# FRAMEWORK NAZIONALE PER LA CYBERSECURITY E LA DATA PROTECTION

## TUTORIAL – PARTE 2/6
## INTRODUZIONE AL FRAMEWORK

Pisa, 12-02-2019

info@cybersecurityframework.it

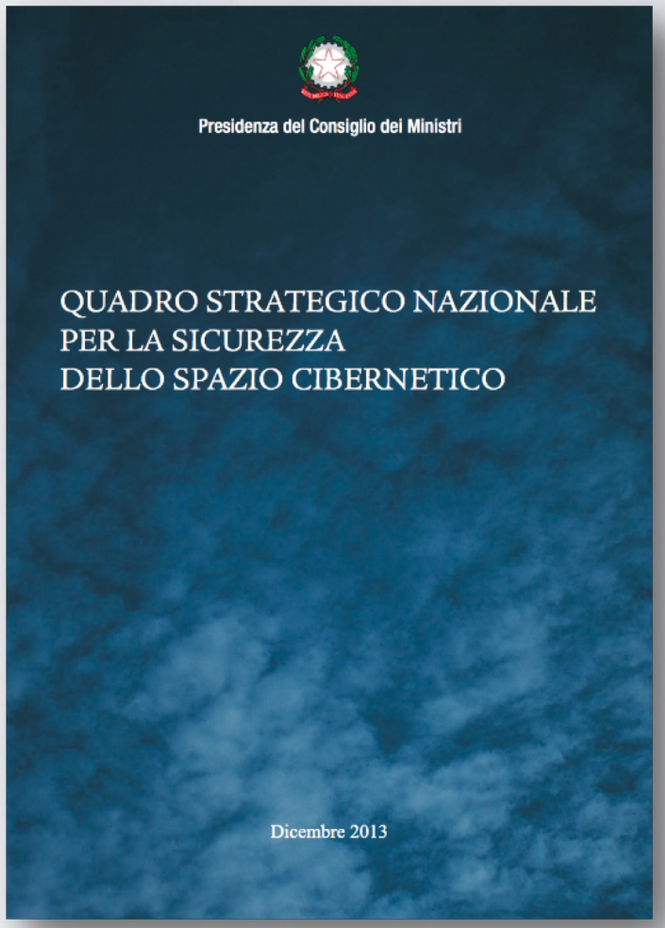
SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cyber Security National Lab

# NASCITA DEL FRAMEWORK

## DPCM 24 gennaio 2013



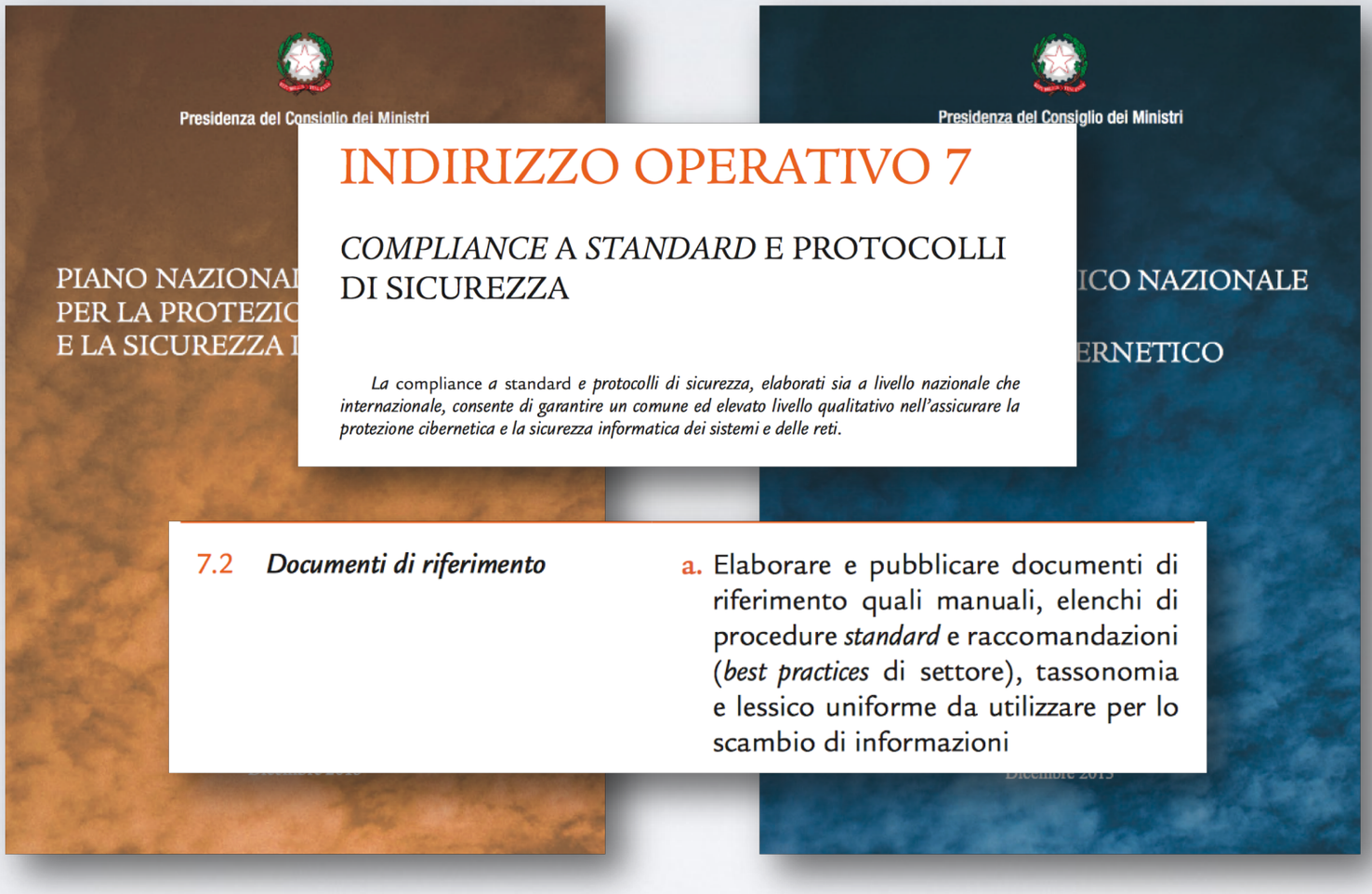

Dalla strategia nazionale al Framework Nazionale



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# NASCITA DEL FRAMEWORK

## DPCM 24 gennaio 2013




## Dalla strategia nazionale al Framework Nazionale



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# NASCITA DEL FRAMEWORK

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

AON
Deloitte.
Enel
eni
hermesbay
KPMG
INTELLIUM

Agenzia per l'Italia Digitale
*Presidenza del Consiglio dei Ministri*

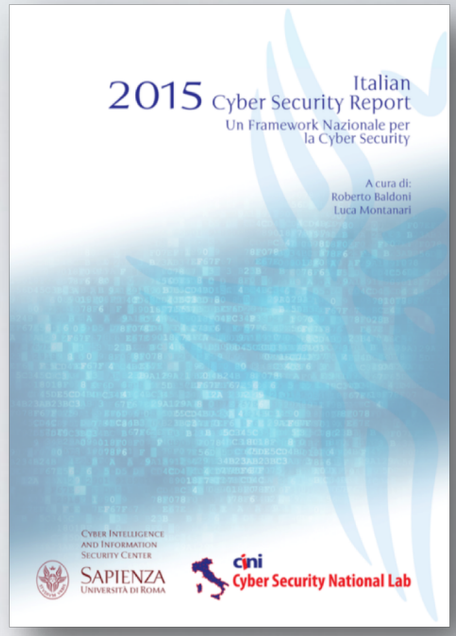
COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

*Ministero dello Sviluppo Economico*

CERT nazionale Italia

Microsoft
pwc




**2014**

Strategia Nazionale 27/12/2013

Definizione degli obiettivi

Definizione del tavolo di lavoro

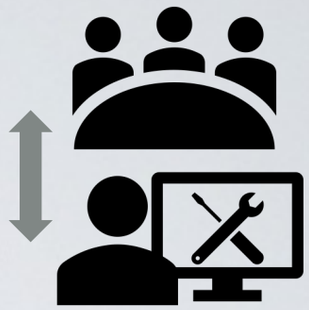
**2015**

Allargamento del tavolo a imprese e PA (PPP)

4 Febbraio 2016

# OBIETTIVI

- Portare la consapevolezza del rischio cyber ai massimi livelli aziendali



- Creare un Framework riconosciuto a livello internazionale

- Considerare il panorama economico italiano

# DA DOVE NASCE IL FRAMEWORK…

NIST
FRAMEWORK FOR
IMPROVING CRITICAL
INFRASTRUCTURE
CYBERSECURITY

FRAMEWORK
NAZIONALE PER LA
CYBERSECURITY

# DA DOVE NASCE IL FRAMEWORK…

NIST
FRAMEWORK FOR
IMPROVING CRITICAL
INFRASTRUCTURE
CYBERSECURITY

- Framework Core
- Implementation Tier
- Profili

FRAMEWORK
NAZIONALE PER LA
CYBERSECURITY

- Livelli di Priorità
- Livelli di Maturità
- Contestualizzazioni

# FRAMEWORK CORE

| Functions | Categories | Subcategories | Informative References |
|---|---|---|---|
| IDENTIFY | | | |
| | | | |
| | | | |
| | | | |
| PROTECT | | | |
| | | | |
| | | | |
| | | | |
| DETECT | | | |
| | | | |
| | | | |
| | | | |
| RESPOND | | | |
| | | | |
| | | | |
| | | | |
| RECOVER | | | |
| | | | |
| | | | |
| | | | |

- 5 Function
- 22 Category
- 98 Subcategory
- Informative Ref.:
  - ISO/IEC 27001
  - COBIT 5
  - NIST SP 800-53 Rev. 4
  - CCS CSC
  - …

# FRAMEWORK CORE

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| IDENTIFY (ID) | **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 | • **CCS CSC** 1<br>• **COBIT 5** BAI09.01, BAI09.02<br>• **ISA 62443-2-1:2009** 4.2.3.4<br>• **ISA 62443-3-3:2013** SR 7.8<br>• **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | • **CCS CSC** 2<br>• **COBIT 5** BAI09.01, BAI09.02, BAI09.05<br>• **ISA 62443-2-1:2009** 4.2.3.4<br>• **ISA 62443-3-3:2013** SR 7.8<br>• **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>• **NIST SP 800-53 Rev. 4** CM-8 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | • **CCS CSC** 1<br>• **COBIT 5** DSS05.02<br>• **ISA 62443-2-1:2009** 4.2.3.4<br>• **ISO/IEC 27001:2013** A.13.2.1<br>• **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| | | **ID.AM-4:** External information systems are catalogued | • **COBIT 5** APO02.02<br>• **ISO/IEC 27001:2013** A.11.2.6<br>• **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 | • **COBIT 5** APO03.03, APO03.04, BAI09.02<br>• **ISA 62443-2-1:2009** 4.2.3.6<br>• **ISO/IEC 27001:2013** A.8.2.1<br>• **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14 |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | • **COBIT 5** APO01.02, DSS06.03<br>• **ISA 62443-2-1:2009** 4.3.2.3.3<br>• **ISO/IEC 27001:2013** A.6.1.1 |



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# IMPLEMENTATION TIER

Forniscono contesto su come l'organizzazione gestisce il rischio cyber

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

- Rischio gestito con processi ad hoc
- Consapevolezza del rischio cyber limitata

- Miglioramento continuo dei processi di cybersecurity
- Adattamento al cambiamento delle minacce e il panorama tecnologico

# PROFILI

- Selezione di specifiche Subcategory del Framework

- Permettono di definire la situazione attuale di un'organizzazione (**profilo attuale**) e quella desiderata (**profilo target**)

- Abilitano la Gap Analysis

- Permettono di identificare una roadmap per raggiungere il profilo target



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# FRAMEWORK NAZIONALE

- Il Framework NIST è pensato per le Infrastrutture Critiche

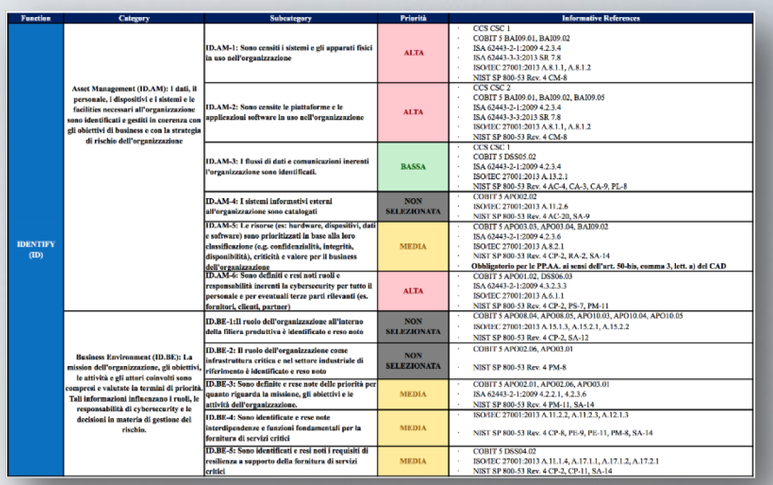
- Nell'ottica di dare la possibilità di adattare il Framework a diversi contesti (es. PMI) il Framework Nazionale introduce 3 nuovi concetti:
  - Livelli di Priorità
  - Livelli di Maturità
  - Contestualizzazioni

| Functions | Categories | Subcategories | Priority Levels | Maturity Levels | | | | Informative References | Guide Lines |
|---|---|---|---|---|---|---|---|---|---|
| | | | | M1 | M2 | M3 | M4 | | |
| IDENTIFY | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| PROTECT | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| DETECT | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| RESPOND | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| RECOVER | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# LIVELLI DI PRIORITÀ



| 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<br>· COBIT 5 BAI09.01, BAI09.02<br>· ISA 62443-2-1:2009 4.2.3.4<br>· ISA 62443-3-3:2013 SR 7.8<br>· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>· 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<br>· COBIT 5 BAI09.01, BAI09.02, BAI09.05<br>· ISA 62443-2-1:2009 4.2.3.4<br>· ISA 62443-3-3:2013 SR 7.8<br>· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2<br>· 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<br>· COBIT 5 DSS05.02<br>· ISA 62443-2-1:2009 4.2.3.4<br>· ISO/IEC 27001:2013 A.13.2.1<br>· 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<br>· ISO/IEC 27001:2013 A.11.2.6<br>· 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<br>· ISA 62443-2-1:2009 4.2.3.6<br>· ISO/IEC 27001:2013 A.8.2.1<br>· NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14<br>· **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<br>· ISA 62443-2-1:2009 4.3.2.3.3<br>· ISO/IEC 27001:2013 A.6.1.1<br>· 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<br>· ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2<br>· 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<br>· 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<br>· ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6<br>· 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<br>· 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<br>· ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>· NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 |

- Sono associate alle Subcategory
- Possibilità di definire la propria scala
- Scala suggerita:
  - ALTA: Subcategory che permettono di ridurre *sensibilmente* il rischio. Vanno implementate indipendentemente dalla difficoltà realizzativa.
  - MEDIA: Subcategory che permettono di ridurre il rischio e risultano di semplice implementazione.
  - BASSA: Subcategory che permettono di ridurre il rischio ma risultano di difficile implementazione.
- Permettono di prioritizzare le azioni della roadmap per raggiungere il profilo target



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# LIVELLI DI MATURITÀ

| 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 |



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# CONTESTUALIZZAZIONE

Adattamento del Framework ad uno specifico contesto:

- Singola realtà aziendale
- Scala (es. micro imprese, PMI, grandi imprese)
- Settore economico/produttivo
- Settore Regolato:
  - PA
  - Banche
  - …

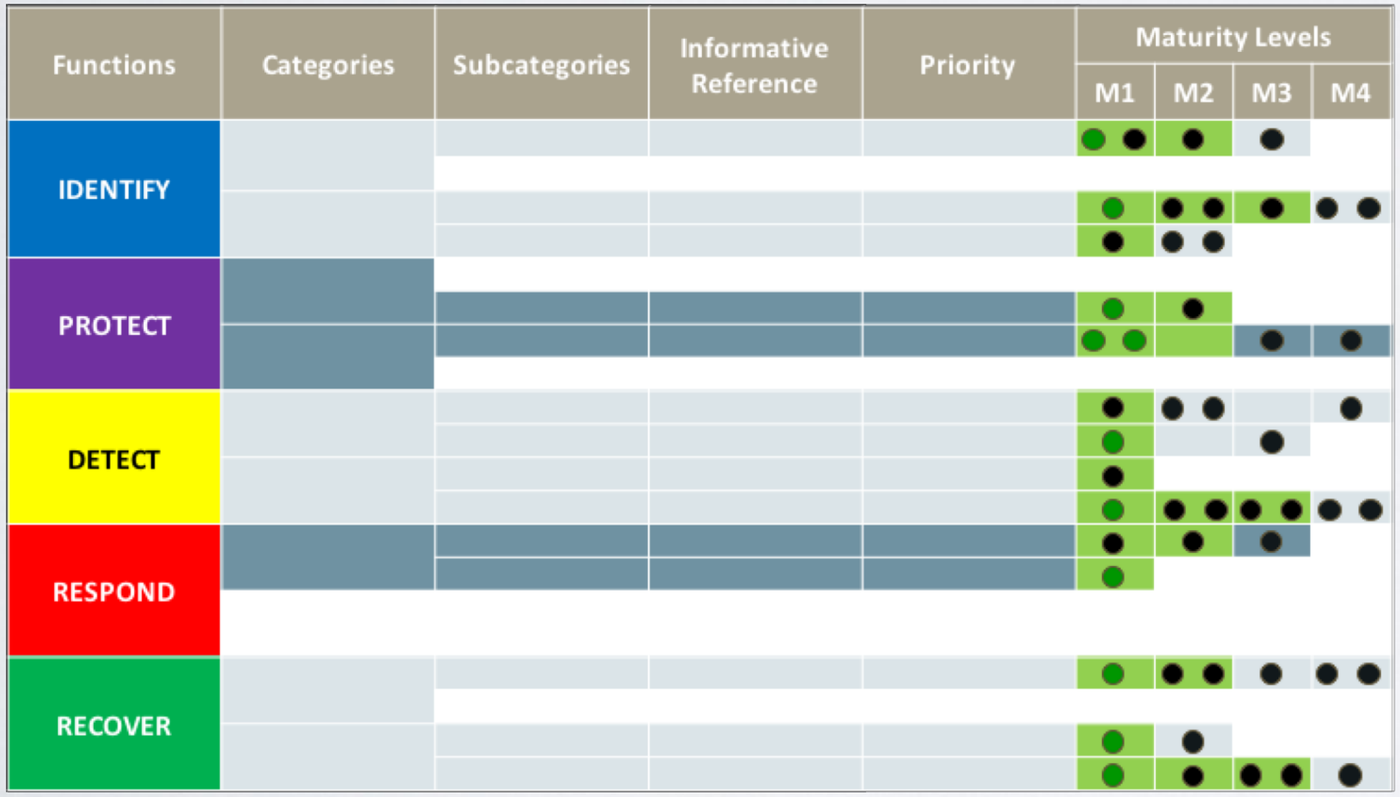


cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# CONTESTUALIZZAZIONE

## Contestualizzazione

- Selezione delle Subcategory
- Definizione dei Livelli di Priorità
- Definizione del Livelli di Maturità…e Controlli di Sicurezza




Data una Contestualizzazione è possible determinare:

- Profilo Corrente
- Profilo Target



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# CONTEXT-PMI

- Una contestualizzazione per PMI

| Function | Category | Subcategory | Priorità | Informative References |
|---|---|---|---|---|
| IDENTIFY (ID) | Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity. | ID.GV-1: E' indetificata e resa nota una policy di sicurezza delle informazioni | MEDIA | · COBIT 5 APO01.03, EDM01.01, EDM01.02<br>· ISA 62443-2-1:2009 4.3.2.6<br>· ISO/IEC 27001:2013 A.5.1.1<br>· NIST SP 800-53 Rev. 4 -1 controls from all families<br>· **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** |
| | | ID.GV-2: Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni | MEDIA | · COBIT 5 APO13.12<br>· ISA 62443-2-1:2009 4.3.2.3.3<br>· ISO/IEC 27001:2013 A.6.1.1, A.7.2.1<br>· NIST SP 800-53 Rev. 4 PM-1, PS-7 |
| | | 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 | ALTA | · COBIT 5 MEA03.01, MEA03.04<br>· ISA 62443-2-1:2009 4.4.3.7<br>· ISO/IEC 27001:2013 A.18.1<br>· NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)<br>· **Obbligatoria ai sensi del D.Lgs. 196/2003**<br>· **Obbligatorio ai sensi dei provvedimenti del Garante per la protezione dei dati personali**<br>· **Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 novembre 2015 e dei relativi decreti n. 4/2015 e n.5/2015** |
| | | ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity | BASSA | · COBIT 5 DSS04.02<br>· ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3<br>· NIST SP 800-53 Rev. 4 PM-9, PM-11 |
| | Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l' operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui. | ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate | MEDIA | · CCS CSC 4<br>· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04<br>· ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12<br>· ISO/IEC 27001:2013 A.12.6.1, A.18.2.3<br>· NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| | | ID.RA-2: L'organizzazione riceve informazioni su minacce e vulnerabilità da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing) | BASSA | · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>· ISO/IEC 27001:2013 A.6.1.4<br>· NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 |
| | | ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate | BASSA | · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04<br>· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>· NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 |
| | | ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento | BASSA | · COBIT 5 DSS04.02<br>· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12<br>· NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 |
| | | ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio | BASSA | · COBIT 5 APO12.02<br>· ISO/IEC 27001:2013 A.12.6.1<br>· NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 |
| | | ID.RA-6: Sono identificate e prioritizzate le risposte al rischio | BASSA | · COBIT 5 APO12.05, APO13.02<br>· NIST SP 800-53 Rev. 4 PM-4, PM-9 |
| | Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale. | ID.RM-1: I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder) | BASSA | · COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02<br>· ISA 62443-2-1:2009 4.3.4.2<br>· NIST SP 800-53 Rev. 4 PM-9 |
| | | ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente | BASSA | · COBIT 5 APO12.06<br>· ISA 62443-2-1:2009 4.3.2.6.5<br>· NIST SP 800-53 Rev. 4 PM-9 |
| | | ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza | BASSA | · NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 |

# FRAMEWORK 2.0

CYBERSECURITY

DATA PROTECTION

FRAMEWORK NAZIONALE PER LA CYBERSECURITY E LA DATA PROTECTION

CONTESTUALIZZAZIONE

**GDPR**

# FRAMEWORK 2.0

## Quali sono le novità introdotte?

- Integrazione del core con nuove category e subcategory relative alla Data Protection
- Introduzione di un nuovo strumento: “prototipo di contestualizzazione”
- Prototipo di Contestualizzazione GDPR
- Arricchimento delle Informative Reference (GDPR, NIS, MM AgID)
- Allineamento alla versione 1.1 del NIST Cybersecurity Framework

# FRAMEWORK 2.0

Integrazione di elementi di data protection nel core

- Viene mantenuta la compatibilità con la versione 1.0 e con il Framework NIST
- Il Framework 2.0 estende il Core con 1 Category e 9 Subcategory aggiuntive
- Nessuna subcategory esistente è stata eliminata o modificata



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# FRAMEWORK 2.0

## Integrazione di elementi di data protection nel core

| FUNCTION | CATEGORY | SUBCATEGORY |
|---|---|---|
| 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 e con la strategia di rischio dell'organizzazione. | **DP-ID.AM-7**: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner) |
| | | **DP-ID.AM-8**: I trattamenti di dati personali sono identificati e catalogati |
| | **Risk Assessment (ID.RA)**: L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui. | **DP-ID.RA-7**: Viene effettuata una valutazione di impatto sulla protezione dei dati personali |

| FUNCTION | CATEGORY | SUBCATEGORY |
|---|---|---|
| IDENTIFY (ID) | **Data Management (DP-ID.DM)**: i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento. | **DP-ID.DM-1**: Il ciclo di vita dei dati è definito e documentato |
| | | **DP-ID.DM-2**: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati |
| | | **DP-ID.DM-3**: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati |
| | | **DP-ID.DM-4**: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato |
| | | **DP-ID.DM-5**: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale |
| RESPOND (RS) | **Communications (RS.CO)**: Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine). | **DP-RS.CO-6**: Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati |



cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# FRAMEWORK 2.0

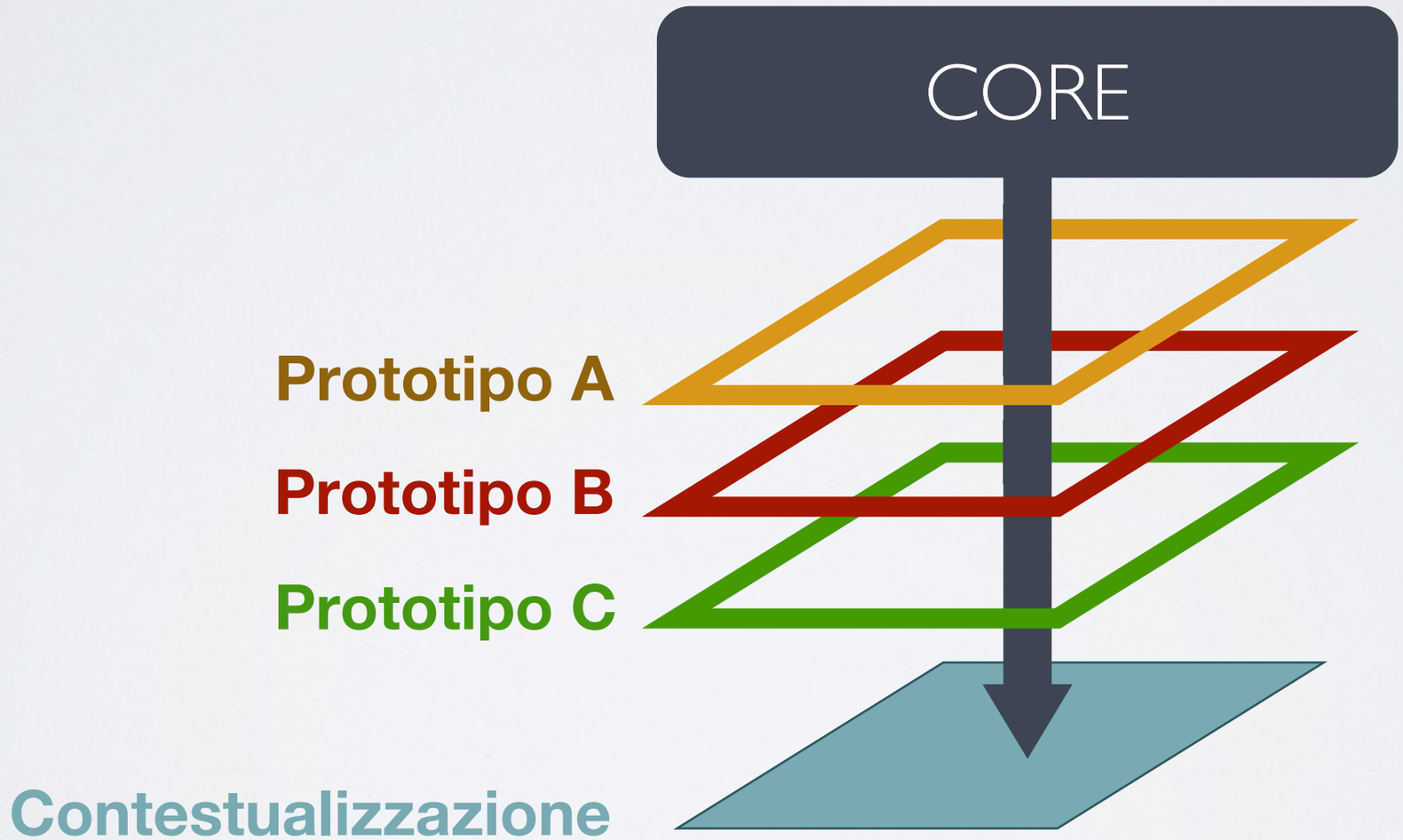
## Introduzione dei “prototipi di contestualizzazione”

- Permettono in fase di contestualizzazione di integrare aspetti trasversali rispetto ai singoli contesti di applicazione, es:
  - normative che richiedono l’attuazione di determinate pratiche indirizzate alla cybersecurity o alla data protection;
  - regolamenti tecnici e di attuazione che indicano puntuali controlli legati alla cybersecurity o alla data protection;
  - best practice di settore inerenti alla cybersecurity o alla data protection.

# FRAMEWORK 2.0

## Introduzione dei “prototipi di contestualizzazione”

- Più prototipi possono essere implementati in fase di contestualizzazione per cogliere aspetti diversi






cini Cyber Security National Lab
SAPIENZA UNIVERSITÀ DI ROMA

# FRAMEWORK 2.0

## Prototipo di contestualizzazione GDPR

- Definizione di un prototipo di contestualizzazione che coglie gli elementi fondamentali di GDPR
  - Ruoli e responsabilità
  - Registri delle attività di trattamento
  - Principi e accountability
  - Valutazione d'impatto sulla protezione dei dati personali
  - Informazione dell'interessato
  - Consenso dell'interessato
  - Diritti dell'interessato
  - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
  - Gestione incidenti che si configurano come violazioni di dati personali
- Guida all'implementazione: Collezione di controlli che possono essere usati in fase di contestualizzazione

# FRAMEWORK 2.0

## Arricchimento delle Informative Reference

- GDPR
- D.Lgs. 65/2018 (recepimento Direttiva NIS)
- “Misure Minime” AgID

# FRAMEWORK 2.0

Allineamento alla versione 1.1 del NIST Cybersecurity Framework

Aggiunte 1 Category e 10 Subcategory al Core:

- Category **Supply Chain Risk Management** (**ID.SC**): gestione del rischio cyber all'interno delle filiere produttive complesse e nelle catene di approvvigionamento (+ 5 Subcategory).
- Subcategory **PR.AC-6** e **PR.AC-7**: gestione delle identità e relativi processi di autenticazione
- Subcategory **PR.DS-8**: controllo di integrità dispositivi hardware
- Subcategory **PR.PT-5**: uso di meccanismi per il soddisfacimento dei requisiti di resilienza
- Subcategory **RS.AN-5**: gestione delle informazioni inerenti alle vulnerabilità

Modifiche minori al testo di altre Category/Subcategory…