

เตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ NIST Cybersecurity

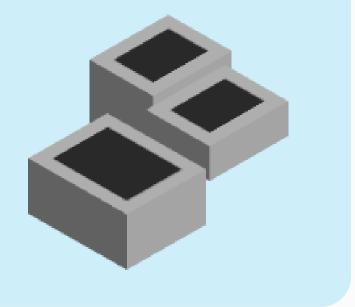
Framework 2.0

สถาบันมาตรฐานอังกฤษ



Agenda discussion

- Overview of NIST Cyber security Framework and What news for NIST Cyber Security Framework Version 2
- What is New function Govern
- Overall implementation of NIST CSF and Cyber security Act.
- NIST CSF Certification Process

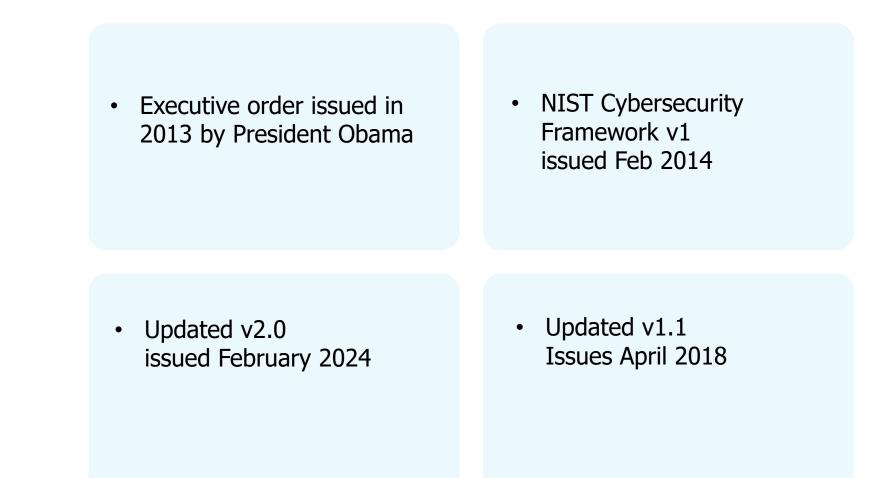






Overview of NIST Cyber security Framework and What news for NIST Cyber Security Framework Version 2

Background



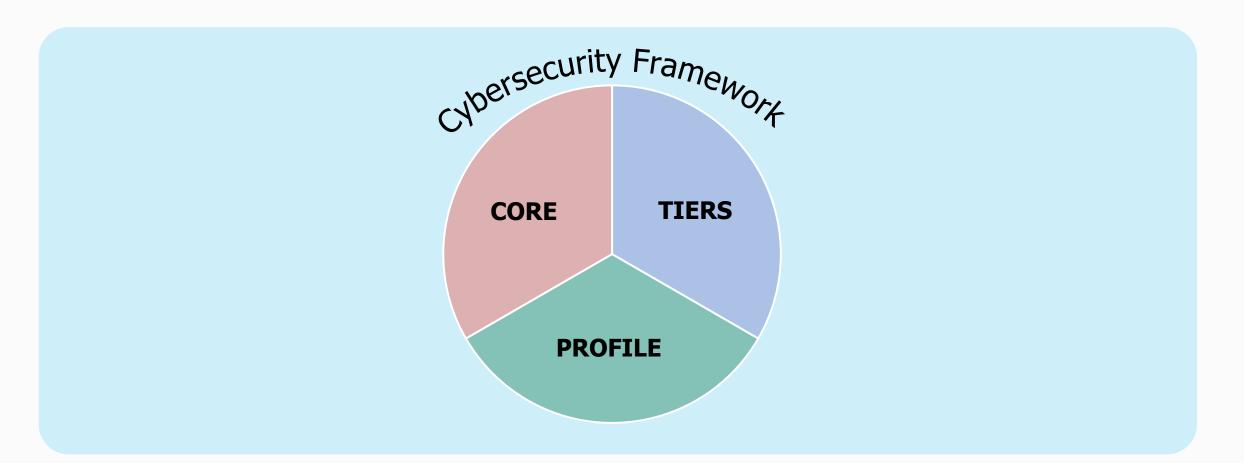


NIST CSF - Version 2.0

- Change name from "Framework for Improving Critical Infrastructure Cybersecurity" to "The Cybersecurity Framework,"
 - All audiences, industry sectors and organization types,
 - All size of organization
 - All degree of cybersecurity sophistication. D
- Change from 5 Main functions to 6 Main functions
- Focus how to implement by any online tools and easy searched for befit tools.
- New function "Govern"
 - o organization can make and execute its own internal decisions to support its cybersecurity strategy
 - cybersecurity is a major source of enterprise risk .VS. Risk from legal, financial and other risks considerations for senior leadership.
- Provides improved and expanded guidance on implementing the CSF profiles, etc.



Three components





Framework Core



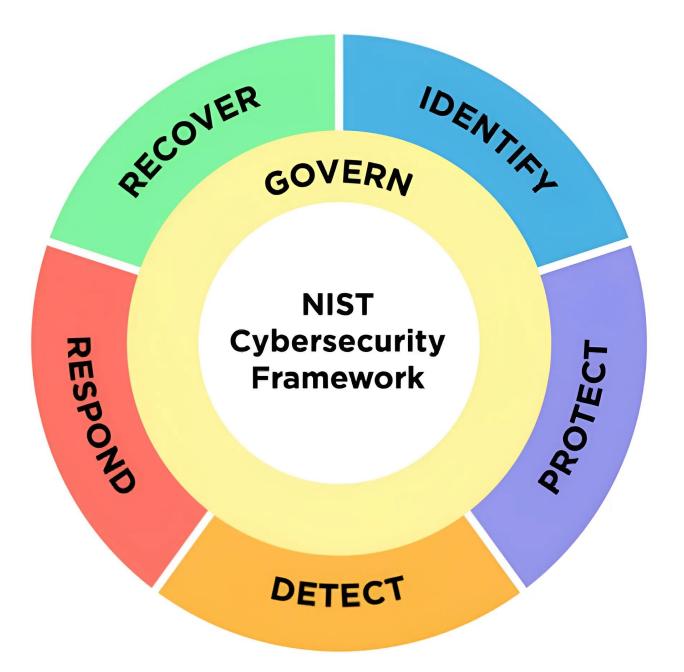
Set of activities/desired outcomes and applicable references

Six functions:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover









Framework Implementation Tiers

- Provide context
- Maturity of risk management practices e.g.:
 - Risk and threat aware
 - Repeatable
 - Adaptive
- Tiers range from Partial (Tier 1) to Adaptive (Tier 4)





Framework Profile

Represents outcomes based on business needs Aligns organization's standards/practices etc. to Framework Core Used to:

- Identify opportunities for improving cybersecurity
- Support prioritization and measure progress
- Conduct self-assessment
- Communicate within an organization or between organizations





Supporting Knowledge of NIST Cyber Security Framework Version 2.0

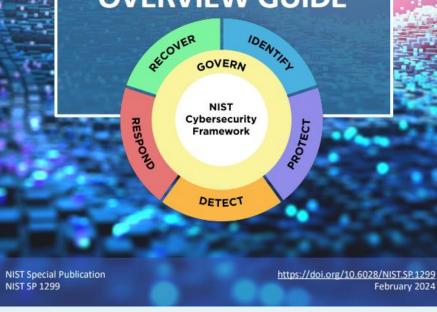






NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE





NIST Cybersecurity White Paper NIST CSWP 32 ipd

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles

Initial Public Draft

Cherilyn Pascoe National Cybersecurity Center of Excellence National Institute of Standards and Technology

Julie Nethery Snyder The MITRE Corporation

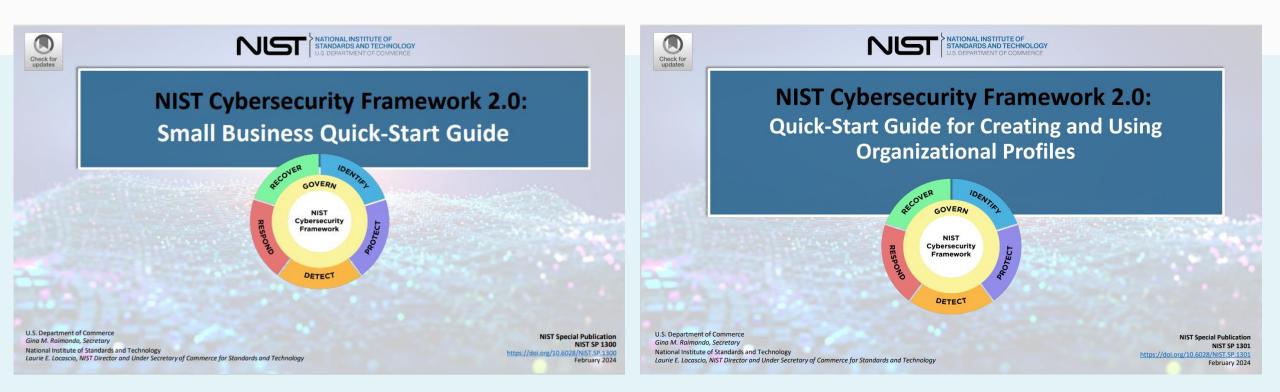
Karen Scarfone Scarfone Cybersecurity

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.32.ipd

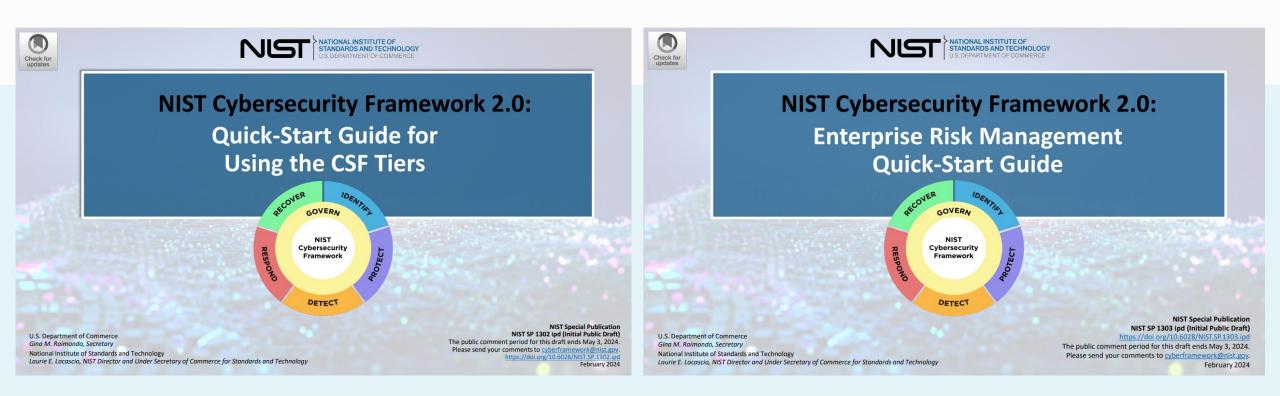
February 26, 2024



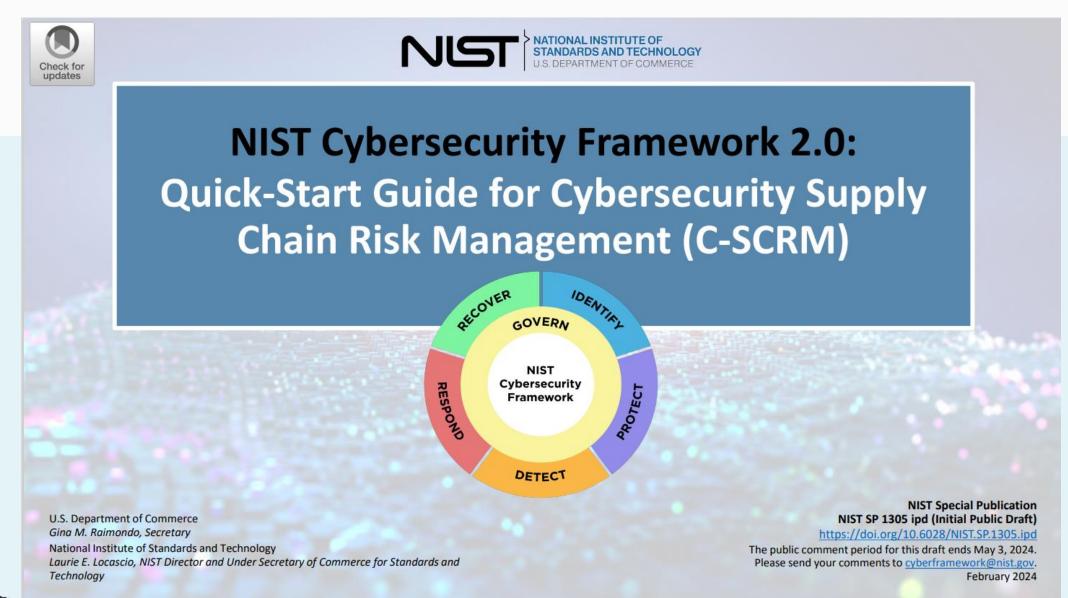












bsi

CSF 2.0 Organization Profile Template

	А	В	С	D	E	F	G	н	I.	J	К	L	M	N	0	Р	Q	R	
1	CSF Outcome (Function, Category, c Subcategor	CSF Outcome Description	Included in Profile	Rationale v	Current Priorit	Current Statu-	Current Policies, Processes, and Procedure 🚽	Current Internal Practices	and	Current Selected Informative Reference 🖵	Current Artifacts	Target Prior	Target CSF T ⁱ →	Target Policies, Processes, and Procedures	Target Internal Practices	Target Roles and Responsibilitie	Target Selected Informative References	Notes	
2	GV	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored																	
3		The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood																	
4		The organizational mission is understood and informs cybersecurity risk management																	
5	SV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered																	
-		Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed																	
0		Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated																	
7	GV.OC-05	understood and communicated Outcomes, capabilities, and services that the organization depends on are understood and communicated																	
	GV.RM	The organization's priorities,																	-
	\leftarrow	Column Descriptions	Current a	and Tar	get Profi	le	(+)												



CRI Profile V 2.0



This work is licensed under the Creative Commons Attribution-Noncommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-



The CRI Profile, ver. 2.0 - An Overview and User Guide -

INFORMATIONAL PURPOSES ONLY: The information contained within this spreadsheet document and in related Profile documents are intended for informational purposes only. The information contained herein is provided on an "as is" basis without warranty of any kind, either express or implied. CRI assumes no liability or responsibility for any errors or omissions in the content of this document. Please be sure to check for the most recent versions at https://cyberriskinstitute.org.

Talk with your regulator; by including mappings and references to various regulatory agencies' publications, that does not mean, nor should it be construed, that the referenced agency necessarily supports, or endorses, the mappings or the Profile's use for regulatory purposes. Additionally, use of the Profile does not limit what a supervisor can review or requires. Rather, the Profile enables financial institutions to confidently produce baseline evidence for review and more quickly respond to iterative and follow-up questions from examiners.

1 Introduction

Cyber Risk Institute (CRI) has developed CRI's Profile v2.0 framework to create an efficient approach to technology and cybersecurity risk management that effectively counters dynamic and evolving threats and provides adequate assurance to government supervisors. This is an updated version of the CRI Profile ver. 1.2.1 that serves to provide additional guidance for organizations to align with technology and cybersecurity regulatory expectations and authorities. The Profile also provides a flexible structure to inform the development of a cybersecurity program according to business needs and specific regulatory expectations within an individual organization, vocabulary, and taxonomy.

Through collaboration and consensus between financial institutions, this document seeks to develop both a self-assessment and tool for institutions to create a common baseline security threshold, and provide a common supervisory engagement approach among state, federal, and international regulatory bodies. This is possible because the Profile has been mapped to and integrated numerous global standards and supervisory expectations, including those from Japan, the European Union, Australia, Singapore, and the United States, among others.

User Guide Impact Tiering Questionnaire CRI Profile v2.0 Structure

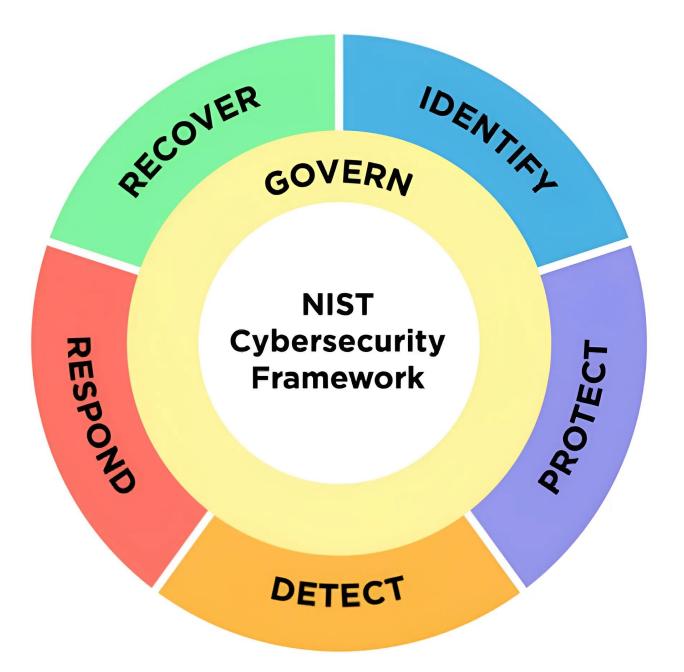
CRI Profile v2.0 Assessmen ... (+) 🕴 🔳





What is New function -Govern

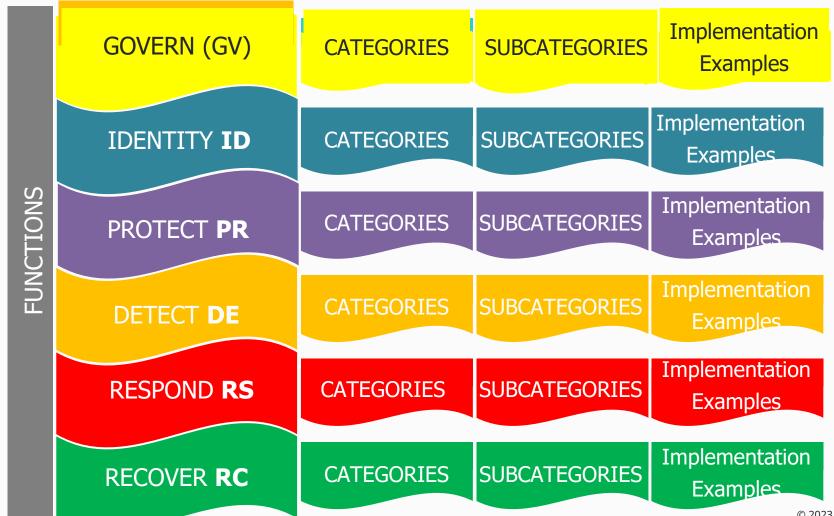
What is NIST CSF Version 2 requirement





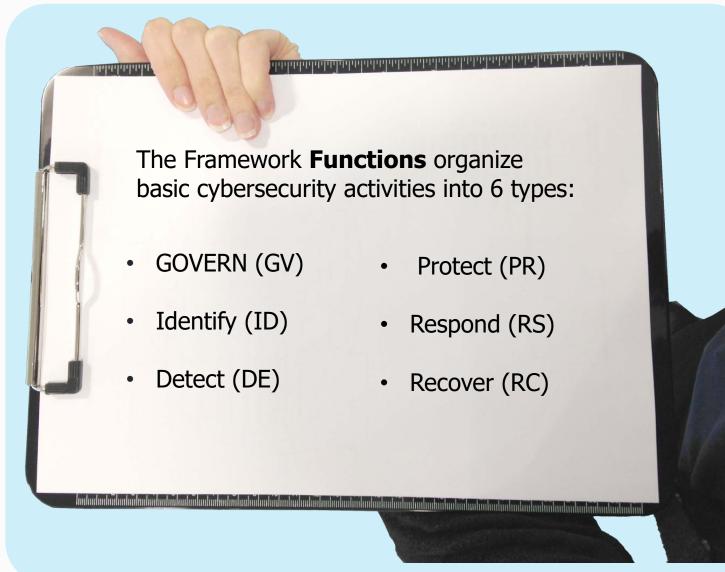
Framework Core

The Framework Core provides a structured set of activities to achieve specific cybersecurity outcomes





Framework Core





Framework Core – Govern (GV): (ID) function

Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

Organizational Context (GV.OC):

Risk Management Strategy (GV.RM):

Cybersecurity Supply Chain Risk Management (GV.SC)

Roles, Responsibilities, and Authorities (GV.RR):

Policies, Processes, and Procedures (GV.PO): Oversight (GV.OV)





Other Function of NIST CSF

Framework Core – Identify (ID) function

Identify - The organization's current cybersecurity risks are understood

Asset Management (ID.AM) Risk Assessment (ID.RA) Improvement (ID.IM)



Framework Core – Protect (PR) function

Protect – Safeguards to manage the organization's cybersecurity risks are used

Identity Management, Authentication, and Access Control (PR.AA) Awareness and Training (PR.AT) Data Security (PR.DS)

Platform Security (PR.PS) Technology Infrastructure Resilience (PR.IR)



Framework Core – Detect (DE) function

Detect – Possible cybersecurity attacks and compromises are found and analyzed

Continuous Monitoring (DE.CM)

Adverse Event Analysis (DE.AE)



Framework Core – Respond (RS) function

Respond – Actions regarding a detected cybersecurity incident are taken

Incident Management (RS.MA) Incident Analysis (RS.AN)

Incident Response Reporting and Communication (RS.CO) **Incident Mitigation (RS.MI)**

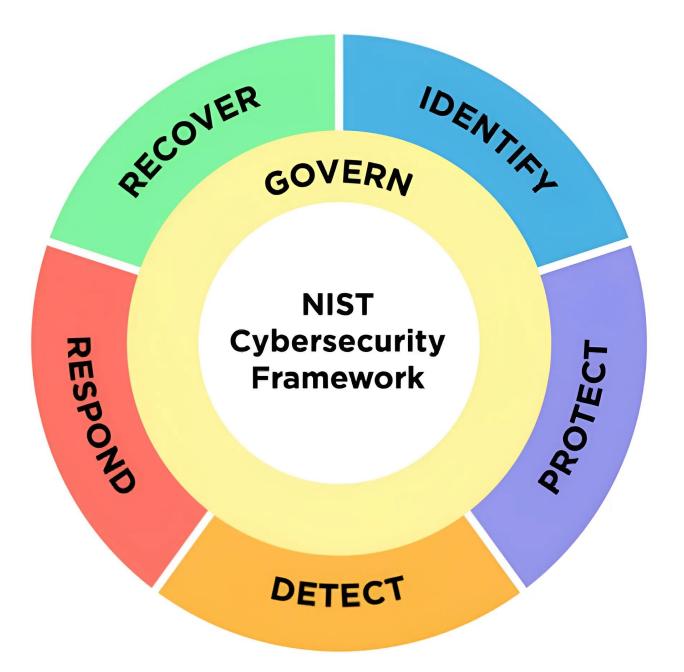


Framework Core – Recover (RC) function

Recover – Assets and operations affected by a cybersecurity incident are restored

Incident Recovery Plan Execution (RC.RP) Incident Recovery Communication (RC.CO)

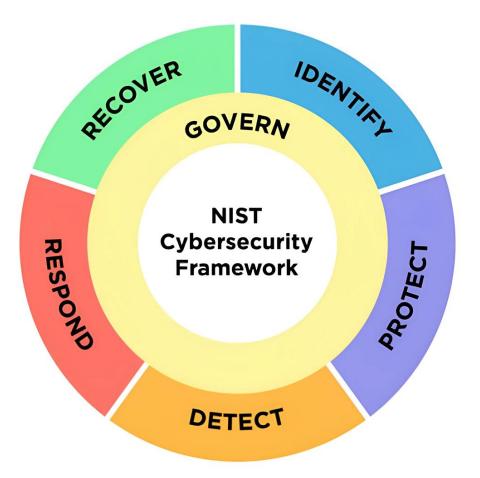






Implement of NIST Cybersecurity Framework 2.0 .VS. Cyber security Act. B.E. 2562





		4			หน้า ๒๐	2007.007		
ເລ່ມ	ດຄາວ	ตอนที่	ba	ก	ราชกิจจานุเบกษา	ାଜଣ	พฤษภาคม	මද්දුම



พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒ เป็นปีที่ ๔ ในรัชกาลปัจจุบัน





กฎหมายลำดับรองที่สำคัญ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไขเบอร์ พ.ศ. 2562

ประกาศ กมช. เรื่อง





ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของ ศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำคัญทางสารสนเทศ พ.ศ. 2564

สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐาน

หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. 2566

หมายเหตุ : สำดับที่ 14 อยู่ระหว่างนำเสนอคณะอนุกรรมการเพื่อพิจารณาร่าง ให้ความเห็นชอบและนำเสนอ กมช.

ประกาศ กกม. เรื่อง

ประกาศ สกมช. เรื่อง



ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสาน การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564



การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจ หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ และการมอบหมายการควบคุม และกำกับดแล พ.ศ. 2564

การกำหนดระดับความรู้ความชำนาญด้านการู



ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิ่น ปราบปรามและระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. 2564

หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์



ระเบียบ กกม. ว่าด้วย การมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการ ทำกับดแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565



ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษา ความมั่นคงปลอดกั้ยไซเบอร์ (พ.ศ. 2565 - 2570)

รักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้ง เป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะ ความมั้นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล

เรื่อระบบสารสนเทศ พ.ศ. 2566

ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือ ระบบสารสนเทศ พ.ศ. 2566

ประกาศ กกม. เรื่อง

W.A. 2566



ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ และหน่วยงาน ควบคุมหรือกำกับดแล พ.ศ. 2567



ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนา ระบบการให้บริการเกี่ยวกับการรักษา ความนั้นคงปลอดกัยไซเบอร์ พ.ศ. 2566



ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะ ความรัและความเชี่ยวชาญในด้านการรักษา ความนั้นคงปลอดกัยไซเบอร์ พ.ศ.



ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษา ความมิ้นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ W.Fl. 2564 ณีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป)



ศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์แห่งชาติ ได้มีการจัดตั้งเมื่อวันที่ 11 สิงหาคม 2564 มีหน้าที่ใบการเฝ้าระวัง ติดตาม ้วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคาม ทางไชเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคาม ทางไซเบอร์





ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศนย์ประสาน การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการกิจหรือให้บริการที่เกี่ยวข้อง W.A. 2564 (มีผลใช้บังคับตั้งแต่วันที่ 23 ฮ.ค. 65 เป็นต้นไป)

สาระสำคัญ เพื่อกำหนดลักษณะ หน้าที่ และความ รับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ (Sectoral CERT) สำหรับหน่วยงาน ้โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

ปัจจุบันมี Sectoral CERT ในประเทศไทย

- 1. Ministry of Defence Computer Security Incident Response Team (MOSCSIRT)
- 2. Thailand Civilian Sector CERT (TCS-CERT)
- 3.Ministry of Finance Computer Security Incident Response Team (MOF-CSIRT)
- 4.ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กรมศลกากร
- 5.ศนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ้ในด้านบริการภาครัฐที่สำคัญที่มีการให้บริการโดยตรงแก่ ประชาชน
- 6. Thailand Banking Sector CERT (TB-CERT)
- 7. Thai Capital Market CERT (TCM-CERT)
- 8. Thailand Telecommunication CERT (TTC-CERT) 9. Health CIRT



ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีการกิจ หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล W.A. 2564 (มีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป)

สาระสำคัญ เพื่อเป็นการประกาศกำหนดการกิจ หรือบริการของหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศทั้งสิ้น 7 ด้าน ปัจจุบันประกาศฯดังกล่าวมี Regulator 19 หน่วยงาน และ Cli 63 หน่วย



ด้านการเงินการธนาคาร และโกรคมนาคม และไลจิสติกส์

NCS







ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการ รักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 (มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 65 เป็นต้นไป)

สาระสำคัญ กำหนดให้หน่วยของรัฐ หน่วยงานควบคุม หรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ มีหน้าที่ในการจัดทำ**ประมวลแนวทางปฏิบัติ** และ**กรอบมาตรฐาน**ด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำ



bsi

ประมวลแนวทางปฏิบัติ มีองค์ประกอบดังนี้ แผนการตราวสวนห

แผนการตรวจสอบฯ
 การประเมินความเสี่ยงฯ
 แผนการรับมือภัยคุกคามทางไชเบอร์

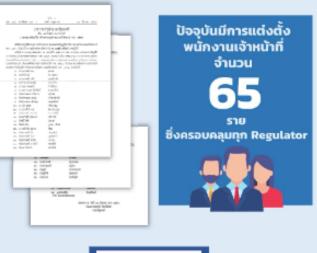
กรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีองค์ประกอบดังนี้

(1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นฯ (Identify)
 (2)มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
 (3)มาตรการตรวจสอบและเฝ้าระวังฯ (Detect)
 (4)มาตรการเผชิญเหตุฯ (Respond)
 (5)มาตรการรักษาและฟื้นฟูความเสียหายฯ (Recover)



ประกาศ กมช. เรื่อง การทำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคง ปลอดภัยไฮเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564 (มีผลใช้บังคับตั้งแต่วันที่ 8 ธ.ค. 64 เป็นต้นไป)

สาระสำคัญ เพื่อกำหนดคุณสมบัติและความรู้ความ ชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ บุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่





ประกาศ กมช. เรื่อง ลักษณะกัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับกัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (มีพฤใช้บังคับตั้งแต่วันที่ 12 ธ.ค. 64 เป็นต้นไป)

สาระสำคัญ เพื่อประโยชน์ในการจำแนกลักษณะของ ภัยคุกคามทางไซเบอร์แต่ละระดับ รวมทั้งประเมินจาก ระดับผลกระทบที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไชเบอร์ในระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ







ระเบียบ กกม. ว่าด้วย การมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 (มีผลใช้บังคับตั้งแต่วันที่ 27 ธ.ค. 65 เป็นต้นไป)

สาระสำคัญ เพื่อให้การดูแลและดำเนินการเพื่อรับมือกับ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ทันท่วงที่ให้ กกม. จึงมีการมอบอ่ำนาจให้คณะกรรมการรับมือกับภัยคุกคาม ทางไซเบอร์ในระดับร้ายแรง (ครร.) พิจารณาสั่งการกรณี เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับ ร้ายแรงหรือระดับวิกฤติ





ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) (มีผลไช้บังคับตั้งแต่วันที่ 10 ธ.ค. 65 เป็นต้นไป)

สาระสำคัญ เพื่อเป็นแผนแม่บทในการรักษาความมั่นคง ปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคง ปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ของประเทศ



ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 (มีผลใช้บังคับตั้งแต่วันที่ 10 พ.ค. 66 เป็นต้นไป)

สาระสำคัญ เพื่อกำหนดแนวทางในการแจ้งและรายงาน กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบ สารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ





ประกาศ สกมช. เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าปำรุง คำตอบแทน และค่าบริการในการดำเนินงาน W.A. 2566 (มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 66 เป็นต้นไป)

สาระสำคัญ เพื่อให้ สกมช. มีแนวทางในการเรียกเก็บ ้ค่าธรรมเนียมและ/หรือค่าบริการจากผู้รับบริการ สำหรับ กรณี ดังต่อไปนี้

(1) การใช้ระบบหรือบริการสารสนเทศ เครื่องมือ หรืออุปกรณ์ หรือสิ่งอำนวยความสะดวกและพื้นที่ หรือสถานที่

(2) การใช้บริการสำรวจ การวางแผน การจัดการ หรือการวิจัย ในลักษณะการว่าจ้าง

(3) การใช้บริการจัดฝึกอบรม สัมมนา หรือประชม เชิงปฏิบัติการ

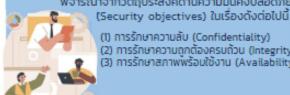
(4) การรับรองมาตรฐานผู้ให้บริการเกี่ยวกับ ความมั่นคงปลอดภัยไซเบอร์

(5) การใช้บริการดำเนินโครงการด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์หรือบริการอื่นที่เกี่ยวกับ หรือเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยไซเบอร์



ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคง ปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ W.A. 2566 ณีผลใช้บังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป)

สาระสำคัญ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ มีการกำหนดคุณลักษณะและการจัดระดับ ผลกระทบของข้อมูลหรือระบบสารสนเทศ



การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ฯ พิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์

> (1) การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity)
> การรักษาสภาพพร้อมใช้งาน (Availability)

การประเมินและจัดระดับผลกระทบ

แบ่งเป็น 3 ระดับ ระดับต่ำ ระดับกลาง ระดับสง



ประกาศ กมช. เรื่อง มาตรฐานขึ้นต่ำของข้อมูลหรือระบบสารสนเทศ W.A. 2566 ซีบังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป)

สาระสำคัญ กรณีหน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ ได้กำหนดคุณลักษณะและการจัดระดับ ผลกระทบของข้อมูลหรือระบบสารสนเทศของตน ว่ามีลักษณะ สูง กลาง หรือต่ำ แล้ว มีหน้าที่ต้องกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรื่อระบบสารสนเทศนั้นในแต่ละระดับ

ตาราง การกำหนุดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ ขึ้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ

			a americal alexandrollar seafulfs (manot)					
	an a line of A		lea merzepinsélő Doos Coleit	٠				
- and a	Print Line	COPUPH	Kin HTP//Perstdecta/Farit Gyten Hedering					
- eh	10014		ton methodological density Connection					
6dereases								
_			 k.a: trust or sustaining from subordnow'd much Epidemicially invariants 	•	•	•		
_	-	_	too track/bullage/orlanvation trainig)					
	•	٠	a americana and scholeyer and so all theats					
·	•	•	 Eglar Threat Britechian and tharitaring 		•	•		
			a areamanhqueqdalmerroeu/neyeruen/seast (rea	and -				
			et a unar riftalla floyor ann donaol (Cylor veraity Institut Regione Plat)	•	•	•		
			Contraction of the second seco	•	•	•		
·	•	٠	star mili Assenzilarniaashi kusé Kylommaty Fancisé	•	•	•		
			e envelopenitepratecularenteprende	of these	and in			
-	-	-	a. retrocollapseatoroliteratoprovised					
	4 • • •	di una 	4 min pi 4 min min	B 984 gs to reveal setup for an order setup of the reveal to reveal the reveal the reveal to reveal the reveal to reveal the reveal the reveal to reveal the reveal to reveal the reveal the reveal the reveal to reveal the reveal the reveal to reveal the reveal the reveal the reveal to reveal the reveal the reveal to reveal the reveal to reveal the reveal th	All and a set of	Bit of the second		





ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไขเบอร์ พ.ศ. 2566 (มีผลใช้บังคับตั้งแต่วันที่ 19 ม.ค. 67 เป็นต้นไป)

สาระสำคัญ เพื่อให้มีกระบวนการตรวจสอบและรับรอง การดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากร ที่เกี่ยวข้องในการดำเนินงาน ว่ามีคุณภาพเป็นไป ตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์





(ร่าง) ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะ ความรู้และความเซียวชาญในด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.

สาระสำคัญ เพื่อกำหนดมาตรการและแนวทาง ในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงาน เจ้าหน้าที่หรือเจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยไซเบอร์ และให้ระดับความรู้ ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของพนักงานเจ้าหน้าที่





ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญกาง สารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567 (มีผลใช้บังคับตั้งแต่วันที่ 22 มิ.ย. 68 เป็นต้นไป)

หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Of Dearty Suits	ana
(2) Solid South	a contractly influence in the structure and the second as a subsection of the second second
	กละดังเป็นประพัฒนจิมพิมพ์มะในปลาย เกราะๆมะ และในสมมณฑรางปฏิบัติและกระบาทหฐามกับสารอังการกระโลกง
our whereas the state	well be latter and a shelp have an electric
	editale de la service de la proversión de la construcción de la construcción de la service de la service de la
(of adopted over	a cramballagres i Defense animi grane anno articles i an éga su considerat
00 & 60 Dimension	xaaxha cuda xaaanii cud
	ometer seciedos hembro este de Alco Adarca?
	Team and a second and the second and the second second and the second second second second second second second
	น มีมหาวามเพื่องด้านการมีการการมนั้นกวนปลุดหรือไปเหตุลี
	สีนอองเรือกระบบการสองสองเรืองสินเว็จที่สุดทางการ
	n ben an de seu ella suber suber suber suber de la transferencia de la seu ella suber suber suber suber suber s Comenta el compañía e suber
	unful feature de une alle se aux avec via contra aux sont de acestra auxontes acestra la matificio de la matificio de la desta de la d
	CALIFICATION OF THE TAXABLE TAXABLE TO THE ET CONTRACTOR STOCKED AND THE TAXABLE TO THE TAXABLE
	หลัง วิเมื่อ และออราสต์แรงกล่องการบาทสระบุว่าวแห่ว่า แหล่ทำใหมาในประกาศสังเขณ เอกาจปฏิเป็ และมะเพิ่
	obe un Cràmba Achiele e nache e Achiele
ini uhutawa	dopas anadronu
OULDARCE	en és were feejnen. Arristoues
	axianiaot sapaha (Bestress Centinutry)
	fumumouridumatio
000 Berlinssons	
(30) chalour reco	of nov tio mu coverne tidel konstandone anarodiante e coverne de l'hinge 👘 🚺 🌉 🔧
	เพิ่าที่ของหน่วยงามควบทุมหรือทำกับตูแล ที่ต้องกำหนดให้ CII ปฏิบัติ
	รฐานที่หมางแข่งการรับปรกับกิดการหายของสระสอไปต่ำกับการรูกเป็นต่ำที่ และ แระการทำหละจ
(2) rhelugue	รฐานที่หมายขมะกรรีเขียวันทีมดากาษ เกิดกลังจะเจไม่ทำกับการฐานในที่ที่ จนม จะเกิดทำหนด อ
 rhelugua ospoacor 	รฐานที่หมางแปนการรับมีอยันที่อยุทศาสา เสอดเสี้ระองไม่ถึงต่ามกรรฐานในที่ที่ คมอ. แระกาศทั้งหมาย ดี เป็นในมีการออง 01
 (2) rhetagua (3) osciazioni (4) binoriusto 	รฐานที่หมายแข่นของให้มีอยันกับอาการหารของสิ่งของไม่ใหญ่มาตรฐานในที่ที่ คมขางอาการทำงนตร G "อย่านในการของ GI เฟอร์ หมือพูม Housema automstada Socia al CEPT 💦 👷 🜟
 rhelugua rhelugua ospaacor bisonusios bisonusios 	รฐานที่หมายแข่งกระวังปังกับเขียงกามหายของส่วนกระไม่ทำกว่ามาระรูจแข็งทำก็ คมมาระกาศทำหมาร CH กระกายสามาระอง CH แฟล คมังคม หลังระเสกมายในการรังกิ่ง Socianial GEPT แฟล์ คมังคมูม หลังระเสกมายในการรังกิ่ง Socianial GEPT
 rhefugue csobacori bisobacori bisobacori	รฐานที่หมายแข่นการรับข้อตับกัดอากามหารของสีระสงไม่ทำงว่ามาจรฐานในที่ได้ แบบ แระกาศทำงแหร่ CF เราะดำเนินการของ CT เครื่อ สนับหนุม หรือแระกาม อานับการรัดตั้ง Sociavial CEPT เกรื่อ สนับหนุม หรือแระกาม อานับการรัดข้อ Sociavial CEPT ใจ และครสามแหร่งออกกับสุดภาพมายสมมายสนับเลย CT
 rhefuqua ospaapur ospaapur bironucio 	sgrufikumendumszkilönündenen in tronniscunskichnörunesgrufuchti nur uzementerune El Indikuumsune Ol Indik münigu Hörschnurunumsztuda Soccarial CEPT Anke münigu Hörschnurunumsztudarenduksuse Ol Da Landensmurungen ummanuszt
 rhefugue ospagoe identudos bientudos bientudos bientudos bientudos bientudos derintutus derintutus derintutus 	sgrufie une autores Substantiale en un troco de canalité de la construire se de la construire de la construi
 rhefugua ospaacor ospaacor bienrudor bienrudor bienrudor bienrudor bienrudor bienrudor derhuhus derhuhus derhuhus derhuhus derhuhus 	sgrufi Humanianszkul baluniaen um troonissa anluich strungsgruf uch Hinau i sammitteare Ministration on Helle milliongun Hisissiam anlumistipale Social La CERT anlie mulangu Hisissiam anlumistipale Social La CERT anlie Millionis La Certain Stational La Certain and Social La CERT anlie Millionis La Certain Stational La Certain Annual Annual La Certain Annual L
 rhefugue rhefugue ospacov biesnutise biesnutise biesnutise biesnutise derhultuut derhultuut derhultuut derhultuut biesnutise biesnutise biesnutise biesnutise biesnutise 	sgnufikurvesskulostutisennuk totonäseakiirhotsunosgnufuchti nus usimerinkure El melin Bilangu Hönstemuruharnstolo Sectorial CERT melin Bilangu Hönstemuruharnstolo Sectorial CERT bi se escensitiosonnäseaminnossuus seuem suljätäkunteuruharnstoluus seuem suljätäkunteuruharnstoluus seuem suljätäkunteuruharna situ ana kenetistauet dhännas isemuon anti-institungu mu
 rhefugue rhefugue rassecut ressecut ressecut<	sgrufin understadioturisen un trockise adult hotunos grufiuthi nue us menthese an Institumises OI entée atlungu Houseme adurmisto de Sector tal CEPT entée atlungu Houseme adurmisto de Sector tal CEPT ente adurgu Houseme adurmisto de Sector tal CEPT enter adurgu Houseme adurmisto de Sector tal Sector de La descence de Sector adures de Centre adures de constante a adurente fondere situ de construisen adre differende adurente fondere situ de construisen adre differende adurente fonderen. Emplities de adre differende adurente fonderen. Emplities adures de adurente de adures de adures de adures de la difference adures de adures de adures de adures de adures de la difference adures de adure
 rhefugua rhefugua osphaeter biesnukse biesnukse biesnukse biesnukse detrikterse detrikterse ufriskerse ufriskerse ufriskerse ufriskerse ufriskerse ufriskerse 	sgnufikurvenziverszkulosturkeen versoonalse anklich ostunos gnufuchti nus us vernemen versoonalse on anklise kulongu klassis en unalamistado Sectorala CERT make mulangu klassis en unalamistado Sectorala CERT make mulangu klassis en unalamistadore su dans anochilau et do se eenonustoorannange uch un eshine su dans anochilau et mulane klassinge antikine still ange mulane anochilau et dhalamis utemuon a shiftinstillangu mula ale dhalau kan unalamistadore mulane anochilau et dise dhalau kan una stillane stillane anochilau et dhalamis utemuon a shiftinstillangu mula ale dhalau kan useda kanga mulane shiftinsa a guefini klause ausertado yan societa koon ama'hiriasa a
 rhefugua ospasour bismutos bismutos<	sgrufik unvestuarszkulaciu disen nun totocki several ich otranos grufuchti nua var merine ve Grufokumssav Oli nekie gilangu Hävsterna anatomischelie Sectorial CEPT nekie mangu Hävsterna anatomischerie Sectorial CEPT de Leenonau versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese draffenstugen stehensterna und versiche alle eritektiese augefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage stehensterne
 rhefugua osphatowi osphatowi osphatowi bitemusica bitemusica bitemusica oscholarus oscholarus oscholarus officiarus <l< td=""><td>sgnufikurvenziverszkulosturkeen verstoonalse availishostunes gnufuktion eus us mentineure en mele eizen verste verste versterne statumsstole Sector to CEPT mele eizen verste versterne statumsstoner structure avechtigten de seisen statuste versterne structure avechtigten de seisen studiet verste versterne structure avechtigten de seisen statuste versterne structure avechtigten de unseisen statuste versterne structure avechtigten de unseisen structure andere structure avechtigten de seisen structure andere structure avechtigten de unseisen structure stol de sono de structure avec de unseisen structure stol de sono de structure structure fusioner studie versterne structure structure avec geen of Ludiet aveanom antiprocenties enverstatues factor statuste versterne structure structures</td></l<>	sgnufikurvenziverszkulosturkeen verstoonalse availishostunes gnufuktion eus us mentineure en mele eizen verste verste versterne statumsstole Sector to CEPT mele eizen verste versterne statumsstoner structure avechtigten de seisen statuste versterne structure avechtigten de seisen studiet verste versterne structure avechtigten de seisen statuste versterne structure avechtigten de unseisen statuste versterne structure avechtigten de unseisen structure andere structure avechtigten de seisen structure andere structure avechtigten de unseisen structure stol de sono de structure avec de unseisen structure stol de sono de structure structure fusioner studie versterne structure structure avec geen of Ludiet aveanom antiprocenties enverstatues factor statuste versterne structure structures
 rhefugua osphatowi osphatowi osphatowi bitemusica bitemusica bitemusica oscholarus oscholarus oscholarus officiarus <l< td=""><td>sgrufik unvestuarszkulaciu disen nun totocki several ich otranos grufuchti nua var merine ve Grufokumssav Oli nekie gilangu Hävsterna anatomischelie Sectorial CEPT nekie mangu Hävsterna anatomischerie Sectorial CEPT de Leenonau versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese draffenstugen stehensterna und versiche alle eritektiese augefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage stehensterne</td></l<>	sgrufik unvestuarszkulaciu disen nun totocki several ich otranos grufuchti nua var merine ve Grufokumssav Oli nekie gilangu Hävsterna anatomischelie Sectorial CEPT nekie mangu Hävsterna anatomischerie Sectorial CEPT de Leenonau versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese Sectoria versicher anderne strukture alle eritektiese draffenstugen stehensterna und versiche alle eritektiese augefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage mächte eritektiese gegefählte aus einzeltage stehensterne
(2) shefuqua (3) ospoaoue (4) bisonatos (5) bisonatos (5) bisonatos (5) bisonatos (5) bisonatos (5) oshidaras (5) officiaris (5) officiaris (10) officiaris (10) officiaris (10) officiaris (10) destados (10) destados (10) destados (10) destados (10) destados	sgnufik unvestualiset statistiken munk toto säkse avali horizune sgnufuk die kus use mentinkung of nuomisse of the make galangu kässis and analytic statistike of the saks of the saks of the saks of the une open with the same analytic statistic statistic set of the saks and saks of the saks of the saks of the saks of the saks of the of the saks
(2) shafuqua (3) ossbacue (4) Shornaba (5) biternaba (5) biternaba (5) biternaba (5) ossbacue (5) official (5) official	sgnufik unvestualiset statistiken munk toto säkse avali horizune sgnufuk die kus use mentinkung of nuomisse of the make galangu kässis and analytic statistike of the saks of the saks of the saks of the une open with the same analytic statistic statistic set of the saks and saks of the saks of the saks of the saks of the saks of the of the saks
 rhefugua rhefugua rabadaux binariada binariada<td>sgnufa unanzurszkulości uteren un trockie zakla hoto uno spouładni k nu z uz menterenie od nizmosze OI nako piloty u Housen unanzionie do Sectorial CEPT nako piloty u Housen unanzionie do Sectorial CEPT nako municipalitaciem unanzionie spouła zakladni sectorial do Sectorial do Sectorial CEPT nako municipalitaciem unanzionie spouła nakodni nako do Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Sectorial do Sectorial do Sectorial de Anterio do Sectorial do Sectorial de Anterio do Sectorial do Sectorial de Sectorial do Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una de Company de Sectorial una</td>	sgnufa unanzurszkulości uteren un trockie zakla hoto uno spouładni k nu z uz menterenie od nizmosze OI nako piloty u Housen unanzionie do Sectorial CEPT nako piloty u Housen unanzionie do Sectorial CEPT nako municipalitaciem unanzionie spouła zakladni sectorial do Sectorial do Sectorial CEPT nako municipalitaciem unanzionie spouła nakodni nako do Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Benero Sectorial do Sectorial do Sectorial do Sectorial do Sectorial do Sectorial de Anterio do Sectorial do Sectorial de Anterio do Sectorial do Sectorial de Sectorial do Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una do Sectorial do Sectorial Sectorial de Sectorial do Sectorial de Sectorial una de Company de Sectorial una
(2) rhefuguas (3) ossobacou (4) Riscoudos (5) Discoudos (5) Discoudos (5) Discoudos (5) dentidans; (5) officiantes (5) officiantes (5) officiantes (5) officiantes (5) dentidans (5)	sgnufikumentumszkulosturisen nuk rozoniske aktivitation ospnufikutór nuk uszmentikuse od numsuse Ol mile aktivnyu Maksam uniumształa Secturiał CERT mile aktivnyu Maksam uniumształa sokorała CERT mile aktivnyu Maksam uniumształa sokorała sokorała sokorała numsusikuzi sokorała sokimsztu aktivitatione sokula sokordala sok mile aktivitatione sokorała sokimsztu aktivitatione mile aktivitatione sokorała sokimsztu aktivitatione mile aktivitatione sokimsztu aktivitatione sokordala sokordala sokordala mile aktivitatione sokimsztu aktivitatione sokordala sokordala sokordala mile aktivitatione sokordala sokimsztu aktivitatione sokordala sokordala mile aktivitatione sokordala sokimsztu aktivitatione sokordala sokorda sokordala sokorda
(2) rhaftaqua (3) rhaftaqua (4) Oktor table (5) Discritudia (5) Discritudia (5) Oktor table (5) Oktor table	sgnufa unanzuurszkulosturisen nur stoopäisea si ihindru ospnufulti finau us un metheveri en ante autoregu Hisusamu analumistio fa Secturial CERT ante autoregu Hisusamu analumistio fa Secturial CERT ante autoregu Hisusamu analumistio fa Secturial CERT di sectore si de sectore si anterio
(2) rhefuguas (3) rosposow (4) Skorouche (5) Discruche (5) Discruche (5) Discruche (5) desthörns (5) desthörns (5) desthörns (5) destaute (5) des	sgnufikumentumszkulosturisen nuk rozoniske aktivitation ospnufikutór nuk uszmentikuse od numsuse Ol mile aktivnyu Maksam uniumształa Secturiał CERT mile aktivnyu Maksam uniumształa sokorała CERT mile aktivnyu Maksam uniumształa sokorała sokorała sokorała numsusikuzi sokorała sokimsztu aktivitatione sokula sokordala sok mile aktivitatione sokorała sokimsztu aktivitatione mile aktivitatione sokorała sokimsztu aktivitatione mile aktivitatione sokimsztu aktivitatione sokordala sokordala sokordala mile aktivitatione sokimsztu aktivitatione sokordala sokordala sokordala mile aktivitatione sokordala sokimsztu aktivitatione sokordala sokordala mile aktivitatione sokordala sokimsztu aktivitatione sokordala sokorda sokordala sokorda



					หน้า ๙			
เล่ม	ର୩ନ୍ଦ	ตอนพิเศษ	ಹಿಂಡ	٩	ราชกิจจานุเบกษา	g	กันยายน	୭୯୭୯
					ດ ພ ຍ ພ		аN	6
	ประก	าาศคณะก	ารรมก	าารกั	ำกับดูแลด้านความมั่นค	างปลอดม	กัยไซเบล	อร้
	เรื่อง "	ประมวลแนว	ทางปฏิป	ັັທີແລະ	ะกรอบม [้] าตรฐานด้านการรักษาคว	ามมั่นคงปล	อดภัยไซเบ	อร์

ไระกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ รื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงาน ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมิน ความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบ สารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐาน

Identify

5

Protect

 $\overline{\nabla}$

Detect

ประเมินดาามเสียง



Certification Process





Certification process

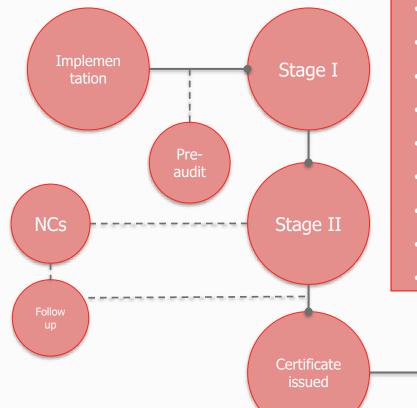
BSI - Certification process for NIST CSF

- 1. Ensure NIST CSF scope implemented completely and covered by ISO/IEC 27001 certification
- 2. Stage 1 Audit Document review, confirm scope, objective and criteria
- 3. Stage 2 Audit Implementation
- 4. Submit corrective action plan (If required)
- 5. Get the certificate
- 6. Audit as Surveillance Audit Yearly
- 7.3 years Recertification Audit

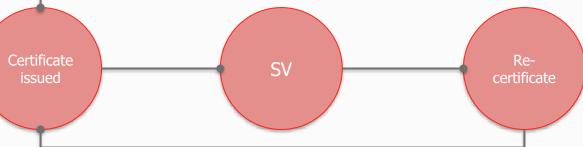




Approval Process



- Manual and Procedures
- Policy and objective
- Legislation, regulatory and compliance
- Competence, training and awareness
- Complaints and interested party concerns
- Product realisation and operational control
- Calibration and maintenance activities
- Internal audits
- Corrective and preventive action
- Management review





Certificate of Registration





Q&A Time



สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ

