Framework Nazionale per la Cyber Security

Luca Montanari, Ph.D
montanari@dis.uniroma1.it
staff@cybersecurityframework.it

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cyber Security National Lab

cini
Cyber Security National Lab

LABORATORIO NAZIONALE PER LA CYBER SECURITY

Cyber Security: un problema nazionale

Il ruolo delle Università nel Piano Strategico

«A livello Nazionale è **imperativo** sviluppare un **approccio coordinato e multi-dimensionale con obiettivi condivisi e ampiamente partecipati** tra le amministrazioni dello Stato, il mondo privato, **accademico** e della ricerca scientifica» (pagina 6)

cini Cyber Security National Lab

240 Faculties
- 68 Full Prof
- 57 Ass. Prof
- 100 Researchers

178 PhD students

76 postdocs

51 Experts

FONDAZIONE BRUNO KESSLER

ENEA

CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER

SAPIENZA UNIVERSITÀ DI ROMA

cini Cyber Security National Lab

Missione del Laboratorio

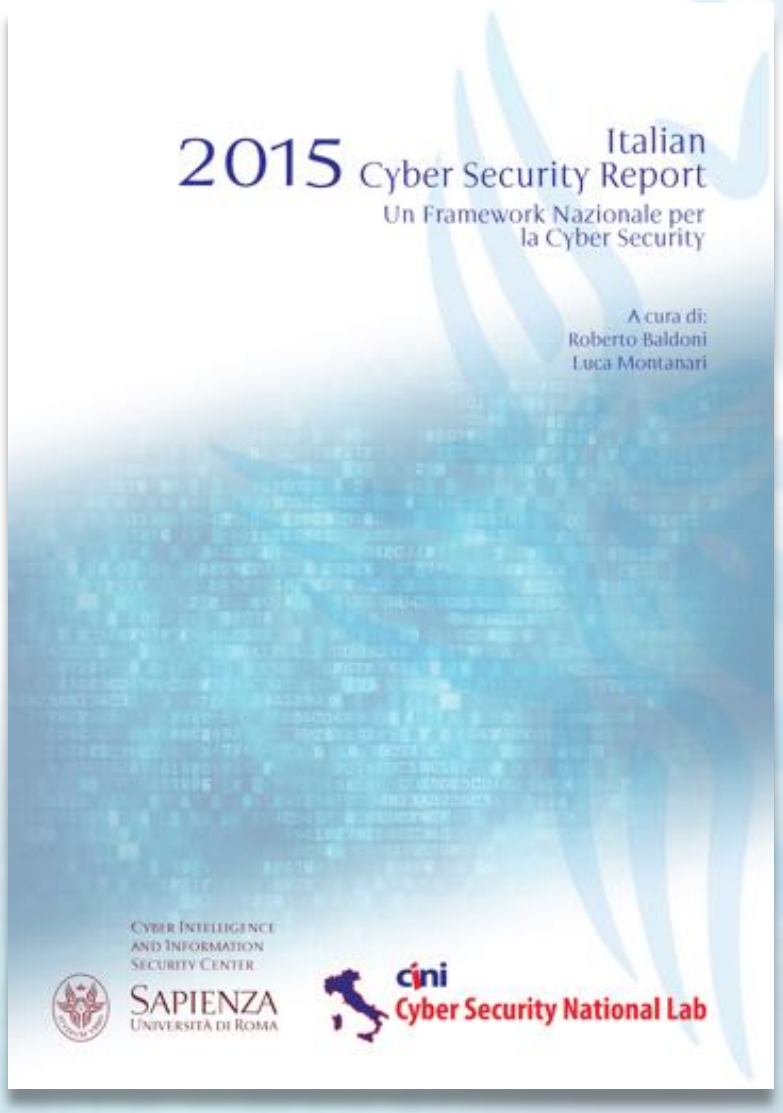
- Diventare un **attore** nel processo di implementazione della **strategia nazionale**
- **Diffondere** la cultura della sicurezza, l'**awareness**, su territorio tramite i nodi locali
- Definizione di **framework** e metodologie utili a livello **nazionale**
- Implementare **progetti** cyber security

Missione del Laboratorio

- Diventar … di impleme… **nazionale**
- **Diffonde**… …zza, l'**awarene**… … i nodi locali
- Definizio… …odologie utili a liv…
- Impleme… …urity

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cyber Security National Lab



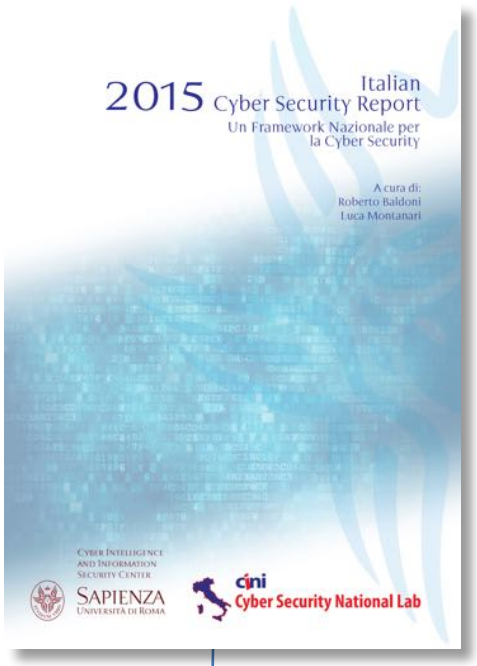
FRAMEWORK NAZIONALE PER LA CYBER SECURITY

Framework Nazionale per la Cyber Security

Decreto Legge
24/1/2013

Strategia
Nazionale
27/12/2013

National CERT
13/11/2014



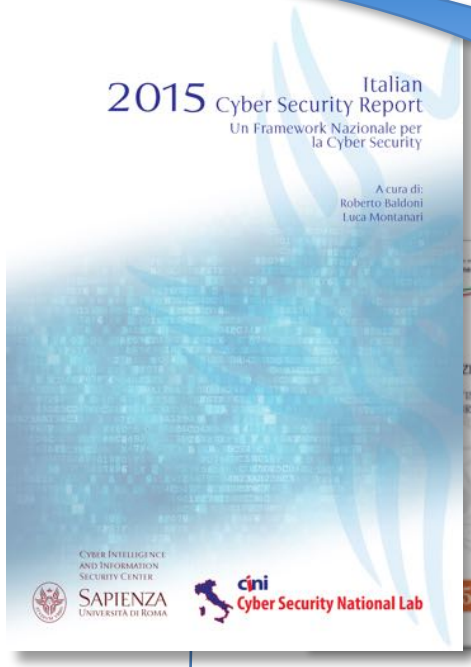
Framework
Nazionale
4/2/2016

Relazione al
parlamento
2/3/2016

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cyber Security National Lab

Framework Nazionale per la Cyber Security



Versione 2.0 della strategia

Decreto Legge 24/1/2013

Strategia Nazionale 27/12/2013

National CERT 13/11/2014

Framework Nazionale 4/2/2016

Relazione al parlamento 2/3/2016

Cyber Intelligence and Information Security Center
SAPIENZA Università di Roma

cini Cyber Security National Lab

Relazione al parlamento

[…] 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 approccio di sistema ed in linea con le* ***best practices internazionalmente riconosciute****.*

Framework Nazionale per la Cyber Security: obiettivi iniziali

- Portare la consapevolezza del rischio cyber ai massimi livelli aziendali
  - non più una cosa per soli tecnici
  - portare le organizzazioni a considerare il rischio cyber come rischio economico parte del risk management

- Considerare il panorama economico italiano
  - 69% del PIL prodotto da Piccole-Medie Imprese
  - Pochissime grandi imprese nazionali

Framework Nazionale per la Cyber Security: obiettivi iniziali

- Creare qualcosa che sia riconosciuto a livello internazionale
  - migliorare la capacità di information sharing
  - innalzare il livello di duty of care nazionale

- Non reinventare la ruota
  - non ha senso creare un nuovo framework da zero
  - siamo partiti dal **NIST Framework for Improving Critical Infrastructure Cybersecurity**

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

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

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Framework core
- Profiles

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Framework Nazionale per la Cybersecurity

- Framework core
- Profiles

Abbiamo Aggiunto:

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

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

*validi per nell'ambito della contestualizzazione

Framework Nazionale per la Cybersecurity

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 missione 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

- Ab
-
-
-
-
-
-
-

della contestualizzazione

Framework Nazionale per la Cybersecurity

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

Contestualizzazioni

Il Framework può essere "customizzato" tramite:

- **la selezione delle subcategory**
  - quali saranno implementate e quali no
- **definizione di livelli di priorità** per ogni subcategory
  - quali andrebbero implementate subito e quali successivamente
- **livelli di maturità** per ogni subcategory
  - quali sono i possibili livelli di impegno da dedicare alla singola subcategory

Contestualizzazioni

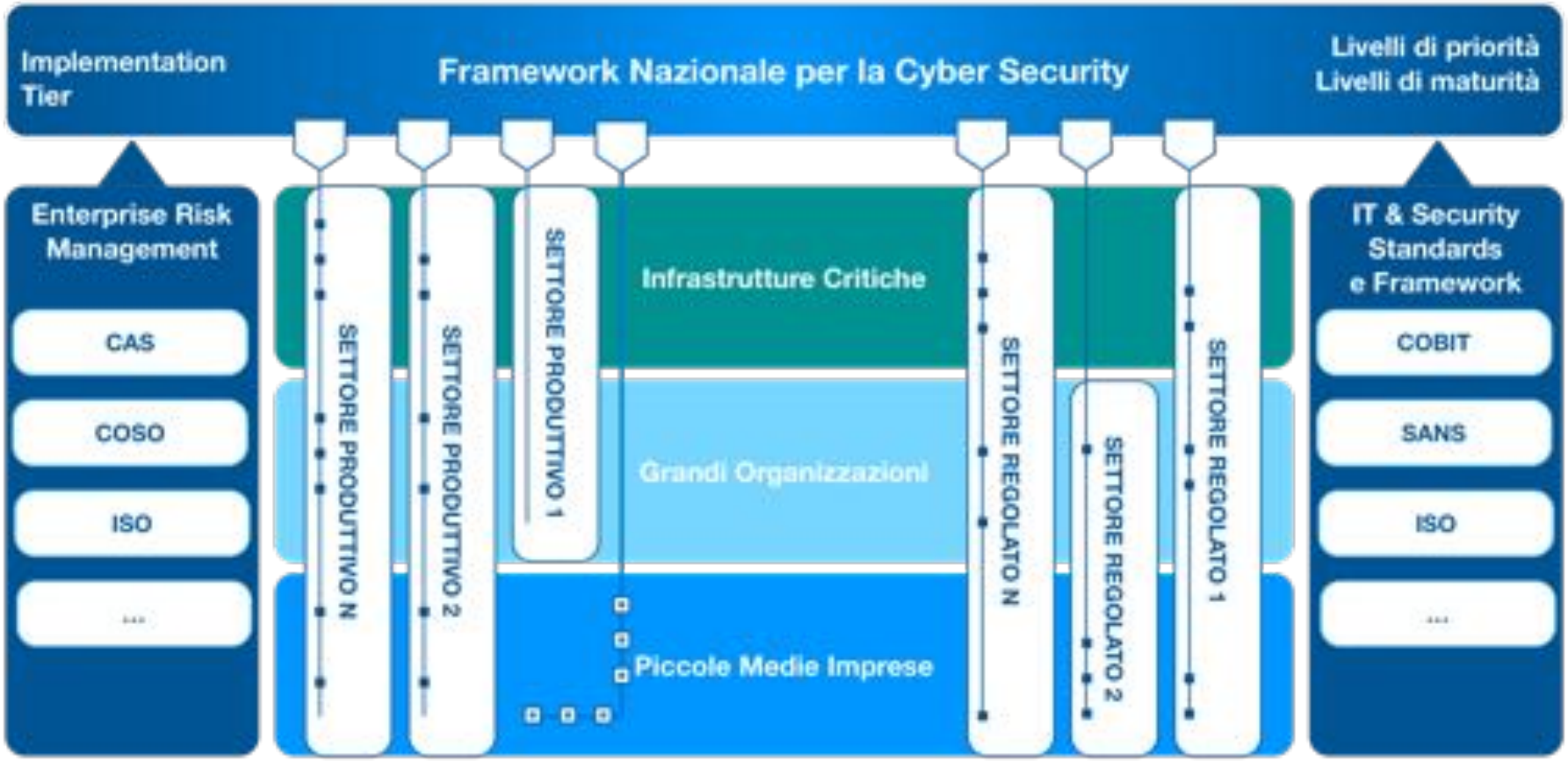
La singola contestualizzazione può essere valida per organizzazioni:

- di un dato settore economico/produttivo
- di una certa dimensione
- appartenenti a un settore regolato
- per pubbliche amministrazioni centrali/locali regionali...
- altro...

Chi può creare contestualizzazioni del Framework

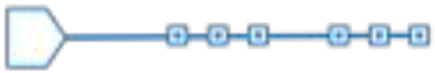
- La singola azienda
- Un'associazione di settore produttivo
- Un regolatore di settore
- Un qualsiasi attore che definisce una contestualizzazione del Framework

Contestualizzazioni



Contestualizzazione per un settore produttivo/regolato

Contestualizzazione del framework



CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER
SAPIENZA UNIVERSITÀ DI ROMA

cini Cyber Security National Lab

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
- Un aiuto nell'approntare un processo evoluto di gestione del rischio cyber

- Raccomandazioni e suggerimenti sulla gestione del rischio cyber

Vantaggi per le grandi imprese

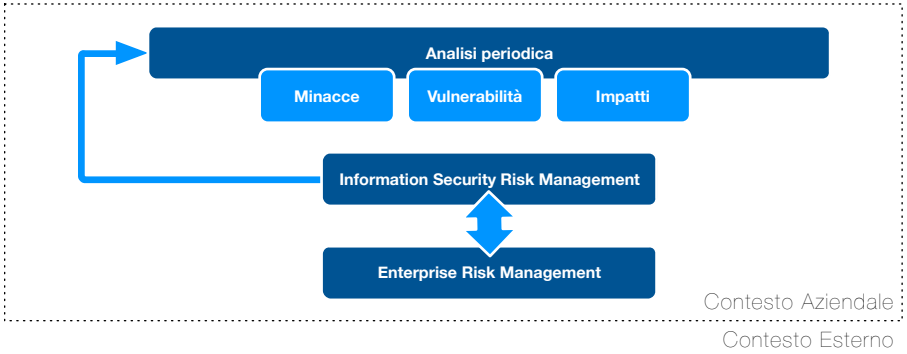


Figura 7.1: Un approccio tradizionale alla gestione del rischio IT.

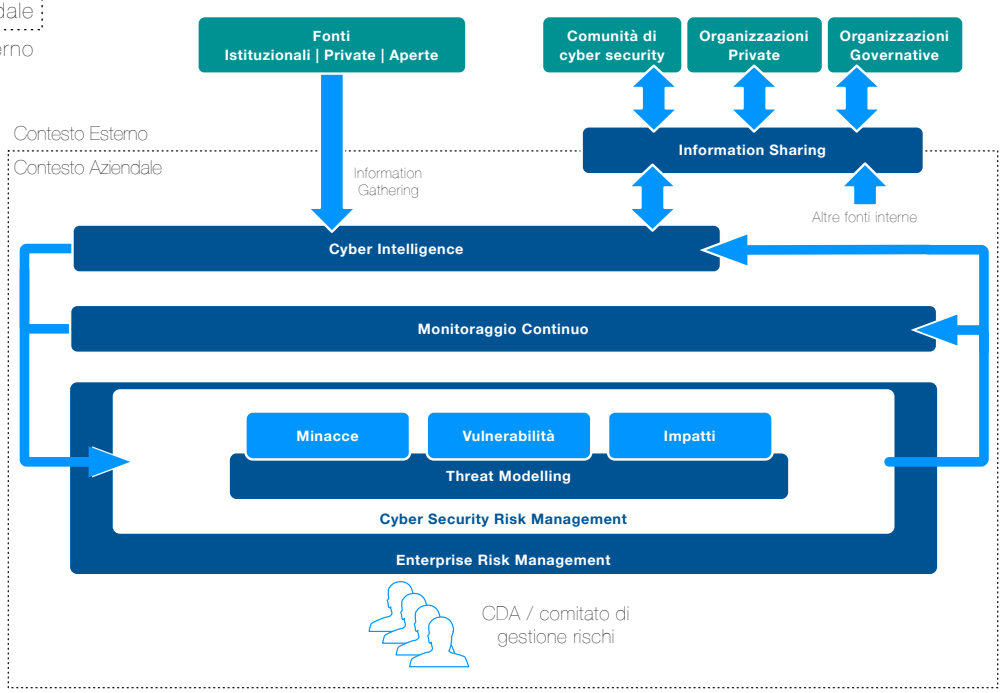


Figura 7.2: Un approccio evoluto alla gestione del rischio cyber.

Vantaggi per le PMI

- Qualcosa da cui partire!
- Una contestualizzazione del Framework dedicata a loro
  - Selezione delle subcategory
  - Livelli di priorità
  - Livelli di maturità
- Guida all'implementazione delle subcategory a priorità alta

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

Framework Nazionale

- **Più generale del** NIST CI-Framework
  - le contestualizzazioni permettono di creare Framework "custom"
- Viene mantenuta la **compliance** con il NIST CI-Framework
  - riconosciuto internazionalmente
- **profili di sicurezza** più accurati
  - sono definiti sui livelli di maturità
- Riconosciuto a livello nazionale
  - potrebbe rafforzare la **supply chain** dell'intero panorama nazionale
  - Fornisce un linguaggio comune per le **interazioni tra pubblico e privato**

Il futuro del Framework

- Il governo ha pubblicamente "**adottato**" il Framework
- Il Framework è un documento "vivo" e **va aggiornato**
  - La minaccia cyber evolve in continuazione
  - recepirà gli aggiornamenti del framework NIST
- Le contestualizzazioni sperabilmente saranno sempre più, per più settori

Il team (oltre 30 persone) Public-Private-Partnership

- CIS-Sapienza
- Laboratorio Nazionale

- PCM (Intelligence)
- CERT Nazionale
- CERT-PA
- Garante della Privacy
- Agid

- Panel di aziende

Il team (oltre 30 persone)
Public-Private-Partnership

Consultazione pubblica:

Cyber Intelligence and Information Security Center

Sapienza Università di Roma

cini Cyber Security National Lab

GRAZIE

www.cybersecurityframework.it

staff@cybersecurityframework.it

@CIS_Sapienza

@lucamontanari