Sectoral Cybersecurity Maturity Model

Public Consultation Draft - Version 1.0 - June 2023

DIGITAL DEVELOPMENT PARTNERSHIP
Cybersecurity MULTI-DONOR TRUST FUND
Administered by WORLD BANK GROUP
TEL AVIV UNIVERSITY Pursuing the Unknown

Table of Contents

ACRONYMS AND ABBREVIATIONS

Acronym	Term
BCEAO	Central Bank of West African States
CCB	Cybersecurity Capacity Building
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIRT	Computer Incident Response Team
CMM	Cyber Maturity Model
CSIRT	Computer Security Incident Response Team
EBRD	European Bank for Reconstruction and Development
GFCE	Global Forum on Cyber Expertise
GCSCC	Global Cyber Security Capacity Centre (Oxford University)
ICT	Information and Communication Technology
IDB	Inter-American Development Bank
INCD	Israel National Cyber Directorate
ISAC	Information Sharing and Analysis Center
ISO	International Standard Organisation
ITU	International Telecommunication Union
LoA	Layer of Assessment
MDA	Ministries, Departments, and Agency
MEWR	Ministry of Energy and Water Resources of Tajikistan
MIC	Ministry of Information and Communication of Sierra Leone
ML	Maturity Level
NC3	National Cybersecurity Coordination Centre of Sierra Leone
NIST	National Institute of Standards and Technologies
OAS	Organization of American States
OT	Operational Technology
PoC	Point of Contact
SCMM	Sectoral Cybersecurity Maturity Model
SDG	Sustainable Development Goals
SOC	Security Operation Center
TTL	Task Team Leader
UEMOA	West African Economic and Monetary Union
WB DD	World Bank Digital Development Global Practice
WEF	World Economic Forum

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.
Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Cover photo: © Adrienguh / Unsplash. No permission required for use.

ACKNOWLEDGEMENTS

This methodology was prepared by the World Bank Digital Development (WB DD) team in cooperation with the Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center (TAU ICRC). The WB team was co-led by Oleg Petrov (Senior Digital Development Specialist) and Hagai Mei-Zahav (Senior Cybersecurity Specialist), and consisted of Giacomo Assenza (Cybersecurity Specialist), Alessandro Ortalda (Cybersecurity Consultant), and Francesca Spidalieri (Senior Cybersecurity Consultant). The TAU's research team included Dr. Lior Tabansky (Head of the Cyber Resilience Lab, TAU ICRC) and Eynan Lichterman (Cybersecurity Expert).

The team would like to thank the WB DD management, including Christine Qiang (Director of the DD Global Practice), Casey Torgusson (Global Program Manager), and Anat Lewin (Global Lead, Digital Safeguards) for their guidance, feedback, and support during the development of this methodology. The methodology benefited from valuable comments by peer reviewers, including World Bank Group colleagues Natalija Gelvanovska-Garcia (Senior Digital Development Specialist), Carlo Rossotto (Principal Investment Officer, IFC), Dorothee Delort (Senior Financial Sector Specialist), Malarvizhi Veerappan (Program Manager), Anders Pedersen (Senior Energy Specialist), and external partners, including Chris Painter (President, Global Forum on Cyber Expertise Foundation) and Carolin Weisser Harris (International Operations Lead at the Global Cyber Security Capacity Centre (GCSCC), Oxford University).

The methodology benefited from technical consultations with cybersecurity experts and practitioners, including Ghislain de Salins (WB DD Senior Cybersecurity Specialist), Melissa Hathaway (President, Hathaway Global Strategies), Donna Dodson (former Chief Cybersecurity Advisor, NIST), Kerry-Ann Barrett (Cybersecurity Program Manager, Organization of American States (OAS)), Roi Yarom (Cybersecurity Associate Director, European Bank for Reconstruction and Development (EBRD)), and Ariel Nowersztern (Senior Cybersecurity Specialist, Inter-American Development Bank (IDB)). The team would like to also recognize contributions from previous WB team leaders Sandra Sargent (Senior Digital Development Specialist) and Edward Hsu (Senior Adviser) in the initial phase of this Project. The team would like to thank many other colleagues from CoE, EBRD, GFCE, IDB, IFC, IMF, INCD, ITU, MoFA Netherlands, OAS, Oxford University, WEF, and the World Bank who contributed guidance and ideas in the inception phase through an informal advisory group and concept review process. The team is also grateful to WB colleagues Khyatee Tewari, Amir Noorbakhsh and Bianca Ruiz for project management and dissemination support.

This methodology would have not been possible without the sustained commitment and collaboration of the countries in which the SCMM was piloted. The team is particularly grateful to the Central Bank of West African States (BCEAO) and the West African Economic and Monetary Union (UEMOA); the Ministry of Energy and Water Resources (MEWR) of the Republic of Tajikistan; the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of the Republic of Georgia; and the Ministry of Information and Communications of Sierra Leone (MIC) and their National Cybersecurity Coordination Center (NC3) for their active participation in the various SCMM sectoral assessments and for coordinating various agencies, organizations, and other key stakeholders who contributed to these efforts.

The methodology was developed under the Critical Infrastructure Protection (CIP) Toolkit Project, funded by the World Bank's Digital Development Partnership (DDP). DDP offers a platform for digital innovation and development financing, bringing public and private sector partners together to advance digital solutions and drive digital transformation in developing countries. For more information, please visit: www.digitaldevelopmentpartnership.org.

INTRODUCTION

Digital transformation is a key enabler of inclusive and sustainable economic growth and social development, and a means to accelerate the achievement of the Sustainable Development Goals (SDGs) and the World Bank's twin goals of ending extreme poverty and driving shared prosperity. Digitalization and increased connectivity yield unquestionable benefits, including enhancing productivity and efficiency, facilitating innovation and modernization, promoting economic growth, and advancing human and social development[1]. Due to these benefits, the adoption of digital technologies **has become so pervasive across value and supply chains that most economic and social activities have become digitally dependent**. Among these activities, some are critical to the delivery of essential services, like the distribution of water and energy, as well as the provision of healthcare, telecommunications, banking services, and government services.[2] **All these essential services rely on the functioning and operational continuity of a country's ICT infrastructure**. Without a reliable digital infrastructure, affordable connectivity, and digital skills, it is difficult for countries to achieve growth and ensure the efficient and effective delivery of essential services.

Despite the benefits of adopting digital technologies, **the rapid digital transformation of critical sectors has also introduced new cybersecurity risks that can undermine the safety, security, operational continuity, and resilience of critical infrastructures (CIs) and the delivery of essential services**. The combination of increased digital dependency and its related risks to CIs requires governments to adopt innovative policies, strategies, and technical measures to **strengthen the cybersecurity and cyber resilience[3] of CIs and ensure the continuous and reliable delivery of essential services**. This is why developing effective critical infrastructure protection (CIP) measures and improving the cyber resilience of CIs are becoming increasingly important for both developed and developing countries undergoing digital transformation. **Although the importance of ensuring that critical sectors and systems are resilient to cyber disruption is widely recognized, its implementation remains challenging**.

Contemporary studies in system science show that the increase in resilience of individual components within a system does not necessarily result in a proportional improvement in the resilience of the system as a whole[4]. Rather, **resilience is intricately linked to the interactions among various components of a system or sector and is not simply the sum of the individual capacity of its constituent parts**. As countries accelerate their digital transformation, their critical

[1] MELISSA HATHAWAY and FRANCESCA SPIDALIERI, *Integrating Cyber Capacity into the Development Agenda*, Global Forum on Cyber Expertise, November 2021, https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

[2] LAURENT BERNAT, *Enhancing the digital security of critical activities*, Going Digital Toolkit Note, No. 17, 2021, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf.

[3] Cyber resilience is defined as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *NIST Special Publication 800-171 Revision 2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020, https://doi.org/10.6028/NIST.SP.800-171r2.

[4] LUCAS D VALDEZ *et al.*, *Cascading failures in complex networks*, Journal of Complex Networks 8, no. 2, 2020, https://doi.org/10.1093/comnet/cnaa013; STEFAN THURNER, PETER KLIMEK, and RUDOLF HANEL, Introduction to the Theory of Complex Systems, Oxford University Press, 2018, https://www.oxfordscholarship.com/10.1093/oso/9780198821939.001.0001/oso-9780198821939; ALIREZA SHAHPARI, MOHAMMAD KHANSARI, and ALI MOEINI, *Vulnerability analysis of power grid with the network science approach based on actual grid characteristics: A case study in Iran*, Physica A: Statistical Mechanics and its Applications 513, 2019, https://doi.org/https://doi.org/10.1016/j.physa.2018.08.059.

sectors are becoming increasingly interconnected and interdependent, and therefore, more vulnerable to cyber risks. The cascading effects of a cybersecurity-related incident in one sector can impact other critical sectors of the economy. Thus, assessing the cyber resilience of a sector requires a holistic approach that takes into account both the individual components that contribute to sectoral cyber resilience (including relevant external entities) and their intersectoral correlations, dependencies, and interactions. In other words, **it requires an approach that looks at a sector as a system**.

In this context, a sector is a coordinated group of organizations that conducts specific activities in an area of a country's economy (e.g., energy, telecommunications, finance, transportation, etc.), provides a particular service or set of services within a defined territory (i.e., country, region, or smaller jurisdiction), and encompasses the following characteristics:

- Shared roles, missions, and types of services provided;
- Functional cooperation and coordination among several organizations – constituents, stakeholders, and community members – each involved in producing and delivering a service inherent to the sector; and
- Governance, oversight, and coordination provided by one or more competent agencies/authorities/stakeholders tasked with steering, guiding, supervising, regulating, and coordinating activities within this sector, including assigning roles and responsibilities to different constituents of the sector, establishing safety, security, and reliability minimum standards, setting sectoral policies and regulation, etc.

While cybersecurity is increasingly recognized as a shared responsibility, each sector exhibits unique characteristics, including different roles and responsibilities across a range of public and private participants, agencies, and stakeholders. Effective CIP calls for coordinated action by the government, public and private sector organizations, and society. However, strategies, policies, and implementations of effective CIP measures vary even among more "cyber-mature" countries and societies. Different CIP approaches reflect a variety of existing risk assessment and management frameworks and the need to tailor solutions and activities to sector-specific contexts, settings, legal and regulatory frameworks, institutional capacities, and cyber capabilities.

Existing assessment methodologies consider cybersecurity maturity from either a national perspective (e.g., Global Cybersecurity Index, Cybersecurity Capacity Maturity Model for Nations, Cyber Readiness Index 2.0, National Capabilities Assessment Framework, or National Cyber Security Index)[5] or from an organizational perspective (e.g., NIST, ISO, etc.). Similarly, the few available sector-specific assessment methodologies focus on single operators within a given sector[6]. These approaches have the merits of providing a high-level overview of cybersecurity capabilities and directly informing national and corporate cybersecurity capacity building (CCB) efforts. However, they are not designed to evaluate the cybersecurity maturity of a sector as the combination of its components' strengths, weaknesses, interactions, and dependencies within a system (rather than the

[5] A detailed overview of available national-level cyber capacity maturity models has been developed by the Global Forum on Cyber Expertise (GFCE), "Global Overview Assessment Tools (GOAT), and can be accessed at https://cybilportal.org/publications/global-overview-of-assessment-tools-goat.

[6] For example, the Electricity Subsector Cybersecurity Risk Management Process (RMP) by the U.S. Department of Energy; the Critical Infrastructure and Digital Resilience (CIDR) mechanism by USAID; the Cybersecurity Capability Maturity Model (C2M2) by NERC; and the Guide to Fostering Financial Sector Cyber Resilience in Developing Countries by CREST. A comprehensive overview of existing national-level and organizational-level resources, curated by Tel Aviv University, can be accessed at https://rcrl.tau.ac.il/rcrl_navigate_cip.

sum of the individual cyber capacity of its constituent parts). **The lack of a more holistic sector-oriented perspective on cybersecurity and cyber resilience hinders the ability of a sector as a whole to objectively and accurately assess its current cybersecurity maturity levels and address systemic cyber risks connected to its increased digitalization and interdependence from other critical sectors of the economy**.

SECTORAL CYBERSECURITY MATURITY MODEL (SCMM)

Seeking to advance and mainstream cyber resilience in support of sustainable development and capacity building in critical sectors of the economy, **the World Bank Digital Development team (DD), in collaboration with Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center, developed a new methodology to assess and improve the cybersecurity maturity and resilience of critical sectors**.

The **Sectoral Cybersecurity Maturity Model** (SCMM) examines a given critical sector of the economy to identify and analyze current gaps in cybersecurity practices, capabilities, and resources within the sector, and develop a roadmap that prioritizes improvements to enhance the sector's future cyber resilience and capacity. The SCMM expands the breadth and depth of traditional cybersecurity assessment methodologies by evaluating a sector's overall cybersecurity maturity rather than assessing individual entities comprising a sector. This methodology takes a holistic approach to analyzing and recommending actions to mature the overall cybersecurity posture of a critical sector. In particular, the SCMM **emphasizes interdependencies, relations, and interactions among various stakeholders that constitute the sector** (e.g., supervisory authorities, individual organizations, etc.) **and with relevant external entities** that may influence or impact the cybersecurity, capabilities, and resilience of the sector, such as Ministries, Departments, and Agencies (MDAs), national competent authorities for cybersecurity, ICT/OT service providers, etc. This sectoral approach allows for a more comprehensive understanding of the sector's cybersecurity landscape, vulnerabilities, capabilities, and relevant stakeholders compared to a national- or organizational-level approach.

The main innovation of this methodology is its ability to capture any sector or sub-sector (hereby referred to as "sector") as an entire system, rather than analyzing a single entity or technical system, and be applied to any sector of the economy (sector-agnostic). The SCMM has been designed to take into account both the needs and desired cyber capabilities of sectoral stakeholders and the dependencies, relations, and interactions among them and with external entities.

An assessment using the Sectoral Cybersecurity Maturity Model (SCMM) involves a rigorous process of data gathering, gap analysis, and review of findings by a team (the Team) of cybersecurity and sectoral experts. The SCMM employs three main methods to gather information: desk research, interviews with individual organizations or senior executives, and interactive focus groups among sectoral and relevant external stakeholders. The SCMM does not use self-assessment questionnaires or surveys.

The final output is an evidence-based report that serves three purposes:

- Presenting an assessment of the current cybersecurity maturity, capabilities, and resilience of the sector under analysis;
- Identifying gaps in cybersecurity practices and capabilities within the sector, and areas that require improvement to gradually enhance the sector's cyber resilience and ability to manage cybersecurity risks in an ever-evolving threat landscape; and
- Providing sector-specific and actionable recommendations to prioritize these improvements.

In addition, **the SCMM assessment helps to systematize information about the sector in a structured way, which can facilitate a better understanding of common challenges, needs, and priorities across sectoral** stakeholders and encourage the adoption of good practices for the benefit of all. This is crucial to, for instance, secure the support of key decision-makers or Ministries, Departments, and Agencies (MDAs) regarding cybersecurity initiatives and investments. It can also help raise cybersecurity awareness across the sector, promote collaboration between sectoral stakeholders, and further define roles and responsibilities.

It is important to note that the SCMM is not intended to conduct audits of individual entities, compare sectors or countries, or assign scores or maturity levels to organizations. Instead, its primary focus is to assess the overall cybersecurity maturity of a sector and provide actionable and prioritized recommendations that are specific to the sector's risks and challenges, as well as its desired capabilities and performance levels.

STRUCTURE OF THE SCMM

The SCMM is designed to capture and assess different aspects of sectoral cybersecurity maturity across three Layers of Assessment (LoAs), which correspond to three different categories of stakeholders: National Entities (LoA1), Sectoral Supervisory Authorities (LoA2), and sector Key Entities (LoA3). For each LoA, the SCMM evaluates five Dimensions (or areas of assessment), namely: Cybersecurity Governance, Cyber Risk Management, Cybersecurity Measures, Cyber Capacity Building, and Incident Response and Crisis Management. Each of these Dimensions comprises of a number of Factors and Indicators, which provide a more granular level of analysis and a set of guiding questions to structure the data gathering.

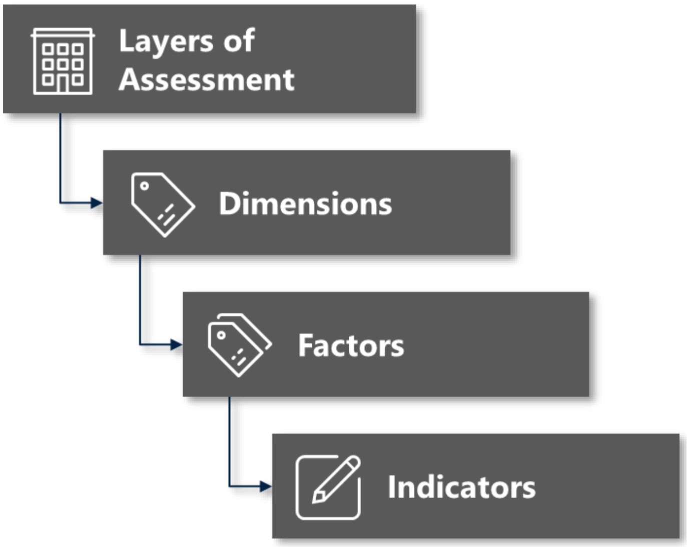


Figure 1 – Overview of the structure of the SCMM's main elements

1.1 Layers of Assessment (LoA)

The SCMM categorizes the different actors involved in the functioning, regulation, and coordination of a sector and, thus, in the assessment and evaluation of the sectoral cybersecurity maturity into three Layers of Assessment (LoAs), namely: National Entities, Sectoral Supervisory Authorities, and sector Key Entities. The three LoAs represent the three broad groups of stakeholders that impact or influence the sectoral cybersecurity maturity, capability, and resilience, and represent the different points of view on the current cybersecurity posture of the sector.

The list of stakeholders involved in the assessment, and their respective LoAs, are identified during the "Kickoff and Scoping" phase of the assessment (see section 1.6 "Kickoff and scoping").

LoA 1 – National Entities

Layer of Assessment 1 (LoA 1) involves national entities that are external to the sector but actively influence the cybersecurity maturity and resilience of the sector due to their overarching roles or responsibilities over national CI or the specific services they provide. These are, for instance, line ministries, national cybersecurity agencies, IT/cybersecurity training and service providers, and academic institutions. LoA 1 recognizes that any sector operates within a broader context, and therefore, the SCMM considers the linkages, resources, and capabilities of such entities outside the specific sector that can nonetheless impact its cybersecurity maturity and resilience.

By including LoA 1 in the SCMM assessment, the model aims to set the national context and analyze whether the country has policies, regulations, laws, standards, guidance, capacity building activities, and other capacities that, even though not specifically tailored to the sector, would nevertheless have an impact on its cybersecurity maturity and resilience. This provides a more comprehensive understanding of the sector's cybersecurity ecosystem and a holistic approach that can help devise higher-level, broader recommendations involving national stakeholders who can impact CIP within the country (e.g., an SCMM report can also inform national governments working on developing or refining their national CIP framework).

LoA 2 – Sectoral Supervisory Authorities

Layer of Assessment 2 (LoA 2) involves the main regulatory and supervisory authorities in the sector, typically the Ministry or Department responsible for regulating and/or overseeing the sector (e.g., the Ministry/Department of Energy, Ministry of Communications and ICT, etc.) and/or independent statutory bodies (e.g., Utility Regulators, Central Banks, etc.). Within this layer, the SCMM identifies the specific roles, responsibilities, policies, plans, guidance, standards, and requirements established at the sectoral level to manage operational, regulatory, and other types of cybersecurity risks. It also assesses the linkages, interdependencies, resources, and capabilities of regulatory/supervisory agencies in relation to key entities within the sector, as well as relevant national entities, including the level of coordination, collaboration, and resource allocation among these stakeholders.

By including LoA 2 in the SCMM assessment, the model aims to contextualize the regulatory and supervisory framework in which the sector operates, assess the extent to which the cybersecurity practices, capabilities, and resources (human, economic, technical, etc.) provided by regulatory and supervisory authorities support the overall cybersecurity maturity and resilience of the sector, and evaluate whether specific cybersecurity roles and responsibilities have been established within the sector. This core component of the methodology relies on extensive consultations with the main regulatory and supervisory authorities in the sector, in addition to desk research and additional data gathering.

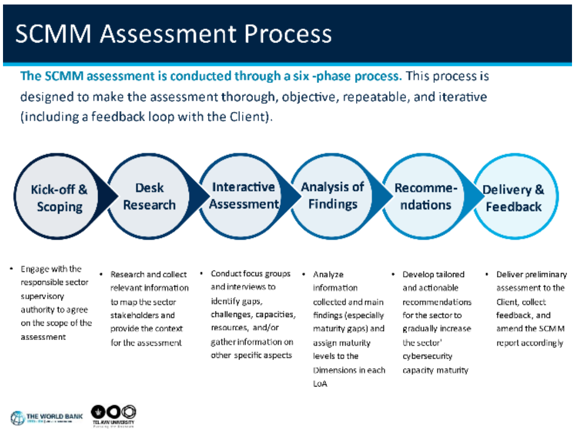
LoA 3 – Key Entities

Layer of Assessment 3 (LoA 3) involves the key entities that own, manage, and operate the sector’s critical infrastructures, essential services, and key resources. Entities included in LoA 3 are selected based on the criticality of the assets they manage, the type of services they provide, and the extent to which their roles and capabilities influence the functioning of the sector. For example, entities that operate critical infrastructure assets (such as power plants or transportation systems) or provide essential services (such as financial institutions or communication networks) are included insofar as they are critical within their respective sectors.

This layer may also include IT/cybersecurity vendors, suppliers, and service providers playing important roles in the sector’s operations (i.e., by market share). LoA 3 assesses the cybersecurity services and capabilities available in the country and their impact on the overall cybersecurity maturity and resilience of the sector. This includes the cybersecurity policies and requirements in place and the linkages, interdependencies, and interactions among key entities within the sector and with sectoral supervisory authorities. Thus, LoA 3 integrates important external dependencies, supply chains, and third-party risk management.

1.2 Dimensions

The SCMM is organized around **five Dimensions, which together constitute the breadth of capacities that a sector should possess to be cyber resilient**. The five Dimensions are the same in each LoA: Cybersecurity Governance, Cyber Risk Management, Cybersecurity Measures, Cyber Capacity Building, and Incident Response and Crisis Management (the annex provides a detailed list of the Factors and Indicators included under each Dimension). While there may be differences between LoAs on specific capacities (e.g., entities belonging to LoA 2 might implement capacities differently than entities belonging to LoA 3), Dimensions are designed to be applicable to all kinds of entities, large and small, internal or external to the sector.



SCMM Assessment Process

The SCMM assessment is conducted through a six -phase process. This process is designed to make the assessment thorough, objective, repeatable, and iterative (including a feedback loop with the Client).

Kick-off & Scoping

- Engage with the responsible sector supervisory authority to agree on the scope of the assessment

Desk Research

- Research and collect relevant information to map the sector stakeholders and provide the context for the assessment

Interactive Assessment

- Conduct focus groups and interviews to identify gaps, challenges, capacities, resources, and/or gather information on other specific aspects

Analysis of Findings

- Analyze information collected and main findings (especially maturity gaps) and assign maturity levels to the Dimensions in each LoA

Recomme-ndations

- Develop tailored and actionable recommendations for the sector to gradually increase the sector' cybersecurity capacity maturity

Delivery & Feedback

- Deliver preliminary assessment to the Client, collect feedback, and amend the SCMM report accordingly

Figure 2 - The five Dimensions of the SCMM

The SCMM assigns a maturity level from 1 to 5 to each Dimension: Start-up, Formative, Established, Strategic, and Dynamic (see section 1.5 on "Maturity Levels"). This evaluation is the result of a qualitative assessment that considers publicly available primary sources such as laws, policies, strategies, and formal statements, secondary sources such as expert analyses and reports (see section 1.7 on "Desk research (phase 2)"), and oral sources such as the outcomes of focus groups and interviews with relevant sectoral stakeholders (see section 1.8 on "Interactive assessment (phase 3)").

Maturity levels are assigned at the Dimension level to balance a high-level overview of individual LoA's cybersecurity maturity with a more granular assessment of the five different essential elements (Dimensions) considered in each LoA.

Cybersecurity governance

This Dimension explores the roles, responsibilities, accountability, and capacities within the sector's stakeholders to understand the institutional, regulatory, and legal context in which they operate (as it relates to cybersecurity) and the mechanisms and processes in place to address cybersecurity-related challenges. This includes (but is not limited to):

- Understanding the cybersecurity risks, challenges, capabilities, and specific needs and priorities of the sector;
- Identifying the risk appetite and managerial engagement in cybersecurity-related discussions;
- Identifying the decision makers. At the sectoral and national levels, this includes governing bodies with a mandate for cybersecurity of CI sectors and accountability frameworks;

- Establishing policies and procedures to make the decision-making process more structured and replicable, set up cybersecurity standards, guidance, and regulations, and monitor their implementation;
- Designating and communicating National Entities/Sectoral Supervisory Authorities/sectoral Key Entities' roles, responsibilities, and capabilities to manage cybersecurity risks; and
- Allocating dedicated resources to support sectoral cybersecurity and ensure decisions taken and policies established can be actioned.

Cyber risk management

This Dimension relates to the capacities of the sector and its stakeholders to assess and manage the cybersecurity risks inherent to the sector, including systemic risks stemming from linkages and interdependencies with other sectoral and external stakeholders.

This Dimension also explores the cybersecurity measures developed and implemented by sectoral stakeholders to minimize the impact of cyber incidents. Measures can vary according to the context and entity that implements them (e.g., technical, organizational, legal, etc.).

This covers aspects such as (but not limited to)

- Identifying critical assets, processes, and operators;
- Identifying threats and vulnerabilities
- Analyzing the likelihood and impacts of potential cybersecurity-related events; and
- Defining a cyber risk management approach.

Cybersecurity measures

This Dimension explores technical and organizational measures implemented by the evaluated entities to increase cybersecurity and reduce the likelihood and impact of cyber incidents. It also explores the level of engagement of national stakeholders (e.g., national cybersecurity authorities) and sectoral supervisory authorities in defining, establishing, and mandating such security measures and their impact on the cybersecurity of the sector.

The Dimension cover aspects such as (but not limited to):

- ID & Access Management;
- Network security;
- Data protection;
- Personnel security;
- Endpoint protection; and
- Cyber-hygiene, and supply chain security.

Cyber capacity building

This Dimension explores the capacity of the sector and its stakeholders to ensure a continuous process of development and strengthening of skills, abilities, processes, competencies, and resources needed to improve cybersecurity and cyber resilience. Improvements can be achieved through, for instance, the development of new skills (e.g., through training) or new tools (e.g., through research and development) or by facilitating cross-sector stakeholder cooperation and partnerships.

Incident response & crisis management

This Dimension explores the capacities of the sector and its stakeholders to detect, respond to, contain, and recover from cybersecurity incidents, implement lessons learned for future reference, and prepare to confront cyber crises. Such capacities include technical and organizational measures to address sector-wide cybersecurity incidents and crises and specific roles and responsibilities assigned to different stakeholders.

1.3 Factors

The SCMM encompasses 12 Factors across the five Dimensions. These factors seek to assess in more detail the sector's current cybersecurity capacities and maturity. Factors are also used to inform the drafting of tailored recommendations as they highlight specific areas needing improvement and specific activities and can help measure their outcomes. As in the case of Dimensions, Factors are the same across all three LoAs. During the course of a SCMM assessment, the assessor is advised to take written notes (see Table 1) about each Factor. These comments will then be used to better understand the maturity level of each Dimension and formulate specific recommendations. For a full list of Factors, please refer to the annex.

1.4 Indicators

Indicators represent the most granular level of assessment of the SCMM. These elements should be used during interviews, meetings, and focus groups as discussion points or guiding questions to further explore individual Factors in a more structured way. While Dimensions and Factors are the same across LoAs, Indicators are tailored for each LoA. They are meant to help the assessor evaluate how different categories of stakeholders perceive and address cybersecurity risks, including by adopting, implementing, and monitoring specific measures, policies, strategies, and other actions. Indicators are not prescriptive; the assessor can use them (or part of them) as guidance to organize the conversation with stakeholders (the WBG recommends using them to ensure a greater standardization of the data collection process). For a full list of Indicators, please refer to the annex.

1.5 Maturity Levels

The SCMM assigns Maturity Levels (MLs) to Dimensions in each LoA on a scale of 1 to 5 (i.e., ML1-Startup; ML2-Formative; ML3-Established; ML4-Strategic; and ML5-Dynamic)[7].

[7] These Maturity Levels are based on the 'Stages' of the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Oxford University's Global Cyber Security Capacity Centre (GCSCC). See https://gcscc.ox.ac.uk/cmm-2021-edition.

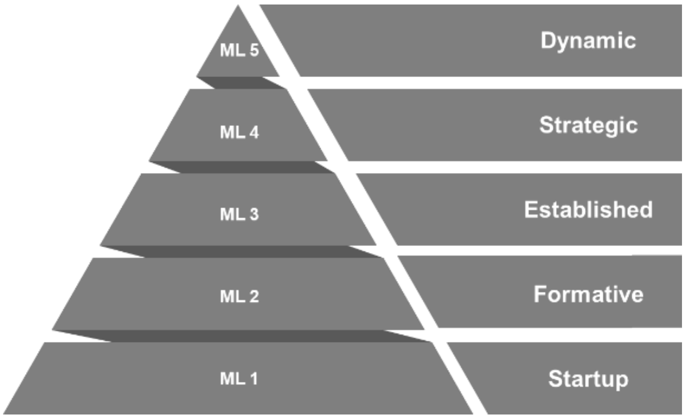


Figure 3 - The five Maturity Levels of the SCMM

The assessors analyze the data and information collected during the SCMM review and, in concert with the full SCMM team, assign a maturity score based on specific considerations, such as the level of commitment of stakeholders to strengthening the cybersecurity posture of their organization or sector as a whole, the effectiveness and efficiency of governance frameworks and coordination mechanisms, the implementation of standards, policies, rules, and requirements, etc. The five maturity levels of the SCMM are defined as:

- **Maturity Level 1 - Startup:** This level is assigned when there is no observable evidence of cybersecurity plans, strategies, or leadership commitment. There might be evidence of initial discussions about cybersecurity risks and activities to address them, or signs that stakeholders intend to address cybersecurity, but no tangible actions have been taken yet.

- **Maturity Level 2 - Formative:** This level is assigned when it is possible to observe that some activities aimed at increasing cybersecurity and resilience are being formulated and implemented, but are characterized by an ad hoc approach, are disorganized or poorly defined, or are simply at a nascent stage and it is not possible to draw meaningful conclusions on their impact on the cybersecurity and resilience of the sector yet.

- **Maturity Level 3 - Established:** This level is assigned when cybersecurity activities are in place, and it is possible to observe evidence that these are having a positive impact on cybersecurity and resilience. There is not, however, a structured design and planning regarding the identification, allocation, and use of resources necessary to ensure the full implementation and positive impact of these activities.

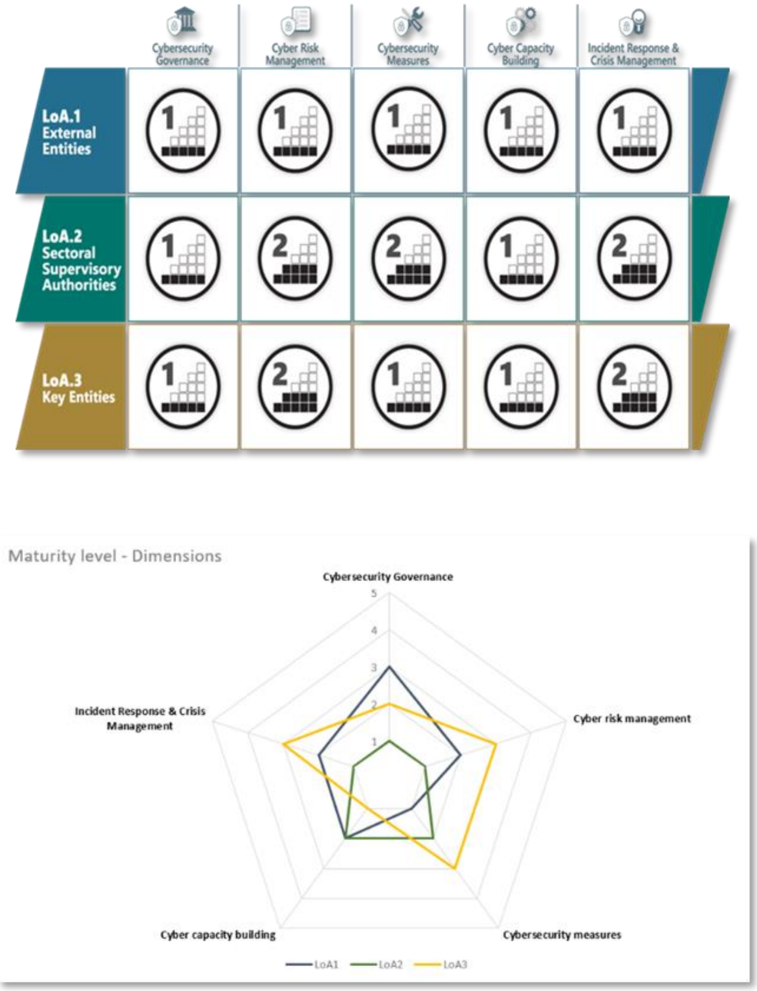
- **Maturity Level 4 - Strategic:** This level is assigned when it is possible to observe a structured approach to the design and planning of activities and an analysis of expected impacts and outcomes. Choices have been made about which cybersecurity activities should be prioritized according to pre-defined goals, but there are no clear mechanisms in place to monitor and adjust these activities as needed.

- **Maturity Level 5 - Dynamic:** This level is assigned when there are clear mechanisms in place to guide the implementation of cybersecurity activities depending on the prevailing circumstances, such as a change in the technology, institutional, or legal environment, evolving risk landscape, or a significant change in an area of concern. There is also evidence of leadership on cybersecurity issues, and it is possible to observe that there are mechanisms and processes in place to change/update strategies at any stage during their development.

Rapid decision-making processes, reallocation of resources, and constant attention to the changing environment are features of this ML.

Assigning maturity levels for the five Dimensions results in 15 separate maturity level scores rather than a combined single score. Assessing individual Dimensions for each category of actors, instead of having an overall score for the entire sector, provides a more granular analysis and detailed overview of how each LoA addresses specific components of cybersecurity and resilience and whether and how these elements are related across different LoAs. It also helps to identify gaps across LoAs that might hinder the ability of the sector to strengthen its overall cybersecurity posture and cyber capabilities and how to address specific deficiencies. For instance, discrepancies between maturity levels in the same Dimension across the three different LoAs may indicate that the sector is not leveraging the linkages and interconnections between its stakeholders to increase cybersecurity capability and resilience, which in turn would require an analysis of the root causes behind that issue. This additional analysis contributes to the development of tailored, effective, and sustainable action paths to strengthen the cybersecurity capability maturity and resilience of the sector.

Maturity levels can be presented using different visual representations (see examples in figure 4).



4

Figure 4 - Outcomes of an SCMM review presented in a matrix (above) and in a radar graph (below)

Even though maturity levels are assigned to Dimensions, Factors are fundamental in supporting the assessors to understand the maturity levels of individual Dimensions. Factors help the assessors by defining narrower and more manageable areas of analysis and providing a common taxonomy to organize the cybersecurity activities and initiatives observed during the SCMM review. The table below provides a snapshot of an assessor's notes and comments, which would inform the determination of a Dimension's ML.

It is important to underline that **the main goal of the SCMM is to provide high-priority, actionable recommendations aimed at increasing the cybersecurity and resilience of the sector**, rather than focusing on assigning scores or maturity levels. MLs should be seen simply as a tool to more easily showcase the results of the cybersecurity capacity maturity assessment and prioritize recommendations for the sector.

Layer of Assessment 1 – National Entities		
Dimension 1.1 – Cybersecurity governance	GENERAL OBSERVATIONS ON DIMENSION 1 The analysis of available information shows that cybersecurity risks and priorities are addressed at the national level through effective allocation of roles, responsibilities, and resources among competent authorities and the establishment of policies and procedures. Moreover, stakeholders at the national level are aware of the most pressing cybersecurity needs of the sector. Despite this, formal governance structures and coordination mechanisms have yet to be created, which prevent the sector from fully benefitting from the cybersecurity activities, institutions, and measures in place at the national level. Following these considerations, the team assigned a Maturity Level 2 to this Dimension in LoA 1.	
	Factor 1.1.1 – Sector environment	NOTES ON THE FACTOR The entities in this LoA have a clear understanding of the intrinsic cybersecurity risks to the sector and actively monitor them.
	Factor 1.1.2 – Roles and responsibilities	NOTES ON THE FACTOR There are clear cybersecurity roles and responsibilities assigned at the national level. However, existing regulation does not provide a clear picture of which roles and responsibilities entities have at the sectoral level. This results in an unstructured uncoordinated implementation of existing policies and procedures, with overlaps in roles and responsibilities and gaps in governance structures.
	Factor 1.1.3 – Policies and procedures	NOTES ON THE FACTOR Policies and procedures at the national level exist and there is evidence of their effectiveness on the national cybersecurity posture.
	Factor 1.1.4 – Budget and spending	NOTES ON THE FACTOR The sources consulted did not provide conclusive evidence on the budget and spending dedicated to cybersecurity activities (often even national entities must use a portion of their IT budget for cybersecurity).

Table 1 - Example of assessor's considerations on the Maturity Level of a Dimension within a LoA

IMPLEMENTATION OF THE SCMM

The SCMM **assessment** is conducted through **a six-phase process**. The phases are: (1) Kick-off and scoping; (2) Desk research; (3) Interactive assessment; (4) Analysis of findings; (5) Formulation of high-priority recommendations; and (6) Delivery and feedback. The process is designed to make the assessment thorough, objective, and repeatable. Parties interested in performing a cybersecurity maturity assessment using the SCMM can refer to these recommended phases and iterative steps:

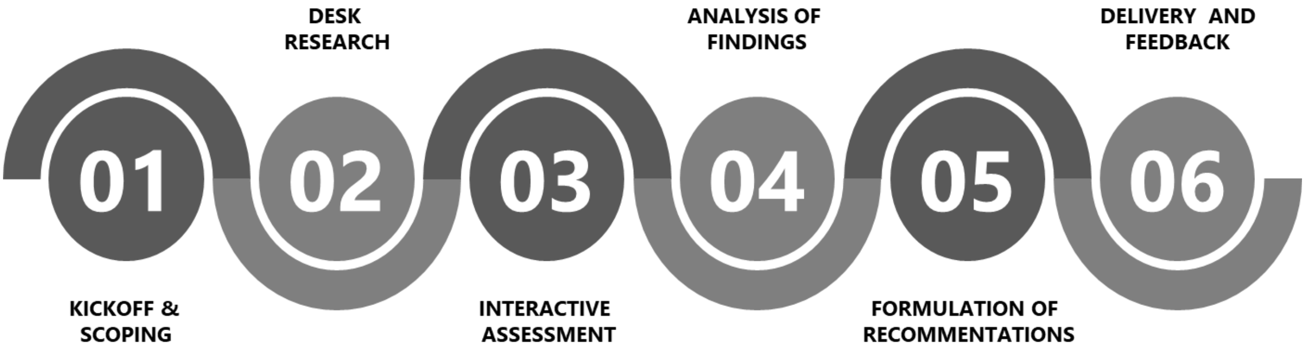


Figure 5 - The six phases of the SCMM review

1.6 Kick-off and scoping (phase 1)

Define the scope of the assessment

In the first step of Phase 1, the SCMM team (the Team) should engage with the responsible sector supervisory authority (and other key stakeholders they may choose to involve) to establish and agree on the scope and objectives of the assessment. This usually entails:

- Identifying the ultimate goals of the assessment (e.g., health check of the sector; informing the revision of national/sectoral strategies; providing input for future investments; etc.). These goals need to be discussed and agreed upon with local stakeholders to ensure that the needs and expectations of all the parties involved are taken into account;

- Securing the ownership, commitment, and mandate of the country or sector to perform the assessment;

- Defining the boundaries of the assessment (e.g., whether the assessment is going to cover an entire sector or sub-sectors (e.g., energy sector vs. electricity sub-sector); the categories of stakeholders that are going to be involved; and whether interviews or meetings with entities outside of the sector can be secured; and

- Defining the list and securing the commitment of stakeholders, including key figures at the national and/or ministerial levels who should take part in the assessment (including external entities).

Assemble a team

In the second step of Phase 1, the Team should identify the roles and expertise required to complete a specific SCMM assessment. The list of roles varies from case to case, since different assessments might require different areas of expertise – the assessment will likely require both cybersecurity and sectoral experts/specialists to serve as assessors. Local experts familiar with the country context are recommended to form part of the assessor team.

Table 2 below provides an overview of the typical roles necessary to complete an SCMM assessment.

Role	Tasks	Characteristics
Project manager	Secures commitment, identifies the needs and goals, and manages resources	A co-owner of the main project and the gateway to the beneficiary country/sector. In the WB, this would be a TTL or Practice Leader
Single PoC	Coordinates communications with the project stakeholders and provides onsite support (e.g., setting up meetings)	A local employee, such as a project manager in the WB country office or a local Short-Term Consultant
Cybersecurity specialist	Leads desk research, interviews, and focus groups to collect relevant information and conducts an analysis of findings	Senior (7+ years of experience) cybersecurity specialist who has received training on deploying the SCMM diagnostic tool
Sector specialist	Brings in sector-specific expertise and tailored questions, enriching information collection and analysis	Experienced practitioner or consultant with strong background in the sector and, ideally, cybersecurity good practices for the sector
Local Specialist*	Brings in local experience, expertise, and perspective, and provides support in bridging cultural differences and "translating" the process into local "terms" ** When the other specialists of the Team are not locals*	Experienced practitioner or consultant with strong understanding of the local sectoral environment

Table 2 - The Team roles and responsibilities

The roles of the Team members should be clearly delineated to ensure a thorough distribution of tasks and expertise. However, this might not always be possible (e.g., due to budget constraints, personnel availability, etc.). Under these circumstances, different roles might be assigned to the same person (e.g., the Project lead might also act as a cybersecurity specialist, the sector specialist might also act as a local specialist, etc.).

Create a project plan

In the third step, the Team should create a project plan and submit it to the counterpart(s) in the country/sector for feedback and approval. A project plan should, at minimum, provide the following information:

- Detailed project timeline, including when the project is expected to start and end and the expected duration of each phase (duration of single phases can vary from case to case, with stakeholders' engagements (interviews and focus groups) and on-site missions lasting usually 2 to 5 days, while the development of the SCMM report lasting usually 1 to 2 months);

- Planned activities and milestones and when these stages are expected to be reached;
- Description of the roles, responsibilities, and estimated effort from local stakeholders;
- What each milestone entails (e.g., identification of relevant stakeholders; submission of deliverable(s); status update meeting; etc.);
- A list of stakeholders to be included in the SCMM review. Identifying the appropriate stakeholders is crucial to ensure the Team can collect the information needed to complete the assessment. Thus, the list is of primary importance, and the Team should draft it with the support of local counterpart;
- A calendar of suggested focus group meetings for the interactive assessment phase (see section 1.8 on "Interactive assessment (phase 3)");
- The resources required from the country/sector to achieve each milestone;
- Presentation of the Team composition, including the appointment of a project manager and introduction of the cybersecurity and sectoral experts (they could be external consultants or internal experts) who will serve as the assessors;
- Main contact point(s) for the country/sector and other relevant stakeholders (as suggested in step 2);
- Expected deliverables (e.g., final report, visual representation(s) of MLs, presentation of findings and recommendations, etc.) and timing of delivery;
- Project risks that could arise during the SCMM review; and
- Measures implemented/planned to mitigate identified project risks.

1.7 Desk research (phase 2)

In Phase 2, the Team should gather relevant information via desk research. The cybersecurity specialist(s) (with the support of sector and local specialists) will decide which information is relevant and should be further explored.

Phase 2 is crucial not only to map key entities and stakeholders and collect preliminary information about the cybersecurity context in the country and in the sector, but also to identify peculiarities and specificities of a specific sector within a country. Indeed, different sectors in a country can be exposed to different threats, be subject to different rules and requirements, or adopt different governance mechanisms. The desk research phase will help the team to clarify these aspects – both before and after the stakeholders' engagements and the on-site mission.

Approaches to collecting information can vary depending on the accessibility of information (open vs. restricted), sources (official vs. unofficial), and type (primary vs. secondary information). The Table below provides examples of documents that assessors may collect and ease of gathering them:

Information sources	Accessibility	Source	Type
Legislative documents	Open	Official	Primary
Strategic documents	Open/restricted*	Official	Primary
Government/leadership statements	Open/restricted*	Official	Secondary
Internal memos	Restricted	Official	Secondary
Media coverage	Open	Unofficial	Secondary
Data and statistics	Open/restricted*	Official/unofficial*	Primary
Press releases	Open	Official/unofficial*	Secondary
Academic research	Open	Unofficial	Secondary
Reports, surveys, analyses	Open	Official/unofficial*	Secondary
Experts' opinions	Open/restricted	Unofficial	Secondary

* Might be either one or the other, depending on the specific situation.

Table 3 – Data Gathering and Documentation

During the desk research, the team may also consider (where applicable) other findings and inputs from other assessments previously performed in the country (e.g., Oxford's CMM, Cyber Readiness Index 2.0, etc.) and/or from the implementation of other relevant toolkits (e.g., World Bank's Data Regulation Toolkit, ID4D Diagnostic, etc.).

The information gathered during Phase 2 is crucial to the success of the assessment process and can be used by the Team to inform subsequent phases by:

- Identifying relevant issues and pain-points that exist in the sector;
- Identifying additional entities that should be included in the assessment process;
- Identifying existing or planned cyber capacity building projects that might respond to current gaps; and
- Providing elements to tailor the questions or topics addressed during interviews and focus groups to drill down on certain aspects of relevance.

Additional desk research shall be conducted after the team engaged with local stakeholders in phase 3, in order to analyze additional resources indicated during the interaction with local stakeholders; fill potential information gaps; and corroborate the collected data.

1.8 Interactive assessment (phase 3)

During Phase 3, the Team directly engages with the entities identified during Phase 1 to gather first-hand information through semi-structured interviews and focus groups.

The Team must clarify from the beginning that the SCMM assessment is not an audit, a performance review, or an inquiry on conduct. Instead, the goal is to directly obtain information from several perspectives, identify gaps and discrepancies, and gradually and constructively explore these aspects to benefit all those involved. Ultimately, the SCMM review intends to encourage more cohesive, collaborative, and cooperative CIP.

The SCMM uses three main interactive methods to perform the assessment, detailed below and summarized in Table 4.

All the interactive engagements should be conducted under Chatham House Rule,[8] and comments and information shared during these meetings should not be attributed to specific individuals or organizations.

Semi-structured focus group across entities (type 1)

Semi-structured focus groups (type 1) bring together people from different entities that hold similar roles (e.g., IT personnel from commercial banks, the central bank, and IT service providers working in a financial services sector).

This type of engagement is intended to uncover commonalities and differences in cybersecurity measures and capacities among entities involved in the sector and may help to identify issues related to the interactions and interdependencies among stakeholders.

Semi-structured focus group single entity (type 2)

Semi-structured focus groups (type 2) bring together senior managers from one entity to gain a higher-level insight into that entity and its relations with other relevant stakeholders. The managers/senior leaders invited to these meetings should belong to different departments, organizational units, or divisions and have different areas of expertise. This type of engagement is useful when assessing CI operators or regulators. Its goal is to investigate an entity’s strategic and governance aspects and understand how cybersecurity fits into its vision, strategic goals, and risk management plans.

Semi-structured interview single entity

Semi-structured interviews in small groups are the most granular approach to gathering information during the SCMM assessment. The goal of this engagement is to collect information on specific aspects that might be difficult to investigate during larger focus group contexts either due to their sensitivity (participants may be less open to sharing such information in a larger group setting) or specificity (senior management taking part in semi-structured interviews may not be aware of the operational and more nuanced aspects of organizational cybersecurity, such as which security measures are in place). During interviews, the Team interacts with a small group of people (maximum 4) from the same entity and/or from the same department/division.

[8] For more information, please refer to https://www.chathamhouse.org/about-us/chatham-house-rule.

Engagement type	Description
Semi-structured focus group across entities (type 1)	Brings together people from different entities with similar roles in the financial services sector Aims to uncover commonalities and differences in cybersecurity measures and capacities among entities Identifies issues related to interactions and interdependencies among stakeholders
Semi-structured focus group single entity (type 2)	Brings together senior managers from one entity Provides higher-level insight into the entity and its relations with other stakeholders Examines strategic and governance aspects, vision, strategic goals, and risk management plans Essential for assessing CI operators or regulators
Semi-structured interview single entity	Interacts with a small group (maximum 4) from the same entity or department/division Most granular approach for gathering information during SCMM assessment Collects information on specific aspects that may be sensitive or require detailed knowledge

Table 4: Types of interviews employed in the SCMM processes

Choosing the best approach for the interactive assessment

Each approach has advantages and disadvantages. For instance, the first type of focus group (people with similar roles across different entities) is recommended when trying to gain deeper insights into different entities within the sector. It is worth noting, however, that bringing the regulator(s) and regulated entities together may hinder the open flow of discussions. Similarly, representatives from law enforcement and the defense /intelligence sector may not be a good pairing for a focus group of participants with similar roles across entities. When the first type of focus groups are used, the pairing of participants should be conducive to open and constructive information sharing. The Team should design the overall assessment adopting the three approaches in a balanced way, considering the local context and the available time and resources.

In-person interactions and engagements can be particularly beneficial to encourage stakeholders' participation, facilitate open and frank discussions, and promote sharing of good practices and lessons learned. Focus groups can help uncover important aspects such as organizational dynamics, tacit power structures, differences in perspectives and opinions, and the level of information sharing within the sector under analysis. Semi-structured interviews should be used when local partners indicate that bringing in different stakeholders in the same room may be counterproductive and unfeasible. The Team should interact with as many relevant stakeholders as possible in a series of focus groups to develop more accurate, tailored, and actionable recommendations. Method selection depends on the particular situation, with the local partners advising the research team on the feasibility and constraints.

Regardless of the approach selected by the Team, the topics that will be discussed during the interviews and focus groups should be shared with stakeholders in advance to give them a chance to ask for clarification ahead of the engagements and help them better prepare for the discussions.

1.9 Analysis of findings (phase 4)

In phase 4, the research Team analyzes the data collected to identify gaps and challenges hindering the ability of the sector to reach a higher level of cybersecurity maturity, then starts to organize them into an assessment report (which will be completed in Phase 5). The report should include at minimum:

- An executive summary providing the main findings and high-priority recommendations;
- An overview of the main aspects related to the digitalization and cybersecurity of the sector under analysis, including a presentation of the specific country and sectoral context;
- An explanation of the overarching project (an SCMM review is usually part of a larger development and/or cybersecurity project), beginning with the first engagement between the research Team and the beneficiary country/sector and a description of the different steps in the review process;
- A list of all the entities involved in the assessment, organized into the three SCMM's Layers of Assessment for the sector, explaining why certain entities were included within certain LoAs;
- A thorough explanation of the key findings, with particular attention to maturity gaps. Whenever possible, findings should be presented following the SCMM structure and accompanied by an annex that presents the data collected during the assessment within each Dimension and Factor (following the SCMM structure); and
- A thorough explanation of the high-level recommendations, organized into Action Paths (see 4.5 on "Formulation of recommendation"), to address the deficiencies uncovered and suggest practical ways to improve the overall cyber capability maturity of the sector.

In this phase, the Team should assign the maturity levels to the Dimensions in each LoA and prepare the sector's current cybersecurity maturity heatmap and/or radar graph.

1.10 Formulation of recommendations (phase 5)

During Phase 5, the Team formulates a set of tailored recommendations to strengthen the cyber capabilities and resilience of the sector. These recommendations should be based on the findings of the SCMM review and the discussions with the beneficiary country/sector about the level of cybersecurity capability and resilience they desire the sector to achieve. They should also be in line with the broader sectoral development objectives and national visions. Team members should meet and discuss a roadmap for improvements that prioritizes specific actions and takes into consideration the specific country/sector's situation, capabilities, and available resources (including technical and financial assistance from development partners and implementers engaged in the country or region).

The SCMM organizes recommendations into Action Paths – a set of actions that should be performed in sequence or in parallel to gradually increase the sector's cybersecurity capacity maturity. To facilitate the implementation of specific remediation or mitigation plans and subsequent measurement of their outcomes it is important for the recommended actions to follow quality criteria, such as specificity (the recommendation should be clear and detailed about the specific actions to be implemented and goals to achieve), responsibility (the recommendation should identify responsible owners and accountable entities), and measurability. It is advisable to link each recommendation to a specific Factor (and, thus, link it to a Dimension as well). Since more than one way to improve cybersecurity maturity typically exists, different Action Paths are possible.

The SCMM should substantiate the logic driving the recommendations with the information and evidence collected and reference internationally recognized standards, guidance, and good practices. The SCMM recommendations should also include a proposed timeline for their implementation and considerations on feasibility, required resources, and accountable/responsible stakeholders. In particular, the recommendations detailed in SCMM reports should provide the following elements:

- Challenges and obstacles for implementation in the specific context of the beneficiary country and sector, as well as action items that have been identified as straightforward and manageable;
- Expected impact or contribution to increasing the Maturity Level of the Dimension or Factor in question;
- Start year – the beginning of the implementation of a specific recommendation within a set timeframe (one to five years); and
- Repeat year – for recommendations that take less than a year to complete, the repeat year points to when a specific action should be re-implemented.

The responsible entities should review the report and use the findings and recommendations to inform their own operation(s), project design, and/or procurement plan in the sector under analysis. They should also decide how to prioritize the recommendations based on the level of urgency, ease of implementation, and level of impact.

1.11 Delivery and feedback (phase 6)

The last phase of the SCMM assessment comprises a formal feedback loop with the sector supervisory authority and other relevant stakeholders. The Team should share its preliminary findings and high-priority recommendations with the sector supervisory authority (which can be further shared with other stakeholders) and prepare a high-level presentation (non-technical briefing) for senior government officials with the action paths and tailored recommendations. Such a briefing is vital to engage senior leaders and secure executive attention, required for the successful adoption and sustainable implementation of recommended actions. Feedback from the sector supervisory authority and other stakeholders in the beneficiary sector should be welcomed and encouraged both before and during the delivery of the draft report and presentation. The recommendations should include the rationale that led to their drafting and an explanation of the suggested timeline for the implementation of specific actions and the expected involvement of relevant local stakeholders. The goal of the presentation is twofold: make the local stakeholders who participated in the assessment process aware of its results and collect their final feedback.

The Team, in collaboration and agreement with the local counterpart, should follow up after 1 to 5 years to verify whether specific actions have been implemented and what their impact was. Such follow-ups can be structured differently, according to the specific needs and available resources (e.g., checkup meetings, a new round of stakeholders’ engagement, selected desk research, etc.). It is advisable to wait at least one year after the delivery of recommendations before running a follow-up.

ANNEX – FULL LIST OF DIMENSIONS, FACTORS, AND INDICATORS

1.12 Layer of Assessment 1 – National Entities

Element type	Title and description
Dimension	**1.1 Cybersecurity Governance**
Factor	**1.1.1 Sector Environment** This factor evaluates National Entities' perceptions of cybersecurity risks, preparedness, and capabilities of the sector. Its primary objective is to assess their understanding of the cybersecurity risks, challenges, objectives, and priorities inherent to the sector, as well as the stakeholders involved, their roles, responsibilities, and activities. In particular, it intends to ascertain external entities' understanding of: • Constituents, stakeholders, and community members involved in the operations of CIs and delivery of essential services in the sector; • Key entities' activities, challenges, and priorities in the sector; • Key entities' roles, responsibilities, and capabilities to manage cybersecurity risks in the sector; • Sectoral Supervisory Authorities' roles, responsibilities, and capabilities to manage cybersecurity risks in the sector; • National Entities' own roles, responsibilities, and capabilities to manage cybersecurity risks in the sector. This factor assesses whether this information is used by National Entities to inform the establishment of specific cybersecurity roles, responsibilities, policies, regulations, actions, and decisions to manage cybersecurity risks in CI sectors, including the sector under analysis.
Indicator	The national competent authorities for cybersecurity (e.g., national cybersecurity agency, CIP/privacy/data protection agency, national CSIRT) recognize/acknowledge/are aware of the most pressing cybersecurity risks to the sector under analysis and its operations, especially about new and emerging risks and vulnerabilities derived from the digitalization of the sector and the integration of digital technologies into networked infrastructure and systems.
Indicator	The national competent authorities' role(s) in critical infrastructure protection (CIP) and assurance of cybersecurity minimum requirements in CI sectors is established and communicated.
Indicator	Dependencies and critical functions for the delivery of critical services are established and managed.

Indicator	National competent authorities for cybersecurity are aware and/or have established the resilience requirements (this refers to operational resilience rather than cybersecurity requirements) to support the delivery of critical services under all operating states (e.g., under duress/attack, during recovery, normal operations).
Indicator	The national competent authorities are addressing cybersecurity risks through multistakeholder engagements with key entities in the sector, awareness campaigns, risk mitigation strategies, policies, and other activities (this indicator will be further explored in more detail in subsequent factors).
Factor	**1.1.2 Roles and Responsibilities** This factor evaluates cybersecurity roles and responsibilities at the national- and sectoral-level, with a focus on oversight, governance, and incident response. Additionally, it evaluates the existence of any specific cybersecurity standards and requirements for CI operators and/or sector stakeholders, as well as the measures in place to monitor and enforce them. The factor also examines whether National Entities encourage dialogue and collaboration among key national and sectoral stakeholders to promote cybersecurity within the sector.
Indicator	There is one (or more) national-level competent authorities (e.g., Department, Center, Unit, Agency) responsible for cybersecurity and/or CI protection.
Indicator	There is a national CIRT/CSIRT/SOC or equivalent that is responsible for IT security, monitoring and analyzing cyber threats to the sector, receiving & issuing warnings, and alerts about potential/ongoing attacks, coordinating incident response and investigation, conducting cybersecurity awareness and educational events, and integrating its capability into the larger national cybersecurity ecosystem as applicable.
Indicator	National competent authorities for cybersecurity have defined cybersecurity roles and responsibilities (e.g., laws, policies, etc.) and communicate them to CI operators and Sectoral Supervisory Authorities.
Factor	**1.1.3 Policies and procedures** This factor examines whether national competent authorities have established specific policies and procedures to formalize their cybersecurity governance and requirements for CI sectors/operators. It also assesses whether the national competent authorities monitor the implementation and outcomes of cybersecurity standards, guidance, requirements/rules/regulations and whether such measures are having an impact on the sector's cybersecurity.
Indicator	The country has identified and formally established cybersecurity strategic goals (i.e., a national cybersecurity strategy) and respective KPIs. These goals are communicated to concerned stakeholders.

Indicator	The national-level competent authorities have issued cybersecurity-related requirements, standards, guidance, rules, and regulations for critical infrastructures, and communicated them to the sector (e.g., baseline security, auditing requirements, breach notification, vulnerability disclosure, etc.).
Indicator	The national-level competent authorities monitor compliance (including audits) with national-level cybersecurity regulations and requirements for operators of critical infrastructure sectors, and sanctions non-compliance/violations. This includes monitoring compliance with international regulations as well (e.g., obligations arising from bilateral/multilateral treaties).
Indicator	The national-level competent authorities discuss cybersecurity with top governmental entities (e.g., presidential cabinet, competent ministries) regularly (e.g., every year).
Indicator	The national-level competent authorities promote the implementation of voluntary cybersecurity standards and good practices.
Factor	**1.1.4 Budget and spending** This factor examines whether National Entities have access to dedicated financial resources, and if such resources are allocated towards supporting cybersecurity at the sector level.
Indicator	The national-level competent authorities allocate/have access to dedicated resources (financial) to support critical infrastructures/key entities' cybersecurity.
Indicator	The budget dedicated to cybersecurity is linked to specific cybersecurity goals and related implementation activities.
Indicator	The national-level competent authorities track % of expenditures of cybersecurity budget (e.g., achieving project's milestones) and adjust the subsequent budgets accordingly (e.g., budget reallocation, request more budget, etc.).
Dimension	**1.2 Cyber risk management**
Factor	**1.2.1 Critical Infrastructure mapping and Risk Management** This factor evaluates whether National Entities are aware of the most critical stakeholders and assets in the sector, and whether they understand their interdependencies, as well as whether such knowledge is continually updated.
Indicator	The national-level competent authorities map critical infrastructures, key entities, and essential services, their internal and external correlations and dependencies, update this list on a recurring basis (e.g., yearly) and prioritize its content.

Indicator	The national-level competent authorities have developed/adopted a cyber risk management strategy which includes assessments of the likelihood and impact of adverse events.
Indicator	The cyber risk management strategy identifies a common methodology for managing cybersecurity risks to ensure efficiency and consistency across all key entities in critical sectors and facilitate the exchange of risk information (e.g., standard taxonomies, normalization models, etc.).
Factor	**1.2.2 Situational Awareness & Information Sharing** This factor examines whether national-level competent authorities monitor pertinent information to understand and analyze the cybersecurity threat landscape and context, as well as to anticipate the emergence of cybersecurity risks in CI sectors. Moreover, it evaluates the tools and approaches used to conduct such assessments and share/exchange relevant, timely, and actionable information with relevant stakeholders to prevent, mitigate, and respond to cyber incidents and enhance cybersecurity within the sector.
Indicator	The national-level competent authorities monitor relevant sources, as well as hardware/software vulnerabilities, intrusions, anomalies, and other exploits of interest, to identify cyber-related threats and assesses the level of risk and then informs/alerts the Sectoral Supervisory Authorities and/or key entities.
Indicator	The national-level competent authorities have established formal and/or informal mechanism(s) to gather, analyze, sanitize, and disseminate actionable information about threats, vulnerabilities, intrusions, and anomalies with stakeholders and government partners (e.g., key entities, regulators, ISACs).
Dimension	**1.3 Cybersecurity Measures**
Factor	**1.3.1 Establishment of cybersecurity measures** This factor evaluates whether National Supervisory Authorities define/establish/mandate technical and organizational measures that should be implemented by key entities, and whether they monitor their effectiveness in mitigating cybersecurity risks. It examines whether the Sectorial Supervisory Authorities have the necessary technical knowledge to understand the measures and their effectiveness, and whether they actively monitor and review their implementation by key entities.
Indicator	The national-level competent authorities define/establish/mandate technical and organizational measures that should be implemented by key entities to manage digital identities accounts, credentials, and authentication mechanisms of their personnel (e.g., unique accounts; need to know/least privilege/separation of duties principles; provisioning and deprovisioning; strong credential; multifactor authentication; etc.).

Indicator	The national-level competent authorities define/establish/mandate technical and organizational measures that should be implemented by key entities to monitor and secure their IT and OT networks (e.g., segmentation; segregation; IDS/IPS; traffic monitoring; etc.) and the risks coming from their integration, especially when legacy systems are involved.
Indicator	The national-level competent authorities define/establish/mandate technical and organizational measures that should be implemented by key entities to protect the data in their systems and ensure their confidentiality (when applicable), integrity and availability (e.g., encryption; DLP measures; regular back up; logical and physical security separation from data source; etc.).
Indicator	The national-level competent authorities define/establish/mandate technical and organizational measures that should be implemented by key entities to mitigate the risk of intentional malicious actions posed by personnel or other individuals who have access to the data and systems of the key entities (e.g., personnel screening and monitoring; sanctions; termination; etc.).
Indicator	The national-level competent authorities define/establish/mandate technical and organizational measures that should be implemented by key entities to mitigate the risk of unintentional harm caused by personnel or other individuals who have access to the data and systems of the key entities (e.g., basic cyber-hygiene practices; proper configuration; removable media control; license management; purge of dismissed devices; etc.).
Factor	**1.3.2 External dependencies/Supply chain/procurement** This factor examines whether the national competent authorities (or other relevant MDAs) consider cybersecurity risks that could arise in the sector due to interconnections and interdependencies among sectors or the inherent networked nature of certain technologies, such as cloud applications. Additionally, it evaluates the legal, risk management, and governance measures available to manage and mitigate such risks. This factor examines whether the national competent authorities (or other relevant MDAs) manage supply chain risks and other external dependencies in the sector by issuing policies, standards, guidance, or requirements
Indicator	The national competent authorities (or other relevant MDAs) regulate procurement practices (e.g., risk management, lifecycle management, software and hardware assurance, outsourcing, use of cloud services, etc.). They provide guidance or establish regulations for CI operators on how to manage supply chain risks and external dependencies, such as IT/OT service providers or vendors that provide services to key entities and/or the Sector Supervisor/Regulator, which cannot be internally procured.
Indicator	The national competent authorities (or other relevant MDAs) monitor compliance with sectoral procurement requirements, organizational and technical measures.
Indicator	The national competent authorities promote the adoption of cybersecurity accreditation/certification for ICT providers (including hardware, software, and digital services).

Dimension	1.4 Cyber capacity building
Factor	**1.4.1 Cybersecurity Skills Development, Training & Awareness Raising** This factor evaluates whether the national competent authorities have identified cybersecurity workforce, skills, and capacity gaps in CI sectors and developed initiatives and measures to fill those gaps and enhance the cybersecurity skills and capacities of individuals and CI operators in CI sectors. It also assesses whether the national competent authorities promote/organize cybersecurity awareness campaigns/activities for CI sector stakeholders and the extent to which such efforts impact the development of human capital within the sector and the awareness of stakeholders at the sector level.
Indicator	The national competent authorities collaborate with other relevant ministries (interior, education, labor, etc.), academic institutions (departments/centers related to the sector's core topic), and relevant industry players and training service providers to promote cybersecurity workforce and skills development and training (i.e., develop human capital) in CI sectors, including the sector under analysis.
Indicator	There are ICT/cybersecurity providers, academic institutions, training centers, and certification providers that offer cybersecurity awareness raising activities, cybersecurity skills development, training, and education programs/courses/certificates for sector stakeholders (develop human capacity; offer career progression education, etc.).
Indicator	The national competent authorities regularly (e.g., annually) carry out cybersecurity awareness activities for sector stakeholders.
Factor	**1.4.2 Foster cybersecurity ecosystem and Cross-Sector cooperation** This factor evaluates the initiatives and measures implemented by national competent authorities to foster cybersecurity research and development and innovation, as well as to encourage collaboration among public and private stakeholders within and outside CI sectors. Additionally, it evaluates the extent to which such efforts impact cybersecurity within the sector, including providing financial support to promote cybersecurity development.
Indicator	The national competent authorities support and incentivize cybersecurity research and development and the dissemination of cybersecurity innovation across CI sectors.
Indicator	The national competent authorities facilitate and promote collaboration among public and private sector entities to increase cybersecurity.
Indicator	The national competent authorities engage in formal and/or informal cooperation mechanisms with stakeholders (across sectors, or from the same sectors in other countries) to share cybersecurity good practices and establish national-level cybersecurity standards and regulations (i.e., influence national policymaking).

Indicator	The national competent authorities allocate dedicated resources to support key entities' cybersecurity programs/activities/capacity building.
Dimension	**1.5 Incident Response & Crisis Management**
Factor	**1.5.1 Incident Response Plan** This factor examines whether national competent authorities have planned their approach to identify/detect, respond to, contain, and recover from cybersecurity incidents that may impact CI sectors. The objective is to assess the preparedness of national competent authorities to manage and coordinate a response with the sector in the event of sector-wide cybersecurity incidents, and to evaluate the extent to which this contributes to support incident management at the sector level.
Indicator	There is a national incident response plan with sector participation (including business continuity & disaster recovery planning), with clear roles, responsibilities, escalation processes, and criteria for their activation (when an incident/emergency/disaster occurs) and de-activation (when an incident/emergency/disaster is resolved).
Indicator	The national competent authorities regularly (e.g., once a year) inspect the sector's incident response plan, with a focus on CI operator plan (e.g., through tests, simulations, drills, assessments, tabletop exercises, etc.).
Indicator	The national competent authorities or National CSIRT take into account emerging risks, the mapping of sector dependencies, and the result of tests/drills and simulations (lessons learned) to draft/update the national and/or sector incident response plan(s).
Factor	**1.5.2 Incident Management** This factor examines the capabilities that national competent authorities (or third-party service providers such as an MSSP) have to detect, respond to, contain, and recover from cybersecurity incidents at the sector level. The objective is to assess whether national competent authorities have established technical and organizational measures to address sector-wide cybersecurity incidents and crises, whether their roles are formalized, to what extent they are involved in incident response, and what specific tasks are expected of them during a sector-wide cybersecurity incident.
Indicator	The national CSIRT is responsible (has capability) for analyzing (incident triage) and classifying the incident, verifying what services/assets have been compromised, assessing the impact of the incidents, and supporting affected stakeholders to resolve and recover from the incident.
Indicator	In case of sector-wide incidents, the national competent authorities and/or the national CSIRT coordinate the incident response (IR) and recovery with the Sector Supervisor/Regulator and alert law enforcement agencies if needed.

Indicator	In case of sector-wide incidents, the national competent authorities and/or the national CSIRT bring in IR capabilities from commercial IR service provider(s) to response, mitigate, and resolve the incident, when/if needed.

1.13 Layer of Assessment 2 - Sectoral Supervisory Authorities

Element type	Title and description
Dimension	**2.1 Cybersecurity Governance**
Factor	**2.1.1 Sector Environment** This factor evaluates Sectoral Supervisory Authorities' perceptions of cybersecurity risks, preparedness, and capabilities of the sector. Its primary objective is to assess Sector Supervisory Authorities' understanding of the cybersecurity risks, challenges, objectives, and priorities inherent to the sector, as well as the stakeholders involved. In particular, it intends to ascertain Sectoral Supervisory Authorities' understanding of: a. Constituents, stakeholders, and community members involved in the operations of CIs and the delivery of essential services in the sector; b. Key entities' cybersecurity-related activities, challenges, and priorities in the sector; c. Key entities' roles, responsibilities, and capabilities to manage cybersecurity risks in the sector; d. Sectoral Supervisory Authorities' own roles, responsibilities, and capabilities to manage cybersecurity risks; e. National Entities' roles, responsibilities, and capabilities to manage cybersecurity risks. This factor also assesses whether this information is used by Sectoral Supervisory Authorities to inform the establishment of specific cybersecurity roles, responsibilities, policies, regulations, and decisions to manage cybersecurity risks within the sector.
Indicator	The Sectoral Supervisory Authorities recognize/acknowledge/are aware of the most pressing cybersecurity risks to the sector and its operations, especially new and emerging risks and vulnerabilities derived from the digitalization of the sector and the integration of digital technologies into networked infrastructure and systems.
Indicator	The Sectoral Supervisory Authorities' role(s) in critical infrastructure protection and assurance of cybersecurity minimum requirements within their industry sector is established and communicated.
Indicator	Dependencies and critical functions for the delivery of critical services within the sector are established and managed.
Indicator	Sectoral Supervisory Authorities are aware and/or have established the resilience requirements to support the delivery of critical services within the sector under all operating states (e.g., under duress/attack, during recovery, normal operations).
Indicator	The Sectoral Supervisory Authorities have begun to address cybersecurity risks through multistakeholder engagements with key entities in the sector, awareness campaigns, risk mitigation strategies, policies, and other activities (this indicator will be further explored in more detail in subsequent factors).

Indicator	The Sectoral Supervisory Authorities' role(s) in regulating and managing the ICT supply chain risks for entities in the sector/under their jurisdiction is identified and communicated.
Factor	**2.1.2 Roles and Responsibilities** This factor evaluates the assignment of cybersecurity roles and responsibilities to appropriate stakeholders throughout the sector, with a focus on oversight, governance, and incident response. Additionally, it evaluates the existence of any specific cybersecurity requirements for sector stakeholders, as well as the measures in place to monitor and enforce them. The factor also examines whether Sectoral Supervisory Authorities encourage dialogue and collaboration to promote cybersecurity and cyber resilience within the sector.
Indicator	There is one (or more) officially appointed Authority responsible for the sector's cybersecurity.
Indicator	There is a dedicated sectoral CIRT/CSIRT/SOC or equivalent (e.g., national CIRT/CSIRT) that acts as single contact point for the sector, responsible for sectoral IT security, monitoring and analyzing cyber threats to the sector, receiving & issuing warnings and alerts about potential/ongoing attacks, coordinating incident response and investigation, conducting cybersecurity awareness and educational events for sector stakeholders, and integrating its capability into the larger national cybersecurity ecosystem as applicable.
Indicator	Sectoral Supervisory Authorities have defined cybersecurity roles and responsibilities (e.g., laws, policies, etc.) and communicate them to CI operators inside the sector and to Sectoral Supervisory Authorities.
Factor	**2.1.3 Policies and procedures** This factor examines whether Sectoral Supervisory Authorities have established specific policies and procedures to formalize their cybersecurity governance and requirements for key entities in the sector. It also assesses whether the Sectoral Supervisory Authorities or other national competent authorities monitor the implementation and outcomes of cybersecurity standards, guidance, requirements/rules/regulations.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities have identified and formally established cybersecurity strategic goals and respective KPIs. The goals are communicated within the sector.
Indicator	The Sectoral Supervisory Authorities and/or other national competent authorities have established sectoral-level cybersecurity requirements (e.g., baseline security, auditing requirements, breach notification, vulnerability disclosure, etc.) for covered entities operating in the sector.

Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities monitor compliance (including audits) with sectoral-level cybersecurity regulation and requirements for relevant sectoral stakeholders, and sanctions non-compliance/violations. This includes monitoring compliance with international regulations as well (e.g., obligations arising from bilateral/multilateral treaties).
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities (e.g., sector agencies, governmental departments, etc.) discuss sector cybersecurity with top governmental entities (e.g., sector competent ministries) regularly (e.g., every year).
Indicator	The Sectoral Supervisory Authorities and/or other relevant stakeholders promote the implementation of voluntary cybersecurity standards and good practices.
Factor	**2.1.4 Budget and spending** This factor examines whether Sectoral Supervisory Authorities have access to dedicated financial resources specifically allocated to support cybersecurity policies and activities at the sector level.
Indicator	The Sectoral Supervisory Authorities and/or other relevant stakeholders allocate/have access to dedicated resources (financial) to support sector's cybersecurity (s).
Indicator	The budget dedicated to sector cybersecurity is linked to specific cybersecurity goals and related implementation activities.
Indicator	The Sectoral Supervisory Authorities and/or other relevant stakeholders track % of expenditures of cybersecurity budget (e.g., achieving project's milestones) and adjust the subsequent budgets accordingly (e.g., budget reallocation, request more budget, etc.).
Dimension	**2.2 Cyber risk management**
Factor	**2.2.1 Sector mapping and Risk Management** This factor assesses whether Sectoral Supervisory Authorities are aware of the most critical stakeholders, assets, and processes in the sector, with specific focus on the potential impact and consequences that may arise from adverse events. It also evaluates whether they have a comprehensive understanding of their interdependencies, and whether such knowledge is regularly updated.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities map the sector's key entities, infrastructures, and services, their internal and external correlations and dependencies, update this list on a recurring basis (e.g., yearly), and prioritize its content based on the criticality for the sector.

Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities have developed/adopted a cyber risk management strategy which includes assessment of the likelihood and impact of adverse events. The sector's cyber risk management strategy is aligned with the national cybersecurity strategy or equivalent document.
Indicator	The cyber risk management strategy identifies a common methodology for managing cybersecurity risks to ensure efficiency and consistency across all key entities in the sector and facilitate the exchange of risk information (e.g., standard taxonomies, normalization models, etc.).
Factor	**2.2.2 Situational Awareness & Information Sharing** This factor examines whether Sectoral Supervisory Authorities monitor pertinent information to understand and analyze the cybersecurity threat landscape and context, as well as to anticipate the emergence of cybersecurity risks in the sector. Moreover, it evaluates the tools and approaches used to conduct such assessments and share/exchange relevant, timely, and actionable information with relevant stakeholders to prevent, mitigate, and respond to cyber incidents and enhance cybersecurity within the sector.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities continuously monitor relevant sources, as well as hardware/software vulnerabilities, intrusions, anomalies, and other exploits of interest, to identify threats to the sector and assess the level of risk and then inform/alert key entities.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities have established formal and/or informal mechanism(s) to gather, analyze, appropriately sanitize, and disseminate timely and actionable information about threats, vulnerabilities, intrusions, and anomalies, as well as best practices with sector stakeholders, government partners (e.g., key entities, regulators, ISACs), and national-level competent authorities.
Dimension	**2.3 Cybersecurity Measures**
Factor	**2.3.1 Establishment of cybersecurity measures** This factor evaluates whether Sectoral Supervisory Authorities define/establish/mandate technical and organizational measures that are implemented by key entities in the sector, and whether they monitor their effectiveness in mitigating cybersecurity risks. It examines whether the Sectorial Supervisory Authorities have the necessary technical knowledge to understand the measures and their effectiveness, and whether they actively monitor and review their implementation by key entities.
Indicator	The Sectoral Supervisory Authorities defines/establishes/mandates technical and organizational measures that should be implemented by key entities to manage digital identities accounts, credentials, and authentication mechanisms of their personnel (e.g., unique accounts; need to know/least privilege/separation of duties principles; provisioning and deprovisioning; strong credential; multifactor authentication; etc.).

Indicator	The Sectoral Supervisory Authorities defines/establishes/mandates technical and organizational measures that should be implemented by key entities to monitor and secure their IT and OT networks (e.g., segmentation; segregation; IDS/IPS; traffic monitoring; etc.) and the risks coming from their integration, especially when legacy systems are involved
Indicator	The Sectoral Supervisory Authorities defines/establishes/mandates technical and organizational measures that should be implemented by key entities to protect the data in their systems and ensure their confidentiality (when applicable), integrity and availability (e.g., encryption; DLP measures; regular back up; logical and physical security separation from data source; etc.).
Indicator	The Sectoral Supervisory Authorities defines/establishes/mandates technical and organizational measures that should be implemented by key entities to mitigate the risk of intentional malicious actions posed by personnel or other individuals who have access to the data and systems of the key entities (e.g., personnel screening and monitoring; sanctions; termination; etc.).
Indicator	The Sectoral Supervisory Authorities defines/establishes/mandates technical and organizational measures that should be implemented by key entities to mitigate the risk of unintentional harm caused by personnel or other individuals who have access to the data and systems of the key entities (e.g., basic cyber-hygiene practices; proper configuration; removable media control; license management; purge of dismissed devices; etc.).
Factor	**2.3.2 External dependencies/Supply chain/procurement** This factor examines whether Sectoral Supervisory Authorities consider cybersecurity risks that could arise in the sector due to interconnections and interdependencies within and outside of the sector or the inherent networked nature of certain instruments, such as cloud technologies. Additionally, it evaluates the legal, risk management, and governance measures available to mitigate such risks and the involvement of Sectoral Supervisory Authorities in developing/implementing them.
Indicator	The process of cyber risk management considers risks coming from sector interdependencies.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities regulate procurement practices in the sector (e.g., risk management, lifecycle management, software and hardware assurance, outsourcing, use of cloud services, etc.). They establish sectoral cybersecurity standards and requirements for procurement of equipment/goods and services in the sector (e.g., risk management, lifecycle management, software and hardware assurance, outsourcing, use of cloud services, etc.).
Indicator	The Sectoral Supervisory Authorities and/or sectoral competent authorities monitor compliance with sectoral procurement requirements, organizational and technical measures.
Indicator	The Sectoral Supervisory Authorities and/or sectoral competent authorities promote the adoption of cybersecurity accreditation/certification for ICT providers (including hardware, software, and digital services).

Dimension	2.4 Cyber capacity building
Factor	**2.4.1 Cybersecurity Skills Development, Training & Awareness Raising** This factor examines whether the Sectoral Supervisory Authorities monitor the sector to identify workforce, skills, and capacity gaps and develop initiatives and measures to fill those gaps and enhance the cybersecurity skills and capacities of individuals and entities operating in the sector. It also assesses whether the sectoral supervisory authorities promote/organize cybersecurity awareness campaigns/activities in the sector and the extent to which such efforts impact the development of human capital within the sector and the awareness of stakeholders at the sector level.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities collaborate with other relevant ministries (interior, education, labor, etc.), academic institutions (departments/centers related to the sector's core topic), relevant industry players, and training service providers to promote cybersecurity workforce and skills development and training (i.e., develop human capital).
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities collaborate with relevant stakeholders (cross-sector, or same sector in different countries) to identify and incorporate lessons learned from other sectors or the same sector in other countries
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities regularly (e.g., annually) carry out cybersecurity awareness activities for sector stakeholders.
Factor	**2.4.2 Foster cybersecurity ecosystem and Cross-Sector cooperation** This factor evaluates the initiatives and measures implemented by Sectoral Supervisory Authorities to foster cybersecurity research and development and innovation, as well as to encourage collaboration among public and private stakeholders both within and outside of the sector. Additionally, it evaluates whether Sectoral Supervisory Authorities provide financial support to promote cybersecurity development.
Indicator	Sectoral Supervisory Authorities and/or other sectoral competent authorities support and incentivize cybersecurity research and development for sector applications and the dissemination of cybersecurity innovation within the sector.
Indicator	Sectoral Supervisory Authorities and/or other sectoral competent authorities facilitate and promote/sponsor formal and informal collaboration between public and private sector entities to increase cybersecurity at sector level and to strengthen the sectoral cybersecurity ecosystem.
Indicator	The Sectoral Supervisory Authorities and/or other sectoral competent authorities allocate dedicated resources to support key entities' cybersecurity programs/activities/capacity building.
Dimension	**2.5 Incident Response & Crisis Management**

Factor	**2.5.1 Incident Response Plan** This factor examines whether Sectoral Supervisory Authorities have planned their approach to identify/detect, respond to, contain, and recover from cybersecurity incidents that impact the sector. The objective is to assess the preparedness of Sectoral Supervisory Authorities to manage and coordinate a response in the event of sector-wide cybersecurity incidents, and to evaluate the extent to which this contributes to support incident management at the sector level.
Indicator	Sectoral Supervisory Authorities and/or other sectoral competent authorities have defined a sector incident response plan (including business continuity & disaster recovery planning), with clear roles, responsibilities, escalation processes, and criteria for their activation (when an incident/emergency/disaster occurs) and de-activation (when an incident/emergency/disaster is resolved) and communicated it to the sector's entities.
Indicator	Sectoral Supervisory Authorities and/or other sectoral competent authorities regularly (e.g., once a year) verify the effectiveness of the sector incident response plan (e.g., through tests, simulations, drills, assessments, tabletop exercises, etc.).
Indicator	Sectoral Supervisory Authorities and/or the sectorial CSIRT/SOC, or other sectoral competent authorities take into account emerging risks, the mapping of sector dependencies, and the result of tests and simulations to draft/update the sector incident response plan.
Factor	**2.5.2 Incident Management** This factor examines the capabilities that Sectoral Supervisory Authorities put in place to detect, respond to, contain, and recover from cybersecurity incidents at the sector level. The objective is to assess whether Sectoral Supervisory Authorities have established technical and organizational measures to address cybersecurity incidents and crises, and whether such measures are tested to assess their effectiveness.
Indicator	There are dedicated incident response (IR) teams at the sector level (e.g., CSIRT/SOC, etc.) tasked with analyzing (incident triage) and classifying the incident, verifying what services/assets have been compromised, assessing the impact of the incidents, and supporting affected stakeholders to resolve and recover from the incident.
Indicator	In case of sector-wide incidents, the appointed sectoral Authority (e.g., sector CSIRT/SOC) coordinates the response and recovery, and informs national-level MDAs such as CIP agency, law enforcement agencies, etc.
Indicator	In case of sector-wide incidents, Sectoral Supervisory Authority brings in IR capabilities from the national or sector CSIRT/SOC or from commercial IR service provider(s) / MSSP to respond, mitigate, and resolve the incident, if needed.

1.14 Layer of Assessment 3 – Key Entities

Element type	Title and description
Dimension	**3.1 Cybersecurity Governance**
Factor	**3.1.1 Sector Environment** This factor evaluates whether key entities have a comprehensive understanding of the sector's cybersecurity challenges, objectives, and priorities, as well as the stakeholders involved, their roles, responsibilities, and activities. Moreover, it seeks to determine if such awareness influences their actions and decisions that could affect the cybersecurity of their respective organizations and, as a consequence, the sector as a whole.
Indicator	The key entities in the sector are aware of the most pressing cybersecurity risks to their respective organizations, computer systems, and critical assets – and therefore to the sector and its functioning, especially new and emerging risks and vulnerabilities derived from the digitalization of their operations and the integration of digital technologies into networked infrastructure and systems.
Indicator	The key entities' role(s) in operating and maintaining critical systems/infrastructure in their industry sector is identified and communicated.
Indicator	Dependencies and critical functions for delivery of critical services are established and managed.
Indicator	Key entities are aware of the resilience requirements to support the delivery of critical services under all operating states (e.g., under duress/attack, during recovery, normal operations).
Indicator	The key entities address cybersecurity risks through communication and in cooperation with their peers, vendors, service providers, Sectoral Supervisory Authorities, and national competent authorities (this indicator will be further explored in more detail in subsequent factors).
Indicator	The key entities have identified and communicated their respective role in managing the ICT supply chain risks internally, and externally to LoA1 and LoA2.
Factor	**3.1.2 Roles and Responsibilities** This factor assesses the allocation of cybersecurity roles to personnel and functions within the key entities, as well as the duties associated with these roles and whether they align with cybersecurity requirements prevalent within the sector.

Indicator	The entity has established and assigned cybersecurity roles and responsibilities (IT department, legal, operational, incident response, etc.), including appointing a person (e.g., CISO, CSO) with the mission and resources to coordinate, develop, implement, and maintain the entity-wide cybersecurity strategy/plan/program/activities.
Indicator	The entity relies on a dedicated sectoral CIRT/CSIRT/SOC or equivalent (e.g., national CIRT/CSIRT) that acts as single contact point for the sector, responsible for sectoral IT security, monitoring and analyzing cyber threats to the sector, receiving & issuing warnings and alerts about potential/ongoing attacks, coordinating incident response and investigation, conducting cybersecurity awareness and educational events for sector stakeholders, and integrating its capability into the larger national cybersecurity ecosystem as applicable.
Indicator	Cybersecurity roles and responsibilities in key entities are communicated internally and to relevant stakeholders including the sectoral supervisory authority.
Factor	**3.1.3Policies and procedures** This factor examines whether key entities have established specific policies and procedures to formalize their cybersecurity governance. Of particular concern is whether these policies and procedures align with cybersecurity requirements coming from LoA1 and LoA2, and whether their implementation and outcomes are monitored.
Indicator	The entity has established cybersecurity policies and procedures. Policies and procedures are communicated to relevant stakeholders, regularly updated and their implementation monitored.
Indicator	The entity is complying with the sector's cybersecurity regulations, requirements, directives, and guidelines (e.g., law on CI protection; requirements on incident reporting for CIs; cybersecurity responsibilities for systematically important entities; voluntary or mandatory baseline cybersecurity performance goals).
Indicator	Top management and/or the Board of Directors is charged with cybersecurity oversight and reviews the entity's cybersecurity program regularly (e.g., annually; bi-annually, etc.).
Indicator	Key entities implement voluntarily cybersecurity good practices even when not required.
Factor	**3.1.4 Budget and spending** This factor examines whether e have access to dedicated financial resources, and if such resources are allocated towards supporting cybersecurity.

Indicator	The entity formally allocates budget to cybersecurity.
Indicator	The budget dedicated to sector cybersecurity is linked to specific cybersecurity goals and related implementation activities.
Indicator	The entity tracks % of expenditures of cybersecurity budget and adjusts the subsequent budgets accordingly.
Dimension	**3.2 Cyber risk management**
Factor	**3.2.1 Asset mapping & Risk Management** This factor evaluates whether key entities have a clear understanding of their assets and their status, particularly their most critical ones, as well as whether they are aware of the potential impact of adverse events on these assets. Furthermore, it assesses whether key entities have a thorough understanding of the interrelationships between their assets, and if this knowledge is regularly updated.
Indicator	The entity maps its assets (software; hardware; data), updates this list on a recurring basis (e.g., monthly) and prioritizes them based on criticality and/or risk level.
Indicator	The entity has developed/adopted a cyber risk management strategy that includes regular (e.g., every 6 months) assessments of the likelihood and impact of an adverse event/attack and the actions to mitigate the risks identified.
Indicator	The cyber risk management strategy adopted by the entity is consistent with the common methodology identified at the sectoral and/or national level to facilitate the exchange of risk information (e.g., standard taxonomies, normalization models, etc.).
Factor	**3.2.2 Situational Awareness & Information Sharing** This factor examines whether key entities monitor pertinent information to comprehend the cybersecurity landscape and context in which they operate and the vulnerabilities of their assets and systems. Moreover, it evaluates the tools and approaches used to conduct such assessments and how their findings are communicated with relevant stakeholders in the sector.
Indicator	The entity regularly performs vulnerability assessments to its assets (especially when new equipment is installed, ports are opened, or services are added).
Indicator	The entity performs penetration tests to identify and validate exploitable pathways, test perimeter defenses, and verify the security of externally available applications.
Indicator	The entity monitors IT and OT environments (when applicable).

Indicator	The entity has established a patch or vulnerability management procedure.
Indicator	The entity established and maintains mechanisms to receive information on known threats, hardware/software vulnerabilities, intrusions, anomalies, and other exploits of interest, and assesses the level of risk.
Indicator	The entity maintains a mechanism to share information about discovered threats, vulnerabilities, or otherwise exploitable assets (including data compromises) with relevant stakeholders (e.g., executives, operations staff, sectoral supervision authority, regulator, sectoral CERT/SOC, other government stakeholders, connected organizations, vendors, sector organizations, s, ISACs).
Indicator	The entity discloses cybersecurity incidents even when not required by existing mandatory regulations.
Dimension	**3.3 Cybersecurity Measures**
Factor	**3.3.1 Implementation of Cybersecurity measures** This factor evaluates the technical and organizational measures that key entities have implemented to mitigate cybersecurity risks. Cybersecurity measures include controls for ID & Access Management, Network Security, Data Protection, Personnel Security, Endpoint Protection, and cyber-hygiene.
Indicator	The entity implements technical and organizational measures to manage digital identities accounts, credentials, and authentication mechanisms of their personnel (e.g., unique accounts; need to know/least privilege/separation of duties principles; provisioning and deprovisioning; strong credential; multifactor authentication; etc.).
Indicator	The entity implements technical and organizational measures to monitor and secure their IT and /OT networks (e.g., segmentation; segregation; IDS/IPS; traffic monitoring; etc.) and the risks coming from their integration, especially when legacy systems are involved.
Indicator	The entity implements technical and organizational measures to protect the data in their systems and ensure their confidentiality (when applicable), integrity and availability (e.g., encryption; DLP measures; regular back up; logical and physical security separation from data source; etc.).
Indicator	The entity implements technical and organizational measures implemented to mitigate the risk of intentional malicious actions posed by personnel or other individuals who have access to the data and systems of the key entities (e.g., personnel screening and monitoring; sanctions; termination; etc.).

Indicator	The entity implements technical and organizational measures to mitigate the risk of unintentional harm caused by personnel or other individuals who have access to the data and systems of the key entities (e.g., basic cyber-hygiene practices; proper configuration; removable media control; license management; purge of dismissed devices; etc.).
Factor	**3.3.2 External dependencies/Supply chain/procurement** This factor examines whether key entities consider cybersecurity risks that could arise from the interconnections with other entities both within and outside of the sector or from the inherent networked nature of certain instruments, such as cloud technologies. Additionally, it evaluates the technical and organizational measures the key entities have implemented to mitigate such risks.
Indicator	The entity's cyber risk management strategy considers risks coming from cross-sectoral interdependencies and has mechanisms in place to manage those risks.
Indicator	The entity's procurement processes include cybersecurity requirements for vendors and/or service providers (e.g., due diligence; third-party audit; certifications; notification of security incidents or vulnerabilities in their assets; etc.).
Indicator	The entity adopts organizational and technical measures to mitigate the risks related to the use of cloud technologies.
Indicator	Key entities require ICT providers to be accredited/certified in cybersecurity before/if procuring hardware, software, digital services, etc. from those vendors.
Dimension	**3.4 Cyber capacity building**
Factor	**3.4.1 Cybersecurity Skills Development, Training & Awareness Raising** This factor examines whether key entities are aware of the skills and capacities that are necessary to reach and maintain higher levels of cybersecurity maturity and evaluate the technical and organizational measures to develop those skills and capacities. It also examines the initiatives and measures taken by key entities to promote cybersecurity awareness across all levels of their organizations, from operational staff to top management.
Indicator	The entity regularly (e.g., annually) carries out training and education initiatives to make sure that all personnel is aligned with the cybersecurity skills and knowledge required by his/her role.
Indicator	The entity regularly (e.g., annually) carries out cybersecurity awareness activities and new employees receive initial cybersecurity training during their onboarding.

Indicator	The entity organizes dedicated cybersecurity awareness training for top management.
Factor	**3.4.2 Foster cybersecurity ecosystem and Cross-Sector cooperation** This factor examines whether the key entities promote or take part in initiatives aimed at fostering cybersecurity research and development and innovation both within and outside of the sector.
Indicator	The entity takes part in PPP initiatives to increase cybersecurity at sector level.
Indicator	The entity takes part in initiatives on cybersecurity or collaboration with academic institutions, NGOs, innovation hubs, professional organizations, international development organizations, etc. To strengthen the sectoral cybersecurity ecosystem.
Indicator	The entity takes advantage of market levers and incentives offered at the national- or sectoral-level to implement/adopt cybersecurity standards and good practices.
Dimension	**3.5 Incident Response & Crisis Management**
Factor	**3.5.1 Incident Response Plan** This factor examines whether key entities have planned their approach to detect, respond to, and recover from cybersecurity incidents. The objective is to comprehend the preparedness of key entities to respond and recover in the event of cybersecurity incidents.
Indicator	The entity has established incident response and disaster recovery plans that outline roles and responsibilities in case of incident/emergency/disaster, an escalation process and clear criteria for their activation (when an incident/emergency/disaster occurs) and de-activation (when an incident/emergency/disaster is resolved).
Indicator	The plan is regularly tested and, when the need arises (e.g., after a test concludes that the plan is not effective), updated.
Indicator	The plan identifies the assets and business processes necessary to sustain minimum operations (given Recovery Time Objective and Recovery Point Objective).
Indicator	OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems (when applicable).

Factor	**3.5.2 Incident Management** This factor examines the measures that key entities put in place to detect, respond to, and recover from cybersecurity incidents. The objective is to comprehend whether key entities have established technical and organizational measures to address cybersecurity incidents and crises, and whether such measures are tested over time to assess their effectiveness. Moreover, it examines whether key entities disseminate knowledge and lessons learned related to incident management.
Indicator	When an incident is detected, there is dedicated personnel (e.g., Incident Response Team) tasked with analyzing (incident triage) and classifying the incident according to pre-defined taxonomy and scenarios, and verifying what assets (e.g., information; applications; servers; etc.) have been compromised.
Indicator	In case of incident, the entity operates dedicated personnel with predefined IR roles, including communications with top management.
Indicator	The entity relies on the services provided by external security groups (e.g., national CSIRT, sector CSIRT, SOC, external IT experts, commercial IR service provider, etc.) to identify and respond to incidents.
Indicator	The entity documents and tracks cybersecurity events and incidents to closure.
Indicator	Internal stakeholders (e.g., executives, legal department, etc.) are identified and notified of incidents and response is coordinated accordingly.
Indicator	The entity knows to whom and how to report cybersecurity incidents (e.g., Sectoral supervision authority, regulator, sectoral CERT/SOC, other governmental agencies, law enforcement agencies, sector organizations, vendors etc.) and coordinates response accordingly.