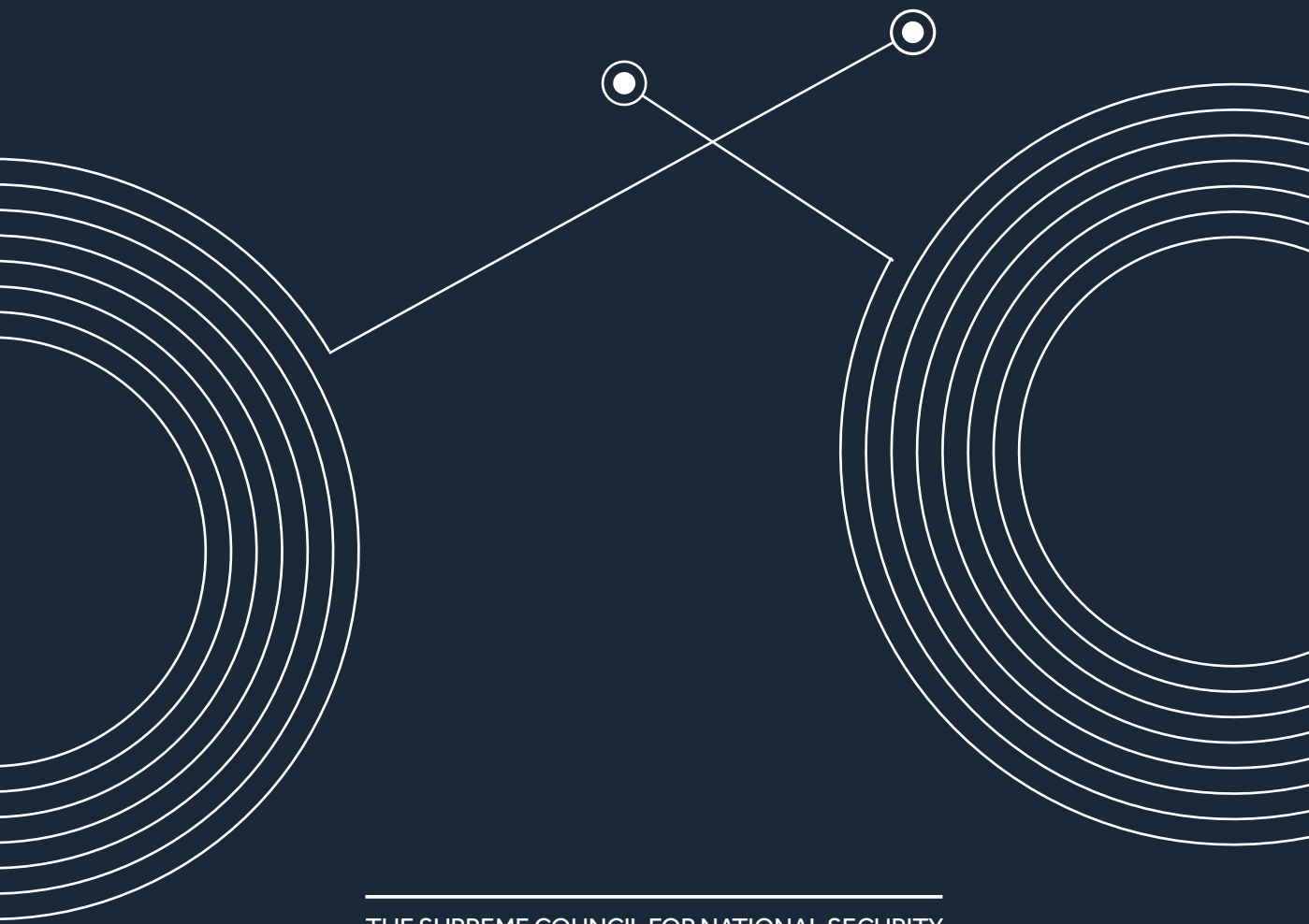
الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

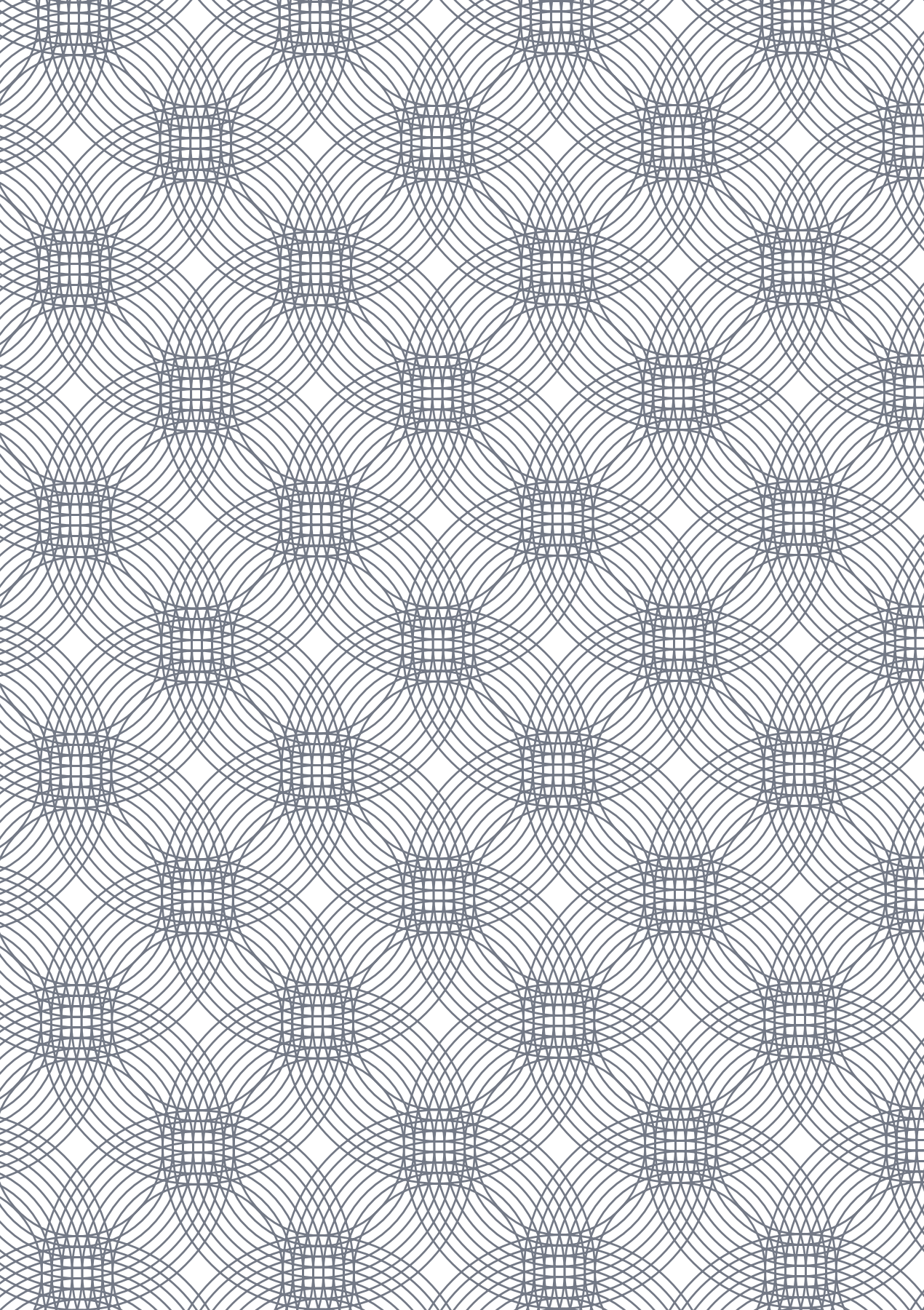
# CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP) POLICY



THE SUPREME COUNCIL FOR NATIONAL SECURITY

# CONTENTS

| | | |
|---|---|---|
| | **FOREWORD** | **1** |
| **1** | **INTRODUCTION** | **3** |
| 1.1 | Purpose of the Document | 5 |
| 1.2 | Importance of Critical Information Infrastructure Protection | 6 |
| 1.3 | Scope of the Policy | 8 |
| **2** | **CIIP PROCESS** | **11** |
| 2.1 | Conduct Sector Baseline | 16 |
| | 2.1.1 Prioritization of Sectors for Implementation | 16 |
| | 2.1.2 Engagement of Stakeholders | 17 |
| | 2.1.3 Identification of Critical National Services | 17 |
| 2.2 | Perform Sector/National Risk Assessment | 18 |
| | 2.2.1 Identification of Supporting Critical Information Infrastructure | 18 |
| | 2.2.2 Threat and Vulnerability Assessment | 19 |
| | 2.2.3 Sector and National Cybersecurity Risk Assessment | 19 |
| 2.3 | Define Sector Plans | 20 |
| | 2.3.1 Identification of CII Cybersecurity Requirements | 20 |
| | 2.3.2 Definition of Sector Plans | 20 |
| 2.4 | Monitor Implementation of Sector Plans | 21 |
| | 2.4.1 Implementation of Sector Plans | 21 |
| | 2.4.2 Monitoring of Implementation | 22 |
| **3** | **UAE CIIP PROGRAM MONITORING** | **25** |
| **4** | **COLLABORATIVE APPROACH TO CIIP** | **29** |
| | **ANNEXES** | **33** |
| Annex 1 | CIIP Supporting Policies | 35 |
| Annex 2 | Key Definitions | 36 |
| Annex 3 | Acronyms | 38 |



## FOREWORD

The increased adoption of Information Technology (IT), electronic communications, and cyberspace – comprising a global network of interdependent information technology infrastructures, telecommunications networks, and computer processing systems – has provided organizations in the UAE with a platform for delivering innovative services and stimulating economic development, as well as facilitating collaboration and communications among individuals. Our dependence on these technologies will continue to grow in the future, and therefore, the UAE Government is committed to the development of a secure national information and communications infrastructure for UAE organizations and individuals to realize the full potential of its benefits, in the face of an evolving set of related cyber threats.

As cyber threats such as hacktivism and cybercrime evolve, so must our efforts to defend against them in a coordinated and systematic manner. To align and direct national cybersecurity efforts, the UAE Government created the National Electronic Security Authority (NESA) to improve our national cybersecurity, and protect our national information and communications infrastructure. As part of this mandate, NESA developed the UAE Information Assurance (IA) Standards to provide requirements for raising the minimum level of IA across all relevant entities in the UAE.

The adoption of these Standards by UAE entities will sustain the benefits of a trusted digital environment for businesses and individuals across the nation. As cybersecurity is the shared responsibility of every organization and individual, collaboration and partnerships between the Government and private sector organizations are key to success. I am confident that our combined efforts will make great strides in achieving the UAE's national cybersecurity objectives and allow our nation's interests to thrive.

**Jassem Bu Ataba Al Zaabi**
Director General

**National Electronic Security Authority**

# CHAPTER 01

## INTRODUCTION

# 1.1
# PURPOSE OF THE DOCUMENT

As the custodian of a safe and secure nation, the UAE government aims to overcome cybersecurity challenges to foster trust and confidence in the UAE's digital and information environment and promote economic growth. In accordance with the Federal Law No. 3 of 2012 (and as amended), the UAE government has therefore created the National Electronic Security Authority (NESA) with the mission to enhance the UAE's national security by improving the protection of its Information and Communication Technologies (ICT) infrastructure through world-class technical and regulatory capabilities, human capital, and increasing public awareness.

The UAE National Cyber Security Strategy (NCSS), outlined and governed by NESA, sets the course for the government's ongoing commitment to protect the national cyberspace. It outlines the strategic areas of focus required to sustain national cyberspace security, specific objectives within each focus area and a roadmap to achieve these goals.

The UAE Critical Information Infrastructure Protection (CIIP) Policy described herein supports the implementation of the NCSS. This document outlines the activities the CIIP program will use to accomplish three key objectives:

- **Identify critical sectors and national services**
- **Identify the information infrastructures supporting critical national services**
- **Raise the security levels of those information infrastructures by implementing mandatory cybersecurity standards and requirements**

# 1.2

## IMPORTANCE OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Critical Information Infrastructure (CII) are physical and virtual information assets that support the carrying-out of a critical function and the delivery of a critical service. They are vital to the functioning of the UAE society and economy, and to providing support services that the UAE government, citizens, and businesses rely upon. While CII often constitutes the main infrastructure of entire economic sectors like telecommunications or financial services, it also offers integral components of more complex infrastructures, such as power supply facilities, air and maritime transport systems, and water facilities.

The digital technologies have enabled increasing efficiencies in the delivery of national critical services. However, as the UAE's dependency on CII has increased, its vulnerabilities to an evolving set of risks have also increased. Such risks are based upon threats that can be natural, man-made, intentional or unintentional, and that can impact the confidentiality, integrity, and availability of information relied upon by governments, citizens, and businesses.

Critical Information Infrastructure Protection is essential, but at the same time addresses inherent challenges. The increase in technology convergence has created a highly complex ICT ecosystem of interdependencies, within and among sectors. This complexity leads to an increased number of stakeholders and a wider scope of management. The unique characteristics of individual sectors present different types of assets, threats, and vulnerabilities requiring sector-specific management. NESA will ensure the deployment of adequate approach and effective collaboration with relevant stakeholders to assist them in their specific activities in this regard.

# 1.3
## SCOPE OF THE POLICY

This Policy is applicable to all information infrastructures, and relative regulators, operators, and relevant participating stakeholders that support critical national services in the following sectors and sub-sectors, as well as any other sector determined by NESA:

| SECTORS | MAIN SUB-SECTORS |
|---|---|
|  CHEMICALS | Basic Chemicals<br>Specialty Chemicals |
|  EMERGENCY SERVICES | Emergency/Rescue Services<br>Law Enforcement |
|  HEALTH | Medical Services<br>Laboratories |
|  NUCLEAR | Reactors<br>Materials<br>Waste |
|  GOVERNMENT (PUBLIC ADMINISTRATION) | National Public Administration<br>Emirate Public Administration<br>Education and Research |

| SECTORS | MAIN SUB-SECTORS |
|---|---|
|  ELECTRICITY & WATER | Generation<br>Transmission<br>Distribution<br>Public Water Supply<br>Public Sewage Disposal |
|  FINANCIAL | Banking<br>Insurance<br>Stock Exchanges<br>Investments |
|  ICT | Information System<br>Telecommunications<br>Satellite<br>Media & Broadcasting |
|  OIL & GAS | Upstream<br>Mid-stream<br>Downstream |
|  TRANSPORT | Terrestrial Transport<br>Air Transport<br>Maritime Transport<br>Logistics and Warehousing |

# CHAPTER 02

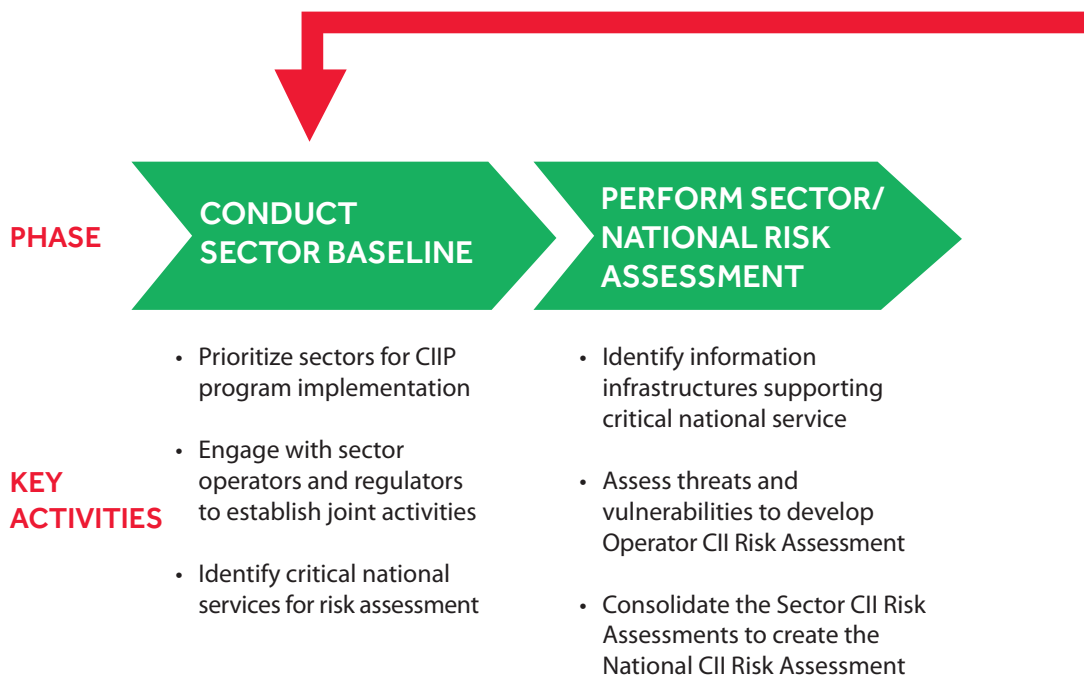
## CIIP PROCESS

# 2.0
# CIIP PROCESS

The process of identifying, assessing, and protecting CII at the sector level represents the core component of the UAE CIIP program. It also focuses on ensuring collaboration between the CII regulators, operators, and other participating stakeholders, while monitoring the progress and performance of the entire program.

The UAE CIIP process has four phases:

**FIGURE 1: UAE CIIP PROCESS PHASES**




The entire process must be repeated on a periodic basis, or whenever it is deemed appropriate by NESA (e.g. a significant change arises) in any critical sector within the scope of the CIIP program.

## DEFINE SECTOR PLANS

- Identify CII Cybersecurity requirements that will reduce the identified risks
- Define Sector Plans to meet the CII Cybersecurity requirements

## MONITOR IMPLEMENTATION OF SECTOR PLANS

- Implement Sector Plans
- Monitor the Sector Plan implementation to ensure requirements are met

Each of the above CIIP process phases is composed of multiple steps involving specific activities to be implemented by relevant stakeholders. This document describes both the activities within each step and the general roles and responsibilities of these stakeholders.

# 2.1
# CONDUCT SECTOR BASELINE

The objective of this phase is to prioritize the implementation of the UAE CIIP Policy across these critical sectors and identify the appropriate regulators (or sector-leader), operators, and relevant participating stakeholders to engage within each critical sector.

## 2.1.1 PRIORITIZATION OF SECTORS FOR IMPLEMENTATION

NESA will implement the CIIP program gradually across the 10 critical sectors in scope, and will prioritize the critical sectors of implementation to facilitate this program expansion. Prioritization will be based upon factors including, but not limited to:

- Political, economic, and social importance of the critical sector
- Estimated maturity of cybersecurity within the critical sector
- Current activity levels of the relevant operators
- The current cyber threat alert level for the critical sector
- Other factors to be determined by NESA and relevant stakeholders

## 2.1.2 ENGAGEMENT OF STAKEHOLDERS

NESA will identify and engage the relevant regulator, operator, and relevant participating stakeholders within each critical sector through CIIP Sector-specific Working Groups, with the aim of fostering collaboration through early dialogue and coordinating to effectively implement CIIP process activities.

NESA will engage with the appropriate sector regulator for each critical sector. In some cases (e.g. absence of regulatory body) NESA may assign to another proper entity relevant appropriate responsibilities and tasks that would normally be assigned to the sector regulator in this regard.

NESA will then, in collaboration with the sector regulator, identify or update the operators and relevant stakeholders within each critical sector to participate in the Sector-specific Working Group. The UAE CIIP Governance Model outlines the organization and mandate of the Sector-specific Working Groups and the process NESA and the regulators will use to identify members.

## 2.1.3 IDENTIFICATION OF CRITICAL NATIONAL SERVICES

In collaboration with sector regulators and operators, NESA will identify critical national services within each critical sector.

To this end, the working group of each sector will identify the taxonomy of services it supports on a national level. The UAE National Risk Management framework defines the criteria that all sectors will use to evaluate the impact of a disruption of such services on a national scale and the threshold indices of a critical national service level.

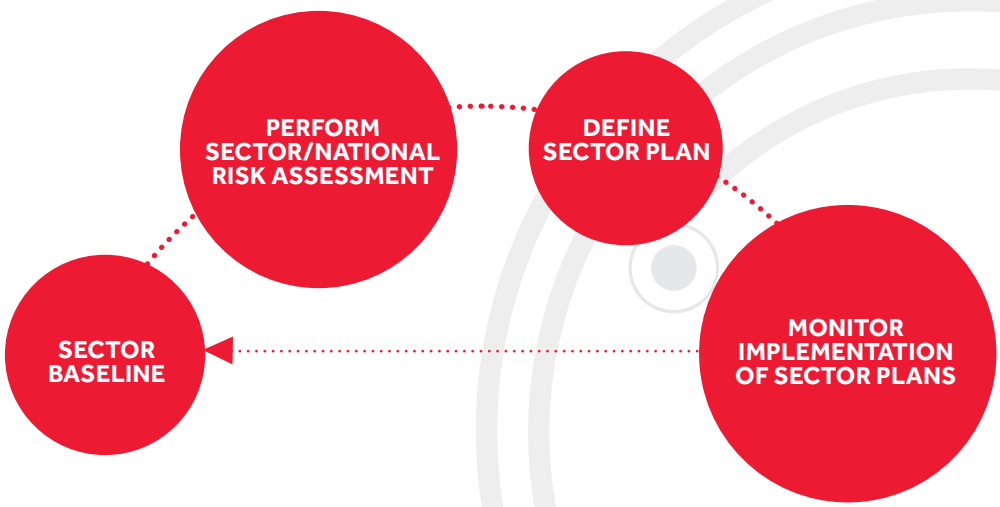
NESA will approve the consolidated list of UAE-critical national services across all sectors.

# 2.2

# PERFORM SECTOR/NATIONAL RISK ASSESSMENT

The objective of Sector/National Risk Assessment is to identify and analyze the threats, consequences, and vulnerabilities surrounding Critical National Services and to prioritize the allocation of resources accordingly. The UAE National Risk Management framework outlines the process for identifying CII, respective owners/operators and risk levels, using a service-oriented approach.

**FIGURE 2: CIIP PROCESS PHASES**




## 2.2.1 IDENTIFICATION OF SUPPORTING CRITICAL INFORMATION INFRASTRUCTURE

The sector working groups will identify the information infrastructure assets that support the delivery of each critical national service (or function) and will determine which elements of that infrastructure, if disrupted, compromised or breached, could negatively affect the national service. These assets will be recognized as part of the UAE Critical Information Infrastructure, and their owners/operators will be designated as CII Operators.

NESA will approve the final list of CII and CII Operators.

## 2.2.2 THREAT AND VULNERABILITY ASSESSMENT

The UAE National Risk Management framework outlines the following steps that CII Operators must perform for each identified CII under their management:

### THREAT ASSESSMENT

Identify potential causes of unwanted incidents that could result in harm to CII.

### VULNERABILITY ASSESSMENT

Evaluate CII weaknesses that could be exploited by one or more threats, and the likelihood of such occurrence in consideration of security controls already in place.

### CONSOLIDATION

Combine the output of the threat and vulnerability assessments with the service impact analysis defined in the National Risk Management framework, to develop an Operator Cybersecurity Risk Assessment for a specific CII.

NESA, in collaboration with the relevant sector regulator, will provide advice and support to CII Operators and relevant stakeholders to help conduct threat and vulnerability assessments and to develop the Operator CII Risk Assessment; the Operators will then submit this to the sector regulator.

## 2.2.3 SECTOR AND NATIONAL CYBERSECURITY RISK ASSESSMENT

Each sector regulator (or designated entity/sector leader) will consolidate the Operator CII Risk Assessments from the Operators within their respective sectors to create a Sector CII Risk Assessment. NESA will provide the necessary advice and support to sector regulators to perform this activity. The sector regulator will then review the Sector CII Risk Assessment together with NESA to identify the highest levels of systemic risk within each sector, and significant risks that could emerge within any individual Operator. NESA will also consolidate the Sector CII Risk Assessments to create the National CII Risk Assessment to identify the highest levels of risk across all sectors, thereby providing a credible basis for prioritizing resources in the interest of national security.

# 2.3
# DEFINE SECTOR PLANS

Sector Plans outline the actions necessary to address the highest levels of risk identified in the Sector and National Risk Assessments.

## 2.3.1 IDENTIFICATION OF CII CYBERSECURITY REQUIREMENTS

In collaboration with sector regulators and CII Operators, NESA will establish mandatory CII Cybersecurity (Protection) Requirements for CII Operators to institute within each sector, and to reduce the risks identified in the Sector and National Risk Assessments. These may include Sector-specific UAE Standards that are applicable to all CII Operators in a sector, as well as entity-specific requirements designed for a single CII Operator.

## 2.3.2 DEFINITION OF SECTOR PLANS

For each of the 10 critical sectors, the regulator (in collaboration with NESA and relevant CII Operators) will prepare a Sector Plan that outlines high level activities, responsible entities and associated timelines for meeting CII Cybersecurity Requirements outlined for their sector. The activities identified in the Sector Plan would target either CII Operators as well as additional identified entities.

NESA will review and approve the Sector Plans before their formal release and ensure coordination and appropriate harmonization between the different Sector Plans at the national level.

Each CII Operator will explain to the regulator (and if required to NESA) its plan to meet the applicable requirements within the timelines specific to the Sector Plan. NESA will approve the CII Operators' plans to meet Sector Plan requirements.

# 2.4 MONITOR IMPLEMENTATION OF SECTOR PLANS

In collaboration with sector regulators (or designated entities/sector leader), NESA will monitor the implementation of Sector Plans to ensure CII Operators are meeting the National CII Cybersecurity Requirements applicable to them.

## 2.4.1 IMPLEMENTATION OF SECTOR PLANS

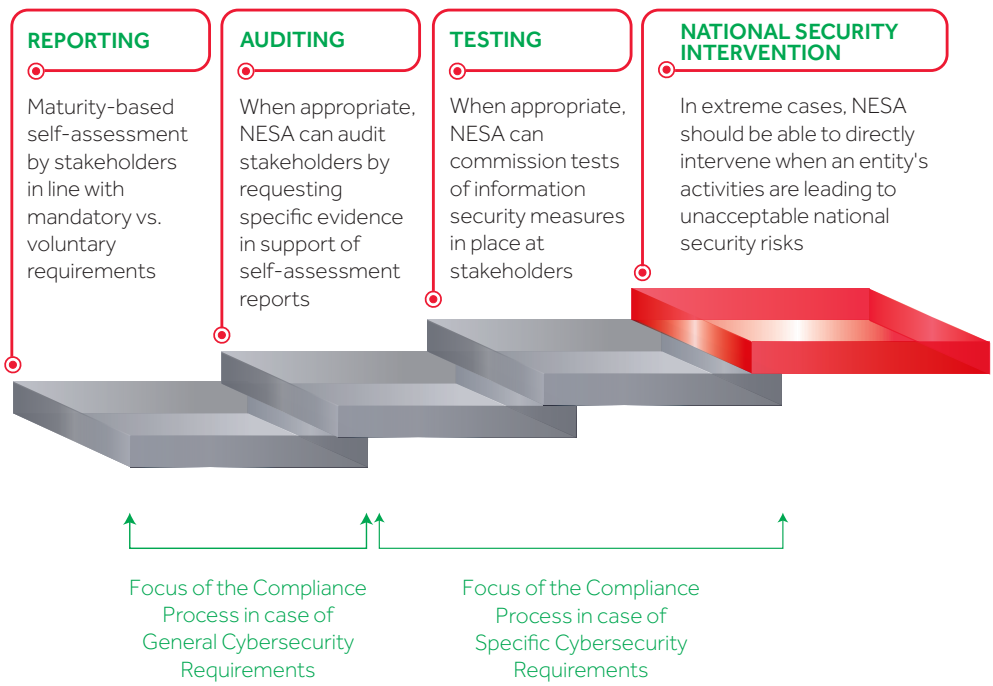
Each CII Operator will meet its applicable requirements within the Sector Plan by executing its approved plan.

## 2.4.2 MONITORING OF IMPLEMENTATION

In collaboration with regulators, NESA will routinely verify that the requirements of the Sector Plan are being implemented by CII Operators. To facilitate this, each CII Operator will periodically update the relevant regulator and NESA on the progress of the implementation. The Sector Plan will define the frequency and content of the CII Operator reporting. Each regulator will consolidate individual CII Operator reports into a Sector CIIP Status Update Report to be submitted to NESA.

The UAE CIIP Governance Model outlines the details for each of the four levels NESA will use to monitor CII Operator implementation across all aspects of the Sector Plans:

## FIGURE 3: ESCALATION OF COMPLIANCE PROCESS




The UAE CIIP Governance Model outlines the process under which NESA may choose to advance the level of implementation monitoring within a specific CII Operator or sector.

# CHAPTER 03

## UAE CIIP PROGRAM MONITORING

# 3.0
# UAE CIIP PROGRAM MONITORING

While monitoring, in collaboration with sector regulators, the implementation of Sector Plans, NESA will also observe the overall UAE CIIP program to measure results, identify potential issues, and promote improvement actions. The UAE CIIP Governance Model outlines a set of metrics to measure three key aspects of the UAE CIIP program:

## IMPLEMENTATION PROGRESS

This measures the progress of implementation of all phases of the CIIP process and highlights variance to original plans, to establish remedial actions.

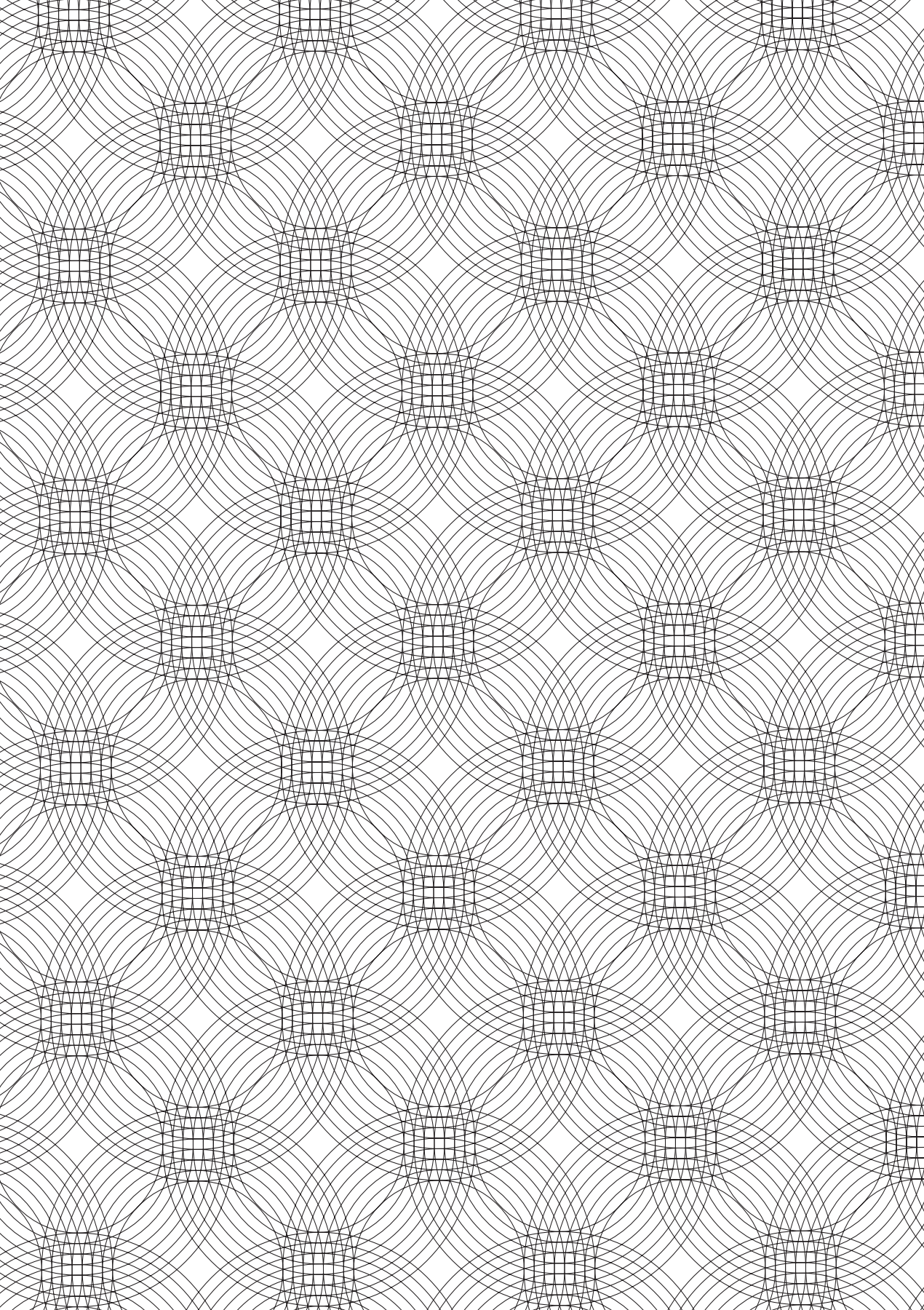
## EFFECTIVENESS

This measures how the CIIP program improves the security of CII in the UAE.

## IMPACT

This measures the impact on the business or mission, attained through the CIIP program.

Regulators and CII Operators will provide NESA with the information needed to update these metrics.



# CHAPTER 04

## COLLABORATIVE APPROACH TO CIIP

# 4.0
# COLLABORATIVE APPROACH TO CIIP

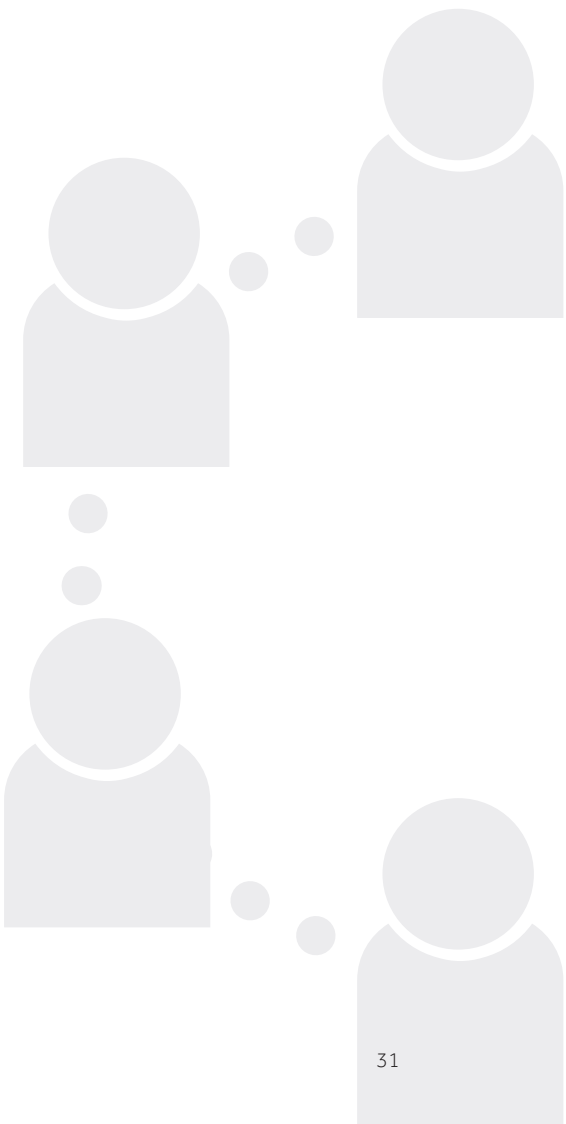
NESA will foster a collaborative working environment with the sector regulators, CII Operators and other relevant stakeholders to facilitate successful implementation of the CIIP program. This collaborative approach will focus on tangible improvements in the protection of CII within a reasonable timeframe. NESA will mandate specific actions when necessary, to progress toward a higher level of cybersecurity in the UAE CII.

The UAE CIIP Governance Model outlines how all CIIP stakeholders will interact through national as well as Sector-specific CIIP Working Groups.

The Working Groups will help NESA and relevant stakeholders to:

- **Shape sector-specific and national CIIP planning activities**
- **Implement activities within the CIIP process phases**
- **Monitor the implementation of the CIIP process within the critical sectors and suggest corrective actions as needed**

The UAE National Information-Sharing framework also outlines the requirements for the UAE national information-sharing capability to support the Working Groups' activities, while protecting the sensitive nature of information shared between potential competitors.



# ANNEXES

# ANNEX 1

## CIIP SUPPORTING POLICIES

| CIIP Program Component | Supporting Policy/Mechanism |
|---|---|
| **CIIP PROCESS** | • UAE CIIP Governance Model<br>• UAE National Risk Management framework |
| **PROGRAM MONITORING** | • UAE CIIP Governance Model |
| **COLLABORATION ON CIIP AND WORKING GROUPS** | • UAE CIIP Governance Model<br>• UAE National Information-Sharing Policy |

# ANNEX 2

## KEY DEFINITIONS

| TERM | DEFINITION |
|---|---|
| CIIP PROGRAM | National level plan developed by NESA comprising key initiatives and actions to enhance the preparedness and response to national cyber incidents targeting the security of the nation's Critical Information Infrastructure. |
| CRITICAL INFORMATION INFRASTRUCTURE | All information assets that support carrying out of a critical function and the delivery of a critical service. |
| CRITICAL INFORMATION INFRASTRUCTURE OPERATOR | An entity responsible for the investments in, and/or day-to-day operation of, a particular critical information infrastructure. |
| CRITICAL SECTOR | A sector identified at the national level that provides critical service(s). |
| CRITICAL FUNCTIONS | Sets of processes that are essential to produce, provide, and maintain critical services and products. |
| CRITICAL SERVICE[1] | Vital service, the disruption or destruction of which may have a debilitating impact on the national security, economy, society, or any combination of these. |
| INFORMATION ASSET | A physical or virtual asset of ICT systems such as data, systems, facilities, network, and computers. |
| INFORMATION INFRASTRUCTURE | The entirety of information assets, both physical and virtual, that are part of a given infrastructure. |
| INFORMATION SHARING CAPABILITY | A set policies, systems, processes, and organizational roles needed to share information based on established requirements. |
| REGULATOR | A government body that sets regulations and monitors compliance and behavior of regulated entities in a particular sector (or market). |
| SECTOR PLAN | A detailed plan developed by the sector regulator and approved by NESA outlining the actions, responsible entities and timelines necessary to address the highest levels of risk identified in the Sector/ National Risk Assessments and guide implementation of related CII Cybersecurity and Protection Requirements. |

| | |
|---|---|
| SECTOR-SPECIFIC CIIP WORKING GROUP | A sector-specific governance body, co-chaired by NESA and sector regulator (sector leader or representative), and compromising NESA, sector regulator, operators and other stakeholders to foster sector collaboration and support sector planning, implementation, and monitoring activities to elevate Critical Information Infrastructure Protection. |
| NATIONAL CIIP WORKING GROUP | A cross-sector governance body, chaired by NESA and compromising NESA, sector regulators (sector leaders or representatives), and other stakeholders to foster sector collaboration and support national/ cross-sector planning, implementation, and monitoring activities to elevate Critical Information Infrastructure Protection. |

[1]Detailed criteria used to define a critical service will be outlined in phase one of the UAE CIIP process.

# ANNEX 3

## ACRONYMS

| | |
|---|---|
| **CII** | CRITICAL INFORMATION INFRASTRUCTURE |
| **CIIP** | CRITICAL INFORMATION INFRASTRUCTURE PROTECTION |
| **ICT** | INFORMATION AND COMMUNICATION TECHNOLOGIES |
| **NESA** | NATIONAL ELECTRONIC SECURITY AUTHORITY |
| **NCSS** | NATIONAL CYBER SECURITY STRATEGY |