UN FRAMEWORK NAZIONALE PER LA CYBER SECURITY

Leonardo Querzoni
querzoni@diag.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cyber Security National Lab

CONTESTO NAZIONALE

DPCM
24/1/2013

CONTESTO NAZIONALE

Quadro strategico
e Piano nazionale
27/1/2014

DPCM
24/1/2013

CONTESTO NAZIONALE

DPCM
24/1/2013

Quadro strategico
e Piano nazionale
27/1/2014

Nasce il
CERT nazionale
Giugno 2014

CONTESTO NAZIONALE

DPCM
24/1/2013

Quadro strategico
e Piano nazionale
27/1/2014

Nasce il
CERT nazionale
Giugno 2014

Direttiva PCM
1/8/2015

CONTESTO NAZIONALE

DPCM
24/1/2013

Quadro strategico
e Piano nazionale
27/1/2014

Nasce il
CERT nazionale
Giugno 2014

Direttiva PC
1/8/2015

15/11/2015

CONTESTO NAZIONALE

DPCM
24/1/2013

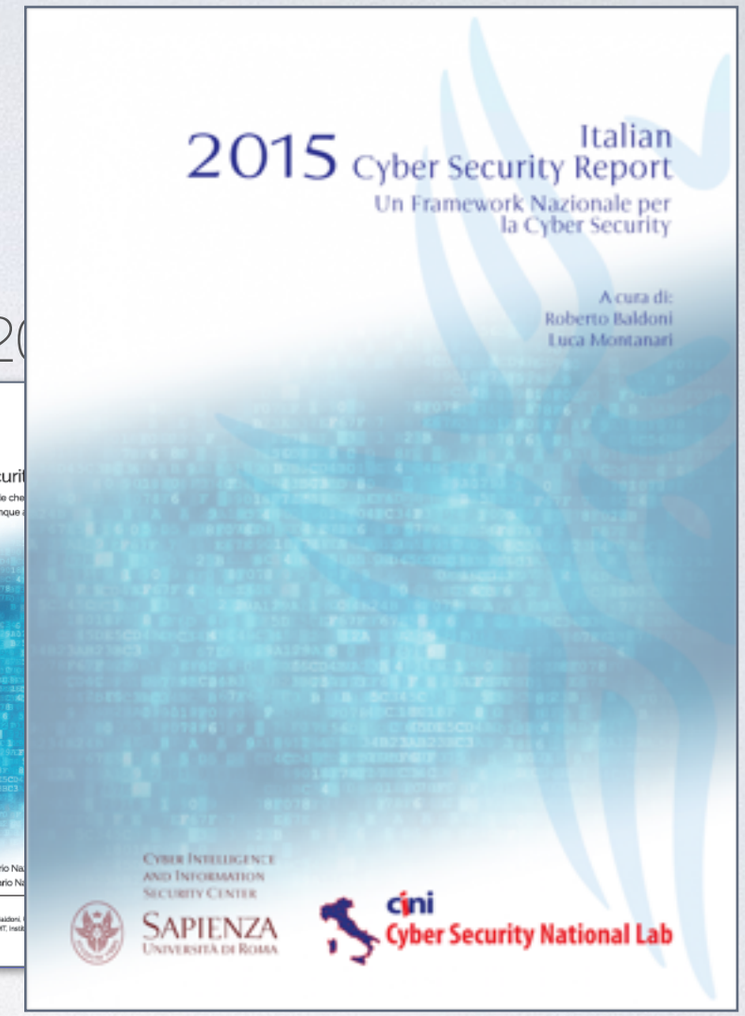
Quadro strategico
e Piano nazionale
27/1/2014

Nasce il
CERT nazionale
Giugno 2014

Direttiva PCM
1/8/2015

15/11/2

4/2/2016



CONTESTO NAZIONALE

DPCM
24/1/2013

Quadro strategico
e Piano nazionale
27/1/2014

Nasce il
CERT nazionale
Giugno 2014

Direttiva PCM
1/8/2015

15/11/

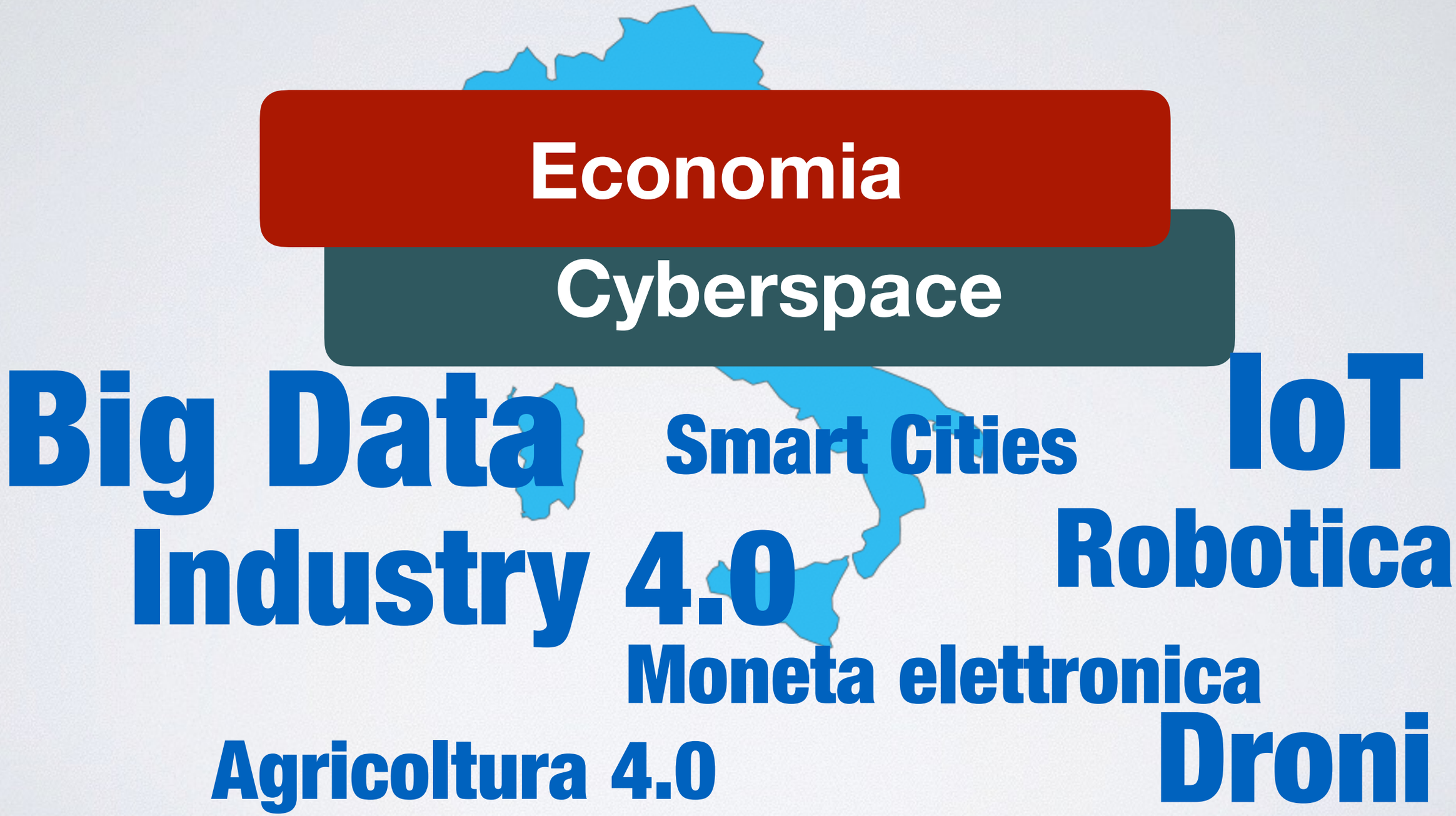
4/2/2016

2/3/2016

VISION DEL PROGETTO

VISION DEL PROGETTO

VISION DEL PROGETTO



VISION DEL PROGETTO

Economia

Cyberspace

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

VISION DEL PROGETTO

Economia

Cyberspace

La protezione del cyberspace non è soltanto un problema tecnico.

OBIETTIVI INIZIALI

1 — Portare il **rischio cyber** sui tavoli dei consigli di amministrazione

- Superare la barriera tecnologica
- Aumentare il livello di consapevolezza del management

OBIETTIVI INIZIALI

2 — Approcciare il rischio cyber come un **rischio economico**

- Consapevolezza dell'impatto economico di un incidente di cyber security
- Gestione integrata nell'*enterprise risk management*
- Superare il limite della *compliance*

OBIETTIVI INIZIALI

3 — Creare un framework adatto al **contesto italiano**

- Un numero limitato di grandi imprese
- Milioni di PMI
  - Più del 69% del PIL
- Strumento flessibile per favorire una ampia adozione

OBIETTIVI INIZIALI

4 — Conforme con altri **standard internazionali**

- Semplificare gli scambi informativi
- Favorire la *duty of care*
- Non reinventare la ruota!
  - Basato sul *NIST Cybersecurity Framework for Critical Infrastructures*

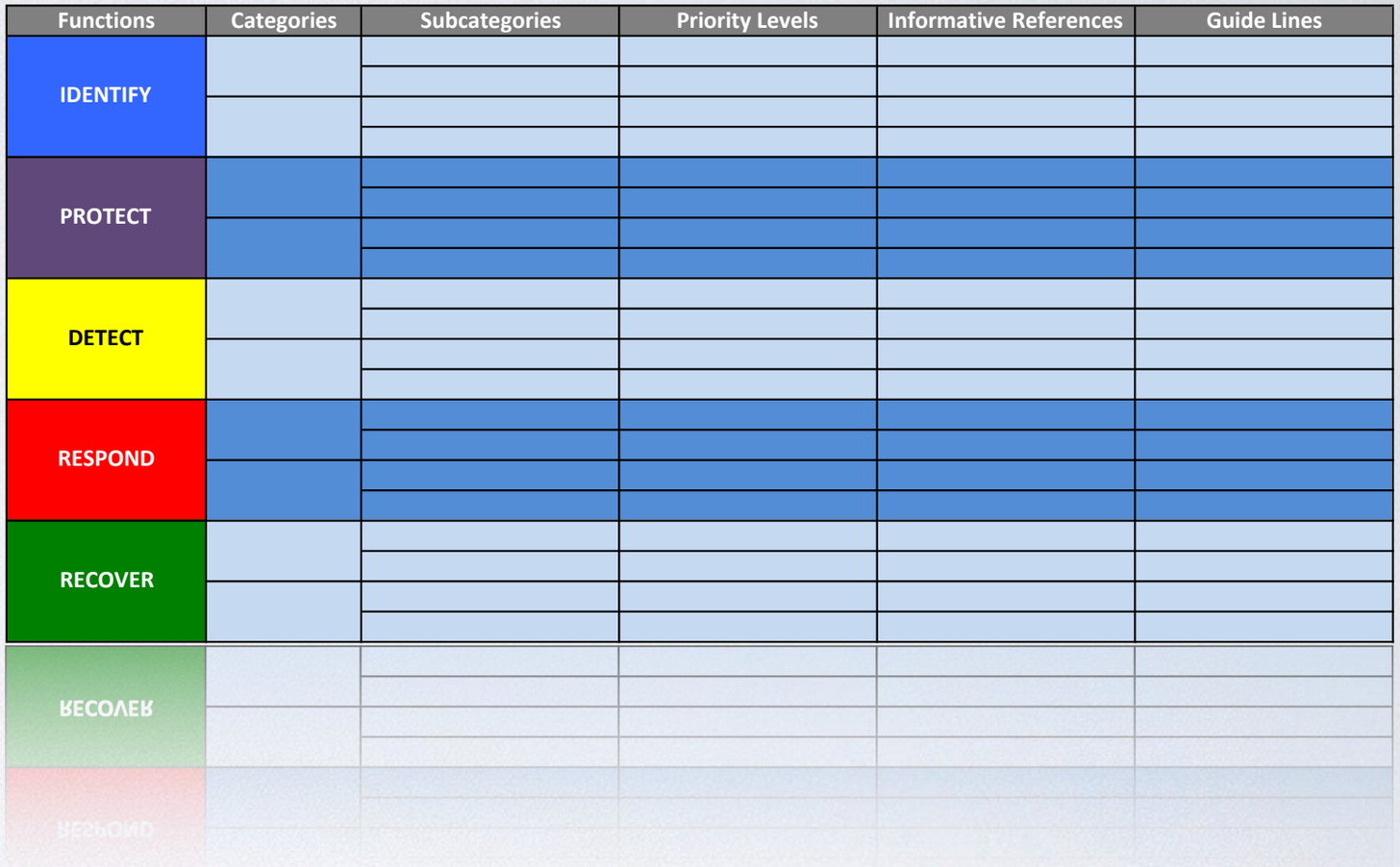
DAL NIST AL FRAMEWORK NAZIONALE

- Framework core
  - Function
  - Categories
  - Subcategories
- Profili
- Implementation tiers

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

DAL NIST AL FRAMEWORK NAZIONALE

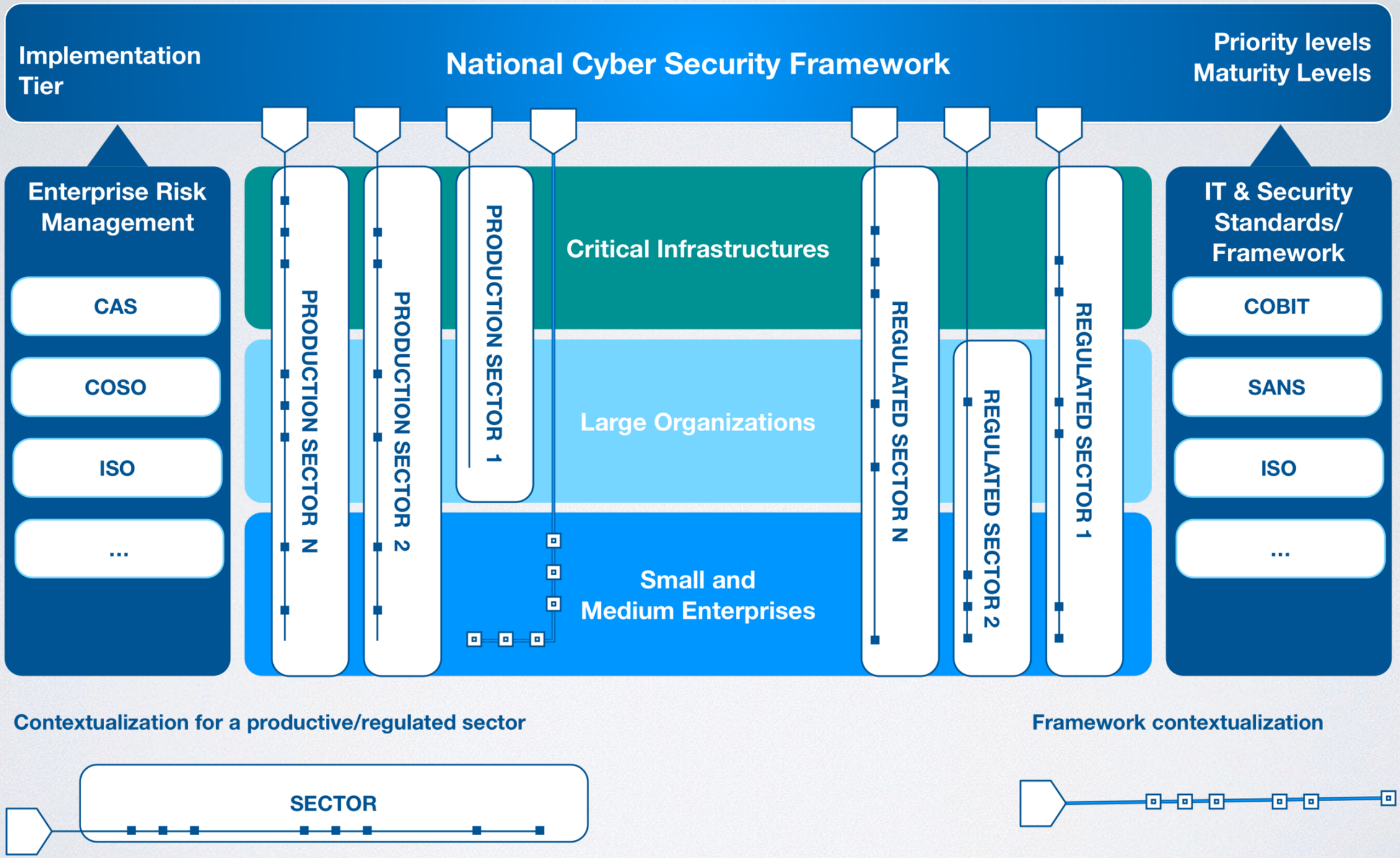
- Framework core
  - Function
  - Categories
  - Subcategories
- Profili
- Implementation tiers
- Livelli di priorità
- Livelli di maturità
- Riferimenti normativi
- Linee guida per l'implementazione



DAL NIST AL FRAMEWORK NAZIONALE

- Framework core
  - Function
  - Categories
  - Subcategories
- Profili
- Implementation tiers
- Livelli di priorità
- Livelli di maturità
- Riferimenti normativi
- Linee guida per l'implementazione

IL FRAMEWORK TRA ERM E STANDARD



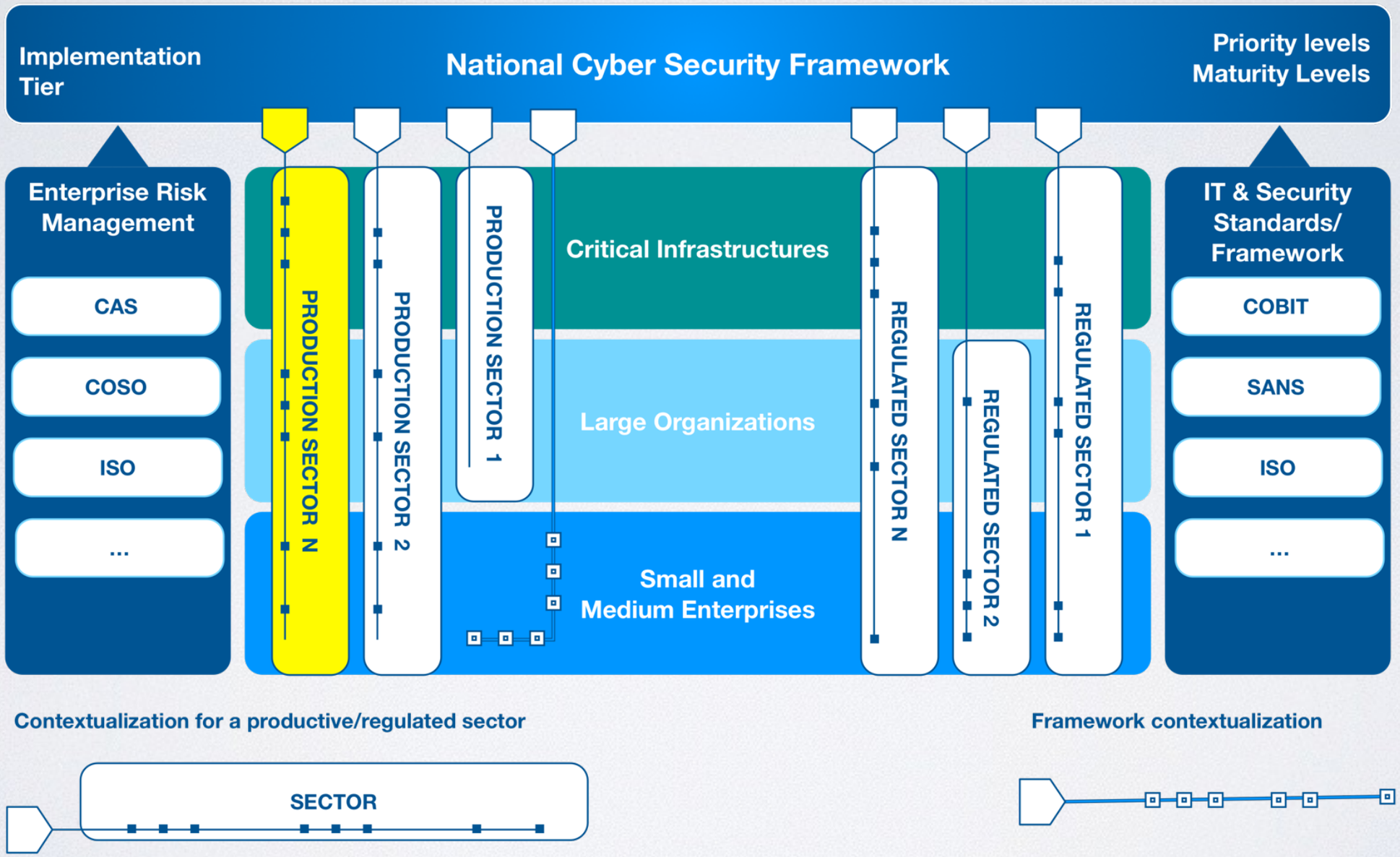
CONTESTUALIZZAZIONI

Il framework per essere applicabile deve essere contestualizzato al dominio di applicazione

- Definizione di un **profilo** tramite selezione delle subcategories
- Identificazione dei **livelli di priorità** nell'implementazione di ciascuna subcategory
- Definizione dei **livelli di maturità** nell'implementazione di ciascuna subcategory

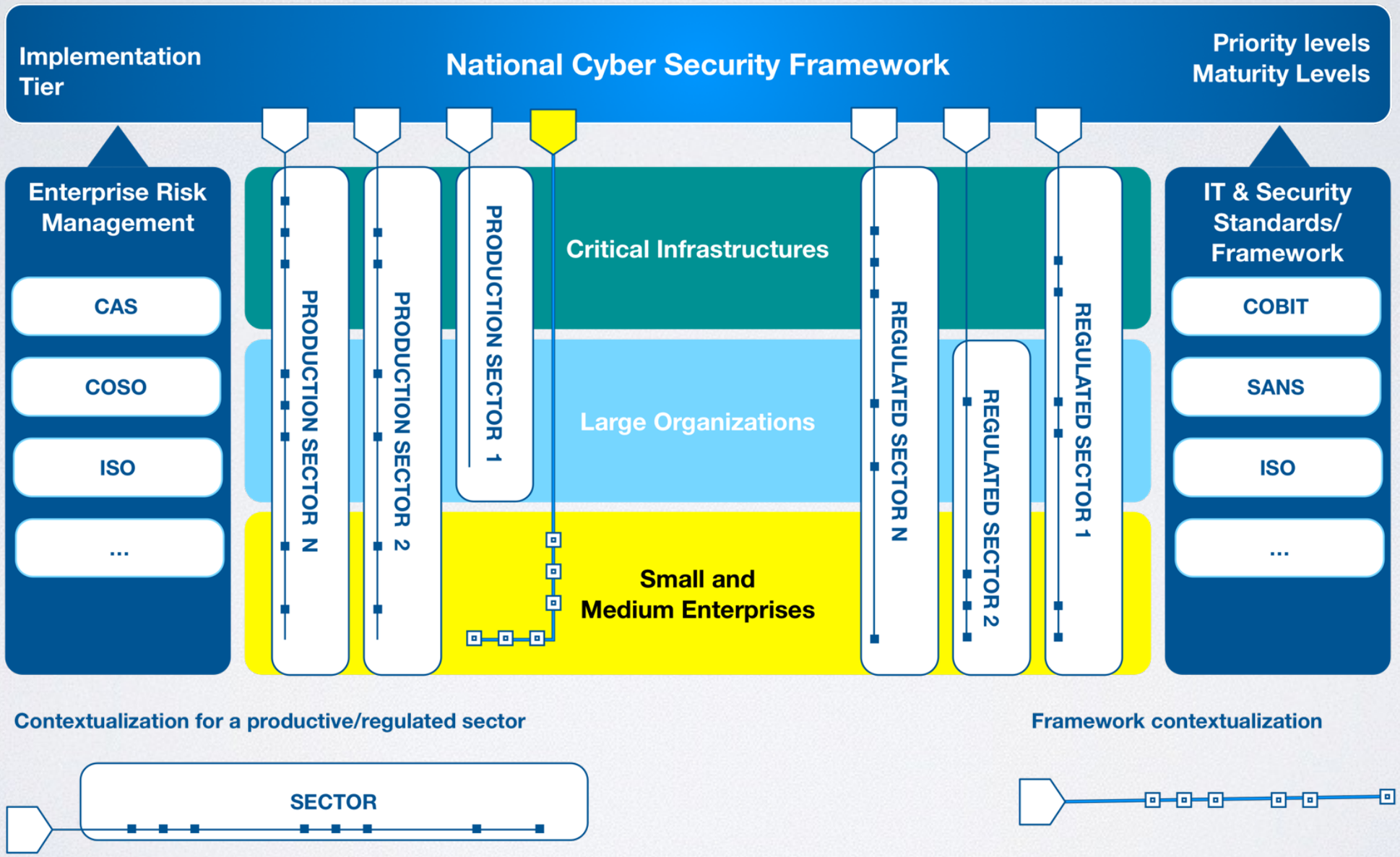
CONTESTUALIZZAZIONI

Contestualizzazione per settore



CONTESTUALIZZAZIONI

Contestualizzazione per dimensione



CONTESTUALIZZAZIONE PMI

Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA	· 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: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA	· 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: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	BASSA	· 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: I sistemi informativi esterni all'organizzazione sono catalogati	NON SELEZIONATA	· 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: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	MEDIA	· 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 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	ALTA	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	MEDIA	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	MEDIA	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	MEDIA	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

CONTESTUALIZZAZIONE PMI

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
IDENTIFY (ID)	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Il censimento, la classificazione e l'aggiornamento degli asset (intesi come informazioni, applicazioni, sistemi ed apparati presenti) avviene in modalità per lo più manuale secondo un processo definito e controllato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema parzialmente automatico, che consenta di automatizzare almeno la fase di "discovery" dei sistemi connessi in rete, rilevando le principali caratteristiche degli stessi (caratteristiche hardware, software installati, configurazioni adottate, ecc.) e registrando l'inventario ottenuto in un repository centralizzato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema completamente automatico, che consenta di gestire l'intero ciclo di vita di un asset (identificazione, assegnazione, cambiamenti di stato, dismissioni)
	ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Vedi ID.AM-1	Vedi ID.AM-1	Vedi ID.AM-1
	ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Tabella 6.2: Assegnazione Responsabilità (AR)	La Proprietà e/o il Vertice Aziendale nomina il referente per la Cyber Security, definendo formalmente le attività in carico. Formalizza inoltre il disciplinare tecnico per l'utilizzo consono delle informazioni e degli strumenti informatici da parte di tutte le parti interessate (e.g. dipendenti, consulenti, terze parti)	Deve essere predisposto un documento di Politica Aziendale per la Cyber Security che definisca e formalizzi chiaramente i ruoli, le responsabilità e le attività richieste a ciascuna parte coinvolta a vario titolo nella gestione della Cyber Security (dipendenti, consulenti, terze parti), comunicando chiaramente l'impegno della Proprietà o dei Vertici Aziendali rispetto a tali necessità	N/A
	ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	Tabella 6.3: Conformità a leggi e regolamenti (CLR)	La conformità a leggi e regolamenti è raggiunta e verificata, anche ricorrendo a specialisti e fornitori esterni, ove ritenuto necessario, in grado di agevolare l'individuazione e la gestione degli aspetti normativi e di conformità, soprattutto quando direttamente o indirettamente connessi con gli aspetti di Cyber Security	N/A	N/A

VANTAGGI PER CHI LO ADOTTA

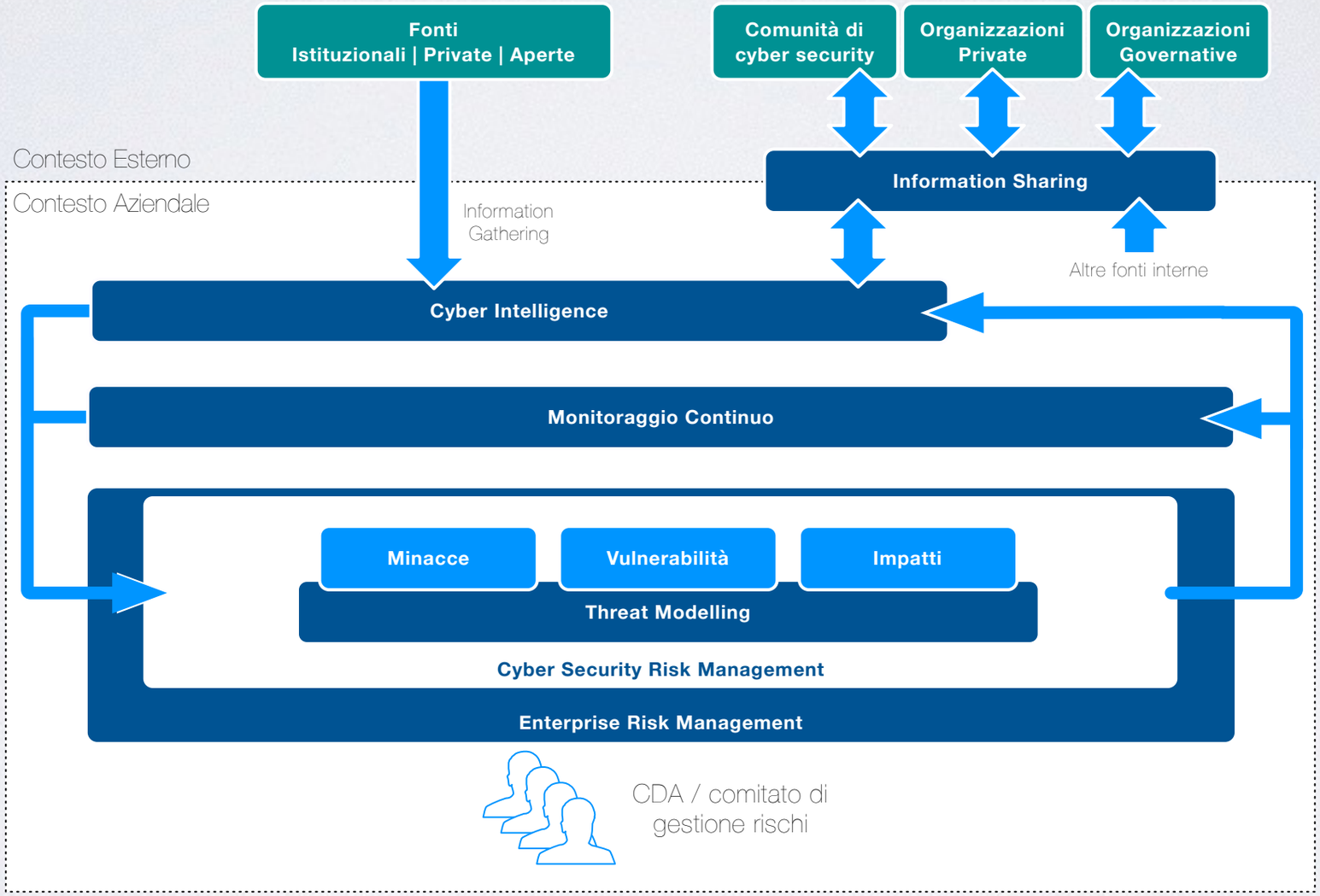
Grandi imprese

- Strumento per la top management awareness
- Permette di definire con quali priorità agire nei confronti del rischio cyber
- Aiuta a pianificare un miglioramento sostenibile nella gestione della cyber security (anche attraverso strumenti assicurativi)
- Semplifica la protezione della catena di approvvigionamento
- Favorisce l'adozione di un processo evoluto di gestione del rischio cyber

VANTAGGI PER CHI LO ADOTTA

Grandi imprese

- Favorisce l'adozione di un processo evoluto di gestione del rischio cyber



VANTAGGI PER CHI LO ADOTTA

Piccole e medie imprese

- Una contestualizzazione del Framework dedicata
- Quick-wins: 20 controlli ad alta priorità
- Guida all'implementazione dei controlli a priorità alta
- Rafforzamento della catena di approvvigionamento

VANTAGGI PER LA NAZIONE

- Fornire un linguaggio comune a diversi soggetti per poter emanare regole in maniera coerente (es.: Garante Privacy, AGID, PCM, ecc.)
- Facilita la *due diligence* internazionale
- Abilita una valutazione complessiva dell'esposizione nazionale al rischio cyber

Il framework può rappresentare un "linguaggio" comune a tutta la nazione nel dominio della cyber security

COME SI USA

- La contestualizzazione può essere definita dal legislatore, da un regolatore di settore, da una associazione di imprese o dal singolo attore che adotta il framework

IL PROCESSO

Prodotto da un team di circa 30 persone appartenenti al settore pubblico e ad imprese private

- CIS - Sapienza
- CINI - Laboratorio Nazionale Cyber Security
- Presidenza del Consiglio dei Ministri

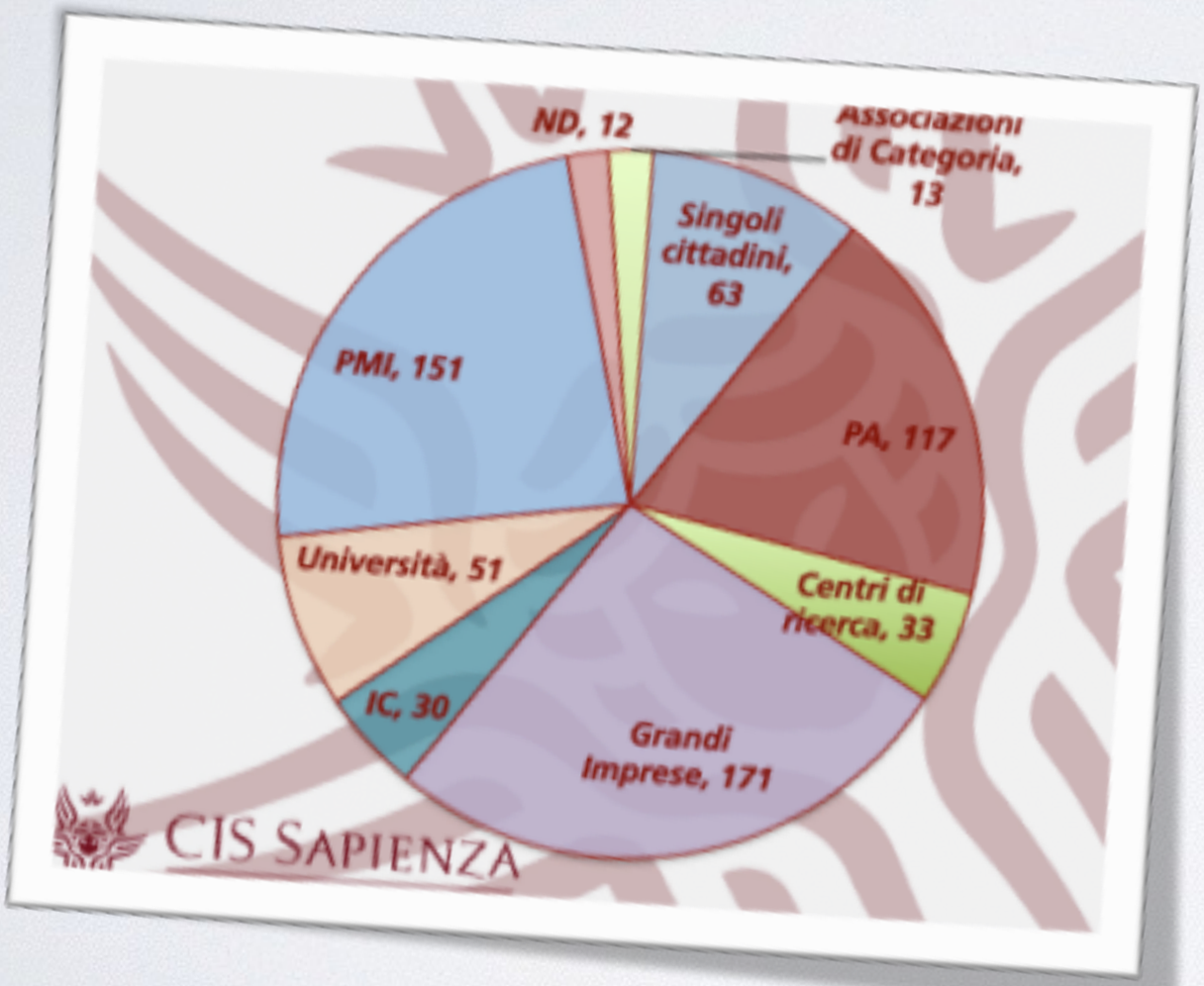
- AGID
- Garante della Privacy
- Ministero dello Sviluppo Economico
- CERT Nazionale

- Panel di imprese

IL PROCESSO

Consultazione pubblica

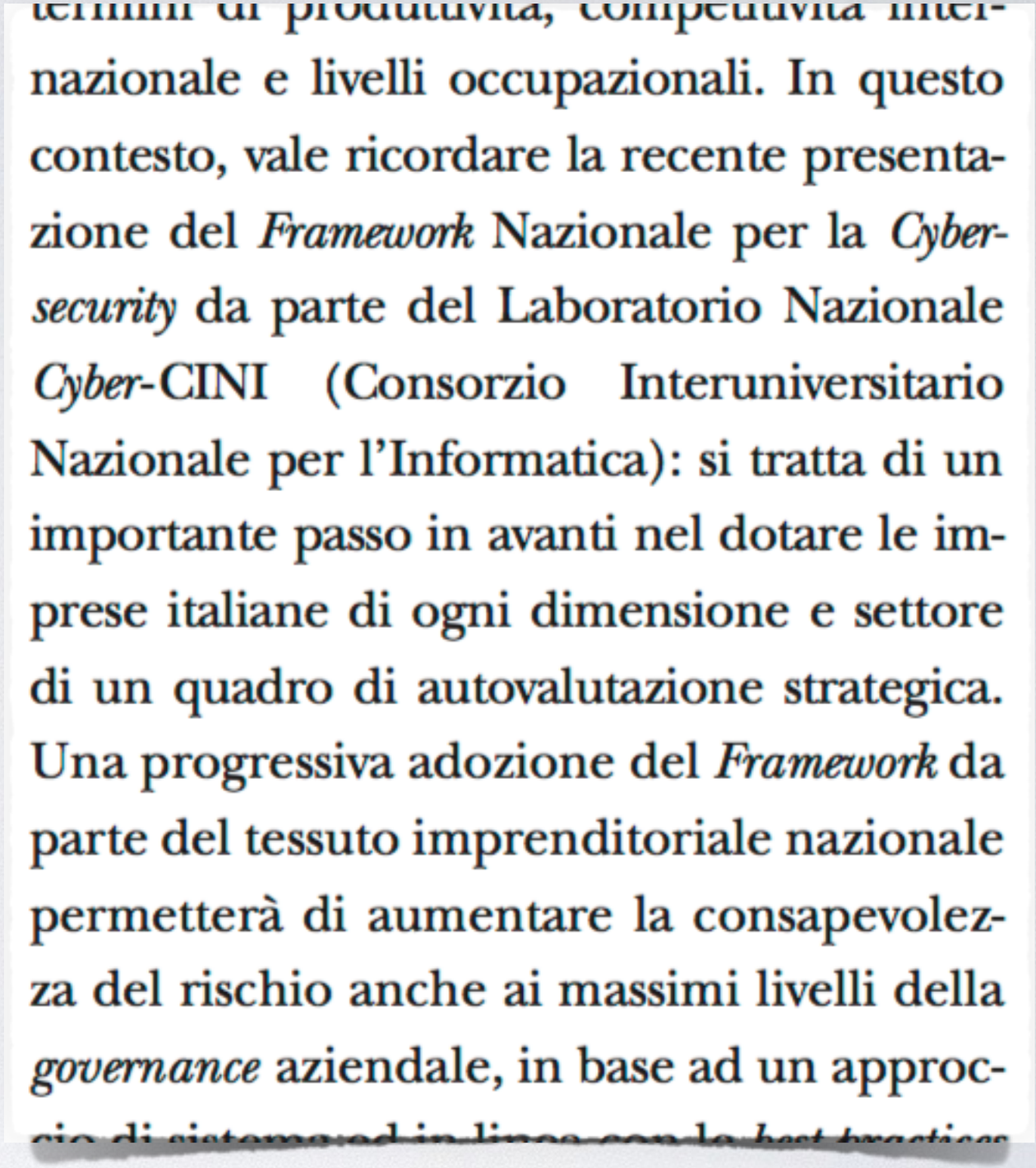
- 2000 download
- 500 emendamenti suggeriti (di cui 300 implementati)



CONCLUSIONI

Il framework è riconosciuto come un importante contributo al miglioramento della gestione del rischio cyber in Italia.

(fonte: Relazione sulla politica dell'informazione per la sicurezza – 2015)


nazionale e livelli occupazionali. In questo contesto, vale ricordare la recente presentazione del *Framework* Nazionale per la *Cyber-security* da parte del Laboratorio Nazionale *Cyber*-CINI (Consorzio Interuniversitario Nazionale per l'Informatica): si tratta di un importante passo in avanti nel dotare le imprese italiane di ogni dimensione e settore di un quadro di autovalutazione strategica. Una progressiva adozione del *Framework* da parte del tessuto imprenditoriale nazionale permetterà di aumentare la consapevolezza del rischio anche ai massimi livelli della *governance* aziendale, in base ad un approc-

CONCLUSIONI

È in corso una fattiva collaborazione con il NIST

- Presentazione del framework nazionale a Washington

Il framework è un documento vivo che andrà aggiornato periodicamente per adeguarlo agli inevitabili mutamenti di scenario

- Aggiornamenti tecnici
- Nuove contestualizzazioni

WWW.CYBERSECURITYFRAMEWORK.IT

Leonardo Querzoni
querzoni@diag.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cyber Security National Lab