Cyber Risk Management: Come prevenire e fronteggiare gli attacchi cibernetici

Open Banking alla prova della sicurezza

Roberto Baldoni
baldoni@dis.uniroma1.it

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

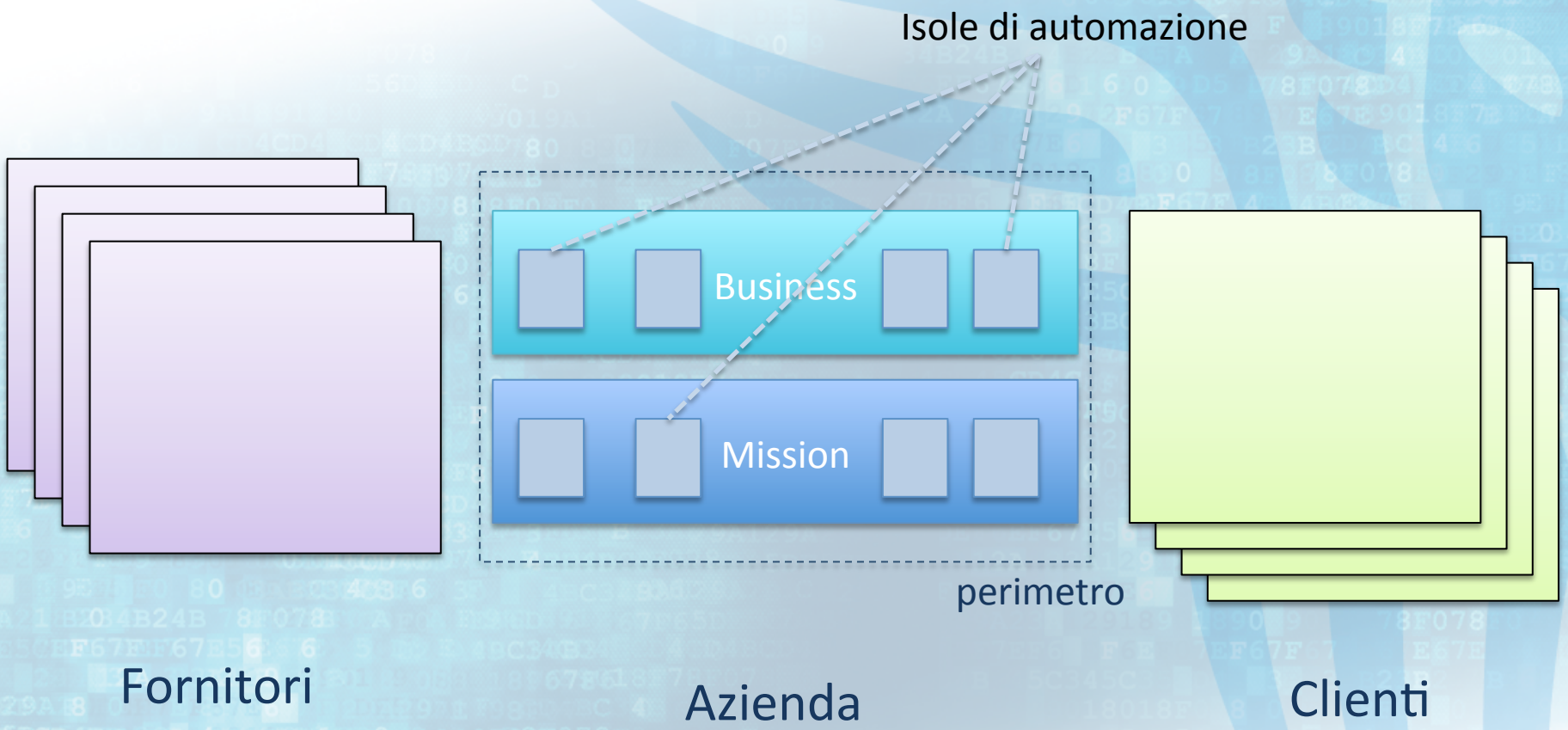
cini Cybersecurity National Lab

Comitato Nazionale Ricerca in Cybersecurity

Milano, 24 Novembre 2017

LA TRASFORMAZIONE DIGITALE

prima del 1993

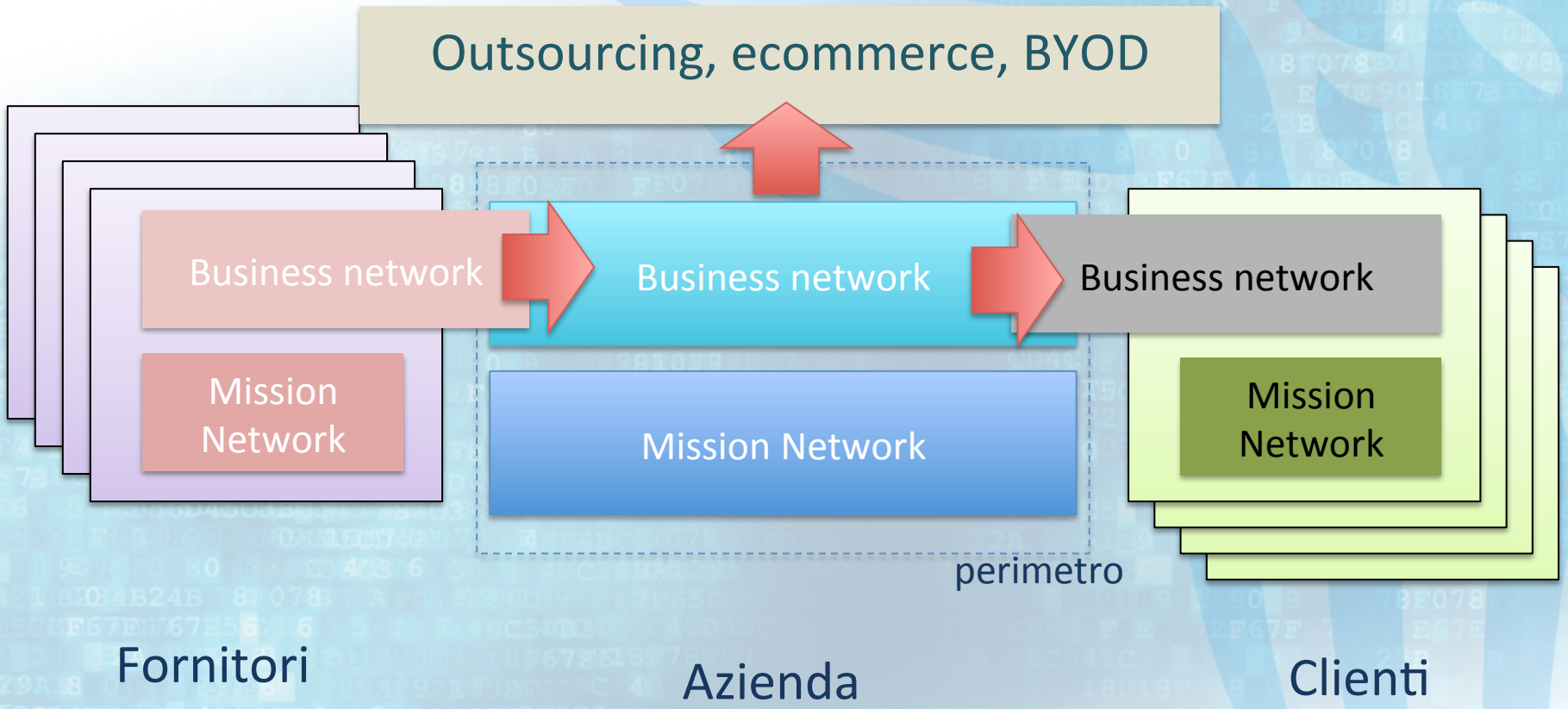


1993-2000: platform and network integration

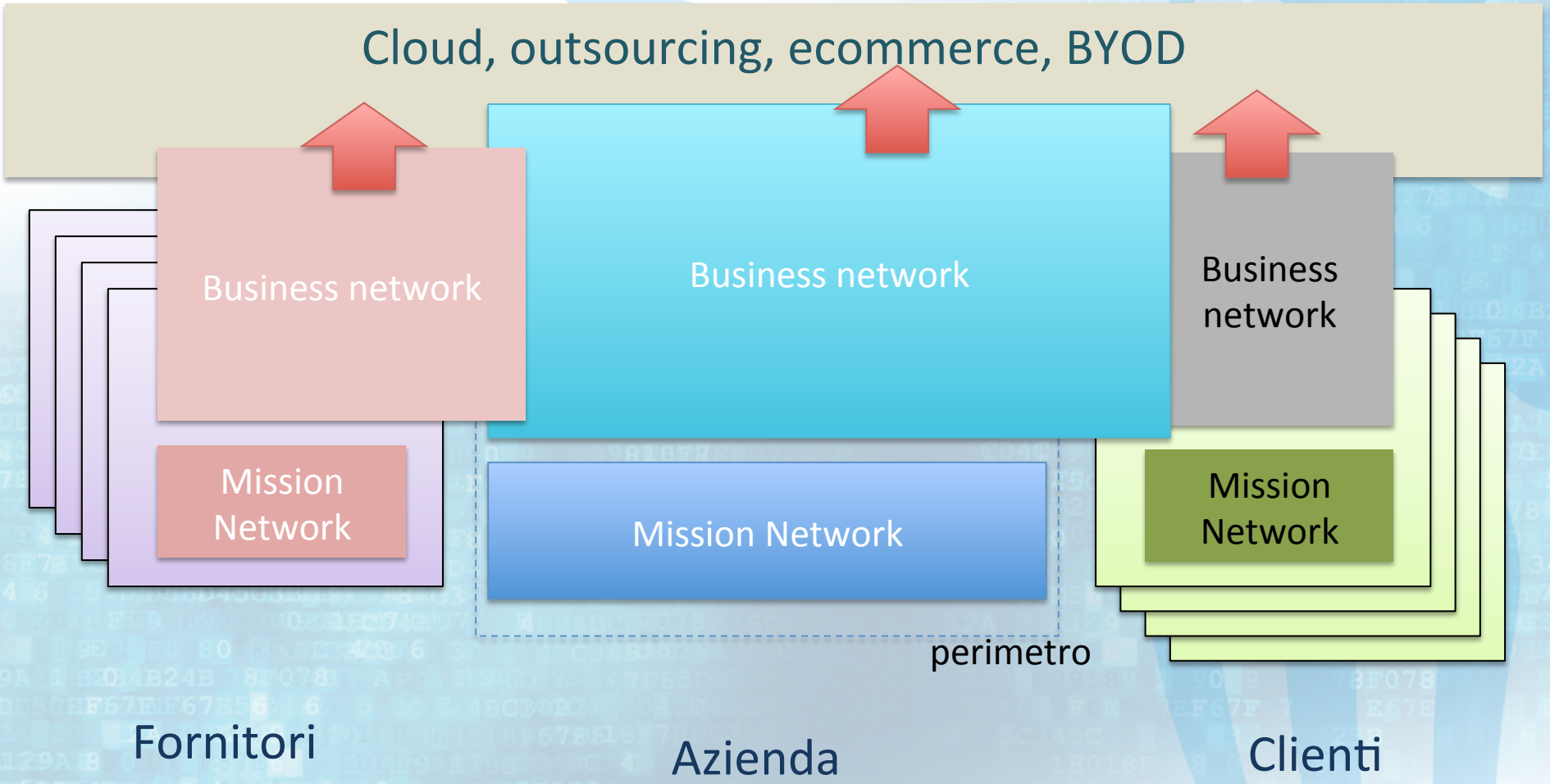
- ANSA
- CORBA
- Publish-Subscribe
- RPC

Middleware

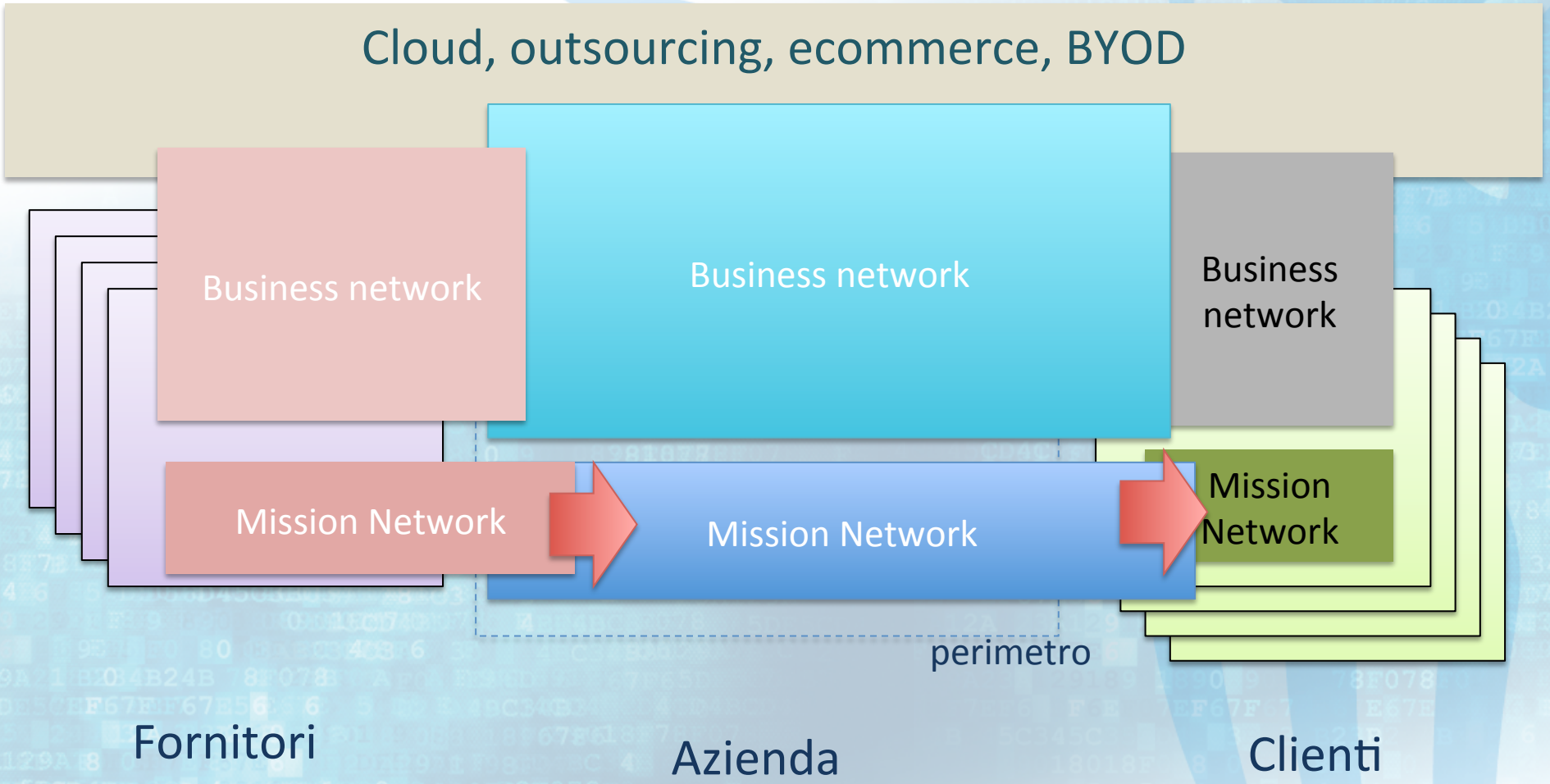
2000-oggi: web services, third parties, ecommerce, BYOD



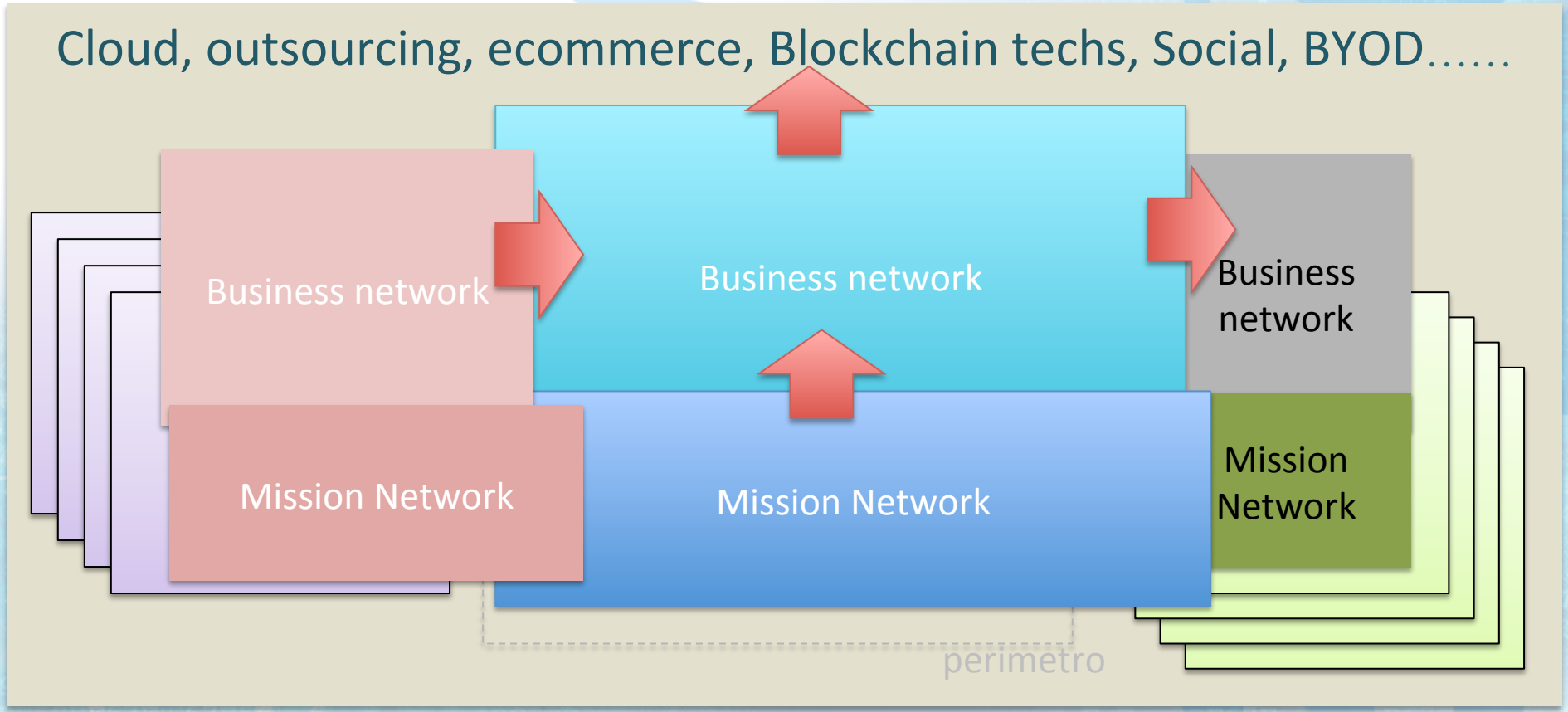
2010-oggi: cloud computing



2015-oggi: cyber-physical systems



Futuro: AI, Pervasive Robotics, IoT, Bigdata, Blockchain



Fornitori

Azienda

Clienti

Application Layer

Smart Home

Smart City

Smart Industry

Smart Building

Smart Transportation

Smart Health

Transmission Layer

Wi-Fi

Bluetooth

Access Point

Router

The Internet

LAN

Perception Layer

Sensors

RFID

Actuators

GPS

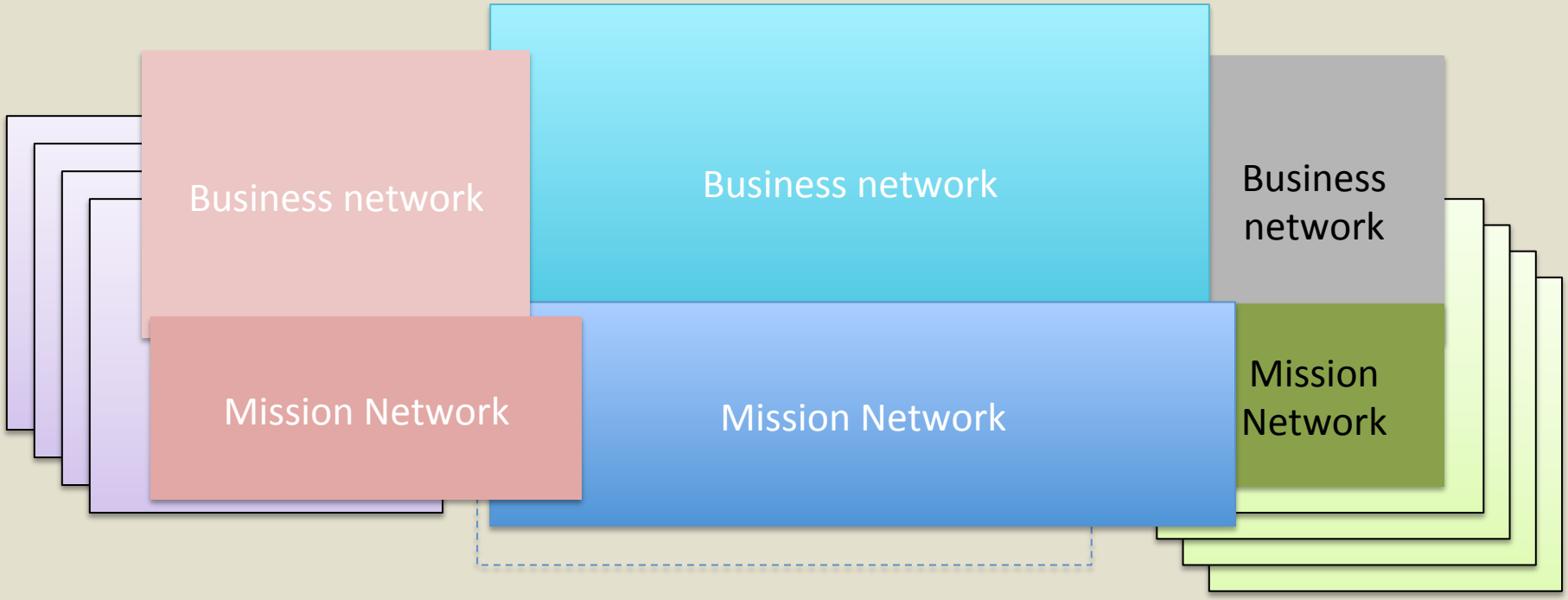
100 miliardi di dispositivi per il 2020

1 miliardo di dispositivi per il 2020 in Italia

Ogni elemento che si connette al cyberspace introduce tra 10 e 100 vulnerabilità conosciute. Numero che aumenta nel tempo

Dove è la Cybersecurity in questo scenario?

Cloud, outsoucing, ecommerce, BYOD, Blockchain techs, Social, ...



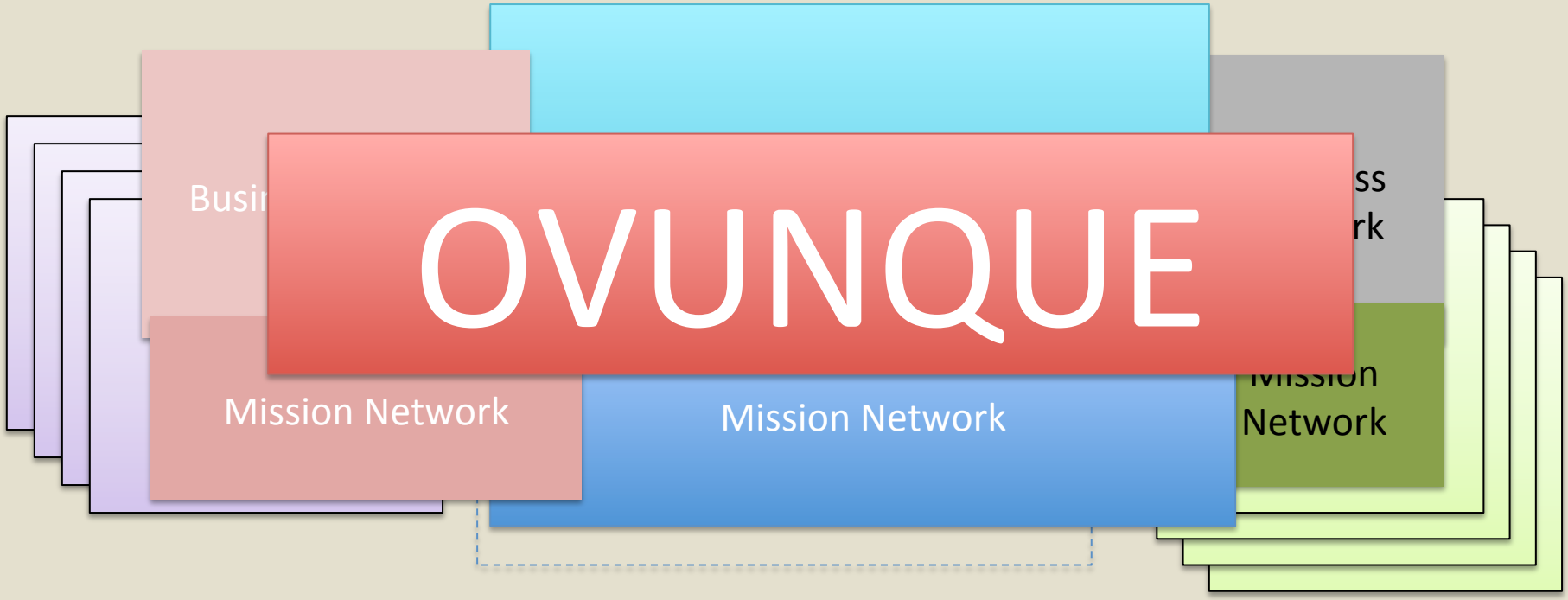
Fornitori

Azienda

Clienti

Dove è la Cybersecurity in questo scenario?

Cloud, outsoucing, ecommerce, BYOD, Blockchain techs, Social, ...



Fornitori

Azienda

Clienti

Ogni cosa ha a che fare con la cybersecurity (multidimensionalità)

- CPUs
- Software
- Smart devices
- Computers
- Fattore Umano

- Aziende
- Processi
- Organizzazione
- Catena di Appovigionamento
- Contratti
- ……

Every piece/layer is concerned by cybersecurity

- CPUs
- Software
- Smart devices
- Computers
- Humans
- Enterprises
- Processes:
  - Design
  - Organization
- Supply Chain
- ……

Aggregazione e coordinamento in un continuo processo di gestione del rischio informatico

Architettura Governativa

cini Cybersecurity National Lab

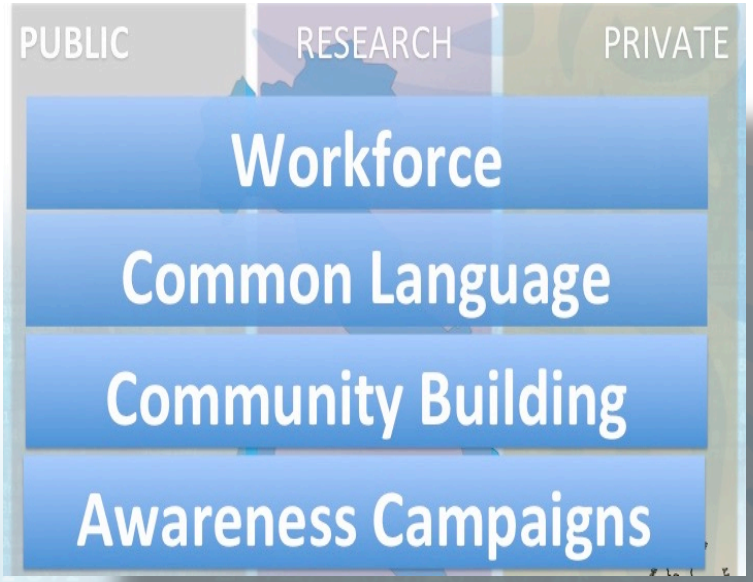
Ricerca

Finanza

Confindustria

CERTFin
CERT Finanziario Italiano

cini Cybersecurity National Lab



FRAMEWORK NAZIONALE PER LA CYBERSECURITY

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cybersecurity National Lab

Nascita del Framework

INDIRIZZO OPERATIVO 7

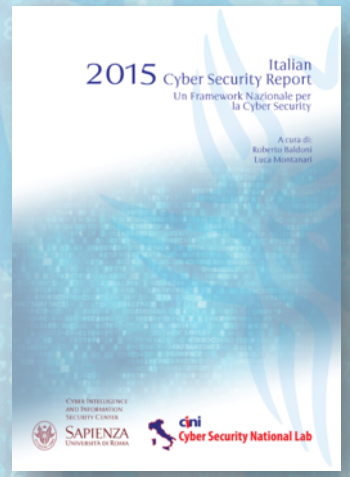
COMPLIANCE A *STANDARD* E PROTOCOLLI DI SICUREZZA

La compliance *a* standard *e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.*

7.2 ***Documenti di riferimento***

a. Elaborare e pubblicare documenti di riferimento quali manuali, elenchi di procedure *standard* e raccomandazioni (*best practices* di settore), tassonomia e lessico uniforme da utilizzare per lo scambio di informazioni

Nascita del Framework



2014 → 2015

- Strategia Nazionale 27/12/2013
- Definizione degli obiettivi
- Definizione del tavolo di lavoro
- Allargamento del tavolo a imprese e PA (PPP)
- 4 Febbraio 2016

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

Alcuni Obiettivi iniziali

- **Portare la consapevolezza del rischio cyber ai massimi livelli aziendali**
  - portare le organizzazioni a considerare il rischio cyber come rischio economico parte del risk management
  - Allargare il mercato della sicurezza informatica Italiana
- **Considerare il panorama economico italiano**
  - 69% del PIL prodotto da Piccole-Medie Imprese
  - Pochissime grandi imprese nazionali, 0,1%

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

- Non è uno standard
- Permette di definire il proprio **profilo attuale** e il **profilo target**
- Aiuta nella definizione della **roadmap** per passare dal profilo attuale al profilo target

Framework Nazionale per la Cybersecurity

- Framework core
- Profiles

Abbiamo Aggiunto:

- Livelli Priorità*
- Livelli di Maturità*
- Linee Guida*
- Riferimenti normativi (CAD, GPDR, NIS, altro*)
- Metodologia di contestualizzazione

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

*validi per nell'ambito della contestualizzazione

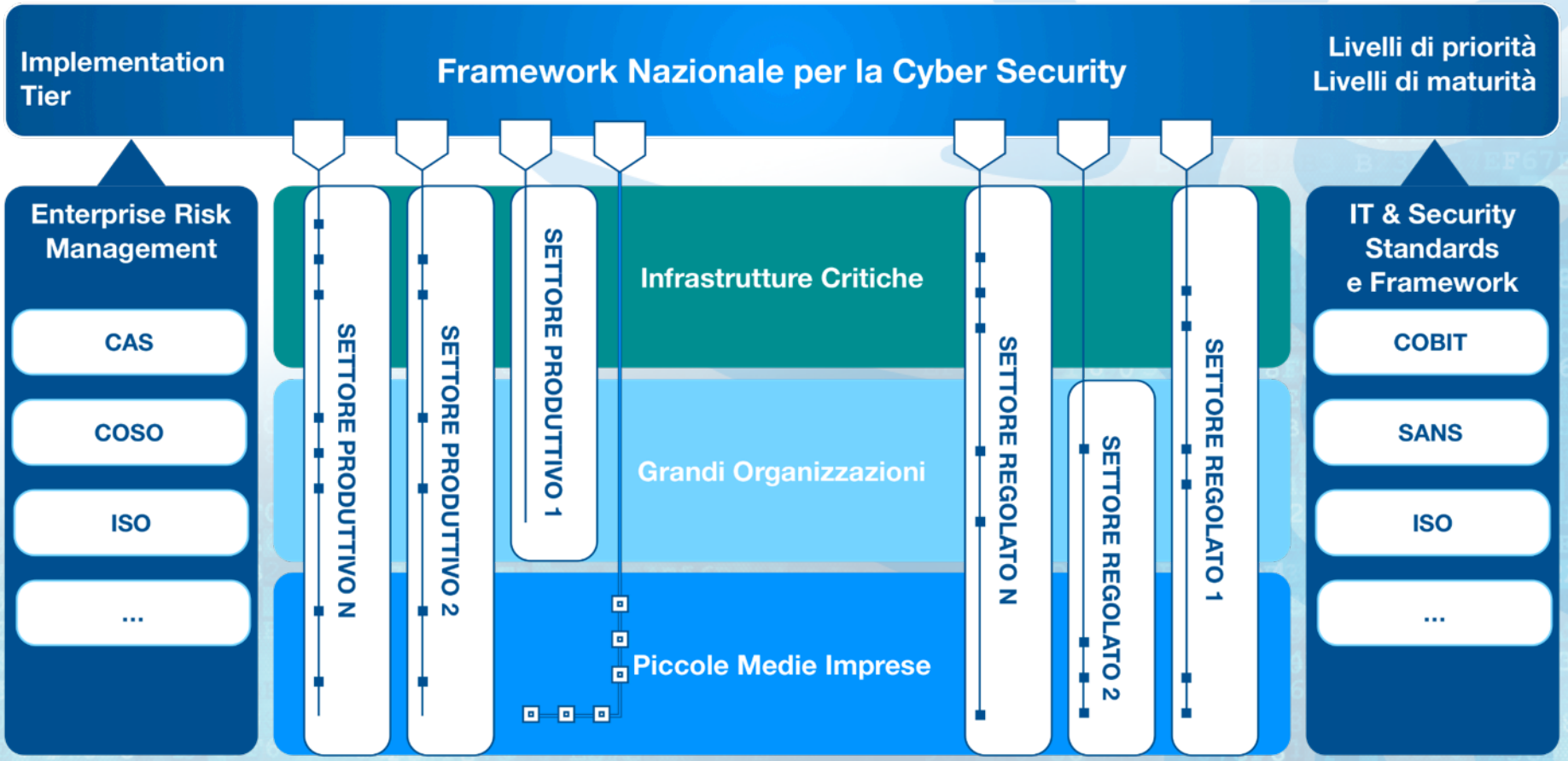
Framework Nazionale per la

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

Contestualizzazioni

Il Framework può essere ”customizzato” tramite:

- la **selezione** delle Subcategory
- **definizione** di livelli di **priorità** per ogni subcategory
- **definizione** livelli di **maturità** per ogni subcategory



Contestualizzazione per un settore produttivo/regolato

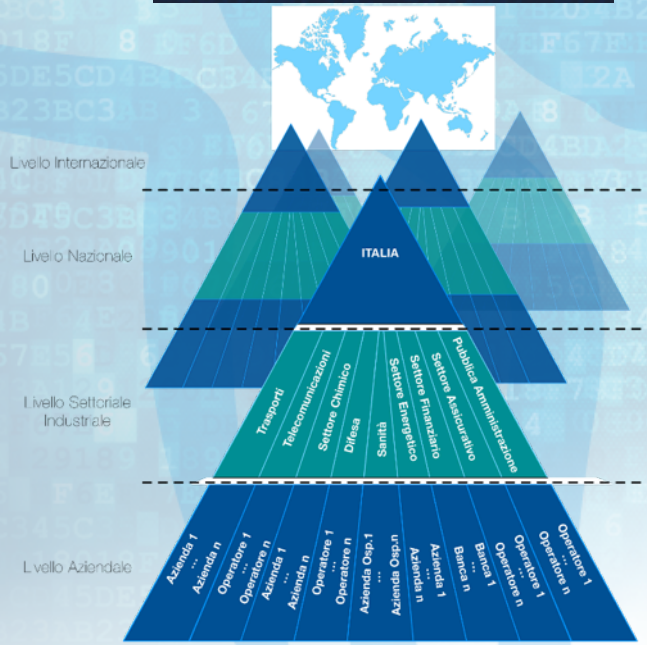
Contestualizzazione del framework

Vantaggi per le grandi imprese

- Strumento per la **top management awareness**
- Un aiuto a definire **piani di spesa** per la gestione del rischio cyber
- Gestione della **catena di approvvigionamento**
- Strumento per rafforzare/rivedere la gestione del **rischio cyber**
- Strumento di **comunicazione** con le altre imprese

Vantaggi per la Nazione

- Fornire un **linguaggio comune** a diversi soggetti in modo da poter emanare regole in maniera coerente e.g.,Garante Privacy, AGID, PCM, ecc.
- **Internazionalità** del framework (US, Japan, Italy, Israel)



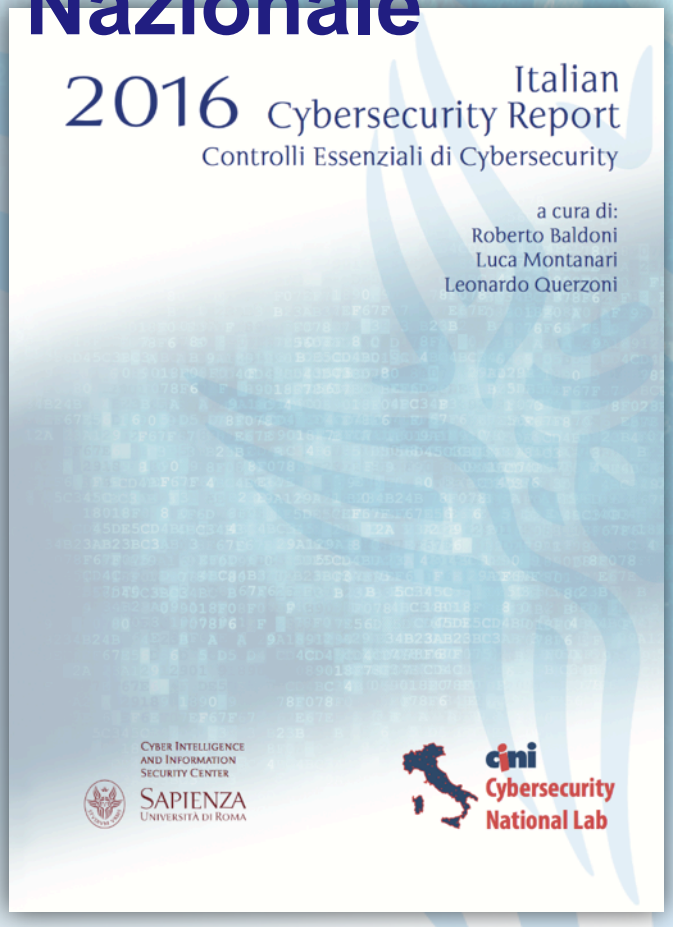
Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Vantaggi per le PMI ?

- Il documento contiene una contestualizzazione del Framework dedicata alle PMI
- E' abbastanza. La risposta è NO!

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 PPAA. 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

Controlli Essenziali sono parte dello stesso processo del Framework Nazionale



Strumento che permette di ”iniziare” a parlare la lingua del Framework Nazionale dedicato a uno specifico target d’imprese

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini
Cybersecurity National Lab

GRAZIE

www.cybersecurityframework.it/csr2016

@CIS_Sapienza
@CyberSecNatLab

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab