Faculty of Information Technology and Digital Innovation
King Mongkut's University of Technology North Bangkok

เตรียมความพร้อม
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
สำหรับผู้บริหาร

รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ

กลุ่มวิจัยความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล
(Information Security and Data Privacy Research Group)
คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ (มจพ.)
papa@itd.kmutnb.ac.th

กรุงเทพมหานคร 23 มีนาคม 2564

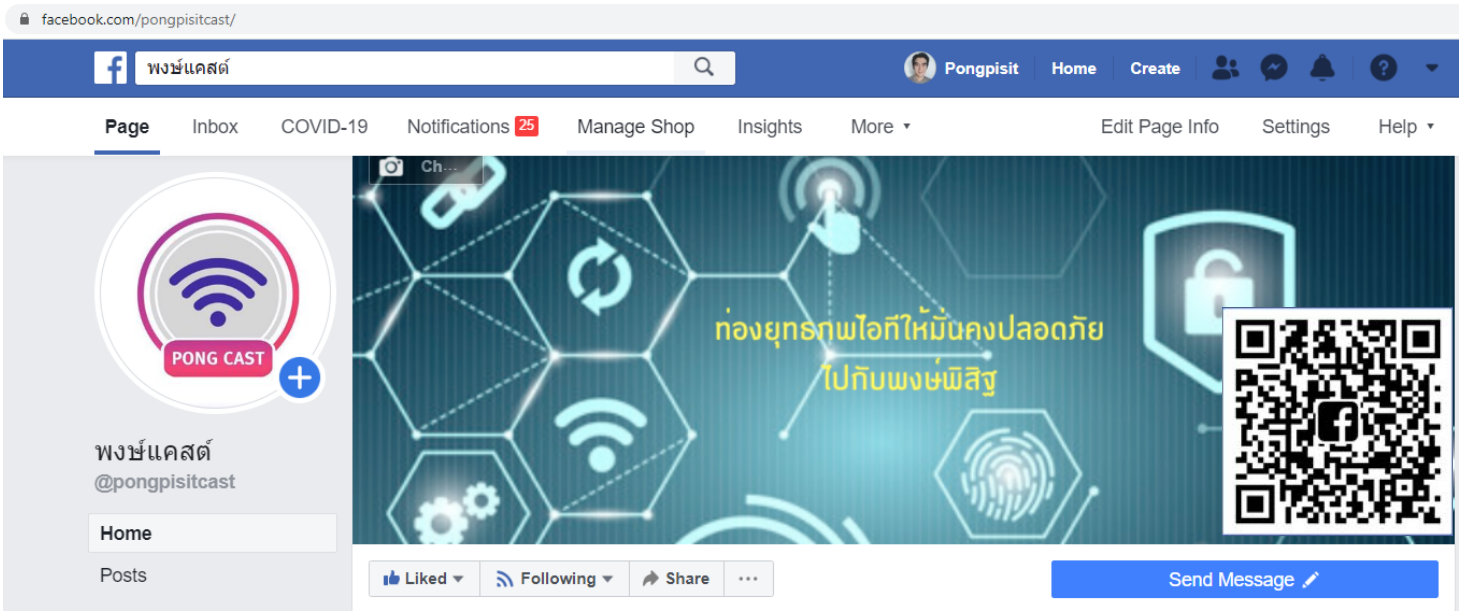
Version 0.1 ปรับปรุงล่าสุด 23 มีนาคม 2564 เวลา 8.00 น.

Faculty of Information Technology and Digital Innovation
King Mongkut's University of Technology North Bangkok

Copyright ©KMUTNB2021.

Faculty of Information Technology and Digital Innovation
King Mongkut's University of Technology North Bangkok

https://www.facebook.com/pongpisitcast/



หัวข้อ

1. (ร่าง) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564-2568

2. (ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564-2568

3. (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

4. (ร่าง) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วิธีการดำเนินการ

1 การศึกษาและการค้นคว้าวิจัย

ศึกษามาตรฐาน และแนวทางสากลประเทศชั้นนำต่าง ๆ และบริบทของไทย

2 สัมภาษณ์ผู้เชี่ยวชาญที่มีส่วนเกี่ยวข้อง

สัมภาษณ์ผู้เชี่ยวชาญที่เกี่ยวข้องและผู้มีส่วนได้เสียหลัก

3 การรับฟังความคิดเห็น (Focus Group) กับกลุ่มผู้มีส่วนได้เสียหลัก 8 กลุ่ม (CII)

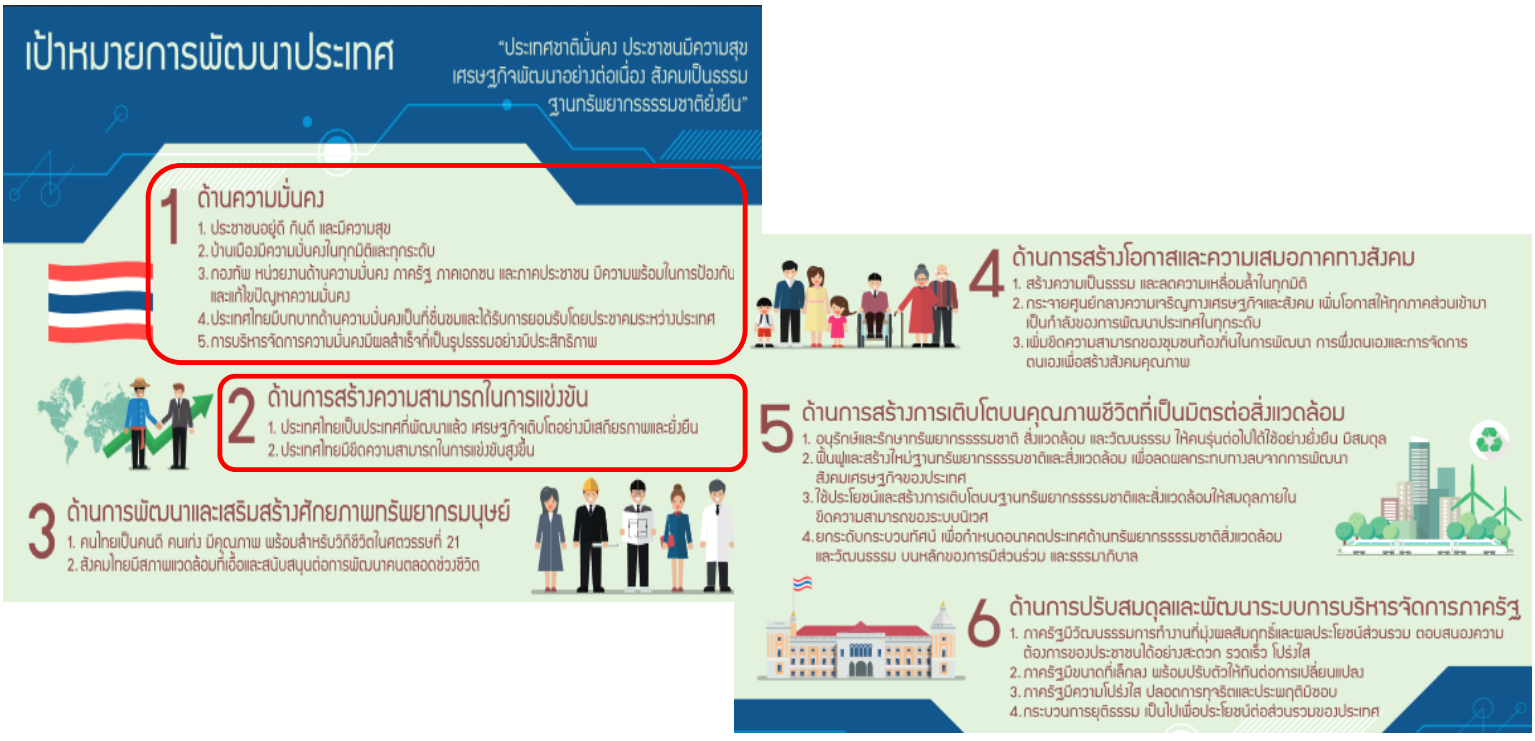
วิธีการดำเนินการ

4 การสัมมนาประชาพิจารณ์ (Public Hearing)

2 รอบ, 15 ธันวาคม 2563 **2 รอบ, 19 มกราคม 2564**

5 การปรับปรุงแก้ไขสุดท้าย (Final Revision)

รวบรวมข้อเสนอแนะข้อคิดเห็นต่าง ๆ และดำเนินการปรับปรุงและจัดทำรูปเล่มเผยแพร่

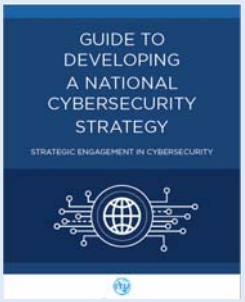


Alignment with Natioanal Context and International practices

ความสอดคล้องกับยุทธศาสตร์ชาติ นโยบาย และแผนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

มาตรฐานและแนวปฏิบัติอ้างอิงที่ได้รับการยอมรับในระดับนานาชาติ

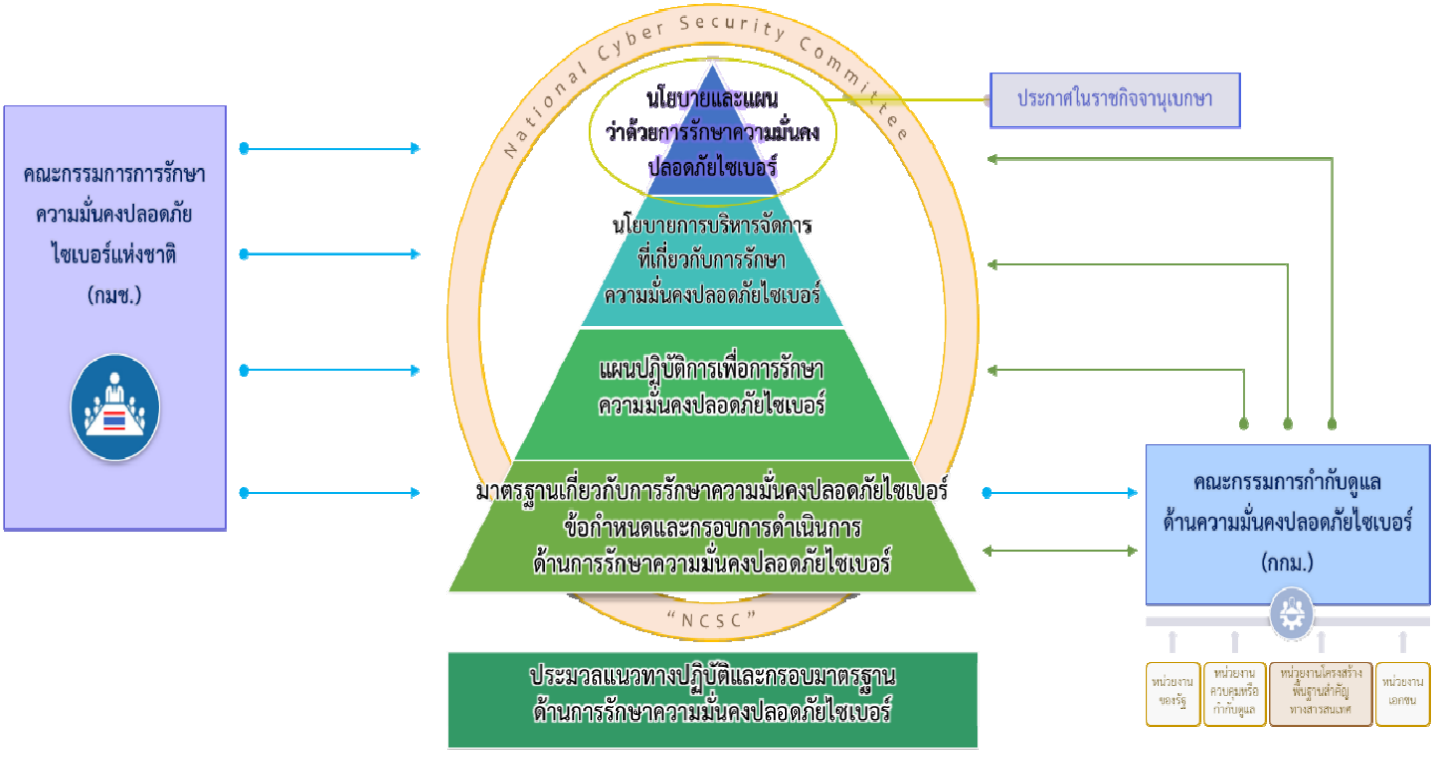
นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564-2568



พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

บริบทของโลก ภูมิภาค และประเทศไทย

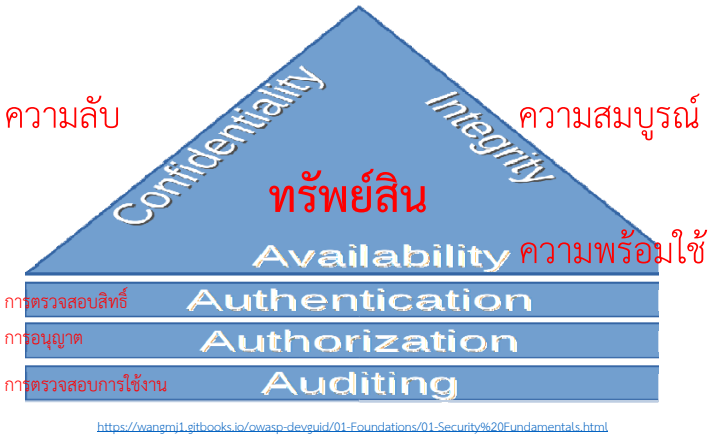
กรณีศึกษาในต่างประเทศ



เป้าหมายของความมั่นคงปลอดภัย (Security)

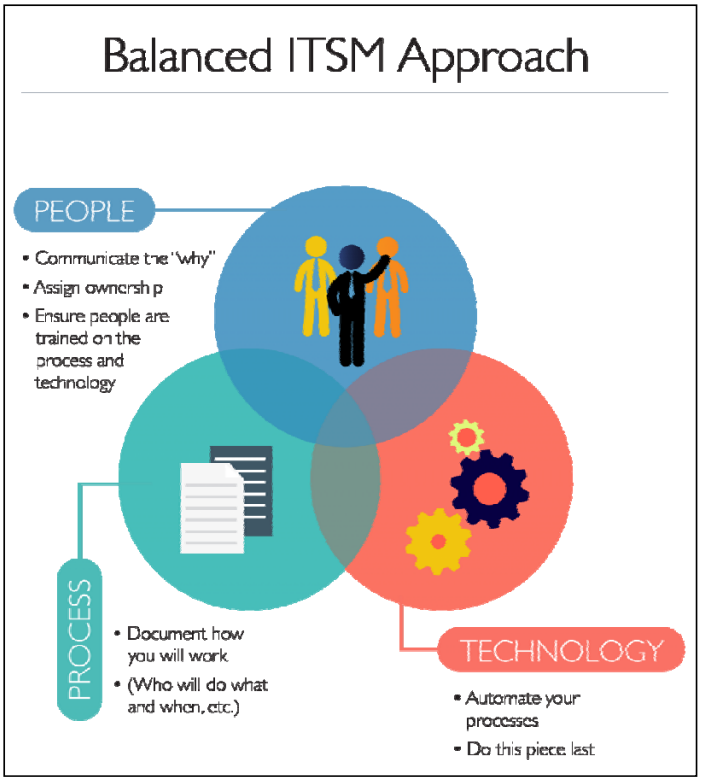
ทรัพย์สินที่มีความมั่นคงปลอดภัย (Security) ต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน

- Confidential (ความลับ) : เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้
- Integrity (ความสมบูรณ์) : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮ็กระบบเพื่อแก้ไขข้อมูล
- Availability (ความพร้อมใช้) : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน



https://wangmj1.gitbooks.io/owasp-devguid/01-Foundations/01-Security%20Fundamentals.html

พื้นฐานด้านความมั่นคงปลอดภัย



มาตรา ๓ ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ
(๒) ด้านบริการภาครัฐที่สำคัญ
(๓) ด้านการเงินการธนาคาร
(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
(๕) ด้านการขนส่งและโลจิสติกส์
(๖) ด้านพลังงานและสาธารณูปโภค
(๗) ด้านสาธารณสุข
(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

1. (ร่าง) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 9 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ

(1) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 42 และมาตรา 43 ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา 42

นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ [มาตรา 42] ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

(1) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(4) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

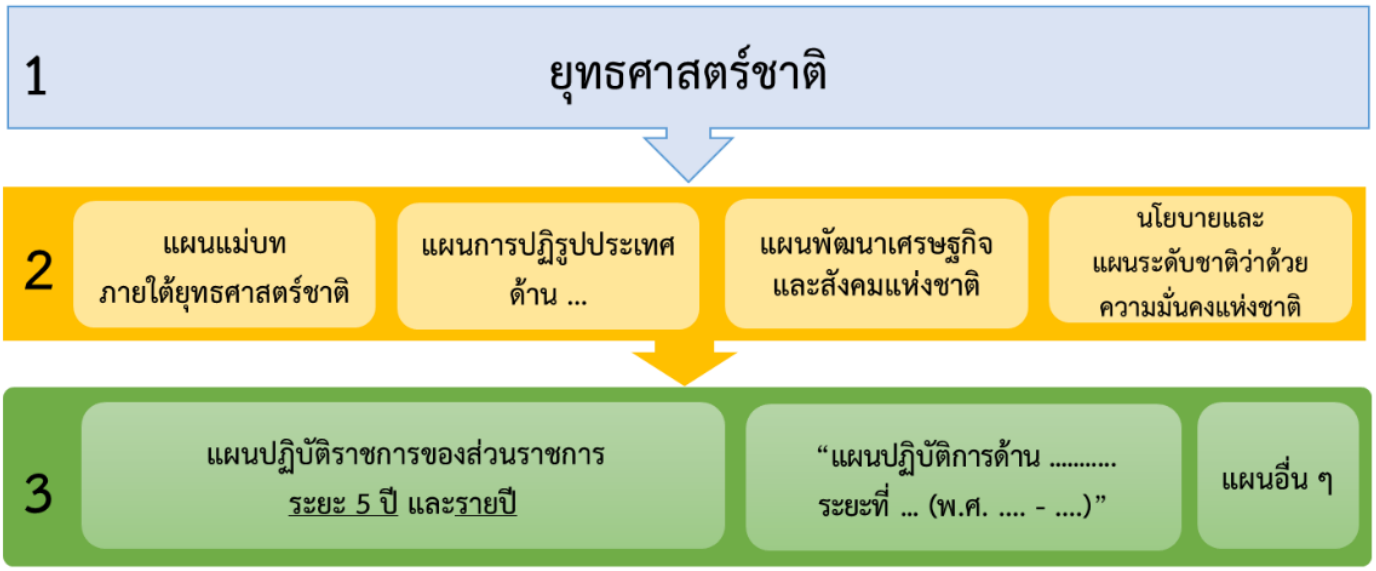
(5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐ และเอกชน

(7) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

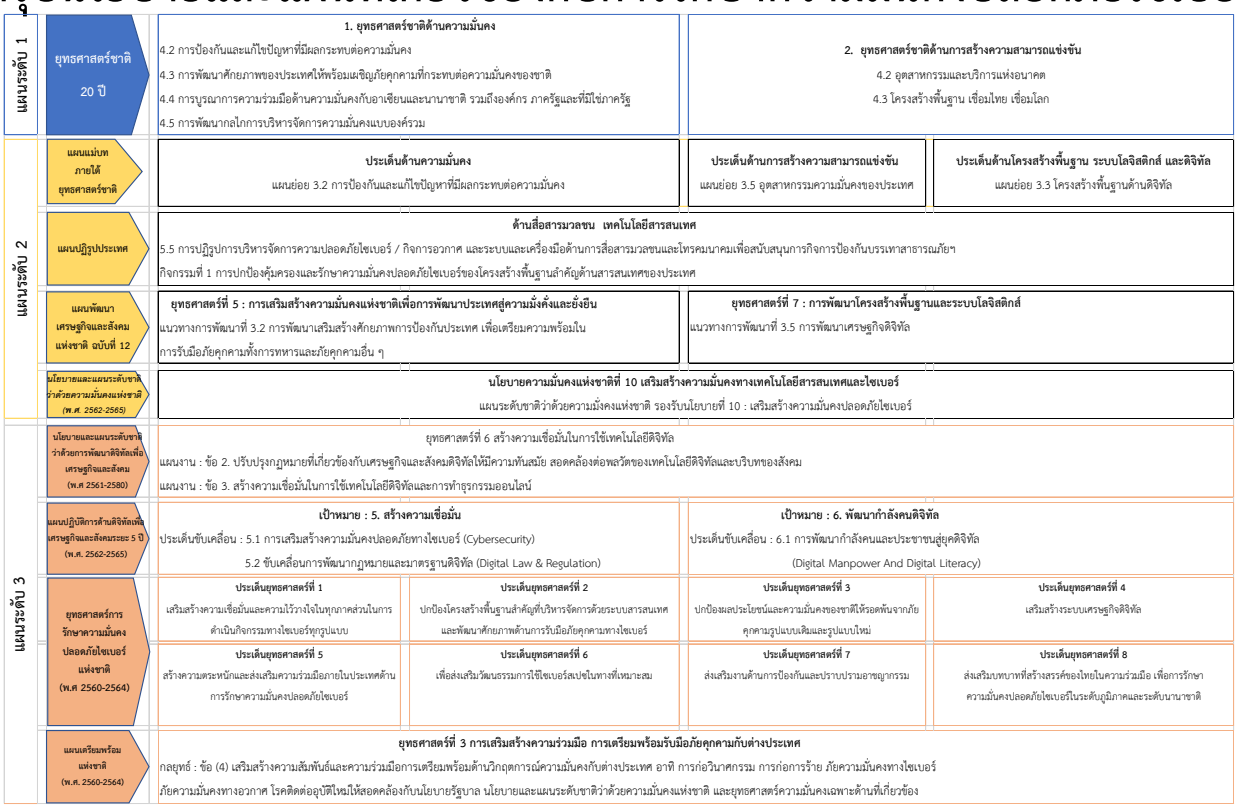
(8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

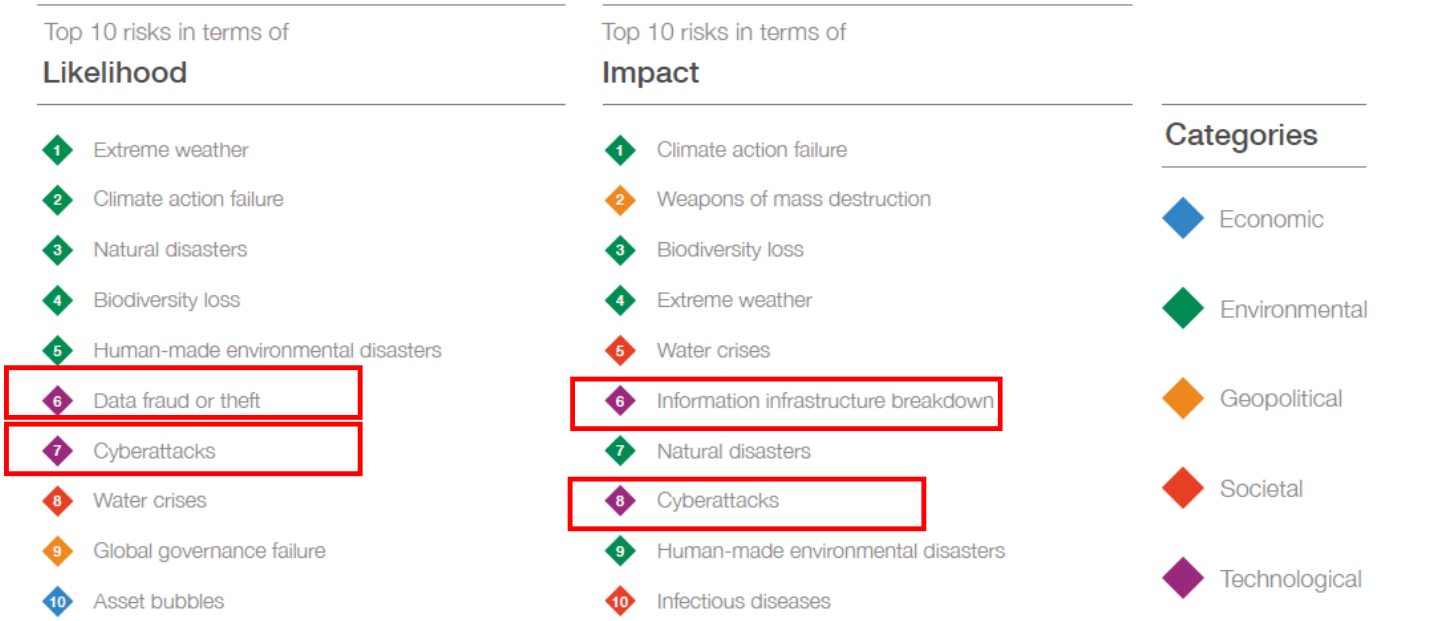
ระดับของแผน



หมายเหตุ : นับตั้งแต่วันที่ 4 ธันวาคม 2560 ครม.มีมติ กำหนดให้ตั้งชื่อแผนในระดับที่ 3 โดยใช้ชื่อว่า “**แผนปฏิบัติการด้านระยะที่ ... (พ.ศ. .... - ....)**” เว้นแต่ได้มีการระบุไว้ในกฎหมายก่อนที่จะมีมติ ครม. วันที่ 4 ธันวาคม 2560 เช่น พระราชบัญญัติ พระราชกำหนด พระราชกฤษฎีกา กฎกระทรวง มติครม. เป็นต้น ได้กำหนดชื่อแผนไว้ว่า แผนแม่บทด้าน... แผนพัฒนา... หรือแผนอื่น ๆ จึงจะสามารถใช้ชื่อแผนตามที่บัญญัติไว้ในกฎหมายนั้น ๆ

สรุปนโยบายและแผนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์





Source: World Economic Forum Global Risks Perception Survey 2019–2020.

Note: Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assessed the impact of each global risk on a scale of 1 to 5, 1 representing a minimal impact and 5 a catastrophic impact. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

Source: World Economic Forum, The Global Risks Report 2020, 15 January 2020

Global Risks Landscape 2021

WORLD ECONOMIC FORUM

Top Global Risks by Likelihood

1st	2nd	3rd	4th	5th
Extreme weather	Climate action failure	Human environmental damage	Infectious diseases	Biodiversity loss
6th	**7th**	**8th**	**9th**	**10th**
Digital power concentration	Digital inequality	Interstate relations fracture	Cybersecurity failure	Livelihood crises

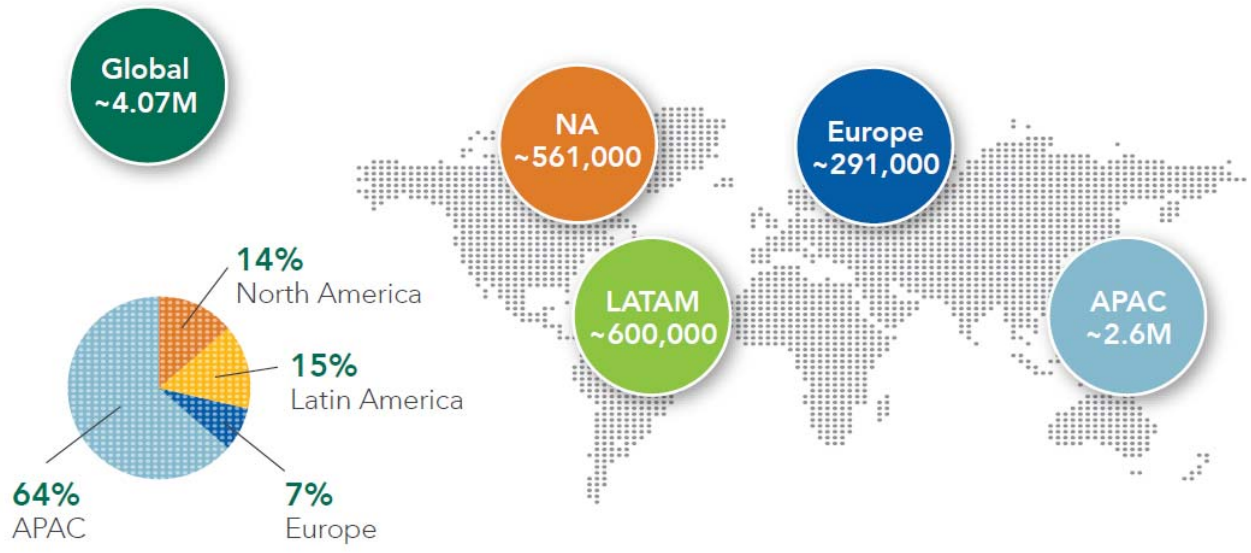
Top Global Risks by Impact

1st	2nd	3rd	4th	5th
Infectious diseases	Climate action failure	Weapons of mass destruction	Biodiversity loss	Natural resource crises
6th	**7th**	**8th**	**9th**	**10th**
Human environmental damage	Livelihood crises	Extreme weather	Debt crises	IT infrastructure breakdown

Economic Environmental Geopolitical Societal Technological

Source: World Economic Forum Global Risks Report 2021

The Cybersecurity Workforce Gap by Region



Source: Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2019

ผลการศึกษาความสามารถด้านการรักษาความปลอดภัยในเอเชียแปซิฟิกประจำปี 2561

ไมโครซอฟท์ ร่วมกับฟรอส แอนด์ ซัลลิแวน เผยมูลค่าความเสียหายต่อเศรษฐกิจที่อาจเกิดขึ้น ถ้าองค์กรธุรกิจไทยโดนภัยคุกคามทางไซเบอร์ จะส่งผลกระทบระดับ 2.86 แสนล้านบาท หรือราว 2.2% ของ GDP ประเทศ

แนะองค์กรที่ก้าวสู่ดิจิทัลควรให้ความสำคัญในการวางแผนรับมืออาชญากรรมไซเบอร์ตั้งแต่เริ่มต้น

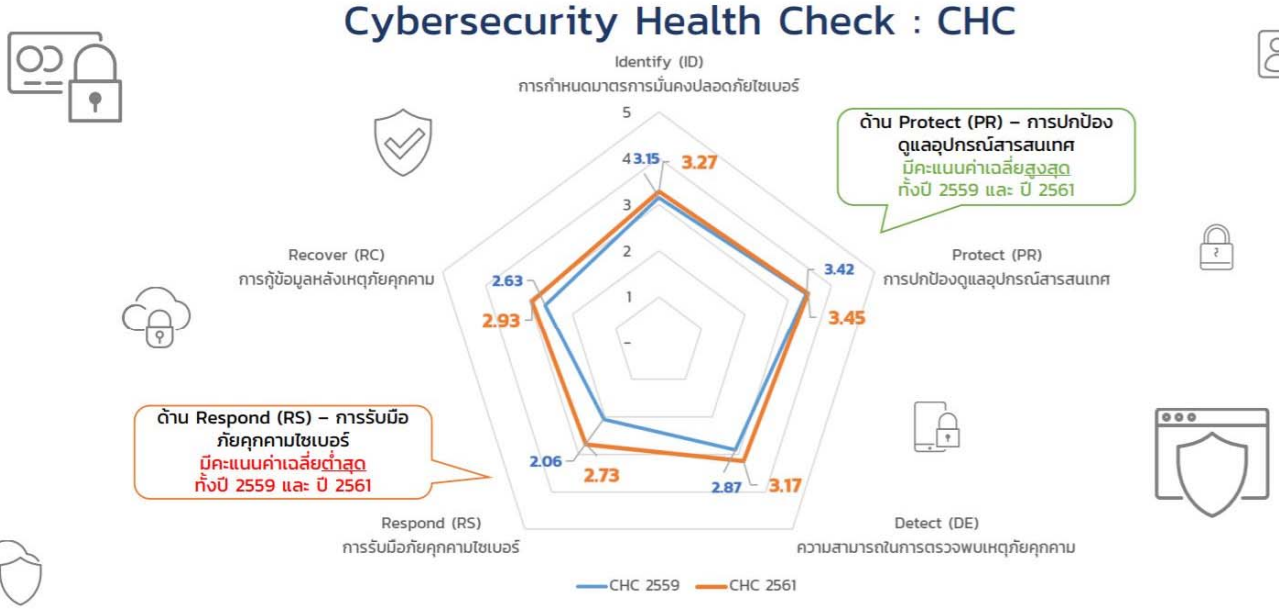
https://mgronline.com/cyberbiz/detail/9610000060481

มูลค่าความเสียหาย จากการถูกโจมตีทางไซเบอร์ของบริษัทไทย

มูลค่าความเสียหาย (เหรียญสหรัฐ)	%
น้อยกว่า 1 แสน	9
1 แสน - 4.99 แสน	6
5 แสน - 9 แสน	18
1 ล้าน - 2.4 ล้าน	40
2.5 ล้าน - 4.9 ล้าน	17
5 ล้าน - 9.9 ล้าน	4
มากกว่า 10 ล้าน	6

https://www.prachachat.net/ict/news-211873, 30 สิงหาคม 2561

Cybersecurity Health Check : CHC



หมายเหตุ: Cybersecurity Health Check : CHC ปี 2559 มาจากหน่วยงานภาครัฐและหน่วยงานเอกชน 547 หน่วยงาน ส่วนปี 2561 มาจากหน่วยงานภาครัฐ 172 หน่วยงาน

ผลจากการสำรวจความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2559 และ 2561 ของ ETDA เพื่อวิเคราะห์ถึงสถานการณ์ ปัญหา อุปสรรค และการรับมือกับภัยคุกคามไซเบอร์ของประเทศในภาพรวมพบว่า การรับมือภัยคุกคามไซเบอร์มีค่าเฉลี่ยต่ำสุดทั้ง 2 ปี จึงความจำเป็นในการวางนโยบายสนับสนุนเพื่อเสริมสร้างศักยภาพในด้านนี้อย่างเข้มแข็ง

https://www.salika.co/2019/06/23/checking-thailand-cybersecurity-2019/

Home › NEWS

เว็บไซต์กว่า 3 ล้านเว็บล่มทันทีหลังจากเกิดเหตุไฟไหม้ที่บริษัทให้บริการ Cloud ประเทศฝรั่งเศส

by Flashfly Content Team — March 11, 2021 in NEWS

https://www.flashfly.net/wp/336152

The State of Cybersecurity in ASEAN, 2020

จากการศึกษาของ University of Maryland

พบว่าเหล่าแฮกเกอร์จำนวนมากพยายามที่จะแฮกระบบในทุก ๆ 39 วินาทีโดยเฉลี่ยหรือมากถึง 2,244 ครั้งต่อวัน!

เหตุผลที่ Cyber Security เข้ามามีความสำคัญต่อธุรกิจไทยเป็นอย่างมากในปี 2020, HardcoreCEO, November 10, 2020
https://hardcoreceo.co/cyber-security-pr/

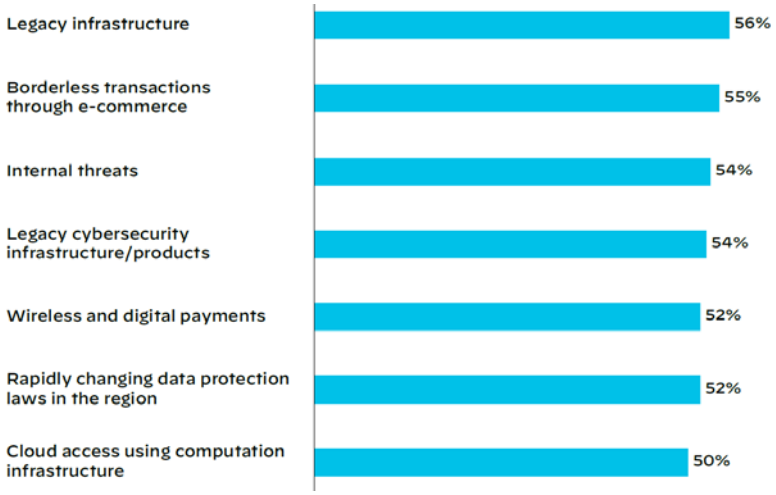
Source: Palo Alto Networks, The State of Cybersecurity in ASEAN, 2020

The State of Cybersecurity in ASEAN, 2020

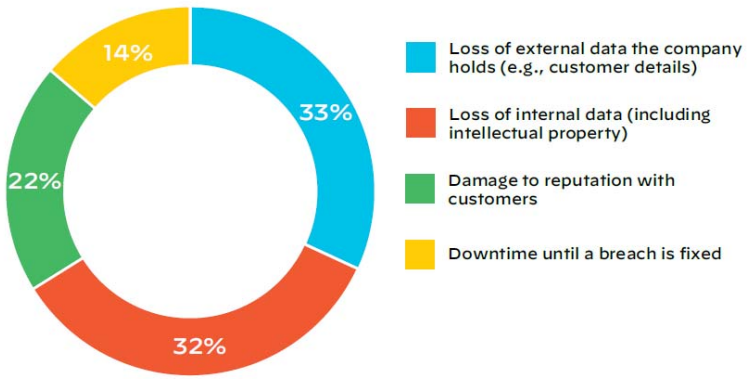
ความท้าทายสูงสุดที่องค์กรอาเซียนต้องเผชิญ

Source: Palo Alto Networks, The State of Cybersecurity in ASEAN, 2020

The State of Cybersecurity in ASEAN, 2020



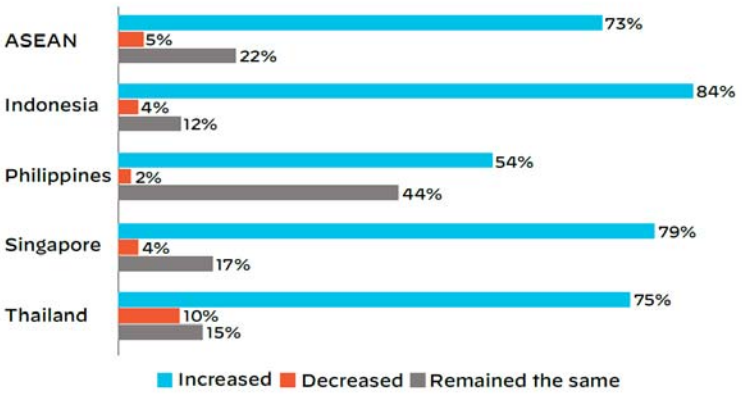
Cybersecurity issues of regional concern



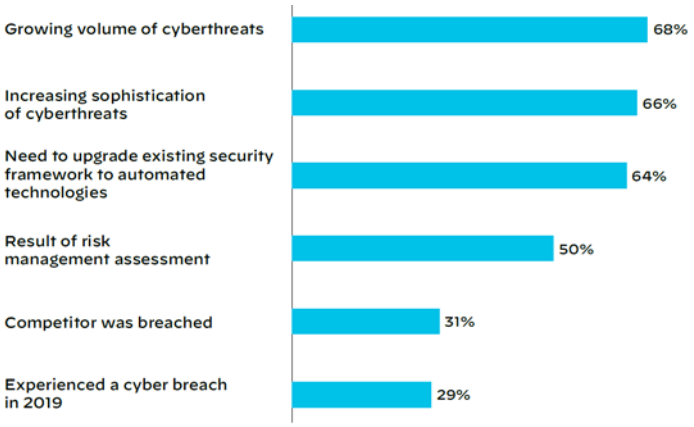
Biggest concerns beyond monetary damages

Source: Palo Alto Networks, The State of Cybersecurity in ASEAN, 2020

The State of Cybersecurity in ASEAN, 2020



Cybersecurity budget trends across the region



Top reasons for cybersecurity budget growth across ASEAN

Source: Palo Alto Networks, The State of Cybersecurity in ASEAN, 2020

The Global Cybersecurity Index (GCI)

Global Top Ranking

GCI 2014

Country	Index	Global Rank
United States of America	0.824	1
Canada	0.794	2
Australia	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand	0.735	4
Norway	0.735	4
Brazil	0.706	5
Estonia	0.706	5
Germany	0.706	5
India	0.706	5
Japan	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5
Thailand	0.412	15

GCI 2017

Country	Index	Global ranking
Singapore	0.92	1
United States	0.91	2
Malaysia	0.89	3
Oman	0.87	4
Estonia	0.84	5
Mauritius	0.82	6
Australia	0.82	7
Georgia	0.81	8
France	0.81	8
Canada	0.81	9
Russian Federation	0.78	10
Thailand	0.68	20

GCI 2018

Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.195	0.200	0.186	0.137
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.162	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137
11	Australia	0.890	0.200	0.174	0.200	0.176	0.139
35	Thailand	0.796					

Source: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.a

GCI Pillars

Asia-Pacific Region: Thailand

UK Cyber Security Strategy

DEFEND is about ensuring that the UK can be defended against cyber threats as they evolve.
DETER aims to make the UK a hard target for attackers.
DEVELOP is the Government expanding the skills base in a growing UK cyber security industry, supporting scientific research and using the National Cyber Security Centre as a centre of excellence that can both support industry in security product selection and advise on current threats and cyber security good practice.

These three objectives are underpinned by **INTERNATIONAL ACTION** which would see expanded relationships with existing international partners and engagement with new partners to improve collective security and to protect UK interests overseas.

https://www.ascentor.co.uk/2017/01/theres-sheriff-town-uk-cyber-security-strategy-2016/

Singapore's National Cyber Security Strategy

https://pt.slideshare.net/benjaminang/singapores-national-cyber-security-strategy/27

วิสัยทัศน์ของออสเตรเลียและการดำเนินการของรัฐบาล ธุรกิจ และชุมชน

Vision

A more secure online world for Australians, their businesses and the essential services upon which we all depend.

การดำเนินการของรัฐบาล (Actions by governments)

ประเด็นสำคัญ:

- ปกป้องโครงสร้างพื้นฐานที่สำคัญ บริการที่จำเป็น และครัวเรือน
- ต่อสู้กับอาชญากรรมทางไซเบอร์รวมถึงเว็บมืด (dark web)
- ปกป้องข้อมูลและเครือข่ายของรัฐบาลออสเตรเลีย
- แบ่งปันข้อมูลภัยคุกคาม (Share threat information)
- เสริมสร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ (Strengthen cyber security partnerships)
- สนับสนุนธุรกิจให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (Support business to meet cyber security standards)
- เพิ่มความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Enhance cyber security capabilities)

การดำเนินการโดยธุรกิจ (Actions by businesses)

ประเด็นสำคัญ:

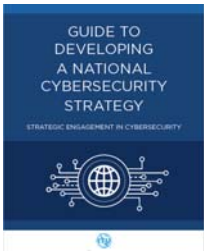
- ปรับปรุงความมั่นคงปลอดภัยขั้นต่ำ (baseline security) สำหรับโครงสร้างพื้นฐานที่สำคัญ
- ยกระดับความมั่นคงปลอดภัยไซเบอร์ของ SME
- จัดหาผลิตภัณฑ์และบริการที่มั่นคงปลอดภัย
- เพิ่มบุคลากรที่มีทักษะ
- ทำตามขั้นตอนเพื่อบล็อกกิจกรรมที่เป็นอันตรายในระดับที่เหมาะสม

การดำเนินการโดยชุมชน (Actions by the community)

ประเด็นสำคัญ:

- เข้าถึงและประยุกต์ใช้แนวทางและข้อมูลเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (guidance and information on cyber security)
- ทำการตัดสินใจซื้ออย่างชาญฉลาด
- รายงานอาชญากรรมทางไซเบอร์
- เข้าถึงความช่วยเหลือและการสนับสนุนเมื่อจำเป็น

Guide to Developing a National Cybersecurity Strategy by ITU



Focus area 1 - Governance

- Ensure the highest level of support
- Establish a competent cybersecurity authority
- Ensure intra-government cooperation
- Ensure inter-sectoral cooperation
- Allocate dedicated budget and resources
- Develop an implementation plan

Focus area 2 - Risk management in national cybersecurity

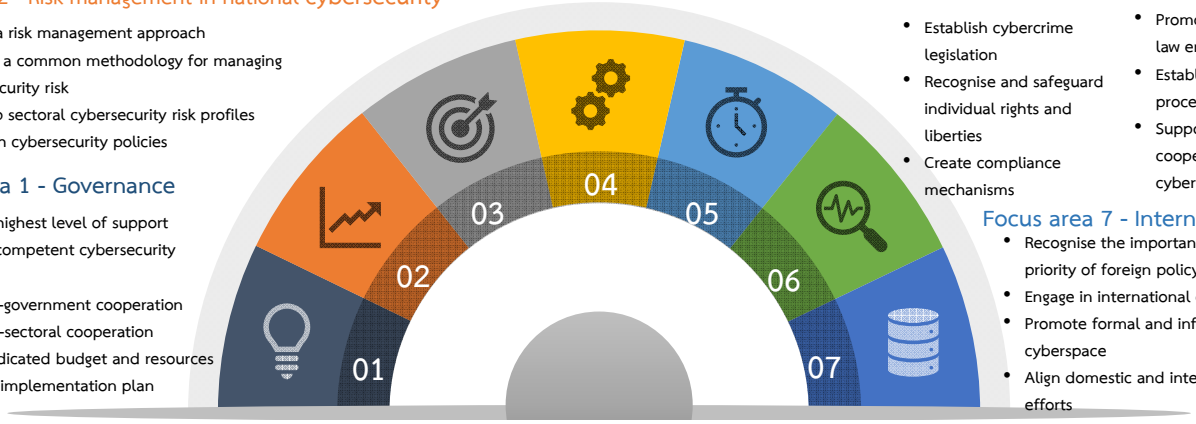
- Define a risk management approach
- Identify a common methodology for managing cybersecurity risk
- Develop sectoral cybersecurity risk profiles
- Establish cybersecurity policies

Focus area 3 - Preparedness and resilience

- Establish cyber-incident response capabilities
- Establish contingency plans for cybersecurity crisis management
- Promote information-sharing
- Conduct cybersecurity exercises

Focus area 4 - Critical infrastructure services and essential services

- Establish a risk-management approach to protecting critical infrastructures and services
- Adopt a governance model with clear responsibilities
- Define minimum cybersecurity baselines
- Utilise a wide range of market levers
- Establish public private partnerships



Focus area 5 - Capability and capacity building and awareness raising

- Develop cybersecurity curricula
- Stimulate skills development and workforce training
- Implement a coordinated cybersecurity awareness-raising programme
- Foster cybersecurity innovation and R&D

Focus area 6 - Legislation and regulation

- Establish cybercrime legislation
- Recognise and safeguard individual rights and liberties
- Create compliance mechanisms
- Promote capacity-building for law enforcement
- Establish inter-organisational processes
- Support international cooperation to combat cybercrime

Focus area 7 - International cooperation

- Recognise the importance of cybersecurity as a priority of foreign policy
- Engage in international discussions
- Promote formal and informal cooperation in cyberspace
- Align domestic and international cybersecurity efforts

จุดเน้นที่สำคัญ (Focus Area) ที่ระบุใน ITU	มาตรา 42 ใน พ.ร.บ ไซเบอร์
1) การกำกับดูแลของภาครัฐ (Governance)	1) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
2) การบริหารความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ (Risk management in national cybersecurity)	2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ 3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
3) การเตรียมความพร้อมและฟื้นคืนสู่สภาพปกติได้ (Preparedness and resilience)	2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
4) บริการโครงสร้างพื้นฐานที่สำคัญและบริการที่สำคัญ (Critical Infrastructure services and essential services)	3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
5) การเสริมสร้างความสามารถและศักยภาพและการสร้างความตระหนักรู้ (Capability and capacity building and awareness raising)	5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน 7) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
6) กฎหมายและระเบียบกฎเกณฑ์ (Legislation and regulation)	8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
7) ความร่วมมือระหว่างประเทศ (International cooperation) 	4) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ (นอกจากนี้ การประสานงานระหว่างภาครัฐและเอกชนยังกระจายไปตามแผนปฏิบัติการ (Initiatives) ที่สำคัญในด้านอื่น ๆ)

Good Practice Guide
Designing and Implementing National Cyber Security Strategies
by ENISA

1. Develop national cyber contingency plans
2. Protect critical information infrastructure
3. Organize cyber security exercises
4. Establish baseline security measures
5. Establish incident reporting mechanisms
6. Raise user awareness
7. Strengthen training and educational programs
8. Establish an incident response capability
9. Address cyber crime
10. Engage in international cooperation
11. Establish a public-private partnership
12. Balance security with privacy and data protection
13. Institutionalize cooperation between public agencies
14. Foster R&D in cyber security
15. Provide incentives for the private sector to invest in security measures

Key Recent Recommendations

- Focus on essential services not infrastructure -- reflect in how to identiy critical services and asset
- Not just availability, explicitly mention integrity and confidentiality
- Cooperation across operators, sectors, and borders
- Promoting C-level commitment
- Promote exercises and drills
- Encourage sharing of risk-related information
- Should focus more on SMEs
- Work with vendor PPP- set product standards

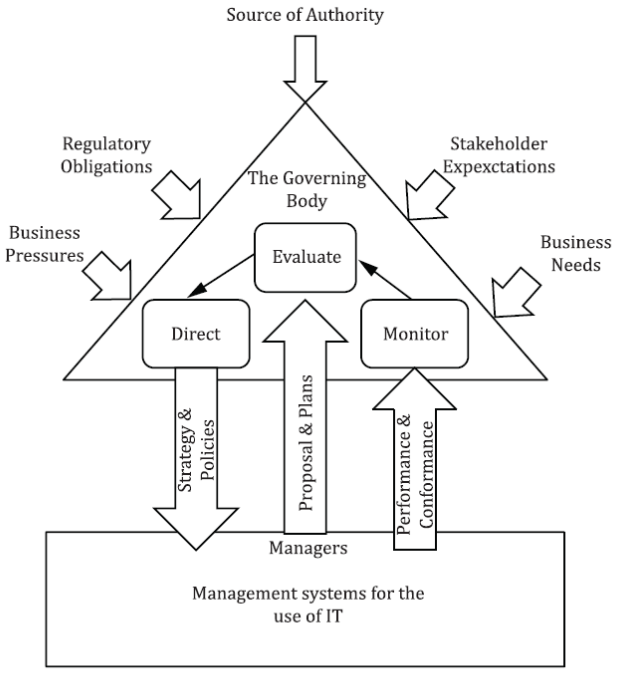
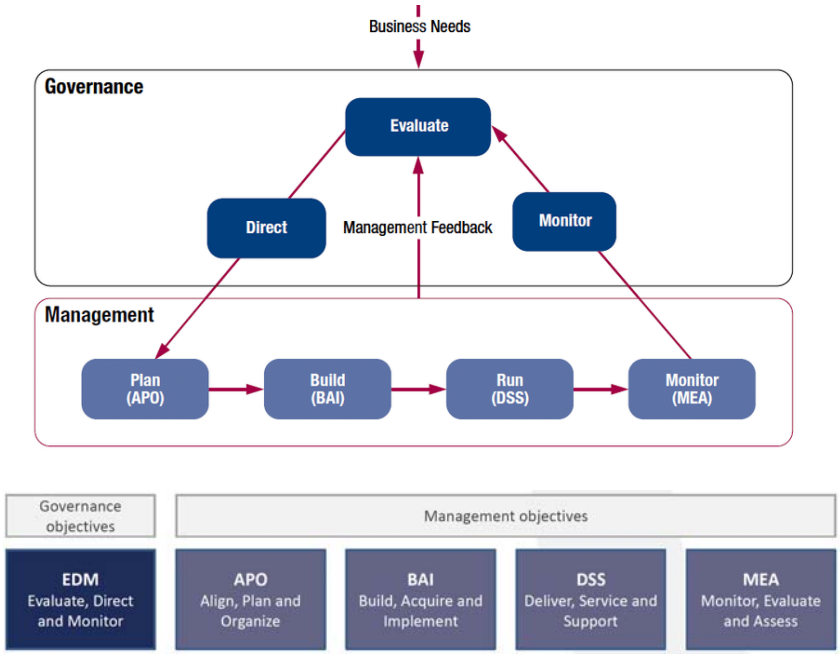


Figure 1 — Model for Governance of IT

ISO/IEC 38500:2015
Information technology — Governance of IT for the organization



COBIT 2019 and COBIT 5 five governance and management objectives, ISACA

Vision

บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์
เพื่อความยั่งยืนทางเศรษฐกิจและสังคม

ประเด็นยุทธศาสตร์ 1
สร้างศักยภาพของหน่วยงานระดับชาติ
ให้มีคุณภาพและมาตรฐาน

ประเด็นยุทธศาสตร์ 2
สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทาง
สารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์
และฟื้นคืนสู่สภาพปกติได้

บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์
เพื่อความยั่งยืนทางเศรษฐกิจและสังคม

ประเด็นยุทธศาสตร์ 3
บูรณาการความร่วมมือเพื่อเตรียมความพร้อมใน
การรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้

ประเด็นยุทธศาสตร์ 4
สร้างขีดความสามารถในการรักษา
ความมั่นคงปลอดภัยไซเบอร์ของประเทศ
(คน องค์ความรู้ และเทคโนโลยี)

ประเด็นยุทธศาสตร์	มาตรา 42 ใน พ.ร.บ ไซเบอร์
1. สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	1) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ 2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ 3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
2. สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ 3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
3.บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ 3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 4) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
4. สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (คน องค์ความรู้ และเทคโนโลยี)	5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน 7) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

[DRAFT]

National Cybersecurity Policy and Strategy Landscape

VISION

วิสัยทัศน์ — บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ และฟื้นคืนสู่สภาพปกติได้ เพื่อความมั่นคงทางเศรษฐกิจและสังคม

4 STRATEGIES / 11 FOCUS AREAS / 37 KEY INITIATIVES

ประเด็นยุทธศาสตร์ 1	ประเด็นยุทธศาสตร์ 2	ประเด็นยุทธศาสตร์ 3	ประเด็นยุทธศาสตร์ 4
สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (คน องค์ความรู้ และเทคโนโลยี)
1.1เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	2.1 กำหนดมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ CII	3.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชน	4.1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์
1.2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม	2.2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับ CII	3.2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม	4.2 สร้างความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพลเมืองไทยและธุรกิจ
1.3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยไซเบอร์ขององค์กรที่ให้บริการที่สำคัญ	2.3 ปกป้องระบบของรัฐบาล (ข้อมูลและเครือข่าย)		4.3 ส่งเสริมและสนับสนุนการวิจัยและพัฒนาและนวัตกรรมในภาคความมั่นคงปลอดภัยไซเบอร์
12 Key Initiatives	9 Key Initiatives	7 Key Initiatives	9 Key Initiatives

Strategic Theme 1

สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

Key Objectives	12 Initiatives
1.1 เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ทางไซเบอร์	1) ส่งเสริมและสนับสนุนการปฏิบัติงานของ สกมช. ให้มีคุณภาพและมาตรฐาน 2) เพิ่มขีดความสามารถ สกมช. ในการให้บริการ 3) ปรับปรุงกฎหมาย ระเบียบและข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์ 4) ผสานรวมการค้นพบภัยคุกคาม การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 5) จัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ 6) จัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ 7) การสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม 8) ส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ
1.2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม	1) สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์ 2) ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ
1.3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรที่ให้บริการที่สำคัญ	1) ขยายการสนับสนุนของ สกมช. ไปยังองค์กรที่ให้บริการที่สำคัญ 2) ส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

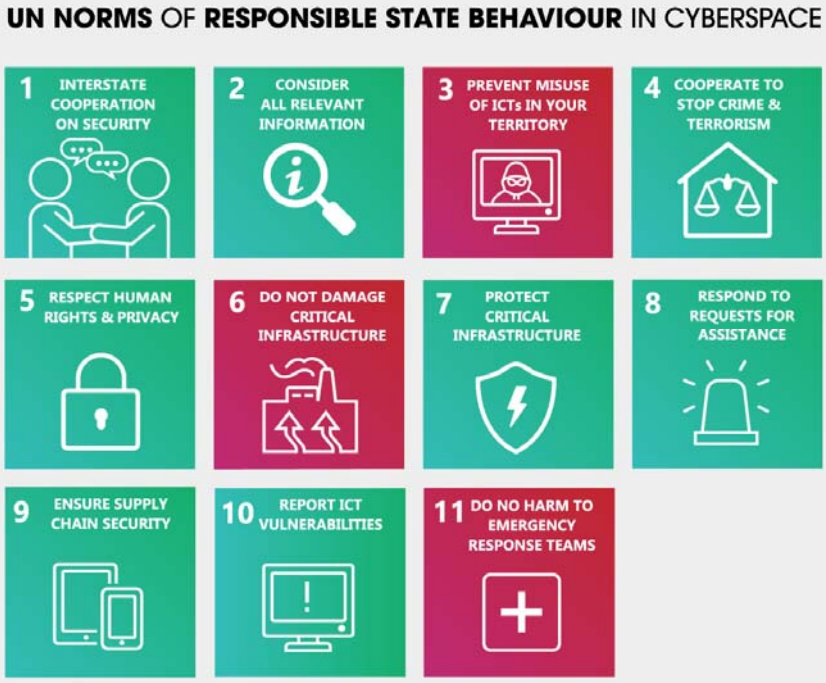
Strategic Theme 2

สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้

Key Objectives	9 Initiatives
2.1 กำหนดมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ CII	1) พัฒนาหลักปฏิบัติ (Code of practices) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance) 2) ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) 3) ส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุด และพนักงาน)
2.2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับ CII	1) กฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ 2) พัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับ CII (แนวทางและการควบคุมกำกับดูแล) 3) พัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของผู้ดำเนินการ CII และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที
2.3 ปกป้องระบบของรัฐบาล (ข้อมูลและเครือข่าย)	1) ส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default) 2) พัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล) 3) สร้างการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ

Strategic Theme 3 | บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้

Key Objectives	7 Initiatives
3.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชน	1) ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว 2) ประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ (เช่น หอการค้า) เพื่อรวมความมั่นคงปลอดภัยไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร 3) สนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง การดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจ และเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์) 4) เป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลสำหรับการจัดแนวระหว่างการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูล
3.2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม	1) สนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ 2) ส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง 3) ส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ **เพื่อสร้างศักยภาพด้านไซเบอร์**



https://www.dfat.gov.au/international-relations/themes/cyber-affairs/international-security-and-cyberspace/un-cyber-norms-resources

UN framework

https://www.dfat.gov.au/international-relations/themes/cyber-affairs/international-security-and-cyberspace/un-cyber-norms-resources

Strategic Theme 4 | สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(คน องค์ความรู้ และเทคโนโลยี)

Key Objectives	9 Initiatives
4.1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	1) พัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ 2) ยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นที่ยอมรับ 3) พัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง
4.2 สร้างความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพลเมืองไทยและธุรกิจ	1) บูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา 2) สร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ 3) พัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต 4) ให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน
4.3 ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมในภาคความมั่นคงปลอดภัยไซเบอร์	1) ส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลตฟอร์มการวิจัย และพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) ส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

2. (ร่าง) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 9 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ

(3) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์

โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

Strategic Theme 1 | **สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน**

Key Objectives	12 Initiatives
1.1 เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ทางไซเบอร์	1) ส่งเสริมและสนับสนุนการปฏิบัติงานของ สกมช. ให้มีคุณภาพและมาตรฐาน 2) เพิ่มขีดความสามารถ สกมช. ในการให้บริการ 3) ปรับปรุงกฎหมาย ระเบียบและข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์ 4) ผสานรวมการค้นพบภัยคุกคาม การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 5) จัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ 6) จัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ 7) การสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม 8) ส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ
1.2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม	1) สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์ 2) ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ
1.3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรที่ให้บริการที่สำคัญ	1) ขยายการสนับสนุนของ สกมช. ไปยังองค์กรที่ให้บริการที่สำคัญ 2) ส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

12 Initiatives

โครงการ	หน่วยงานรับผิดชอบหลัก	หน่วยงานรับผิดชอบรอง
1.1-1) ส่งเสริมและสนับสนุนการปฏิบัติงานของ สกมช. ให้มีคุณภาพและมาตรฐาน	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ สกมช.	
1.1-2) เพิ่มขีดความสามารถ สกมช. ในการให้บริการ	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ สกมช.	หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. กห. สตช. สดช. สทป. อว. DEPA
1.1-3) ปรับปรุงกฎหมาย ระเบียบและข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์	สกมช.	กระทรวงยุติธรรม กห. สตช. สพร. สพธอ.
1.1-4) ผสานรวมการค้นพบภัยคุกคาม การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล
1.1-5) จัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล สมช. บก.ทท. เนื่องจากผู้บัญชาการทหารสูงสุด ในฐานะกรรมการ กกม.โดยตำแหน่ง มีอำนาจหน้าที่ตามมาตรา 12-14 ในการร่วมรับมือกับภัยคุกคามทางไซเบอร์ ในระดับร้ายแรง
1.1-6) จัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	สกมช.	สพร. สพธอ. สมช.หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. เนื่องจากเป็นหน่วยงานหลักในการจัดการฝึกซ้อมความมั่นคงปลอดภัยทาง ไซเบอร์ ให้กับศูนย์ไซเบอร์เหล่าทัพ กลาโหม และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตั้งแต่ปี พ.ศ. 2561

โครงการ	หน่วยงานรับผิดชอบหลัก	หน่วยงานรับผิดชอบรอง
1.1-7) การสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม	สกมช.	กสทช.
1.1-8) ส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
1.2-1) สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. สตช.
1.2-2) ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. สตช.
1.3-1) ขยายการสนับสนุนของ สกมช. ไปยังองค์กรที่ให้บริการที่สำคัญ	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล
1.3-2) ส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล บีโอไอ

Strategic Theme 2

สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้

Key Objectives	9 Initiatives
2.1 กำหนดมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ CII	1) พัฒนาหลักปฏิบัติ (Code of practices) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance) 2) ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) 3) ส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุด และพนักงาน)
2.2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับ CII	1) กฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ 2) พัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับ CII (แนวทางและการควบคุมกำกับดูแล) 3) พัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของผู้ดำเนินการ CII และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที
2.3 ปกป้องระบบของรัฐบาล (ข้อมูลและเครือข่าย)	1) ส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default) 2) พัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล) 3) สร้างการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ

9 Initiatives

โครงการ	หน่วยงานรับผิดชอบหลัก	หน่วยงานรับผิดชอบรอง
2.1-1) พัฒนาหลักปฏิบัติ (Code of practices) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance)	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.1-2) ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.1-3) ส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุดและพนักงาน)	สกมช.	สพร. สพธอ. กพ. หน่วยงานควบคุมหรือกำกับดูแล
2.2-1) กฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์	สกมช.	ยธ. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.2-2) พัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับ CII (แนวทางและการควบคุมกำกับดูแล)	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.2-3) พัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของผู้ดำเนินการ CII และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที	สกมช.	ยธ. กต. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.3-1) ส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.3-2) พัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล)	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
2.3-3) สร้างการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

Strategic Theme 3 | บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้

Key Objectives	7 Initiatives
3.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชน	1) ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว 2) ประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ (เช่น หอการค้า) เพื่อรวมความมั่นคงปลอดภัยไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร 3) สนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง การดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจ และเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์) 4) เป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลสำหรับการจัดแนวระหว่างการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูล
3.2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม	1) สนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ 2) ส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง 3) ส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ **เพื่อสร้างศักยภาพด้านไซเบอร์**

7 Initiatives

โครงการ	หน่วยงานรับผิดชอบหลัก	หน่วยงานรับผิดชอบรอง
3.1-1) ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว	สกมช.	สพร. สพธอ. สตช. หน่วยงานควบคุมหรือกำกับดูแล
3.1-2) ประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ (เช่น หอการค้า) เพื่อรวมความมั่นคงปลอดภัยไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร	สกมช.	สพร. สพธอ. ดศ. สดช. สศด. หน่วยงานควบคุมหรือกำกับดูแล
3.1-3) สนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง การดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจ และเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์)	สกมช.	สพร. สพธอ. สตช. หน่วยงานควบคุมหรือกำกับดูแล กระทรวงยุติธรรม กระทรวงกลาโหม บก.ทท.
3.1-4) เป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลสำหรับการจัดแนวระหว่างการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูล	สกมช.	สพร. สพธอ. ดศ. หน่วยงานควบคุมหรือกำกับดูแล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
3.2-1) สร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ	สกมช.	สพร. สพธอ. สตช. หน่วยงานควบคุมหรือกำกับดูแล
3.2-2) ส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
3.2-3) ส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ เพื่อสร้างศักยภาพด้านไซเบอร์	สกมช.	สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

Strategic Theme 4 | สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(คน องค์ความรู้ และเทคโนโลยี)

Key Objectives	9 Initiatives
4.1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	1) พัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ 2) ยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นที่ยอมรับ 3) พัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง
4.2 สร้างความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพลเมืองไทยและธุรกิจ	1) บูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา 2) สร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ 3) พัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต 4) ให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน
4.3 ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมในภาคความมั่นคงปลอดภัยไซเบอร์	1) ส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลตฟอร์มการวิจัย และพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) ส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

9 Initiatives

โครงการ	หน่วยงานรับผิดชอบหลัก	หน่วยงานรับผิดชอบรอง
4.1-1) พัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ	สกมช.	สพร. สพธอ. กพ. ดศ. สคช. สดช. สอศ. อว. หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. สปท. บีโอไอ
4.1-2) ยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นที่ยอมรับ	สกมช.	สพร. สพธอ. กพ. สคช. อว. สดช. สอศ. สพฐ. ดศ. สำนักงบประมาณ หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. สปท.
4.1-3) พัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง	สกมช.	สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สำนักงบประมาณ หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. สปท.
4.2-1) บูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา	สกมช.	สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแล
4.2-2) สร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ	สกมช.	สพร. สพธอ. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแล บีโอไอ
4.2-3) พัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ
4.2-4) ให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ.
4.3-1) ส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลตฟอร์มการวิจัย และพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล สพร. สพธอ. กพ. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ
4.3-2) ส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	สกมช.	หน่วยงานควบคุมหรือกำกับดูแล สพร. สพธอ. กพ.

3. (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา 9 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ

(2) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การกำกับดูแล
การบริหารความเสี่ยง และการปฏิบัติตาม
(Governance, Risk and Compliance: GRC)

IT Governance , Risk and Compliance Objectives

"Combining disciplines for better enterprise security. Adopting a unified IT governance, risk management and compliance (IT GRC) approach, and managing the associated activities coherently will create efficiencies, provide a holistic view of the IT environment and ensure accountability"

https://www.pwc.com/th/en/rcs/it-grc.html

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Reliability
- Confidentiality

(ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)
2. การบริหารความเสี่ยง (Risk Management)
3. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนี้มีผลบังคับใช้ภายในหนึ่ง (1) ปี นับถัดจากวันที่ประกาศ

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

1.1 ต้องกำหนดโครงสร้างการกำกับดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจน และจัดทำเป็นเอกสารลายลักษณ์อักษร โดยมีรายละเอียด ดังนี้

(ก) ระบุโครงสร้างองค์กรสำหรับการจัดการความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) ระบุสิ่งที่เจ้าหน้าที่เหล่านี้ได้รับอนุญาตและ/หรืออนุมัติให้ทำ

(ค) ระบุว่าบุคคลใดมีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นไปตามพระราชบัญญัติกฎหมายย่อยใด ๆ ที่ทำภายใต้พระราชบัญญัติตลอดจนหลักปฏิบัติ หรือมาตรฐานการปฏิบัติงานทั้งหมดที่ออกโดยคณะกรรมการตามมาตรา 9 (4) ของพระราชบัญญัติ

1.2 ต้องมีกระบวนการตรวจสอบให้แน่ใจว่าบุคลากรที่ได้รับมอบหมาย มีการปฏิบัติตามนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)(ต่อ)

1.3 การกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.3.1 หน่วยงานของรัฐ**ต้อง**จัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน ภายในหนึ่ง (1) ปี นับถัดจากวันที่ประกาศ

โดยบุคคลดังกล่าว**ต้อง**เป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ผู้บริหารที่ทำหน้าที่ดังกล่าว**ควร**มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยดังนี้

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด
- มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)
- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ
- ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)(ต่อ)

1.3.2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**ต้อง**จัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน ภายในหนึ่ง (1) ปี นับถัดจากวันกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าว**ควร**เป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

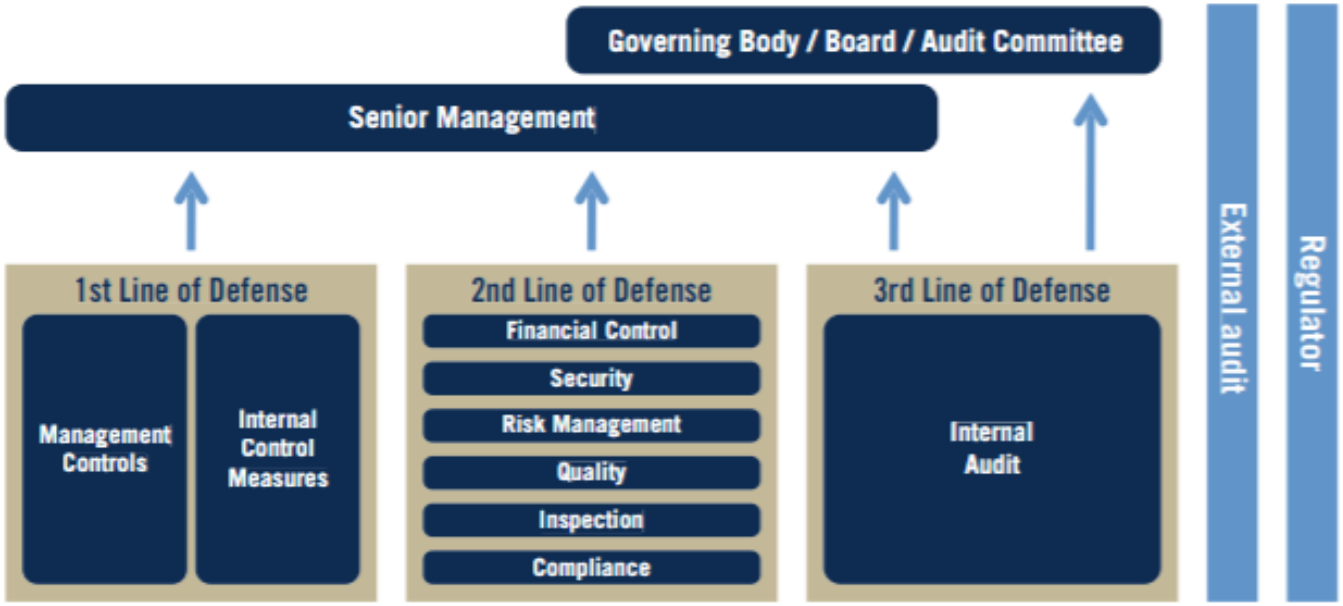
- รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และคณะกรรมการที่เกี่ยวข้องโดยตรง
- ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญ

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)(ต่อ)

1.4 ต้องจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร และหน้าที่ความรับผิดชอบที่เกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งต้องมีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน ทั้งหน่วยงานหรือผู้ที่ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) หน่วยงานกำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) และหน่วยงานตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม โดยให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถือปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องในปัจจุบัน รวมถึงแนวปฏิบัติในเรื่องดังกล่าวที่จะออกโดยหน่วยงานควบคุมหรือกำกับดูแล และจะมีผลบังคับใช้กับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต่อไป

ทั้งนี้ กรณีที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศรวมกับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบตาม Three Lines of Defense ให้สามารถพิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกัน

The Three Lines of Defense Model



ประกาศธนาคารแห่งประเทศไทย

ที่ สกส. ๑๒/๒๕๖๒

เรื่อง ธรรมาภิบาลของสถาบันการเงินเฉพาะกิจ

หน้า ๑๖ (เล่มที่ ๑)
เล่ม ๑๓๖ ตอนพิเศษ ๒๔๑ ง ราชกิจจานุเบกษา ๒๗ กันยายน ๒๕๖๒

(๒) การควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีหน่วยงานที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งต้องมีการกำหนดหน้าที่ความรับผิดชอบของแต่ละหน่วยงานอย่างชัดเจน ทั้งหน่วยงานหรือผู้ที่ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) หน่วยงานกำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) หน่วยงานสอบทานสินเชื่อ (Credit Review) และหน่วยงานตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม โดยให้สถาบันการเงินเฉพาะกิจถือปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องในปัจจุบัน รวมถึงแนวปฏิบัติในเรื่องดังกล่าวที่จะออกโดยธนาคารแห่งประเทศไทย และจะมีผลบังคับใช้กับสถาบันการเงินเฉพาะกิจต่อไป

2. การบริหารความเสี่ยง (Risk Management)

2.1 ต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร กรอบจะรวมถึง:

(ก) บทบาทและความรับผิดชอบในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์รวมถึงสายการรายงานและความรับผิดชอบ

(ข) การระบุและการจัดลำดับความสำคัญของทรัพย์สินบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) ระบุเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

(ง) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และ

(จ) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.2 ต้องเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.3 ต้องตรวจสอบความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ให้ได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ที่ระบุไว้ในข้อ 2.1 (ค)

3. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

3.1 ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์ นโยบาย มาตรฐาน และแนวปฏิบัติจะต้อง:

(ก) สอดคล้องกับหลักประมวลแนวทางปฏิบัตินี้ ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ และ

(ข) เผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

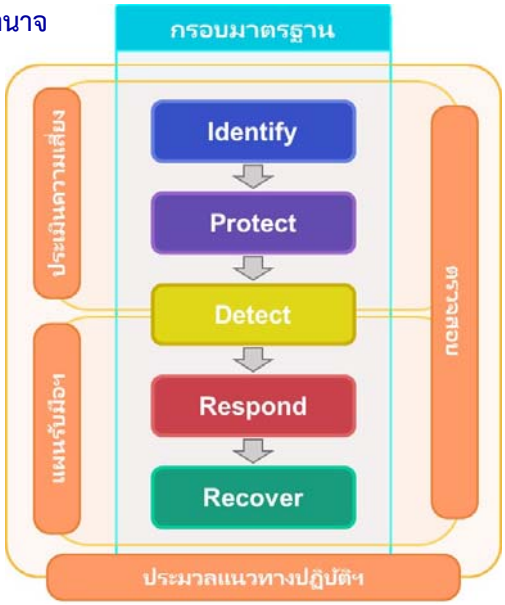
3.2 ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่ง (1) ครั้งโดยนับถัดจากวันที่การทบทวนครั้งสุดท้าย หรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวปฏิบัติแต่ละข้อ

ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 13 คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ

(4) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

มาตรา 44 ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง **อย่างน้อย**ต้องประกอบด้วยเรื่อง ดังต่อไปนี้
(1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
(2) แผนการรับมือภัยคุกคามทางไซเบอร์



4. (ร่าง) ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

1. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3. แผนการรับมือภัยคุกคามทางไซเบอร์

หมายเหตุ
“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

1.แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1 ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่ง (1) ครั้ง โดยมีขอบเขตของการตรวจสอบจะรวมถึง:

(ก) การวิเคราะห์ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัติและประมวลแนวทางปฏิบัตินี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และทิศทางที่คณะกรรมการอาจออกให้

1.2 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการ ต่อสำนักงานภายในสามสิบ (30) วัน นับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 แห่งพระราชบัญญัติ พร้อมทั้งสำเนาส่งให้หน่วยงานควบคุมหรือกำกับดูแล

หมายเหตุ: รูปแบบสรุปรายงานการตรวจสอบ สกมช. จะกำหนดรายละเอียดในการดำเนินการต่อไป

1. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

1.3 ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ของพระราชบัญญัติ ระบุการไม่ปฏิบัติตาม หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ๆ กับข้อกำหนดที่ระบุไว้ในพระราชบัญญัติ หรือประมวลแนวทางปฏิบัติ หรือมาตรฐานการปฏิบัติงานที่ออกภายใต้พระราชบัญญัติ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในสามสิบ (30) วันทำการนับถัดจากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตามทั้งหมด และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อย่อย (ก)

1.4 ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมทั้งสำเนาส่งให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

1.5 เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้เสร็จสิ้นภายในระยะเวลาตามที่ระบุไว้ในนั้นเพื่อผ่านเกณฑ์พิจารณาของ กกม. โดยหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเอง

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

2.1 การประเมินความเสี่ยง (Risk assessment)

(ก) การระบุความเสี่ยง (Risk identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk appetite)

2.การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

2.2 การจัดการความเสี่ยง (Risk treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ (Key risk indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

2.3 การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

2.4 การรายงานความเสี่ยง (Risk reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่ง (1) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

3. แผนการรับมือภัยคุกคามทางไซเบอร์

3.1 ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องระบุรายละเอียดอย่างน้อย ดังนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ซึ่งกำหนดว่า หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึง แต่ไม่จำกัดเพียงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement protocols) กับบุคคลภายนอกรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์ / การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-action review process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

3. แผนการรับมือภัยคุกคามทางไซเบอร์ (ต่อ)

3.2 ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3.3 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้ง โดยเริ่มตั้งแต่การจัดทำแผน

3.4 ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

5. (ร่าง) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้
(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนด**กรอบมาตรฐาน**ตามวรรคหนึ่ง (๔) ให้คำนึงถึง**หลักการบริหารความเสี่ยง** โดยอย่างน้อยต้องประกอบด้วย**วิธีการและมาตรการ** ดังต่อไปนี้

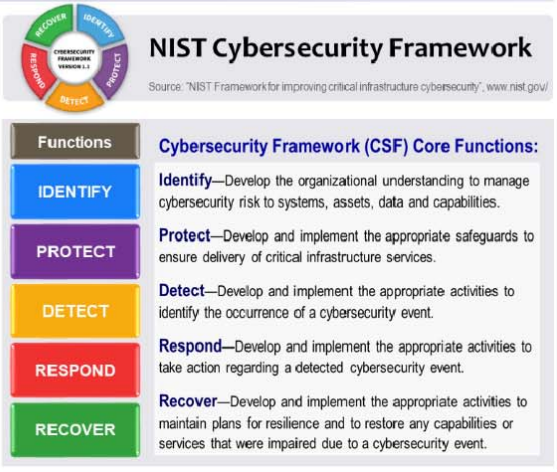
(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์



กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะมีผลบังคับใช้ภายในหนึ่ง (1) ปี หลังจากวันที่ประกาศ

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPONSE	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Strategy	Protective Technology			
What processes and assets need protection?	What safeguards are available?	What techniques can identify incidents?	What techniques can contain impacts of incidents?	What techniques can restore capabilities?

ห.ร.บ. ไซเบอร์	การระบุความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	มาตรา 13 (4)

แนวทางการกำหนด แนวทางปฏิบัติและกรอบมาตรฐาน (Baseline Security Measures)

- What to include as minimum security measures
- and accommodate for sector-specific that is advanced
- and scale up as CII and sectors become more mature

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

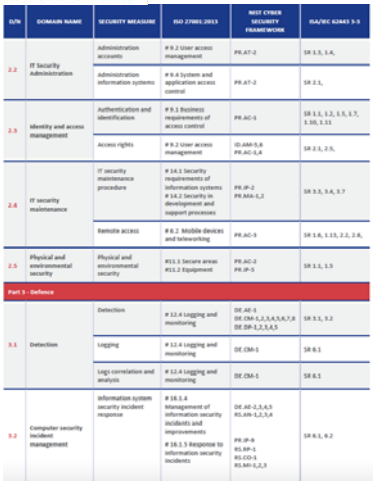
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03

Reference document on security measures for Operators of Essential Services

CG Publication 01/2018

Mapping the Baseline Security Measures for OES to cross sector international standards

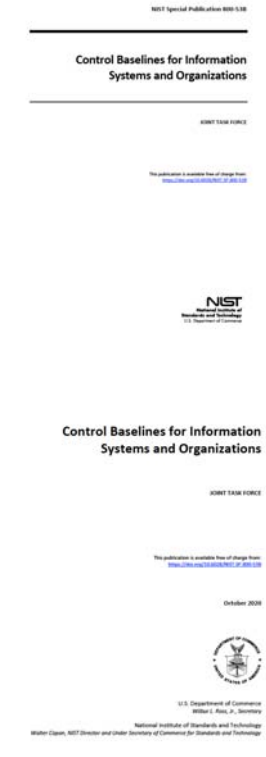
D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
Part 1 – Governance and Ecosystem					
1.1	Information System Security Governance & Risk Management	Information system security risk analysis	# 8.2 Information security risk assessment (ISO 27001) # 8.3 Information security risk treatment (ISO 27001)	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2	SR 5.2, 5.3,
		Information system security policy	# 5.1 Management direction for information security	ID.GV-1,2,3	–



D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
		Incident report	# 16.1.5 Response to information security incidents	RS.CO-1,2,3,4,5	SR 6.2
		Communication with competent authorities	–	–	–
Part 4 - Resilience					
4.1	Continuity of Operations	Business continuity management	# 17.1 Information security continuity	ID.BE-5 PR.DS-4 PR.IP-4	SR 7.3, 7.4
		Disaster recovery management	# 17.2 Redundancies	PR.DS-4 PR.IP-10	SR 7.4, 7.5
4.2	Crisis Management	Crisis management organization	# 17.1 Information security continuity	PR.DS-4 PR.IP-10	SR 7.4, 7.5
		Crisis management process	# 17.1 Information security continuity	PR.DS-4	SR 7.4, 7.5

Table 22: Mapping of the information security measures to the international information security standards applied to all the sectors

DOMAIN NAMES	SECURITY MEASURES	FINANCIAL AND BANKING					HEALTHCARE		DRINKING WATER SUPPLY AND DISTRIBUTION	DIGITAL INFRASTRUCTURES
		PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX	ISO27799	HIPAA	(Table 22)	ISO 27011
Part 1 – Governance and Ecosystem										
Information System Security Governance & Risk Management	Information system security risk analysis	•	–	•	•	–	•	•	–	–
	Information system security policy	•	•	•	•	•	•	•	–	•
	Information system security accreditation	•	–	•	•	•	•	•	–	–
	Information system security indicators	•	•	•	•	•	•	•	–	–
	Information system security audit	•	–	•	•	•	•	•	–	–
	Human resource security	•	–	•	•	–	•	•	–	•
	Asset Management	•	•				•	•	–	•



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53B

NIST

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53B

October 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

3.1 ACCESS CONTROL FAMILY

Table 3-1 provides a summary of the controls and control enhancements assigned to the Access Control Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "w" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	**Policy and Procedures**	x	x	x	x
AC-2	**Account Management**		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE	W: Incorporated into AC-2k.			
AC-2(11)	USAGE CONDITIONS				x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS			x	x
AC-3	**Access Enforcement**		x	x	x
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTION	W: Incorporated into AC-6.			
AC-3(2)	DUAL AUTHORIZATION				
AC-3(3)	MANDATORY ACCESS CONTROL				
AC-3(4)	DISCRETIONARY ACCESS CONTROL				
AC-3(5)	SECURITY-RELEVANT INFORMATION				
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	W: Incorporated into MP-4, SC-28.			
AC-3(7)	ROLE-BASED ACCESS CONTROL				
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS				
AC-3(9)	CONTROLLED RELEASE				
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS				
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES				
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS				
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL				
AC-3(14)	INDIVIDUAL ACCESS	x			
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL				
AC-4	**Information Flow Enforcement**			x	x
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES				

Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

August 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

Mapping NIST Framework with

1) enisa baseline security measures
2) NIST Control Baselines

Function	Category	Subcategory	All SP 800-53 Controls
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6,
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	-1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PM-1, PM-2, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	PM-3, PM-7, PM-9, PM-10, PM-11, SA-2
		ID.RA-1: Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

(ร่าง) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น

1.1 การจัดการทรัพย์สิน (Asset Management)

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1.3 การประเมินช่องโหว่ และหรือการทดสอบเจาะระบบ (Vulnerability Assessment and/or Penetration Testing)

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

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)

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity exercise)

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

หมายเหตุ

“คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“ผู้ให้บริการภายนอก ” หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น

1.1 การจัดการทรัพย์สิน (Asset Management)

1.1.1 ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ / คำอธิบายของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เจ้าของและ / หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละรายการ และ

(จ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ / เครือข่ายภายในและ / หรือภายนอก

1.1.2 ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and significant interface)

1.1.3 ต้องปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละหนึ่ง (1) ครั้ง และเมื่อมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญใด ๆ ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.1.4 ตามมาตรา 54 ของพระราชบัญญัติ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ 1.1.1 อย่างน้อยปีละหนึ่ง (1) ครั้ง

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1.2.1 ต้องดำเนินการตามข้อ 2 การบริหารความเสี่ยง (Risk Management) ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.2.2 ทะเบียนความเสี่ยงจะได้รับการปรับปรุงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารดังต่อไปนี้

(ก) วันที่ระบุความเสี่ยง

(ข) คำอธิบายของความเสี่ยง

(ค) โอกาสที่จะเกิดขึ้น

(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)

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

1.3 การประเมินช่องโหว่ และ/หรือการทดสอบเจาะระบบ (Vulnerability Assessment and/or Penetration Testing)

1.3.1 ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุม

(ก) สำหรับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็นระบบเทคโนโลยีสารสนเทศหรือ IT (Information Technology system)

(ข) สำหรับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็นระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรมหรือ ICS (Industrial Control System)

1.3.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย:

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

1.3.3 ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน การอัปเกรดระบบ และการปรับเปลี่ยนเทคโนโลยี

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

1.3 การประเมินช่องโหว่ และ/หรือการทดสอบเจาะระบบ (Vulnerability Assessment and/or Penetration Testing) (ต่อ)

1.3.4 **ควรพิจารณา**ดำเนินการทดสอบเจาะระบบ (Penetration testing) บริการที่สำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะที่เชื่อมต่อกับอินเทอร์เน็ต (Internet facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการเจาะระบบด้วย

1.3.5 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a penetration test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.3.6 ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยหนึ่ง (1) ครั้งตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การอัปเกรดระบบ และการปรับเปลี่ยนเทคโนโลยี

1.3.7 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration testers) ที่กำลังทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะ

1.3.8 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบโดยดำเนินการภายใต้การดูแลของหน่วยงาน

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

1.3 การประเมินช่องโหว่ และ/หรือการทดสอบเจาะระบบ (Vulnerability Assessment and/or Penetration Testing) (ต่อ)

1.3.9 ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในการประเมินช่องโหว่และในการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

1.3.10 หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบข้อมูล ซึ่งถูกพิจารณาให้เป็นไปตามมาตรา 54 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงานภายในสามสิบ (30) วันหลังนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา 54 แห่งพระราชบัญญัติ พร้อมทั้งสำเนาส่งให้หน่วยงานควบคุมหรือกำกับดูแล เพื่อดำเนินการตามมาตรา 55 แห่งพระราชบัญญัติด้วย

หมายเหตุ รูปแบบสรุปรายงานการตรวจสอบ สกมช. จะกำหนดรายละเอียดในการดำเนินการต่อไป

1.การระบุและประเมินความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

1.4.1 ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษา/ความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะการดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1.4.2 ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service level agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดควรคำนึงถึงสิ่งต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ และ

(ง) สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

1.4.3 ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

1.4.4 ควรพิจารณาดำเนินเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้เป็นสอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ๆ

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

2.1 การควบคุมการเข้าถึง (Access Control)

2.1.1 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ

(ข) อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาต

2.1.2 ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ 2.1.1 หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity risk profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.1.3 ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of all access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

2.1.4 ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอลมีการกำกับดูแลโดย

(ก) ทำภายใต้การดูแลของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น และ

(ข) ดำเนินการในสถานที่ หากเป็นไปได้

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.2.1 ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity risk profile) ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.2.2 มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) จะกล่าวถึงหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least access privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ และ

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening) (ต่อ)

2.2.3 ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.2.4 ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration standard) ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

2.2.5 ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change management process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.3 การเชื่อมต่อระยะไกล (Remote Connection)

2.3.1 ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.2 สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น

(ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission security) และความสมบูรณ์ของข้อความ (Message integrity) ที่แข็งแกร่ง

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing system commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ

(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

2.4.1 ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ 2.1.1 (ข) เท่านั้น และ

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2.4.2 ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนสื่อบันทึกข้อมูลแบบถอดได้

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.5.1 ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ อย่างน้อยจะรวมถึงสิ่งต่อไปนี้

กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

(ก) พนักงานใหม่ (New employees)

(ข) ผู้ใช้และระดับบริหาร (Users and management)

(ค) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS และ

(ง) ผู้ขาย ผู้รับเหมา และผู้ให้บริการ (Vendors, contractors and service providers)

(จ) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ฉ) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎระเบียบนโยบาย แนวปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ

(ช) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

2.5.2 ต้องทบทวนแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (ต่อ)

2.6 การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

หมายเหตุ สกมช. จะกำหนดรายละเอียด แนวทาง และรูปแบบในการแบ่งปันในการดำเนินการต่อไป

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

3.1.1 ต้องสร้างกลไกและกระบวนการเพื่อ

(ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และ

(ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่

3.1.2 ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพตามวัตถุประสงค์ภายใต้ข้อ 3.1.1

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์

4.1.1 ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่ง (1) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.2.1 ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.2.2 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต:

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

(จ) ระบุแพลตฟอร์ม / ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

4.2.3 ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

4.2.4 ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละหนึ่ง (1) เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (ต่อ)

4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity exercise)

4.3.1 ตามมาตรา 22(13) ของพระราชบัญญัติ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

4.3.2 ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ 4.2 และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

5.1.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (“Business Continuity Plan: BCP”) เพื่อให้แน่ใจว่าบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

5.1.2 ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละหนึ่ง (1) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์