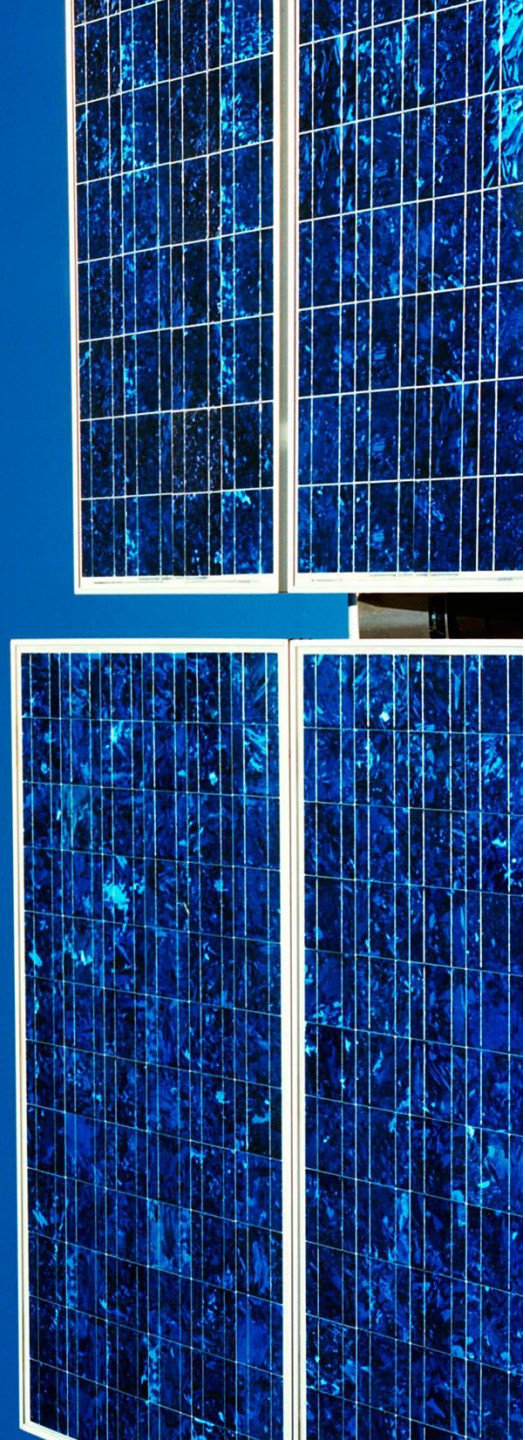
# KPMG Advisory

# Approccio custom al FNCS

17 Gennaio 2017



# Presentazioni

**Andrea Zapparoli Manzoni – azapparolimanzoni@kpmg.it**

- **Head of Cyber Security Services - KPMG Advisory**
- Membro **Osservatorio per la Sicurezza Nazionale** (OSN) 2012-2014
- Docente **NATO RSSCD** (Regional Summer School on Cyber Defense) e **NATO ATC** (Advanced Training Course)
- Board Advisor **CSCSS Center for Strategic Cyberspace + Security Science (UK)**
- **Clusit (Ass. Italiana Sicurezza Informatica)**: membro del Consiglio Direttivo
- Co-autore del **Rapporto Clusit** 2012, 2013, 2014, 2015, 2016, 2017…
- Co-autore del **Framework Nazionale di Cyber Security** (2016)
- Co-autore paper ENISA **Security and Resilience for Smart Health Service and Infrastructures** (2016)
- Co-autore numerosi white papers: Sicurezza Social, Frodi Online, Cyber Crime, ROSI

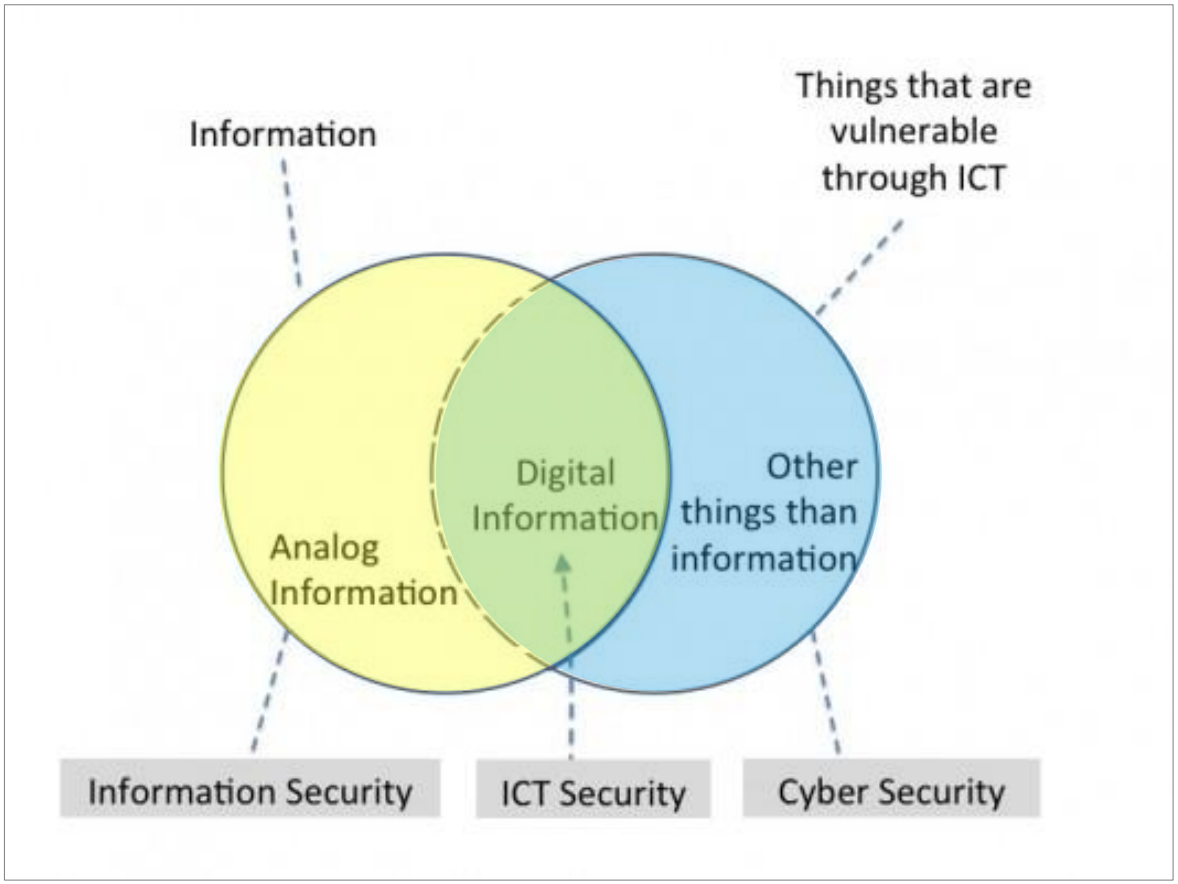
KPMG

# Cyber Security ?

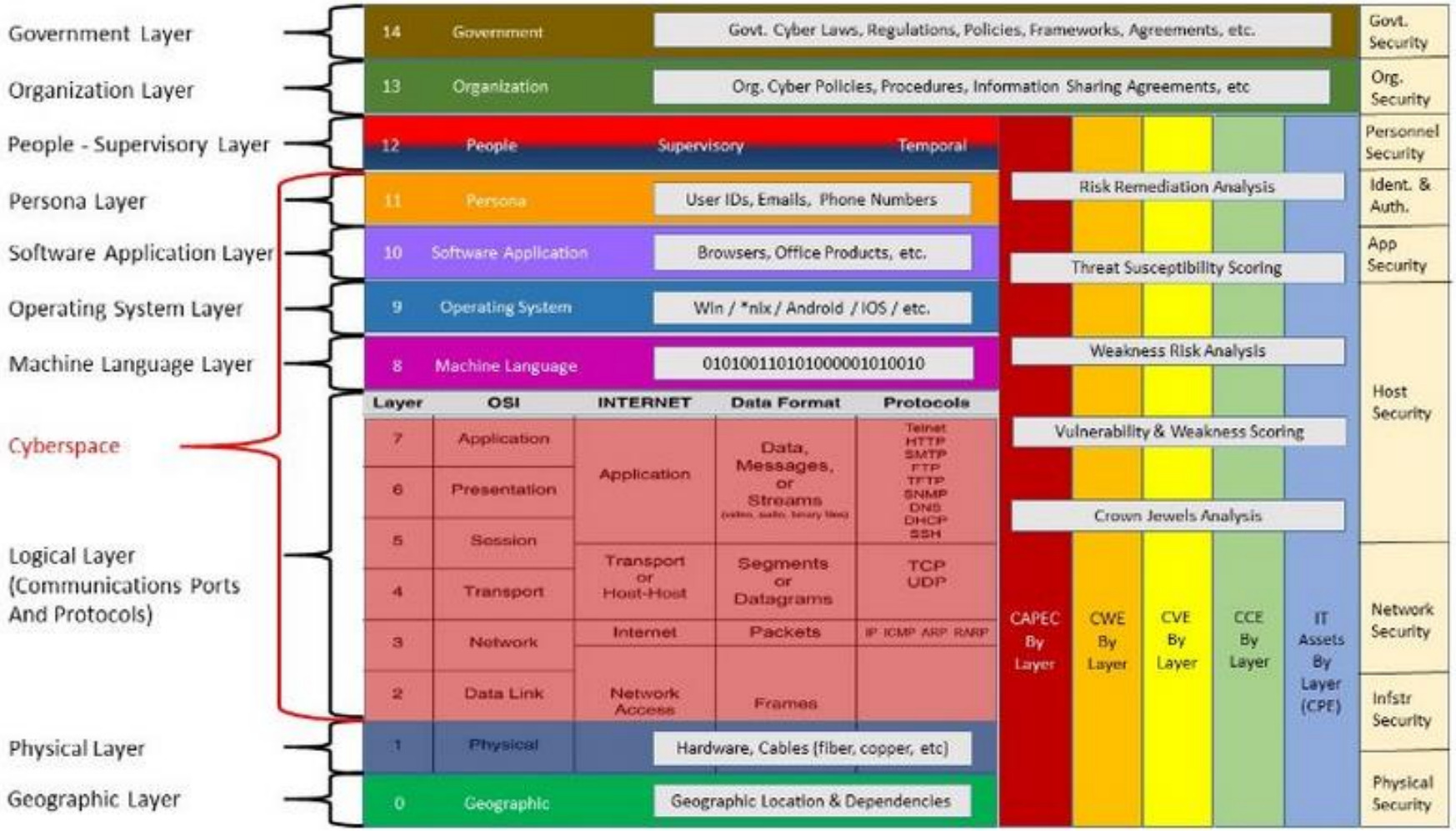
**Esempi e dimostrazioni**

# Cos'è la "cyber security" ?

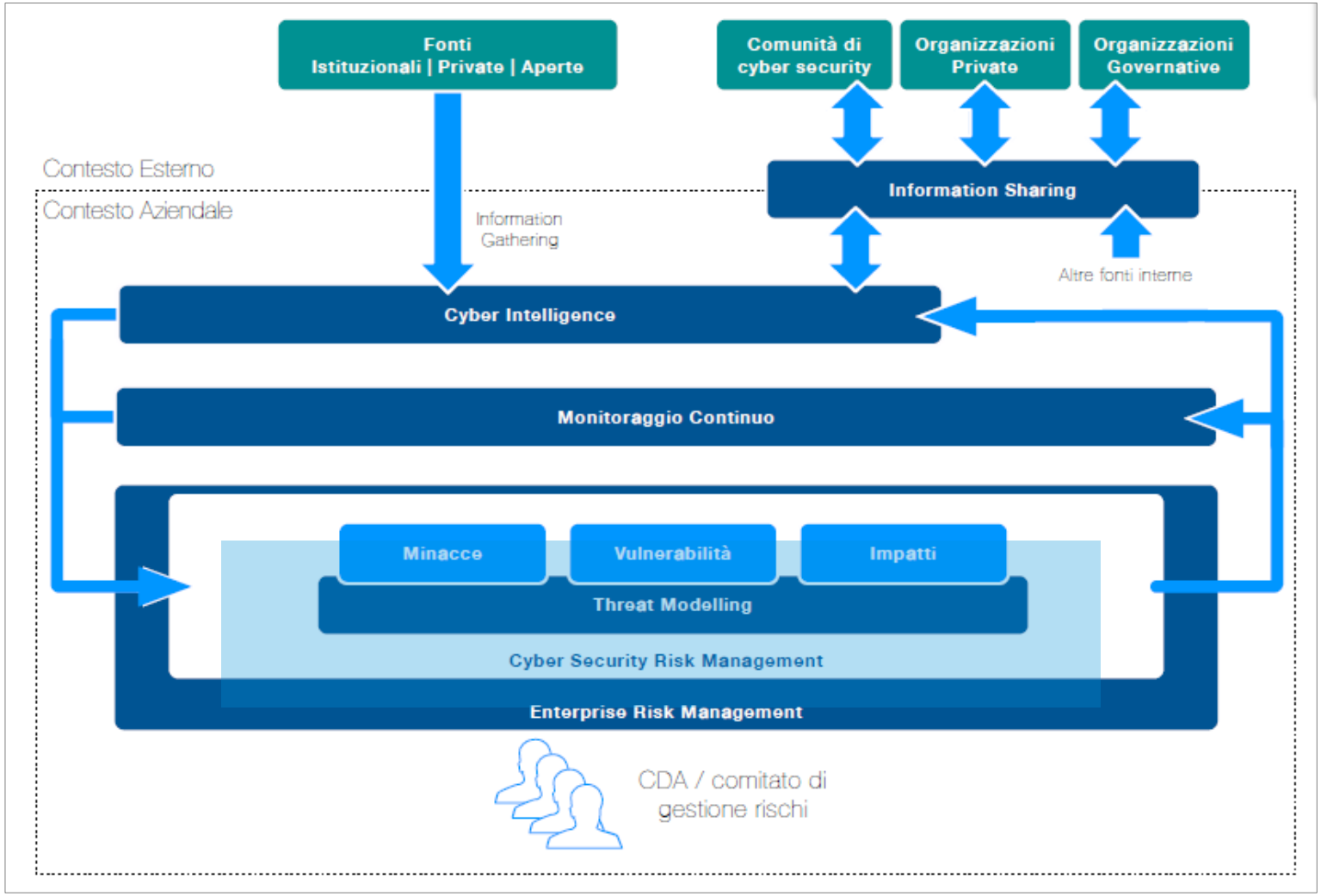
Il perimetro degli asset, molti dei quali "non-IT", **resi vulnerabili tramite l'ICT** sta aumentando in modo *esponenziale (IoT, Social, connected-everything, etc)*. A **rischio** oltre ai dati sono la reputazione, i processi di business, le finanze, la salute, la vita umana, etc.



# Cos'è lo "spazio cibernetico" ?



# Cos'è il "Cyber Risk Management" ?



KPMG

# Il costo della Cyber inSecurity

**Esempi e dimostrazioni**

# Ok, tutto bello, però.....

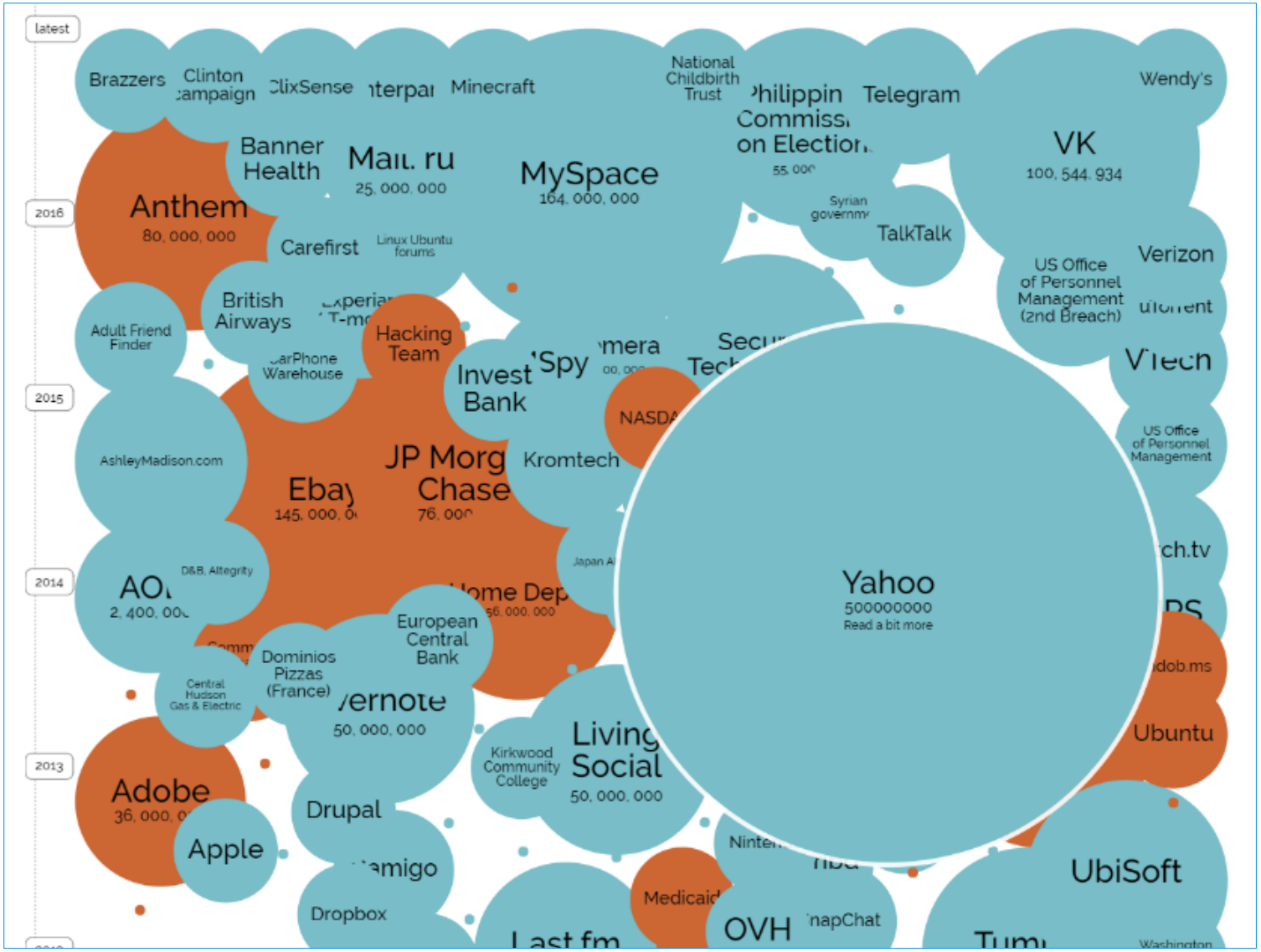
| Rank | Password | Frequency |
|---|---|---|
| 1 | 123456 | 706,689 |
| 2 | 123456789 | 237,898 |
| 3 | 12345 | 107,211 |
| 4 | 000000 | 78,924 |
| 5 | 111111 | 62,445 |
| 6 | 12345678 | 61,658 |
| 7 | azerty | 56,688 |
| 8 | paSSword | 54,128 |
| 9 | 1234567 | 53,003 |
| 10 | badoo | 49,918 |
| 11 | 123123 | 37,082 |
| 12 | 1234567890 | 33,945 |
| 13 | 654321 | 28,728 |
| 14 | qwerty | 25,736 |
| 15 | 666666 | 25,000 |
| 16 | juventus | 23,659 |
| 17 | antonio | 21,679 |
| 18 | andrea | 21,153 |
| 19 | 121212 | 19,960 |
| 20 | 010203 | 18,632 |
| 21 | 987654321 | 18,590 |

# Il contesto globale - Evoluzione delle minacce - 1

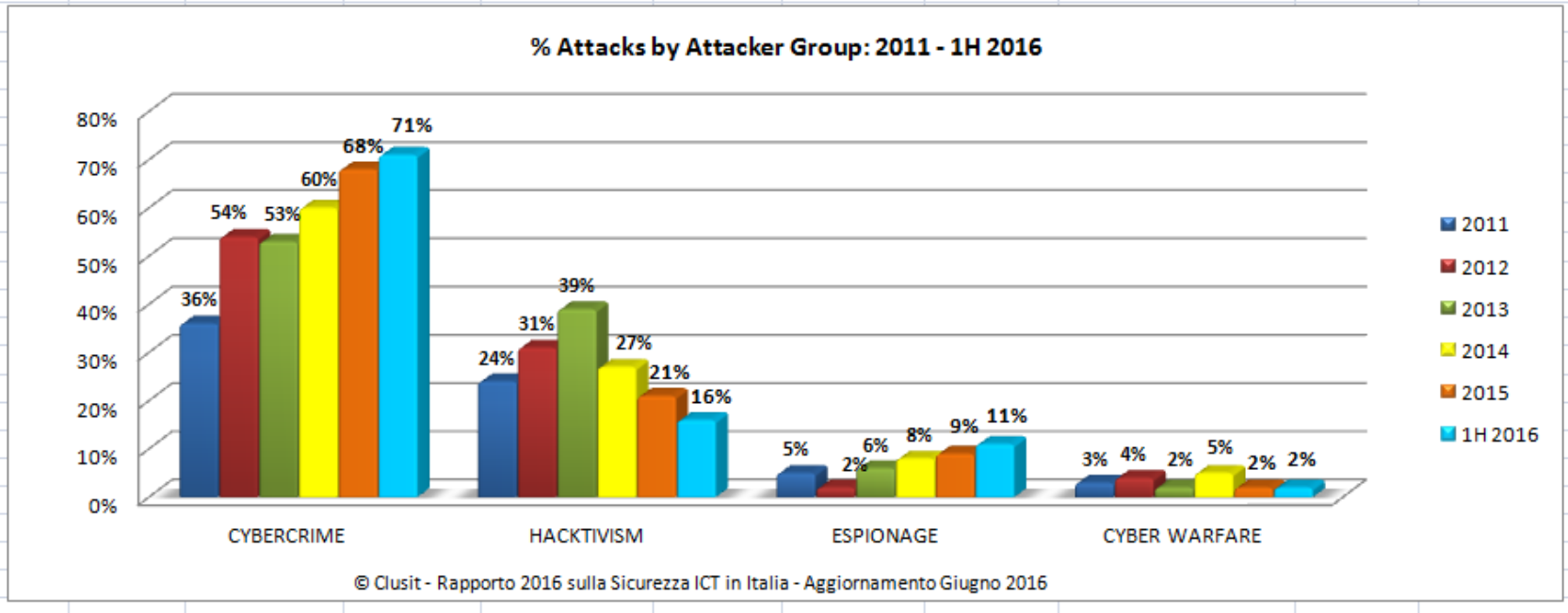
## Cybercrime now 'number one' threat – Europol chief

'It's become a global problem and we urgently need global instruments to deal with it,' says Europol chief Rob Wainwright

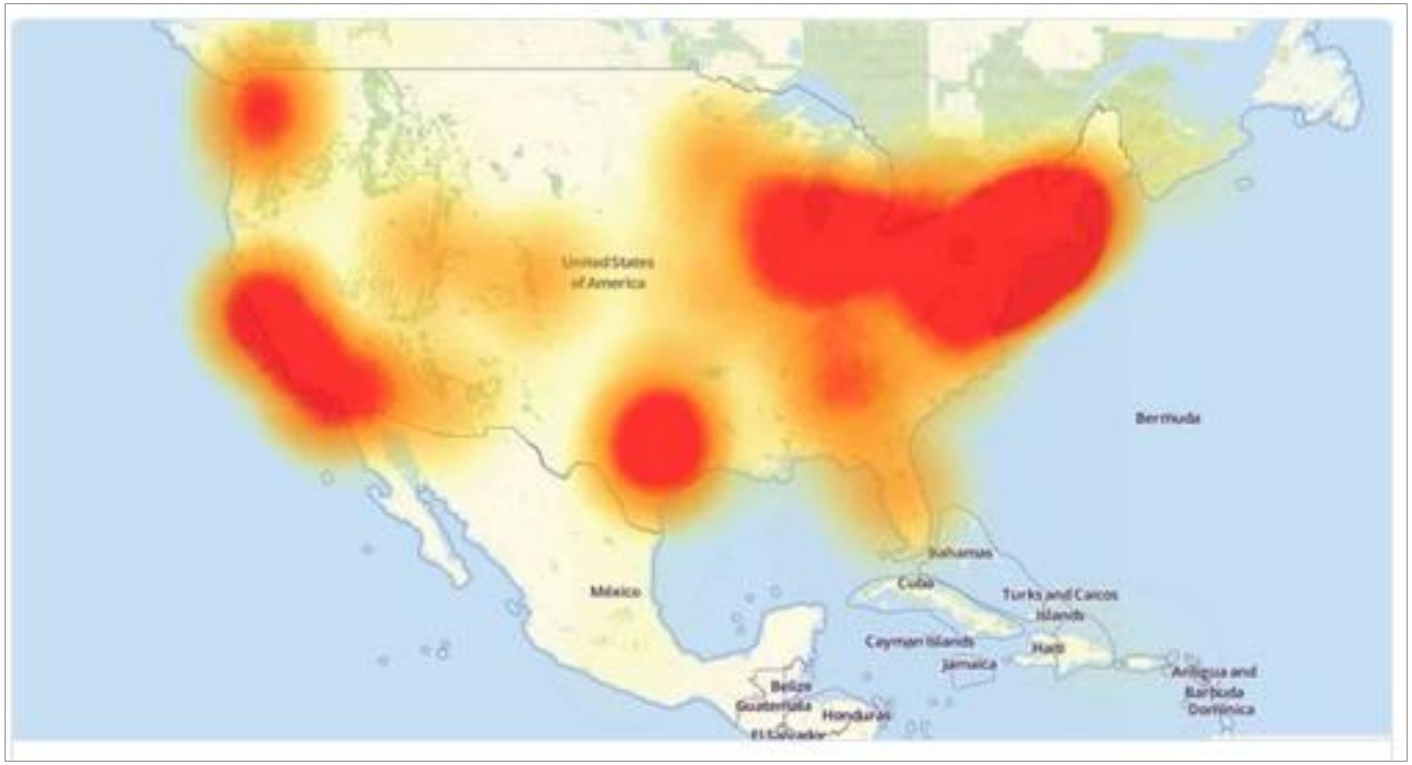
# Il contesto globale - Evoluzione delle minacce - 2



# Il contesto globale - Evoluzione delle minacce - 3

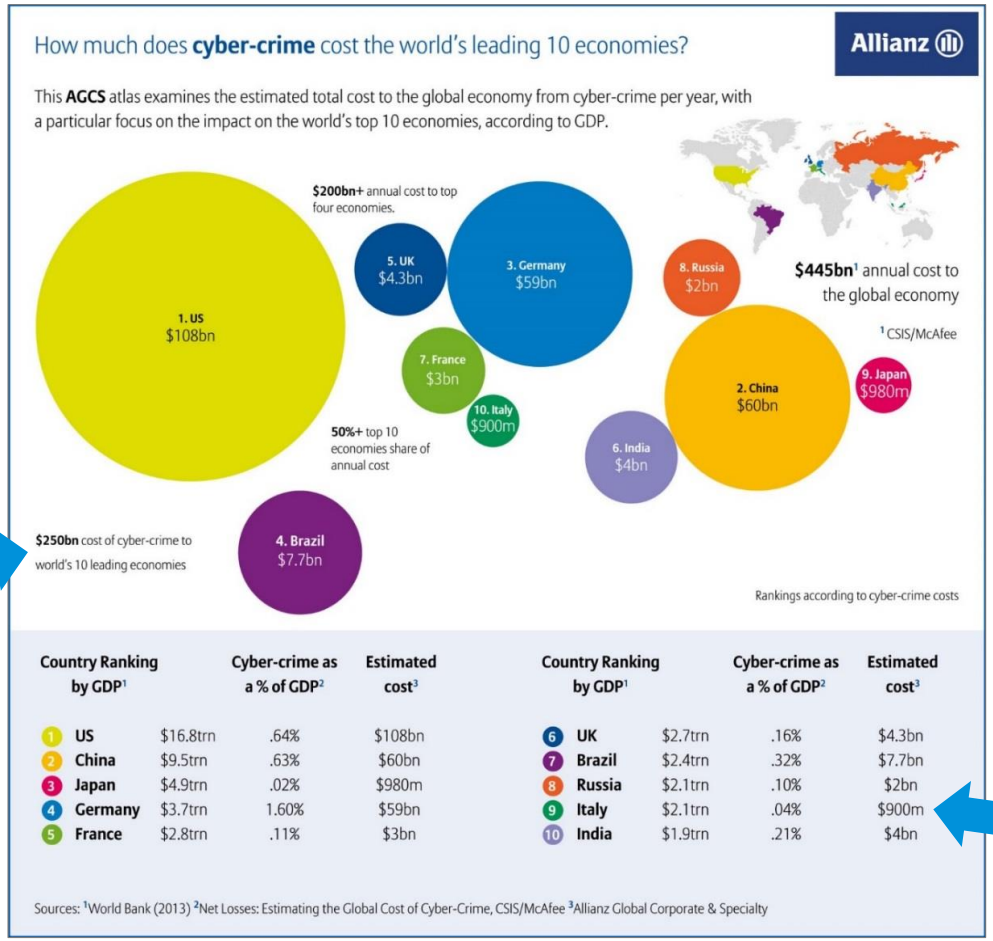


# Il contesto globale - Evoluzione delle minacce - 4




Conseguenze sistemiche del cyber attacco a Dyn. Per molte ore una significativa porzione della rete USA è risultata irraggiungibile a causa di un attacco DDoS contro un fornitore privato di servizi DNS (risoluzione dei nomi di dominio). Tale attacco è stato realizzato tramite centinaia di migliaia di device IoT compromessi.

# Il costo della Cyber (in)Security



KPMG

# Goal: governare la transizione (da Info a Cyber)

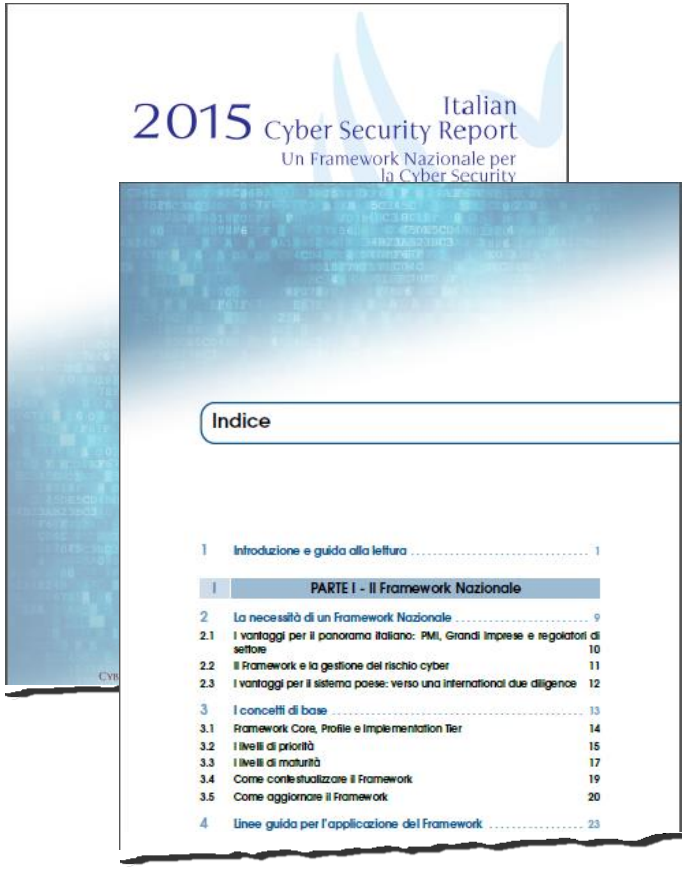
**Esempi e dimostrazioni**

# Framework Nazionale per la Cyber Security

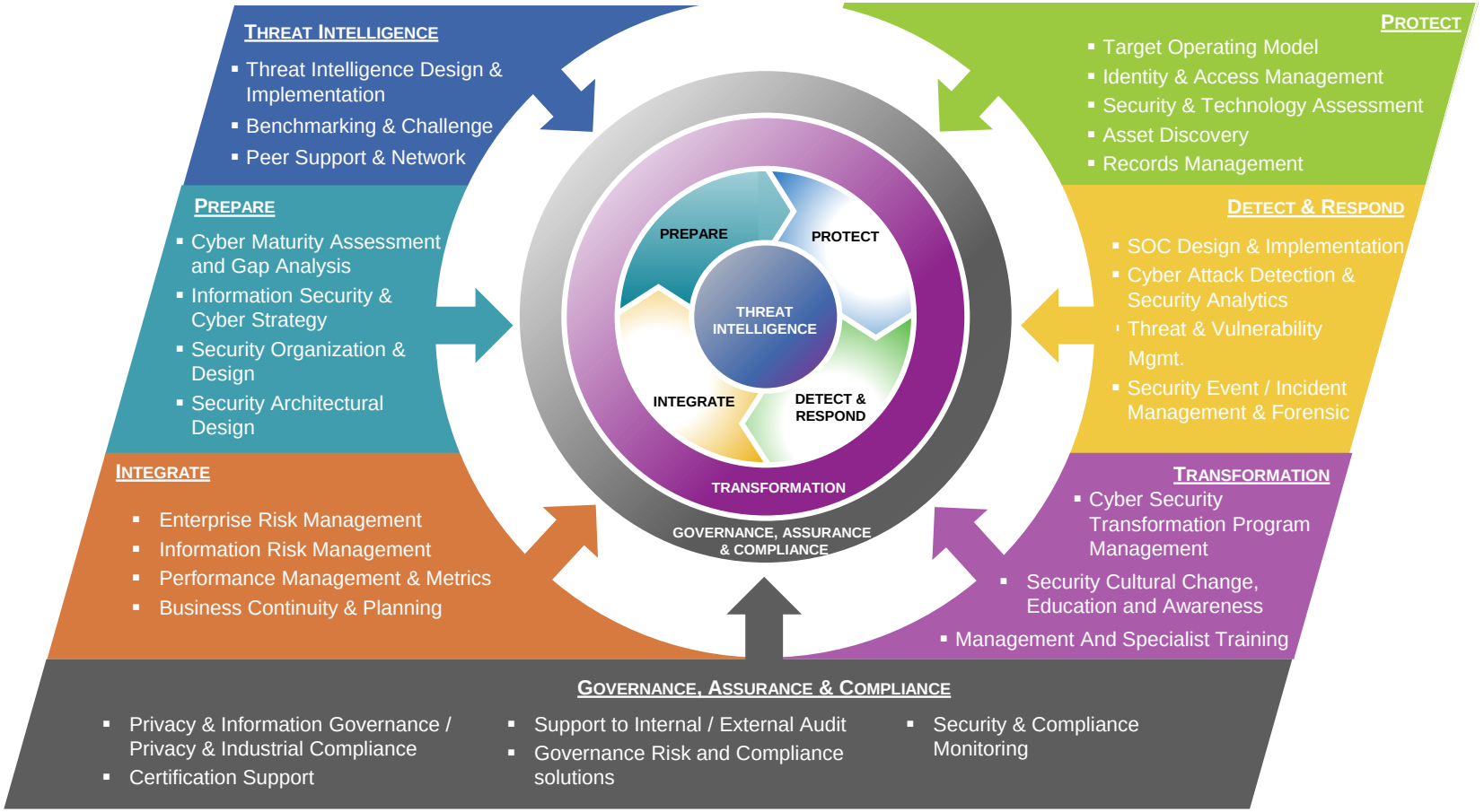
Il **Framework Nazionale per la Cyber Security** formalizza un quadro di riferimento che le aziende possono utilizzare per comprendere il loro livello di preparazione alle minacce cyber e valutare conseguentemente, sulla base dei risultati, le più adeguate misure di riduzione e mitigazione dei rischi.

Redatto con il contributo di **KPMG** il framework presenta un approccio calabile nel contesto di qualsiasi settore, ambito di riferimento e capacità produttiva. Questo grazie alla collocazione agnostica dello stesso che, prescindendo da standard metodologici o tecnologici, permette ad ogni azienda di prendere il framework come riferimento di alto livello e di eseguire le attività di analisi secondo qualsiasi metodologia l'azienda voglia utilizzare.

In tale contesto, **KPMG** ha definito **un proprio approccio personalizzato, che trova compimento nell'unione tra il FNCS e il Cyber Maturity Assessment (CMA), una metodologia di misurazione del livello di maturità aziendale relativamente alle tematiche cyber utile a governare la complessità di questa fase storica di transizione (da InfoSec a CyberSec).**



# Il Framework di Cyber Security di KPMG

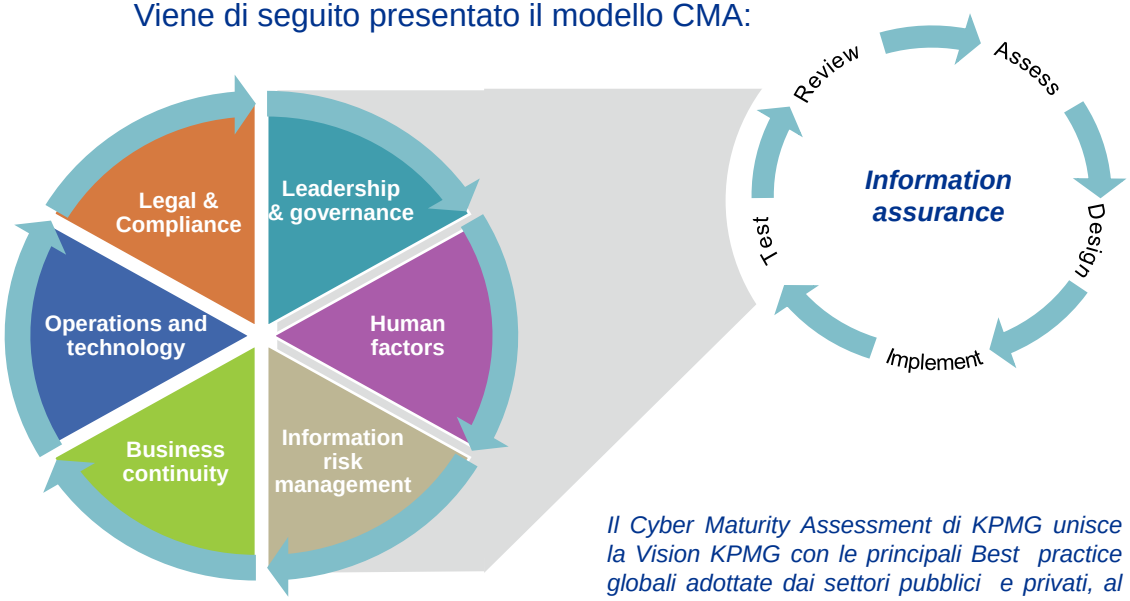


# Cyber Maturity Assessment KPMG

KPMG ha sviluppato un modello di misurazione e valutazione dei principali **rischi** di cybersecurity.

In particolare tramite l'applicazione del Cyber Maturity Assessment (CMA) sviluppato da KPMG è possibile mappare le diverse aree di rischio cyber evidenziate dal FNCS considerando, attraverso l'adozione di un approccio che può essere definito "olistico", non soltanto i fattori (rischi/controlli) prettamente tecnologici.

Viene di seguito presentato il modello CMA:




*Il Cyber Maturity Assessment di KPMG unisce la Vision KPMG con le principali Best practice globali adottate dai settori pubblici e privati, al fine di guidare il cambiamento del business attraverso un approccio basato sull'appropriato utilizzo degli asset informativi.*

**Leadership and governance**

Capacità del Management di governo e di gestione del rischio, delle verifiche e dell'ownership.

**Human factors**

La Cultura sulla Sicurezza delle Informazioni che crea ed assicura le giuste persone, competenze, formazione e conoscenze.

**Information risk management**

L'approccio per raggiungere una completa ed efficace gestione del rischio sulle informazioni e sulla proprietà intellettuale all'interno dell'organizzazione e delle terze parti.

**Business continuity**

Capacità di rispondere ad eventi di sicurezza e di prevenirne o minimizzarne l'impatto attraverso l'efficace gestione delle crisi e degli stakeholder.

**Operations and technology**

Il livello delle misure di controllo implementate all'interno dell'organizzazione per indirizzare i rischi identificati al fine di minimizzare gli impatti derivanti dall'accettazione del rischio.

**Legal & Compliance**

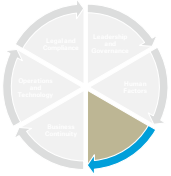
Le metodologie sulle quali l'organizzazione si basa per gestire il rischio di compliance con i requisiti legali rilevanti e con gli standard di riferimento.

# Cyber Maturity Assessment KPMG

## Leadership and Governance

**Capacità del Management di governo e di gestione del rischio, delle verifiche e dell'ownership**

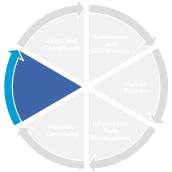
- Policy documentation
- Leadership
- Understanding of Cyber



## Information Risk Management

**L'approccio per la gestione del rischio sulle informazioni e sulla proprietà intellettuale all'interno dell'organizzazione e delle terze parti**

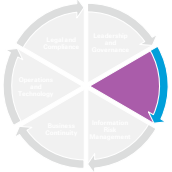
- Information Sharing
- Architecture
- Risk Appetite
- Asset Management
- IRM Processes & Policy
- Third Parties



## Operations and Technology

**Misure di controllo implementate per indirizzare i rischi tecnologici e operativi identificati**

- Personnel Security
- Physical Security
- IAM
- Threat & Vulnerability
- Network Security
- Cyber Hygiene
- Service Delivery
- Logging & Monitoring
- Remote, Mobile & Wireless Security



## Human Factors

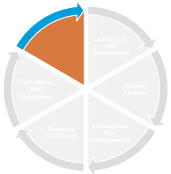
**La Cultura sulla Sicurezza delle Informazioni che crea ed assicura le giuste persone, competenze, formazione e conoscenze**

- Specialist Skills
- Culture
- Training & Awareness
- Talent Management

## Business Continuity and Crisis Management

**Capacità di rispondere ad eventi di sicurezza e di prevenirne o minimizzarne l'impatto**

- BCP with Cyber
- Stakeholder Management
- BIA & Disaster Recovery
- Incident Response



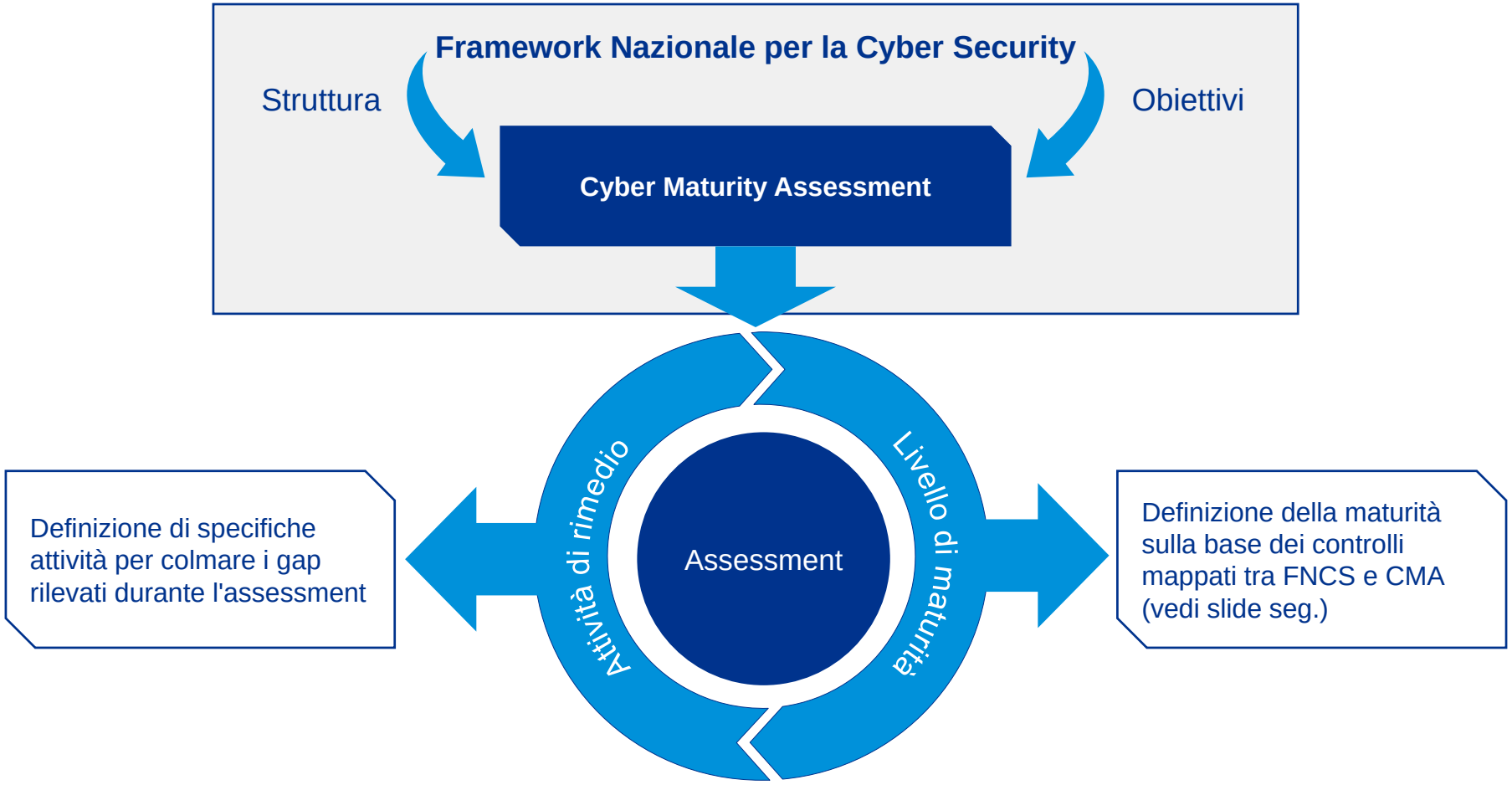
## Legal and Compliance

**Le metodologie per gestire il rischio di compliance con i requisiti legali rilevanti e con gli standard di riferimento**

- Three Lines of Defence
- Financial Risk Transfer
- Legislative Compliance

# FNCS e CMA: la personalizzazione di KPMG

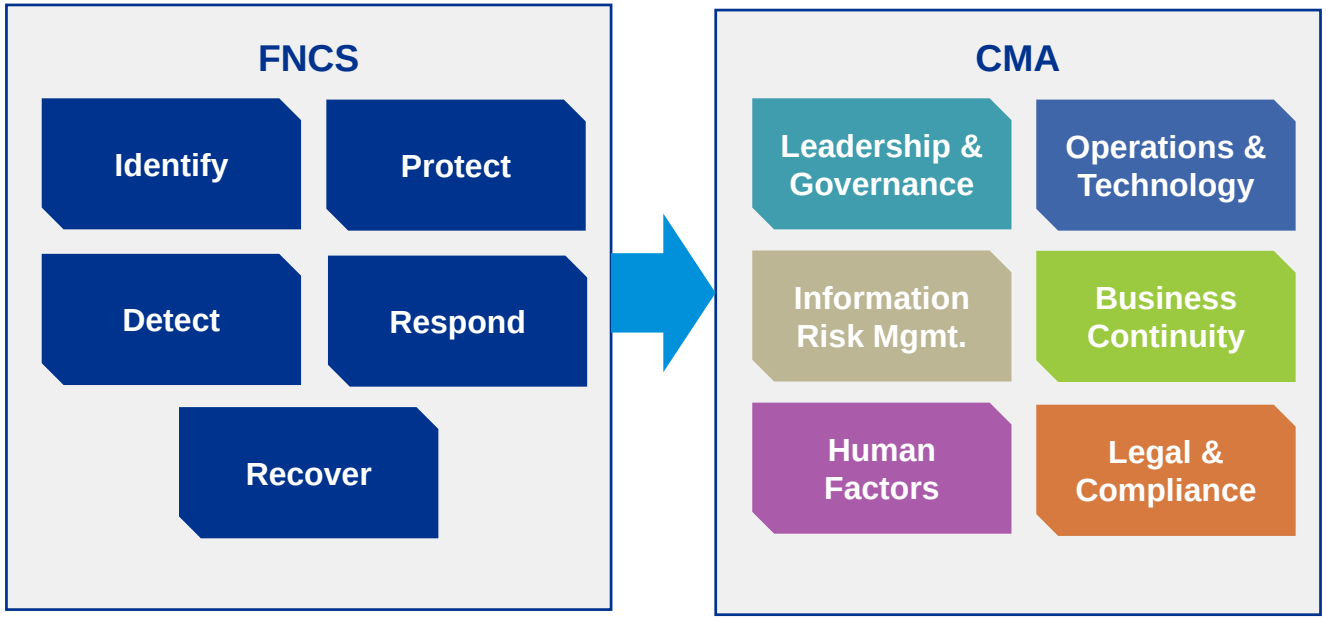
Dall'unione del FNCS e del CMA è stato possibile ricavare una metodologia che permetta a KPMG di valutare **rapidamente** lo stato di maturità cyber dei suoi clienti, mantenendo al contempo la granularità e la **completezza** che contraddistinguono il FNCS.



# Mappatura tra FNCS e CMA

L'implementazione dell'unione tra FNCS e CMA trova compimento, a livello operativo, nella mappatura effettuata tra i controlli del primo con quelli del secondo e arricchita con elementi proprietari e controlli di KPMG.

Nello specifico, i **controlli del FNCS** sono stati **mappati** sulle aree di dominio identificate dal **CMA** al fine di poter indicare in maniera agevole e puntuale quali siano le aree e funzioni coinvolte dalle rilevazioni e, conseguentemente, preparare un **piano di remediation** aderente alle necessità ed all'operatività delle aziende.




La mappatura è stata definita da un team di esperti interni che ha analizzato ogni area di controllo presente nel FNCS, incrociandola con quanto presente all'interno del CMA.

KPMG

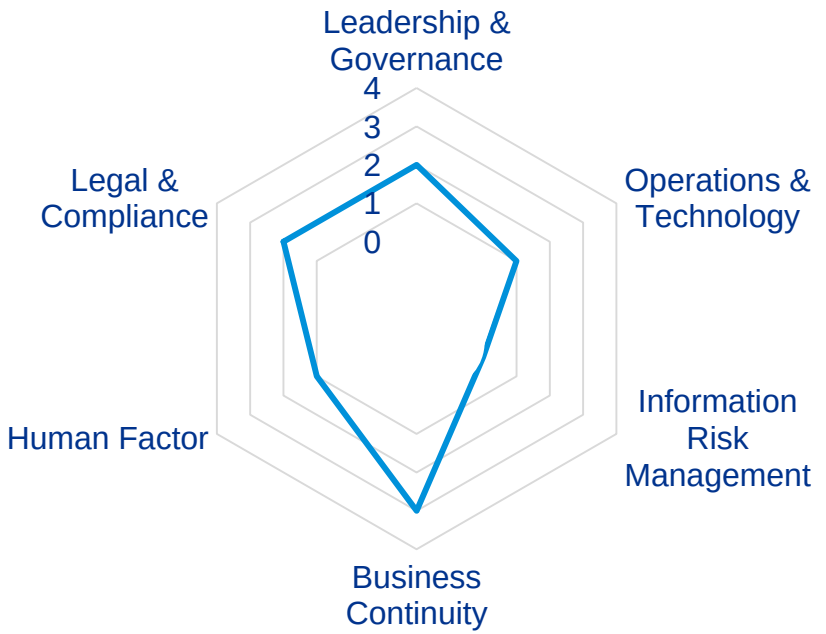
# Cyber Maturity Monitoring & Governance

**Esempi e dimostrazioni**

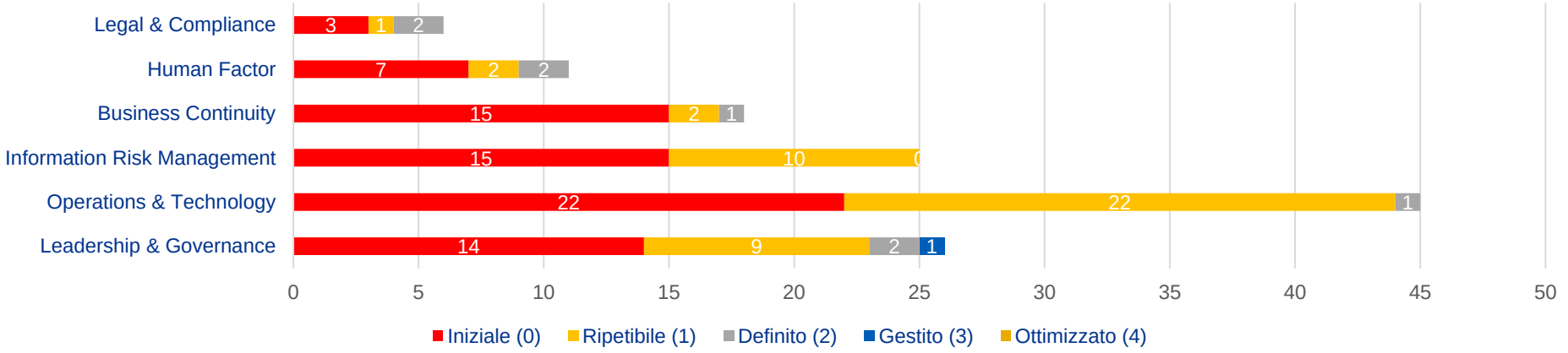
# Presentazione dei risultati

ESEMPIO

| Dominio | Livello di maturità (media) |
|---|---|
| Leadership & Governance | 2 |
| Operations & Technology | 1 |
| Information Risk Management | 0 |
| Business Continuity | 3 |
| Human Factor | 1 |
| Legal & Compliance | 2 |




Numero di controlli per dominio raggruppati per livello di maturità



ESEMPIO

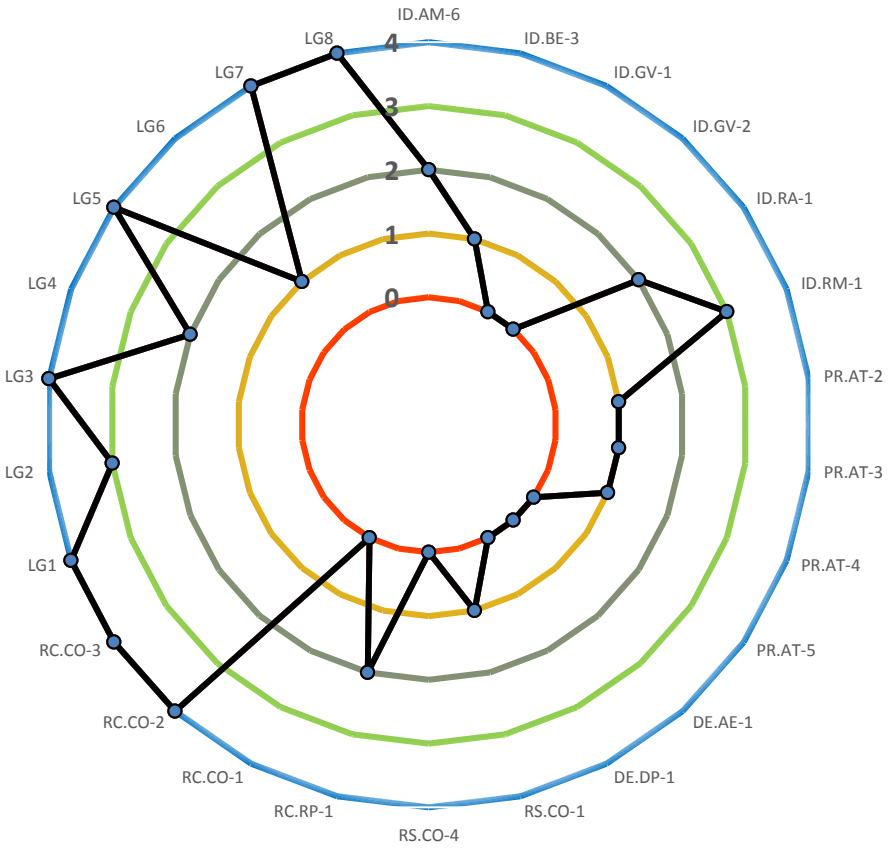
# Dominio: Leadership & Governance

## Punti di forza

- Il board aziendale è perfettamente allineato alle tematiche di cyber security
- Sono state formalizzate le necessarie policy e procedure

## Punti di debolezza

- Il mid-management non risulta sufficientemente allineato alle tematiche di cyber security
- Mancanza di un budget dedicato alla cyber security, adeguato ai rischi e al contesto aziendale



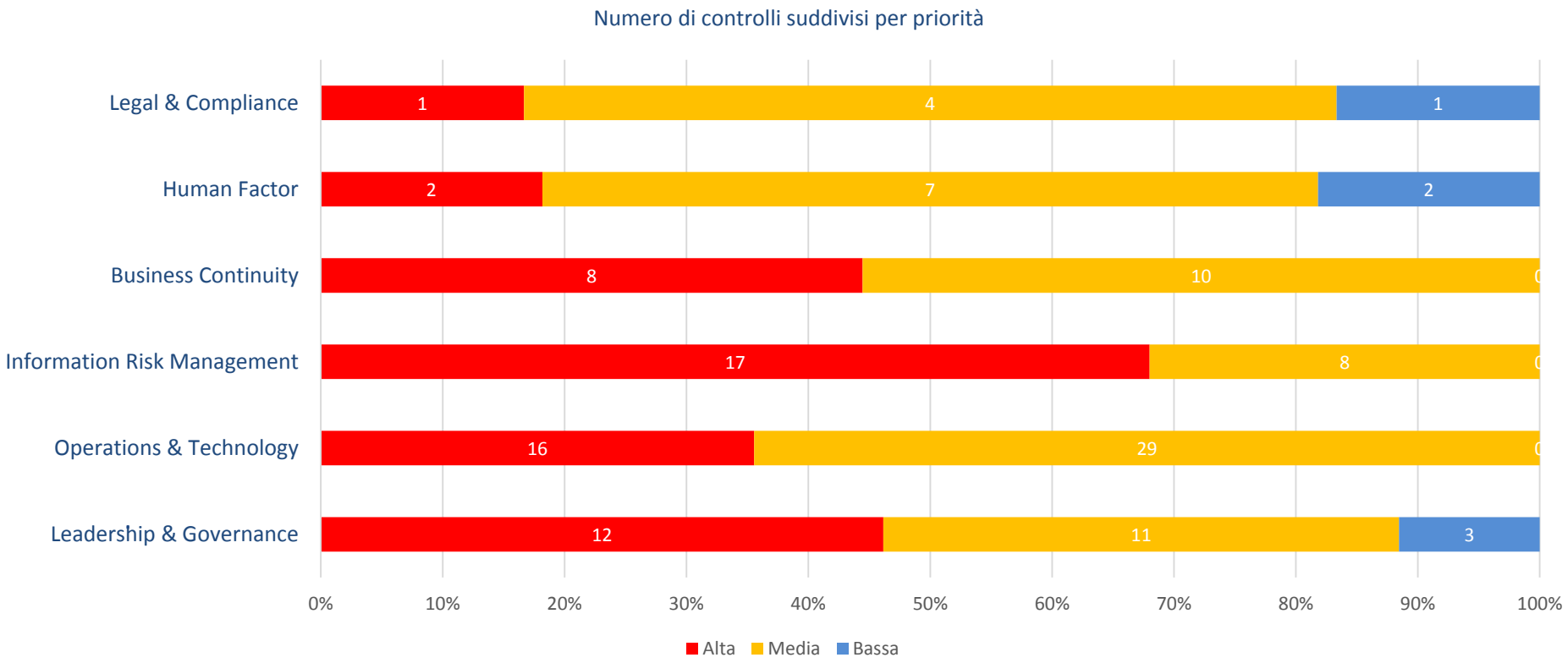

## Principali rischi individuati

- La mancanza di consapevolezza da parte del mid-management espone l'azienda al rischio di errori nella gestione dell'operatività legata alla cyber security
- La mancanza di un budget dedicato non permette di indirizzare adeguatamente alcuni interventi in ambito cyber security già avviati

# Attività di rimedio e migliorative

ESEMPIO

A seguito delle analisi svolte, sono state definite delle attività di rimedio con l'obiettivo di supportare il Cliente nel miglioramento del livello di maturità in ambito cyber security. Inoltre, sulla base del contesto su cui opera il Cliente e sulla nostra esperienza, per ogni attività è stato definito un livello di priorità.



# Attività di rimedio e migliorative

ESEMPIO

✓ Attività "Quick Win"

## Information Risk Management

| Dominio | Iniziativa | Attività | Criticità | Complessità |
|---|---|---|---|---|
| Information Risk Management | Definizione di una politica per la classificazione delle informazioni | ◦ Definizione delle procedure di classificazione dei dati<br>◦ Definizione di politiche di gestione delle informazioni classificate | Alta | Media |
| Information Risk Management | Definizione di un processo di risk management che tenga conto delle tematiche relative alla cybersecurity | ◦ Definizione di procedure di risk assessment<br>◦ Definizione di un piano di raggiungimento e mantenimento della soglia di tolleranza al rischio identificata | Alta | Alta |
| Information Risk Management | Definizione di un processo strutturato e formalizzato di verifica dei rischi derivanti da contratti di fornitura con terze parti | ◦ Definizione di proecedure di assessment di terze parti e fornitori<br>◦ Implementazione di tool per la verifica ed il monitoraggio di terze parti e fornitori (es. questionari e cruscotti)<br>◦ Definizione di requisiti di sicurezza IT ai quali i fornitori devono risultare conforme | Bassa | Bassa |

✓

# Piano strategico di massima

ESEMPIO

Il 2017-2019 può prevedere il consolidamento delle iniziative avviate nel 2016 e l'avvio di iniziative per la protezione delle informazione e la continuità operativa.

## 2017

Iniziative finalizzate a **consolidare** i progetti avviati nel corso del 2016, **valutare** il livello di esposizione dei rischi cyber e **predisporre** di una strategia di dettaglio.
Per il **2017** sono state proposte le seguenti iniziative:

- **Definizione ruoli e responsabilità**
- **Policy relative alla Sicurezza delle Informazioni**
- **Security Awareness**
- **Patch Management**
- **Cyber Risk Management**
- **Policy per la classificazione delle informazioni**
- **Gestione degli incidenti di sicurezza**

## 2018

Iniziative volte ad **implementare** processi e soluzioni tecnologiche.
Per il **2018** sono state proposte le seguenti iniziative:

- **Processo di VA/PT**
- **Change Management**
- **Business Impact Analysis (BIA)**
- **Log Management & SIEM**
- **Gestione degli asset**
- **Gestione degli accessi (fisici / logici)**
- **Identity Access Management (IAM)**

## 2019

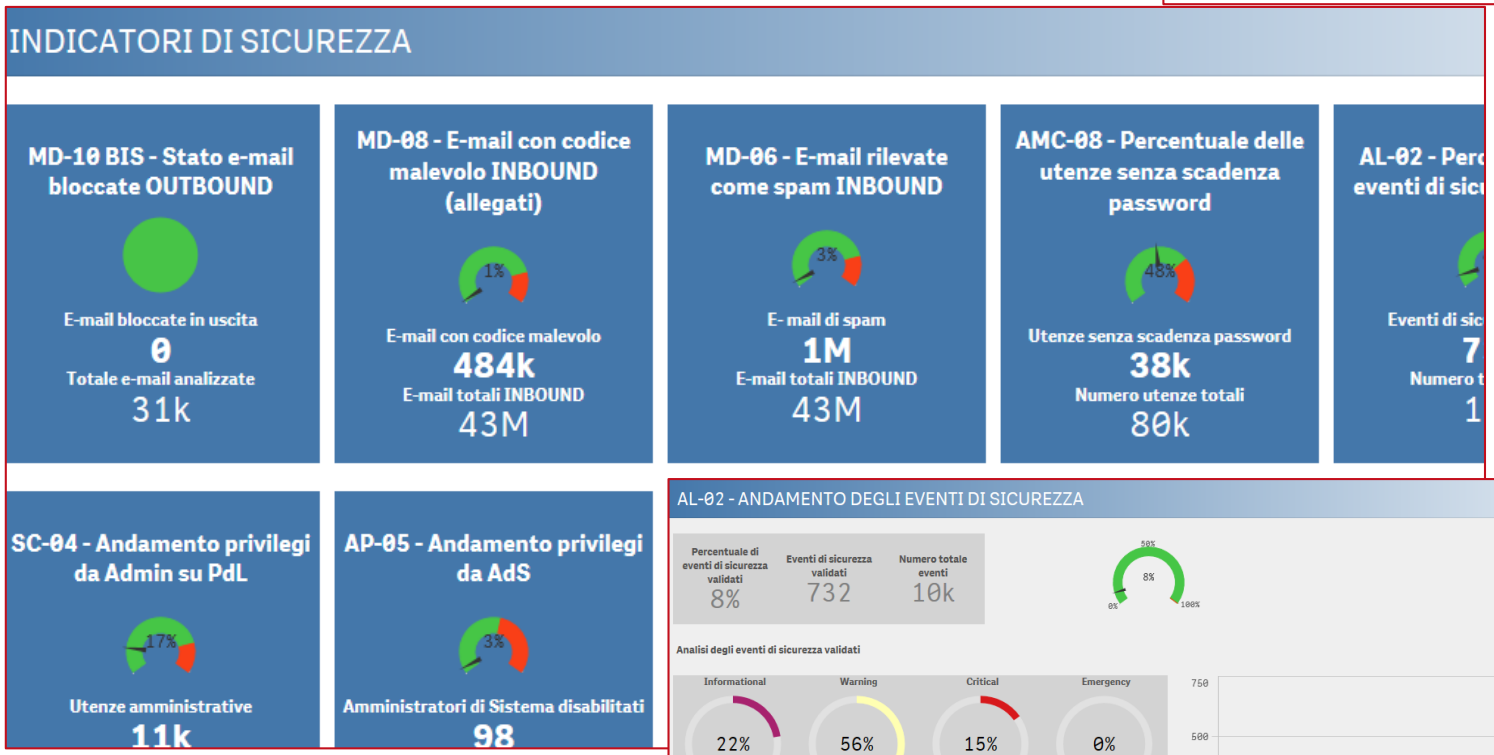
Iniziative rivolte al miglioramento del livello di maturità generale.
Per il **2019** sono state proposte le seguenti iniziative:

- **Internal Auditing**
- **Certificazioni aziendali e personali**
- **Business Continuity / Disaster Recovery Plan**
- **Gestione terze parti**

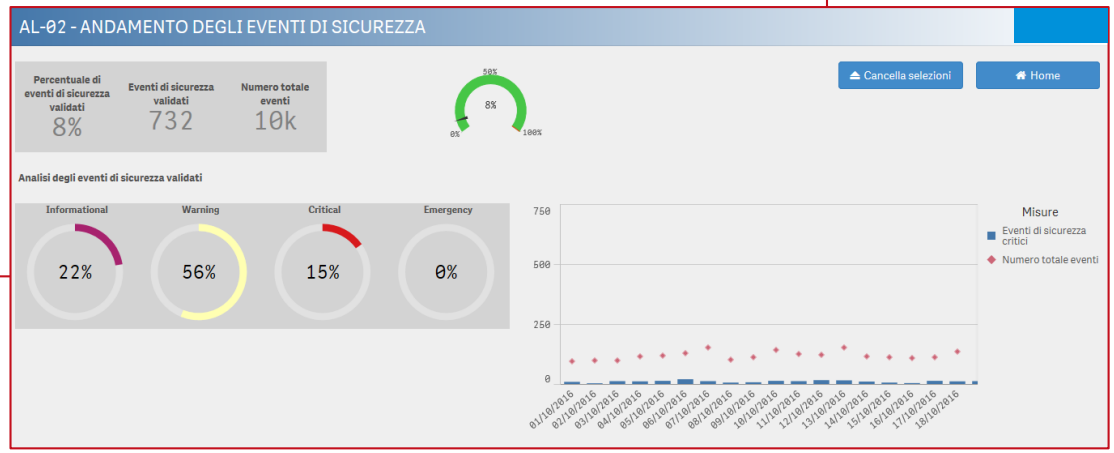
# Monitoraggio Cyber Trends

ESEMPIO

Dashboard di presentazione dei KPI




Esempio di dettaglio KPI



KPMG

# Grazie

**Andrea Zapparoli Manzoni**

Senior Manager

azapparolimanzoni@kpmg.it

**kpmg.com/socialmedia**


**kpmg.com/app**