# Cybersecurity Industry Development Strategic Maturity Model (CIDSMM)

The ITU Arab Regional Cyber Security Center (ITU-ARCC), in partnership with Huawei, launched a new programme to help strengthen the cybersecurity industry in the Arab and Islamic Titled the '**Cybersecurity Industry Development Strategy Maturity Module (CIDSMM)**,' the programme provides a comprehensive guide for regulatory authorities, industry stakeholders, and academic researchers to assess and improve their cybersecurity capabilities.

The first of its kind in the region and the world, the programme is designed specifically for the Arab and Islamic region's cybersecurity industry. The programme is one of the key outcomes of a partnership between ITU-ARCC and Huawei that was established in May 2022 to promote knowledge transfer, capacity building, and collaboration in the Arab world's cybersecurity sector. By implementing this programme, the ITU-ARCC aims to create a vibrant Arab and

Islamic cybersecurity ecosystem where results and action plans can be shared as a success case stories for adaption by other Arab nations, thereby promoting success and alignment and reducing opportunity cost of failures. It will also provide pillars of collaboration via a public-private partnership model for practical academic research and innovation in cybersecurity, fostering regional digital talents to bridge the digital divide and uplift the regional cybersecurity industry maturity as a whole.

The ITU-ARCC believes that cybersecurity is a shared responsibility that requires a team effort from all stakeholders. Public-private partnerships are essential to identify risks, prevent cyber-attacks, and protect data and assets. Such partnerships enable information sharing, joint development of cybersecurity solutions, and adoption of best practices. By leveraging the strengths of both sectors, governments and businesses can improve their defense capabilities, proactively detect and respond to threats, and ensure the overall security of critical infrastructures

## Program Objectives:

The assessment programme aims to provide the following:

1. A guideline for measuring and enhancing the cybersecurity maturity of various entities involved in the digital ecosystem, such as digital infrastructure protection, data security, cloud computing security, emerging technology, and telecommunication security, among others.

2. Provides accurate and effective information to support developing a long-term cybersecurity Industry strategy.

3. Helps to identify best practices from other countries to summarize lessons learned for self-improvement.

4. Provides a national baseline for building cybersecurity capacity.

5. Drives demand for cybersecurity-related services, products and services, stimulating the digital economy.

## Foundational Characteristics Shaping the Comprehensive Program

We summarized and generalized the good practices of each from existing cybersecurity assessment models, and synthesized the objectives of this project to arrive at the following:

**Structure**

### Category-Element-Aspect-Indicator-Checklist

The **five-layer** structure is the basis for the development of this Program, and the division and disassembly of each layer makes the Program more **specific** and **comprehensive**.

**Coverage**

### Generic and Scenario-based Assessment

Both **generic and scenario-specific** elements are used as part of the Program, aiming to address the customization for the increasingly changing cybersecurity environment

**Questionnaire Granularity Design**

### Binary Answer with Evidence Collection

**Binary** responses are used to determine if the indicator requirements are satisfied in the checklist. And checklists are with **samples of materials** that can be provided as **supporting documentation** for the indicators.

**Assessment Method**

### Self-assessment and Cooperation

**Flexible** assessment methods incorporating **self-assessment** and **cooperation**, combined with easy-to-understand checklists, increase the **flexibility** of Program assessments.

**Result Presentation**

### Maturity Level, Heatmap and Radar Chart

The Program provides a more **intuitive representation** of maturity level results through the three charts mentioned above, which **assist in making decisions**, which is a rare representation of existing models in the market.

## Introduction to Category - Summary

The categories CIDSMM include all assessment content of these 5 industry-renowned models

| CIDSMM Categories |
|---|
| **Category 1. Policy and Strategy** |
| **Definition:** This category explores the national capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience while maintaining the benefits of cyberspace vital for government, international business, and society. |
| **Category 2. Legal and Regulatory** |
| **Definition:** This category refers to the capacity of the government to develop and enact national legislation directly or indirectly related to cybersecurity, including primarily the capacity of law enforcement, prosecution, regulatory agencies, and courts. |
| **Category 3. Standard, Organization and Technology** |
| **Definition:** This category examines the development and implementation of cybersecurity standards and best practices, the establishment of cybersecurity agencies and mechanisms, as well as the implementation of processes and technical controls in order to reduce cybersecurity risks. |
| **Category 4. Culture and Knowledge** |
| **Definition:** This category explores the creation of a strong culture of cybersecurity for the population, the public and private sectors, which will lead to increased awareness of cybersecurity, the development of professionals, and the accumulation of research outcomes in the field of cybersecurity. |
| **Category 5. Commercial Gain and Cooperation** |
| **Definition:** This category examines the growth and development of the cybersecurity industry, as well as the multi-dimensional cooperation approach of government organizations, public welfare institutions, and enterprises. |