Framework Nazionale per la Cyber Security

www.cybersecurityframework.it

Roberto Baldoni

baldoni@dis.uniroma1.it

@robertobaldoni

Cyber Security National Laboratory Director

Consorzio Interuniversitario Nazionale Informatica (CINI)

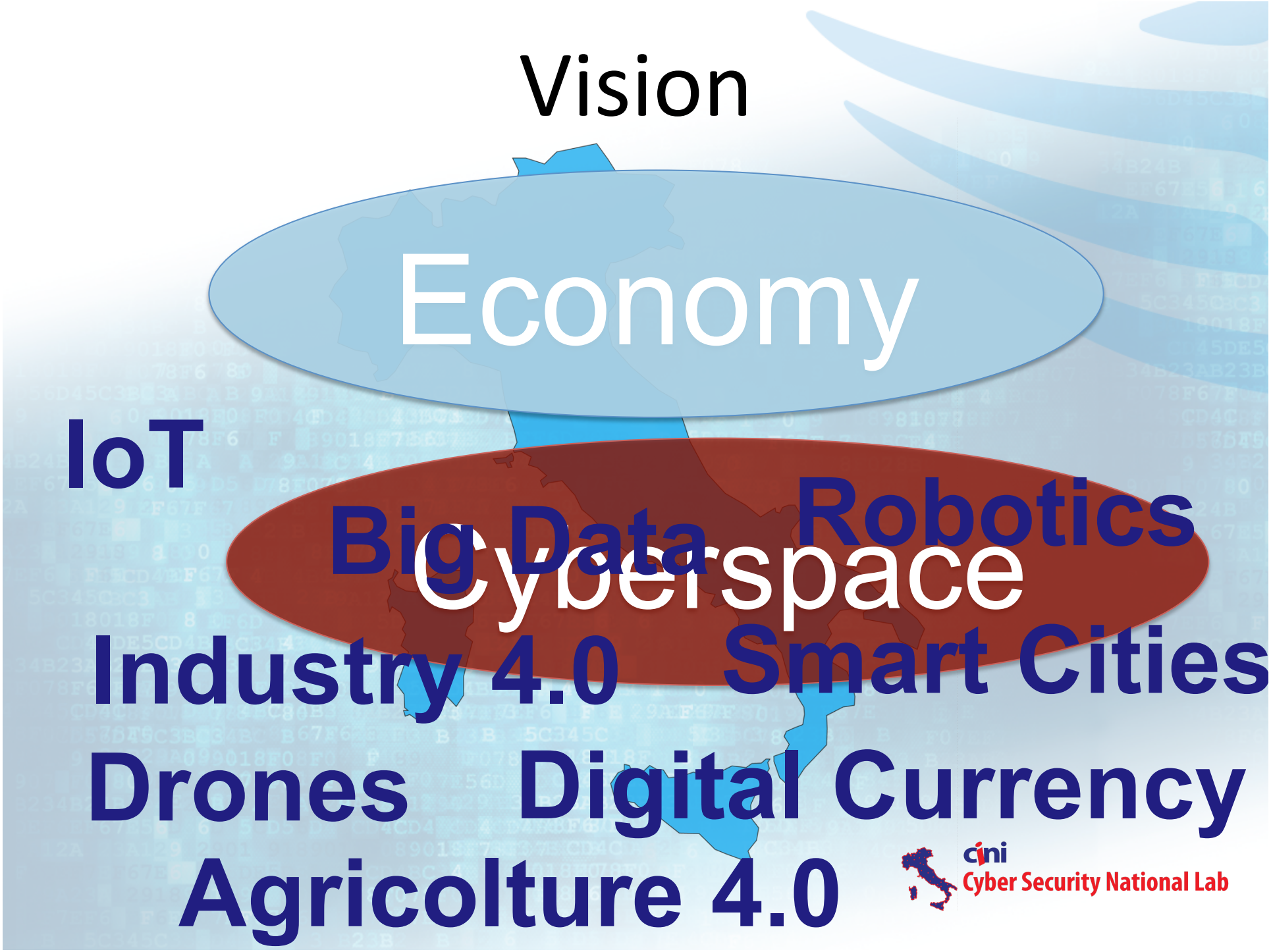
also Director of Research Center of Cyber Intelligence and Information Security

University of Rome La Sapienza

cini

Cyber Security National Lab

Vision


Economy
IoT
Big Data
Robotics
Cyberspace
Industry 4.0
Smart Cities
Drones
Digital Currency
Agricolture 4.0
cini
Cyber Security National Lab

Il concetto di velocità

- La trasformazione economica sarà sempre più veloce, inarrestabile, implacabile cambierà il lavoro, uccidendo vecchi posti e creandone di nuovi
- Cambierà pesantemente gli equilibri tra stati, tra aziende e tra stati e aziende

Economia

Cyberspace

La protezione del Cyberspace è condizione necessaria per la prosperità economica di una nazione

cini
Cyber Security National Lab

Economia

Cyberspace

La protezione del cyberspace non è (solo) un problema tecnico, ma è un problema di business

Cyber Security National Lab

Unicità del Cyberspace

- Non esiste divisione tra pubblico e privato, tra militare e civile. Un ambiente dove tutto è duale!
- Vulnerabilità non numerabili, attacchi in costante aumento per precisione e potenza
- Nessuno può pensare di gestire questa complessità in isolamento

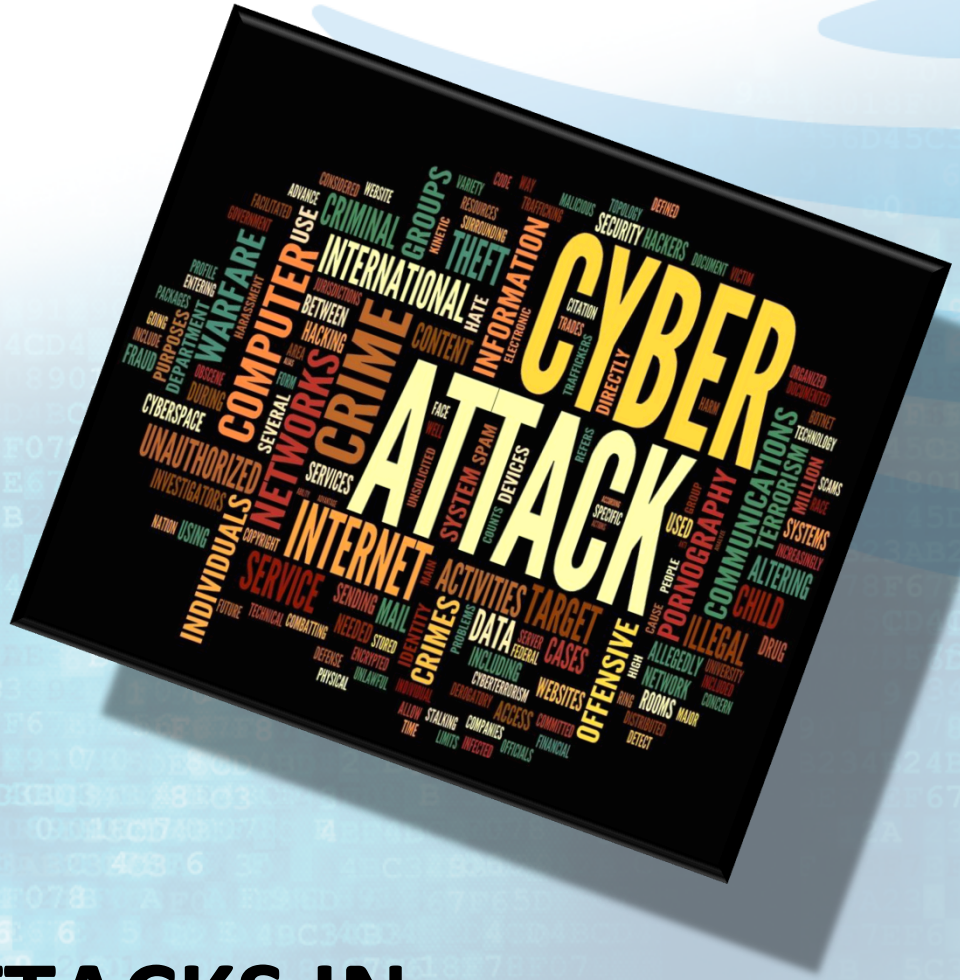
cini
Cyber Security National Lab

Economia

Cyberspace

Risposta come sistema paese alla protezione del cyberspace nazionale

cini
Cyber Security National Lab



2015 TRENDY ATTACKS IN CYBERSPACE

Ramsonware
Denial of service
Cyber espionage
Wiping
Cyber2Physical
Dox(x)ing

cini
Cyber Security National Lab

Ramsc

Denial

Cyber

Wiping

Cyber2Physical

Dox(x

MILITARY

FOR THE SECOND TIME EVER, A CYBERATTACK CAUSES PHYSICAL DAMAGE

IT'S THE DAWN OF A NEW KIND OF WAR

By Kelsey D. Atherton Posted 12 hours ago

35 Shares

ThyssenKrupp

Connect with us

cnet Search CNET Reviews News Video How To Deals US

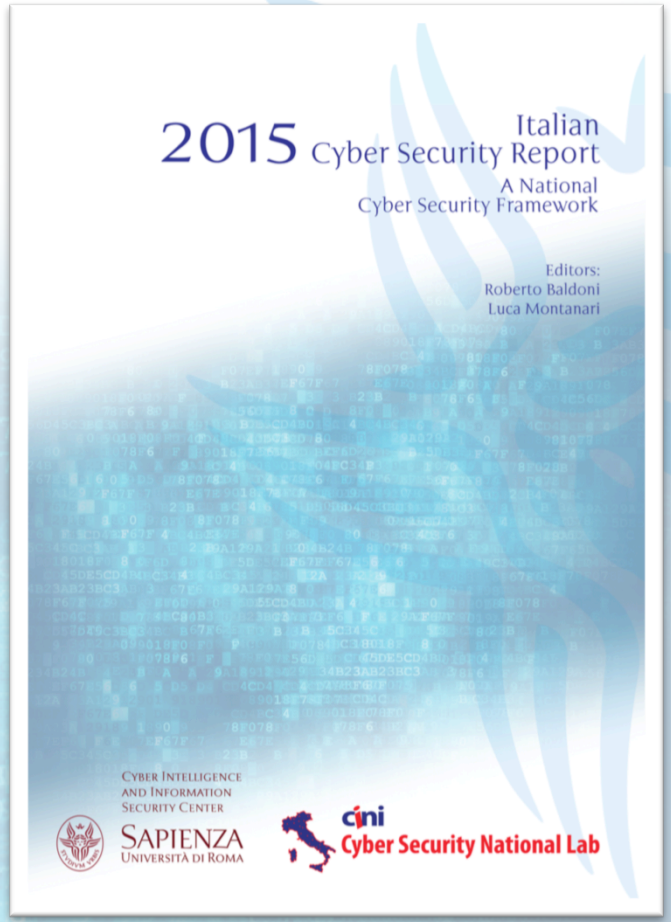
CNET › Security › Ukraine blackout is a cyberattack milestone

Ukraine blackout is a cyberattack milestone

Attacco a Swift

- Conti statunitensi della banca centrale del Bangladesh
- Traferiti attraverso 30 transazioni swift false per un totale di 850M$. Di cui 80M$ scomparsi in una banca filippina
- Truffa avvenuta inserendo operazioni fraudolente nel protocollo swift
- Altre situazioni simili stanno emergendo

cini
Cyber Security National Lab



NATIONAL CYBER SECURITY FRAMEWORK

WWW.CYBERSECURITYFRAMEWORK.IT

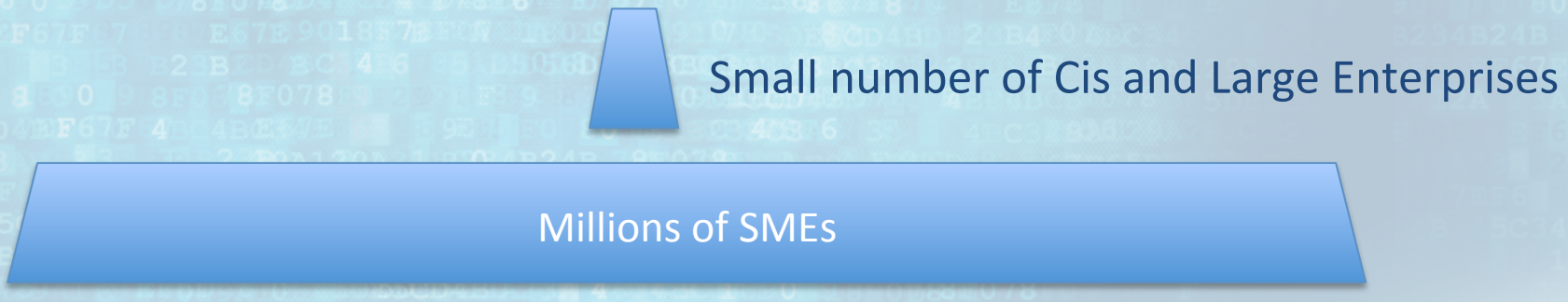
Framework initial objectives

- Bring **cyber risk** in the **executive board** of organizations (not confined to the technical space)
- Approach **cyber risk** as an economic risk (part of the organization's overall **risk management** and decision making processes)

cini
Cyber Security National Lab

Framework initial objectives

- Take **economic landscape** of Italy into account
  - More than 69% of the Gross Domestic Product comes from SMEs



- Usable by SMEs

cini
Cyber Security National Lab

Framework initial objectives

- Be **compliant** with other **international** frameworks and standards in order to improve information sharing and national **duty of care**
- Be compliant with other frameworks and not reinventing the wheel (starting from **NIST Cyber Security Framework** for CI)
- Increase the computer security market helping the structuring of the demand

cini
Cyber Security National Lab

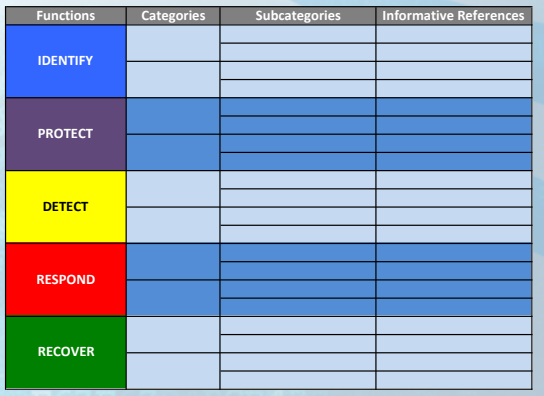
"...it is an important step toward the empowerment of the italian companies irrespective of size and market sector with a strategic self evaluation reference....."

2015 Intelligence report to the Italian Parliament (march2016)

cini
Cyber Security National Lab

From NIST CI Framework to Italian National Framework

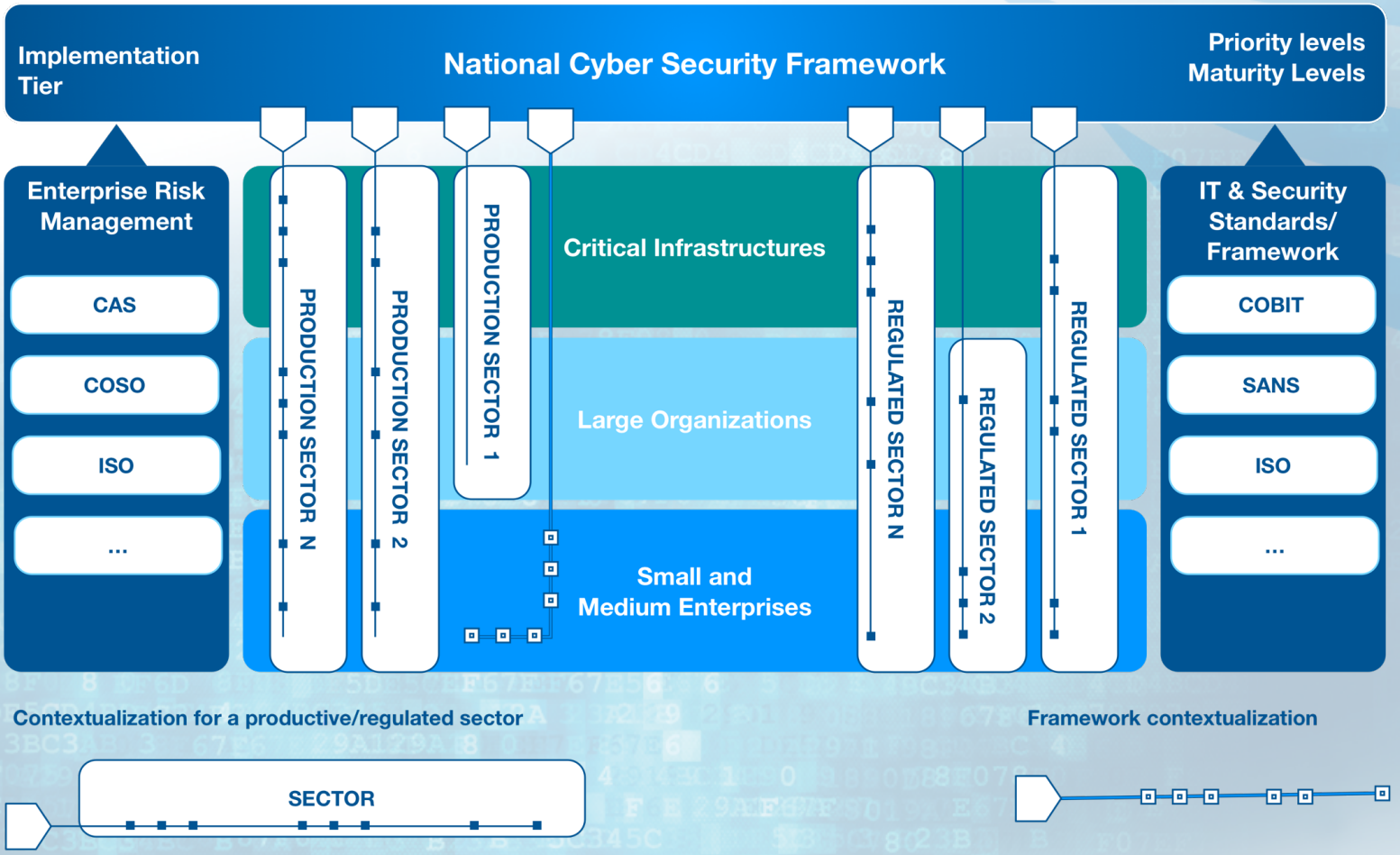
- Implementation tiers
- Framework core
- Profiles



- Priority levels
- Maturity levels
- Some Legal IR
- Guidelines

cini
Cyber Security National Lab

Framework as link between ERM & IT Standards



cini Cyber Security National Lab

6. A Framework contextualization for SMEs

Function	Category	Subcategory	Priority	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**HIGH**	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**HIGH**	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**LOW**	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**NOT SELECTED**	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**MEDIUM**	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. A of CAD**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are	**HIGH**	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	Table 6.1: Assets identification (IA)	Assets inventory, classification and update (intended as information, applications, available systems and equipment) are performed mainly manually according to a defined and controlled process	Assets inventory, classification and update are performed in part in automatic mode that allows at least to automate the "discovery" phase of systems connected to the network, by detecting their characteristics (installed hardware, software, configurations, etc.) and registering the target inventory in a central repository	Inventory, classification and update of assets is done completely in automatic mode, allowing to manage the entire lifecycle of an asset (identification, assignment, status changes, removal, etc.)
	ID.AM-2: Software platforms and applications within the organization are inventoried	Table 6.1: Assets identification (IA)	See ID.AM-1	See ID.AM-1	See ID.AM-1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Table 6.2: Responsibility assignment (AR)	The Company Owner and/or the Top Management designates the representative for Cyber Security, formally defining its tasks. They also establish technical specifications for an adequate use of information and IT tools by all involved parties (e.g.	A Company Policy document for the Cyber Security defining and clearly formalizing roles, responsibilities and activities required to all involved parties, clearly communicating to them the commitment of the Owner and of the Company Top	N/A

Contextualization of the framework

The framework can be “contextualized” by:

- Selecting the subcategories of interest
- Defining priority levels
- Defining maturity levels

According to (for example):

- Organization’s economic sector
- Organization’s size
- Organization’s business
- …

cini
Cyber Security National Lab

1 Introduction and reading guide 1

I PART I – A National Framework

2 The need for a National Framework 9
2.1 The advantages for the Italian context: SMEs, Large Enterprises and sector regulators 10
2.2 Framework and cyber risk management 11
2.3 Advantages for the country system: Towards an international due diligence 11

3 Basics 13
3.1 Framework Core, Profile and Implementation Tier 14
3.2 Priority levels 15
3.3 Maturity levels 17
3.4 How to contextualize the Framework 18
3.5 How to update the Framework 19

4 Guidelines for the implementation of the Framework 21
4.1 Small and Medium Enterprises 21
4.2 Large Enterprises 22
4.3 Critical Infrastructures 25
4.4 Sector regulators 25

II PART II – Framework support documents

5 Framework Core 29

6 A Framework contextualization for SMEs 45
6.1 Selection of Subcategories 45
6.2 Priority levels 46
6.3 Maturity levels 62
6.4 Guidelines to implement high priority Subcategories 70

7 Recommendations for Large Enterprises 79
7.1 The top management role in managing cyber risk 80
7.2 The cyber security risk management process 83
7.3 Computer Emergency Readiness Team (CERT) 86

III PART III – Aspects related to the application context

8 Enterprise Risk Management: reference context 91
8.1 Risk analysis 92
8.2 The advantages of the ERM process implementation 95

9 Cyber risk policies 97
9.1 Risk perception and spread of cyber policies 99
9.2 Guidelines to a cyber risk insurance coverage implementation 100

10 Privacy aspects linked to the Framework 103
10.1 The Privacy Code 103
10.2 Classified information and State secret 106

11 Sector Regulators 109
11.1 Government agencies 109
11.2 Bank and financial sector 111
11.3 Listed companies on regulated markets 113

cini Cyber Security National Lab

Framework come insieme di pratiche di un Duty-of-care per mitigare rischi cyber

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

cini Cyber Security National Lab

6. A Framework contextualization for SMEs

Function	Category	Subcategory	Priority	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**HIGH**	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**HIGH**	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**LOW**	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**NOT SELECTED**	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**MEDIUM**	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. A of CAD**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are	**HIGH**	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1

6. A Framework contextualization for SMEs

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	Table 6.1: Assets identification (IA)	Assets inventory, classification and update (intended as information, applications, available systems and equipment) are performed mainly manually according to a defined and controlled process	Assets inventory, classification and update are performed in part in automatic mode that allows at least to automate the "discovery" phase of systems connected to the network, by detecting their characteristics (installed hardware, software, configurations, etc.) and registering the target inventory in a central repository	Inventory, classification and update of assets is done completely in automatic mode, allowing to manage the entire lifecycle of an asset (identification, assignment, status changes, removal, etc.)
	ID.AM-2: Software platforms and applications within the organization are inventoried	Table 6.1: Assets identification (IA)	See ID.AM-1	See ID.AM-1	See ID.AM-1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Table 6.2: Responsibility assignment (AR)	The Company Owner and/or the Top Management designates the representative for Cyber Security, formally defining its tasks. They also establish technical specifications for an adequate use of information and IT tools by all involved parties (e.g.	A Company Policy document for the Cyber Security defining and clearly formalizing roles, responsibilities and activities required to all involved parties, clearly communicating to them the commitment of the Owner and of the Company Top	N/A

Current cyber profile

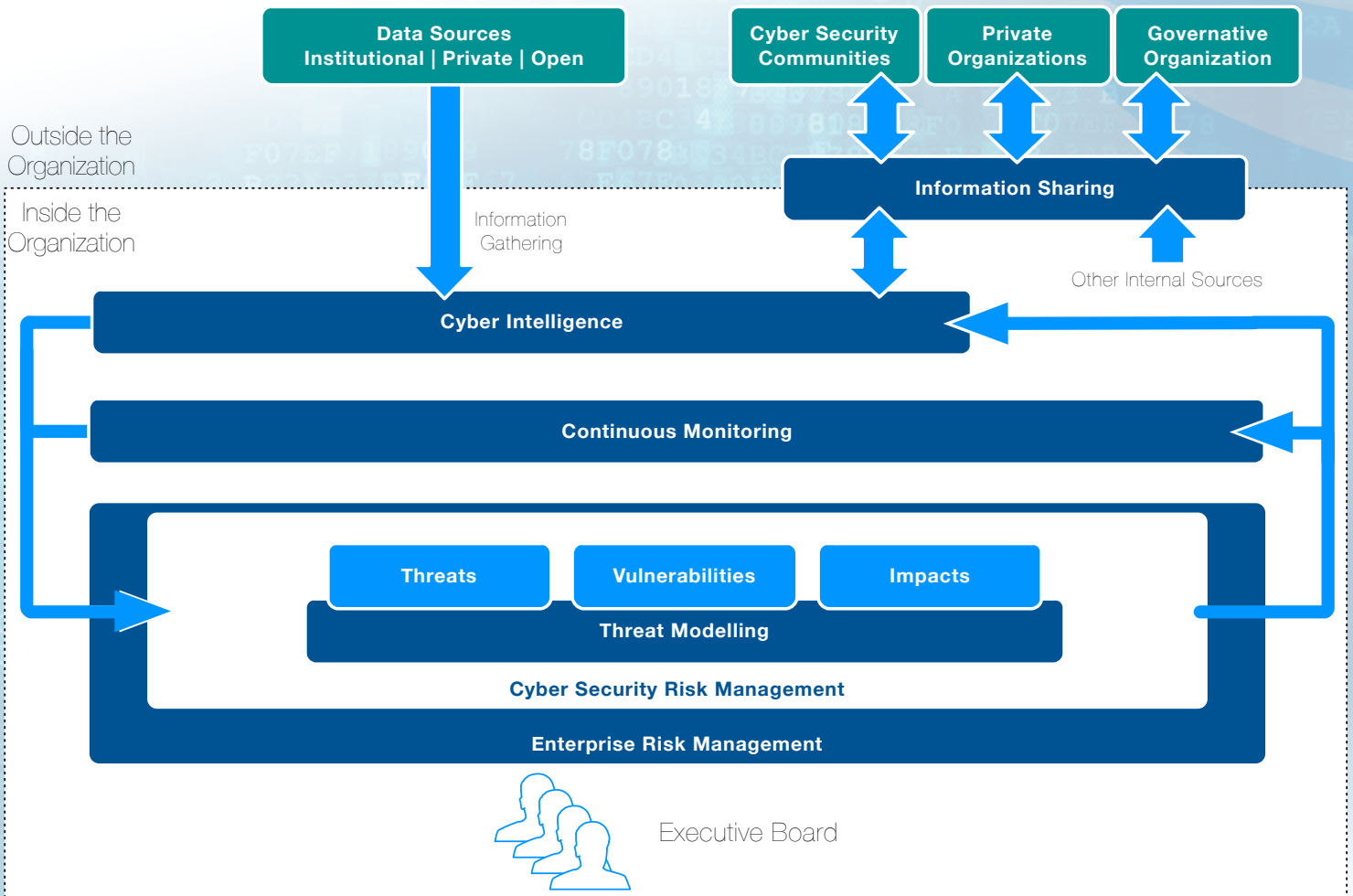
Target profile

National Cyber Security Framework: Advantages for large enterprises

- **Top Management Awareness**
- **Help to prioritize their cyber security actions**
- **Help to create a substainable improvement of cyber security (including cyber insurance)**
- **Protection of the supply chain**

cini
Cyber Security National Lab

Advanced Cyber Risk Management



cini
Cyber Security National Lab

National Cyber Security Framework: Advantages for SMEs

- A contextualization of the framework well suited to SMEs
- 20 quick-wins (similar to cyber essential but coherent with the national framework)
- A guide on how to implement high priority security controls
- Reinforcing the supply chain

cini
Cyber Security National Lab

Advantages for the Nation

- Provide a **common ground** where national authorities can issue regulations in a coherent way e.g.,
  - Autority for Privacy,
  - Agency for digitalization of Italy (AgID)
  - Presidency of ministry council
  - Regulated sector authorities
- **International due diligence**
- **Evaluation** of the cyber risk for the whole nation

cini
Cyber Security National Lab

Realizzato da:

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

Tavolo di lavoro:

AON

Deloitte.

Enel

eni

hermesbay

KPMG

INTELLIUM

In collaborazione con:

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ministero dello Sviluppo Economico

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

CERT nazionale Italia

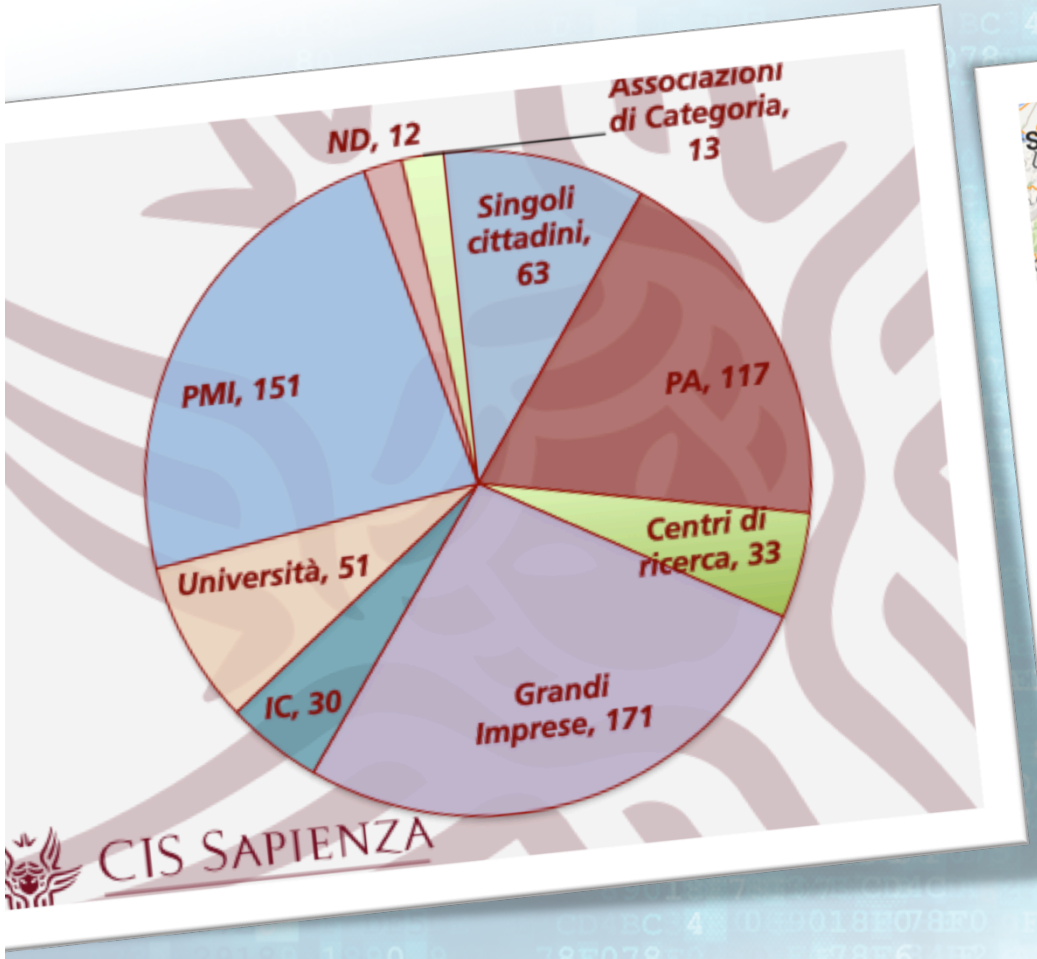
e:

Microsoft

pwc

Con il supporto del Dipartimento delle Informazioni per la Sicurezza della PresidenzaDel Consiglio dei ministri

>1000 Registrazioni alla consultazione pubblica >500 emendamenti ricevuti



Thank you!

www.cybersecurityframework.it

baldoni@dis.uniroma1.it

@robertobaldoni
@CIS_Sapienza
@CyberSecNatLab

cini
Cyber Security National Lab