



REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

CYBERSECURITY in the FINANCE SECTOR



2022 1ST PAGBA SEMINAR

Bacolod City
November 23-26, 2022



DICT

NATIONAL CYBERSECURITY PLAN 2022

Various

of

the

country

is

to

be

the

first

01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 01010000 01101100 01100001 01101110 01000011 01111001 01100010 01100101 01110010 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001 01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 01010000 01101100 01100001 01101110 01000011 01111001 01100010 01100101 01110010 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

National Cybersecurity Plan 2022

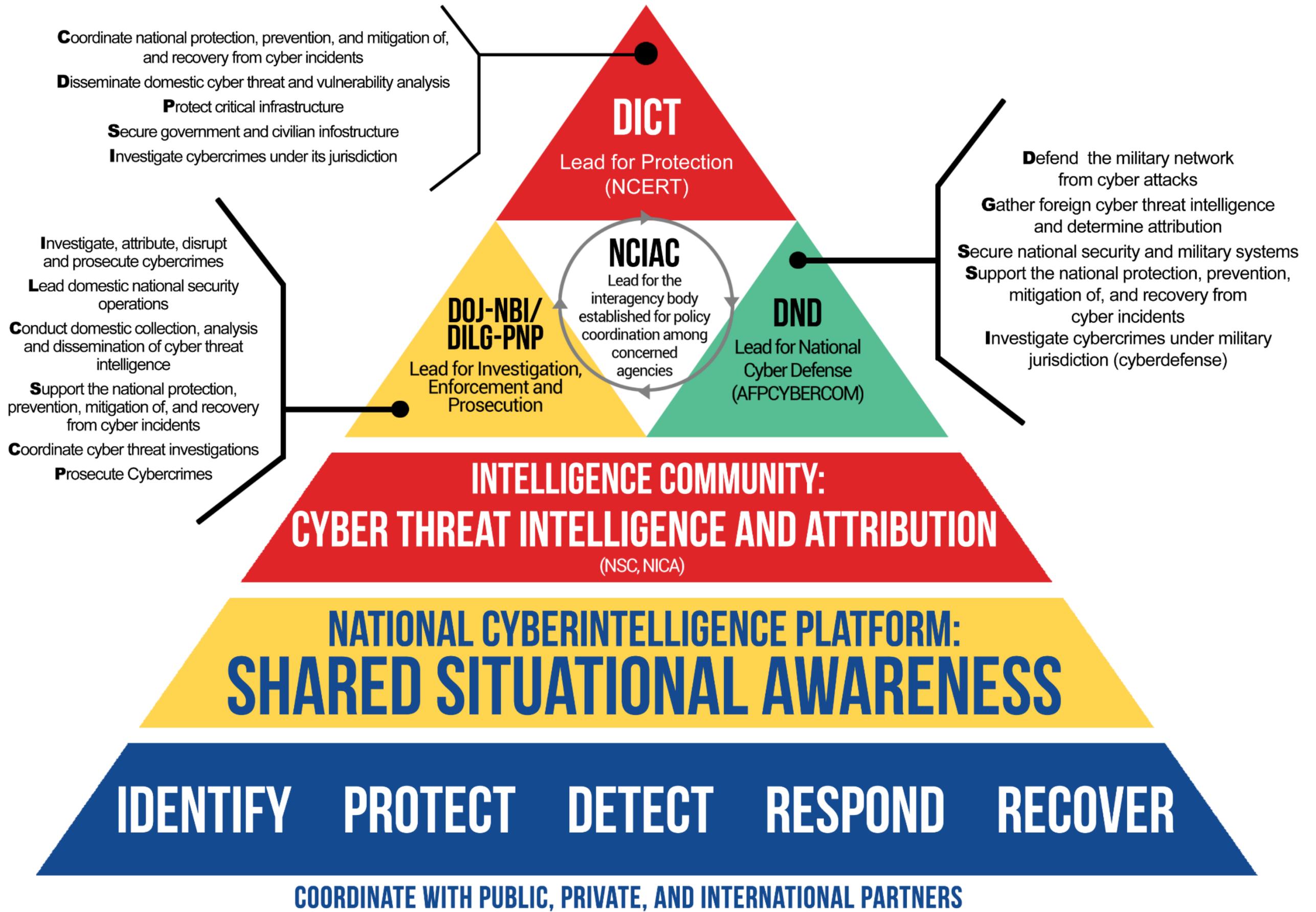
The NCSP 2022 refers to a comprehensive plan of action designed to improve the security and enhance cyber resilience of Philippine infrastructures and services. It is a top-down approach to cybersecurity that contains broad policy statements and establishes a set of national objectives and priorities that should be achieved within a specific timeframe.



4 Key Imperatives of the NCSP 2022

- Protection of Critical Infostructures (CII)
- Protection of Government Networks
- Protection of Businesses and Supply Chains
- Protection of Individuals





Cybersecurity Policies

- Memorandum Circular 005-2017. Prescribing the Policies, Rules and Regulations on the Protection of Critical Infostructure (CII) Stipulated in the National CyberSecurity Plan (NCSP) 2022
- Memorandum Circular 006-2017. Prescribing the Policies, Rules and Regulations on the Protection of Government Agencies Stipulated in the National CyberSecurity Plan (NCSP) 2022
- Memorandum Circular 007-2017. Prescribing the Policies, Rules and Regulations on the Protection of Individuals Stipulated in the National CyberSecurity Plan (NCSP) 2022



Cybersecurity Policies

- Department Circular 003-2020. Supplementing the DICT Memorandum Circular nos. 005, 006 and 007, series of 2017 and policies, rules and regulations on the implementation of the National CyberSecurity Plan 2022
- Department Circular No 006-2020. Guidelines on the Application and Issuance of PNPKI Digital Certificates for External Clients during the State of Public Health Emergency

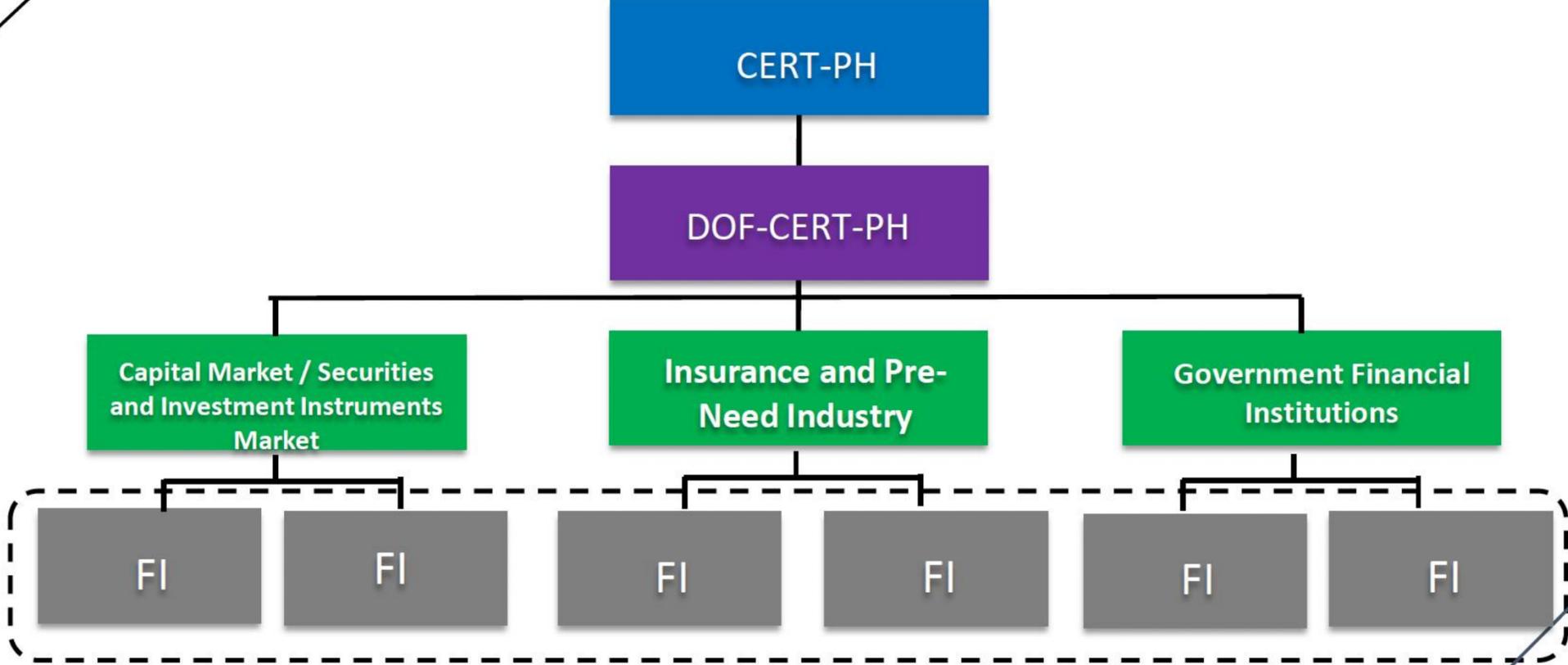


DICT Department Circular 003-2020

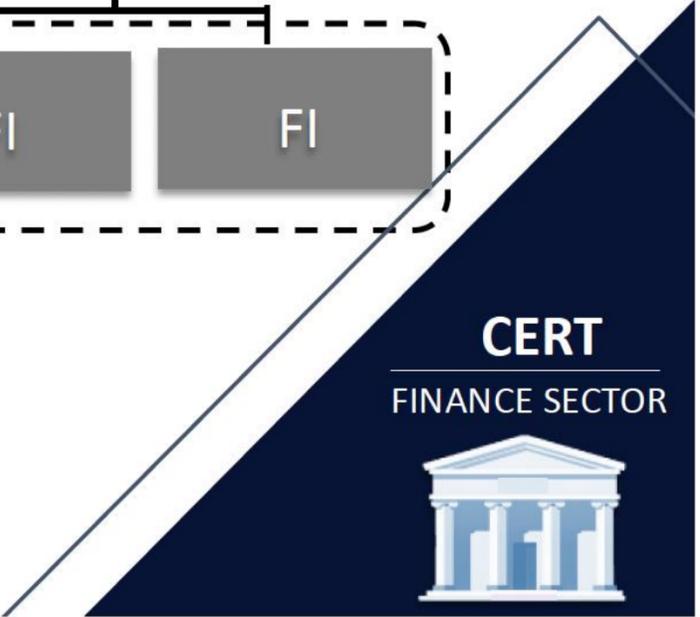
- Sectoral CERT
 - Government & Emergency Services - DICT[MISS]-CERT-PH
 - Business Process Outsourcing - DTI-CERT-PH
 - Healthcare - DOH-CERT-PH
 - Media - PCOO-CERT-PH
 - Banking - BSP-CERT-PH
 - Financial - DOF-CERT-PH
 - Power - DOE-CERT-PH
 - Water - NWRB-CERT-PH
 - Telecommunications - NTC-CERT-PH
 - Transport and Logistics - DOTr-CERT-PH
- Escalation Protocol
- Connection to the National Security Operations Center
- Cybersecurity Training



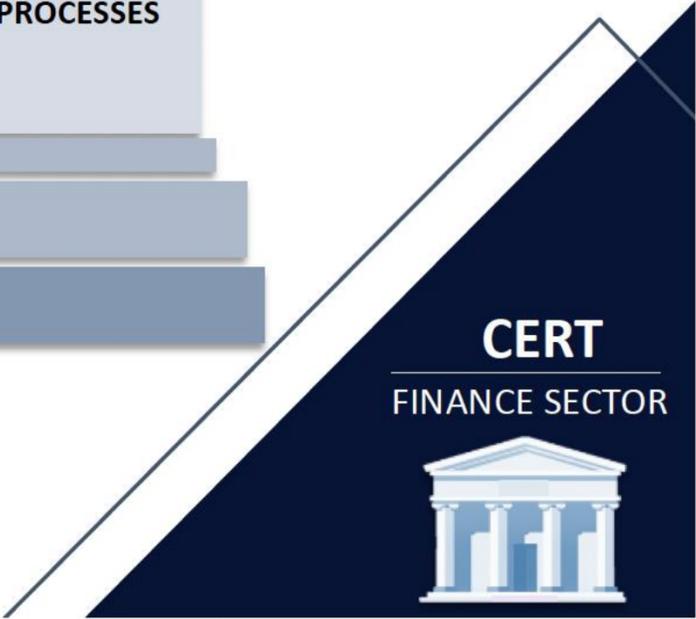
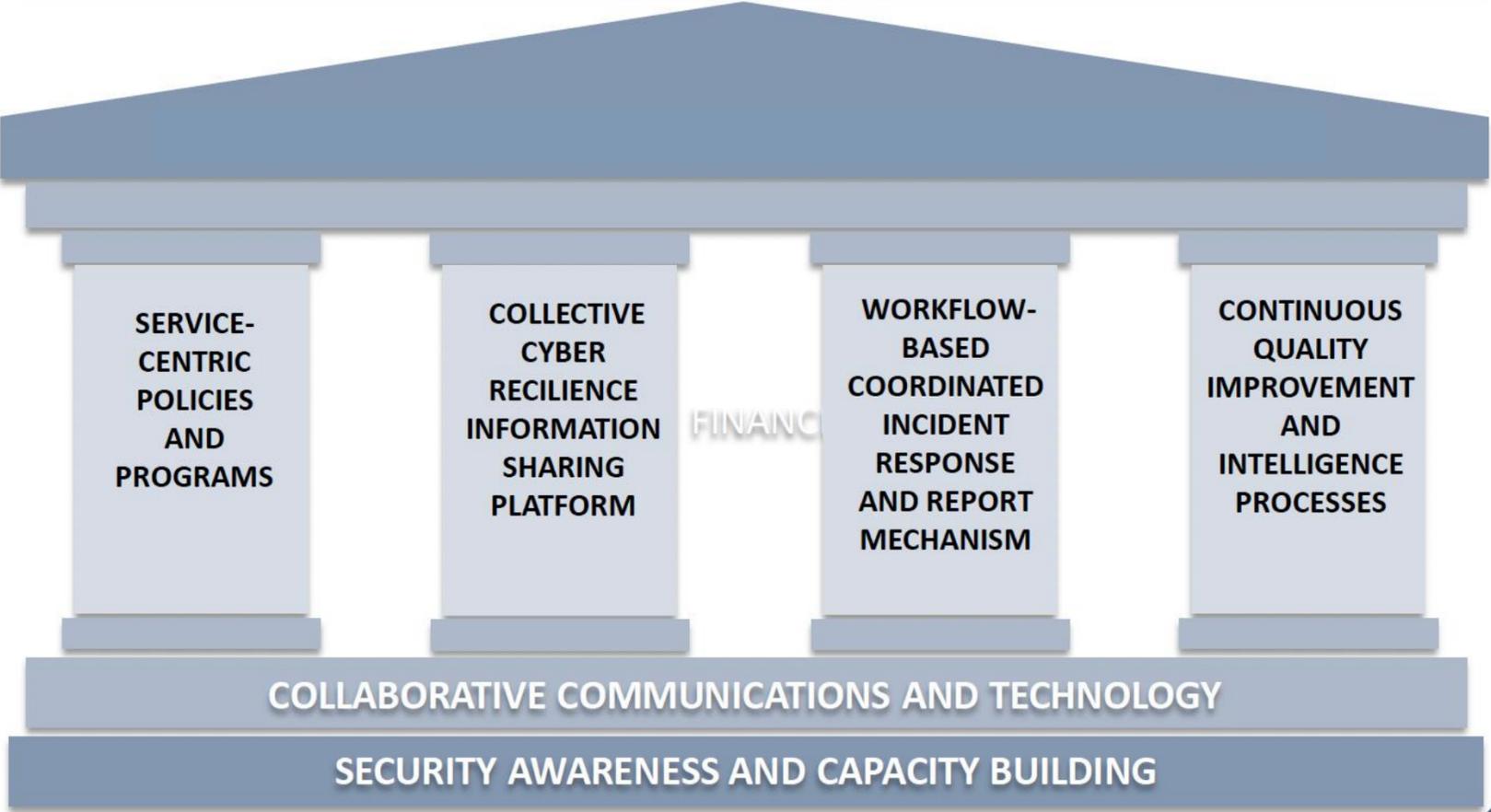
FINANCE SECTOR HIERARCHY OF CERT



LEGEND:
DICT as National CERT
DOF as Lead Sectoral CERT
Sub-sectoral Co-Leads
Financial Institution Organizational CERT

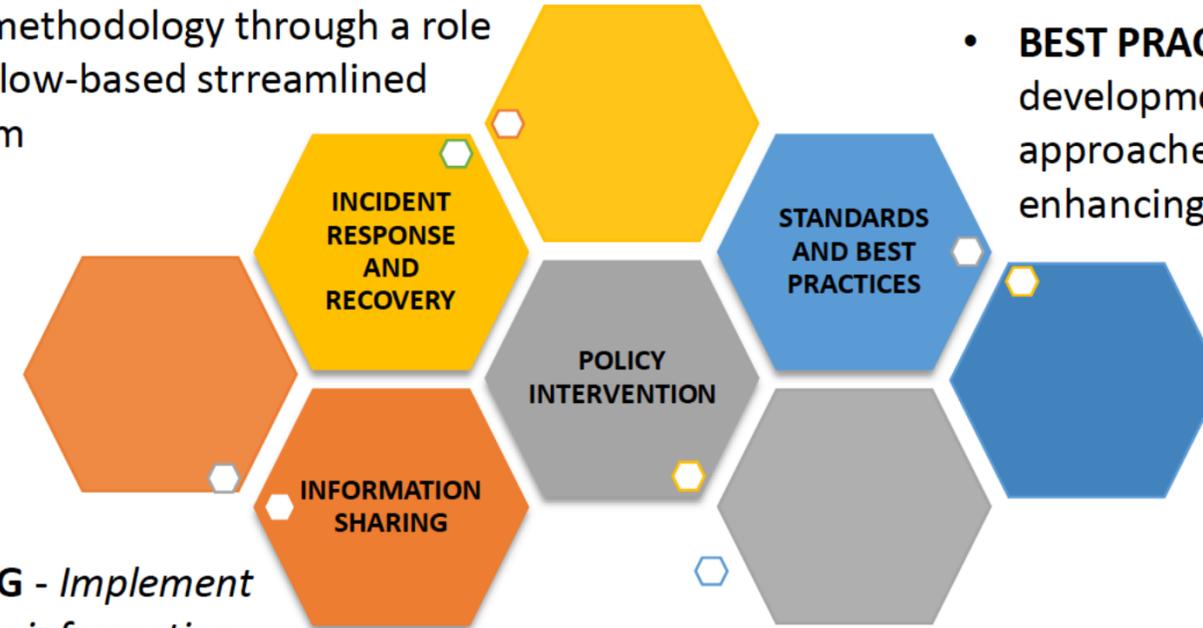


FINANCE SECTOR FRAMEWORK



FINANCE SECTOR STRATEGIC GOALS

- **INCIDENT RESPONSE AND RECOVERY** – Coordinate a responsive incident and recovery methodology through a role and workflow-based streamlined mechanism



- **BEST PRACTICES** – Encourage development and use of common approaches and industry standards for enhancing security and resilience

- **INFORMATION SHARING** - *Implement and maintain a cross-sector information sharing platform for collaboration to establish a single view of actionable information related to cybersecurity and physical threats and vulnerabilities across government and multi-stakeholder financial industries*

- **POLICY INTERVENTION** – *Develop risk-based policy and regulatory initiatives by enhancing critical infrastructure minimizing consequences and employing effective response and recovery*

CERT
FINANCE SECTOR



DOF-CERT-PH ACTION ITEMS

- DEVELOPMENT OF DOF-CERT-PH CYBER RESILIENCY PLAN
- DESIGN A SECTOR-WIDE COORDINATED INCIDENT REPORTING METHODOLOGY
- DEVELOPMENT OF CERT - FINANCIAL SECTOR PORTAL

CERT
FINANCE SECTOR





Angelica I. Sarmiento
Director IV
Sept 28, 2021
Virtual Roundtable for Finance Sector

The Department of Finance (DOF) fully supports the initiative of the Department of Information and Communication Technology (DICT) in the implementation and realization of National Cybersecurity Security Plan 2022. The DOF, being the designated CII Lead CERT for the financial sector, is looking forward to having a comprehensive collaboration with different financial institutions and government agencies to establish a general framework for the constitution of policies and programs to promote operational resilience, risk management, and implement cyber-attack countermeasures. Additionally, this will help the financial sector to have advanced threat intelligence as the financial services in the country move towards digitalization. With this, the DOF appreciates the effort of the DICT Team in building the drive to have optimal cyber resiliency not only in the financial sector but across all industries in the country.

  @CYBERSECgovph /@DICTgovph

 /DICTCybersecurity



Cyber resiliency is a moving target. Staying still is not an option.





REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

Email: oupla@dict.gov.ph
Website: <https://dict.gov.ph>