 2.0	GV.RR-02, GV.RR-04, PR.AT-01, PR.AT-02, RC.RP-04
ISO/IEC27001:2022	Clause 7.3, Annex A 5.10, Annex A 5.34, Annex A 6.2, Annex A 6.3, Annex A 6.4, Annex A 6.6
ISO/IEC27701:2025	Clause 7.3, A.3.17, A.3.18
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.4.3

ISO/IEC TS 27008:2019	7.1.2, 7.2.2, 7.2.3, 8.1.3, 8.2.3, 13.2.4, 18.1.4
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (6) (ค), 4 (7)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีกระบวนการชี้แจงและให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่พนักงานใหม่ และพนักงานปัจจุบันอย่างไร ครอบคลุมถึงผู้บริหาร ผู้ให้บริการ IT และ ICS และผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers) หรือไม่ 2. หน่วยงานมีการประเมินความรู้ความเข้าใจของบุคลากรหลังจากการอบรมหรือการสื่อสาร เนื้อหาหรือไม่ อย่างไร ■ การสอบทานเอกสาร 1. สอบทานแผนงานการสร้างความรู้ด้านความมั่นคงปลอดภัย (Security Awareness Plan) และหลักสูตรการอบรมประจำปี ว่าครอบคลุมกิจกรรมให้ความรู้แก่บุคลากรทุกประเภท การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคล การตระหนักรู้กฎหมายความมั่นคงปลอดภัย ไซเบอร์ รวมถึงข้อมูลภัยคุกคาม ผลกระทบ และการบรรเทาผลกระทบ 2. สอบทานช่องทางการสื่อสาร (เช่น อีเมลแจ้งเตือน, Intranet) ว่ามีความสม่ำเสมอ 3. สอบทานสัญญาจ้างผู้ให้บริการภายนอก ว่ามีการระบุข้อกำหนดให้ต้องผ่านการอบรมการสร้าง ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ก่อนเข้าปฏิบัติงานจริง ■ เอกสารที่เกี่ยวข้อง 1. แผนงานการสร้างความรู้ด้านความมั่นคงปลอดภัย (Security Awareness Plan) 2. เอกสารประกอบการฝึกอบรมการสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 3. หลักฐานการสื่อสารข้อมูลภัยคุกคาม (เช่น อีเมลเวียน, โปสเตอร์, บันทึกรายการประชุม) 4. รายชื่อและผลประเมินผู้เข้ารับการอบรม 5. สัญญาว่าจ้างผู้ให้บริการภายนอก ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	

3.1.48 การทบทวนแผนงานในการสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Review of Cybersecurity Awareness Program)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการติดตามและปรับปรุงแผนงานสร้างความรู้อย่างต่อเนื่อง สม่ำเสมอ และทันต่อสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงไป
ความเสี่ยง
บุคลากรขาดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมและทันต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นใหม่ ส่งผลให้ข้อมูลหรือระบบสำคัญมีความเสี่ยง
การควบคุมที่พึงมี
ต้องทบทวนแผนงานในการสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องอย่างเหมาะสม

แนวทางการประเมิน	
- ตรวจสอบรอบการทบทวนแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง - ตรวจสอบเนื้อหาในแผนงานฉบับปรับปรุง ว่ามีความทันสมัย ครอบคลุมรายละเอียดที่เกี่ยวข้องกับสถานการณ์ปัจจุบัน (เช่น ภัยคุกคามใหม่ หรือเทคโนโลยีที่เปลี่ยนไป)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.5.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	ข้อ 5 ของประกาศ
NIST CSF 2.0	ID.IM-01
ISO/IEC27001:2022	Clause 7.3, Annex A 6.3
ISO/IEC27701:2025	Clause 7.3, Annex A 3.17
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.4.3
ISO/IEC TS 27008:2019	7.2.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - ใครคือผู้รับผิดชอบหลักในการทบทวนและปรับปรุงเนื้อหาแผนงานการสร้างความตระหนักรู้ - หน่วยงานนำผลประเมินการอบรม หรือเหตุการณ์ภัยคุกคามใหม่ ๆ มาเป็นข้อมูลนำเข้า (Input) ในการปรับปรุงเนื้อหาแผนงานในแต่ละปีอย่างไร ■ การสอบถามเอกสาร - สอบถามประวัติการแก้ไขเอกสาร (Version Control/Document History) ในแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness Plan) เพื่อยืนยันว่าการทบทวนอย่างน้อยปีละ 1 ครั้งตามรอบเวลาที่กำหนด - สอบถามแผนงานการสร้างความตระหนักรู้ เพื่อให้แน่ใจว่า เนื้อหาของแผนงานยังคงเป็นปัจจุบัน ■ เอกสารที่เกี่ยวข้อง - แผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness Plan) - รายงานการประชุมเพื่อพิจารณาทบทวนแผนงาน - บันทึกการอนุมัติแผนงานจากผู้บริหาร ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	

การแบ่งปันข้อมูล (Information Sharing)

3.1.49 การแบ่งปันข้อมูล (Information Sharing)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการและขั้นตอนที่ชัดเจนในการแจ้งเตือนและแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามหรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ไปยังผู้มีส่วนได้ส่วนเสียหรือผู้ที่อาจได้รับผลกระทบ

ความเสี่ยง

ผู้มีส่วนได้ส่วนเสียหรือผู้ที่อาจได้รับผลกระทบไม่สามารถใช้มาตรการป้องกันภัยคุกคามได้อย่างเหมาะสม

การควบคุมที่พึงมี

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ผู้ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. ประกาศกำหนด

แนวทางการประเมิน

1. ตรวจสอบว่ามีการกำหนดขั้นตอนสำหรับการแบ่งปันข้อมูล (Information Sharing) เกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์
2. ตรวจสอบว่าขั้นตอนครอบคลุมการแจ้งข้อมูลให้แก่บุคคล/หน่วยงานที่ได้รับผลกระทบ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ)
3. ตรวจสอบว่าแนวทางและรูปแบบการแบ่งปันข้อมูลเป็นไปตามหลักเกณฑ์ที่ สกมช. ประกาศกำหนด (เช่น การใช้ระดับชั้นความลับ TLP - Traffic Light Protocol)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 22.6
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 11
NIST CSF 2.0	ID.RA-02, RS.CO-02, RS.CO-03
ISO/IEC27001:2022	Annex A 5.5, Annex A 5.6, Annex A 5.7, Annex A 5.26
ISO/IEC27701:2025	A.3.12
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.3, 6.1.4, 16.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. การแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์มีขั้นตอนอย่างไร
2. เมื่อเกิดเหตุการณ์ภัยคุกคาม หน่วยงานมีเกณฑ์การตัดสินใจอย่างไรว่าต้องแบ่งปันข้อมูลใดให้แก่ผู้ให้บริการภายนอก หรือผู้ให้บริการทราบ
3. ใครเป็นผู้มีอำนาจอนุมัติในการส่งข้อมูลภัยคุกคามออกสู่ภายนอก
4. เมื่อมีการแจ้งเตือนภัยคุกคามไปยังหน่วยงานภายนอก หน่วยงานมีการบันทึกรายละเอียดใดบ้าง (เช่น วันเวลา, ผู้รับ, ระดับ TLP)
5. หน่วยงานมีมาตรการอย่างไรในการกำกับดูแลให้บุคคลภายนอกปฏิบัติตาม NDA อย่างเคร่งครัดหลังจากได้รับข้อมูลภัยคุกคามไปแล้ว และมีการทบทวนรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูลความลับเหล่านี้หรือไม่
6. บุคลากรมีความเข้าใจในการติดป้ายกำกับระดับความลับของข้อมูล (เช่น TLP: RED, TLP: AMBER) ก่อนการแบ่งปันอย่างไร

■ การสอบถามเอกสาร

1. สอบถามขั้นตอนการแบ่งปันข้อมูล (Information Sharing Procedure) ว่ามีการระบุรายละเอียดของข้อมูลที่จะมีการแบ่งปัน มาตรฐานการกำกับความลับ (เช่น TLP) และช่องทางการสื่อสารที่ปลอดภัย (Secure Channels)
2. สอบถามหลักฐานการสื่อสารแจ้งเตือนเหตุการณ์จริงไปยังกลุ่มผู้ที่เกี่ยวข้อง เพื่อดูว่ามีการแบ่งปันข้อมูลอย่างน้อยดังนี้
 - เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์
 - มาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว
 - ผู้ได้รับผลกระทบจากเหตุการณ์
3. สอบถามเอกสารข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) ว่ามีการระบุขอบเขตของข้อมูลภัยคุกคามทางไซเบอร์ไว้ครอบคลุมหรือไม่ และวันหมดอายุของสัญญายังคงมีผลบังคับใช้อยู่
4. สอบถามบัญชีรายชื่อผู้ติดต่อ (Contact List) ความถูกต้องและเป็นปัจจุบันของข้อมูลติดต่อของบุคคล/หน่วยงานภายนอกที่ได้รับผลกระทบ

■ เอกสารที่เกี่ยวข้อง

1. ขั้นตอนการแบ่งปันข้อมูล (Information Sharing Procedure)
2. หลักฐานบันทึกการแบ่งปันข้อมูล (Information Sharing Logs)
3. ข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA) กับบุคคลภายนอก
4. บัญชีรายชื่อผู้ติดต่อ (Contact List) ของบุคคล/หน่วยงานภายนอกที่ได้รับผลกระทบ

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	
การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
3.1.50 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีกลไกและกระบวนการที่สามารถตรวจจับเหตุการณ์ผิดปกติ วิเคราะห์ผลกระทบ และระบุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการสำคัญได้อย่างถูกต้องและทันทั่วทั้ง	
ความเสี่ยง	
ไม่สามารถตรวจจับและวิเคราะห์เหตุการณ์ผิดปกติ และระบุภัยคุกคามทางไซเบอร์ได้	
การควบคุมที่พึงมี	
ต้องสร้างกลไกและกระบวนการเพื่อ (ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับ บริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และ (ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่	
แนวทางการประเมิน	
- ตรวจสอบว่ามีกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ครอบคลุมการควบคุมที่พึงมี ข้อ (ก) - (ค) - ตรวจสอบว่ามีกลไกเชิงเทคนิคในการเฝ้าระวังภัยคุกคามทางไซเบอร์ ครอบคลุมการควบคุมที่พึงมี ข้อ (ก) - (ค)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 23.1.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 12
NIST CSF 2.0	DE.CM-01, DE.CM-02, DE.CM-06, DE.CM-09
ISO/IEC27001:2022	Annex A 5.7, Annex A 5.24, Annex A 5.25, Annex A 7.4, Annex A 8.15, Annex A 8.16
ISO/IEC27701:2025	A.3.11, A.3.25
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.4.1, 12.4.2, 12.4.3, 16.1.1, 16.1.4
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)
ขั้นตอนการตรวจสอบ	
การสัมภาษณ์	

1. หน่วยงานใช้เครื่องมือหรือระบบใด (เช่น SIEM, IDS/IPS, EDR) ในการรวบรวม Log และเฝ้าระวังภัยคุกคาม และครอบคลุมบริการที่สำคัญ (CII) หรือไม่
2. เมื่อระบบตรวจพบเหตุการณ์ผิดปกติ หน่วยงานมีเกณฑ์การตัดสินใจอย่างไรในการจัดประเภทของภัยคุกคาม
3. เมื่อระบบมีการแจ้งเตือน (Alert) ทีมงานมีขั้นตอนในการวิเคราะห์และคัดแยก (Triage) เหตุการณ์เบื้องต้นอย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายและขั้นตอนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ว่าครอบคลุมการควบคุมที่พึงมี ข้อ (ก) - (ค) ได้แก่ ขั้นตอนการตรวจจับเหตุการณ์ การจัดประเภท การวิเคราะห์ และการคัดกรองเหตุการณ์ และการระบุภัยคุกคาม
2. สอบทานตารางการจัดระดับความรุนแรงของเหตุการณ์ ว่าสอดคล้องกับประกาศของ สกมช. หรือไม่ (ไม่ร้ายแรง ร้ายแรง วิกฤต)
3. สอบทานรายงานเหตุการณ์ผิดปกติ (Incident Report) เพื่อดูว่าเหตุการณ์ที่ผ่านมาได้รับการจัดการที่ถูกต้องตามขั้นตอนที่กำหนด

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
2. รายงานเหตุการณ์ผิดปกติ (Incident Report)
3. แผนภาพสถาปัตยกรรมสำหรับเครื่องมือและระบบเฝ้าระวัง

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบไฟล์บันทึกประวัติการใช้งานย้อนหลัง (Log) โดยดูจากวันและเวลา (Timestamp) ในไฟล์ประวัติ เพื่อยืนยันว่าระบบสามารถเก็บข้อมูลย้อนหลังไว้ได้นานกว่าหรือเท่ากับระยะเวลาที่ตกลงไว้
2. ทดสอบว่าระบบได้ป้องกันไม่ให้ผู้ใช้งานที่มีสิทธิ์พิเศษ (แม้จะเข้าสู่ระบบอย่างถูกต้องแล้ว) สามารถเข้าไปลบหรือแก้ไข Log ได้

3.1.51 การทบทวนกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Review of Cyber Threat Detection and Monitoring Mechanisms and Processes)

วัตถุประสงค์

เพื่อให้มั่นใจว่า กลไกและกระบวนการที่ใช้ในการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ได้รับการตรวจสอบความถูกต้องและประเมินประสิทธิภาพอย่างสม่ำเสมอ

ความเสี่ยง

ไม่สามารถตรวจจับและวิเคราะห์เหตุการณ์ผิดปกติ และระบุภัยคุกคามทางไซเบอร์ได้อย่างถูกต้อง

การควบคุมที่พึงมี

ต้องดำเนินการทบทวนกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

แนวทางการประเมิน

1. ตรวจสอบประวัติการทบทวนกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคาม ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง
2. ตรวจสอบว่ามีการกำหนดเกณฑ์ในการประเมินประสิทธิภาพของกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคาม ผ่านตัวชี้วัด เช่น อัตราการตรวจจับเหตุการณ์ (Detection Rate) หรืออัตราการแจ้งเตือนที่ผิดพลาด (False Positive Rate) หรือระยะเวลาเฉลี่ยที่ใช้ในการตรวจพบเหตุการณ์ (Mean Time to Detect)
3. ตรวจสอบว่ามีการนำผลประเมินไปปรับปรุง (Tuning) ระบบให้มีประสิทธิภาพยิ่งขึ้น

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 23.1.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 12
NIST CSF 2.0	ID.IM-03
ISO/IEC27001:2022	Clause 9.1, Annex A 5.36
ISO/IEC27701:2025	Clause 9.1, A.3.16
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.5.3
ISO/IEC TS 27008:2019	18.2.2, 18.2.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 5

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีรอบการทบทวนกลไกและกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ประจำปีอย่างไร ใครเป็นผู้รับผิดชอบ และครอบคลุมประเด็นใดบ้าง
2. หน่วยงานมีเกณฑ์การประเมินประสิทธิภาพของระบบตรวจจับและเฝ้าระวังภัยคุกคาม (เช่น SIEM/IDS) อย่างไร และมีรอบความถี่ในการปรับปรุงกฎ (Rule Tuning) เพื่อลด False Positive หรือเพิ่มการตรวจจับภัยคุกคามใหม่ ๆ อย่างไร
3. หน่วยงานมีการนำผลจากการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาใช้เป็นข้อมูลเพื่อปรับปรุงระบบเฝ้าระวังให้ทันสมัยอยู่เสมออย่างไร

■ การสอบทานเอกสาร

1. สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของนโยบาย/ขั้นตอนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ เพื่อยืนยันว่ามีการทบทวนอย่างน้อยปีละ 1 ครั้งตามรอบเวลาที่กำหนด
2. สอบทานรายงานผลการทบทวนกลไกเชิงเทคนิคในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ เพื่อยืนยันว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้งตามรอบเวลาที่กำหนด
3. สอบทาน บันทึก/ตารางตัวชี้วัดประสิทธิภาพ (KPI Metrics) เพื่อตรวจสอบค่าเฉลี่ยด้านความเร็วและความแม่นยำ (เช่น MTTD, False Positive Rate) ว่าเป็นไปตามเกณฑ์ที่หน่วยงานตั้งไว้
4. สอบทานบันทึกหลักฐานการปรับปรุงกฎการตรวจจับ (Rule Tuning Logs) เพื่อดูความสอดคล้องระหว่างประวัติการปรับปรุงเทียบกับปัญหาที่พบในรายงานตัวชี้วัด

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
2. รายงานผลการทบทวนกลไกและกระบวนการเฝ้าระวังประจำปี
3. บันทึก/ตารางตัวชี้วัดประสิทธิภาพของระบบ (KPI Metrics)
4. บันทึกการปรับปรุงและปรับแต่งกฎการตรวจจับ (Rule Tuning Logs)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	
แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	
3.1.52 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีวงจรการบริหารจัดการแผนการรับมือภัยคุกคามทางไซเบอร์ที่ครบถ้วน ตั้งแต่ การจัดทำแผนที่สมบูรณ์ การสื่อสารให้ผู้เกี่ยวข้องทราบ การฝึกซ้อมเพื่อเตรียมความพร้อม ตลอดจนการ ทบทวนและปรับปรุงแผนให้ทันสมัยอย่างสม่ำเสมอ	
ความเสี่ยง	
ไม่สามารถป้องกันและรับมือภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม	
การควบคุมที่พึงมี	
ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อย ปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจ ว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล	
แนวทางการประเมิน	
- ตรวจสอบว่าหน่วยงานมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ซึ่งผ่านการสื่อสารให้ ผู้เกี่ยวข้องรับทราบ รวมถึงมีการทบทวนและปรับปรุงเนื้อหาของแผนให้เป็นปัจจุบันตามผล การซ้อมหรือการเปลี่ยนแปลงของภัยคุกคาม อย่างน้อยปีละ 1 ครั้ง เพื่อยืนยันความพร้อมใน การปฏิบัติงานจริงอย่างมีประสิทธิภาพและประสิทธิผลตามที่กฎหมายกำหนด - ตรวจสอบหลักฐานการฝึกซ้อมตามสถานการณ์จำลอง (เช่น Tabletop หรือ Simulation) ว่า มีการดำเนินการอย่างน้อยปีละ 1 ครั้ง	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.1.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 3
NIST CSF 2.0	ID.IM-02, ID.IM-04
ISO/IEC27001:2022	Annex A 5.24, Annex A 5.27
ISO/IEC27701:2025	-
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.1, 16.1.6
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - หน่วยงานมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ครอบคลุมบริการใดบ้าง ครอบคลุมบริการที่สำคัญ (CII) ทั้งหมดหรือไม่ - ในรอบปีที่ผ่านมา มีการสื่อสารแผนและบทบาทหน้าที่ให้แก่ผู้ที่เกี่ยวข้อง (รวมถึงหน่วยงาน ภายนอก/Outsource ถ้ามี) รับทราบผ่านช่องทางใดบ้าง (เช่น การอบรม อีเมลแจ้งเวียน)	

3. ในรอบปีที่ผ่านมา มีการจัดฝึกซ้อมแผนรับมือภัยคุกคามในรูปแบบใดบ้าง (เช่น Tabletop, Simulation)
4. จากการฝึกซ้อมครั้งล่าสุด พบข้อบกพร่องในแผนรับมือภัยคุกคามอย่างไร และนำมาปรับปรุงแผนอย่างไร
5. หน่วยงานได้นำข้อบกพร่องที่พบจากเหตุการณ์ที่เกิดขึ้นจริง มาจัดทำแนวทางปรับปรุงแผนอย่างไร

■ การสอบทานเอกสาร

1. สอบทานแผนการรับมือภัยคุกคามทางไซเบอร์ ว่ามีการระบุรายละเอียดที่สอดคล้องกับประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 ข้อ 19.1
2. สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อยืนยันว่ามีการทบทวนอย่างน้อยปีละ 1 ครั้งตามรอบเวลาที่กำหนด
3. สอบทานบันทึกการสื่อสารหรือรายชื่อผู้รับทราบแผน (เช่น บัญชีรายชื่อลงนาม, Log การอ่านอีเมล) เพื่อยืนยันว่าแผนถูกสื่อสารไปยังผู้ปฏิบัติงานและหน่วยงานสนับสนุนที่เกี่ยวข้องจริง
4. สอบทานรายงานผลการฝึกซ้อม (Exercise Report) และรายงานการทบทวนหลังการดำเนินการ (After-Action Review Report / Lessons Learned) เพื่อดูรายการข้อบกพร่องที่พบและสถานะการแก้ไข

■ เอกสารที่เกี่ยวข้อง

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)
2. รายงานการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
3. บันทึกการสื่อสารหรือรายชื่อผู้รับทราบแผน
4. รายงานการทบทวนหลังการดำเนินการ (After-Action Review Report / Lessons Learned)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
3.1.53 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีการเตรียมความพร้อมในการบริหารจัดการข้อมูลข่าวสารเมื่อเกิดเหตุการณ์วิกฤตทางไซเบอร์
ความเสี่ยง
การสื่อสารข้อมูลข่าวสารเมื่อเกิดเหตุการณ์วิกฤตทางไซเบอร์ไม่เหมาะสม และส่งผลเสียต่อภาพลักษณ์องค์กร
การควบคุมที่พึงมี

ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

แนวทางการประเมิน

1. ตรวจสอบว่ามีการจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
2. ตรวจสอบเนื้อหาในแผนครอบคลุมการตอบสนองและรองรับวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.2.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 13
NIST CSF 2.0	ID.IM-04
ISO/IEC27001:2022	Annex A 5.24, Clause 7.4
ISO/IEC27701:2025	Clause 7.4
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	A.4.4
ISO/IEC TS 27008:2019	16.1.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

- การสัมภาษณ์
 1. หน่วยงานมีการจัดทำแผนการสื่อสารในภาวะวิกฤตหรือไม่ ครอบคลุมการตอบสนองและรองรับวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือไม่
- การสอบถามเอกสาร
 1. สอบถามแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ว่ามีเนื้อหาในแผนครอบคลุมการตอบสนองและรองรับวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
 2. สอบถามว่าแผนมีจุดเชื่อมต่อกับแผนการรับมือภัยคุกคามทางไซเบอร์ (เช่น เมื่อความรุนแรงระดับใดถึงต้องเริ่มใช้แผนสื่อสารภาวะวิกฤต)
- เอกสารที่เกี่ยวข้อง
 1. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
 2. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)
- เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.1.54 รายละเอียดของแผนการสื่อสารในภาวะวิกฤต (Details of Crisis Communication Plan)

วัตถุประสงค์

เพื่อให้มั่นใจว่า แผนการสื่อสารในภาวะวิกฤตมีองค์ประกอบและรายละเอียดเชิงปฏิบัติที่ครบถ้วนชัดเจน สามารถรองรับการดำเนินงานในสถานการณ์จริงได้อย่างมีประสิทธิภาพ

ความเสี่ยง

การสื่อสารข้อมูลข่าวสารเมื่อเกิดเหตุการณ์วิกฤตทางไซเบอร์ไม่เหมาะสม และส่งผลเสียต่อภาพลักษณ์องค์กร

การควบคุมที่พึงมี

ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีรายละเอียดดังนี้

- (ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต
- (ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
- (ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
- (ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ
- (จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

แนวทางการประเมิน

1. ตรวจสอบความครบถ้วนขององค์ประกอบในแผนการสื่อสารฯ ว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (จ)
2. ตรวจสอบว่าข้อมูลที่ระบุตามการควบคุมที่พึงมีข้อ (ก) - (จ) ได้รับการทบทวนและปรับปรุงให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.2.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 13
NIST CSF 2.0	GV.RR-02, RS.CO-02
ISO/IEC 27001:2022	Annex A 5.24, Annex A 5.26
ISO/IEC 27701:2025	A.3.12
ISO/IEC 27017:2015	16.1.1
ISO/IEC 27007:2020	-
ISO/IEC TS 27008:2019	16.1.1, 16.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. โครงสร้างทีมสื่อสารในภาวะวิกฤตเป็นอย่างไร
2. หน่วยงานมีการจำแนกกลุ่มเป้าหมายเพื่อเลือกช่องทางการสื่อสารที่เหมาะสมไว้ล่วงหน้าหรือไม่
3. ใครเป็นผู้มีอำนาจตัดสินใจประกาศเข้าสู่ภาวะวิกฤตเพื่อเริ่มกระบวนการสื่อสาร

■ การสอบถามเอกสาร

1. สอบทานเอกสารคำสั่งแต่งตั้งทีมงาน หรือ รายชื่อติดต่อ (Contact List) ของโฆษกและผู้เชี่ยวชาญ ซึ่งต้องระบุข้อมูลติดต่อที่ใช้งานได้จริง

2. สอบทานแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ว่ามีการเตรียมร่างแถลงการณ์ล่วงหน้าสำหรับกรณีต่าง ๆ เช่น เหตุการณ์ระบบล่ม ข้อมูลรั่วไหล 3. สอบทานเอกสารแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ว่าได้ระบุช่องทางการสื่อสารที่เป็นทางการของหน่วยงาน เช่น เว็บไซต์หลัก เพจ Facebook ที่ได้รับการยืนยันตัวตน เพื่อป้องกันข่าวปลอม 4. สอบทานรายชื่อผู้มีส่วนได้ส่วนเสีย (Stakeholders) ที่ต้องแจ้งเตือนตามกฎหมายหรือข้อกำหนด ว่าเป็นข้อมูลปัจจุบันและติดต่อได้ (เช่น สกมช. ผู้ใช้บริการ สื่อมวลชน หรือหน่วยงานกำกับดูแลตามกฎหมาย) ■ เอกสารที่เกี่ยวข้อง 1. คำสั่งแต่งตั้งทีมสื่อสารในภาวะวิกฤตและโฆษก 2. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) 3. ทะเบียนรายชื่อและช่องทางติดต่อทีมงาน และผู้มีส่วนได้ส่วนเสียสำหรับการสื่อสารในภาวะวิกฤต 4. ร่างแม่แบบแถลงการณ์ฉุกเฉิน (Press Release Templates) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

3.1.55 การประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบในแผนการสื่อสารในภาวะวิกฤต (Coordination among Affected Parties in Crisis Communication Plan)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า กระบวนการสื่อสารในสภาวะวิกฤตมีการประสานงานร่วมกันอย่างเป็นระบบระหว่างทุกฝ่ายที่เกี่ยวข้อง ทั้งหน่วยงานภายในและพันธมิตรภายนอกที่ได้รับผลกระทบ	
ความเสี่ยง	
การสื่อสารข้อมูลข่าวสารเมื่อเกิดเหตุการณ์วิกฤตทางไซเบอร์ไม่เหมาะสม และส่งผลเสียต่อภาพลักษณ์องค์กร	
การควบคุมที่พึงมี	
ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต	
แนวทางการประเมิน	
1. ตรวจสอบโครงสร้างในแผนการสื่อสารฯ ว่ามีการระบุขั้นตอนการประสานงานระหว่างทีมสื่อสาร ทีม CIRT ทีมผู้บริหาร และฝ่ายอื่น ๆ ที่ได้รับผลกระทบ 2. ตรวจสอบกระบวนการไหลของข้อมูล เพื่อให้มั่นใจว่าการให้ข่าวสารเป็นไปในทิศทางเดียวกันและสอดคล้องกัน	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.2.3
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 13
NIST CSF 2.0	RS.CO-02

ISO/IEC27001:2022	Annex A 5.26
ISO/IEC27701:2025	A.3.12
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ทีม CIRT มีขั้นตอนส่งข้อมูลให้ทีมสื่อสารอย่างไร เมื่อเกิดเหตุวิกฤตทางไซเบอร์ 2. ใครเป็นผู้มีอำนาจตัดสินใจสูงสุดในการอนุมัติ ข้อความที่จะแถลงต่อสาธารณะ และมีกระบวนการทบทวนความถูกต้องร่วมกับฝ่ายกฎหมายหรือฝ่ายบริหารอย่างไรก่อนการสื่อสาร ■ การสอบถามเอกสาร 1. สอบทานแผนการสื่อสารในภาวะวิกฤต เพื่อยืนยันกระบวนการไหลของข้อมูลข่าวสารที่เชื่อมโยงระหว่างทีม CIRT ทีมบริหาร และทีมสื่อสารชัดเจน 2. สอบทานแบบฟอร์มการอนุมัติแถลงการณ์ ว่ามีการลงนามรับรองจากผู้มีอำนาจในการสื่อสาร 3. สอบทานขั้นตอนการอนุมัติในแผนว่ามีการระบุลำดับขั้นการตัดสินใจ (Escalation) เพื่อให้การให้ข่าวสารเป็นไปในทิศทางเดียวกันและไม่เกิดความขัดแย้ง ■ เอกสารที่เกี่ยวข้อง 1. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) 2. แบบฟอร์มการอนุมัติแถลงการณ์ 3. ระเบียบปฏิบัติเกี่ยวกับการให้ข่าวสารต่อสาธารณะ ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	

3.1.56 การฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต (Cybersecurity Crisis Communication Exercise)
วัตถุประสงค์
เพื่อให้มั่นใจว่า บุคลากรและทีมงานที่เกี่ยวข้องมีความพร้อมในการปฏิบัติหน้าที่ตามแผนการสื่อสารในภาวะวิกฤต สามารถใช้เครื่องมือหรือช่องทางการสื่อสารได้อย่างทันท่วงทีและมีประสิทธิภาพ
ความเสี่ยง
บุคลากรและทีมงานที่เกี่ยวข้องไม่สามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างถูกต้องและทันท่วงที เมื่อเผชิญเหตุการณ์วิกฤตจริง
การควบคุมที่พึงมี
ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิภาพในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
แนวทางการประเมิน

1. ตรวจสอบประวัติการดำเนินกิจกรรมฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง 2. ตรวจสอบผลการฝึกซ้อม ว่าทีมงานสามารถสื่อสารและเผยแพร่ข้อมูลได้ครบถ้วนถูกต้อง และเป็นไปตามกรอบเวลาที่กฎหมายกำหนด	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.2.4
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 13
NIST CSF 2.0	ID.IM-02
ISO/IEC27001:2022	Clause 7.4, Annex A 5.24
ISO/IEC27701:2025	Clause 7.4
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	A4.4
ISO/IEC TS 27008:2019	16.1.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ในรอบปีที่ผ่านมา มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตหรือไม่ แบบใด (เช่น Tabletop Exercise ร่วมกับทีมเทคนิค หรือการซ้อมเฉพาะทีมสื่อสาร) 2. จากการฝึกซ้อมครั้งล่าสุด พบอุปสรรคในการสื่อสารหรือการให้ข่าวสารอย่างไร และนำมาปรับปรุงแผนอย่างไร ■ การสอบทานเอกสาร 1. สอบทานรายงานผลการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง 2. สอบทานรายงานผลการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี ว่ามีการบันทึกเวลาของการสื่อสารแต่ละขั้นตอน 3. สอบทานบันทึกบทเรียนที่ได้รับ (Lessons Learned) เพื่อตรวจสอบว่าทีมงานพบข้อติดขัดหรืออุปสรรคใดในการประสานงาน และมีการระบุข้อเสนอแนะในการปรับปรุงแผน ■ เอกสารที่เกี่ยวข้อง 1. รายงานผลการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี 2. บันทึกบทเรียนที่ได้รับ (Lessons Learned) 3. ตารางกำหนดการฝึกซ้อมประจำปี ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค	
-	

การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

3.1.57 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีความพร้อมในการ
เข้าร่วมฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ในระดับชาติหรือระดับภาคส่วนตามที่กฎหมายกำหนด

ความเสี่ยง

หน่วยงานไม่สามารถดำเนินงานร่วมกับหน่วยงานภายนอกได้อย่างถูกต้อง เมื่อเกิดการโจมตีทางไซเบอร์ขึ้น
จริง

การควบคุมที่พึงมี

ตาม พรบ. ไซเบอร์ มาตรา 22 วรรคหนึ่ง (13) หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทาง
สารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์
อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้
ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมใน
การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

แนวทางการประเมิน

1. ตรวจสอบหนังสือคำสั่งหรือการร้องขอจากคณะกรรมการฯ ที่ให้เข้าร่วมการฝึกซ้อมรับมือภัย
คุกคามทางไซเบอร์
2. ตรวจสอบการจัดสรรบุคลากรที่เกี่ยวข้องตามที่ระบุในแผนรับมือภัยคุกคามฯ (เช่น CIRT) เพื่อ
เข้าร่วมการฝึกซ้อม
3. ตรวจสอบผลการมีส่วนร่วมของบุคลากรในการฝึกซ้อมทั้งระดับชาติหรือระดับภาคส่วนตามที่
ได้รับมอบหมาย

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.3.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 14
NIST CSF 2.0	ID.IM-02, PR.AT-02
ISO/IEC27001:2022	Annex A 5.5, Annex A 5.24
ISO/IEC27701:2025	-
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.3, 16.1.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีหลักเกณฑ์การพิจารณาคัดเลือกบุคลากรเข้าร่วมการฝึกซ้อม ให้ตรงตามบทบาทที่
ระบุไว้ในแผนรับมือภัยคุกคามฯ อย่างไร
2. มีการนำข้อเสนอแนะหรือบทเรียน (Lessons Learned) จากการฝึกซ้อมส่วนกลางมาปรับปรุง
กระบวนการภายในอย่างไร

■ การสอบทานเอกสาร

1. สอบทานหนังสือจากหน่วยงานกำกับดูแล (เช่น หนังสือจาก สกมช.) และบันทึกข้อความภายในที่ระบุการอนุมัติให้บุคลากรเข้าร่วมการฝึกซ้อม 2. สอบทานว่ารายชื่อบุคลากรที่ส่งไป (เช่น ทีม CIRT ผู้บริหาร หรือฝ่ายกฎหมาย) สอดคล้องกับบทบาทหน้าที่ที่ระบุไว้ในแผนรับมือภัยคุกคามทางไซเบอร์ของหน่วยงาน 3. สอบทานประกาศนียบัตร (Certificate) ภาพถ่ายกิจกรรม รายงานสรุปผลการฝึกซ้อมที่ผู้แทนเขียนรายงานต่อผู้บริหาร หรือบันทึกคะแนนการทดสอบ เพื่อประเมินระดับการมีส่วนร่วม ■ เอกสารที่เกี่ยวข้อง 1. หนังสือคำสั่งหรือจดหมายเชิญการฝึกซ้อมจากหน่วยงานภายนอก (เช่น สกมช., CERT ภาคส่วน หรือกระทรวงต้นสังกัด) 2. คำสั่งแต่งตั้งตัวแทนหน่วยงานหรือบันทึกข้อความอนุมัติการเข้าร่วมฝึกซ้อม 3. รายชื่อบุคลากรที่เข้าร่วม (Attendance Sheet) 4. รายงานสรุปผลการเข้าร่วมการฝึกซ้อม 5. ใบประกาศนียบัตรหรือวุฒิบัตรการเข้าร่วมฝึกซ้อม ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.1.58 การให้ข้อมูลเพื่อการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ (Provision of Information for Cyber Exercise Planning and Execution)
วัตถุประสงค์ เพื่อให้มั่นใจว่า หน่วยงานมีความพร้อมในการสนับสนุนข้อมูลและเอกสารที่จำเป็นแก่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (คณะกรรมการ) หรือ สกมช. เพื่อใช้ในการวางแผนและออกแบบสถานการณ์การฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์
ความเสี่ยง การออกแบบสถานการณ์ฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ไม่สอดคล้องกับบริการที่สำคัญของหน่วยงาน
การควบคุมที่พึงมี ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึง แผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามประมวลแนวปฏิบัติฯ พ.ศ. 2564 ข้อ 24.1 และข้อ 24.2 ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
แนวทางการประเมิน 1. ตรวจสอบช่องทางการรับคำร้องต่อคำขอข้อมูลจากคณะกรรมการ 2. ตรวจสอบกระบวนการรวบรวมและจัดส่งข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญต่อคณะกรรมการ 3. ตรวจสอบความถูกต้อง ครบถ้วน และกรอบเวลาในการส่งข้อมูลตามคำร้องของคณะกรรมการ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 24.3.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 14
NIST CSF 2.0	GV.OC-03, ID.IM-02
ISO/IEC27001:2022	Annex A 5.5
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	6.1.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีกระบวนการหรือผู้รับผิดชอบหลัก (Point of Contact) ในการรับและติดตามคำร้องขอข้อมูลจากคณะกรรมการ หรือ สกมช. อย่างไร
2. เมื่อได้รับการร้องขอแผนการรับมือภัยคุกคามทางไซเบอร์ แผนการสื่อสารในภาวะวิกฤต หรือ ขั้นตอนการปฏิบัติงานฯ จาก สกมช. หรือหน่วยงานกำกับดูแล หน่วยงานมีกระบวนการรวบรวมและตรวจสอบความถูกต้องของข้อมูลก่อนส่งมอบอย่างไร
3. ในการส่งมอบข้อมูลที่ละเอียดอ่อน หน่วยงานมีมาตรการป้องกันความลับของข้อมูลในระหว่างการส่งมอบอย่างไร (เช่น การใช้การเข้ารหัสไฟล์ หรือช่องทางสื่อสารที่ปลอดภัย)

■ การสอบทานเอกสาร

1. สอบทานหนังสือจากคณะกรรมการ หรือ สกมช. และบันทึกข้อความภายในที่ระบุการร้องขอข้อมูล เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์
2. สอบทานประวัติการรับ-ส่งข้อมูลระหว่างหน่วยงานกับคณะกรรมการฯ (เช่น บันทึกข้อความ, อีเมลตอบรับ) ว่ามีการปฏิบัติตามคำขอภายในกรอบเวลาที่กำหนด และสอบทานว่าข้อมูลที่ส่งไปสอดคล้องกับคำขอ
3. สอบทานบันทึกการอนุมัติจากผู้บริหารในการเปิดเผยข้อมูลดังกล่าวให้แก่คณะกรรมการ เพื่อยืนยันว่าการให้ข้อมูลเป็นไปตามนโยบายชั้นความลับของหน่วยงาน

■ เอกสารที่เกี่ยวข้อง

1. หนังสือคำขอข้อมูลจากคณะกรรมการ หรือ สกมช.
2. บันทึกการส่งมอบข้อมูล หรืออีเมลยืนยันการรับ-ส่งข้อมูล / ทะเบียนคุมการรับ-ส่งหนังสือราชการ
3. สำเนาข้อมูลที่ส่งมอบที่มีการประทับตราชั้นความลับ
4. บันทึกการอนุมัติจากผู้บริหาร

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	
การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	
3.1.59 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) ที่สามารถรองรับเหตุการณ์หยุดชะงักจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยมีการกำหนดเป้าหมายการกู้คืนข้อมูลและระบบ (RTO, RPO) ที่ชัดเจน และมีการประสานงานกับผู้ให้บริการภายนอกอย่างสอดคล้องกัน เพื่อให้บริการที่สำคัญสามารถกลับมาดำเนินงานได้ภายในระยะเวลาที่ยอมรับได้	
ความเสี่ยง	
ข้อมูลและบริการสำคัญไม่สามารถกลับมาดำเนินงานได้ในระยะเวลาที่ยอมรับได้เมื่อเกิดภัยคุกคามทางไซเบอร์	
การควบคุมที่พึงมี	
ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตค่านิยมและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด	
แนวทางการประเมิน	
1. ตรวจสอบการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อรองรับกรณีระบบหยุดชะงักจากภัยไซเบอร์ และครอบคลุมการให้บริการที่สำคัญ (CII) ให้สามารถดำเนินต่อไปได้ 2. ตรวจสอบแผน BCP ของผู้ให้บริการภายนอก (Outsource) ว่ามีความสอดคล้องกับแผน BCP ของหน่วยงาน และมีความสอดคล้องของขอบเขตค่านิยมและการกำหนดระยะเวลาที่สำคัญ เช่น MTPD, RTO, และ RPO 3. ตรวจสอบว่าโครงสร้างแผน BCP เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. กำหนด	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 25.1.1
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 15
NIST CSF 2.0	GV.SC-08, ID.IM-04, RC.RP-04
ISO/IEC27001:2022	Annex A 5.20, Annex A 5.22, Annex A 5.29, Annex A 5.30, Annex A 7.5, Annex A 7.11, Annex A 7.13, Annex A 8.6, Annex A 8.14

ISO/IEC27701:2025	A.3.10
ISO/IEC27017:2015	12.1.3, 15.1.2
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	11.1.4, 11.2.2, 11.2.4, 12.1.3, 15.1.1, 15.1.2, 15.2.1, 15.2.2, 17.1.1, 17.1.2, 17.1.3, 17.2.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3), 4 (4)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. แผน BCP ที่จัดทำขึ้นมีการระบุขั้นตอนเฉพาะสำหรับเหตุการณ์ที่เกิดจากภัยไซเบอร์ (Cyber-induced Disruption) หรือไม่ 2. หน่วยงานมีเกณฑ์อย่างไรในการกำหนดค่า Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) สำหรับบริการสำคัญ (CII) และระยะเวลาเหล่านี้สอดคล้องกับผลกระทบต่อประชาชนหรือความมั่นคงอย่างไร 3. หน่วยงานมีกระบวนการอย่างไรในการตรวจสอบว่าแผน BCP ของผู้ให้บริการภายนอก (เช่น Cloud Provider, Managed Service) สามารถรองรับค่า RTO และ RPO ที่หน่วยงานกำหนดไว้ได้จริง ■ การสอบทานเอกสาร 1. สอบทานรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ว่ามีการกำหนดค่า MTPD, RTO, และ RPO ครอบคลุมทุกบริการสำคัญของ CII และมีความสอดคล้องกับผลกระทบต่อประชาชนหรือความมั่นคง 2. สอบทานว่าโครงสร้างและหัวข้อในแผนความต่อเนื่องทางธุรกิจ (BCP) เป็นไปตามหลักเกณฑ์ที่สำนักงานประกาศกำหนด 3. สอบทานแผนความต่อเนื่องทางธุรกิจ (BCP) ว่ามีการระบุขั้นตอนการกู้คืนสำหรับภัยไซเบอร์ (เช่น Ransomware Recovery) และมีการระบุทรัพยากรที่จำเป็น (คน, ระบบ, สถานที่) 4. สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อยืนยันว่ามีการทบทวนอย่างน้อยปีละ 1 ครั้งตามรอบเวลาที่กำหนด 5. สอบทานบันทึกการประเมิน หรือผลการทดสอบความสอดคล้องระหว่างแผนความต่อเนื่องทางธุรกิจ (BCP) ของหน่วยงานกับแผนความต่อเนื่องทางธุรกิจ (BCP) ของผู้ให้บริการภายนอก 6. สอบทานสัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) เทียบกับค่า RTO/RPO ที่กำหนดในแผนความต่อเนื่องทางธุรกิจ (BCP) ■ เอกสารที่เกี่ยวข้อง 1. รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 2. แผนความต่อเนื่องทางธุรกิจ (BCP) ของหน่วยงาน 3. แผนความต่อเนื่องทางธุรกิจ (BCP) ของผู้ให้บริการภายนอก	

4. สัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) กับผู้ให้บริการภายนอก
- เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

3.1.60 การฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan Exercise)

วัตถุประสงค์

เพื่อให้มั่นใจว่า แผนความต่อเนื่องทางธุรกิจ (BCP) ที่หน่วยงานจัดทำขึ้น สามารถนำไปปฏิบัติได้จริงและมีประสิทธิภาพในการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ รวมถึงเพื่อให้บุคลากรที่เกี่ยวข้องมีความเข้าใจในบทบาทหน้าที่และขั้นตอนการดำเนินงานในสภาวะวิกฤต

ความเสี่ยง

บุคลากรขาดความเข้าใจและไม่สามารถกู้คืนข้อมูลและบริการสำคัญได้อย่างเหมาะสมเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ขึ้นจริง

การควบคุมที่มี

ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 (หนึ่ง) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

แนวทางการประเมิน

1. ตรวจสอบแผนงานและการกำหนดรอบการฝึกซ้อมแผน BCP ประจำปี ว่ามีการดำเนินการอย่างน้อยปีละ 1 ครั้ง
2. ตรวจสอบหลักฐานการดำเนินการฝึกซ้อมแผน BCP ประจำปี และรายงานผลการฝึกซ้อมแผน BCP ประจำปี รวมถึงผลการประเมินประสิทธิภาพของแผน BCP ในการรับมือภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	ข้อ 25.1.2
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	เอกสารแนบ 15
NIST CSF 2.0	ID.IM-02
ISO/IEC27001:2022	Annex A 5.29, Annex A 5.30
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	17.1.1, 17.1.2, 17.1.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. ในรอบปีที่ผ่านมา หน่วยงานเลือกสถานการณ์จำลองใดสำหรับการซ้อมแผน BCP ประจำปี และใช้รูปแบบการฝึกซ้อม BCP แบบใด (เช่น Tabletop, Simulation, Full Interruption) และมีเกณฑ์การเลือกหรือไม่

2. ในรอบปีที่ผ่านมา มีการประสานงานร่วมกับผู้ให้บริการภายนอก เพื่อทดสอบการกู้คืนข้อมูลตามค่า RTO และ RPO ที่กำหนดไว้ในแผนอย่างไร
3. หากผลการซ้อมแผน BCP ไม่เป็นไปตามเป้าหมาย MTPD/RTO/RPO ที่ตั้งไว้ หน่วยงานมีกระบวนการจัดการเพื่อปรับปรุงแผนอย่างไร

■ การสอบทานเอกสาร

1. สอบทานแผนการฝึกซ้อม BCP ประจำปี ว่ามีการระบอบการฝึกซ้อม อย่างน้อยปีละ 1 ครั้ง
2. สอบทานบันทึกการเข้าอบรมหรือรายชื่อผู้เข้าร่วมการฝึกซ้อม และการซ้อม เช่น ภาพถ่ายกิจกรรม รายชื่อผู้เข้าร่วมจากฝ่ายที่เกี่ยวข้อง หรือ Log การกู้คืนระบบจำลอง เพื่อยืนยันว่าการซ้อมจริง
3. สอบทานบันทึกบทเรียนที่ได้รับ (Lessons Learned) ว่ามีการบันทึกข้อจำกัดหรืออุปสรรคที่พบ การระบุสาเหตุที่แท้จริงที่ทำให้แผนไม่เป็นไปตามเป้า (ถ้ามี) และข้อเสนอแนะเพื่อการปรับปรุง
4. สอบทานรายงานผลการฝึกซ้อม (BCP Test Report) ว่ามีผลการทดสอบเทียบกับค่าเป้าหมาย MTPD/RTO/RPO
5. สอบทานรายงานผลการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP Test Report) ว่าในสถานการณ์จำลองมีการซ้อมกู้คืนระบบร่วมกับผู้ให้บริการภายนอกหรือไม่ และผลลัพธ์ที่ได้สอดคล้องกับข้อตกลงระดับการให้บริการ (SLA)
6. สอบทานบันทึกการปรับปรุงแผน BCP จากข้อบกพร่องที่พบจากการฝึกซ้อม

■ เอกสารที่เกี่ยวข้อง

1. แผนงานหรือกำหนดการฝึกซ้อม BCP ประจำปี
2. บันทึกการเข้าอบรมหรือรายชื่อผู้เข้าร่วมการฝึกซ้อม
3. บันทึกบทเรียนที่ได้รับ (Lessons Learned)
4. รายงานผลการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP Test Report)
5. สัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) กับผู้ให้บริการภายนอก
6. หลักฐานการปรับปรุงแผน BCP หลังการฝึกซ้อม

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.2 แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามแนวทางปฏิบัติที่ดี (Best Practices)

แนวทางการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามแนวทางปฏิบัติที่ดี (Best Practices) จะเป็นส่วนต่อขยายของเนื้อหา 2 ส่วน ตามแนวทางของประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 รวมทั้งหมด 19 ข้อ ได้แก่

ส่วนที่ 1 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติ

แนวทางปฏิบัติที่ดีสำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติ มุ่งเน้นการยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรให้สอดคล้องกับมาตรฐานสากล โดยมีการกำหนดข้อกำหนดเพิ่มเติมจำนวน 2 ข้อ เพื่อเพิ่มประสิทธิภาพในการควบคุมดูแลและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่เหมาะสม

ส่วนที่ 2 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางปฏิบัติที่ดีสำหรับการตรวจประเมินตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีวัตถุประสงค์หลักในการเสริมสร้างศักยภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เทียบเท่าระดับสากล โดยครอบคลุมการปฏิบัติที่เข้มข้นยิ่งขึ้นผ่านข้อกำหนดเพิ่มเติมจำนวน 17 ข้อ เพื่อให้มั่นใจว่าระบบสารสนเทศและโครงสร้างพื้นฐานสำคัญมีความพร้อมในการรับมือกับภัยคุกคามในรูปแบบต่าง ๆ

การตรวจประเมินตามแนวทางปฏิบัติที่ดีทั้งสองส่วน มีรายละเอียดของข้อกำหนดที่ต้องดำเนินการตรวจสอบและประเมินผล ดังนี้

ส่วนที่ 1 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติ

องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
การประเมินความเสี่ยง
3.2.1 ความรับผิดชอบของผู้นำองค์กรและการส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์
วัตถุประสงค์
เพื่อให้มั่นใจว่า ผู้นำองค์กรมีความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งส่งเสริมการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์
ความเสี่ยง
การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ไม่ประสบความสำเร็จตามเป้าหมาย ส่งผลให้ไม่สามารถควบคุมความเสี่ยงและปกป้องข้อมูลหรือบริการสำคัญได้อย่างเหมาะสม
การควบคุมที่พึงมี
ผู้นำองค์กรควรมีความรับผิดชอบและภาวะรับผิดชอบต่อความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมวัฒนธรรมที่ตระหนักถึงความเสี่ยง (Risk-aware culture) และการปฏิบัติตามหลักจริยธรรม (Ethical) และมีการปรับปรุงอย่างต่อเนื่อง
แนวทางการประเมิน

1. ตรวจสอบการกำหนดความรับผิดชอบ (Responsible) และการรับผิดชอบ (Accountable) ของผู้นำองค์กรหรือผู้บริหารระดับสูงต่อความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 2. ประเมินการส่งเสริมวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยง (Risk-aware culture) และการปฏิบัติตามหลักจริยธรรม (Ethical) 3. ตรวจสอบบทบาทของผู้นำในการสนับสนุนและผลักดันให้เกิดการปรับปรุงกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง (Continually improving)	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	GV.RR-01
ISO/IEC27001:2022	Clause 7.2, Annex A 5.4
ISO/IEC27701:2025	Clause 7.2
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.4.2
ISO/IEC TS 27008:2019	7.2.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ผู้บริหารระดับสูง (เช่น CEO, คณะกรรมการบริหาร) แสดงบทบาท ภาระรับผิดชอบ และการมีส่วนร่วมในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านไซเบอร์ขององค์กรอย่างไร มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ไว้อย่างไร 2. องค์กรมีกลไก นโยบาย หรือกิจกรรมใดบ้างที่ผู้บริหารระดับสูงใช้เพื่อส่งเสริมวัฒนธรรมความตระหนักรู้ด้านความเสี่ยงไซเบอร์และจริยธรรมในการทำงานให้กับบุคลากรทุกระดับ 3. ผู้บริหารระดับสูงมีการติดตามผล ทบทวน และสนับสนุนทรัพยากรเพื่อการปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่องอย่างไร ■ การสอบทานเอกสาร 1. สอบทานโครงสร้างการกำกับดูแลองค์กร (Governance Structure) และข้อบังคับ/กฎบัตร คณะกรรมการ (Board Charter) ที่ระบุอำนาจและหน้าที่รับผิดชอบด้านความเสี่ยงไซเบอร์ของผู้บริหารระดับสูง 2. สอบทานรายงานการประชุมระดับบริหาร (Board/Executive Meeting Minutes) เพื่อดูบันทึกการพิจารณา การรับทราบ และการตัดสินใจในวาระที่เกี่ยวข้องกับความเสี่ยงด้านไซเบอร์ 3. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) ว่ามีการลงนามรับทราบและอนุมัติแผนจัดการความเสี่ยง (Risk Treatment Plan) โดยผู้บริหารระดับสูง 4. สอบทานหลักฐานการสื่อสารจากผู้บริหารระดับสูงถึงพนักงานในเรื่องความมั่นคงปลอดภัยไซเบอร์ ■ เอกสารที่เกี่ยวข้อง	

1. โครงสร้างองค์กรและกฎบัตรคณะกรรมการ/ผู้บริหาร (Organization Chart & Board/Committee Charters) 2. รายงานการประเมินความเสี่ยง (Risk Assessment Report) 3. รายงานการประชุมคณะกรรมการหรือผู้บริหารระดับสูง (Board/Management Meeting Minutes) 4. นโยบายจากผู้บริหารระดับสูง เช่น จรรยาบรรณองค์กร (Code of Conduct / Ethics Policy) นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) นโยบายการใช้งานเทคโนโลยีอย่างมีจริยธรรม 5. หลักฐานการสื่อสารจากผู้บริหารระดับสูง (Executive Communications / Townhall Records) ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -
--

3.2.2 การกำกับดูแล การทบทวน และการปรับปรุงกลยุทธ์และผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์
วัตถุประสงค์
เพื่อให้มั่นใจว่า องค์กรมีกลไกในการเฝ้าติดตามและประเมินผลการดำเนินงานตามกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์อย่างเป็นรูปธรรม
ความเสี่ยง
ไม่สามารถตอบสนองต่อภัยคุกคามในปัจจุบัน และขาดทิศทางการพัฒนาศักยภาพเพื่อปกป้องข้อมูลหรือบริการสำคัญได้อย่างมีประสิทธิภาพ
การควบคุมที่พึงมี
การกำกับดูแลและกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Governance and Strategy Standards) ควรประกอบด้วยกระบวนการบริหารจัดการอย่างน้อย 3 ประการ ได้แก่ (ก) ผลลัพธ์จากการบริหารจัดการความเสี่ยงต้องถูกนำมาประเมินเพื่อใช้เป็นข้อมูลในการปรับปรุงกลยุทธ์และทิศทางขององค์กรให้สอดคล้องกับสถานการณ์ปัจจุบัน (ข) กลยุทธ์ต้องได้รับการทบทวนอย่างสม่ำเสมอเพื่อให้มั่นใจว่าครอบคลุมทุกข้อกำหนดทางกฎหมาย มาตรฐานสากล และบริบทความเสี่ยงเฉพาะขององค์กร และ (ค) ผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการวัดผลและทบทวนอย่างเป็นระบบ เพื่อกำหนดแนวทางการปรับปรุงและเพิ่มประสิทธิภาพการดำเนินงานที่จำเป็น
แนวทางการประเมิน
1. ตรวจสอบผลลัพธ์จากการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ว่ามีการนำไปใช้เป็นปัจจัยในการตัดสินใจเชิงกลยุทธ์และทิศทางของหน่วยงาน 2. ตรวจสอบการทบทวนและปรับเปลี่ยนกลยุทธ์การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ว่ามีความครอบคลุมถึงข้อกำหนดและความเสี่ยงของหน่วยงานที่เปลี่ยนแปลงไป 3. ตรวจสอบว่ามีการดำเนินการวัดผล การทบทวน และประเมินผลการดำเนินงานด้านการบริหารความเสี่ยงระดับองค์กร และทำการปรับปรุงแก้ไข

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	GV.OV-01, GV.OV-02, GV.OV-03, GV.RM-07
ISO/IEC27001:2022	Clause 9.1, Annex A 5.1, Annex A 5.4, Annex A 5.19, Annex A 5.20
ISO/IEC27701:2025	Clause 9.1, A.3.3
ISO/IEC27017:2015	5.1.1, 15.1.1, 15.1.2
ISO/IEC27007:2020	A.5.3
ISO/IEC TS 27008:2019	5.1.1, 5.1.2, 7.2.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีการนำผลลัพธ์จากการจัดการความเสี่ยงไซเบอร์ หรือผลการตรวจประเมินด้านความมั่นคงปลอดภัยไซเบอร์ ไปใช้เป็นปัจจัยในการตัดสินใจเชิงกลยุทธ์หรือการลงทุนในโครงการต่าง ๆ ของหน่วยงานหรือไม่
2. องค์กรมีระยะเวลาหรือกลไกในการทบทวนกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ และผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กรอย่างไร (เช่น รายไตรมาส หรือรายปี)
3. เมื่อมีการเปลี่ยนแปลงข้อกำหนดทางธุรกิจ กฎหมาย หรือพบความเสี่ยง/ภัยคุกคามรูปแบบใหม่ องค์กรมีกระบวนการนำประเด็นเหล่านี้มาปรับปรุงกลยุทธ์ด้านไซเบอร์อย่างไรให้ครอบคลุมความเสี่ยงใหม่ ๆ
4. องค์กรใช้ตัวชี้วัดหรือข้อมูลใด (เช่น KPI, KRI, ผลการตรวจสอบ, หรือรายงานเหตุการณ์) ในการประเมินผลการดำเนินงาน และหากพบว่าผลไม่เป็นไปตามเป้าหมาย มีการนำเสนอผู้บริหารเพื่อพิจารณาปรับปรุงแก้ไขอย่างไร

■ การสอบทานเอกสาร

1. สอบทานรายงานความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เสนอต่อผู้บริหาร เพื่อดูว่ามีการระบุความเชื่อมโยงกับเป้าหมายขององค์กร
2. สอบทานแผนกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์ ว่าได้มีการทบทวนและปรับปรุง โดยสอดคล้องกับผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ในปัจจุบัน
3. สอบทานผลการวัดตามตัวชี้วัด (KPI/KRI) เพื่อตรวจสอบความครบถ้วนถูกต้องของข้อมูล และแนวโน้ม (Trends) ของความเสี่ยง
4. สอบทานบันทึกการประชุมระดับบริหาร หรือ คณะกรรมการ (Board/Management Meeting Minutes) ที่แสดงให้เห็นวาระการพิจารณาผลการดำเนินงานและอนุมัติการปรับปรุงกลยุทธ์

■ เอกสารที่เกี่ยวข้อง

1. รายงานความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2. แผนกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์
3. รายงานการประชุมคณะกรรมการหรือผู้บริหารระดับสูง
4. รายงานตัวชี้วัดประสิทธิภาพและความเสี่ยง (KPI/KRI Reports) หรือ รายงานผลการประเมิน
การดำเนินงาน (Performance Evaluation Reports)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

ส่วนที่ 2 : แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)
การจัดการผู้ให้บริการภายนอก (Third Party Management)
3.2.3 การจัดทำนโยบายและกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์ของห่วงโซ่อุปทาน
วัตถุประสงค์
เพื่อให้มั่นใจว่า หน่วยงานมีกลไกการจัดการความเสี่ยงห่วงโซ่อุปทานที่มีประสิทธิภาพ
ความเสี่ยง
ผู้ไม่หวังดีสามารถใช้ช่องทางเชื่อมต่อหรือสิทธิ์การเข้าถึงของผู้ให้บริการภายนอกเป็นทางผ่านในการเข้าถึงข้อมูลหรือบริการที่สำคัญของหน่วยงานโดยมิชอบ
การควบคุมที่พึงมี
ควรกำหนดนโยบาย กลยุทธ์ กระบวนการ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อจัดการความเสี่ยงที่เกิดจากห่วงโซ่อุปทาน รวมถึงการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ลูกค้า และพันธมิตรทางธุรกิจ โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้ (ก) ประเภทและโพรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile and Type) ของผู้ให้บริการภายนอกที่เข้าถึงทรัพยากรสารสนเทศที่สนับสนุนภารกิจหรือบริการที่สำคัญของหน่วยงาน (ข) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องภารกิจหรือบริการที่สำคัญของหน่วยงาน (ค) ความเสี่ยงและการควบคุมที่เกี่ยวข้องกับภารกิจหรือบริการและห่วงโซ่อุปทานผลิตภัณฑ์ โดยพิจารณาให้ครอบคลุมมิติขององค์กร เทคโนโลยี บุคลากร และสภาพแวดล้อมทางกายภาพ และ (ง) สิทธิ์ของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก
แนวทางการประเมิน
1. ตรวจสอบการจัดทำนโยบาย กลยุทธ์ กระบวนการ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อจัดการความเสี่ยงที่เกิดจากห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management: C-SCRM) ที่ได้รับการอนุมัติและตกลงร่วมกันจากผู้มีส่วนได้ส่วนเสียของหน่วยงาน 2. ตรวจสอบข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ลูกค้า และพันธมิตรทางธุรกิจ ของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญ ว่ามีรายละเอียดสอดคล้องกับนโยบาย กลยุทธ์ กระบวนการ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อจัดการความเสี่ยงที่เกิดจากห่วงโซ่อุปทาน รวมถึงการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญของหน่วยงาน 3. ตรวจสอบข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ลูกค้า และพันธมิตรทางธุรกิจ ของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญ ว่ามีรายละเอียดสอดคล้องการควบคุมที่พึงมีข้อ (ก) - (ง)

4. ตรวจสอบว่ามีการจัดประเภทและโพรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile and Type) ของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินสารสนเทศที่สนับสนุนภารกิจหรือบริการที่สำคัญของหน่วยงาน

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	GV.SC-01
ISO/IEC27001:2022	Clause 8.1, Annex A 5.1, Annex A 5.19, Annex A 5.20, Annex A 5.21, Annex A 5.22
ISO/IEC27701:2025	Clause 8.1, A.3.3, A.3.10
ISO/IEC27017:2015	5.1.1, 15.1.1, 15.1.2, 15.1.3
ISO/IEC27007:2020	A.5.1
ISO/IEC TS 27008:2019	5.1.1, 5.1.2, 15.1.1, 15.1.2, 15.1.3, 15.2.1, 15.2.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ **การสัมภาษณ์**

- องค์กรมีกระบวนการและผู้รับผิดชอบในการร่างนโยบาย กลยุทธ์ และข้อกำหนด C-SCRM อย่างไร และผู้มีส่วนได้ส่วนเสียกลุ่มใดบ้าง (เช่น จัดซื้อ, กฎหมาย, ฝ่ายปฏิบัติการ) ที่เข้าร่วมกันพิจารณาข้อกำหนดให้เหมาะสมกับบริบทของหน่วยงาน
- ฝ่ายกฎหมายหรือฝ่ายจัดซื้อจัดจ้างของหน่วยงาน มีกระบวนการนำข้อกำหนดด้านไซเบอร์บรรจุลงในสัญญาหรือ SLA และมีการตรวจสอบความสอดคล้องกับนโยบาย C-SCRM ก่อนลงนามสัญญาอย่างไร
- ฝ่ายจัดซื้อจัดจ้างของหน่วยงาน มีการนำกระบวนการคัดเลือกและประเมินผู้ขายตามนโยบายการจัดการความเสี่ยงจากห่วงโซ่อุปทานอย่างไร
- เจ้าหน้าที่พัสดุหรือผู้บริหารโครงการ (PM) มีการแจ้งเงื่อนไขด้านความมั่นคงปลอดภัย และสิทธิในการเข้าถึงข้อมูล/ระบบ ให้แก่ผู้ให้บริการภายนอก ลูกค้า หรือพันธมิตร รับทราบล่วงหน้าในขั้นตอนการจัดซื้อจัดจ้าง (เช่น ใน TOR) อย่างไร

■ **การสอบทานเอกสาร**

- สอบทานนโยบาย กลยุทธ์ และกระบวนการบริหารจัดการความเสี่ยงจากห่วงโซ่อุปทาน (C-SCRM Policy & Strategy) ว่ามีการระบุวัตถุประสงค์ ขอบเขต และข้อกำหนดด้านความปลอดภัยในห่วงโซ่อุปทานที่ชัดเจน พร้อมหลักฐานการอนุมัติ (เช่น รายงานการประชุม คณะกรรมการ หรือลายมือชื่อผู้บริหาร)
- สอบทานนโยบายและขั้นตอนด้านการจัดการความเสี่ยงจากห่วงโซ่อุปทาน ว่ามีการกำหนดรอบการปรับปรุง และมีการลงนามอนุมัติอย่างเป็นทางการ
- สอบทานบันทึกผลการดำเนินงานตามกระบวนการ เช่น รายงานการประเมินความเสี่ยงของผู้ขาย เพื่อยืนยันว่าได้ทำตามนโยบายกำหนด

4. สอบทานร่างสัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) เพื่อยืนยันการมีอยู่ของเงื่อนไขบังคับข้อ (ก) ถึง (ง)
5. สอบทานทะเบียนโพรไฟล์ความเสี่ยงของผู้ให้บริการภายนอก เพื่อยืนยันว่ามีรายการครบถ้วนและเป็นปัจจุบัน

■ เอกสารที่เกี่ยวข้อง

1. นโยบาย กลยุทธ์ และกระบวนการบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน
2. นโยบายการจัดซื้อจัดจ้าง
3. สัญญาว่าจ้างและข้อตกลงระดับการให้บริการ (Contract and SLA) ฉบับมาตรฐานและฉบับที่ใช้งานจริง
4. รายงานการประเมินความเสี่ยงของผู้ขาย
5. ทะเบียนโพรไฟล์ความเสี่ยงของผู้ให้บริการภายนอก

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

2. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

การควบคุมการเข้าถึง (Access Control)

3.2.4 การจัดการบัญชีผู้ใช้

วัตถุประสงค์

เพื่อให้มั่นใจว่า การบริหารจัดการบัญชีผู้ใช้และสิทธิ์การเข้าถึง (Identity and Access Management) มีกลไกการพิสูจน์ตัวตน การควบคุมการใช้งานบัญชีร่วม การเฝ้าระวังพฤติกรรมผิดปกติ และการตรวจสอบทบทวนสิทธิ์ให้ถูกต้องและสอดคล้องกับระดับความเสี่ยงของทรัพยากรสารสนเทศ

ความเสี่ยง

บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงบริการที่สำคัญได้

การควบคุมที่พึงมี

การจัดการบัญชีผู้ใช้ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

- (ก) มีการพิสูจน์และตรวจสอบอัตลักษณ์ของบุคคล (Identity Proofing) รวมทั้งผูกข้อมูลอัตลักษณ์กับข้อมูลรับรองการเข้าถึง (Binding Identities to Credentials) ให้เหมาะสมและสอดคล้องกับระดับความเสี่ยงของการใช้งานและทรัพยากรที่เข้าถึง
- (ข) ปกป้องและตรวจสอบความถูกต้องของข้อมูลการยืนยันตัวตน (Identity Assertions) รวมทั้งต้องส่งข้อมูลดังกล่าวผ่านช่องทางที่ปลอดภัย โดยให้สอดคล้องกับระดับความเสี่ยง
- (ค) ตรวจสอบให้แน่ใจว่าไม่มีการสร้างบัญชีผู้ใช้ร่วมกัน ยกเว้นกรณีมีความจำเป็นในด้านการดำเนินการเท่านั้น
- (ง) กำหนดกลไกและกระบวนการในการติดตามกิจกรรมของแต่ละบัญชี รวมถึงรูปแบบพฤติกรรมความผิดปกติ และเพื่อส่งสัญญาณเตือนในการสืบสวนเมื่อตรวจพบความผิดปกติ
- (จ) ลบหรือปิดการใช้งานบัญชีที่ไม่จำเป็นและบัญชีที่ไม่ได้ใช้งาน
- (ฉ) ต้องดำเนินการตรวจสอบเพื่อให้แน่ใจว่าสิทธิ์ที่กำหนดให้กับแต่ละบัญชีถูกต้องอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง

แนวทางการประเมิน

1. ตรวจสอบนโยบายและขั้นตอนการบริหารจัดการอัตลักษณ์และสิทธิ์การเข้าถึง (Identity and Access Management Procedure) ที่เกี่ยวข้องกับบัญชีผู้ใช้ของโปรแกรมประยุกต์ บริการ หรือบัญชีระบบ
2. ตรวจสอบการตั้งค่าระบบหรือสังเกตการณ์หน้าจอการทำงานของระบบบริหารจัดการสิทธิ์ตามข้อ (ก) – (จ)
3. ตรวจสอบประวัติการทบทวนสิทธิ์ที่กำหนดให้กับแต่ละบัญชี ว่าดำเนินการถูกต้องอย่างน้อยปีละ 1 (หนึ่ง) ครั้ง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.AA-01, PR.AA-02
ISO/IEC27001:2022	Annex A 5.16, Annex A 8.2, Annex A 8.3, Annex A 8.5
ISO/IEC27701:2025	A.3.8, A.3.23
ISO/IEC27017:2015	9.2.1, 9.2.3, 9.4.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	9.2.1, 9.2.3, 9.4.1, 9.4.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีขั้นตอนการตรวจสอบว่าบุคคลที่มาขอเปิดบัญชีผู้ใช้คือตัวจริง ก่อนการสร้างบัญชีผู้ใช้ใหม่อย่างไร (เช่น ใช้บัตรประชาชน หรือพาสปอร์ต หรือเอกสารอื่นที่ออกโดยรัฐ หรือการยืนยันตัวตนแบบเห็นหน้า) มีขั้นตอนโดยเฉพาะเมื่อต้องเข้าถึงระบบหรือทรัพยากรที่มีความเสี่ยงสูงหรือไม่ (เช่น มีการตรวจสอบประวัติอาชญากรรมเพิ่มเติม)
2. หน่วยงานมีการกำหนดการยืนยันตัวตนตามระดับความเสี่ยงอย่างไร (เช่น ความเสี่ยงสูง ต้องมีการใช้ MFA)
3. หน่วยงานมีวิธีการส่งข้อมูลยืนยันตัวตน (Identity Assertions) ผ่านโปรโตคอลใด (เช่น HTTPS/TLS 1.2+)
4. มีการอนุญาตให้สร้างบัญชีใช้งานร่วมกัน (Shared Account) หรือไม่ หากมี มีขั้นตอนการพิจารณาความจำเป็นและควบคุมการใช้งานอย่างไร
5. หน่วยงานมีเครื่องมือหรือกลไกใด (เช่น SIEM, Log Monitoring) ในการติดตามกิจกรรมของแต่ละบัญชีเพื่อวิเคราะห์เหตุการณ์ที่ผิดปกติและแจ้งเตือน
6. หน่วยงานมีกระบวนการในการลบ/ปิดบัญชีที่ไม่ได้ใช้งาน และกระบวนการทบทวนสิทธิ์การเข้าถึง (Access Review) อย่างไร

■ การสอบทานเอกสาร

1. สอบทานนโยบายและขั้นตอนการบริหารจัดการอัตลักษณ์และสิทธิ์การเข้าถึง (Identity and Access Management Procedure) ว่ามีการระบุเกณฑ์การพิสูจน์ตัวตน (Identity Proofing) และการผูกตัวตนกับข้อมูลรับรอง (Binding) ตามระดับความเสี่ยงของทรัพยากร
2. สอบทานแบบฟอร์มการขอสิทธิ์และยกเลิกสิทธิ์ที่เกี่ยวข้องกับบัญชีผู้ใช้ของโปรแกรมประยุกต์ บริการ หรือบัญชีระบบ ว่าได้มีการดำเนินการตามนโยบายและขั้นตอนที่กำหนด
3. สอบทานแบบฟอร์มการขออนุมัติใช้งานบัญชีร่วม (Shared Account Request) และเหตุผลความจำเป็นที่ระบุ ว่าได้มีการดำเนินการตามนโยบายและขั้นตอนที่กำหนด
4. สอบทานบันทึกการติดตามเฝ้าระวังบัญชี (Account Activity Logs) และรายงานการแจ้งเตือนความผิดปกติ
5. สอบทานรายงานการทบทวนสิทธิ์ (User Access Review Report) ที่ได้ดำเนินการย้อนหลังไม่เกิน 1 ปี

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการบริหารจัดการอัตลักษณ์และสิทธิ์การเข้าถึง
2. ทะเบียนบัญชีใช้งานโปรแกรมประยุกต์ บริการ หรือบัญชีระบบ
3. บันทึกคำขออนุมัติการใช้บัญชีร่วม
4. รายงานผลการวิเคราะห์แจ้งเตือนพฤติกรรมผิดปกติของบัญชีผู้ใช้จากระบบเฝ้าระวัง
5. รายงานผลการทบทวนสิทธิ์การเข้าถึง (User Access Review Report)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบความเชื่อมโยงของบัญชีผู้ใช้ในระบบ เช่น บัญชีผูกอยู่กับเลขบัตรประชาชนใด หรือพนักงานรหัสใด
2. ตรวจสอบทะเบียนบัญชีใช้งานเพื่อค้นหาบัญชีที่มีลักษณะเป็น Shared Account (เช่น บัญชีชื่อ admin, guest, หรือชื่อแผนก) และตรวจสอบบันทึกการขออนุมัติใช้งานบัญชีร่วม
3. ตรวจสอบ Correlation Rules ในระบบ SIEM หรือ Log Management ว่ามีการตั้งค่าแจ้งเตือนพฤติกรรมผิดปกติ (เช่น Brute Force, Impossible Travel, หรือการยกระดับสิทธิ์สูงขึ้นผิดปกติ)
4. ตรวจสอบว่ามีการตั้งค่าให้บัญชีหมดอายุอัตโนมัติ เทียบกับรายชื่อบัญชีที่ไม่เคยเข้าใช้งานเลย (ดูจากวันเวลาที่ล็อกอินล่าสุด) ว่าเกินกว่าระยะเวลาที่กำหนดไว้หรือไม่ (เช่น เกิน 90 วัน)
5. ตรวจสอบบัญชีของพนักงานที่ลาออกแล้วหรือไม่ได้ใช้แล้ว เพื่อยืนยันว่าได้ถูกระงับสิทธิ์แล้ว

การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

3.2.5 การรักษาความมั่นคงปลอดภัยของข้อมูล

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลครอบคลุมทั้งในขณะจัดเก็บ (Data-at-Rest) ขณะส่งผ่าน (Data-in-Transit) และขณะถูกใช้งาน (Data-in-Use) รวมถึงการบริหารจัดการวงจรชีวิตของข้อมูลผ่านการสำรองข้อมูล การทำลายข้อมูลอย่างปลอดภัย และการควบคุมสื่อเก็บข้อมูลแบบถอดได้

ความเสี่ยง

ข้อมูลสำคัญรั่วไหล ส่งผลให้เกิดความเสียหายต่อหน่วยงาน และเสี่ยงต่อการละเมิดกฎหมายที่เกี่ยวข้อง เช่น กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล

การควบคุมที่พึงมี

การรักษาความมั่นคงปลอดภัยของข้อมูล ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

1. กำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ถูกจัดเก็บ (Data-at-Rest) เช่น การเข้ารหัสข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในอุปกรณ์จัดเก็บข้อมูล
2. กำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะส่งผ่าน (Data-in-Transit) เช่น การส่งข้อมูลจากต้นทางไปยังปลายทางโดยใช้โพรโทคอลการสื่อสารที่มีความมั่นคงปลอดภัย
3. กำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะถูกใช้งาน (Data-in-Use) เช่น การกำหนดสิทธิ์ขั้นต่ำของการเข้าถึงข้อมูลที่กำลังถูกประมวลผลหรือใช้งานโดยระบบหรือผู้ใช้
4. มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลตามข้อ 1, 2 และ 3 ควรเหมาะสมกับระดับความเสี่ยงที่ถูกประเมินไว้ ซึ่งรวมถึงการพิจารณาความเสี่ยงด้านอธิปไตยของข้อมูล (Data Sovereignty) และข้อกำหนดทางกฎหมายของต่างประเทศที่อาจมีผลบังคับใช้นอกอาณาเขต (Extraterritorial Laws) ด้วย
5. มีการจัดเก็บ ป้องกัน ดูแลรักษา และทดสอบข้อมูลสำรอง (Backups of Data)
6. มีการทำลายข้อมูลที่ไม่ได้ใช้แล้วอย่างมั่นคงปลอดภัย ตามลำดับชั้นความลับและประเภทสื่อการจัดเก็บ

แนวทางการประเมิน

1. ตรวจสอบด้านนโยบายและมาตรฐานว่ามีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ถูกจัดเก็บ (Data-at-Rest) มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะส่งผ่าน (Data-in-Transit) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะถูกใช้งาน (Data-in-Use)
2. ประเมินความเหมาะสมของมาตรการ (ตามข้อ 1-3) กับระดับความเสี่ยง เทียบกับความเสี่ยงด้านอธิปไตยของข้อมูล (Data Sovereignty) และข้อกำหนดต่างประเทศ (Extraterritorial Laws)
3. ตรวจสอบว่ามีข้อกำหนดเกี่ยวกับข้อมูลสำรอง เช่น ความถี่ (Frequency) ระยะเวลาการเก็บรักษา (Retention) และการป้องกัน ดูแลรักษา และการเก็บสำรองนอกสถานที่ (Offsite)
4. ตรวจสอบการทำลายข้อมูลที่ไม่ได้ใช้แล้วอย่างมั่นคงปลอดภัย ตามลำดับชั้นความลับและประเภทสื่อ

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11
ISO/IEC27001:2022	Clause 4.2, Clause 5.2, Annex A 5.1, Annex A 5.3, Annex A 5.10, Annex A 5.13, Annex A

	5.14, Annex A 5.15, Annex A 6.1, Annex A 6.2, Annex A 6.5, Annex A 7.7, Annex A 7.10, Annex A 7.14, Annex A 8.2, Annex A 8.3, Annex A 8.4, Annex A 8.7, Annex A 8.8, Annex A 8.10, Annex A 8.13, Annex A 8.17, Annex A 8.19, Annex A 8.20, Annex A 8.22, Annex A 8.26
ISO/IEC27701:2025	Clause 4.2, Clause 5.2, A.3.3, A.3.6, A.3.7, A.3.19, A.3.20, A.3.21, A.3.24, A.3.28
ISO/IEC27017:2015	5.1.1, 8.2.2, 9.1.2, 9.2.3, 9.4.1, 12.3.1, 12.4.4, 12.6.1, 13.1.3
ISO/IEC27007:2020	A.1.2, A.2.2
ISO/IEC TS 27008:2019	5.1.1, 5.1.2, 6.1.2, 7.1.1, 7.1.2, 7.3.1, 8.1.3, 8.2.2, 8.2.3, 8.3.1, 8.3.2, 8.3.3, 9.1.1, 9.2.3, 9.4.1, 9.4.5, 11.2.5, 11.2.7, 11.2.9, 12.2.1, 12.3.1, 12.4.4, 12.5.1, 12.6.1, 12.6.2, 13.1.1, 13.1.3, 13.2.1, 13.2.2, 13.2.3, 14.1.3, 14.2.2, 14.2.3
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีมาตรการปกป้องข้อมูลทั้งขณะจัดเก็บ (Data-at-Rest) ส่งผ่าน (Data-in-Transit) และใช้งาน (Data-in-Use) อย่างไร
2. หน่วยงานได้นำเรื่องอธิปไตยข้อมูล (ข้อมูลต้องอยู่ภายใต้กฎหมายของประเทศที่ข้อมูลนั้นถูกประมวลผลหรือจัดเก็บ) หรือกฎหมายต่างประเทศมาพิจารณาความเสี่ยงด้วยหรือไม่ (เช่น เขตอำนาจศาลของผู้ให้บริการ Cloud หรือกฎหมายต่างประเทศที่บังคับให้ผู้ให้บริการต้องส่งมอบข้อมูลให้รัฐบาลนั้น ๆ)
3. หน่วยงานมีเกณฑ์ที่ใช้ในการจัดชั้นความลับของข้อมูล และวิธีการเลือกใช้เทคโนโลยีรักษาความลับ (เช่น การเข้ารหัส) ให้เหมาะสมกับชั้นความลับนั้น ๆ อย่างไร
4. หน่วยงานมีกระบวนการติดตามข้อมูลที่ครบกำหนดตามนโยบายการเก็บรักษาข้อมูล (Retention) หรือไม่ และหน่วยงานมีวิธีการระบุและคัดแยกข้อมูลที่หมดความจำเป็นออกจากระบบจัดเก็บหลักอย่างไร
5. แผนการสำรองข้อมูล (Backup) และการนำข้อมูลสำรองมาทดสอบกู้คืน (Restore Test) มีกระบวนการและรอบเวลาอย่างไร
6. หน่วยงานมีกระบวนการทำลายข้อมูลและอุปกรณ์ที่ไม่ได้ใช้แล้ว (Secure Disposal) อย่างไรให้สอดคล้องกับชั้นความลับของข้อมูล และมีวิธีการตรวจสอบอย่างไรว่าข้อมูลไม่สามารถกู้คืนกลับมาได้อีก

■ การสอบทานเอกสาร

1. สอบทานนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล ว่าครอบคลุม Data-at-Rest, in-Transit, in-Use
2. สอบทานรายงานประเมินความเสี่ยง เพื่อยืนยันว่าได้ครอบคลุมประเด็นข้อบังคับทางกฎหมาย เรื่องที่ตั้งและการจัดเก็บข้อมูล
3. สอบทาน นโยบายด้านระยะเวลาการเก็บรักษา (Retention) ว่าครอบคลุมทั้งข้อมูล อิเล็กทรอนิกส์และเอกสารกระดาษ รวมถึงสอดคล้องกับข้อกำหนดทางกฎหมาย (เช่น PDPA หรือกฎหมายเฉพาะภาคส่วน)
4. สอบทาน แผนการสำรอง/กู้คืนข้อมูล เทียบกับ รายงานผลการทดสอบ เพื่อยืนยันว่ามีการซ้อม กู้คืนจริงตามรอบเวลาที่กำหนด และผลการกู้คืนประสบความสำเร็จ
5. สอบทาน แนวทางหรือขั้นตอนในการทำลายข้อมูล เพื่อดูความเหมาะสมของวิธีการทำลายในแต่ละระดับความสำคัญ
6. ตรวจสอบรายงานผลการทำลายว่ามีรายละเอียดครบถ้วน (เช่น วันที่ทำลาย, วิธีการ, รายการ ข้อมูลที่ทำลาย, และพยานผู้ตรวจสอบ) เพื่อยืนยันว่าและอุปกรณ์ที่ไม่ได้ใช้แล้ว ถูกทำลาย อย่างถูกต้องตามมาตรฐาน

■ เอกสารที่เกี่ยวข้อง

1. นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล
2. นโยบายการจัดชั้นความลับของข้อมูล
3. นโยบายด้านระยะเวลาการเก็บรักษา (Retention)
4. แผนและรายงานผลการทดสอบการสำรอง/กู้คืนข้อมูล
5. แนวทางหรือขั้นตอนในการทำลายข้อมูลและอุปกรณ์ที่ไม่ได้ใช้แล้ว และผลรับรองการทำลาย

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

3.2.6 การจัดการแพตช์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีระบบการจัดการแพตช์ความมั่นคงปลอดภัย (Patch Management) ที่มี ประสิทธิภาพ โดยเน้นการติดตามและติดตั้งแพตช์ตามลำดับความสำคัญของความเสี่ยงอย่างทันทั่วทั้งที่ พร้อมทั้งมีการทดสอบความสมบูรณ์ก่อนใช้งาน การกำหนดมาตรการควบคุมขดเซกกรณิไม่สามารถติดตั้ง แพตช์ได้ และมีแผนการย้อนกลับ (Roll Back)

ความเสี่ยง

การให้บริการสำคัญหยุดชะงัก หรือถูกจารกรรมข้อมูลผ่านจุดอ่อนที่ยังไม่ได้รับการแก้ไข

การควบคุมที่พึงมี

การตามกระบวนการจัดการความมั่นคงปลอดภัยแพตช์ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้
(ก) การจัดลำดับความสำคัญของการใช้แพตช์ความมั่นคงปลอดภัยโดยพิจารณาจากระดับความ เสี่ยงที่มีผลต่อการดำเนินงานของหน่วยงาน

- (ข) การติดตามการเผยแพร่แพตช์ความมั่นคงปลอดภัยที่เกี่ยวข้องตามรายการทรัพย์สิน
- (ค) การใช้แพตช์ความมั่นคงปลอดภัยอย่างทันท่วงทีเพื่อลดช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะช่องโหว่ความเสี่ยงสูงที่เปิดเผยโดยผู้ผลิตอุปกรณ์ดั้งเดิม (OEM) หรือผู้ให้บริการภายนอก ทั้งนี้ ต้องมีการตรวจสอบและทดสอบแพตช์เพื่อให้มั่นใจว่าแพตช์มีความสมบูรณ์ก่อนการใช้งาน
- (ง) การใช้มาตรการควบคุมแบบชดเชย (Compensating Controls) ในกรณีที่ไม่สามารถใช้แพตช์ความมั่นคงปลอดภัยได้
- (จ) การย้อนกลับ (Roll Back) การใช้แพตช์ความมั่นคงปลอดภัยหากจำเป็น

แนวทางการประเมิน

1. ตรวจสอบว่ามีกระบวนการจัดการความมั่นคงปลอดภัยแพตช์มีรายละเอียดอย่างน้อย (ก) – (จ)
2. ตรวจสอบหลักฐานการปฏิบัติงานที่เกี่ยวข้อง เช่น รายงานการสแกนช่องโหว่ (Vulnerability Scan Report) บันทึกการขออนุมัติการเปลี่ยนแปลง (Change Request) หน้าจอการตั้งค่า (Configuration) ของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่าย
3. ตรวจสอบหลักฐานการจัดการในกรณีที่ระบบไม่สามารถลงแพตช์ได้ ว่ามีการระบุมาตรการชดเชยไว้จริง
4. ตรวจสอบว่ามีการกำหนดกระบวนการย้อนกลับ (Roll Back)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.PS-02
ISO/IEC27001:2022	Annex A 5.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	8.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 8.1.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีเกณฑ์การจัดลำดับความสำคัญของแพตช์อย่างไร และมีการกำหนดกรอบเวลาที่ต่างกันอย่างไรระหว่างกรณีเร่งด่วน (Emergency) กับกรณีปกติ
2. ปัจจุบันหน่วยงานมีช่องทางหรือกระบวนการอย่างไรในการติดตามข่าวสารการประกาศแพตช์ใหม่ ๆ จากผู้ผลิตให้ครอบคลุมทุกอุปกรณ์และซอฟต์แวร์ในบัญชีทรัพย์สิน
3. ก่อนที่แพตช์จะถูกนำไปติดตั้งบนระบบการให้บริการจริง (Production) มีขั้นตอนการตรวจสอบและทดสอบ (Testing) เพื่อป้องกันผลกระทบข้างเคียงอย่างไร

4. หากระบบเป็นระบบเก่า หรือซอฟต์แวร์ผู้ผลิตไม่สามารถปรับปรุงแพตช์ได้ องค์กรมีมาตรการชดเชย (Compensating Controls) เช่น การปิดพอร์ต การเพิ่มไฟร์วอลล์เพื่อแยกส่วนระบบอย่างไร
5. มีการกำหนดขั้นตอนในการย้อนกลับ (Roll Back) ระบบให้กลับไปสู่สถานะก่อนหน้าอย่างไร หากแพตช์ที่ติดตั้งทำให้ระบบเกิดความขัดข้องหรือหยุดทำงาน

■ การสอบทานเอกสาร

1. สอบทานนโยบายและขั้นตอนการจัดการแพตช์ (Patch Management) ว่ามีรายละเอียดอย่างน้อย (ก) – (จ)
2. สอบทานรายงานการสแกนช่องโหว่ (Vulnerability Scan Report) เพื่อยืนยันว่ามีการติดตามแพตช์ที่เกี่ยวข้องจริง
3. สอบทานใบคำขออนุมัติการเปลี่ยนแปลง (Change Request) ที่ระบุผลการทดสอบแพตช์ในระบบ Test/UAT ก่อนติดตั้งจริง
4. สอบทานเอกสารแผนการย้อนกลับ (Rollback Plan) ที่แนบมากับ Change Request
5. สอบทานบันทึกการประเมินความเสี่ยงและมาตรการชดเชย (Compensating Controls) สำหรับระบบที่ไม่ได้ปรับปรุงแพตช์
6. สอบทานรายงานสรุปผลการจัดการแพตช์ เพื่อดูสัดส่วนจำนวนอุปกรณ์ที่ได้รับการอัปเดตแพตช์สำเร็จเทียบกับทั้งหมด

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการจัดการแพตช์ (Patch Management)
2. รายงานผลการสแกนช่องโหว่ (Vulnerability Scan Report)
3. ใบคำขออนุมัติการเปลี่ยนแปลง (Change Request)
4. รายงานการติดตั้งแพตช์ (Patch Compliance Report)
5. บันทึกการยอมรับความเสี่ยงและการใช้มาตรการชดเชย
6. รายงานสรุปผลการจัดการแพตช์

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบหน้าจอการตั้งค่า (Configuration) ของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายเพื่อยืนยันว่าแพตช์เป็นปัจจุบัน

3.2.7 การจัดการซอฟต์แวร์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการจัดการความมั่นคงปลอดภัยซอฟต์แวร์ (Software Management) ที่ครอบคลุมการควบคุมรายการซอฟต์แวร์อนุญาต (Authorized Software List) การตรวจสอบความถูกต้องครบถ้วน (Integrity) ก่อนใช้งาน และการแยกชั้นสถาปัตยกรรมระบบเพื่อความปลอดภัย รวมถึงการบริหารจัดการซอฟต์แวร์ที่สิ้นสุดการสนับสนุน (EoL/EoS)

ความเสี่ยง

มีการแพร่กระจายของมัลแวร์ผ่านการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต หรือถูกโจมตีผ่านช่องโหว่ของซอฟต์แวร์ รวมถึงความเสี่ยงทางกฎหมายจากการละเมิดลิขสิทธิ์ซอฟต์แวร์

การควบคุมที่พึงมี

การจัดการความมั่นคงปลอดภัยซอฟต์แวร์ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

- (ก) การกำหนดกระบวนการพิจารณาอนุญาตซอฟต์แวร์และการจัดเก็บรายการซอฟต์แวร์ที่ได้รับอนุญาต เพื่อให้มั่นใจว่าซอฟต์แวร์ที่มีความจำเป็นต้องใช้งานของหน่วยงานและการดูแลด้านความมั่นคงปลอดภัยเป็นซอฟต์แวร์ที่ได้รับอนุญาต พร้อมทั้งดูแลให้รายการซอฟต์แวร์ดังกล่าวเป็นปัจจุบัน
- (ข) ทบทวนรายการซอฟต์แวร์ที่ได้รับอนุญาต อย่างน้อยทุก 1 ปี ทั้งนี้ การตรวจสอบครั้งแรกต้องดำเนินการให้แล้วเสร็จภายใน 1 ปี จากเวลาที่สร้างรายการซอฟต์แวร์
- (ค) ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของซอฟต์แวร์ก่อนนำไปใช้งานเช่น การตรวจสอบแหล่งที่ Download (Provenance) และค่าแฮช (Hash) ของซอฟต์แวร์
- (ง) ตรวจสอบให้มั่นใจว่าคอมพิวเตอร์และดีบั๊กเกอร์จะถูกใช้เฉพาะในกรณีที่จำเป็นและเฉพาะบนอุปกรณ์ที่ได้รับอนุญาตเท่านั้น
- (จ) หากสามารถกระทำได้ ต้องแยกชั้นแอปพลิเคชันและชั้นฐานข้อมูลออกจากกันและทำการควบคุมความมั่นคงปลอดภัยในแต่ละชั้น
- (ฉ) การจัดการซอฟต์แวร์ที่สิ้นสุดอายุการใช้งาน (EoL) หรือสิ้นสุดการสนับสนุน (EoS) เพื่อบรรเทาความเสี่ยงจากช่องโหว่ที่ผู้ผลิตอุปกรณ์ดั้งเดิมหรือผู้ให้บริการภายนอกไม่สนับสนุนหรือแก้ไขให้แล้ว

แนวทางการประเมิน

1. ตรวจสอบว่ามีกระบวนการจัดการความมั่นคงปลอดภัยซอฟต์แวร์ที่มีรายละเอียดอย่างน้อย (ก) – (ฉ)
2. ตรวจสอบว่ามีนโยบายการใช้งานซอฟต์แวร์ และข้อกำหนดการห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต
3. ตรวจสอบบัญชีรายชื่อซอฟต์แวร์ (Inventory) มีความจำเป็นต้องใช้งานของหน่วยงาน และทบทวนรายการซอฟต์แวร์ที่ได้รับอนุญาต อย่างน้อยทุก 1 ปี
4. ตรวจสอบหลักฐานการตรวจสอบความถูกต้อง (Integrity) ของซอฟต์แวร์ก่อนติดตั้ง เช่น บันทึกการตรวจสอบค่า Hash หรือการยืนยันแหล่งที่มาที่เชื่อถือได้
5. ตรวจสอบการตั้งค่าระบบ (Configuration) บนเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์สำคัญ เพื่อยืนยันว่าไม่มีการติดตั้ง Compiler หรือ Debugger โดยไม่จำเป็น
6. ตรวจสอบผังโครงสร้างระบบ (Network/System Diagram) และการตั้งค่าการควบคุมการเข้าถึง เพื่อยืนยันการแยกชั้น (Isolation) ระหว่างแอปพลิเคชันและฐานข้อมูล
7. ตรวจสอบแผนการรองรับสำหรับซอฟต์แวร์ที่สิ้นสุดอายุการใช้งาน (EoL) หรือสิ้นสุดการสนับสนุน (EoS) รวมถึงขั้นตอนการเปลี่ยนทดแทน
8. ตรวจสอบกระบวนการและหลักฐานการขออนุมัติใช้งานซอฟต์แวร์ที่ไม่เป็นไปตามนโยบายที่กำหนด

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.PS-02, PR.PS-05

ISO/IEC27001:2022	Annex A 5.9, Annex A 8.19
ISO/IEC27701:2025	-
ISO/IEC27017:2015	8.1.1, 12.6.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 8.1.2, 12.5.1, 12.6.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีขั้นตอนการพิจารณาและอนุมัติซอฟต์แวร์ก่อนนำมาติดตั้งใช้งานอย่างไร และใครเป็นผู้ดูแลรายการซอฟต์แวร์ที่อนุญาต (Authorized Software List) 2. มีกระบวนการตรวจสอบความถูกต้องและแหล่งที่มา (เช่น ตรวจสอบ Hash/Digital Signature) ของซอฟต์แวร์ก่อนติดตั้งอย่างไร 3. หน่วยงานมีนโยบายห้ามติดตั้งเครื่องมือพัฒนาโปรแกรม (เช่น Compiler/Debugger) บนระบบโปรดักชัน (Production) อย่างไร และหากจำเป็นต้องใช้ มีการควบคุมอย่างไร 4. ระบบงานสำคัญมีการออกแบบแยกชั้น (Tier Separation) ระหว่างแอปพลิเคชันและฐานข้อมูลอย่างไร และมีการควบคุมความปลอดภัยในแต่ละชั้นผ่านกลไกใด (เช่น Firewall, VLAN, ACL) 5. เมื่อซอฟต์แวร์เข้าสู่สถานะ EoL หรือ EoS หน่วยงานมีแผนการเปลี่ยนทดแทนอย่างไร และหากยังไม่สามารถเปลี่ยนได้ทันที มีมาตรการชดเชยความเสี่ยงอย่างไร ■ การสอบทานเอกสาร 1. สอบทานนโยบายการใช้งานซอฟต์แวร์ (Acceptable Use Policy) และขั้นตอนการจัดการซอฟต์แวร์ ว่าครอบคลุมข้อกำหนด (ก) – (ฉ) 2. สอบทานทะเบียนรายการซอฟต์แวร์ที่ได้รับอนุญาต (Authorized Software List) และรายงานประวัติการทบทวนรอบ 1 ปี 3. สอบทานแผนภาพสถาปัตยกรรมระบบ (System Architecture) เพื่อตรวจสอบการแยกชั้น (Multi-tier Architecture) 4. สอบทานทะเบียนความเสี่ยงและแผนการจัดการซอฟต์แวร์ EoL/EoS รวมถึงบันทึกการประเมินความเสี่ยงและมาตรการชดเชย (Compensating Controls) ■ เอกสารที่เกี่ยวข้อง 1. นโยบายการบริหารจัดการซอฟต์แวร์ (Software Management Policy) 2. ทะเบียนรายการซอฟต์แวร์ที่อนุญาต/ไม่อนุญาต (Authorized/Unauthorized Software Inventory) 3. รายงานการทบทวนรายการซอฟต์แวร์ประจำปี 4. บันทึกการตรวจสอบค่า Hash หรือการตรวจสอบแหล่งที่มาของซอฟต์แวร์สำคัญก่อนติดตั้ง 5. แผนภาพสถาปัตยกรรมระบบ (Architecture Diagram) 6. แผนการจัดการซอฟต์แวร์ EoL/EoS 7. ทะเบียนบันทึกรายการข้อยกเว้น (Security Exception Log)	

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบซอฟต์แวร์ที่ติดตั้งในระบบงานสำคัญ เปรียบเทียบค่า Hash กับค่าที่ระบุโดยผู้ผลิต (Official Hash) เพื่อยืนยันว่าไม่มีการถูกดัดแปลง
2. ตรวจสอบหน้าจอการตั้งค่าหรือใช้คำสั่ง (Commands) บนเครื่องแม่ข่าย เพื่อยืนยันว่าไม่มี Compiler/Debugger ติดตั้งอยู่บนเครื่องที่ไม่ได้รับอนุญาต
3. ตรวจสอบรายชื่อซอฟต์แวร์ที่ติดตั้งจริงมาเปรียบเทียบกับบัญชีรายชื่อที่ได้รับอนุญาตเพื่อหาซอฟต์แวร์แปลกปลอม

3.2.8 การจัดการฮาร์ดแวร์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีการจัดการความมั่นคงปลอดภัยฮาร์ดแวร์ (Hardware Management) ที่ครอบคลุมการบำรุงรักษาตามวงจร และการทำลายอุปกรณ์ที่ถูกถอดถอนออกจากระบบอย่างปลอดภัย

ความเสี่ยง

บริการสำคัญหยุดชะงักจากการชำรุดของอุปกรณ์ หรือเกิดการรั่วไหลของข้อมูลผ่านอุปกรณ์ที่ถูกทิ้งทำลายอย่างไม่ถูกวิธี

การควบคุมที่พึงมี

การจัดการความมั่นคงปลอดภัยฮาร์ดแวร์ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

- (ก) การบำรุงรักษาฮาร์ดแวร์ เช่น การตรวจสอบและซ่อมบำรุงตามรอบการตรวจสอบความพร้อมใช้งานของอุปกรณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- (ข) การจัดการอุปกรณ์ที่สิ้นสุดการรับประกันหรือสิ้นสุดการผลิตและขาย (End-of-Life) หรือสิ้นสุดการสนับสนุน (End-of-Support)
- (ค) การทำลายอุปกรณ์ที่ถูกถอดถอนออกจากระบบ

แนวทางการประเมิน

1. ตรวจสอบว่ามีกระบวนการจัดการความมั่นคงปลอดภัยฮาร์ดแวร์ที่มีรายละเอียดอย่างน้อย (ก) – (ค)
2. ตรวจสอบการแผนการบำรุงรักษาฮาร์ดแวร์ (Hardware Maintenance) เช่น มีการตรวจสอบและซ่อมบำรุงตามรอบ
3. ประเมินกระบวนการบริหารจัดการอุปกรณ์ที่สิ้นสุดการรับประกัน สิ้นสุดการผลิตและขาย (End-of-Life: EoL) หรือสิ้นสุดการสนับสนุน (End-of-Support: EoS)
4. ตรวจสอบกระบวนการทำลายอุปกรณ์ที่ถูกถอดถอนออกจากระบบ (Secure Disposal)

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.PS-03
ISO/IEC27001:2022	Annex A 5.9
ISO/IEC27701:2025	-
ISO/IEC27017:2015	8.1.1

ISO/IEC 27007:2020	-
ISO/IEC TS 27008:2019	8.1.1, 8.1.2
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีการจัดทำแผนบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) สำหรับฮาร์ดแวร์และอุปกรณ์ด้านความปลอดภัยไซเบอร์อย่างไร และมีรอบการตรวจสอบความพร้อมใช้งานบ่อยเพียงใด 2. เมื่ออุปกรณ์เข้าสู่สภาวะ EoL/EoS หน่วยงานมีขั้นตอนการพิจารณาความเสี่ยงอย่างไร และมีเกณฑ์การตัดสินใจอย่างไรในการจัดหาอุปกรณ์ทดแทนหรือการใช้งานต่อภายใต้มาตรการชดเชย 3. เมื่อฮาร์ดแวร์ถูกถอดออกจากระบบ หน่วยงานมีวิธีการมั่นใจได้อย่างไรว่าข้อมูลที่ตกค้างในสื่อบันทึกข้อมูลถูกทำลายอย่างถาวรก่อนนำอุปกรณ์ออกไปทิ้งหรือทำลายทางกายภาพ ■ การสอบทานเอกสาร 1. สอบทาน นโยบายการบริหารจัดการทรัพย์สิน (Asset Management Policy) ที่ครอบคลุมการบำรุงรักษาและการทำลายอุปกรณ์ตามข้อกำหนด (ก) – (ค) 2. สอบทาน Maintenance Logs หรือ PM Reports ย้อนหลัง 1 ปี เพื่อยืนยันว่ามีการตรวจสอบอุปกรณ์ตามรอบที่กำหนดจริง 3. สอบทานทะเบียนทรัพย์สินฮาร์ดแวร์ (Asset Inventory) เพื่อดูข้อมูลวันหมดการรับประกัน (Warranty Expire) และสถานการณ์สนับสนุน (Support Status) ของอุปกรณ์สำคัญ 4. สอบทานขั้นตอนการทำลายอุปกรณ์/สื่อจัดเก็บข้อมูล และหลักฐานการทำลาย 5. สอบทานทะเบียนความเสี่ยงและแผนการจัดการฮาร์ดแวร์ EoL/EoS รวมถึงบันทึกการประเมินความเสี่ยงและมาตรการชดเชย (Compensating Controls) ■ เอกสารที่เกี่ยวข้อง 1. แผนการบำรุงรักษาฮาร์ดแวร์ประจำปี 2. ทะเบียนทรัพย์สิน (Asset Inventory) 3. รายงานและบันทึกการบำรุงรักษาอุปกรณ์ (Equipment Maintenance) 4. รายงานการทำลายอุปกรณ์/สื่อจัดเก็บข้อมูล 5. แผนการจัดการฮาร์ดแวร์ EoL/EoS ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค 1. ตรวจสอบอุปกรณ์จริงว่า Serial Number ตรงกับที่ระบุในบัญชีทรัพย์สินหรือไม่ 2. ตรวจสอบอุปกรณ์จริงสังเกตสภาพภายนอกทั่วไป การดูแลรักษา อายุการใช้งาน 3. ตรวจสอบอุปกรณ์ที่รอการทำลาย ว่ามีการติดป้ายสถานะชัดเจน และสื่อบันทึกข้อมูลถูกถอดแยกออกมาเพื่อรอการทำลายข้อมูลตามมาตรฐานความปลอดภัย	

3.2.9 การจัดการบันทึกเหตุการณ์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีระบบการจัดการบันทึกเหตุการณ์ (Log Management) ที่ครอบคลุมการจับเก็บข้อมูลจราจรจากอุปกรณ์เครือข่ายและบริการสำคัญ รวมถึงการตรวจสอบบันทึกการเข้าถึงเพื่อเฝ้าระวังพฤติกรรมผิดปกติอย่างสม่ำเสมอตามระดับความเสี่ยง

ความเสี่ยง

ไม่สามารถตรวจพบและยับยั้งภัยคุกคามที่เกิดขึ้นในระบบได้ทันทั่วทั้งที่

การควบคุมที่พึงมี

การจัดการบันทึกเหตุการณ์ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

- (ก) สร้างและจัดเก็บบันทึกเหตุการณ์ของอุปกรณ์และบริการต่อไปนี้ Network Firewall, Domain Name System (DNS), Web Proxy และ Network Intrusion Detection/Prevention System (NIDS/NIPS) และ
- (ข) ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงานและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

แนวทางการประเมิน

1. ตรวจสอบการสร้างและจัดเก็บบันทึกเหตุการณ์ (Event Logs) ของอุปกรณ์และบริการที่กำหนดอย่างครบถ้วน ได้แก่ Network Firewall, Domain Name System (DNS), Web Proxy และ Network Intrusion Detection/Prevention System (NIDS/NIPS)
2. ตรวจสอบหลักฐานการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน (ทั้งกรณีสำเร็จและล้มเหลว)
3. ตรวจสอบความสม่ำเสมอ/ความถี่ในการตรวจสอบบันทึกเหตุการณ์

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.PS-04
ISO/IEC27001:2022	Annex A 8.15, Annex A 8.17
ISO/IEC27701:2025	A.3.25
ISO/IEC27017:2015	12.4.4
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.4.1, 12.4.2, 12.4.3, 12.4.4
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. หน่วยงานมีเกณฑ์อย่างไรในการเลือกจัดเก็บ Log จากอุปกรณ์ต่าง ๆ และมั่นใจได้อย่างไรว่าครอบคลุมจุดสำคัญตามข้อ (ก)
2. ปัจจุบันมีการกำหนดความถี่ในการตรวจสอบ Log การเข้าถึงบริการสำคัญอย่างไร และใช้เครื่องมือใดในการช่วยวิเคราะห์พฤติกรรมที่ผิดปกติ

3. เมื่อตรวจพบพฤติกรรมที่ผิดปกติจาก Log (เช่น ความพยายามเข้าถึงที่น่าสงสัย) หน่วยงานมีขั้นตอนการแจ้งเตือนและการดำเนินการต่อไปอย่างไร
4. หน่วยงานมีความถี่ในการสำรองข้อมูล Log อย่างไร
5. หน่วยงานมีการควบคุมการเข้าถึงและป้องกันการแก้ไข Log อย่างไร

■ การสอบทานเอกสาร

1. สอบทานว่ามีกระบวนการและระบบการจัดเก็บ Log ที่ครอบคลุม (ก) – (ข)
2. สอบทานรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report) แสดงว่ามีการวิเคราะห์และรายงานพฤติกรรมผิดปกติให้ผู้มีอำนาจทราบ

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการบริหารจัดการ Log (Log Management Policy and Procedure)
2. บันทึกการตรวจสอบ Log ประจำวัน/สัปดาห์
3. รายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report)
4. แผนผังการไหลของข้อมูล Log (Log Flow Diagram) จากอุปกรณ์ต่าง ๆ ไปยังระบบจัดเก็บส่วนกลาง (Centralized Log/SIEM Architecture)
5. รายชื่อบัญชีผู้ใช้ที่มีสิทธิ์เข้าถึงระบบ Log
6. ตัวอย่างหน้าจอการตั้งค่า Alert Rules สำหรับตรวจจับกิจกรรมผิดปกติ
7. หลักฐานการสำรองข้อมูล Log

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบว่ามีการส่ง Log จากอุปกรณ์ Network Firewall, DNS, Web Proxy และ NIDS/NIPS เข้าสู่ระบบจัดเก็บส่วนกลาง (Centralized Log Management/SIEM)
2. ตรวจสอบว่ามีการกำหนดระยะเวลาการเก็บรักษา Log ที่สอดคล้องกับกฎหมาย (เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์) และความสำคัญของระบบ
3. ตรวจสอบ Log ของระบบสำคัญ (Critical Services) เพื่อยืนยันว่ามีการบันทึกข้อมูลการเข้าถึงทั้งหมด (All Access) และความพยายามในการเข้าถึง (Access Attempts) ทั้งที่สำเร็จและไม่สำเร็จ
4. เรียกดู Log ย้อนหลังตามระยะเวลาที่นโยบายกำหนด (เช่น 90 วัน) เพื่อยืนยันว่าข้อมูลไม่ได้ถูกลบทิ้งก่อนกำหนด
5. ตรวจสอบว่าบันทึกเหตุการณ์ถูกป้องกันการแก้ไข (Integrity) และจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่เกี่ยวข้องเท่านั้น
6. ตรวจสอบการตั้งค่าเงื่อนไข (Rules/Use Cases) ในการตรวจจับกิจกรรมที่ผิดปกติ เช่น การพยายามเดารหัสผ่าน (Brute Force) หรือการเชื่อมต่อจาก IP ที่เป็นอันตราย
7. ตรวจสอบว่ามีพื้นที่จัดเก็บเพียงพอ และมีนโยบายการเก็บรักษา (Retention Period) ที่สอดคล้องกับกฎหมาย เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือ PDPA
8. ตรวจสอบว่าอุปกรณ์ทุกตัวตั้งค่าเวลาที่ถูกต้อง หรือมีการใช้ NTP (Network Time Protocol)

3.2.10 การพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย (Secure SDLC) ครอบคลุม ตั้งแต่การประเมินความเสี่ยง การกำหนดข้อกำหนดด้านความปลอดภัย การพัฒนาด้วยแนวทาง Secure Coding การแยกสภาพแวดล้อมระบบ การทดสอบก่อนใช้งาน ตลอดจนการเฝ้าระวังและการทำลายข้อมูล อย่างปลอดภัยเมื่อเลิกใช้งาน

ความเสี่ยง

ซอฟต์แวร์ถูกโจมตีจากช่องโหว่ที่เกิดจากการพัฒนาไม่เหมาะสม เช่น Injection หรือ Broken Access Control

การควบคุมที่พึงมี

การพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย (Secured Software Development) ควรดำเนินการอย่างน้อย ดังนี้

- (ก) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของโครงการ (Security Risk Assessment)
- (ข) กำหนดข้อกำหนดของโครงการ (Terms of Reference) โดยคำนึงถึงปัจจัยความมั่นคง ปลอดภัยทางไซเบอร์
- (ค) ออกแบบและพัฒนา (Design and Development) โดยคำนึงถึงความมั่นคงปลอดภัยทางไซ เบอร์ เช่น การใช้แนวทางการเขียนโค้ดปลอดภัย (Secure Coding) การแบ่งแยกสภาพแวดล้อม สำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน
- (ง) ทดสอบระบบและตรวจสอบความสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ ก่อนนำไปใช้งาน
- (จ) บำรุงรักษาและเฝ้าระวังการเข้าถึงข้อมูล การใช้งานระบบ และกิจกรรมที่ผิดปกติ
- (ฉ) เมื่อเลิกใช้งาน (Disposal) ให้ทำลายข้อมูลสำคัญอย่างปลอดภัย

แนวทางการประเมิน

1. ตรวจสอบว่ามีกระบวนการพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย ที่มีรายละเอียด ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ฉ)
2. ตรวจสอบหลักฐานการปฏิบัติงานที่เกี่ยวข้อง เช่น รายงานการประเมินความเสี่ยงด้านความ มั่นคงปลอดภัยของโครงการ (Security Risk Assessment) ก่อนเริ่มพัฒนา TOR หรือสัญญา จ้างมีการระบุข้อกำหนดด้านความปลอดภัย (Security Requirements)
3. ตรวจสอบสถาปัตยกรรมระบบ (System Architecture) การแบ่งแยกสภาพแวดล้อม (Environment Isolation) สำหรับการพัฒนา (Development) การทดสอบ (Test) และการ ให้บริการ (Production)
4. ตรวจสอบรายงานการทดสอบความปลอดภัย เช่น ผลการสแกนโค้ด (SAST/DAST) หรือ รายงานการทดสอบเจาะระบบ (Penetration Testing)
5. ตรวจสอบการตั้งค่า Log และระบบ Monitoring ของซอฟต์แวร์ว่าสามารถตรวจจับกิจกรรมที่ ผิดปกติได้สอดคล้องกับความเสี่ยงของระบบ
6. ตรวจสอบกระบวนการเมื่อสิ้นสุดโครงการหรือเลิกใช้งานซอฟต์แวร์ว่ามีขั้นตอนการล้างข้อมูล ในฐานข้อมูลหรือการลบสิทธิ์การเข้าถึงอย่างปลอดภัย

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

-

แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.PS-06
ISO/IEC27001:2022	Annex A 8.25, Annex A 8.28, Annex A 8.31, Annex A 8.33
ISO/IEC27701:2025	A.3.27, A.3.31
ISO/IEC27017:2015	14.2.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.1.4, 14.1.2, 14.2.1, 14.2.6, 14.3.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ก่อนเริ่มต้นโครงการพัฒนาหรือจัดหาซอฟต์แวร์ หน่วยงานมีการประเมินความเสี่ยงและนำปัจจัยด้านความมั่นคงปลอดภัยไประบุใน TOR อย่างไร 2. ในขั้นตอนการเริ่มโครงการ หน่วยงานมีกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร และผลลัพธ์จากรายงานการประเมินความเสี่ยงนั้นถูกนำไปเขียนเป็นข้อกำหนดใน TOR หรือสัญญาจ้างอย่างไร 3. ในกรณีที่มีการจ้างงานภายนอก (Outsource) หน่วยงานมีการกำหนดเกณฑ์การคัดเลือกหรือข้อตกลงระดับการให้บริการ (SLA) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ไว้อย่างไร 4. ผู้พัฒนาซอฟต์แวร์ (ทั้งภายในและ Outsource) ได้รับการฝึกอบรมหรือปฏิบัติตามแนวทางการเขียนโค้ดที่ปลอดภัย (Secure Coding) หรือไม่ อย่างไร 5. ข้อมูลที่ใช้ในการทดสอบระบบ (UAT/Test) นำมาจากแหล่งใด มีการนำข้อมูลจริงจากระบบที่ให้บริการจริงหรือไม่ 6. หากจำเป็นต้องใช้ข้อมูลจากระบบที่ให้บริการจริงมาทดสอบ หน่วยงานมีกระบวนการทำ Data Masking, Anonymization หรือ Sanitization อย่างไร เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคล (PII) หรือข้อมูลความลับจะไม่หลุดออกไป 7. สิทธิ์ในการเข้าถึงข้อมูลทดสอบต่างจากข้อมูลบนระบบที่ให้บริการจริงอย่างไร และผู้พัฒนาซอฟต์แวร์ มีสิทธิ์เข้าถึงข้อมูลทดสอบที่มีความอ่อนไหวหรือไม่ 8. หน่วยงานมีมาตรการทางเทคนิคอย่างไรในการแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน 9. เมื่อเสร็จสิ้นกระบวนการทดสอบในแต่ละรอบ มีการจัดการหรือลบข้อมูลทดสอบออกจากระบบทดสอบอย่างไร เช่น การลบข้อมูลออกจากฐานข้อมูล การคืนค่าของเครื่องและสภาพแวดล้อม การใช้เครื่องมือลบข้อมูลแบบปลอดภัย 10. ก่อนการอนุมัติยอมรับระบบ (Sign-off) หน่วยงานมีการทดสอบความมั่นคงปลอดภัยประเภทใดบ้าง (เช่น SAST, DAST หรือ Penetration Testing) และหากพบช่องโหว่ระดับสูง มีขั้นตอนการสั่งแก้ไขก่อนนำขึ้นใช้งานจริงอย่างไร	

11. หลังจากระบบเปิดใช้งานแล้ว มีการตั้งค่า Log ของแอปพลิเคชันเพื่อเฝ้าระวังกิจกรรมที่ผิดปกติ (เช่น การเดารหัสผ่าน หรือการเข้าถึงข้อมูลลับ) ไว้อย่างไร และใครเป็นผู้รับผิดชอบในการตรวจสอบบันทึกเหตุการณ์เหล่านี้
12. เมื่อซอฟต์แวร์สิ้นสุดอายุการใช้งานหรือปิดโครงการ หน่วยงานมีขั้นตอนในการถอนสิทธิ์การเข้าถึง และการล้างข้อมูลสำคัญในฐานะข้อมูลอย่างไร

■ การสอบทานเอกสาร

1. สอบทานว่านโยบายและขั้นตอนการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development Life Cycle) ครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ง)
2. สอบทานรายงานการประเมินความเสี่ยงโครงการและเอกสารข้อกำหนดโครงการ (TOR) หรือสัญญาจ้างมีการระบุข้อกำหนดด้านความปลอดภัย (Security Requirements) ไว้อย่างชัดเจน
3. สอบทานคู่มือแนวทางการเขียนโค้ดปลอดภัย ว่ามีการอ้างอิงมาตรฐานสากลที่เป็นที่ยอมรับ (เช่น OWASP Top 10, SANS 25)
4. สอบทานแผนภาพสถาปัตยกรรมระบบที่แสดงการแบ่งแยกสภาพแวดล้อมการทำงานสำหรับการพัฒนา (Development) การทดสอบ (Test) และการให้บริการ (Production)
5. สอบทานรายงานผลการทดสอบความมั่นคงปลอดภัยของซอฟต์แวร์ และเอกสารการอนุมัติยอมรับระบบ (UAT / Security Sign-off) ว่าดำเนินการก่อนการเริ่มใช้งานจริง
6. ข้อมูลสำหรับระบบที่เลิกใช้งานสอบทานบันทึกการเฝ้าระวังระบบ (System/Application Logs) และบันทึกหลักฐานการทำลาย
7. ตรวจสอบกระบวนการเมื่อสิ้นสุดโครงการหรือเลิกใช้งานซอฟต์แวร์ ว่ามีขั้นตอนการลบข้อมูลในฐานะข้อมูลหรือการลบสิทธิ์การเข้าถึงอย่างปลอดภัยและบันทึกหลักฐานการทำลาย

■ เอกสารที่เกี่ยวข้อง

1. นโยบายและขั้นตอนการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development Life Cycle)
2. รายงานการประเมินความเสี่ยงโครงการ
3. เอกสารข้อกำหนดโครงการ (TOR) หรือสัญญาจ้างพัฒนาซอฟต์แวร์
4. แนวทางปฏิบัติในการเขียนโค้ดอย่างปลอดภัย (Secure Coding)
5. บันทึกการตรวจสอบ Source Code (Code Review)
6. Test Plan / Test Case (ที่ระบุวิธีการเตรียมข้อมูลทดสอบ)
7. Script หรือเครื่องมือที่ใช้สร้างข้อมูลจำลอง (Synthetic Data) สำหรับการทดสอบ
8. แผนภาพสถาปัตยกรรมที่แสดงการแบ่งแยกสภาพแวดล้อม (Environment Segregation Architecture Diagram)
9. รายงานผลการทดสอบความมั่นคงปลอดภัยของซอฟต์แวร์ (Security Testing Report / VAPT Report)
10. หลักฐานการทำลายข้อมูล

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบการตั้งค่า Log และระบบ Monitoring ของซอฟต์แวร์ว่าสามารถตรวจจับกิจกรรมที่ผิดปกติได้สอดคล้องกับความเสี่ยงของระบบ

2. ตรวจสอบ Log ของซอฟต์แวร์ว่ามีการบันทึกกิจกรรมสำคัญ (เช่น การแก้ไขสิทธิ์ผู้ใช้ การเข้าถึงข้อมูลที่อ่อนไหว) และสามารถระบุตัวตนผู้เข้าถึงได้จริง
3. สุ่มตรวจสอบระบบทดสอบ (UAT/Test) ว่าไม่มีการนำข้อมูลจริง (Production Data) ที่เป็นข้อมูลส่วนบุคคลหรือความลับมาใช้โดยไม่มีการทำ Data Masking

การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี (Technology Infrastructure Resilience)

3.2.11 การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีโครงสร้างพื้นฐานทางเทคโนโลยีมีความพร้อมรับมือ (Technology Infrastructure Resilience) ผ่านการแบ่งส่วนเครือข่าย (Network Segmentation) การจำกัดการสื่อสาร และการแยกส่วนระบบที่ได้รับผลกระทบ (Isolation) รวมถึงการป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม พร้อมทั้งจัดสรรทรัพยากรและระบบสำรองให้เพียงพอต่อการดำเนินงานอย่างต่อเนื่องทั้งในสภาวะปกติและวิกฤต

ความเสี่ยง

การหยุดชะงักของบริการสำคัญเป็นวงกว้าง และความล้มเหลวในการกู้คืนระบบเมื่อเกิดเหตุวิกฤต

การควบคุมที่พึงมี

การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี ควรดำเนินการอย่างน้อย ดังนี้

1. การแบ่งส่วนเครือข่าย (Network Segmentation)
 - (ก) ต้องแบ่งส่วนสถาปัตยกรรมเครือข่ายออกเป็นกลุ่มตามระดับความมั่นคงปลอดภัยและความเสี่ยง
 - (ข) ต้องจำกัดการสื่อสารระหว่างส่วนเครือข่ายที่แตกต่างกันให้เหลือเพียงเท่าที่จำเป็นสำหรับการทำงานของหน่วยงานเท่านั้น
 - (ค) ต้องมีกลไกการรักษาความมั่นคงปลอดภัยเครือข่ายระหว่างส่วนเครือข่ายที่แตกต่างกัน เพื่อตรวจจับและปิดกั้นการรับส่งข้อมูลเครือข่ายที่เป็นอันตราย
 - (ง) ต้องกำหนดกลไกและกระบวนการในการตัดการเชื่อมต่อกับส่วนของเครือข่ายที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ (Isolation)
2. ป้องกันทรัพย์สินทางสารสนเทศ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย และระบบจัดเก็บข้อมูล จากอัคคีภัย น้ำท่วม หรือภัยจากสภาพแวดล้อมอื่น ๆ
3. มีมาตรการหรือกลไกเพื่อให้ระบบหรือบริการสำคัญสามารถทำงานต่อเนื่องได้ตามความต้องการด้านความพร้อมรับมือ (Resilience Requirement) ทั้งในสถานการณ์ปกติและไม่ปกติ เช่น มีอุปกรณ์หรือระบบสำรอง
4. มีการเฝ้าระวังทรัพยากรและทำให้มั่นใจว่ามีทรัพยากรเพียงพอเพื่อรองรับการให้บริการอย่างต่อเนื่อง

แนวทางการประเมิน

1. ตรวจสอบนโยบายการแบ่งส่วนเครือข่าย (Network Segmentation) ครอบคลุมการควบคุมที่พึงครอบคลุมข้อ 1 (ก) - (ง)

2. ตรวจสอบการป้องกันภัยจากสภาพแวดล้อมโดยการสังเกตการณ์ทางกายภาพ เช่น ระบบตรวจจับและระวังอัคคีภัย ระบบตรวจจับน้ำรั่วซึม
3. ตรวจสอบความพร้อมรับมือและความต่อเนื่องในการทำงานของระบบ/บริการสำคัญ เช่น การตั้งค่า High Availability (HA) ความพร้อมของระบบไฟฟ้าสำรอง (UPS และ Generator)
4. ตรวจสอบระบบเฝ้าระวังที่ใช้ดูแลการใช้งานทรัพยากร (CPU, RAM, Disk, Bandwidth) และการวางแผนขยายทรัพยากรล่วงหน้า เพื่อให้มั่นใจว่ามีทรัพยากรเพียงพอรองรับการให้บริการอย่างต่อเนื่อง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.IR-02, PR.IR-03, PR.IR-04
ISO/IEC27001:2022	Clause 4.2, Clause 6.1.1, Annex A 5.29, Annex A 7.5, Annex A 8.6, Annex A 8.14
ISO/IEC27701:2025	-
ISO/IEC27017:2015	12.1.3
ISO/IEC27007:2020	A.1.2, A.3.1.1
ISO/IEC TS 27008:2019	11.1.4, 12.1.3, 17.1.1, 17.1.2, 17.1.3, 17.2.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. สถาปัตยกรรมเครือข่ายมีการแบ่งโซน (Segmentation) ตามระดับความเสี่ยงอย่างไร
2. หากพบภัยคุกคามลูกกลามในเครือข่าย มีกลไกในการตัดการเชื่อมต่อ (Isolate) โซนที่มีการแพร่กระจายของภัยคุกคามอย่างไร
3. อุปกรณ์หรือระบบเครือข่ายที่สำคัญมีการออกแบบให้มีระบบสำรอง (Redundancy) เพื่อทำงานทดแทนกันอย่างไรเมื่อเกิดเหตุขัดข้อง
4. ศูนย์ข้อมูล (Data Center) มีระบบป้องกันภัยทางกายภาพและสภาพแวดล้อม (เช่น ระบบดับเพลิงอัตโนมัติ, ระบบป้องกันน้ำท่วม/ความชื้น) อย่างไร
5. ในกรณีไฟฟ้าดับเป็นเวลานาน ระบบ UPS และ Generator สามารถรองรับการทำงานของอุปกรณ์ทั้งหมดได้นานเพียงใด และมีกระบวนการเติมเชื้อเพลิงสำรองอย่างไร
6. หน่วยงานมีเกณฑ์การแจ้งเตือน (Threshold) อย่างไรเมื่อทรัพยากรระบบ (เช่น CPU, RAM, Bandwidth) เริ่มใกล้เต็มขีดจำกัด และมีกระบวนการวางแผนขยายทรัพยากร (Capacity Planning) ล่วงหน้าอย่างไรก่อนที่จะกระทบต่อผู้ใช้งาน

■ การสอบทานเอกสาร

1. สอบทานแผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram) เพื่อดูการแบ่งโซน และตำแหน่งการวางอุปกรณ์รักษาความปลอดภัย (เช่น Firewall, IPS) ระหว่างโซน

2. สอบทานรายงานการซ้อมแผนความต่อเนื่องว่ามีการซ้อมแผนในสถานการณ์ที่ครอบคลุมถึงระบบโครงสร้างพื้นฐานขัดข้อง และมีผลการทดสอบกู้คืนบริการภายในระยะเวลาที่กำหนด (RTO)
3. สอบทานรายงานการเฝ้าระวังทรัพยากร (Capacity Report) เพื่อดูแนวโน้มการใช้งาน (Trend Analysis) ย้อนหลังเพื่อยืนยันว่าหน่วยงานมีการติดตามปริมาณการใช้ทรัพยากรอย่างต่อเนื่อง
4. สอบทานบันทึกการบำรุงรักษาอุปกรณ์ป้องกันความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เช่น การตรวจเช็คระบบดับเพลิง (Gas Suppression System) ระบบปรับอากาศ (Precision AC) และระบบไฟฟ้าสำรอง ว่ามีการทดสอบตามรอบเวลาที่กำหนดโดยผู้เชี่ยวชาญ

■ เอกสารที่เกี่ยวข้อง

1. แผนภาพสถาปัตยกรรมและผังเครือข่าย (Network and Architecture Diagram)
2. รายการกฎการตั้งค่า Firewall (Firewall Policy/Rule Base)
3. รายงานผลการฝึกซ้อมแผนความต่อเนื่องและการกู้คืนระบบ (BCP/DRP Test Report)
4. รายงานการเฝ้าระวังทรัพยากรระบบ (System Performance & Capacity Report)
5. บันทึกการตรวจสอบและบำรุงรักษาอุปกรณ์ป้องกันความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบการตั้งค่า VLAN บน Switch เพื่อยืนยันว่าการแบ่งโซนสอดคล้องกับผังเครือข่าย
2. สอบทานรายการกฎการตั้งค่า Firewall ว่าไม่มีกฎที่เป็น "Any-Any" ในจุดที่ข้ามเขตความปลอดภัย และมีการตั้งค่า Logging สำหรับกิจกรรมที่ถูกปฏิเสธ (Deny Logs)
3. ตรวจสอบตำแหน่งของอุปกรณ์ป้องกันความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เช่น อุปกรณ์ดับเพลิง เซนเซอร์ตรวจจับน้ำ
4. ตรวจสอบสถานะ Real-time ของอุปกรณ์ป้องกันความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เช่น เซนเซอร์วัดอุณหภูมิ ความชื้น
5. ตรวจสอบว่าไม่มีวัสดุไวไฟเก็บไว้ในบริเวณจุดติดตั้งอุปกรณ์
6. ตรวจสอบหน้าจอ Dashboard ของระบบ Monitoring (เช่น Zabbix, PRTG, SolarWinds) เพื่อยืนยันว่ามีการตั้งค่าการแจ้งเตือน (Alerts) เมื่อ CPU/RAM หรือ Bandwidth สูงถึงเกณฑ์ที่กำหนด

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การวิเคราะห์เหตุการณ์ไม่พึงประสงค์ (Adverse Event Analysis)

3.2.12 การวิเคราะห์เหตุการณ์ไม่พึงประสงค์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการวิเคราะห์เหตุการณ์ไม่พึงประสงค์ (Adverse Event Analysis) ที่มีประสิทธิภาพ โดยครอบคลุมการรวบรวมและเชื่อมโยงข้อมูลจากหลายแหล่งร่วมกับข้อมูลข่าวกรองภัยคุกคาม (Cyber Threat Intelligence)

ความเสี่ยง	
การตัดสินใจที่ผิดพลาดในการตอบสนองต่อเหตุการณ์ และไม่สามารถป้องกันการโจมตีซ้ำซ้อนจากภัยคุกคามได้	
การควบคุมที่พึงมี	
การตรวจวิเคราะห์เหตุการณ์ไม่พึงประสงค์ของบริการที่สำคัญ ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้ (ก) วิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ (ข) รวบรวมและเชื่อมโยงข้อมูลจากหลายแหล่ง และหากเป็นไปได้ควรพิจารณาใช้เทคโนโลยีการวิเคราะห์และเชื่อมโยงเหตุการณ์ (ค) ประเมินขอบเขตและผลกระทบของเหตุการณ์ (ง) แจ้งเตือนและส่งข้อมูลไปยังผู้มีหน้าที่ตอบสนองต่อเหตุการณ์หรือเครื่องมือตอบสนองต่อเหตุการณ์ (จ) บูรณาการข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์และข้อมูลเชิงบริบทอื่น ๆ เข้ากับกระบวนการวิเคราะห์เหตุการณ์ (ฉ) ระบุว่ามีความเสี่ยงภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานหรือไม่	
แนวทางการประเมิน	
- ตรวจสอบว่ามีกระบวนการและระบบวิเคราะห์เหตุการณ์ที่มีรายละเอียดครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ฉ) - ตรวจสอบเทคโนโลยีหรือเครื่องมือหลักที่ช่วยให้การดำเนินการ (ก) - (ฉ) เป็นไปอย่างอัตโนมัติและมีประสิทธิภาพ	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08
ISO/IEC27001:2022	Annex A 5.7, Annex A 5.24, Annex A 5.25, Annex A 5.26, Annex A 8.15, Annex A 8.16
ISO/IEC27701:2025	A.3.11, A.3.12, A.3.25
ISO/IEC27017:2015	16.1.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.4.1, 12.4.2, 12.4.3, 16.1.1, 16.1.4, 16.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์	

1. เมื่อระบบตรวจพบความผิดปกติ ทีมงานมีขั้นตอนในการวิเคราะห์อย่างไรเพื่อยืนยันว่าเป็นภัยคุกคามจริง (True Positive) และมีการคัดแยกเหตุการณ์ที่ไม่ใช่ภัยคุกคาม (False Positive) ออกจากรายงานสรุปอย่างไร
2. ปัจจุบันมีการใช้เทคโนโลยีหรือระบบใด (เช่น SIEM) ในการเชื่อมโยงข้อมูล (Correlation) จากอุปกรณ์ที่แตกต่างกัน เช่น Firewall, Server และ Endpoint เพื่อให้เห็นภาพรวมของเหตุการณ์เดียวกันหรือไม่
3. หน่วยงานใช้หลักเกณฑ์ใดในการระบุว่าเหตุการณ์เกี่ยวข้องกับบริการที่สำคัญ (CII)
4. หน่วยงานใช้เกณฑ์ใดในการกำหนดการแจ้งเตือนและส่งข้อมูลไปยังผู้เกี่ยวข้อง เพื่อประเมินขอบเขตและผลกระทบของเหตุการณ์
5. หน่วยงานมีการกำหนดตารางผู้รับผิดชอบ (Incident Responder) ในแต่ละระดับความรุนแรง ลำดับการแจ้งเตือน และกรอบระยะเวลาไว้หรือไม่ อย่างไร
6. หน่วยงานมีการบูรณาการข้อมูลข่าวกรอง (CTI) เช่น รายชื่อ IP, Domain หรือ Malware Hash ที่เป็นอันตราย เข้ากับระบบวิเคราะห์เหตุการณ์อย่างไรเพื่อเพิ่มความแม่นยำในการตรวจจับ
7. หน่วยงานได้นำข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ (CTI) จากภายนอก (เช่น IOCs จาก สกมช. หรือ Threat Feeds) มาใช้ประกอบการวิเคราะห์พฤติกรรมความผิดปกติของเหตุการณ์ร่วมด้วยอย่างไร

■ การสอบทานเอกสาร

1. สอบทานขั้นตอนหรือแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ง)
2. สอบทานรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report) ย้อนหลัง เพื่อดูความครบถ้วนของการวิเคราะห์ (ก, ค, ง)
3. สอบทานหลักฐานการแจ้งเตือน (Alert/Notification Logs) เช่น อีเมลแจ้งเตือน หรือบันทึกในระบบ Ticket
4. สอบทานหลักฐานการบูรณาการข้อมูลข่าวกรองภัยคุกคาม (CTI) มาใช้ประกอบการวิเคราะห์เหตุการณ์ (เช่น การวิเคราะห์เทียบกับ IP/Hash Blacklist)
5. สอบทานบันทึกหลักฐานการแจ้งเตือนและการส่งต่อข้อมูลไปยังผู้มีหน้าที่ตอบสนองต่อเหตุการณ์หรือเครื่องมือตอบสนองต่อเหตุการณ์

■ เอกสารที่เกี่ยวข้อง

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2. ตารางเกณฑ์การประเมินผลกระทบและแนวทางการแจ้งเตือนยกระดับ (Escalation Matrix)
3. รายงานการวิเคราะห์เหตุการณ์รายวัน/รายเดือน (Incident Analysis Dashboard/Report)
4. รายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report)
5. บัญชีรายชื่อข้อมูลข่าวกรองที่เชื่อมต่อกับระบบ (Threat Intelligence Sources List)
6. รายงานข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence Reports / Feeds)
7. บันทึกการแจ้งเหตุไปยังผู้มีส่วนเกี่ยวข้อง (Communication Logs)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบ Configuration ของระบบ SIEM/Correlation Rules ที่แสดงให้เห็นถึงกฎที่ใช้เชื่อมโยงเหตุการณ์จากหลายแหล่งข้อมูล
2. ตรวจสอบข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ เพื่อยืนยันว่ามีการปรับปรุงข้อมูลข่าวกรองให้เป็นปัจจุบันเสมอ

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Incident Analysis)

3.2.13 การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการวิเคราะห์เหตุภัยคุกคาม (Incident Analysis) ที่ครอบคลุมการจัดลำดับเหตุการณ์ (Timeline) และการวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause)

ความเสี่ยง

การถูกโจมตีผ่านช่องโหว่หรือความบกพร่องเดิมซ้ำอีกในอนาคต

การควบคุมที่พึงมี

การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Incident Analysis) ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

1. ต้องวิเคราะห์เพื่อระบุลำดับเหตุการณ์ (Timeline of Events) ในระหว่างที่เหตุภัยคุกคามทางไซเบอร์เกิดขึ้น โดยครอบคลุมตั้งแต่การตรวจพบครั้งแรกจนถึงการจำกัดขอบเขต วิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์เพื่อทำความเข้าใจว่าช่องโหว่ (Vulnerability) หรือความบกพร่องของกระบวนการใดที่ถูกใช้ประโยชน์โดยผู้ไม่ประสงค์ดี รวมถึงตรวจสอบระบบอื่นที่อาจได้รับผลกระทบเพื่อค้นหาหลักฐานการโจมตีและร่องรอยความต่อเนื่องของเหตุภัยคุกคามทางไซเบอร์
2. ต้องเก็บรวบรวมข้อมูลเหตุการณ์ ข้อมูลเมตา (เช่น IP, ชื่อผู้ใช้, วันและเวลาที่เก็บ) และบันทึกการดำเนินการที่เกิดขึ้นระหว่างการตรวจสอบและวิเคราะห์เหตุการณ์ (เช่น ใครทำอะไร เวลาใด ทำอย่างไร) โดยต้องมีมาตรการเพื่อให้แน่ใจว่าข้อมูลและบันทึกดังกล่าวมีความน่าเชื่อถือ และถูกต้องครบถ้วน เช่น การทำให้บันทึกไม่สามารถแก้ไขย้อนหลังได้ (Immutable)

แนวทางการประเมิน

1. ตรวจสอบกระบวนการวิเคราะห์และระบุลำดับเหตุการณ์ ว่ามีขั้นตอนครอบคลุมตั้งแต่การตรวจพบครั้งแรกจนถึงการจำกัดขอบเขต วิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์
2. ตรวจสอบหลักฐานการวิเคราะห์ระบบข้างเคียง เพื่อยืนยันว่าหน่วยงานได้ค้นหาการแพร่กระจายของภัยคุกคาม (Persistence/Lateral Movement) อย่างครบถ้วน
3. ตรวจสอบการเก็บรวบรวมข้อมูลเหตุการณ์ ความครบถ้วนของ Metadata บันทึกการปฏิบัติงานของเจ้าหน้าที่ และความน่าเชื่อถือของหลักฐาน
4. ตรวจสอบทางเทคนิคว่าบันทึกเหตุการณ์ (Logs) ถูกจัดเก็บในระบบที่ป้องกันการแก้ไขย้อนหลัง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08
ISO/IEC27001:2022	Annex A 5.25, Annex A 5.27, Annex A 5.28
ISO/IEC27701:2025	A.3.11
ISO/IEC27017:2015	16.1.7
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.4, 16.1.6, 16.1.7
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - เมื่อเกิดเหตุภัยคุกคาม ทีมงานมีกระบวนการสืบสวนเพื่อจัดทำลำดับเหตุการณ์ (Timeline) และวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) อย่างไร มีการตรวจสอบร่องรอยการฝังตัว (Persistence) หรือการบุกรุกไปเครื่องอื่น (Lateral Movement) แล้วหรือไม่ - เมื่อระบุสาเหตุที่แท้จริงได้แล้ว หน่วยงานมีขั้นตอนการนำผลการวิเคราะห์นั้นไปปรับปรุงนโยบายหรือปิดช่องโหว่เพื่อป้องกันการเกิดซ้ำอย่างไร - ระหว่างการสืบสวน มีการจดบันทึกการปฏิบัติงานของเจ้าหน้าที่ (ใคร ทำอะไร เวลาใด) และเก็บข้อมูลเมตา (เช่น IP, Username) ไว้อย่างไรเพื่อใช้เป็นหลักฐาน - หน่วยงานมีมาตรการเชิงเทคนิคหรือระเบียบปฏิบัติใด (เช่น การทำ Hashing, การตั้งค่าการจับเก็บแบบอ่านได้อย่างเดียว) เพื่อรับประกันว่าบันทึกหลักฐานและ Log ต่าง ๆ จะไม่ถูกดัดแปลงหรือลบแก้ไขย้อนหลัง (Immutable) รวมถึงผู้ดูแลระบบเองก็ไม่สามารถลบได้ - หน่วยงานมีการส่ง Log ไปยังหน่วยงานภายนอกที่เชื่อถือได้ทันทีที่เกิดเหตุหรือไม่ ■ การสอบทานเอกสาร - สอบทานแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ว่าครอบคลุมขั้นตอนการวิเคราะห์และระบุลำดับเหตุการณ์ ตั้งแต่การตรวจพบครั้งแรกจนถึงการจำกัดขอบเขต วิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์ - สอบทานรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report) ว่ามีการระบุลำดับเวลาอย่างละเอียด ตั้งแต่จุดเริ่มต้น (Initial Access) ไปจนถึงการตรวจพบช่องโหว่ และการจำกัดขอบเขต (Containment) รวมถึงการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) - สอบทานบันทึกข้อมูลเมตา ว่ามีการจัดเก็บข้อมูลสำคัญครบถ้วน เช่น Source/Destination IP, User Account, Timestamps (UTC/Local), และเครื่องมือที่ใช้ - สอบทานบันทึกการปฏิบัติงาน (Event Logs, Metadata, and Activity Logs) เพื่อประเมินความครบถ้วนของรายละเอียดเจ้าหน้าที่ผู้ปฏิบัติงาน วันเวลา และการกระทำ และนำเชื่อถือของหลักฐานดิจิทัลในระหว่างการสืบสวน	

5. สอบทานแบบฟอร์มบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody Form) เพื่อประเมินความครบถ้วนของรายละเอียด และกลไกการรักษาความสมบูรณ์ของหลักฐานดิจิทัล (เช่น ค่า Hash ในแบบฟอร์มตรงกับรายงานผลการวิเคราะห์ทาง Forensic)
6. สอบทานผลการปฏิบัติตามกฎหมาย มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด อย่างน้อย ดังนี้
 - ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 - กำหนดให้หน่วยงานดำเนินการวิเคราะห์เพื่อหาสาเหตุที่แท้จริง (Root Cause Analysis) รวมถึงจัดเก็บรวบรวมข้อมูลสำหรับรายงานเหตุภัยคุกคามทางไซเบอร์ตามรายละเอียดเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

■ เอกสารที่เกี่ยวข้อง

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2. รายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report)
3. รายงานการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis)
4. บันทึกเหตุการณ์ ข้อมูลเมตา และบันทึกการปฏิบัติงาน (Event Logs, Metadata, and Activity Logs)
5. แบบฟอร์มบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody Form)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบค่า Hash ของไฟล์หลักฐานหรือ Log และยืนยันว่าระบบจัดเก็บมีการควบคุมสิทธิ์ที่เข้มงวด (Access Control) และไม่มีฟังก์ชันการลบ/แก้ไขสำหรับผู้ทั่วไป
2. ตรวจสอบว่าอุปกรณ์ทั้งหมดที่ส่ง Log มานั้นมีการทำ Time Synchronization (NTP) ให้ตรงกัน

การบรรเทาเหตุภัยคุกคามทางไซเบอร์ (Incident Mitigation)

3.2.14 การบรรเทาเหตุภัยคุกคามทางไซเบอร์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีขั้นตอนและทรัพยากรที่พร้อมสำหรับการจำกัดขอบเขต (Contain) และกำจัด (Eradicate) ภัยคุกคามออกจากระบบได้อย่างรวดเร็ว

ความเสี่ยง

ภัยคุกคามแพร่กระจายจนไม่สามารถควบคุมได้ ส่งผลเสียหายต่อข้อมูลและระบบสำคัญ

การควบคุมที่พึงมี

การบรรเทาเหตุภัยคุกคามทางไซเบอร์ (Incident Mitigation) ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

1. มีขั้นตอนและทรัพยากรที่พร้อมใช้งานเพื่อจำกัดขอบเขต (Contain) และกำจัด (Eradicate) ภัยคุกคามทางไซเบอร์ที่ตรวจพบออกจากระบบ โดยอาจใช้เทคโนโลยีอัตโนมัติ ใช้การดำเนินการโดยผู้ปฏิบัติ ใช้บริการจากผู้ให้บริการภายนอกที่เชื่อถือได้ หรือขอความช่วยเหลือจากหน่วยงานที่เกี่ยวข้องตามความจำเป็น

2. เฝ้าระวังอย่างต่อเนื่อง เพื่อตรวจสอบยืนยันว่าภัยคุกคามถูกจำกัดและไม่มีการแพร่กระจายไปยังส่วนอื่นของระบบ	
แนวทางการประเมิน	
- ตรวจสอบว่ามีขั้นตอนปฏิบัติ (Playbooks) ที่ระบุวิธีการจำกัดขอบเขต (Containment) และการกำจัด (Eradication) ตามประเภทภัยคุกคามที่สำคัญ (เช่น Malware, Phishing, Ransomware) - ตรวจสอบความพร้อมของทรัพยากรทั้งในด้านบุคคล และเครื่องมือที่ใช้ในจำกัดขอบเขต (Contain) และกำจัด (Eradicate) ภัยคุกคามทางไซเบอร์ - ตรวจสอบกระบวนการเฝ้าระวังอย่างต่อเนื่อง (Continuous Monitoring) ภายหลังการจำกัดขอบเขต เช่น หลักฐานการสแกนหรือการตั้งค่า Monitoring พิเศษหลังเกิดเหตุ เพื่อยืนยันว่าไม่มีมัลแวร์ตกค้าง รายงานผลการตรวจสอบระบบข้างเคียงภายในโซนเครือข่ายเดียวกัน เพื่อยืนยันว่าภัยคุกคามไม่ได้แพร่กระจายไปส่วนอื่นก่อนถูกกำจัด	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RS.MI-01, RS.MI-02
ISO/IEC27001:2022	Annex A 5.26
ISO/IEC27701:2025	A.3.12
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.5
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ - ในสถานการณ์จริง ทีมงานมีการนำ Playbooks มาใช้ในการตัดสินใจเลือกวิธีจำกัดขอบเขต (Containment) อย่างไร - ในการยับยั้งภัยคุกคาม หน่วยงานมีการใช้เทคโนโลยีอัตโนมัติ (เช่น EDR/SOAR) เพื่อระงับภัยคุกคามเบื้องต้นหรือไม่ หรือเป็นการดำเนินการด้วยตนเอง (Manual) - หากเครื่องมือภายในไม่สามารถกำจัดภัยคุกคามได้ (Eradication) หน่วยงานมีกระบวนการเรียกใช้ทรัพยากรเสริมจากผู้ให้บริการภายนอก (Outsource/MSSP) หรือหน่วยงานกำกับดูแลอย่างไร - หลังจากการแยกหรือจำกัดขอบเขตภัยคุกคามแล้ว ทีมงานมีกระบวนการเฝ้าระวังระบบเครือข่ายและระบบข้างเคียงอย่างต่อเนื่องอย่างไร เพื่อยืนยันว่าภัยคุกคามถูกจำกัดและไม่เกิดการแพร่กระจาย (Lateral Movement) และมีการตั้งค่า Monitoring พิเศษหลังเกิดเหตุไว้นานเพียงพอ ■ การสอบทานเอกสาร	

1. สอบทานแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) และขั้นตอนปฏิบัติการรับมือกับภัยคุกคามไซเบอร์ (Playbooks) ว่าครอบคลุมเทคนิคการจำกัดขอบเขตและกำจัดภัยคุกคามตามความเสี่ยงสำคัญ (Malware, Ransomware, Web Attack) และเป็นปัจจุบัน
2. สอบทานบันทึกการจัดการเหตุการณ์ (Incident Handling Logs) หรือรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report) ล่าสุด เพื่อดูหลักฐานการดำเนินการจำกัดขอบเขต การกำจัด และเวลาที่ใช้ในการตอบสนอง
3. สอบทานหลักฐานการสแกนหรือการตรวจสอบ Log ในเครือข่ายส่วนเดียวกัน เพื่อยืนยันว่าภัยคุกคามไม่ได้แพร่กระจายก่อนถูกระงับ
4. สอบทานหลักฐานการตั้งค่าการแจ้งเตือนพิเศษ หรือการทำ Malware Scanning รอบพิเศษ หลังการกู้คืนระบบ
5. สอบทานสัญญากับผู้ให้บริการภายนอก (SLA/MSSP) เพื่อดูข้อกำหนดว่าผู้ให้บริการต้องเข้ามาช่วยเหลือภายในกี่ชั่วโมง (Response Time SLA) เมื่อมีการแจ้งเหตุฉุกเฉิน
6. สอบทานรายชื่อผู้ติดต่อประสานงานฉุกเฉิน (Emergency Contact List) ทั้งภายในและภายนอก เพื่อยืนยันความพร้อมใช้งาน ความถูกต้องและความเป็นปัจจุบัน และการดำเนินการตามกฎหมาย (เช่น สกมช. หรือ ThaiCERT) เพื่อบันทึกเหตุการณ์ภายในระยะเวลาที่ระบุ (เช่น ภายใน 24 ชม.)

■ เอกสารที่เกี่ยวข้อง

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2. ขั้นตอนปฏิบัติการรับมือกับภัยคุกคามไซเบอร์ (Playbooks)
3. บันทึกการจัดการเหตุการณ์ (Incident Handling Logs)
4. รายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report)
5. สัญญาการให้บริการ (SLA) กับผู้ให้บริการด้านความมั่นคงปลอดภัย (เช่น MSSP, Forensic Service) หรือประกันภัยไซเบอร์
6. รายชื่อผู้ติดต่อประสานงานฉุกเฉิน (Emergency Contact List) ทั้งภายในและภายนอก

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบในระบบ Endpoint Protection (EDR) เพื่อดูประวัติการทำ Isolation หรือ Quarantine ย้อนหลังว่ามีการทำงานจริงตามที่ระบุใน Incident Logs
2. ตรวจ Firewall/Switch Configuration ในช่วงที่เกิดเหตุล่าสุด เพื่อดูความสอดคล้องของกิจกรรมเช่น การสั่งปิด Port หรือการ Block IP ชั่วคราว

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

แผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan)

3.2.15 การจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) ที่เป็นระบบและพร้อมใช้งาน โดยครอบคลุมการจัดลำดับความสำคัญตามค่า RTO/RPO การระบุบทบาทความรับผิดชอบ และขั้นตอนการกู้คืนที่มีการทดสอบยืนยันความถูกต้อง

ความเสี่ยง

เกิดการหยุดชะงักของบริการสำคัญ หรือการสูญเสียข้อมูลสำคัญอย่างถาวร

การควบคุมที่พึงมี

ควรจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) เพื่อให้มั่นใจได้ว่าหน่วยงานสามารถฟื้นฟูระบบและกู้คืนข้อมูลที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และลดผลกระทบต่อการดำเนินตามภารกิจและบริการของหน่วยงาน ซึ่งหน่วยงานอาจจัดทำแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์แยกออกมาเป็นแผนหนึ่งหรือเป็นส่วนหนึ่งของแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ก็ได้ โดยควรมีเนื้อหาอย่างน้อยดังนี้

- (ก) ระดับความสำคัญของระบบและข้อมูล เพื่อใช้จัดลำดับความเร่งด่วนในการฟื้นฟู โดยสอดคล้องกับ ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) ของหน่วยงาน
- (ข) บทบาทหน้าที่และความรับผิดชอบของสมาชิกในทีม
- (ค) ขั้นตอนปฏิบัติในการฟื้นฟูระบบ
- (ง) ขั้นตอนการทดสอบและยืนยันว่าระบบที่ฟื้นฟูนั้นมีความถูกต้อง
- (จ) ขั้นตอนการสื่อสารทั้งภายในและภายนอกหน่วยงานในระหว่างการฟื้นฟู รวมถึงกลไกการรายงานต่อผู้ที่เกี่ยวข้อง

แนวทางการประเมิน

1. ตรวจสอบแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) โดยต้องมีเนื้อหาครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (จ)
2. ตรวจสอบบันทึกการฟื้นฟูระบบ (Recovery Logs) (ถ้ามีเหตุการณ์เกิดขึ้นจริง) ว่าทำได้ทันเวลาตามค่า RTO และ RPO หรือไม่
3. ตรวจสอบว่ามีกระบวนการยืนยันความถูกต้องและความปลอดภัยหลังระบบได้รับการฟื้นฟู
4. ตรวจสอบแผนการสื่อสาร (Communication) ว่ามีการระบุช่องทางและลำดับการแจ้งข้อมูล รวมถึงผู้รับผิดชอบในการรายงานเหตุการณ์ต่อหน่วยงานกำกับดูแลหรือผู้มีส่วนได้ส่วนเสีย

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RC.RP-02
ISO/IEC27001:2022	Annex A 5.26
ISO/IEC27701:2025	A.3.12
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	16.1.5

มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีการจัดลำดับความสำคัญของระบบและข้อมูลที่จะต้องกู้คืนก่อน-หลังอย่างไร และสอดคล้องกับค่า RTO/RPO ที่ได้จากการทำ BIA อย่างไร 2. หน่วยงานมีการฝึกอบรมหรือซักซ้อมความเข้าใจเพื่อให้สมาชิกในทีมฟื้นฟูระบบมีความเข้าใจในบทบาทหน้าที่ของตนเองตามที่ระบุในแผนหรือไม่ 3. หน่วยงานมีขั้นตอนการยืนยันความถูกต้องของระบบที่กู้คืนกลับมาอย่างไร เพื่อให้มั่นใจว่าระบบมีความมั่นคงปลอดภัยและมีความพร้อมใช้งานจริง (เช่น มีขั้นตอนการตรวจสอบช่องโหว่ (Vulnerability Scan) หรือการทำ Hardening ระบบที่กู้คืนมาใหม่ก่อนที่จะเปิดให้ผู้ใช้งานเข้าถึง) 4. ในระหว่างที่ระบบกำลังถูกฟื้นฟู หน่วยงานมีขั้นตอนการสื่อสารเพื่อแจ้งสถานะให้ผู้ใช้งานและผู้มีส่วนได้ส่วนเสียทราบอย่างไร ■ การสอบทานเอกสาร 1. สอบทานแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) เพื่อยืนยันความครบถ้วนของเนื้อหาทั้ง 5 องค์ประกอบ (ก - จ) 2. สอบทานรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) เพื่อเทียบเคียงความสอดคล้องของเป้าหมายเวลา RTO และ RPO ที่ระบุในแผนฟื้นฟู 3. สอบทานรายชื่อผู้ติดต่อสื่อสารในภาวะวิกฤต (Crisis Communication Contact List) เพื่อดูความครบถ้วนและเป็นปัจจุบัน ■ เอกสารที่เกี่ยวข้อง 1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) 2. แผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) 3. รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) 4. โครงสร้างทีมรับมือและฟื้นฟู (Incident Response & Recovery Team Chart) 5. คู่มือ/ขั้นตอนการปฏิบัติงานสำหรับการกู้คืนระบบ 6. ทะเบียนรายชื่อและช่องทางติดต่อทีมงาน และผู้มีส่วนได้ส่วนเสียสำหรับการสื่อสารในภาวะวิกฤต ■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค -	

3.2.16 การทดสอบ ทบทวน และปรับปรุงแผน

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) มีความพร้อมใช้งานและบุคลากรมีความเข้าใจในบทบาทหน้าที่ผ่านการทดสอบและซักซ้อมอย่างสม่ำเสมอ รวมถึง

มีการทบทวนและปรับปรุงเนื้อหาให้เป็นปัจจุบันสอดคล้องกับระดับความเสี่ยงและบริบทของหน่วยงานที่เปลี่ยนแปลงไป

ความเสี่ยง

เกิดความล่าช้าหรือความล้มเหลวในการกู้คืนบริการสำคัญในสถานการณ์เหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริง

การควบคุมที่พึงมี

1. ควรทดสอบและฝึกซ้อมแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์อย่างน้อยปีละหนึ่งครั้งเพื่อให้มั่นใจว่ากระบวนการฟื้นฟูสามารถใช้งานได้จริง และบุคลากรที่เกี่ยวข้องมีความเข้าใจในบทบาทหน้าที่
2. ควรทบทวนและปรับปรุงแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้แผนมีความเป็นปัจจุบันและสอดคล้องกับระดับความเสี่ยง

แนวทางการประเมิน

1. ตรวจสอบหลักฐานการทดสอบและฝึกซ้อมแผนฟื้นฟู อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการทดสอบและฝึกซ้อมแผนฟื้นฟู (Recovery Drill) อย่างน้อยปีละ 1 ครั้ง และครอบคลุมระบบหรือบริการสำคัญ (CII)
2. ตรวจสอบความเข้าใจของบุคลากรที่ระบุในแผน ว่ามีความรู้ ความเข้าใจ และสามารถปฏิบัติงานได้จริงตามบทบาทหน้าที่ที่ได้รับมอบหมายในระหว่างการซักซ้อม
3. ตรวจสอบประวัติการทบทวนและปรับปรุงแผนฟื้นฟู ว่าดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ (เช่น การเปลี่ยนเทคโนโลยี, การปรับโครงสร้างองค์กร) เพื่อให้แผนสอดคล้องกับสถานการณ์ปัจจุบัน และระดับความเสี่ยง

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RC.RP-04
ISO/IEC27001:2022	Annex 5.30
ISO/IEC27701:2025	-
ISO/IEC27017:2015	-
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-

ขั้นตอนการตรวจสอบ

■ การสัมภาษณ์

1. ในการฝึกซ้อมแผนฟื้นฟูครั้งล่าสุด หน่วยงานใช้สถานการณ์จำลอง (Scenario) อะไร และมีการทดสอบในระดับใด (เช่น Tabletop Exercise หรือ Technical Simulation)
2. สมาชิกในทีมกู้คืนระบบ (Recovery Team) ได้รับการชี้แจงบทบาทหน้าที่อย่างไรก่อนเริ่มการซักซ้อม และมีปัญหาอุปสรรคใดหรือไม่ในการประสานงานระหว่างหน่วยงาน

3. หากมีการเปลี่ยนแปลงระบบโครงสร้างพื้นฐานที่สำคัญ หรือพบภัยคุกคามรูปแบบใหม่ หน่วยงานมีกระบวนการนำประเด็นดังกล่าวมาปรับปรุงแผนฟื้นฟูฯ ให้สอดคล้องกับการเปลี่ยนแปลงนั้นอย่างไร

■ การสอบทานเอกสาร

1. กรณีแผนฟื้นฟูฯ เป็นส่วนหนึ่งของแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2. กรณีแผนฟื้นฟูฯ แยกออกจากแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของแผนฟื้นฟูฯ เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง
3. สอบทานแผนฟื้นฟูฯ ว่ามีการระบุรายละเอียดการเปลี่ยนแปลงในตัวแผนฟื้นฟูฯ ที่สอดคล้องกับผลการซักซ้อมหรือความเสี่ยงที่เปลี่ยนไป
4. สอบทานรายงานการประเมินความเสี่ยง (Risk Assessment Report) เพื่อดูว่าแผนฟื้นฟูฯ ถูกปรับปรุงให้สอดคล้องกับความเสี่ยงใหม่ ๆ
5. สอบทานรายงานการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือ รายงานผลการฝึกซ้อมแผนฟื้นฟูภัยคุกคามทางไซเบอร์ (Incident Recovery Plan Exercise Report) ว่ามีการระบุวันเวลา สถานการณ์ ผลการซักซ้อม และปัญหาที่พบ และมีการลงนามรับรองผล
6. สอบทานบันทึกการเข้าร่วมซักซ้อม เพื่อยืนยันว่าบุคลากรที่เข้าซ้อมคือบุคคลเดียวกับที่มีชื่อในแผนฟื้นฟูฯ
7. สอบทานบันทึกการ Restore ข้อมูล หรือภาพหน้าจอการทำงานของระบบสำรอง เพื่อยืนยันว่ามีการซ้อมจริง

■ เอกสารที่เกี่ยวข้อง

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2. แผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan)
3. รายงานการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) หรือ รายงานผลการฝึกซ้อมแผนฟื้นฟูภัยคุกคามทางไซเบอร์ (Incident Recovery Plan Exercise Report)
4. รายงานการประเมินความเสี่ยง (Risk Assessment Report)
5. บันทึกการ Restore ข้อมูล หรือภาพหน้าจอการทำงานของระบบสำรอง

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

3.2.17 การดำเนินการตามแผนฟื้นฟูจากเหตุจริง

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีกระบวนการปฏิบัติงานตามแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery) อย่างเป็นขั้นตอน โดยครอบคลุมตั้งแต่การยืนยันการกำจัดภัยคุกคาม การจัดลำดับความสำคัญของภารกิจตามผลวิเคราะห์ BIA และ RTO การตรวจสอบความถูกต้องของข้อมูลสำรอง ตลอดจนการทดสอบยืนยันความสมบูรณ์ของระบบก่อนประกาศกลับเข้าสู่สภาวะปกติ

ความเสี่ยง

ระบบยังมีภัยคุกคามแอบแฝง หรือการกู้คืนข้อมูลหรือระบบสำคัญไม่ครบถ้วน ทำให้บริการสำคัญหยุดชะงักนานเกินกว่ากรอบเวลาที่กำหนดไว้

การควบคุมที่พึงมี

การดำเนินการตามแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

- (ก) ยืนยันว่าภัยคุกคามถูกกำจัดออกจากระบบแล้ว (Eradicated) เพื่อที่จะส่งมอบงานจากทีมรับมือ (Respond) ไปยังทีมฟื้นฟู (Recovery) ตามขั้นตอนการเรียกใช้งานกระบวนการฟื้นฟูที่ระบุไว้ในแผนรับมือเหตุภัยคุกคามทางไซเบอร์
- (ข) จัดลำดับการฟื้นฟูระบบและบริการตามความสำคัญของภารกิจ (Critical Mission Functions) ของหน่วยงาน โดยอ้างอิงจากผลการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) และ Recovery Time Objective (RTO)
- (ค) ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของการสำรองข้อมูล (Backup) ก่อนนำมาใช้ในการกู้คืนข้อมูล
- (ง) ดำเนินการฟื้นฟูระบบตามลำดับความสำคัญที่ถูกจัดลำดับตามความสำคัญของภารกิจ
- (จ) หลังจากการฟื้นฟูเสร็จสิ้น ต้องมีการตรวจสอบยืนยัน (Validation) เพื่อให้มั่นใจว่า ทรัพย์สินที่ฟื้นฟูนั้นมีความสมบูรณ์ และทำงานได้ถูกต้อง
- (ฉ) ประกาศสิ้นสุดกระบวนการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (End of Incident Recovery) เพื่อยืนยันการกลับสู่สภาวะการปฏิบัติงานปกติ (Normal Operations)

แนวทางการประเมิน

1. ตรวจสอบแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) โดยมีเนื้อหาครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ฉ)
2. ตรวจสอบลำดับการฟื้นฟูระบบและบริการตามความสำคัญของภารกิจ (Critical Mission Functions) ของหน่วยงาน โดยอ้างอิงจากผลการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) และ Recovery Time Objective (RTO)
3. ตรวจสอบหลักฐานการปฏิบัติงาน เช่น ผลยืนยันว่าภัยคุกคามถูกกำจัดออกจากระบบแล้ว (Eradicated) ผลตรวจสอบความถูกต้องครบถ้วน (Integrity) ของการสำรองข้อมูล (Backup) ก่อนนำมาใช้ในการกู้คืนข้อมูล ผลการทดสอบระบบ (Sanity Check/UAT) หลังกู้คืนเสร็จสิ้น อีเมลแจ้งพนักงานประกาศแจ้งสิ้นสุดเหตุการณ์

มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RC.RP-01, RC.RP-03, RC.RP-05, RC.RP-06

ISO/IEC27001:2022	Annex 5.26, Annex 5.27, Annex 8.13
ISO/IEC27701:2025	A.3.12, A.3.24
ISO/IEC27017:2015	12.3.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.3.1, 16.1.5, 16.1.6
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานมีเกณฑ์หรือเอกสารยืนยันอย่างไรว่าภัยคุกคามถูกกำจัด (Eradicated) อย่างสมบูรณ์แล้ว ก่อนที่จะอนุญาตให้ทีมฟื้นฟูเริ่มกู้คืนระบบ และใครเป็นผู้มีอำนาจสั่งเริ่มกระบวนการฟื้นฟูระบบ 2. ในกรณีที่สงสัยว่าข้อมูลสำรองอาจปนเปื้อนมัลแวร์ ทีมงานมีกระบวนการตรวจสอบความถูกต้อง (Integrity) และความปลอดภัยของข้อมูลนั้นอย่างไรก่อนนำมาใช้ (เช่น สแกนมัลแวร์ หรือเช็คค่า Hash) 3. เมื่อฟื้นฟูระบบเสร็จสิ้น หน่วยงานมีการทดสอบการทำงานของระบบอย่างไรเพื่อให้มั่นใจว่าระบบกลับสู่สภาวะปกติจริง และใครมีอำนาจในการประกาศสิ้นสุดกระบวนการฟื้นฟู (End of Incident Recovery) ■ การสอบทานเอกสาร 1. ตรวจสอบแผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) เพื่อยืนยันความครบถ้วนของเนื้อหาว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ฉ) 2. สอบทานบันทึกเหตุการณ์ (Incident Handling Logs) หรือรายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report) ในช่วงรอยต่อระหว่างการจัด (Eradication) และการฟื้นฟู (Recovery) เพื่อยืนยันว่า มีการตรวจสอบว่าภัยคุกคามถูกกำจัดแล้วจริง 3. สอบทานบันทึกการกู้คืนระบบ (Restoration Logs) ที่แสดงลำดับเวลาการกู้คืนระบบ เทียบกับผล BIA และเวลาที่ใช้จริงตั้งแต่เริ่มกู้คืนจนระบบพร้อมใช้ เกินค่า RTO หรือไม่ 4. สอบทานหลักฐานการตรวจสอบ Backup Integrity ก่อนกู้คืนระบบ เพื่อดูความน่าเชื่อถือของข้อมูล 5. สอบทานผลการทดสอบระบบ (Sanity Check/UAT) หลังกู้คืนเสร็จสิ้น เพื่อยืนยันว่ามีการตรวจสอบความถูกต้องและพร้อมใช้ของข้อมูลที่กู้มาล่าสุด 6. สอบทานรายงานผลการทดสอบการทำงานหลังกู้คืน เพื่อยืนยันว่ามีการตรวจสอบประสิทธิภาพของระบบ 7. ตรวจสอบเอกสาร/อีเมล ประกาศสิ้นสุดกระบวนการฟื้นฟู เพื่อยืนยันว่ามีการสื่อสารที่ชัดเจน ■ เอกสารที่เกี่ยวข้อง 1. แผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan) 2. บันทึกเหตุการณ์ (Incident Handling Logs) 3. รายงานเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Security Incident Report)	

4. บันทึกการกู้คืนระบบ (Restoration Logs)
5. รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
6. หลักฐานการตรวจสอบ Backup Integrity
7. ผลการทดสอบระบบ (Sanity Check/UAT) หลังกู้คืน
8. รายงานผลการทดสอบการทำงานหลังกู้คืน
9. ประกาศหรือแถลงการณ์สิ้นสุดการฟื้นฟู

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

แผนการสำรองข้อมูล (Backup Plan)

3.2.18 แผนการสำรองข้อมูล

วัตถุประสงค์

เพื่อให้มั่นใจว่า หน่วยงานมีแนวทางที่ชัดเจนและเป็นมาตรฐานในการกู้คืนข้อมูลสำคัญเมื่อเกิดเหตุขัดข้องหรือเกิดความเสียหายของข้อมูล

ความเสี่ยง

สูญเสียข้อมูลสำคัญอย่างถาวร หรือไม่สามารถกู้คืนระบบให้กลับมาดำเนินงานได้ตามปกติเมื่อเกิดเหตุการณ์วิกฤต

การควบคุมที่พึงมี

แผนการสำรองข้อมูล (Backup Plan) ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้

1. จัดทำแผนการสำรองข้อมูล (Backup Plan) เพื่อให้มั่นใจว่าข้อมูลสำคัญสามารถกู้คืนได้ในกรณีเกิดการขัดข้องของระบบหรือเกิดความเสียหายของข้อมูล โดยแผนการสำรองและกู้คืนข้อมูลต้องมีเนื้อหาอย่างน้อยดังนี้
 - (ก) ขอบเขต/รายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล
 - (ข) วิธีการ/เทคโนโลยีการสำรองข้อมูลและรูปแบบข้อมูล (Data Format)
 - (ค) ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
 - (ง) การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
 - (จ) ขั้นตอนและวิธีการกู้ข้อมูล
 - (ฉ) การทดสอบความสามารถในการกู้คืนข้อมูลจากอุปกรณ์สำรองข้อมูล (Restoration Test)
 - (ซ) สถานที่จัดเก็บข้อมูลสำรอง
2. สำรองข้อมูลเป็นระยะ ตามความถี่ที่เหมาะสมและมีความสอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) และต้องตรวจสอบให้มั่นใจว่าการสำรองข้อมูลสำเร็จทุกครั้ง
3. จัดเก็บข้อมูลสำรองไว้ในอุปกรณ์หรือสื่อที่แยกออกจากระบบงานหลัก (Offline/Offsite) และต้องไม่เชื่อมต่อกับคอมพิวเตอร์หรืออินเทอร์เน็ต รวมทั้งต้องมีมาตรการป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึง แก้วไข หรือทำลายข้อมูลสำรองได้

4. ทดสอบกระบวนการกู้คืนข้อมูลจากชุดข้อมูลสำรองเป็นระยะ เพื่อยืนยันว่าข้อมูลสามารถกู้คืนได้เมื่อจำเป็น ความถี่ในการทดสอบต้องสอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ของทรัพย์สินสารสนเทศที่เกี่ยวข้อง 5. ทบทวนแผนการสำรองและกู้คืนข้อมูลอย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่าแผนดังกล่าวยังคงมีความเหมาะสมและเป็นปัจจุบัน	
แนวทางการประเมิน	
1. ตรวจสอบการจัดทำแผนการสำรองข้อมูล (Backup Plan) ว่ามีเนื้อหาครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ข) และมีการทบทวนปรับปรุงแผนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ 2. ตรวจสอบว่ารอบเวลาการสำรองข้อมูล (Backup Frequency) สอดคล้องกับค่า RPO ที่หน่วยงานกำหนดไว้สำหรับแต่ละระบบ และตรวจสอบ Backup Logs เพื่อยืนยันว่าการสำรองข้อมูลสำเร็จ หากการสำรองล้มเหลว ต้องมีขั้นตอนและหลักฐานการแก้ไข 3. ตรวจสอบแหล่งการจัดเก็บข้อมูลสำรอง และมาตรการป้องกันความปลอดภัย 4. ตรวจสอบหลักฐานการทดสอบกู้คืนข้อมูล (Restoration Test) จากสื่อจัดเก็บจริง โดยความถี่ต้องเหมาะสมกับระดับความเสี่ยงของระบบนั้น ๆ 5. ตรวจสอบการแผนและผลทดสอบกู้คืน และหลักฐานการปรับปรุงแผน อย่างน้อยปีละหนึ่งครั้ง	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	PR.DS-11
ISO/IEC27001:2022	Annex A 8.13
ISO/IEC27701:2025	A3.24
ISO/IEC27017:2015	12.3.1
ISO/IEC27007:2020	-
ISO/IEC TS 27008:2019	12.3.1
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อ 4 (3)
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. หน่วยงานใช้เกณฑ์ใดในการกำหนดความถี่การสำรองข้อมูลเพื่อให้มั่นใจว่าสอดคล้องกับค่า RPO ของแต่ละระบบ และในกรณีที่ Backup ล้มเหลว (Failed) มีกระบวนการแจ้งเตือนและแก้ไขอย่างไรภายในระยะเวลาเท่าใด 2. มาตรการที่ใช้ป้องกันไม่ให้ข้อมูลสำรองถูกโจมตีหรือแก้ไขโดยผู้ไม่หวังดี (เช่น Ransomware) มีอะไรบ้าง 3. หน่วยงานมีรอบความถี่ในการทดสอบกู้คืนข้อมูล (Restoration Test) อย่างไร 4. ในการทดสอบกู้คืน (Restoration Test) ครั้งล่าสุด หน่วยงานเลือกใช้ข้อมูลจากสื่อประเภทใด (เช่น Disk, Tape, Cloud) และผลการทดสอบสามารถตอบโต้ภัยการใช้งานจริงในภาวะวิกฤตได้หรือไม่	

5. เมื่อมีการเพิ่มระบบงานใหม่หรือเปลี่ยนโครงสร้างพื้นฐาน หน่วยงานมีขั้นตอนการนำข้อมูลเหล่านั้นเข้าสู่แผนการสำรองข้อมูลและปรับปรุงคู่มือปฏิบัติงานอย่างไร

■ การสอบทานเอกสาร

1. สอบทานความครบถ้วนของแผนการสำรองข้อมูล เพื่อยืนยันความครบถ้วนของเนื้อหาว่าครอบคลุมการควบคุมที่พึงมีข้อ (ก) - (ข)
2. สอบทานรายงาน BIA เพื่อเทียบเคียงค่า RPO กับความถี่ในตารางสำรองข้อมูลจริง
3. สอบทานบันทึก/รายงานระบบสำรองข้อมูล (Backup Logs) เพื่อตรวจสอบความสำเร็จของการสำรองข้อมูล
4. สอบทานบันทึกเหตุการณ์ (Incident Log) ในกรณีที่ Backup ล้มเหลว (Failed) เพื่อยืนยันว่าได้มีการติดตามปัญหาและแก้ไข
5. สอบทานบันทึกการนำส่งข้อมูล Offsite ไปยังสถานที่จัดเก็บภายนอก ว่ามีการระบุวันเวลา ผลการปฏิบัติงาน
6. ตรวจสอบสิทธิ์ของผู้ดูแลระบบว่ามีการแยกหน้าที่ (Segregation of Duties) หรือมีการจำกัดสิทธิ์เพื่อป้องกันการลบข้อมูลสำรองโดยไม่ได้รับอนุญาต
7. สอบทานรายงานการทดสอบกู้คืน ว่ามีการระบุวันเวลาที่ทดสอบ ระบบที่ทดสอบ ผลลัพธ์ และข้อเสนอแนะเพื่อการปรับปรุง
8. สอบทานประวัติการแก้ไขเอกสาร (Version Control/Document History) ของแผนการสำรองข้อมูล เพื่อยืนยันรอบระยะเวลาการทบทวนอย่างน้อยปีละ 1 ครั้ง
9. สอบทานผลการปฏิบัติตามกฎหมาย มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด อย่างน้อย ดังนี้
 - ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (มีผลบังคับใช้ 10 กันยายน 2569) - ในกรณีที่หน่วยงานมีการประยุกต์ใช้บริการระบบคลาวด์ (Cloud Computing) จะต้องปฏิบัติตามข้อกำหนด 5.2.6.3 การสำรองข้อมูล (Information Backup)

■ เอกสารที่เกี่ยวข้อง

1. แผนการสำรองข้อมูล (Backup Plan)
2. รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
3. บันทึกผลการสำรองข้อมูล (Backup Logs)
4. บันทึกเหตุการณ์ (Incident Log) ในกรณีที่ Backup ล้มเหลว (Failed)
5. บันทึกการนำส่งข้อมูล Offsite
6. รายงานการทดสอบกู้คืน (Restoration Test Report)

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

1. ตรวจสอบการตั้งค่า Retention Policy ในซอฟต์แวร์สำหรับการสำรองข้อมูล ว่าสอดคล้องกับแผนการสำรองข้อมูล
2. ตรวจสอบว่ามีการเก็บข้อมูลสำรอง 3 ชุด ในสื่อ 2 ชนิด และ 1 ชุดอยู่นอกสถานที่ (Offsite) หรือตัดขาดจากเครือข่ายหลัก (Offline) จริง
3. ตรวจสอบว่าระบบสำรองข้อมูลมีการตั้งค่า Immutable Backup (เช่น S3 Object Lock หรือ Linux Hardened Repository) เพื่อป้องกันการลบไฟล์สำรองแม้จะได้สิทธิ์ Admin

การสื่อสารระหว่างการฟื้นฟูเหตุการณ์ความทางไซเบอร์ (Incident Recovery Communication)	
3.2.19 การสื่อสารระหว่างการฟื้นฟูเหตุการณ์ความทางไซเบอร์	
วัตถุประสงค์	
เพื่อให้มั่นใจว่า หน่วยงานมีการสื่อสารระหว่างการฟื้นฟูเหตุการณ์ความทางไซเบอร์ (Incident Recovery Communication) ที่ชัดเจน โดยครอบคลุมการแจ้งสถานะความคืบหน้าของการกู้คืนระบบแก่ผู้มีส่วนได้ส่วนเสีย และการสื่อสารต่อสาธารณชนผ่านช่องทางที่ได้รับอนุมัติ	
ความเสี่ยง	
เกิดความสับสนในการปฏิบัติงาน และเกิดความเสียหายต่อชื่อเสียงและภาพลักษณ์ของหน่วยงาน	
การควบคุมที่พึงมี	
การสื่อสารระหว่างการฟื้นฟูเหตุการณ์ความทางไซเบอร์ (Incident Recovery Communication) ควรครอบคลุมการดำเนินการอย่างน้อยต่อไปนี้ 1. สื่อสารความคืบหน้าของกิจกรรมการฟื้นฟู (เช่น ระบบใดที่ฟื้นฟูสำเร็จแล้วระบบใดที่อยู่ระหว่างการดำเนินการ) รวมถึงเมื่อระบบหรือบริการกลับมาใช้งานได้ปกติแล้วต้องแจ้งให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกทราบ 2. ให้ข้อมูลความคืบหน้าของกิจกรรมการฟื้นฟูกับสาธารณชน ต้องใช้วิธีการ ช่องทาง และข้อความ ที่ผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงาน	
แนวทางการประเมิน	
1. ตรวจสอบกระบวนการและช่องทางการสื่อสาร เพื่อยืนยันว่ามีกลไกการแจ้งสถานะการฟื้นฟูระบบที่เป็นระบบ 2. ตรวจสอบกระบวนการควบคุมข้อมูลและการสื่อสารสาธารณะ ว่าได้ระบุการใช้วิธีการ ช่องทาง และข้อความ ที่ผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงาน	
มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิงในการตรวจสอบ	
ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	-
แนวทางการจัดทำประมวลฯ พ.ศ. 2568	-
NIST CSF 2.0	RC.CO-03, RC.CO-04
ISO/IEC27001:2022	Clause 7.4
ISO/IEC27701:2025	Clause 7.4
ISO/IEC27017:2015	-
ISO/IEC27007:2020	A.4.4
ISO/IEC TS 27008:2019	-
มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	-
ขั้นตอนการตรวจสอบ	
■ การสัมภาษณ์ 1. ในระหว่างขั้นตอนการฟื้นฟูระบบ หน่วยงานมีกลไกในการปรับปรุงความคืบหน้า (เช่น ระบบใดใช้งานได้แล้ว ระบบใดยังแก้ไขอยู่) ให้กับผู้บริหาร พนักงาน ลูกค้า หรือผู้มีส่วนได้ส่วนเสียทราบอย่างไร	

2. หากจำเป็นต้องสื่อสารสถานการณ์หรือความคืบหน้าในการฟื้นฟูระบบให้สาธารณชนหรือสื่อมวลชนทราบ ใครคือผู้มีอำนาจในการอนุมัติเนื้อหาข้อความ (Message) และตัดสินใจเลือกช่องทาง (Channel) ก่อนที่จะเผยแพร่ข้อมูล

■ การสอบทานเอกสาร

1. สอบทานแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ว่าได้มีการระบุถึงขั้นตอน โครงสร้างการอนุมัติการแจ้งความคืบหน้าระหว่างการฟื้นฟู การประกาศสิ้นสุดเหตุการณ์ และรายชื่อผู้รับการสื่อสารทั้งภายในและภายนอก
2. สอบทานบันทึกการสื่อสาร (Communication Logs/Emails) ในเหตุการณ์จริง หรือจากการซ้อมแผน เพื่อดูความต่อเนื่องของการแจ้งสถานะ
3. สอบทานหลักฐานกระบวนการตรวจสอบและอนุมัติข้อความแถลงการณ์ต่อสาธารณะ (Press Release / Public Statement)

■ เอกสารที่เกี่ยวข้อง

1. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
2. บันทึกการสื่อสาร (Communication Logs/Emails)
3. บันทึกการขออนุมัติเนื้อหาและการเผยแพร่การสื่อสารต่อสาธารณชน (Approval Logs for Public Communication)
4. รายชื่อผู้มีสิทธิให้ข้อมูล (Authorized Spokespersons List)
5. แม่แบบข้อความสื่อสาร (Message Templates) ที่เตรียมไว้ล่วงหน้าสำหรับเหตุการณ์แต่ละระดับ

■ เทคนิคในการตรวจสอบ ในกรณีที่เป็นการตรวจสอบเชิงเทคนิค

-

บทที่ 4 การพัฒนากระบวนการตรวจประเมินหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ

การดำเนินการพัฒนากระบวนการตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้สอดคล้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตามประกาศฯ จะมีเครื่องมือสำหรับการตรวจประเมินอย่างน้อย 9 รายการ ดังนี้

1. แบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ (Statement of Applicability : SOA)
2. โปรแกรมการตรวจประเมิน (Audit Program)
3. แผนการตรวจประเมิน (Audit Plan)
4. รายงานการตรวจประเมิน (Audit Report)
5. แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)
6. แผนการแก้ไข (Corrective Action Plan)
7. รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)
8. ข้อเสนอแนะมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องตามประมวลแนวทางปฏิบัติสำหรับบริการทั้ง 4 บริการ
9. คู่มือขั้นตอนการปฏิบัติงานของกระบวนการตรวจประเมิน (Audit Manual) ซึ่งในคู่มือจะต้องมีการระบุรายละเอียดที่สำคัญ ได้แก่
 - วัตถุประสงค์ในการตรวจสอบ, ความเสี่ยง, การควบคุมที่พึงมี และแนวทางการประเมิน
 - มาตรฐานหรือกรอบปฏิบัติงานที่ใช้อ้างอิง (เช่น COBIT, COSO ERM, ISO ที่เกี่ยวข้อง)
 - ขั้นตอนการตรวจสอบอย่างละเอียด (เช่น ขั้นตอนการสัมภาษณ์, การสอบทานเอกสาร, เอกสารที่เกี่ยวข้อง และเทคนิคสำหรับการตรวจสอบเชิงเทคนิค)

4.1 แบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ (Statement of Applicability : SOA)

แบบฟอร์ม SOA เป็นเอกสารสำคัญที่หน่วยงานควรใช้เพื่อจัดเตรียมก่อนเข้าสู่กระบวนการตรวจสอบเพื่อรับรองว่าได้นำมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ไปประยุกต์ใช้ครบถ้วนตามข้อกำหนดของพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประมวลแนวทางปฏิบัติที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

1) วัตถุประสงค์ของเครื่องมือ

แบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ (SOA) มีวัตถุประสงค์ดังนี้

- (1) เพื่อบันทึกว่าหน่วยงานได้นำมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ใดไปประยุกต์ใช้จริงบ้าง โดยครอบคลุมทั้งข้อกำหนดภาคบังคับ (Mandatory Requirements) จำนวน 60 มาตรการ และแนวทางปฏิบัติที่ดี (Best Practices) จำนวน 19 มาตรการ รวม 79 มาตรการ
- (2) เพื่อเป็นเอกสารประกอบในการยืนยันขอบเขตและความครอบคลุมของระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งผู้ตรวจประเมินใช้เป็นจุดเริ่มต้นในการวางแผนและกำหนดขอบเขตการตรวจประเมิน

(3) เพื่อสรุปจำนวนเอกสารประกอบ (Document Lists) ที่หน่วยงานต้องจัดเตรียมสำหรับแต่ละมาตรการควบคุม

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

(1) หน่วยงานที่รับการตรวจสอบ ได้แก่ เจ้าหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และผู้บริหารระดับสูงของหน่วยงาน ซึ่งทำหน้าที่กรอกข้อมูลสถานะการนำมาตรการควบคุมไปใช้ พร้อมลงนามรับรองความถูกต้อง

(2) ผู้ตรวจสอบ ได้แก่ ผู้ตรวจสอบหลัก (Lead Auditor) และคณะผู้ตรวจสอบ ซึ่งใช้ข้อมูลจาก SOA เพื่อวางแผนการตรวจสอบ กำหนดขอบเขต และระบุเอกสารหลักฐานที่ต้องตรวจสอบในแต่ละมาตรการ

3) วิธีการใช้งาน

แบบฟอร์ม SOA ประกอบด้วย 3 แผ่นงาน (Sheet) ดังนี้

แผ่นงานที่ 1 สรุปการนำมาตรการควบคุมไปใช้ เป็นหน้าปกและสรุปภาพรวม โดยหน่วยงานต้องระบุชื่อหน่วยงาน ชื่อระบบงาน และวันที่ปรับปรุง พร้อมแสดงจำนวนมาตรการควบคุมที่นำไปใช้จำแนกตามประเภท (Mandatory / Best Practices) และลงนามโดยผู้จัดทำ ผู้ทบทวน และผู้อนุมัติ

แผ่นงานที่ 2 SOA เป็นแผ่นงานหลักที่บันทึกรายละเอียดมาตรการควบคุมทั้ง 79 รายการ แบ่งออกเป็น 4 ส่วน ได้แก่ (1) แนวทางการตรวจประเมินตามประมวลแนวทางปฏิบัติ (3.1.1–3.1.13) (2) แนวทางการตรวจประเมินตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (3.1.14–3.1.60) (3) แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามประมวลแนวทางปฏิบัติ (3.2.1–3.2.2) และ (4) แนวทางปฏิบัติที่ดี (Best Practices) สำหรับการตรวจประเมินตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (3.2.3–3.2.19) สำหรับแต่ละมาตรการ หน่วยงานต้องระบุสถานะการนำไปใช้ รายละเอียดของมาตรการปัจจุบัน และเอกสารจริงที่เป็นหลักฐาน

แผ่นงานที่ 3 Document Lists เป็นตารางรายการเอกสารประกอบทั้งหมดที่หน่วยงานต้องจัดเตรียม พร้อมระบุว่ามีเอกสารแต่ละรายการสัมพันธ์กับมาตรการควบคุมข้อใดบ้าง เพื่อให้หน่วยงานสามารถรวบรวมเอกสารได้อย่างครบถ้วน

4) โครงสร้างของเครื่องมือ

โครงสร้างของเครื่องมือแบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ มีรายละเอียดดังนี้

ตารางที่ 16 โครงสร้างแบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้

ชื่อหัวข้อ	คำอธิบาย
สพร. / รหัสมาตรการ	รหัสอ้างอิงมาตรการควบคุม เช่น 3.1.1, 3.1.6
หัวข้อ	ชื่อมาตรการควบคุม เช่น การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

ชื่อหัวข้อ	คำอธิบาย
อ้างอิง ประมวลแนวทางปฏิบัติฯ ข้อที่	ข้อที่ของประมวลแนวทางปฏิบัติที่สอดคล้อง
สาระสำคัญ	ข้อกำหนดหลักที่หน่วยงานต้องปฏิบัติตาม
ตัวอย่างเอกสารที่เกี่ยวข้อง	รายชื่อเอกสารหลักฐานที่แนะนำให้จัดเตรียม
การนำมาตรการควบคุมมาใช้	สถานะ: นำไปใช้ / ไม่นำไปใช้ พร้อมเหตุผล
รายละเอียดของมาตรการควบคุมปัจจุบัน	สิ่งที่หน่วยงานดำเนินการจริงในปัจจุบัน
เอกสารจริงของหน่วยงาน	รายชื่อเอกสารหลักฐานจริงที่หน่วยงานจัดเตรียม
หมายเหตุ	ข้อสังเกตหรือข้อมูลเพิ่มเติม

แบบฟอร์มคำรับรองการนำข้อควบคุมไปใช้ ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.2 โปรแกรมการตรวจประเมิน (Audit Program)

โปรแกรมการตรวจสอบ (Audit Program) เป็นเครื่องมือหลักที่ผู้ตรวจประเมินใช้ดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยครอบคลุมการตรวจสอบตามข้อกำหนดภาคบังคับ (Mandatory Requirements) และแนวทางปฏิบัติที่ดี (Best Practices) ตามลำดับ

1) วัตถุประสงค์ของเครื่องมือ

โปรแกรมการตรวจสอบ (Audit Program) มีวัตถุประสงค์ดังนี้

- (1) เพื่อกำหนดขอบเขต วัตถุประสงค์ และเกณฑ์การตรวจสอบแต่ละหัวข้ออย่างชัดเจน ให้ผู้ตรวจประเมินและหน่วยงานที่รับการตรวจสอบมีความเข้าใจตรงกัน
- (2) เพื่อเป็นแนวทางการตรวจสอบ (Audit Program) ที่ระบุสิ่งที่ควรตรวจสอบ วิธีการประเมิน และแนวคำถามสำหรับแต่ละมาตรการควบคุม ช่วยให้การตรวจสอบมีความสม่ำเสมอและครอบคลุม

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) หน่วยงานที่รับการตรวจสอบ ได้แก่ ผู้ประสานงานและเจ้าหน้าที่ผู้รับผิดชอบ ซึ่งใช้แผนงานนี้เป็นข้อมูลอ้างอิงเพื่อเตรียมเอกสารหลักฐานและตอบคำถามผู้ตรวจประเมิน
- (2) ผู้ตรวจสอบ ได้แก่ ผู้ตรวจสอบหลัก (Lead Auditor) และคณะผู้ตรวจสอบ ซึ่งทำหน้าที่กรอกผลการตรวจสอบในแต่ละข้อ พร้อมอ้างอิงหลักฐานที่ตรวจสอบ

3) วิธีการใช้งาน

โปรแกรมการตรวจสอบ (Audit Program) แยกออกเป็น 2 แผนงาน ตามประเภทของข้อกำหนด ได้แก่ แผนงานสำหรับข้อกำหนดภาคบังคับ (Mandatory) จำนวน 60 มาตรการ และแผนงานสำหรับแนวทางปฏิบัติที่ดี (Best Practices) จำนวน 19 มาตรการ ผู้ตรวจสอบ ศึกษาข้อมูลในแต่ละแถว ประกอบด้วย

วัตถุประสงค์ การควบคุมที่พึงมี และแนวทางการประเมิน จากนั้นดำเนินการตรวจสอบโดยใช้แนวคำถามและวิธีการที่ระบุ แล้วบันทึกระดับผลการตรวจสอบในคอลัมน์ ระดับผลการตรวจสอบ

4) โครงสร้างของเครื่องมือ

โครงสร้างของโปรแกรมการตรวจสอบ (Audit Program) รายละเอียดดังนี้

ตารางที่ 17 โครงสร้างโปรแกรมการตรวจสอบ (Audit Program)

ชื่อหัวข้อ	คำอธิบาย
ลำดับ	ลำดับที่ของมาตรการควบคุมในการตรวจสอบ
เลขอ้างอิงจากหลักเกณฑ์ฯ	รหัสอ้างอิงมาตรการควบคุม เช่น 3.1.1, 3.1.6
หัวข้อ	ชื่อมาตรการควบคุม เช่น การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
วัตถุประสงค์	เป้าหมายของการตรวจสอบมาตรการนั้น ๆ ว่าต้องการยืนยันสิ่งใด
การควบคุมที่พึงมี	ข้อกำหนดหรือมาตรการที่หน่วยงานต้องปฏิบัติตาม
แนวทางการประเมิน	วิธีการและแนวคำถามที่ผู้ตรวจประเมินใช้ตรวจสอบหลักฐาน
เลขอ้างอิงจากประมวลฯ	ข้อที่ของประมวลแนวทางปฏิบัติที่สอดคล้อง
ระดับผลการตรวจสอบ	ผลการตรวจ: Major NC / Minor NC / C / OBS / OFI (กรอกโดยผู้ตรวจสอบ)
ผลการตรวจสอบและหลักฐานการตรวจสอบ	ใช้บันทึกรายละเอียดผลการตรวจสอบของผู้ตรวจประเมินจากการสัมภาษณ์ การสอบถามเอกสาร และ/หรือการสังเกตการณ์การปฏิบัติงาน รวมถึงระบุเอกสาร หลักฐาน หรือข้อมูลที่ตรวจพบ ซึ่งใช้สนับสนุนการดำเนินการที่สอดคล้องตามข้อกำหนด
รายละเอียดความไม่สอดคล้อง/ ประเด็นที่พบ	ใช้บันทึกรายละเอียดความไม่สอดคล้องหรือประเด็นที่ควรปรับปรุง ที่ตรวจพบจากการประเมิน รวมถึงผลกระทบหรือสาเหตุที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลสำหรับการกำหนดแนวทางแก้ไขและปรับปรุงต่อไป

แบบร่างโปรแกรมการตรวจสอบ (Audit Program) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.3 แผนการตรวจประเมิน (Audit Plan)

แผนการตรวจสอบ (Audit Plan) เป็นเอกสารกำหนดการที่ผู้ตรวจสอบต้องจัดทำขึ้นในขั้นตอนเตรียมความพร้อมก่อนการตรวจสอบ เพื่อระบุกำหนดการ ขอบเขต และผู้เกี่ยวข้องในการตรวจ และสื่อสารให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบล่วงหน้า

1) วัตถุประสงค์ของเครื่องมือ

แผนการตรวจสอบ (Audit Plan) มีวัตถุประสงค์ดังนี้

- (1) เพื่อสื่อสารข้อมูลสำคัญให้ทุกฝ่ายรับทราบล่วงหน้า ได้แก่ วัตถุประสงค์และขอบเขตการตรวจสอบ เกณฑ์ที่ใช้ตรวจสอบ กำหนดการและช่วงเวลาของแต่ละกิจกรรม รายชื่อผู้ตรวจประเมินและผู้รับการตรวจสอบ
- (2) เพื่อกำหนดขอบเขตการตรวจสอบอย่างชัดเจน โดยระบุกระบวนการ/บริการที่ตรวจ ข้อมูลสำคัญที่เกี่ยวข้อง ระบบสารสนเทศ สถานที่ และผู้รับผิดชอบในแต่ละส่วน
- (3) เพื่อจัดสรรงานให้คณะผู้ตรวจสอบ โดยผู้ตรวจสอบแต่ละคนจะรับผิดชอบหัวข้อการตรวจสอบเฉพาะด้านตามกำหนดการ

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) หน่วยงานที่รับการตรวจสอบ ได้แก่ ผู้ประสานงาน คณะผู้บริหาร และคณะทำงานด้านความมั่นคงปลอดภัย ซึ่งใช้แผนนี้เพื่อจัดเตรียมบุคลากร เอกสารหลักฐาน และสถานที่ตามวันและเวลาที่กำหนด
- (2) ผู้ตรวจสอบ ได้แก่ ผู้ตรวจสอบหลัก (Lead Auditor) และคณะผู้ตรวจสอบ ซึ่งจะใช้แผนนี้เป็นกรอบการดำเนินงานตลอดวันตรวจสอบ

3) วิธีการใช้งาน

แผนการตรวจสอบ (Audit Plan) ประกอบด้วย 2 แผนงาน ได้แก่ Template (แบบว่าง) และตัวอย่าง (ข้อมูลตัวอย่างประกอบการกรอก) ผู้จัดทำแผนใช้แผนงาน Template และกรอกข้อมูลตามโครงสร้าง 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลเกี่ยวกับผู้จัดทำ ระบุชื่อผู้จัดทำ ชื่อหน่วยงาน เบอร์โทรศัพท์ และอีเมล

ส่วนที่ 2 ข้อมูลเกี่ยวกับการตรวจสอบ ระบุวัตถุประสงค์การตรวจสอบ และเกณฑ์ที่ใช้ในการตรวจสอบ เช่น หลักเกณฑ์การตรวจประเมินหน่วยงาน CII ของ สพร. และประมวลแนวทางปฏิบัติฯ

ส่วนที่ 3 ขอบเขตการตรวจสอบ ระบุกระบวนการ/บริการที่ตรวจสอบ พร้อมข้อมูลสำคัญ ระบบสารสนเทศที่เกี่ยวข้อง สถานที่ ผู้รับผิดชอบ และผู้ให้บริการภายนอก (ถ้ามี)

ส่วนที่ 4 แผนการตรวจสอบ (กำหนดการประจำวัน) ระบุวันที่ ช่วงเวลา หัวข้อการตรวจสอบ เกณฑ์อ้างอิง ผู้ตรวจสอบ และผู้รับการตรวจสอบ สำหรับแต่ละกิจกรรมตลอดวัน

4) โครงสร้างของเครื่องมือ

โครงสร้างของแผนการตรวจสอบ (Audit Plan) มีรายละเอียดดังนี้

ตารางที่ 18 โครงสร้างแผนการตรวจสอบ (Audit Plan)

คอลัมน์	คำอธิบาย / ตัวอย่าง
ส่วนที่ 1	ข้อมูลเกี่ยวกับผู้จัดทำ
ผู้จัดทำ	ชื่อผู้จัดทำแผนการตรวจสอบ หรือหัวหน้าคณะผู้ตรวจสอบ

คอลัมน์	คำอธิบาย / ตัวอย่าง
ชื่อหน่วยงาน	หน่วยงานที่รับผิดชอบการตรวจสอบ เช่น กลุ่มตรวจสอบภายใน / ฝ่ายตรวจสอบภายใน
เบอร์โทรศัพท์	เบอร์โทรศัพท์ติดต่อของผู้ประสานงานการตรวจสอบ
อีเมล	อีเมลสำหรับติดต่อประสานงาน เช่น audit@องค์กร.go.th
ส่วนที่ 2	ข้อมูลเกี่ยวกับการตรวจสอบ
วัตถุประสงค์การตรวจสอบ	ระบุวัตถุประสงค์ของการตรวจ เช่น ประเมินความสอดคล้องตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อกำหนดที่เกี่ยวข้อง
เกณฑ์ในการตรวจสอบ	ระบุข้อกำหนดที่ใช้เป็นเกณฑ์ในการตรวจ เช่น หลักเกณฑ์การตรวจประเมิน CII ของ สพร.
ส่วนที่ 3	ขอบเขตการตรวจสอบ
ชื่อกระบวนการ/บริการ	บริการหรือภารกิจสำคัญที่ตรวจ เช่น ระบบบริการประชาชน ระบบชำระเงิน ระบบฐานข้อมูลกลาง
ข้อมูลสำคัญ	ข้อมูลที่เกี่ยวข้องกับระบบ เช่น ข้อมูลผู้ใช้งาน ข้อมูลส่วนบุคคล ข้อมูลธุรกรรม หรือข้อมูลสำคัญขององค์กร
ชื่อระบบสารสนเทศ	ชื่อระบบที่อยู่ในขอบเขต เช่น ERP System, HR System, Data Center, Mobile Application
สถานที่	สถานที่ตั้งระบบหรือสถานที่ตรวจ เช่น สำนักงานใหญ่ ศูนย์ข้อมูล หรือ Cloud Environment
ผู้รับผิดชอบ	เจ้าของระบบหรือหน่วยงานที่รับผิดชอบ เช่น IT Department, System Owner
ผู้ให้บริการภายนอก (ถ้ามี)	ผู้ให้บริการ Cloud, Outsource, Managed Service Provider หรือ Vendor ที่เกี่ยวข้อง
ส่วนที่ 4	แผนการตรวจสอบ
วันที่	วันที่ดำเนินการตรวจสอบ
เวลา	ช่วงเวลาของแต่ละกิจกรรม เช่น 9:00–9:15 น. / 9:15–10:00 น.
หัวข้อการตรวจสอบ	เช่น การกำกับดูแลและการบริหารความเสี่ยง / การตรวจสอบและติดตามผลการแก้ไข / การสร้างความตระหนักรู้
เกณฑ์ในการตรวจสอบ	เช่น หลักเกณฑ์ฯ สพร. 3.1.6, 3.1.7–3.1.9 / ประมวลแนวทางปฏิบัติฯ 17.1–17.5
ผู้ตรวจสอบ	ผู้ตรวจสอบทีมที่ 1 หรือทีมที่ 2 (ทำงานคู่ขนานกัน)
ผู้รับการตรวจสอบ	เช่น คณะผู้บริหาร / คณะทำงานด้านความมั่นคงปลอดภัย / ฝ่าย IT / CERT

แบบร่างแผนการตรวจสอบ (Audit Plan) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.4 รายงานการตรวจประเมิน (Audit Report)

รายงานการตรวจสอบ (Audit Report) ออกแบบโดยสอดคล้องกับ **แนวทางการจัดทำประมวลฯ พ.ศ. 2568** เป็นเอกสารทางการที่ผู้ตรวจประเมินจัดทำขึ้นภายหลังการตรวจประเมินเสร็จสิ้น เพื่อบันทึกและนำเสนอผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยมีชั้นความลับระดับ ลับมาก (Secret) สำหรับรายงานแก่ผู้บริหารระดับสูงของหน่วยงานที่รับการตรวจประเมิน และจัดส่งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานควบคุมหรือกำกับดูแล เป็นกรณีเฉพาะ

1) วัตถุประสงค์ของเครื่องมือ

รายงานการตรวจสอบ (Audit Report) มีวัตถุประสงค์ดังนี้

- (1) เพื่อบันทึกและรายงานผลการตรวจสอบความสอดคล้องด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเกณฑ์มาตรฐานที่กำหนด ครอบคลุมทั้งข้อกำหนดภาคบังคับ 60 ข้อ และแนวทางปฏิบัติที่ดี 19 ข้อ
- (2) เพื่อสรุปประเด็นบกพร่อง (non-conformity) ที่พบ พร้อมจำแนกระดับความรุนแรงเป็น Major NC, Minor NC, C, OBS และ OFI เพื่อให้หน่วยงานเข้าใจลำดับความสำคัญในการดำเนินการแก้ไข
- (3) เพื่อเป็นฐานข้อมูลอ้างอิงในการจัดทำแผนการแก้ไข (Corrective Action Plan) และติดตามความคืบหน้าในรอบการตรวจประเมินถัดไป รวมทั้งใช้ประกอบการรายงานต่อ สกมช. และหน่วยงานกำกับดูแลตามข้อกำหนดกฎหมาย

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) ผู้บริหารและผู้มีส่วนได้ส่วนเสียของหน่วยงาน ได้แก่ ผู้บริหารระดับสูง คณะกรรมการกำกับดูแล และผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งรับรายงานเพื่อรับทราบสถานะความสอดคล้องและใช้ประกอบการตัดสินใจเชิงบริหาร รวมถึงการวางแผนปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ขององค์กร
- (2) ผู้ตรวจสอบ ได้แก่ ผู้ตรวจสอบหลัก (Lead Auditor) และคณะผู้ตรวจสอบ ซึ่งทำหน้าที่จัดทำและรับรองรายงาน โดยรวบรวมข้อมูลจากโปรแกรมการตรวจสอบ (Audit Program) และแบบฟอร์ม CAR มาสรุปเป็นรายงานที่ครอบคลุมและมีความน่าเชื่อถือ

3) วิธีการใช้งาน

ผู้ตรวจสอบใช้แบบร่าง Audit Report เป็นกรอบในการจัดทำรายงาน โดยกรอกข้อมูลตามโครงสร้าง 11 หัวข้อหลัก ดังนี้

- (1) บทสรุปผู้บริหาร (Executive Summary) สรุปภาพรวมผลการตรวจสอบ สถานะความสอดคล้อง และประเด็นสำคัญที่ต้องดำเนินการแก้ไขเร่งด่วน รวมถึงติดตามผลการแก้ไขจากรอบการตรวจก่อนหน้า (ถ้ามี)
- (2) วัตถุประสงค์ (Purpose) ระบุเป้าหมายของการตรวจสอบครั้งนี้
- (3) คำจำกัดความ (Definition) นิยามคำศัพท์เฉพาะที่ใช้ในรายงาน
- (4) เกณฑ์ในการตรวจสอบ (Audit Criteria) ระบุกฎหมาย มาตรฐาน และหลักเกณฑ์ที่ใช้อ้างอิง
- (5) การจำแนกระดับผลการตรวจสอบ แสดงตารางเกณฑ์จำแนก 5 ระดับ (Major NC / Minor NC / C / OBS / OFI)
- (6) ขอบเขตการตรวจสอบ (Audit Scope) ระบุระบบ กระบวนการ และบริการที่อยู่ในขอบเขต
- (7) ข้อมูลเกี่ยวกับการตรวจสอบ (Audit Timeline & Stakeholders) ระยะเวลาและรายชื่อคณะผู้ตรวจสอบ
- (8) วิธีการและแนวทางการตรวจสอบ (Audit Methodology) อธิบายวิธีการตรวจสอบ 3 ด้าน ได้แก่ การสัมภาษณ์ การตรวจสอบเอกสาร และการสังเกตการณ์/ตรวจสอบค่าตั้งระบบ
- (9) สิ่งที่พบจากการตรวจสอบ (Audit Finding) สรุปจำนวนและประเภทข้อบกพร่องที่พบ อ้างอิงรายละเอียดจากแบบฟอร์ม CAR
- (10) แผนการแก้ไข (Corrective Action Plan) สรุปแนวทางและกรอบระยะเวลาการแก้ไข
- (11) สรุปผลการตรวจสอบ (Auditor Conclusion) ความเห็นสรุปของคณะผู้ตรวจประเมินต่อระดับความสอดคล้องโดยรวมของหน่วยงาน

4) โครงสร้างของเครื่องมือ

โครงสร้างของรายงานการตรวจสอบ (Audit Report) มีรายละเอียดดังนี้

ตารางที่ 19 โครงสร้างรายงานการตรวจสอบ (Audit Report)

หัวข้อ	ชื่อหัวข้อ	เนื้อหาสำคัญ
1	บทสรุปผู้บริหาร (Executive Summary)	ภาพรวมผล สถานะจากรอบก่อน จำนวน NC แยกตามประเภท ประเด็นสำคัญ และ กรอบเวลาแก้ไข
2	วัตถุประสงค์ (Purpose)	เป้าหมายการตรวจสอบ
3	คำจำกัดความ (Definition)	นิยามคำศัพท์เฉพาะที่ใช้ในรายงาน
4	เกณฑ์การตรวจสอบ (Audit Criteria)	พ.ร.บ. ไซเบอร์ 2562, หลักเกณฑ์ สพร., ประมวลแนวทางปฏิบัติฯ และกรอบมาตรฐานอื่น ๆ
5	การจำแนกระดับผลการตรวจสอบ	ตารางนิยาม 5 ระดับ: Major NC / Minor NC / C / OBS / OFI
6	ขอบเขตการตรวจสอบ (Audit Scope)	ระบบ กระบวนการ บริการ และสถานที่ที่ตรวจสอบ
7	ข้อมูลเกี่ยวกับการตรวจสอบ (Audit Timeline & Stakeholders)	ระยะเวลา ช่วงเวลาตรวจ และรายชื่อคณะผู้ตรวจสอบ

หัวข้อ	ชื่อหัวข้อ	เนื้อหาสำคัญ
8	วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	วิธีการดำเนินการตรวจสอบ เช่น การสัมภาษณ์ ตรวจสอบเอกสาร สังเกตการณ์ และ หน้าที่การตั้งค่าระบบจริง
9	สิ่งที่พบจากการตรวจสอบ (Audit Finding)	ตารางสรุปจำนวน NC ทุกระดับ อ้างอิงรายละเอียดจากภาคผนวก ก (CAR)
10	แผนการแก้ไข (Corrective Action Plan)	ตารางสรุปแนวทางและกรอบเวลา อ้างอิงรายละเอียดจากภาคผนวก ก (CAR)
11	สรุปผลการตรวจสอบ (Auditor Conclusion)	ความเห็นของคณะผู้ตรวจประเมินต่อระดับความสอดคล้องโดยรวม

แบบร่างแผนการตรวจสอบ (Audit Plan) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ขดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.5 แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)

แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR) เป็นเอกสารที่ผู้ตรวจประเมินจัดทำขึ้นหลังพบข้อบกพร่องหรือความไม่สอดคล้องในระหว่างการตรวจประเมิน เพื่อแจ้งและกำหนดให้หน่วยงานดำเนินการแก้ไขอย่างเป็นทางการ

1) วัตถุประสงค์ของเครื่องมือ

แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR) มีวัตถุประสงค์ดังนี้

- (1) เพื่อบันทึกข้อบกพร่องหรือความไม่สอดคล้อง (Non-Conformity) ที่พบจากการตรวจประเมิน พร้อมระบุระดับความรุนแรงตามเกณฑ์มาตรฐาน ได้แก่ Major NC, Minor NC, OBS และ OFI
- (2) เพื่อแจ้งหน่วยงานอย่างเป็นทางการให้ดำเนินการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) และจัดทำแผนการแก้ไขภายในกรอบเวลาที่กำหนด
- (3) เพื่อติดตามความคืบหน้าของการแก้ไขในทุกระดับ ตั้งแต่หน่วยงานผู้ดำเนินการแก้ไข ผู้ตรวจสอบ จนถึงการรายงานต่อ สกมช. และหน่วยงานกำกับดูแล

2) กลุ่มผู้ใช้งานเครื่องมือ

ผู้ตรวจสอบ บันทึกข้อมูลในส่วนที่ 1 (สิ่งที่พบจากการตรวจสอบ)

3) วิธีการใช้งาน

แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR) ผู้ตรวจประเมินกรอกรายละเอียดข้อบกพร่องที่พบในส่วนที่ 1 โดยระบุสิ่งที่พบจากการตรวจสอบในแต่ละข้อ พร้อมระบุระดับผลการตรวจสอบและผลกระทบ ข้อมูลส่วนนี้อ้างอิงโดยตรงจากแผนงานโปรแกรมการตรวจประเมิน

4) โครงสร้างของเครื่องมือ

โครงสร้างของแบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR) มีรายละเอียดดังนี้

ตารางที่ 16 โครงสร้างแบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR)

ชื่อหัวข้อ	คำอธิบาย
(1) ข้อ / (2) เลขอ้างอิงจากหลักเกณฑ์ฯ / (3) หัวข้อ / (4) เลขอ้างอิงจากประมวลฯ	ระบุมাত্রการที่พบข้อบกพร่อง อ้างอิงจากโปรแกรมการตรวจประเมิน
(5) รายละเอียดความไม่สอดคล้อง / (6) ระดับผลการตรวจสอบ / (7) ผลกระทบ / (8) ข้อเสนอแนะ	บรรยายข้อบกพร่องพร้อมระดับ: Major NC / Minor NC / OBS / OFI

แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request : CAR) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.6 แผนการแก้ไข (Corrective Action Plan)

แผนการแก้ไข (Corrective Action Plan) เป็นเอกสารที่หน่วยงานจัดทำขึ้นเพื่อตอบสนองต่อข้อบกพร่องที่ผู้ตรวจประเมินระบุไว้ โดยครอบคลุมการวิเคราะห์สาเหตุที่แท้จริง การกำหนดมาตรการแก้ไข และการติดตามความคืบหน้าจนกระทั่งปิดข้อบกพร่องได้สำเร็จ

1) วัตถุประสงค์ของเครื่องมือ

แผนการแก้ไข (Corrective Action Plan) มีวัตถุประสงค์ดังนี้

- (1) เพื่อให้หน่วยงานวิเคราะห์สาเหตุที่แท้จริง (Root Cause) ของข้อบกพร่องที่พบ โดยเฉพาะกรณีที่เป็น Major NC หรือ Minor NC ซึ่งต้องมีการวิเคราะห์อย่างเป็นระบบ
- (2) เพื่อกำหนดมาตรการแก้ไขที่เหมาะสม ทั้งการแก้ไขเบื้องต้น (Correction) เพื่อบรรเทาผลกระทบในทันที และแผนการแก้ไขระยะยาว (Corrective Action) เพื่อป้องกันการเกิดซ้ำ
- (3) เพื่อเป็นเอกสารติดตามความคืบหน้าที่ผู้ตรวจประเมินใช้ตรวจสอบและพิจารณาความเหมาะสมของการแก้ไข ก่อนส่งต่อผลให้หน่วยงานระดับนโยบาย

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) คณะทำงานของหน่วยงานที่รับการตรวจสอบ ได้แก่ ผู้รับผิดชอบด้านความมั่นคงปลอดภัย และทีมงานที่เกี่ยวข้อง ซึ่งทำหน้าที่กรอกข้อมูลวิเคราะห์สาเหตุ กำหนดมาตรการแก้ไข ผู้รับผิดชอบ และกรอบเวลาดำเนินการ
- (2) ผู้ตรวจสอบ ซึ่งทำหน้าที่พิจารณาความเหมาะสมและความครบถ้วนของแผนการแก้ไขที่หน่วยงานนำเสนอ และบันทึกผลการพิจารณาในส่วนที่ 3

3) วิธีการใช้งาน

แผนการแก้ไข (Corrective Action Plan) ถูกบรรจุไว้ในส่วนที่ 2 ของแบบฟอร์ม และมีขั้นตอนการใช้งานดังนี้

ขั้นตอนที่ 1 หน่วยงานรับทราบข้อบกพร่องจากส่วนที่ 1 (Audit Finding) แล้ววิเคราะห์สาเหตุที่แท้จริงในคอลัมน์ (1) วิเคราะห์สาเหตุ โดยเน้นการหาสาเหตุของปัญหา ไม่ใช่เพียงอาการที่ปรากฏ

ขั้นตอนที่ 2 กำหนดการแก้ไขเบื้องต้น (Correction) ในคอลัมน์ (2) เพื่อแก้ไขผลกระทบที่เกิดขึ้นแล้ว และกำหนดแผนการแก้ไขระยะยาว (Corrective Action Plan) ในคอลัมน์ (3) เพื่อป้องกันการเกิดซ้ำ

ขั้นตอนที่ 3 ระบุกรอบเวลาในคอลัมน์ (4) วันที่เริ่มต้น และ (5) วันที่คาดว่าจะแล้วเสร็จ พร้อมปรับปรุงสถานะในคอลัมน์ (6) และบันทึกวันที่เสร็จจริงในคอลัมน์ (7) เมื่อดำเนินการครบถ้วน

ขั้นตอนที่ 4 ผู้ตรวจประเมินตรวจสอบและบันทึกผลการพิจารณาในส่วนที่ 3 (การติดตามการแก้ไข) เพื่อยืนยันว่าแผนและผลการแก้ไขมีความเหมาะสม

4) โครงสร้างของเครื่องมือ

โครงสร้างของแผนการแก้ไข (Corrective Action Plan) มีรายละเอียดดังนี้

ตารางที่ 21 โครงสร้างแผนการแก้ไข (Corrective Action Plan)

ชื่อหัวข้อ	คำอธิบาย
(1) วิเคราะห์สาเหตุ (Root Cause)	ระบุสาเหตุที่แท้จริงของข้อบกพร่อง (บังคับสำหรับ Major NC และ Minor NC)
(2) การแก้ไขเบื้องต้น (Correction)	มาตรการแก้ไขทันทีเพื่อลดผลกระทบที่เกิดขึ้นแล้ว
(3) แผนการแก้ไข (Corrective Action Plan)	มาตรการระยะยาวเพื่อป้องกันการเกิดซ้ำ
(4) วันที่เริ่มต้น	วันที่คาดว่าจะเริ่มดำเนินการแก้ไข
(5) วันที่คาดว่าจะแล้วเสร็จ	กำหนดส่งผลการแก้ไข
(6) ผู้รับผิดชอบ	ผู้รับผิดชอบการแก้ไข
(7) สถานะการแก้ไข	ระบุสถานะ เช่น รอดำเนินการ / กำลังดำเนินการ / แล้วเสร็จ
(8) วันที่แล้วเสร็จจริง	วันที่ดำเนินการแก้ไขครบถ้วนจริง
(9) หมายเหตุ / คำอธิบายเพิ่มเติม	ข้อมูลเพิ่มเติมหรือเหตุการณ์ที่ล่าช้า

แผนการแก้ไข (Corrective Action Plan) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ขดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.7 รายงานการทบทวนโดยฝ่ายบริหาร (Management Review)

รายงานการทบทวนโดยฝ่ายบริหาร (Management Review) เป็นเอกสารทางการที่จัดทำขึ้นภายหลังการตรวจประเมินและการจัดทำรายงาน Audit Report เสร็จสิ้น เพื่อนำเสนอผลการตรวจสอบต่อ

ผู้บริหารระดับสูงสำหรับทบทวนผลการดำเนินงาน มีมติสั่งการให้ปรับปรุง และรับรองความพร้อมของระบบ
การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยมีชั้นความลับระดับ ลับ (Confidential)

1) วัตถุประสงค์ของเครื่องมือ

รายงานการทบทวนโดยฝ่ายบริหาร (Management Review) มีวัตถุประสงค์ดังนี้

- (1) เพื่อนำเสนอผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารระดับสูงอย่างเป็นระบบ ครอบคลุมสถานะความสอดคล้องโดยรวม จำนวนข้อบกพร่องจำแนกตามระดับ และประเด็นสำคัญที่ต้องดำเนินการแก้ไข
- (2) เพื่อรับทราบมติที่ประชุมและข้อสั่งการจากฝ่ายบริหาร ซึ่งเป็นการแสดงความรับผิดชอบและความมุ่งมั่นของผู้นำองค์กรในการขับเคลื่อนการแก้ไขปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์
- (3) เพื่อประเมินความเพียงพอของทรัพยากร งบประมาณ และบุคลากร รวมทั้งพิจารณาปัจจัยภายนอกและภายในที่มีผลกระทบต่อระบบความมั่นคงปลอดภัย เพื่อกำหนดทิศทางการพัฒนาในรอบถัดไป

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) ผู้บริหารระดับสูงและคณะกรรมการกำกับดูแลของหน่วยงาน ซึ่งทำหน้าที่รับทราบผลการตรวจสอบ ออกมติสั่งการ และรับรองแผนการแก้ไข เพื่อให้การดำเนินการปรับปรุงได้รับการสนับสนุนจากระดับนโยบาย
- (2) ผู้ตรวจสอบและผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งทำหน้าที่จัดทำและนำเสนอรายงาน รวบรวมข้อมูลจาก Audit Report และ CAR มาสรุปเป็นรายงานที่เหมาะสมสำหรับระดับบริหาร

3) วิธีการใช้งาน

ผู้จัดทำรายงานใช้แบบร่างรายงานการทบทวนโดยฝ่ายบริหาร (Management Review) เป็นกรอบในการจัดทำรายงาน โดยกรอกข้อมูลตามโครงสร้าง 8 หัวข้อหลัก ดังนี้

- (1) บทนำ บริบทการตรวจสอบ ชื่อหน่วยงาน ช่วงเวลา และวัตถุประสงค์โดยสรุป
- (2) สถานะการดำเนินการจากรายงานครั้งก่อน (ถ้ามี) ทบทวนมติและข้อสั่งการจากการประชุมฝ่ายบริหารรอบก่อน ติดตามสถานะว่าเสร็จสิ้น อยู่ระหว่างดำเนินการ หรือล่าช้า พร้อมระบุผลลัพธ์
- (3) สรุปผลการตรวจสอบภายใน นำเสนอจำนวนข้อบกพร่องจำแนกตามระดับ (Major NC / Minor NC / C / OBS / OFI) พร้อมตารางรายละเอียดความไม่สอดคล้อง งบประมาณ/ทรัพยากรที่จำเป็น และผู้รับผิดชอบ

- (4) สรุปมติที่ประชุม/ข้อสั่งการจากฝ่ายบริหาร บันทึกหลังการประชุม ระบุมติและข้อสั่งการ เฉพาะรายการ CAR พร้อมผู้รับผิดชอบและกำหนดเสร็จ
- (5) ประเมินความเหมาะสมของทรัพยากร วิเคราะห์ข้อจำกัดด้านบุคลากร เทคโนโลยี และ งบประมาณ พร้อมข้อเสนอแนะการจัดสรรทรัพยากรเพิ่มเติม
- (6) การเปลี่ยนแปลงภายนอกและภายในที่มีผลกระทบ ระบุมติเปลี่ยนแปลงด้านกฎหมาย ภัยคุกคาม หรือโครงสร้างองค์กรที่ส่งผลกระทบต่อระบบความมั่นคงปลอดภัย
- (7) ข้อเสนอแนะและทิศทางการพัฒนา กำหนดเป้าหมายเชิงกลยุทธ์ระยะสั้นและระยะยาวเพื่อยกระดับความสอดคล้องสู่มาตรฐานสากล
- (8) การดำเนินการตามกฎหมาย ระบุมติสถานะการจัดส่งรายงานและแผนการแก้ไขให้หน่วยงาน กำกับดูแลตามข้อกำหนด พ.ร.บ. ไซเบอร์ พ.ศ. 2562

4) โครงสร้างของเครื่องมือ

โครงสร้างของรายงานการทบทวนโดยฝ่ายบริหาร (Management Review) มีรายละเอียดดังนี้

ตารางที่ 22 โครงสร้างรายงานการทบทวนโดยฝ่ายบริหาร (Management Review)

หัวข้อ	ชื่อหัวข้อ	เนื้อหาสำคัญ / ตัวอย่างเนื้อหา
1	บทนำ	บริบทการตรวจสอบ ชื่อหน่วยงาน CII วันที่ดำเนินการ และวัตถุประสงค์
2	สถานะการดำเนินการจากรายงานครั้งก่อน	ตารางติดตามมติ: หมายเลข CAR / สรุปประเด็น / ข้อสั่งการ / ผู้รับผิดชอบ / สถานะ (เสร็จสิ้น/อยู่ระหว่างดำเนินการ/ล่าช้า)
3	สรุปผลการตรวจสอบภายใน	ตารางจำนวน NC ตามระดับ + ตารางรายละเอียด CAR: หมายเลข / ระดับ / รายละเอียด / ผู้รับผิดชอบ / งบประมาณที่จำเป็น
4	สรุปมติที่ประชุม/ข้อสั่งการจากฝ่ายบริหาร	ตารางมติ: หมายเลข CAR / ระดับ NC / รายละเอียดประเด็น / มติและข้อสั่งการ (กรอกหลังการประชุม)
5	ประเมินความเหมาะสมของทรัพยากร	วิเคราะห์ข้อจำกัดบุคลากร/เทคโนโลยี/งบประมาณ และข้อเสนอแนะการจัดสรรทรัพยากรเพิ่มเติม
6	การเปลี่ยนแปลงภายนอกและภายใน	ปัจจัยที่มีผลกระทบ เช่น ประกาศ สกมช. ฉบับใหม่ ภัยคุกคามที่เพิ่มขึ้น การเปลี่ยนแปลงโครงสร้างองค์กร
7	ข้อเสนอแนะและทิศทางการพัฒนา	เป้าหมายเชิงกลยุทธ์ระยะสั้น/ยาว เช่น การนำ SIEM มาใช้ การพัฒนาศักยภาพบุคลากร การจัดทำ C-SCRM

หัวข้อ	ชื่อหัวข้อ	เนื้อหาสำคัญ / ตัวอย่างเนื้อหา
8	การดำเนินการตามกฎหมาย	สถานการณ์จัดส่งรายงานและแผน CAP ให้หน่วยงานกำกับดูแล ภายใน 30 วันตามข้อกำหนด พ.ร.บ. ไซเบอร์ พ.ศ. 2562

ร่างรายงานการทบทวนโดยฝ่ายบริหาร (Management Review) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ขดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

4.8 ข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องตามประมวลแนวทางปฏิบัติสำหรับบริการทั้ง 4 บริการ

ข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) เป็นเอกสารอ้างอิงที่รวบรวมการเชื่อมโยง (mapping) ระหว่างข้อกำหนดตามหลักเกณฑ์การตรวจประเมิน CII ของ สพร. จำนวน 79 มาตรการ เข้ากับมาตรฐานสากล 7 ฉบับ ได้แก่ NIST CSF 1.1, NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27701:2025, ISO/IEC 27017:2015, ISO/IEC 27007:2020, และ ISO/IEC TS 27008:2019 รวมถึงแนวทางการจัดทำประมวลฯ พ.ศ. 2568 และมาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565

1) วัตถุประสงค์ของเครื่องมือ

ข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ มีวัตถุประสงค์ดังนี้

- (1) เพื่อเป็นแหล่งอ้างอิงให้หน่วยงาน CII เข้าใจความสัมพันธ์ระหว่างข้อกำหนดของ สพร. กับมาตรฐานสากล ช่วยให้หน่วยงานที่ได้รับการรับรองมาตรฐานสากลอยู่แล้ว สามารถประเมินระดับความพร้อมต่อข้อกำหนดของ สพร. ได้ล่วงหน้า
- (2) เพื่อช่วยให้ผู้ตรวจสอบและคณะทำงานมองเห็นภาพรวมของมาตรการควบคุมในเชิงเปรียบเทียบ และระบุช่องว่าง (Gap) ที่ยังต้องดำเนินการเพิ่มเติม
- (3) เพื่อสนับสนุนการวางแผนปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับกรอบมาตรฐานหลายฉบับพร้อมกัน

2) กลุ่มผู้ใช้งานเครื่องมือ

เครื่องมือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) หน่วยงาน CII ได้แก่ เจ้าหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศ ผู้บริหาร และทีมตรวจสอบภายใน ซึ่งใช้เครื่องมือนี้ประกอบการวางแผนปรับปรุงระบบ และการเตรียมความพร้อมก่อนรับการตรวจประเมิน
- (2) ผู้ตรวจสอบ ซึ่งใช้เครื่องมือนี้เพื่อวิเคราะห์ความสอดคล้องของการควบคุมที่หน่วยงานมีอยู่ กับมาตรฐานสากล และระบุแนวทางการแก้ไขที่มีประสิทธิภาพ

3) วิธีการใช้งาน

ค้นหาข้อกำหนดที่ต้องการในคอลัมน์ A (รหัส สพร.) จากนั้นอ่านการเชื่อมโยง (mapping) กับมาตรฐานสากลในคอลัมน์ E-M เพื่อระบุว่ามาตรการควบคุมเดิมที่หน่วยงานมีครอบคลุมข้อกำหนดใดบ้าง

4) โครงสร้างของเครื่องมือ

โครงสร้างของข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ มีรายละเอียดดังนี้

ตารางที่ 23 โครงสร้างข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ

คอลัมน์	ชื่อหัวข้อ	คำอธิบาย
A	สพร. (รหัสมาตรการ)	รหัสอ้างอิงข้อกำหนด เช่น 3.1.1, 3.2.3
B	หัวข้อ	ชื่อมาตรการควบคุม เช่น การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
C	อ้างอิง ประมวลแนวทางปฏิบัติฯ ข้อที่	ข้อที่ของประมวลแนวทางปฏิบัติที่สอดคล้อง เช่น 17.1
D	สาระสำคัญ	ข้อกำหนดหรือแนวทางที่หน่วยงานต้องหรือควรปฏิบัติ
E	NIST CSF 1.1	รหัส NIST Cybersecurity Framework เวอร์ชัน 1.1 ที่สอดคล้อง เช่น ID.GV-3
F	NIST CSF 2.0	รหัส NIST CSF เวอร์ชัน 2.0 ที่สอดคล้อง เช่น GV.OC-03
G	ISO/IEC 27001:2022	ข้อกำหนด ISO/IEC 27001:2022 ที่สอดคล้อง เช่น Clause 9.2.1, Annex A 5.35
H	ISO/IEC 27701:2025	ข้อกำหนด ISO/IEC 27701:2025 ที่สอดคล้อง (ด้านข้อมูลส่วนบุคคล)
I	ISO/IEC 27017:2015	ข้อกำหนด ISO/IEC 27017:2015 ที่สอดคล้อง (ด้านบริการคลาวด์)
J	ISO/IEC 27007:2020	ข้อกำหนด ISO/IEC 27007:2020 ที่สอดคล้อง (ด้านการตรวจประเมิน)
K	ISO/IEC TS 27008:2019	ข้อกำหนด ISO/IEC TS 27008:2019 ที่สอดคล้อง (ด้านการทบทวนมาตรการ)
L	แนวทางการจัดทำประมวลฯ พ.ศ. 2568	อ้างอิงเอกสารแนบที่เกี่ยวข้อง เช่น เอกสารแนบ 1, เอกสารแนบ 2
M	มาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565	ข้อที่ของประกาศมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้อง เช่น ข้อ 4 (3)

ข้อสรุปมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ฯ ได้ถูกรวบรวมไว้ใน ภาคผนวก ข. การเปรียบเทียบประมวลแนวทางปฏิบัติ พ.ศ. 2564 ของเอกสารฉบับนี้

4.9 คู่มือขั้นตอนการปฏิบัติงานของกระบวนการตรวจสอบ (Audit Manual)

คู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการตรวจสอบ (Audit Manual) เป็นเอกสารอ้างอิงหลักที่รวบรวมแนวทางการตรวจสอบสำหรับมาตรการควบคุมทุกข้อในหลักเกณฑ์การตรวจประเมินหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งส่วนที่เป็นข้อกำหนดภาคบังคับ (Mandatory Requirements) จำนวน 60 มาตรการ และแนวทางปฏิบัติที่ดี (Best Practices) จำนวน 19 มาตรการ รวม 79 มาตรการ

1) วัตถุประสงค์ของคู่มือ

คู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการตรวจสอบ (Audit Manual) มีวัตถุประสงค์ดังนี้

- (1) เพื่อเป็นแนวทางปฏิบัติเชิงลึกสำหรับผู้ตรวจประเมินในการตรวจสอบความสอดคล้องของหน่วยงาน CII ครอบคลุมมาตรการควบคุมทั้ง 79 ข้อ โดยระบุสิ่งที่ต้องตรวจ วิธีตรวจ และหลักฐานที่ต้องพบในแต่ละมาตรการไว้อย่างชัดเจน
- (2) เพื่อเป็นการรับรองความสม่ำเสมอของกระบวนการตรวจสอบ ให้ผู้ตรวจสอบทุกคนใช้แนวทางและเกณฑ์ตัดสินเดียวกัน ลดความแตกต่างของผลการตรวจสอบที่เกิดจากดุลพินิจส่วนบุคคล
- (3) เพื่อเชื่อมโยงข้อกำหนดในหลักเกณฑ์ฯ กับมาตรฐานสากล (NIST CSF, ISO/IEC 27001, ISO/IEC 27007) และกฎหมายที่เกี่ยวข้อง ช่วยให้ผู้ตรวจสอบเข้าใจบริบทและความสำคัญของแต่ละมาตรการควบคุม

2) กลุ่มผู้ใช้งานคู่มือ

คู่มือนี้มีกลุ่มผู้ใช้งานหลัก 2 กลุ่ม ดังนี้

- (1) ผู้ตรวจสอบ ทั้งผู้ตรวจสอบหลัก (Lead Auditor) และคณะผู้ตรวจสอบ ซึ่งใช้คู่มือนี้เพื่อวางแผนการตรวจ กำหนดคำถามสัมภาษณ์ ระบุเอกสารหลักฐานที่ต้องตรวจสอบ และตัดสินระดับผลการตรวจสอบในแต่ละมาตรการควบคุม
- (2) หน่วยงานที่เตรียมรับการตรวจประเมิน ได้แก่ เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ และทีมงานที่เกี่ยวข้อง ซึ่งสามารถศึกษาคู่มือนี้เพื่อทำความเข้าใจขั้นตอนการตรวจสอบ เตรียมเอกสารหลักฐาน และประเมินความพร้อมของหน่วยงานก่อนรับการตรวจประเมินจริง

3) วิธีการใช้งาน

คู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการตรวจสอบ (Audit Manual) จัดเนื้อหาตามหมายเลขข้อกำหนด (3.1.1–3.1.60 สำหรับ Mandatory และ 3.2.1–3.2.19 สำหรับ Best Practices) โดยแต่ละมาตรการควบคุมจะนำเสนอข้อมูลเป็นลำดับขั้นตอน ดังนี้

ขั้นตอนที่ 1 ศึกษาวัตถุประสงค์และความเสี่ยง เพื่อเข้าใจว่ามาตรการควบคุมนั้นมุ่งป้องกันความเสี่ยงใด และผลกระทบที่อาจเกิดขึ้นหากไม่มีการควบคุมที่เพียงพอ

ขั้นตอนที่ 2 ทบทวนการควบคุมที่พึงมี เพื่อกำหนดว่าสิ่งที่หน่วยงานต้องมีและปฏิบัติตามคืออะไร ก่อนเริ่มการตรวจสอบจริง

ขั้นตอนที่ 3 ใช้แนวทางการประเมินและขั้นตอนการตรวจสอบ ซึ่งประกอบด้วย 4 วิธีการ ได้แก่ การสัมภาษณ์ (Interview) ผู้รับผิดชอบ, การสอบทานเอกสาร (Document Review) ตามรายการที่ระบุ, การตรวจสอบเชิงเทคนิค (Technical Inspection) สำหรับข้อกำหนดที่เกี่ยวข้องกับระบบและอุปกรณ์, และการสังเกตการณ์ (Observation) กระบวนการทำงานจริง

ขั้นตอนที่ 4 เปรียบเทียบผลกับมาตรฐานอ้างอิง (NIST CSF, ISO/IEC 27001, ISO/IEC 27007 เป็นต้น) เพื่อยืนยันความสอดคล้อง และบันทึกระดับผลการตรวจสอบตามเกณฑ์ที่กำหนด (Major NC / Minor NC / C / OBS / OFI)

4) โครงสร้างของเครื่องมือ

โครงสร้างของคู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการการตรวจสอบ (Audit Manual) มีรายละเอียดดังนี้

ตารางที่ 24 โครงสร้างคู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการการตรวจสอบ (Audit Manual)

องค์ประกอบ	รายละเอียด
(1) วัตถุประสงค์การตรวจสอบ (Audit Objective)	ระบุจุดมุ่งหมายของการตรวจสอบในแต่ละข้อกำหนด เพื่อให้ผู้ตรวจประเมินเข้าใจว่าต้องการยืนยันสิ่งใด
(2) ความเสี่ยงที่เกี่ยวข้อง (Related Risk)	อธิบายความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นหากหน่วยงานไม่ดำเนินการตามข้อกำหนดนั้น
(3) การควบคุมที่พึงมี (Expected Control)	ระบุมาตรการควบคุมที่หน่วยงานต้องจัดให้มีตามข้อกำหนดของกฎหมายและประมวลแนวทางปฏิบัติ
(4) แนวทางการประเมิน (Assessment Guidance)	แนวทางปฏิบัติสำหรับผู้ตรวจประเมินในการรวบรวมหลักฐานและพิจารณาระดับความสอดคล้อง
(5) การเชื่อมโยงมาตรฐาน (Standard Reference)	ตารางแสดงการเชื่อมโยงข้อกำหนดกับกรอบมาตรฐานสากล ได้แก่ NIST CSF 1.1, NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27007, ISO/IEC TS 27008 และกฎหมายไทย
(6) ขั้นตอนการตรวจสอบ (Audit Steps)	รายละเอียดการตรวจสอบแบ่งเป็น 4 วิธี ได้แก่ การสัมภาษณ์ (Interview) การสอบทานเอกสาร (Document Review) การสังเกตการณ์ (Observation) และการตรวจสอบทางเทคนิค (Technical Testing)

คู่มือขั้นตอนการปฏิบัติงานของแต่ละกระบวนการการตรวจสอบ (Audit Manual) ได้ถูกรวบรวมไว้ใน ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ ของเอกสารฉบับนี้

บรรณานุกรม

- [1] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562). คัดจากราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 69 ก วันที่ 27 พฤษภาคม 2562.
- [2] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562). คัดจากราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 69 ก วันที่ 27 พฤษภาคม 2562.
- [3] คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566. คัดจากราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 18 ง วันที่ 18 มกราคม 2567.
- [4] คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. (2564). ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564. คัดจากราชกิจจานุเบกษา เล่มที่ 138 ตอนพิเศษ 303 ง วันที่ 10 ธันวาคม 2564.
- [5] คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565. คัดจากราชกิจจานุเบกษา เล่มที่ 139 ตอนพิเศษ 140 ง วันที่ 20 มิถุนายน 2565.
- [6] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2568). ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2568.
- [7] International Organization for Standardization. (2015). Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC Standard No. 27017:2015). Retrieved from <https://www.iso.org/standard/43757>
- [8] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022). Retrieved from <https://www.iso.org/standard/27001>
- [9] International Organization for Standardization. (2025). Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC Standard No. 27701:2025). Retrieved from <https://www.iso.org/standard/27701>
- [10] International Organization for Standardization. (2025). Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC Draft International Standard No. 27017:2025 DIS). Retrieved from <https://www.iso.org/standard/27017>

- [11] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Special Publication [SP] 1297). U.S. Department of Commerce. Retrieved from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29>

ภาคผนวก

- ภาคผนวก ก. รายงานการศึกษาเพิ่มเติม
- ภาคผนวก ข. การเปรียบเทียบประมวลแนวทางปฏิบัติ พ.ศ. 2564 และมาตรฐานสากล
- ภาคผนวก ค. เอกสารต้นแบบที่สำคัญ

ภาคผนวก ก. รายงานการศึกษาเพิ่มเติม

1. สรุปผลการวิเคราะห์ ประกาศ กม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564 และ ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 จัดทำขึ้นเพื่อกำหนดกรอบการดำเนินงานและแนวทางปฏิบัติสำหรับ หน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญ ที่ต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางดิจิทัลที่เพิ่มสูงขึ้น เนื้อหาของเอกสารมุ่งเน้นไปที่หลักการ ความรับผิดชอบร่วมกัน (Shared Responsibility) ระหว่าง ผู้ใช้บริการคลาวด์ (CSC) และ ผู้ให้บริการคลาวด์ (CSP) เพื่อสร้างระบบนิเวศที่ปลอดภัยและมีประสิทธิภาพตามนโยบาย Cloud First โดยมีการแบ่งข้อกำหนดและกระบวนการตรวจรับรองออกเป็น 3 ระดับ ตามความรุนแรงของผลกระทบ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง ซึ่งครอบคลุมตั้งแต่การกำกับดูแลเชิงนโยบายไปจนถึงมาตรการทางเทคนิคเชิงลึก เช่น การควบคุมการเข้าถึง การเข้ารหัสข้อมูล และการจัดการเหตุการณ์ละเมิดความปลอดภัย เพื่อให้สอดคล้องกับมาตรฐานสากลและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ทั้งนี้ประกาศจะมีผลบังคับใช้เมื่อพ้นกำหนดสองปีนับแต่วันที่ประกาศในราชกิจจานุเบกษา (10 กันยายน 2567)

ความสอดคล้องและความแตกต่างระหว่างเอกสารทั้งสองฉบับ

มาตรฐานฉบับนี้ มีการอ้างอิงและใช้หลักการพื้นฐานต่อยอดมาจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยเอกสารทั้งสองฉบับโดยภาพรวมมีการกำหนดมาตรการรักษาความปลอดภัยบางส่วนในหมวดหมู่ที่ใกล้เคียงกัน เช่น การควบคุมการเข้าถึง (Access Control), การจัดการผู้ให้บริการภายนอก (Third Party/Supplier Management), การจัดการเหตุภัยคุกคาม (Incident Management) และการเข้ารหัสข้อมูล อย่างไรก็ตาม มาตรฐานฯ คลาวด์ พ.ศ. 2567 เป็นมาตรฐานเฉพาะทางสำหรับสภาพแวดล้อมระบบคลาวด์ (IaaS, PaaS, SaaS) โดยใช้หลักการ ความร่วมรับผิดชอบ (Shared Responsibilities) ซึ่งแบ่งแยกข้อกำหนดชัดเจนระหว่าง ผู้ใช้บริการคลาวด์ (CSC) และ ผู้ให้บริการคลาวด์ (CSP) โดยมีความเชื่อมโยงระหว่างข้อประกาศ ดังนี้

ตารางที่ 25 ความสอดคล้องของ มาตรฐานฯ คลาวด์ พ.ศ. 2567 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
ส่วนที่ 1: ประมวลแนวทางปฏิบัติ (Code of Practice)	
องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
17.1 จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง โดยขอบเขตครอบคลุม:(ก) กระบวนการและผลวิเคราะห์ผลกระทบทางธุรกิจ (BIA)(ข) บริการที่สำคัญของหน่วยงาน(ค) การปฏิบัติตาม พ.ร.บ. ไซเบอร์ฯ และแนวปฏิบัติ	- แบ่งระดับความเข้มข้นของการตรวจรับรองตามระดับผลกระทบ (ต่ำ, กลาง, สูง) ของข้อมูลหรือระบบสารสนเทศ โดยมีตั้งแต่การประเมินตนเอง (Self-assessment), การรับรองโดยหน่วยงานกำกับดูแล (Attestation) ไปจนถึงการรับรองโดย

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
	หน่วยงานตรวจรับรอง (Certify Body) รวมถึง บังคับให้ผู้ให้บริการคลาวด์ต้องมีใบรับรองสากล ระดับสูง เช่น ISO/IEC 27001, 27017, 27018, 27701 หรือ CSA STAR ตามระดับผลกระทบ - 5.1.3.5 การทบทวนด้านการรักษาความมั่นคง ปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)
17.2 จัดส่งผลสรุปรายงานการตรวจสอบฯ ต่อสำนักงาน (สกมช.) ภายใน 30 วันนับแต่ดำเนินการแล้วเสร็จ และส่ง สำเนาให้หน่วยงานควบคุมหรือกำกับดูแล	- ให้หน่วยงานจัดส่งผลสรุปการดำเนินการต่อ สำนักงาน (สกมช.) ภายใน 30 วัน นับตั้งแต่วันที่ ดำเนินการแล้วเสร็จ - 5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)
17.3 หากผลตรวจสอบพบการไม่ปฏิบัติตาม (Non-compliance) ให้จัดส่ง แผนการดำเนินการแก้ไข (Corrective Action Plan) ไปยังสำนักงานภายใน 30 วัน โดยระบุ รายละเอียดการแก้ไขและระยะเวลาดำเนินการ	ไม่ระบุ
17.4 หาก กกม. ให้ปรับปรุงแผนการดำเนินการแก้ไข หน่วยงานต้องปรับปรุงและนำส่งแผนแก้ไขใหม่ภายใน ระยะเวลาที่กำหนด พร้อมส่งสำเนาให้หน่วยงานกำกับดูแล	ไม่ระบุ
17.5 เมื่อแผนดำเนินการแก้ไขได้รับความเห็นชอบ หน่วยงาน ต้องดำเนินการตามแผนให้แล้วเสร็จภายในระยะเวลาที่ระบุไว้	ไม่ระบุ
องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์	
นโยบายและระเบียบวิธีปฏิบัติ อันประกอบไปด้วยกำหนด นโยบาย โครงสร้างองค์กร บทบาทหน้าที่ และจัดทำระเบียบวิธี ปฏิบัติ/กระบวนการในการบริหารความเสี่ยง โดยต้องประเมิน ความเสี่ยงอย่างน้อยปีละ 1 ครั้ง	5.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies) 5.1.2.1 บทบาทและความรับผิดชอบด้านการรักษา ความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)
18.1 การประเมินความเสี่ยง (Risk Assessment)	
18.1 (ก) การระบุความเสี่ยง (Risk Identification) ระบุความ เสี่ยงจากภัยคุกคามและช่องโหว่ ที่มาจากกระบวนการ ระบบงาน บุคลากร หรือปัจจัยภายนอก	ไม่ระบุ
18.1 (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ทำความ เข้าใจและวิเคราะห์ความเสี่ยงเพื่อหาแนวทางจัดการที่เหมาะสม	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
18.1 (ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ประเมินโอกาสเกิด ผลกระทบ และกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ไม่ระบุ
18.2 การจัดการความเสี่ยง (Risk Treatment) มีแนวทางจัดการ ควบคุม ป้องกันความเสี่ยง เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงความคุ้มค่า และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ไม่ระบุ
18.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) มีกระบวนการติดตามและทบทวนความเสี่ยง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้	ไม่ระบุ
18.4 การรายงานความเสี่ยง (Risk Reporting) รายงานผลต่อคณะกรรมการเป็นประจำ และทบทวนกระบวนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	ไม่ระบุ
องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์	
19.1 การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	
19.1 (ก) โครงสร้างทีมรับมือเหตุการณ์ (CIRT) ระบุบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ	5.1.2.1 บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities) 5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
19.1 (ข) โครงสร้างการรายงานเหตุการณ์ ให้เป็นไปตามการรายงานตามภาระหน้าที่ภายใต้ พ.ร.บ. และกฎหมายที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities) 5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures) 5.2.10.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)
19.1 (ค), (ง), (จ), (ฉ) ขั้นตอนการเผชิญเหตุ ต้องมีการกำหนดเกณฑ์การเรียกใช้งาน (Activate), การจำกัดขอบเขต (Containment), กระบวนการกู้คืน (Recovery) และการสอบสวน (Investigate) สาเหตุและผลกระทบ	ไม่ระบุ
19.1 (ซ) การเก็บรักษาหลักฐาน (Preservation of Evidence) ขั้นตอนการเก็บรักษาหลักฐานก่อนเริ่มกระบวนการกู้คืน รวมถึงหลักฐานทางคอมพิวเตอร์เพื่อสนับสนุนการสอบสวน	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
19.1 (ข) ระเบียบวิธีการมีส่วนร่วมกับบุคคลภายนอก สำหรับการทำงานร่วมกับบุคคลภายนอก เช่น ผู้ขายบริการด้านนิติวิทยาศาสตร์, การกู้คืน, และการบังคับใช้กฎหมายเพื่อดำเนินคดี	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities) 5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures) 5.1.3.3 การปกป้องบันทึกข้อมูล (Protection of Records)
19.1 (ฉ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review) การทบทวนหลังการดำเนินการเพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ไม่ระบุ
19.2 การสื่อสารแผนการรับมือ ต้องสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมด	5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
19.3 การทบทวนแผนตามรอบเวลา ทำการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ	5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
19.4 การทบทวนแผนเมื่อมีการเปลี่ยนแปลง	5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
ส่วนที่ 2: กรอบมาตรฐาน (Standard Framework)	
หัวข้อหลักที่ 1 Identify	
21.1 การจัดการทรัพย์สิน (Asset Management)	
21.1.1 จัดทำและปรับปรุงทะเบียนทรัพย์สิน (Inventory) ให้เป็นปัจจุบัน ระบุชื่อ ฟังก์ชัน ความสำคัญ เจ้าของ ที่ตั้ง และการพึ่งพากันของทรัพย์สิน	5.2.2.1 ทะเบียนทรัพย์สิน (Inventory of Assets) 5.2.2.2 การบ่งชี้ข้อมูล (Labelling of Information) 5.1.3.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)
21.1.2 ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง (Network scope & interface)	5.2.7.2 การแบ่งแยกในเครือข่าย (Segregation in Networks)
21.1.3 ตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง	5.2.2.1 ทะเบียนทรัพย์สิน (Inventory of Assets)
21.1.4 ประเมินความเสี่ยงด้านไซเบอร์ของทรัพย์สินที่อยู่ในทะเบียน อย่างน้อยปีละ 1 ครั้ง	ไม่ระบุ
21.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง	
21.2.1 ประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
21.2.2 ปรับปรุงทะเบียนความเสี่ยง (Risk Register) โดยระบุวันที่, คำอธิบาย, โอกาสเกิด, ความรุนแรง, การจัดการความเสี่ยง, เจ้าของ, สถานะ และความเสี่ยงที่เหลือ (Residual Risk)	ไม่ระบุ
21.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ	
21.3.1 - 21.3.2 หน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญต้องประเมินช่องโหว่ระบบ IT และ ICS ตามหลักบริหารความเสี่ยง โดยต้องครอบคลุมทั้งด้านโฮสต์ เครือข่าย และการตรวจสอบสถาปัตยกรรมให้ครบถ้วน	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
21.3.3 หน่วยงานรัฐและหน่วยงาน CII ต้องประเมินช่องโหว่เพื่อระบุจุดอ่อนก่อนเริ่มทดสอบระบบใหม่หรือเปลี่ยนแปลงระบบสำคัญ เช่น การเพิ่มโมดูลและการอัปเดตเทคโนโลยี	5.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification) 5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities) 5.2.8.2 นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)
21.3.4 ดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเน้นระบบ IT ที่เชื่อมต่ออินเทอร์เน็ตตามความเหมาะสมของระดับความเสี่ยง และต้องพิจารณาผลกระทบที่อาจเกิดขึ้นจากการทดสอบอย่างรอบคอบด้วย	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
21.3.5 การกำหนดขอบเขตการทดสอบเจาะระบบต้องครอบคลุมทั้งส่วนของโฮสต์ เครือข่าย และแอปพลิเคชันที่เกี่ยวข้องกับบริการสำคัญ โดยต้องให้ความสำคัญเป็นพิเศษกับทุกระบบที่มีการเชื่อมต่อกับอินเทอร์เน็ตโดยตรงเพื่อให้เกิดความมั่นคงปลอดภัยสูงสุด	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
21.3.6 ควรทดสอบเจาะระบบอย่างน้อยปีละครั้งหรือเมื่อมีการเปลี่ยนแปลงระบบสำคัญเพื่อยืนยันความมั่นคงปลอดภัยของหน่วยงานรัฐและ CII	5.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification) 5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities) 5.2.8.2 นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)
21.3.7 ผู้ทดสอบเจาะระบบ CII ต้องมีใบเซอร์ฯ ระดับสากล มีความเป็นอิสระ และมีคุณสมบัติตามเกณฑ์ของหน่วยงานกำกับดูแล	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
21.3.8 การทดสอบเจาะระบบโดยผู้ให้บริการภายนอกต้องอยู่ภายใต้การกำกับดูแลของหน่วยงานอย่างใกล้ชิดทุกขั้นตอน	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
21.3.9 สร้างกระบวนการติดตามและจัดการแก้ไขช่องโหว่ที่พบ	5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
21.3.10 นำส่งสำเนารายงานผลการทดสอบเจาะระบบให้ สกมช. หากได้รับการร้องขอ	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)
21.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)	
21.4.1 องค์กรต้องรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ แม้จะใช้ผู้ให้บริการภายนอก	5.2.9.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)
21.4.2 กำหนดข้อกำหนดด้านไซเบอร์ในข้อตกลง SLA หรือ เงื่อนไขสัญญากับผู้ให้บริการภายนอก ครอบคลุมภาระหน้าที่, ห่วงโซ่อุปทาน (Supply chain) และสิทธิในการตรวจสอบ	5.2.9.2 การจัดการกับการรักษาความมั่นคง ปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements) 5.2.9.3 ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศ และการสื่อสาร (Information and Communication Technology Supply Chain)
21.4.3 สร้างกระบวนการตรวจสอบความถูกต้อง (Audit/Review) ผู้ให้บริการภายนอกตามสัญญา	ไม่ระบุ
21.4.4 เปรียบเทียบเงื่อนไขของสัญญาจ้างให้สอดคล้องกับ ข้อกำหนดทางกฎหมาย/ข้อบังคับใหม่	5.1.3.1 การระบุกฎหมายที่บังคับใช้และข้อกำหนด ตามสัญญา (Identification of Applicable Legislation and Contractual Requirements) 5.1.3.4 กฎระเบียบที่เกี่ยวข้องกับมาตรการควบคุมการ เข้ารหัสข้อมูล (Regulation of Cryptographic Controls)
หัวข้อหลักที่ 2 Protect	
22.1 การควบคุมการเข้าถึง (Access Control)	
22.1.1 จำกัดการเข้าถึงบริการสำคัญ เฉพาะบุคลากร กิจกรรม อุปกรณ์ และอินเทอร์เน็ตที่ได้รับอนุญาตเท่านั้น	5.2.3.1 การควบคุมเข้าถึงเครือข่ายและบริการ เครือข่าย (Access to Networks and Network Services) 5.2.3.2 การลงทะเบียนและยกเลิกการลงทะเบียน สำหรับผู้ใช้ (User Registration and Deregistration) 5.2.3.6 การจำกัดการเข้าถึงข้อมูล (Information Access Restriction) 5.2.3.7 การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
22.1.2 ใช้เทคนิคการตรวจสอบสิทธิ์ (Authentication) ที่สอดคล้องกับโปรไฟล์ความเสี่ยง	5.2.3.5 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users) 5.2.3.8 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)
22.1.3 เก็บบันทึกการเข้าถึงทั้งหมด (Logs) และตรวจสอบบันทึกเพื่อหากิจกรรมที่ผิดปกติอย่างสม่ำเสมอ	5.1.3.3 การปกป้องบันทึกข้อมูล (Protection of Records) 5.2.6.4 การบันทึกเหตุการณ์ (Event Logging) 5.2.6.5 การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information) 5.2.6.6 บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้บริหารงาน (Administrator and Operator Logs) 5.2.6.7 การซิงโครไนซ์นาฬิกา (Clock Synchronization)
22.1.4 การเข้าถึงอินเทอร์เน็ต (เช่น USB) และแบบลอจิคอล ต้องมีการกำกับดูแลและดำเนินการในสถานที่หากเป็นไปได้	ไม่ระบุ
22.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	
22.2.1 จัดทำมาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้ครอบคลุมทุกระบบและอุปกรณ์โดยสอดคล้องกับโปรไฟล์ความเสี่ยงของบริการสำคัญ	ไม่ระบุ
22.2.2 มาตรฐานต้องมี: สิทธิเข้าถึงน้อยสุด (Least Privilege), แบ่งแยกหน้าที่ (Separation of Duties), รหัสผ่านซับซ้อน, ลบบัญชี/แอป/พอร์ตที่ไม่ใช้, ป้องกันมัลแวร์, และอัปเดตแพตช์	5.2.3.5 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users) 5.2.3.3 การจัดสรรการเข้าถึงของผู้ใช้ (User Access Provisioning) 5.2.3.4 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights) 5.2.6.8 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
22.2.3 หน่วยงานรัฐและ CII ต้องบังคับใช้มาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้เรียบร้อยก่อนเริ่มเชื่อมต่ออุปกรณ์หรือปรับปรุงระบบทุกครั้ง	ไม่ระบุ
22.2.4 หน่วยงานรัฐและ CII ต้องทบทวนมาตรฐาน Security Baseline อย่างน้อยปีละครั้งเพื่อให้มั่นใจว่ายังรับมือกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
22.2.5 จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบการเปลี่ยนแปลงระบบ	5.2.6.1 การจัดการการเปลี่ยนแปลง (Change Management) 5.2.6.9 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments)
22.3 การเชื่อมต่อระยะไกล (Remote Connection)	
22.3.1 มีมาตรการป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต สำหรับการเชื่อมต่อระยะไกล	ไม่ระบุ
22.3.2 เปิดใช้เมื่อจำเป็น, ใช้การพิสูจน์ตัวตนที่แข็งแกร่ง, ใช้การเข้ารหัส (เช่น https, ssh), ไม่อนุญาตคำสั่งระบบระยะไกลโดยไม่จำเป็น, และจำกัดการไหลของข้อมูล	5.2.7.1 นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures) 5.2.3.8 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures) 5.2.4.1 นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls) 5.2.4.2 การจัดการกุญแจ (Key Management)
22.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	
22.4.1 ควบคุมการใช้สื่อแบบถอดได้ (เช่น ปิดพอร์ต USB และเปิดเมื่อจำเป็น), ใช้เฉพาะที่ได้รับอนุญาต, และตรวจสอบมัลแวร์ก่อนเชื่อมต่อ	5.2.5.2 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment) 5.2.4.1 นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)
22.4.2 เข้ารหัสข้อมูลที่ละเอียดอ่อนบนสื่อบันทึกข้อมูลแบบถอดได้	ไม่ระบุ
22.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	
22.5.1 หน่วยงานรัฐและ CII ต้องสร้างความตระหนักรู้ด้านไซเบอร์ให้บุคลากรทุกระดับและบุคคลภายนอกอย่างทั่วถึง โดยครอบคลุมทั้งหน้าที่ความรับผิดชอบ ความรู้ด้านกฎหมาย และการแจ้งเตือนภัยคุกคามอย่างสม่ำเสมอเพื่อให้เกิดความปลอดภัยในการปฏิบัติงานอย่างเป็นรูปธรรม	5.2.1.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษาและการฝึกอบรม (Information Security Awareness, Education and Training)
22.5.2 ต้องทบทวนแผนสร้างความตระหนักรู้ไซเบอร์อย่างน้อยปีละครั้งเพื่อให้เนื้อหาทันสมัยและเหมาะสมกับสถานการณ์ปัจจุบัน	5.2.1.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษาและการฝึกอบรม

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
	(Information Security Awareness, Education and Training)
22.6 การแบ่งปันข้อมูล (Information Sharing)	
22.6 กำหนดขั้นตอนแบ่งปันข้อมูลเหตุการณ์และภัยคุกคามไซเบอร์ รวมถึงมาตรการบรรเทาผลกระทบ กับบุคคลที่เกี่ยวข้องหรือได้รับผลกระทบ เพื่อให้สามารถป้องกันตนเองได้	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)
หัวข้อหลักที่ 3 Detect	
23.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
23.1.1 (ก) สร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน	5.2.6.4 การบันทึกเหตุการณ์ (Event Logging) 5.2.6.5 การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information) 5.2.6.6 บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)
23.1.1 (ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ	5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
23.1.1 (ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญหรือไม่	ไม่ระบุ
23.1.2 ดำเนินการทบทวนกลไกและกระบวนการ (ตามข้อ 23.1.1) อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ	ไม่ระบุ
หัวข้อหลักที่ 4 Respond	
24.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	ไม่ระบุ
24.1.1 จัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้การรับมือดำเนินการได้อย่างมีประสิทธิภาพ	5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
24.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	
24.2.1 จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ภัยคุกคาม	ไม่ระบุ
24.2.2 แผนสื่อสารต้องประกอบด้วย: การจัดตั้งทีมสื่อสาร, ระบุสถานการณ์จำลอง, ระบุกระบวนการแจ้งกลุ่มเป้าหมาย,	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
ระบุโฆษก/ผู้เชี่ยวชาญ และกำหนดแพลตฟอร์ม/ช่องทางการเผยแพร่	
24.2.3 ต้องแน่ใจว่าแผนการสื่อสารรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้สอดคล้องกันในช่วงวิกฤต	ไม่ระบุ
24.2.4 ฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง	ไม่ระบุ
24.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	
24.3.1 หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน หากได้รับคำสั่งเป็นลายลักษณ์อักษรจากคณะกรรมการ	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities) 5.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)
24.3.2 ปฏิบัติตามคำขอของคณะกรรมการในการให้ข้อมูลที่เกี่ยวข้องเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อม เช่น แผนการรับมือภัยคุกคาม ขั้นตอนการปฏิบัติงาน (SOP) และแผนการสื่อสาร	5.1.2.2 การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)
หัวข้อหลักที่ 5 Recover	
25.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	
25.1.1 จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการสำคัญสามารถดำเนินการต่อไปได้เมื่อเกิดการหยุดชะงักจากเหตุการณ์ด้านไซเบอร์กำหนดระยะเวลาและเกณฑ์ที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) สอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน	5.2.9.2 การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)
25.1.2 ตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนในการรับมือและฟื้นฟูระบบจากภัยคุกคามไซเบอร์	ไม่ระบุ
ข้ออื่น ๆ เพิ่มเติม	
-	5.2.5.1 ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานฯ คลาวด์ พ.ศ. 2567
-	5.2.6.2 การบริหารจัดการความจุ (Capacity Management)
-	5.2.6.3 การสำรองข้อมูล (Information Backup)

สรุปข้อสังเกต

แม้ข้อกำหนดในประกาศทั้งสองฉบับ จะมีจุดร่วมที่สามารถเชื่อมโยงและอ้างอิงถึงกันได้ในระดับหลักการปฏิบัติ (General Practice) แต่จากการศึกษาเชิงลึกพบว่าในรายละเอียดข้อกำหนดรายข้อนั้นมีความแตกต่างกันมีนัยสำคัญ ดังนั้น (ร่าง) หลักเกณฑ์การตรวจประเมินฯ ในเอกสารฉบับนี้ จึงถูกออกแบบมาเพื่อใช้เป็น บรรทัดฐานการตรวจประเมินขั้นพื้นฐาน (Baseline Audit) ในข้อประกาศดังกล่าวที่สอดคล้องกันเท่านั้น ทั้งนี้ หน่วยงานจำเป็นต้องพิจารณารายละเอียดทางเทคนิคและข้อกำหนดเฉพาะเจาะจงเพิ่มเติม เพื่อให้การดำเนินงานสอดคล้องกับ มาตรฐานฯ คลาวด์ พ.ศ. 2567 อย่างครบถ้วนสมบูรณ์

2. สรุปผลการวิเคราะห์ ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564 และ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ พ.ศ. 2568

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 เป็นข้อกำหนดทางกฎหมายและเทคนิคที่ออกโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยมีวัตถุประสงค์เพื่อยกระดับขีดความสามารถในการป้องกันภัยคุกคามทางไซเบอร์สำหรับโครงสร้างพื้นฐานดิจิทัลของประเทศ ประกาศฉบับนี้อาศัยอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดมาตรฐานขั้นต่ำในการบริหารจัดการคอมพิวเตอร์และระบบสารสนเทศที่ให้บริการผ่านเว็บ มาตรฐานฉบับนี้มีผลบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยครอบคลุมเว็บไซต์ทุกรูปแบบที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ไม่ว่าจะเป็นการติดตั้งในรูปแบบ On-Premises, Cloud Service หรือ Web Hosting โดยสาระสำคัญของมาตรฐานแบ่งออกเป็น 2 องค์ประกอบหลัก ได้แก่

1. การกำกับดูแลด้านความมั่นคงปลอดภัย (Website Security Governance) มุ่งเน้นการบริหารจัดการเชิงนโยบายและการควบคุมเชิงบริหารตามกรอบ NIST CSF 2.0

2. การรักษาความมั่นคงปลอดภัยเชิงปฏิบัติการ (Website Security Operation) ครอบคลุมวงจรการทำงานตั้งแต่การระบุความเสี่ยง การป้องกัน การตรวจสอบ การเผชิญเหตุ และการฟื้นฟูระบบ

ในด้านการบังคับใช้ หน่วยงานภายใต้ประกาศจะต้องดำเนินการประเมินตนเอง (Self-Assessment) ตามแบบฟอร์ม ค1 อย่างน้อยปีละครั้ง หากพบข้อบกพร่องที่ยังไม่สอดคล้องกับมาตรฐาน หน่วยงานจะต้องจัดทำรายงานการแก้ไขตามแบบฟอร์ม ค2 เพื่อเสนอต่อผู้บริหารระดับสูงสุดเพื่อดำเนินการปรับปรุงให้เป็นไปตามเกณฑ์ที่กำหนด ทั้งนี้ ประกาศจะมีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันที่ประกาศในราชกิจจานุเบกษา (16 กันยายน 2568) เพื่อให้หน่วยงานมีระยะเวลาในการปรับตัวและพัฒนาโครงสร้างพื้นฐานให้สอดคล้องกับข้อกำหนดดังกล่าว

ความสอดคล้องและความแตกต่างระหว่างเอกสารทั้งสองฉบับ

มาตรฐานฉบับนี้ มีการอ้างอิงและใช้หลักการพื้นฐานต่อยอดมาจากประมวลแนวทางปฏิบัติฯ พ.ศ. 2564 โดยมาตรฐานฯ เว็บไซต์ พ.ศ. 2568 ได้จัดหมวดหมู่ 5 หมวด ได้แก่

- ข้อ 6.1 การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)
- ข้อ 6.2 การป้องกันความเสี่ยงที่อาจเกิดขึ้นกับเว็บไซต์ (Website Security Protection)
- ข้อ 6.3 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Website Security Detection)
- ข้อ 6.4 การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Website Incident Response)
- ข้อ 6.5 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Website Recovery)

เอกสารทั้งสองฉบับโดยภาพรวมมีการกำหนดมาตรการรักษาความปลอดภัยบางส่วนในหมวดหมู่ที่ใกล้เคียงกัน เช่น การจัดการทรัพย์สิน (Asset Management), การควบคุมการเข้าถึง (Access Control),

การประเมินช่องโหว่และการทดสอบเจาะระบบ อย่างไรก็ตาม มาตรฐานฯ เว็บไซต์ พ.ศ. 2568 เป็นมาตรฐานเฉพาะทางสำหรับเว็บไซต์ เพื่อกำหนดเกณฑ์ขั้นต่ำ (Baseline Security) ในการคุ้มครองระบบสารสนเทศประเภทเว็บไซต์ของหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยมีความเชื่อมโยงระหว่างข้อประกาศ ดังนี้

ตารางที่ 26 ความสอดคล้องของ มาตรฐานฯ เว็บไซต์ พ.ศ. 2568 และประมวลแนวทางปฏิบัติฯ พ.ศ. 2564

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
ส่วนที่ 1: ประมวลแนวทางปฏิบัติ (Code of Practice)	
องค์ประกอบที่ 1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
17.1 จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง โดยขอบเขตครอบคลุม: (ก) กระบวนการและผลวิเคราะห์ผลกระทบทางธุรกิจ (BIA) (ข) บริการที่สำคัญของหน่วยงาน (ค) การปฏิบัติตาม พ.ร.บ. ไซเบอร์ฯ และแนวปฏิบัติ	ไม่ระบุ
17.2 จัดส่งผลสรุปรายงานการตรวจสอบฯ ต่อสำนักงาน (สกมช.) ภายใน 30 วัน นับแต่ดำเนินการแล้วเสร็จ และส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแล	ไม่ระบุ
17.3 หากผลตรวจสอบพบการไม่ปฏิบัติตาม (Non-compliance) ให้จัดส่ง แผนการดำเนินการแก้ไข (Corrective Action Plan) ไปยังสำนักงานภายใน 30 วัน โดยระบุรายละเอียดการแก้ไขและระยะเวลาดำเนินการ	ไม่ระบุ
17.4 หาก กกม. ให้ปรับปรุงแผนการดำเนินการแก้ไข หน่วยงานต้องปรับปรุงและนำส่งแผนแก้ไขใหม่ภายในระยะเวลาที่กำหนด พร้อมส่งสำเนาให้หน่วยงานกำกับดูแล	ไม่ระบุ
17.5 เมื่อแผนดำเนินการแก้ไขได้รับความเห็นชอบ หน่วยงานต้องดำเนินการตามแผนให้แล้วเสร็จภายในระยะเวลาที่ระบุไว้	ไม่ระบุ
องค์ประกอบที่ 2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
นโยบายและระเบียบวิธีปฏิบัติ อันประกอบไปด้วยกำหนดนโยบาย โครงสร้างองค์กร บทบาทหน้าที่ และจัดทำระเบียบวิธีปฏิบัติ/กระบวนการในการบริหารความเสี่ยง โดยต้องประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง	ไม่ระบุ
18.1 การประเมินความเสี่ยง (Risk Assessment)	
18.1 (ก) การระบุความเสี่ยง (Risk Identification) ระบุความเสี่ยงจากภัยคุกคามและช่องโหว่ ที่มาจากกระบวนการ ระบบงาน บุคลากร หรือปัจจัยภายนอก	ไม่ระบุ
18.1 (ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ทำความเข้าใจและวิเคราะห์ความเสี่ยงเพื่อหาแนวทางจัดการที่เหมาะสม	ไม่ระบุ
18.1 (ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ประเมินโอกาสเกิดผลกระทบ และกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
18.2 การจัดการความเสี่ยง (Risk Treatment) มีแนวทางจัดการ ควบคุม ป้องกัน ความเสี่ยง เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงความคุ้มค่า และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)	ไม่ระบุ
18.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) มีกระบวนการติดตามและทบทวนความเสี่ยง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้	ไม่ระบุ
18.4 การรายงานความเสี่ยง (Risk Reporting) รายงานผลต่อคณะกรรมการเป็น ประจำ และทบทวนกระบวนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	ไม่ระบุ
องค์ประกอบที่ 3 แผนการรับมือภัยคุกคามทางไซเบอร์	
19.1 การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	
19.1 (ก) โครงสร้างทีมรับมือเหตุการณ์ (CIRT) ระบุบทบาท และความรับผิดชอบที่ กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ	ไม่ระบุ
19.1 (ข) โครงสร้างการรายงานเหตุการณ์ ให้เป็นไปตามการรายงานตามภาระหน้าที่ ภายใต้ พ.ร.บ. และกฎหมายที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ	ไม่ระบุ
19.1 (ค), (ง), (จ), (ฉ) ขั้นตอนการเผชิญเหตุ ต้องมีการกำหนดเกณฑ์การเรียกใช้งาน (Activate), การจำกัดขอบเขต (Containment), กระบวนการกู้คืน (Recovery) และการสอบสวน (Investigate) สาเหตุและผลกระทบ	ไม่ระบุ
19.1 (ช) การเก็บรักษาหลักฐาน (Preservation of Evidence) ขั้นตอนการเก็บ รักษาหลักฐานก่อนเริ่มกระบวนการกู้คืน รวมถึงหลักฐานทางคอมพิวเตอร์เพื่อ สนับสนุนการสอบสวน	ไม่ระบุ
19.1 (ซ) ระเบียบวิธีการมีส่วนร่วมกับบุคคลภายนอก สำหรับการทำงานร่วมกับ บุคคลภายนอก เช่น ผู้ขายบริการด้านนิติวิทยาศาสตร์, การกู้คืน, และการบังคับใช้ กฎหมายเพื่อดำเนินคดี	ไม่ระบุ
19.1 (ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review) การ ทบทวนหลังการดำเนินการเพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกัน การเกิดซ้ำ	ไม่ระบุ
19.2 การสื่อสารแผนการรับมือ ต้องสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมด	ไม่ระบุ
19.3 การทบทวนแผนตามรอบเวลา ทำการทบทวนแผนการรับมือภัยคุกคามทาง ไซเบอร์ อย่างน้อยปีละ 1 ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ	ไม่ระบุ
19.4 การทบทวนแผนเมื่อมีการเปลี่ยนแปลง	ไม่ระบุ

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคง ปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
ส่วนที่ 2: กรอบมาตรฐาน (Standard Framework)	
หัวข้อหลักที่ 1 Identify	
21.1 การจัดการทรัพย์สิน (Asset Management)	
21.1.1 จัดทำและปรับปรุงทะเบียนทรัพย์สิน (Inventory) ให้เป็นปัจจุบัน ระบุชื่อ ฟังก์ชัน ความสำคัญ เจ้าของ ที่ตั้ง และการพึ่งพากันของทรัพย์สิน	6.1.1
21.1.2 ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อ โดยตรง (Network scope & interface)	6.1.1
21.1.3 ตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง	6.1.1
21.1.4 ประเมินความเสี่ยงด้านไซเบอร์ของทรัพย์สินที่อยู่ในทะเบียน อย่างน้อยปีละ 1 ครั้ง	6.1.1
21.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง	
21.2.1 ประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ	6.1.1
21.2.2 ปรับปรุงทะเบียนความเสี่ยง (Risk Register) โดยระบุวันที่, คำอธิบาย, โอกาสเกิด, ความรุนแรง, การจัดการความเสี่ยง, เจ้าของ, สถานะ และความเสี่ยง ที่เหลือ (Residual Risk)	6.1.1
21.3 การประเมินช่องโหว่และการทดสอบเจาะระบบ	6.1.1
21.3.1 - 21.3.2 หน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญต้องประเมิน ช่องโหว่ระบบ IT และ ICS ตามหลักบริหารความเสี่ยง โดยต้องครอบคลุมทั้งด้าน ฮาร์ดแวร์ เครือข่าย และการตรวจสอบสถาปัตยกรรมให้ครบถ้วน	6.1.1
21.3.3 หน่วยงานรัฐและหน่วยงาน CII ต้องประเมินช่องโหว่เพื่อระบุจุดอ่อนก่อนเริ่ม ทดสอบระบบใหม่หรือเปลี่ยนแปลงระบบสำคัญ เช่น การเพิ่มโมดูลและการอัปเดต เทคโนโลยี	6.1.1
21.3.4 ดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเน้นระบบ IT ที่ เชื่อมต่ออินเทอร์เน็ตตามความเหมาะสมของระดับความเสี่ยง และต้องพิจารณา ผลกระทบที่อาจเกิดขึ้นจากการทดสอบอย่างรอบคอบด้วย	6.1.1
21.3.5 การกำหนดขอบเขตการทดสอบเจาะระบบต้องครอบคลุมทั้งส่วนของฮาร์ด แวร์ เครือข่าย และแอปพลิเคชันที่เกี่ยวข้องกับบริการสำคัญ โดยต้องให้ความสำคัญเป็น พิเศษกับทุกระบบที่มีการเชื่อมต่อกับอินเทอร์เน็ตโดยตรงเพื่อให้เกิดความมั่นคง ปลอดภัยสูงสุด	6.1.1
21.3.6 ควรทดสอบเจาะระบบอย่างน้อยปีละครั้งหรือเมื่อมีการเปลี่ยนแปลงระบบ สำคัญเพื่อยืนยันความมั่นคงปลอดภัยของหน่วยงานรัฐและ CII	6.1.1
21.3.7 ผู้ทดสอบเจาะระบบ CII ต้องมีใบเซอร์ฯ ระดับสากล มีความเป็นอิสระ และมี คุณสมบัติตามเกณฑ์ของหน่วยงานกำกับดูแล	6.1.1

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคง ปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
21.3.8 การทดสอบเจาะระบบโดยผู้ให้บริการภายนอกต้องอยู่ภายใต้การกำกับดูแล ของหน่วยงานอย่างใกล้ชิดทุกขั้นตอน	6.1.1
21.3.9 สร้างกระบวนการติดตามและจัดการแก้ไขช่องโหว่ที่พบ	6.1.1
21.3.10 นำส่งสำเนารายงานผลการทดสอบเจาะระบบให้ สกมช. หากได้รับการร้อง ขอ	6.1.1
21.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)	
21.4.1 องค์กรต้องรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ แม้จะใช้ผู้ให้บริการ ภายนอก	6.1.1
21.4.2 กำหนดข้อกำหนดด้านไซเบอร์ในข้อตกลง SLA หรือเงื่อนไขสัญญากับผู้ ให้บริการภายนอก ครอบคลุมภาระหน้าที่, ห่วงโซ่อุปทาน (Supply chain) และสิทธิ ในการตรวจสอบ	6.1.1
21.4.3 สร้างกระบวนการตรวจสอบความถูกต้อง (Audit/Review) ผู้ให้บริการ ภายนอกตามสัญญา	6.2.4
21.4.4 เจรจาทอรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมาย/ ข้อบังคับใหม่	6.2.4
หัวข้อหลักที่ 2 Protect	
22.1 การควบคุมการเข้าถึง (Access Control)	6.2.4
22.1.1 จำกัดการเข้าถึงบริการสำคัญ เฉพาะบุคลากร กิจกรรม อุปกรณ์ และ อินเทอร์เน็ตที่ได้รับอนุญาตเท่านั้น	6.2.4
22.1.2 ใช้เทคนิคการตรวจสอบสิทธิ์ (Authentication) ที่สอดคล้องกับโปรไฟล์ ความเสี่ยง	6.2.4
22.1.3 เก็บบันทึกการเข้าถึงทั้งหมด (Logs) และตรวจสอบบันทึกเพื่อหากิจกรรมที่ ผิดปกติอย่างสม่ำเสมอ	6.2.4
22.1.4 การเข้าถึงอินเทอร์เน็ต (เช่น USB) และแบบลอจิคอล ต้องมีการกำกับดูแล และดำเนินการในสถานที่หากเป็นไปได้	6.2.4
22.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	6.2.4
22.2.1 จัดทำมาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้ครอบคลุมทุกระบบและอุปกรณ์โดยสอดคล้องกับโปรไฟล์ความเสี่ยงของบริการ สำคัญ	6.2.4
22.2.2 มาตรฐานต้องมี: สิทธิเข้าถึงน้อยสุด (Least Privilege), แบ่งแยกหน้าที่ (Separation of Duties), รหัสผ่านซับซ้อน, ลบบัญชี/แอป/พอร์ตที่ไม่ใช้, ป้อง กันมัลแวร์, และอัปเดตแพตช์	6.2.4

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคง ปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
22.2.3 หน่วยงานรัฐและ CII ต้องบังคับใช้มาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้น ต่ำ (Security Baseline) ให้เรียบร้อยก่อนเริ่มเชื่อมต่ออุปกรณ์หรือปรับปรุงระบบทุก ครั้ง	6.2.4
22.2.4 หน่วยงานรัฐและ CII ต้องทบทวนมาตรฐาน Security Baseline อย่างน้อยปี ละครั้งเพื่อให้มั่นใจว่ายังรับมือกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ	6.2.4
22.2.5 จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบการเปลี่ยนแปลงระบบ	6.2.4
22.3 การเชื่อมต่อระยะไกล (Remote Connection)	6.2.4
22.3.1 มีมาตรการป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต สำหรับการ เชื่อมต่อระยะไกล	6.2.4
22.3.2 เปิดใช้เมื่อจำเป็น, ใช้การพิสูจน์ตัวตนที่แข็งแกร่ง, ใช้การเข้ารหัส (เช่น https, ssh), ไม่อนุญาตคำสั่งระบบระยะไกลโดยไม่จำเป็น, และจำกัดการไหลของข้อมูล	6.2.4
22.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	6.2.4
22.4.1 ควบคุมการใช้สื่อแบบถอดได้ (เช่น ปิดพอร์ต USB และเปิดเมื่อจำเป็น), ใช้ เฉพาะที่ได้รับอนุญาต, และตรวจสอบมัลแวร์ก่อนเชื่อมต่อ	6.2.4
22.4.2 เข้ารหัสข้อมูลที่ละเอียดอ่อนบนสื่อบันทึกข้อมูลแบบถอดได้	6.2.4
22.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	6.2.4
22.5.1 หน่วยงานรัฐและ CII ต้องสร้างความตระหนักรู้ด้านไซเบอร์ให้บุคลากรทุก ระดับและบุคคลภายนอกอย่างทั่วถึง โดยครอบคลุมทั้งหน้าที่ความรับผิดชอบ ความรู้ ด้านกฎหมาย และการแจ้งเตือนภัยคุกคามอย่างสม่ำเสมอเพื่อให้เกิดความปลอดภัย ในการปฏิบัติงานอย่างเป็นรูปธรรม	6.2.4
22.5.2 ต้องทบทวนแผนสร้างความตระหนักรู้ไซเบอร์อย่างน้อยปีละครั้งเพื่อให้เนื้อหา ทันสมัยและเหมาะสมกับสถานการณ์ปัจจุบัน	6.2.4
22.6 การแบ่งปันข้อมูล (Information Sharing)	6.2.4
22.6 กำหนดขั้นตอนแบ่งปันข้อมูลเหตุการณ์และภัยคุกคามไซเบอร์ รวมถึงมาตรการ บรรเทาผลกระทบ กับบุคคลที่เกี่ยวข้องหรือได้รับผลกระทบ เพื่อให้สามารถป้องกัน ตนเองได้	6.2.4
หัวข้อหลักที่ 3 Detect	
23.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
23.1.1 (ก) สร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน	6.3.1

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคง ปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
23.1.1 (ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ	6.3.1
23.1.1 (ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญหรือไม่	6.3.1
23.1.2 ดำเนินการทบทวนกลไกและกระบวนการ (ตามข้อ 23.1.1) อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ	6.3.1
หัวข้อหลักที่ 4 Respond	
24.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	6.4.1
24.1.1 จัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้การรับมือดำเนินการได้อย่างมีประสิทธิภาพ	6.4.1
24.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	6.4.1
24.2.1 จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ภัยคุกคาม	6.4.1
24.2.2 แผนสื่อสารต้องประกอบด้วย: การจัดตั้งทีมสื่อสาร, ระบุสถานการณ์จำลอง, ระบุกระบวนการแจ้งกลุ่มเป้าหมาย, ระบุโฆษก/ผู้เชี่ยวชาญ และกำหนดแพลตฟอร์ม/ช่องทางการเผยแพร่	6.4.1
24.2.3 ต้องแน่ใจว่าแผนการสื่อสารรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้สอดคล้องกันในช่วงวิกฤต	6.4.1
24.2.4 ฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง	6.4.1
24.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	6.4.1
24.3.1 หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน หากได้รับคำสั่งเป็นลายลักษณ์อักษรจากคณะกรรมการ	6.4.1
24.3.2 ปฏิบัติตามคำขอของคณะกรรมการในการให้ข้อมูลที่เกี่ยวข้องเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อม เช่น แผนการรับมือภัยคุกคาม ขั้นตอนการปฏิบัติงาน (SOP) และแผนการสื่อสาร	6.4.1
หัวข้อหลักที่ 5 Recover	
25.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	6.5.1

ประมวลแนวทางปฏิบัติฯ พ.ศ. 2564	มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
25.1.1 จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการสำคัญสามารถดำเนินการต่อไปได้เมื่อเกิดการหยุดชะงักจากเหตุการณ์ด้านไซเบอร์กำหนดระยะเวลาและเกณฑ์ที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) สอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน	6.5.1
25.1.2 ตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนในการรับมือและฟื้นฟูระบบจากภัยคุกคามไซเบอร์	6.5.1

นอกจากนี้ ยังมีมาตรการเฉพาะข้ออื่น ๆ นอกเหนือจากที่ระบุในตารางที่หน่วยงานจำเป็นต้องดำเนินการเพิ่มเติมหากต้องปฏิบัติตามประกาศฉบับนี้ ดังนี้

ที่	รายละเอียด (อ้างอิงลำดับตามเอกสาร ค1)
1.1	หน่วยงานจะต้องมีการทำความเข้าใจสถานการณ์ต่าง ๆ ที่เกี่ยวข้องกับการตัดสินใจในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงาน โดยหน่วยงานอาจจะพิจารณารายละเอียดการดำเนินการสำรวจบริบทของหน่วยงาน (Organization Context) ตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 5.1.1)
2.1	หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยมีการจัดลำดับความสำคัญ มีการสื่อสาร รวมถึงมีการบังคับใช้ (หัวข้อ 5.2.1)
2.2	หน่วยงานจะต้องมีการทบทวน ปรับปรุง สื่อสาร และบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อสะท้อนการเปลี่ยนแปลงความต้องการ ภัยคุกคาม เทคโนโลยี รวมถึงภารกิจของหน่วยงาน (หัวข้อ 5.2.2)
3.1	หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์การบริหารความเสี่ยงและมีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์เป็นลายลักษณ์อักษร (หัวข้อ 5.3.1)
3.2	เฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหน่วยงานจะต้องพิจารณาดำเนินการประเมินความเสี่ยงตามคำแนะนำของ สกมช. เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ 5.3.2)
3.3	หน่วยงานจะต้องมีการจัดทำ สื่อสาร และมีการเก็บรักษารายการความเสี่ยงที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ให้เป็นปัจจุบัน และติดตามระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ (หัวข้อ 5.3.3)
4.1	หน่วยงานจะต้องมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยหน่วยงานอาจจะใช้แนวคิดการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) มาประยุกต์ใช้กับการจัดโครงสร้างองค์กรให้มีการถ่วงดุล ในการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 5.4.1)

ที่	รายละเอียด (อ้างอิงลำดับตามเอกสาร ค1)
4.2	หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำและบริหารจัดการเว็บไซต์ของหน่วยงาน รวมถึงดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งต้องเป็นนิติบุคคลหรือเป็นส่วนหนึ่งของนิติบุคคลที่สามารถรับผิดชอบตามกฎหมายได้ และการมอบหมายหน้าที่จะต้องทำโดยไม่ขาดช่วง (หัวข้อ 5.4.2)
4.3	หน่วยงานจะต้องกำหนด สื่อสาร ทำความเข้าใจและบังคับใช้บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ รวมถึงจัดสรรทรัพยากรให้เพียงพอ (หัวข้อ 5.4.3)
5.1	หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์และความต้องการในการจัดทำเว็บไซต์ ด้านฟังก์ชัน ด้านประสิทธิภาพ และที่สำคัญความต้องการ ด้านความมั่นคงปลอดภัย โดยหน่วยงานควรจะมีการวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ โดยพิจารณาให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 5.5.1)
6.1	หน่วยงานจะต้องมีแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐานตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการเตรียมความพร้อมใช้งาน (Availability) โดยหน่วยงานควรดำเนินการตามแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐาน ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 5.6.1)
6.2	หน่วยงานจะต้องมีการกำหนดคุณลักษณะความมั่นคงปลอดภัยให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ ตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน 3 ระดับให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (หัวข้อ 5.6.2)
6.3	เฉพาะหน่วยงานมีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 (หัวข้อ 5.6.3)
6.4	เฉพาะหน่วยงานภาครัฐ หน่วยงานจะต้องดำเนินการตามมาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard) Version 3.0 หัวข้อที่ 7 ความมั่นคงปลอดภัยสำหรับเว็บไซต์(หัวข้อ 5.6.4)
6.5	หน่วยงานจะต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ใช้บริการคลาวด์ ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (หัวข้อ 5.6.5)
6.6	หน่วยงานจะต้องพิจารณาเลือกผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ เช่น การดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) ของเว็บไซต์ ที่ได้รับการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม (หัวข้อ 5.6.6)
6.7	หน่วยงานจะต้องปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ของ สกมช. (หัวข้อ 5.6.7)

ที่	รายละเอียด (อ้างอิงลำดับตามเอกสาร ค1)
6.8	หน่วยงานจะต้องมีการกำหนดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบที่เกิดขึ้นหากเว็บไซต์ของหน่วยงานโดนโจมตีจากภัยคุกคามทางไซเบอร์ โดยหน่วยงานอาจจะพิจารณาองค์ประกอบในการสำรองข้อมูลซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 5.6.8)
6.9	หน่วยงานจะต้องมีการจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และที่แก้ไขเพิ่มเติม (หัวข้อ 5.6.9)
6.10	หน่วยงานจะต้องกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ เพื่อป้องกันภัยคุกคามไซเบอร์ที่อาจเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ตทั่วไป ผู้ให้บริการ โดยหน่วยงานควรที่จะกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ หรือหน่วยงานอาจจะพิจารณาการทำลายข้อมูลตามข้อเสนอแนะให้เป็นไปตาม NIST Special Publication 800-88 และขั้นตอนหลักของการทำลายข้อมูล (หัวข้อ 5.6.10)
8.1	หน่วยงานจะต้องกำหนดแนวทางในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) อย่างมั่นคงปลอดภัย เช่น พิจารณาใช้หลักการ DevSecOps ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริงโดยมีการคำนึงถึงสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยในการพัฒนาโปรแกรมประยุกต์บนเว็บ โดยหน่วยงานควรที่จะพิจารณาปรับใช้ตัวอย่างในการปรับใช้หลักการ DevSecOps และอาจจะพิจารณาสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของการพัฒนาโปรแกรมประยุกต์บนเว็บ รวมถึงอาจจะพิจารณาประยุกต์ใช้หลักการ DevSecOps โดยใช้หลักการ DSOMM ของมูลนิธิ OWASP ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 6.2.1)
8.2	หน่วยงานจะต้องพิจารณาถึงปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยของมูลนิธิ OWASP ในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) (หัวข้อ 6.2.2)
8.3	หน่วยงานจะต้องพิจารณาการออกแบบสถาปัตยกรรมเว็บอย่างมั่นคงปลอดภัย ในส่วนของโครงสร้างของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บ โดยอาจจะพิจารณาส่วนประกอบของการออกแบบที่คำนึงถึงการแบ่งส่วนเครือข่าย (Network segmentation) มีการจัดวางเครื่องบริการเว็บ (Web Server) และเครื่องบริการฐานข้อมูล (Database Server) ร่วมกับอุปกรณ์รักษาความมั่นคงปลอดภัย (หัวข้อ 6.2.3)
8.5	หน่วยงานจะต้องพิจารณาการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือพิจารณาการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามข้อเสนอแนะของ สพร. นอกเหนือจากการควบคุมการเข้าถึง (Access Control) ข้อ 6.2.4 โดยหน่วยงานควรที่จะพิจารณาตรวจสอบตัวตนของผู้ใช้งานโดยใช้ปัจจัยที่แตกต่างกันมากกว่าหนึ่งปัจจัย และอาจจะพิจารณาตัวอย่างการใช้งาน MFA ให้เป็นไปตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 6.2.5)
8.6	หน่วยงานจะต้องตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (CMS) ระบบปฏิบัติการ (Operating System) และการตั้งค่าฐานข้อมูล (หัวข้อ 6.2.6)
8.7	หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์ ประกอบด้วย เครื่องบริการเว็บ (Web Server) ระบบบริหารจัดการเว็บไซต์ (CMS) เลือกบริการโดเมนและชื่อโดเมน และขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate (หัวข้อ 6.2.7)
8.8	หน่วยงานจะต้องตั้งค่าไฟร์วอลล์เพื่อควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ โดยควรที่จะพิจารณาหลักการตั้งค่าอย่างน้อย ดังนี้ การกำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การตั้งค่ากฎการกรอง (Configure Filtering Rules) การจำกัดการเข้าถึงโดยภูมิศาสตร์ (Geographic

ที่	รายละเอียด (อ้างอิงลำดับตามเอกสาร ค1)
	Restrictions) การป้องกันการโจมตี (Protect Against Attacks) การตรวจสอบและบันทึก (Monitoring and Logging) และการปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) โดยอาจจะพิจารณาหลักการตั้งค่าไฟร์วอลล์ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ 6.2.8)

สรุปข้อสังเกต

แม้ข้อกำหนดในประกาศทั้งสองฉบับ จะมีจุดร่วมที่สามารถเชื่อมโยงและอ้างอิงถึงกันได้ในระดับหลักการปฏิบัติ (General Practice) แต่จากการศึกษาเชิงลึกพบว่าในรายละเอียดข้อกำหนดรายข้อนั้นมีความแตกต่างกันอย่างมีนัยสำคัญ ดังนั้น (ร่าง) หลักเกณฑ์การตรวจประเมินฯ ในเอกสารฉบับนี้ จึงถูกออกแบบมาเพื่อใช้เป็น บรรทัดฐานการตรวจประเมินขั้นพื้นฐาน (Baseline Audit) ในข้อประกาศดังกล่าวที่สอดคล้องกันเท่านั้น ทั้งนี้ หน่วยงานจำเป็นต้องพิจารณารายละเอียดทางเทคนิคและข้อกำหนดเฉพาะเจาะจงเพิ่มเติม เพื่อให้การดำเนินงานสอดคล้องกับ มาตรฐานฯ เว็บไซต์ พ.ศ. 2568 อย่างครบถ้วนสมบูรณ์

ภาคผนวก ข. การเปรียบเทียบประมวลแนวทางปฏิบัติ พ.ศ. 2564 และมาตรฐานสากล

ผลการศึกษาการเปรียบเทียบประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์
เทียบกับมาตรฐานสากล โดยมาตรฐานสากล ประกอบด้วย

- (1) NIST CSF 1.1
- (2) NIST CSF 2.0
- (3) ISO/IEC 27001:2022
- (4) ISO/IEC 27701:2025
- (5) ISO/IEC 27017:2015
- (6) ISO/IEC 27008:2019

โดยสามารถดูผลการเปรียบเทียบได้ที่ <https://standard.dga.or.th/dga-regulator/>

ภาคผนวก ค. ชุดเครื่องมือสนับสนุนการตรวจสอบ

ชุดเครื่องมือสนับสนุนสำหรับการตรวจสอบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลตามแนวทาง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกอบด้วย

- (1) แบบฟอร์มคำรับรองการนำมาตรการควบคุมไปใช้
- (2) โปรแกรมการตรวจประเมิน (Audit Program)
- (3) แผนการตรวจประเมิน (Audit Plan)
- (4) รายงานผลการตรวจประเมิน (Audit Report)
- (5) แบบฟอร์มขอดำเนินการแก้ไข (Corrective Action Request)
- (6) แผนการแก้ไข (Corrective Action Plan)
- (7) รายงานทบทวนโดยฝ่ายบริหาร (Management Review)
- (8) แม่แบบรายงานผลการดำเนินการตามมาตรา 54

โดยเครื่องมือสนับสนุนการตรวจสอบจะสามารถดาวน์โหลดใช้งานได้ที่
<https://standard.dga.or.th/dga-regulator/>