



เตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์

# NIST Cybersecurity

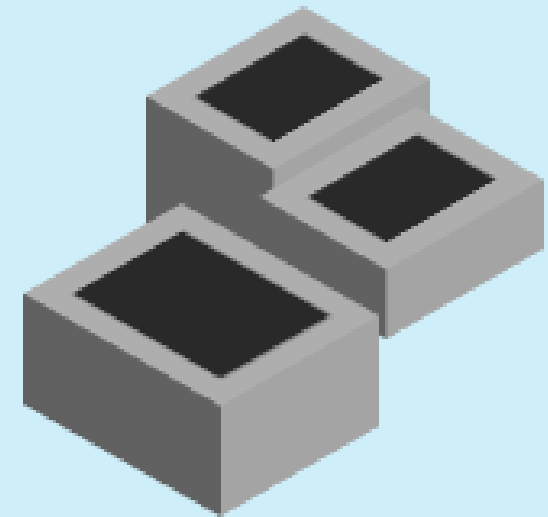
# Framework 2.0

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

- Executive order issued in 2013 by President Obama

- NIST Cybersecurity Framework v1 issued Feb 2014

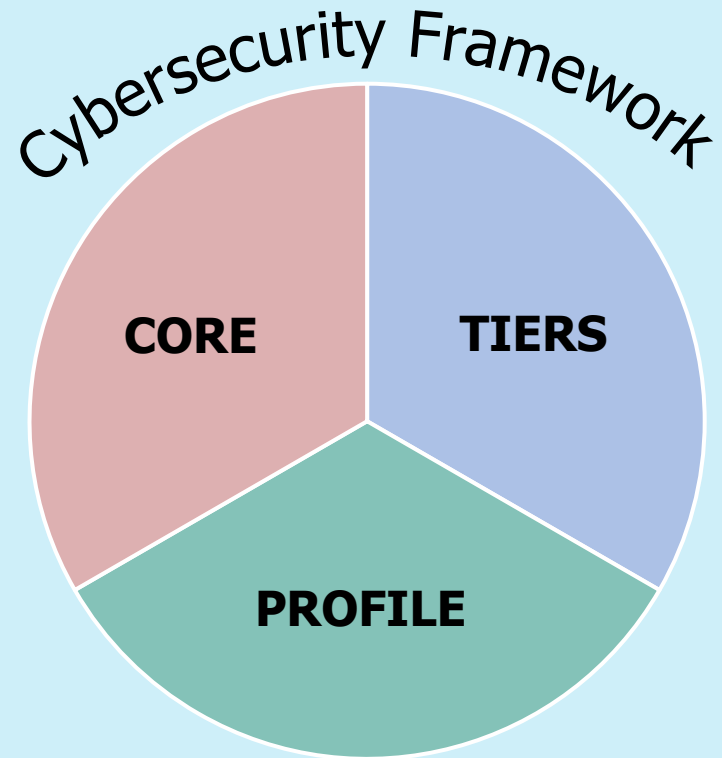
- Updated v2.0 issued February 2024

- Updated v1.1 Issues April 2018

# 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 benefit tools.
- New function “Govern”
  - 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



Check for updates

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

# NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE



NIST Special Publication  
NIST SP 1299

<https://doi.org/10.6028/NIST.SP.1299>  
February 2024

Check for updates

**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

**NIST** NATIONAL CYBERSECURITY CENTER OF EXCELLENCE





# NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide



# NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles





# NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers



U.S. Department of Commerce  
Gina M. Raimondo, Secretary  
National Institute of Standards and Technology  
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication  
**NIST SP 1302 ipd (Initial Public Draft)**  
The public comment period for this draft ends May 3, 2024.  
Please send your comments to [cyberframework@nist.gov](mailto:cyberframework@nist.gov).  
<https://doi.org/10.6028/NIST.SP.1302.ipd>  
February 2024



# NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide



U.S. Department of Commerce  
Gina M. Raimondo, Secretary  
National Institute of Standards and Technology  
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication  
**NIST SP 1303 ipd (Initial Public Draft)**  
<https://doi.org/10.6028/NIST.SP.1303.ipd>  
The public comment period for this draft ends May 3, 2024.  
Please send your comments to [cyberframework@nist.gov](mailto:cyberframework@nist.gov).  
February 2024





# NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*  
National Institute of Standards and Technology  
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

**NIST Special Publication  
NIST SP 1305 ipd (Initial Public Draft)**  
<https://doi.org/10.6028/NIST.SP.1305.ipd>  
The public comment period for this draft ends May 3, 2024.  
Please send your comments to [cyberframework@nist.gov](mailto:cyberframework@nist.gov).  
February 2024



# CSF 2.0 Organization Profile Template

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	CSF Outcome (Function, Category, Subcategory)	CSF Outcome Description	Included in Profile	Rationale	Current Priority	Current Status	Current Policies, Processes, and Procedure	Current Internal Practices	Current Roles and Responsibilities	Current Selected Informative Reference	Current Artifacts and Evidence	Target Priority	Target CSF	Target Policies, Processes, and Procedures	Target Internal Practices	Target Roles and Responsibilities	Target Selected Informative References	Notes
1	GV	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored																
2	GV.OC	The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood																
3	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management																
4	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered																
5	GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed																
6	GV.OC-04	Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated																
7	GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated																
8	GV.RM	The organization's priorities,																





# 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-nd/4.0/>



## 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.





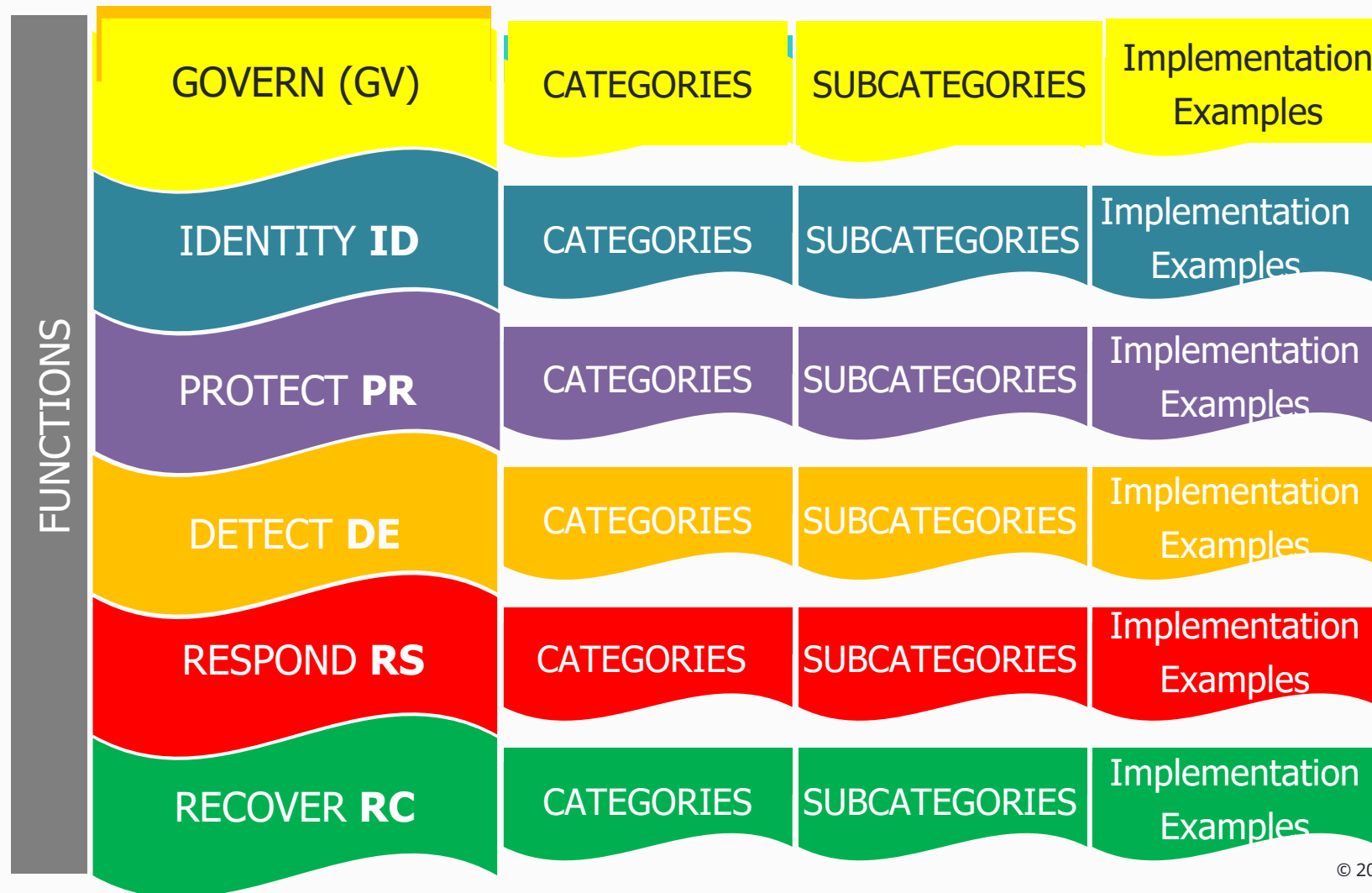
**What is New function -  
Govern**

**What is NIST CSF Version 2  
requirement**

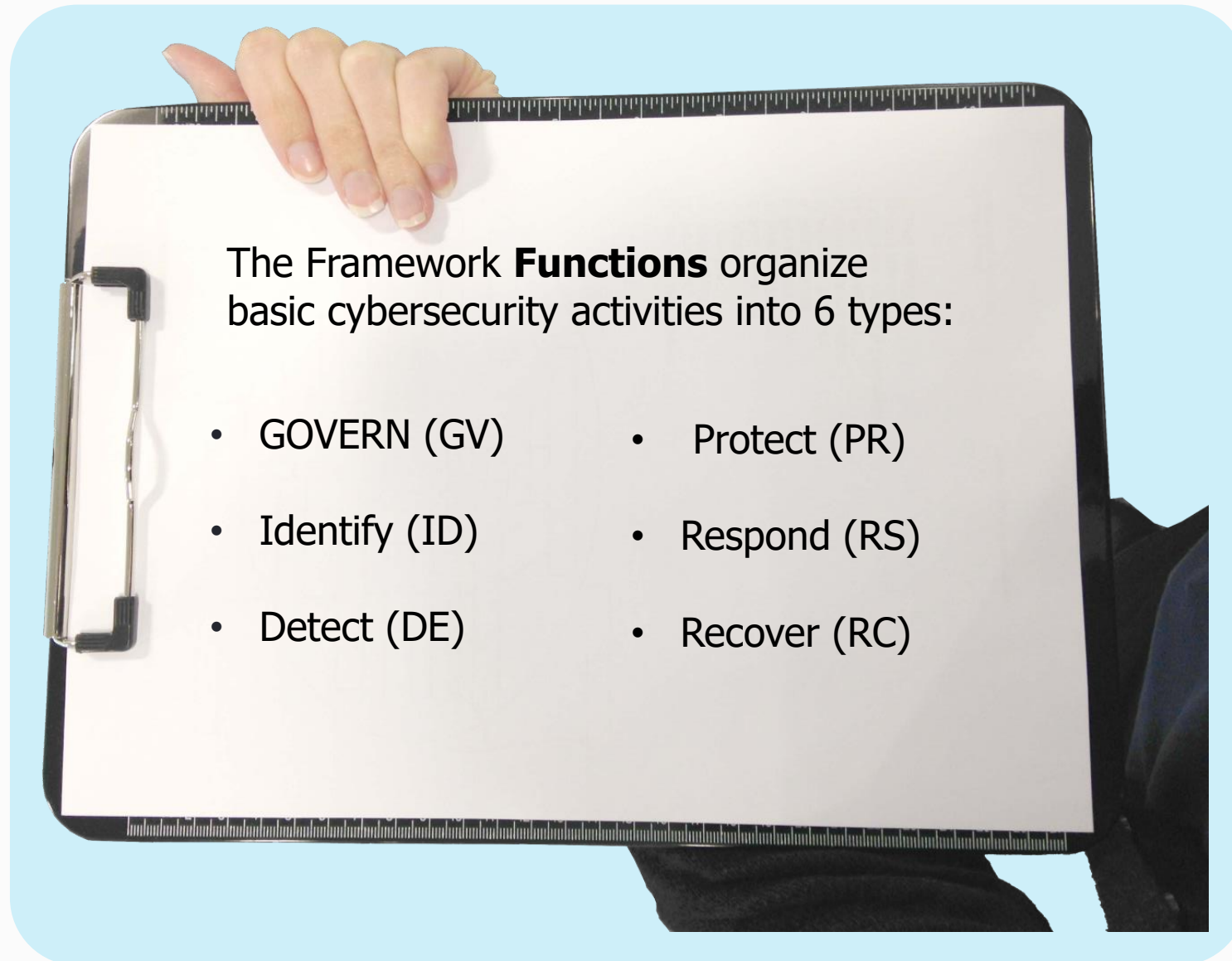


# Framework Core

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**





พระราชบัญญัติ  
การรักษาความมั่นคงปลอดภัยไซเบอร์  
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒

เป็นปีที่ ๔ ในรัชกาลปัจจุบัน



# กฎหมายลำดับรองที่สำคัญ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562



1

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

2

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

3

ประกาศ กมช. เรื่อง  
การทำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีการกิจ  
หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ  
ทางสารสนเทศ และการมอบหมายการควบคุม  
และกำกับดูแล พ.ศ. 2564

4

ประกาศ กกม. เรื่อง  
ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน  
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์  
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐาน  
สำคัญทางสารสนเทศ พ.ศ. 2564

5

ประกาศ กมช. เรื่อง  
การทำหนดระดับความรู้ความชำนาญด้านการ  
รักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้ง  
เป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564

6

ประกาศ กมช. เรื่อง  
ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน  
รับมือ ประเมิน ปรามปรามและระงับภัยคุกคาม  
ทางไซเบอร์แต่ละระดับ พ.ศ. 2564

7

ระเบียบ กกม. ว่าด้วย  
การมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการ  
กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565

8

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

9

ประกาศ กกม. เรื่อง  
หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์  
พ.ศ. 2566

10

ประกาศ สกมช. เรื่อง  
หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน  
และค่าบริการในการดำเนินงาน พ.ศ. 2566

11

ประกาศ กมช. เรื่อง  
มาตรฐานการทำหนดคุณลักษณะ  
ความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล  
หรือระบบสารสนเทศ พ.ศ. 2566

12

ประกาศ กมช. เรื่อง  
มาตรฐานขั้นต่ำของข้อมูลหรือ  
ระบบสารสนเทศ พ.ศ. 2566

13

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

14 (ร่าง)

ประกาศ กมช. เรื่อง  
มาตรการและแนวทางในการยกระดับทักษะ  
ความรู้และความเชี่ยวชาญในด้านการรักษา  
ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ...

15

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

หมายเหตุ : ลำดับที่ 14 อยู่ระหว่างนำเสนอคณะกรรมการเพื่อพิจารณาร่าง ให้ความเห็นชอบและนำเสนอ กมช.





**1** ประกาศ กมช. เรื่อง  
การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษา  
ความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ  
พ.ศ. 2564  
(มีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป)



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้มีการจัดตั้งเมื่อวันที่ 11 สิงหาคม 2564 มีหน้าที่ในการเฝ้าระวัง ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์



**2** ประกาศ กมช. เรื่อง  
ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสาน  
การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์  
สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ  
และการให้บริการหรือให้บริการที่เกี่ยวข้อง  
พ.ศ. 2564  
(มีผลใช้บังคับตั้งแต่วันที่ 23 ส.ค. 65 เป็นต้นไป)

**สาระสำคัญ** เพื่อกำหนดลักษณะ หน้าที่ และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Sectoral CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 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 กรมศุลกากร
5. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญที่มีการให้บริการโดยตรงแก่ประชาชน
6. Thailand Banking Sector CERT (TB-CERT)
7. Thai Capital Market CERT (TCM-CERT)
8. Thailand Telecommunication CERT (TTC-CERT)
9. Health CIRT



**3** ประกาศ กมช. เรื่อง  
การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีการกิจ  
หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ  
ทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล  
พ.ศ. 2564  
(มีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป)

**สาระสำคัญ** เพื่อเป็นการประกาศกำหนดภารกิจหรือบริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งสิ้น 7 ด้าน ปัจจุบันประกาศฯดังกล่าวมี **Regulator 19 หน่วยงาน และ CII 63 หน่วยงาน**



# 4

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

**สาระสำคัญ** กำหนดให้หน่วยของรัฐ หน่วยงานควบคุม หรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ในการจัดทำ**ประมวลแนวทางปฏิบัติ** และ**กรอบมาตรฐาน**ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำ



### ประมวลแนวทางปฏิบัติ

มีองค์ประกอบดังนี้

1. แผนการตรวจสอบฯ
2. การประเมินความเสี่ยงฯ
3. แผนการรับมือภัยคุกคามทางไซเบอร์

### กรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มีองค์ประกอบดังนี้

- (1) การระบุความเสี่ยงที่อาจเกิดขึ้นฯ (Identify)
- (2) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)
- (3) มาตรการตรวจสอบและเฝ้าระวังฯ (Detect)
- (4) มาตรการเผชิญเหตุฯ (Respond)
- (5) มาตรการรักษาและฟื้นฟูความเสียหายฯ (Recover)



# 5

ประกาศ กคช. เรื่อง  
การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคง  
ปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่  
พ.ศ. 2564  
(มีผลใช้บังคับตั้งแต่วันที่ 8 ธ.ค. 64 เป็นต้นไป)

**สาระสำคัญ** เพื่อกำหนดคุณสมบัติและความรู้ความ  
ชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ  
บุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่



ปัจจุบันมีการแต่งตั้ง  
พนักงานเจ้าหน้าที่  
จำนวน  
**65**  
ราย  
ซึ่งครอบคลุมทุก Regulator



# 6

ประกาศ กคช. เรื่อง  
ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ  
ประเมิน ประเมินและระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ  
พ.ศ. 2564  
(มีผลใช้บังคับตั้งแต่วันที่ 12 ธ.ค. 64 เป็นต้นไป)

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

ระดับของภัยคุกคาม  
ทางไซเบอร์

- ระดับวิกฤติ**
  - การโจมตีของ CS ระดับสูงซึ่งส่งผลกระทบต่อระบบที่เป็นวงกว้างทำให้การบริหารและควบคุมระบบ/ไม่สามารถรับมือได้โดยขาดการแจ้งเตือนทันที มีความเสี่ยงที่ภัยคุกคามของ CS นั้นๆ อาจทำให้ระบบ/ระบบที่เกี่ยวข้องทั้งหมดหยุดทำงานเป็นวงกว้าง ระดับประเทศ
  - กระทบต่อความสงบเรียบร้อยของประชาชน/กบฏ/กบฏต่อความมั่นคงของรัฐ อาจทำให้ระบบ/ระบบที่เกี่ยวข้องหยุดทำงานหรือระบบที่เกี่ยวข้องหยุดทำงานโดยสมบูรณ์ หรือระบบที่เกี่ยวข้องหยุดทำงานโดยสมบูรณ์
- ระดับร้ายแรง**
  - ภัยคุกคามทางไซเบอร์ในระดับปานกลางถึงสูง โดยมุ่งโจมตีระบบ/ระบบที่เกี่ยวข้องบางส่วน
  - มีความเสียหายของข้อมูลสารสนเทศหรือข้อมูลที่สำคัญ (ความมั่นคงของรัฐ/ความสงบเรียบร้อยของประชาชน/ความมั่นคงของระบบ/ระบบที่เกี่ยวข้อง)
- ระดับไม่ร้ายแรง**
  - มีความเสี่ยงอย่างมีนัยสำคัญที่ส่งผลกระทบต่อระบบ/ระบบที่เกี่ยวข้องบางส่วน



## 7 ระเบียบ กคท. ว่าด้วย การมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการ กำกับดูแลความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 (มีผลใช้บังคับตั้งแต่วันที่ 27 ธ.ค. 65 เป็นต้นไป)

**สาระสำคัญ** เพื่อให้การดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ทันท่วงทีให้ กคท. จึงมีการมอบอำนาจให้คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (ครร.) พิจารณาสั่งการกรณีเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือระดับวิกฤติ



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

**สาระสำคัญ** เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมทั้งครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ



## 9 ประกาศ กคท. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 (มีผลใช้บังคับตั้งแต่วันที่ 10 พ.ค. 66 เป็นต้นไป)

**สาระสำคัญ** เพื่อกำหนดแนวทางในการแจ้งและรายงานกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ





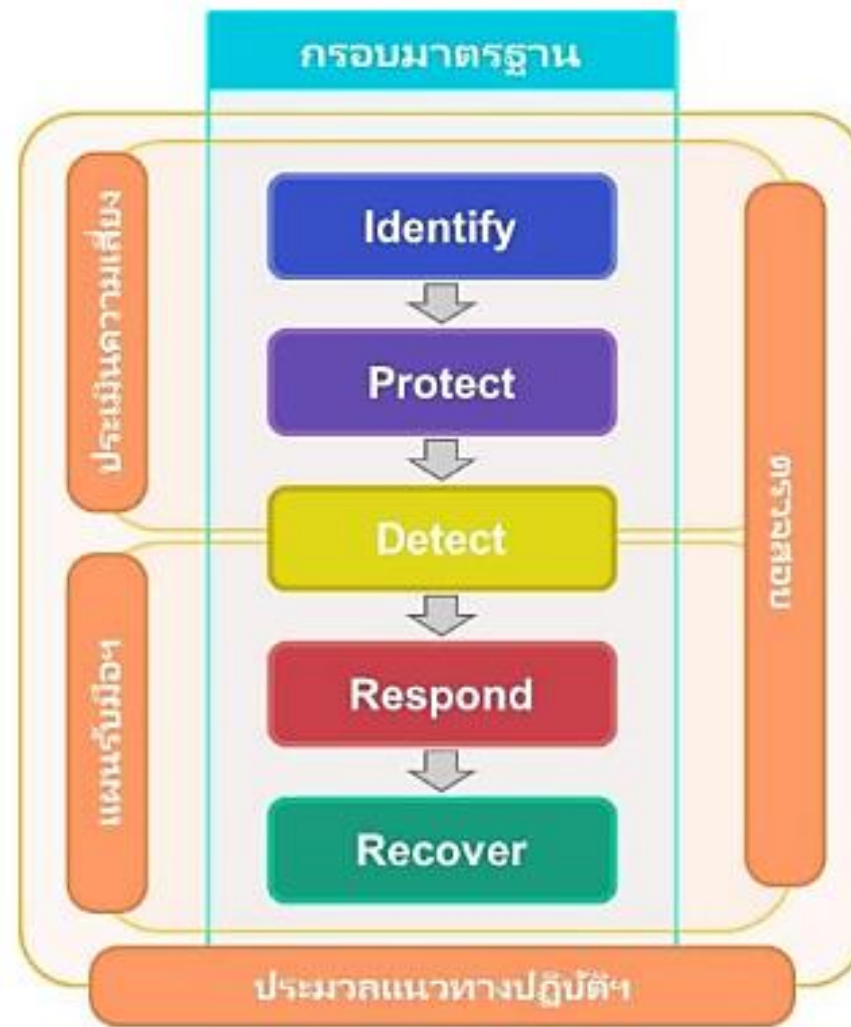


# ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์  
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

//

# Certification Process





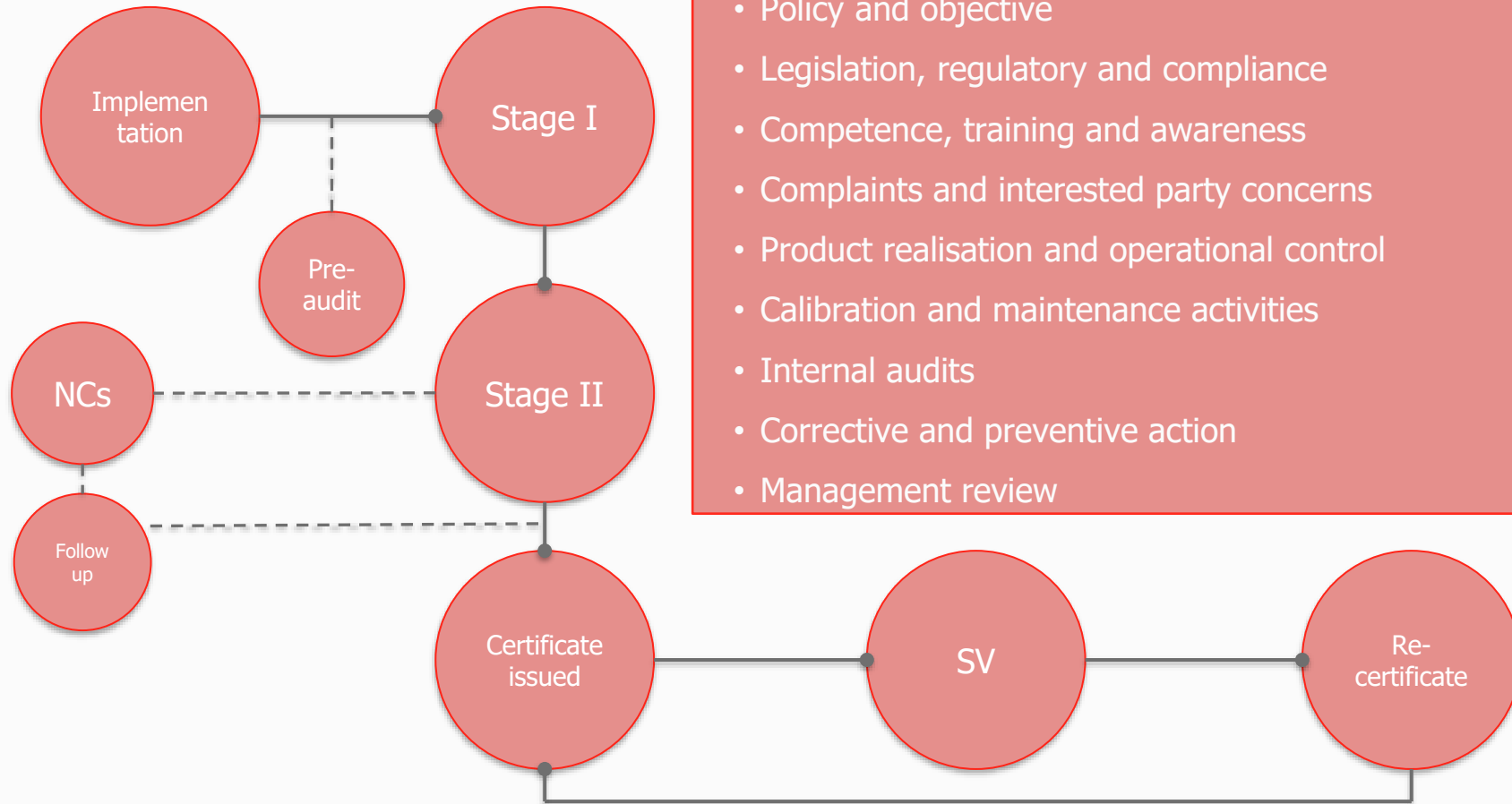
# Certification process

## 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



# // Q&A Time



สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ

