



Management of cybersecurity governance in healthcare infrastructures

Raniero Rapone

Aon Hewitt Cyber Risk Unit Team Manager

Funded by the European Commission
Horizon 2020 – Grant # 740129



Cybersecurity Governance Meaning

To Govern the cyber security means:

- Know the IT Resources I need to protect
- Know how I can protect these resources
- Know how I can understand if my IT resources are under attack
- Know how I can respond to an attack
- Know how I can restore my resources if they have been compromised

Cybersecurity Governance Model (ISMS)

The Modern Cyber Security Governance model
is based on:


- “Conceptual Areas”
- “Categories” able to describe a single objective in order to map an area as better as possible.
- "Controls to be implemented" able to achieve the objective of each category



Cybersecurity Governance Model in PANACEA

What we are doing in PANACEA Project about Cyber Security Governance:

- Select of the best Controls for the Healthcare
- Bind them to the Standards or Healthcare regulations



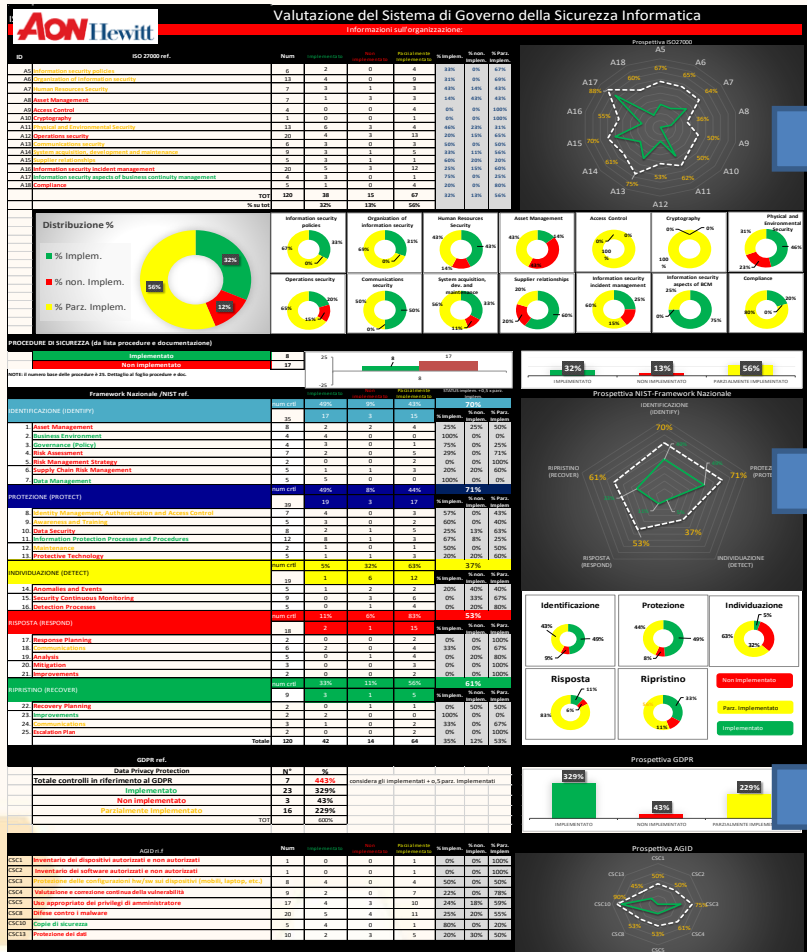
Standard's relationship (ISO27k, FN, NIST, etc)

VISTE DATI	AREA	CATEGORIA	Obiettivo di controllo	Valutazione	Pesi	Evidenze de
Valutazione	IDENTIFICAZIONE (IDENTIFY)	Asset Management	Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione, ovvero è in essere una soluzione (es. software ADM) che permetta di identificare le risorse informatiche dell'organizzazione e le informazioni sulle stesse di varia natura, es. assegnatario, ruolo nei processi business, stato di manutenzione, livello di trattamento dei dati, etc.)	Parzialmente Implementato	3	
AREA	IDENTIFICAZIONE (IDENTIFY)	Asset Management	Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione, ovvero è in essere una soluzione (es. software ADM) che permetta di identificare le risorse informatiche dell'organizzazione e le informazioni sulle stesse di varia natura, es. assegnatario, ruolo nei processi business, stato di manutenzione, livello di trattamento dei dati, etc.)	Parzialmente Implementato		
CATEGORIA	IDENTIFICAZIONE (IDENTIFY)	Asset Management	I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati, ovvero è in essere una soluzione o meglio una mappatura dei flussi di comunicazione tra le varie risorse IT che supportano i processi business critici e non critici	Parzialmente Implementato		
	IDENTIFICAZIONE (IDENTIFY)	Asset Management	I sistemi informativi dell'organizzazione ma critici per l'organizzazione sono note le informazioni di assegnatario, ruolo nei processi business, stato di manutenzione, pa	Non Implementato		

VISTE DATI	ID	Cod	AREA	CATEGORIA	Obiettivo di controllo	Valutazione	NIST	ISO27k	FN	COBIT 5	cis csc
Valutazione	36	8.1	PROTEZIONE (PROTECT)	Identity Management, Authentication and Access Control	Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrare (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrare, verificate, revocate e sottoposte a audit sicurezza)	Parzialmente Implementato					
AREA											
CATEGORIA											
	37	8.2	PROTEZIONE (PROTECT)	Identity Management, Authentication and Access Control	L'accesso fisico alle risorse è protetto e amministrato	Implementato					
	38	8.3	PROTEZIONE (PROTECT)	Identity Management, Authentication and Access Control	L'accesso remoto alle risorse è amministrato	Implementato					
	39	8.4	PROTEZIONE (PROTECT)	Identity Management, Authentication and Access Control	Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del	Parzialmente Implementato					

Set of Controls

Cybersecurity Governance Outcomes in PANACEA



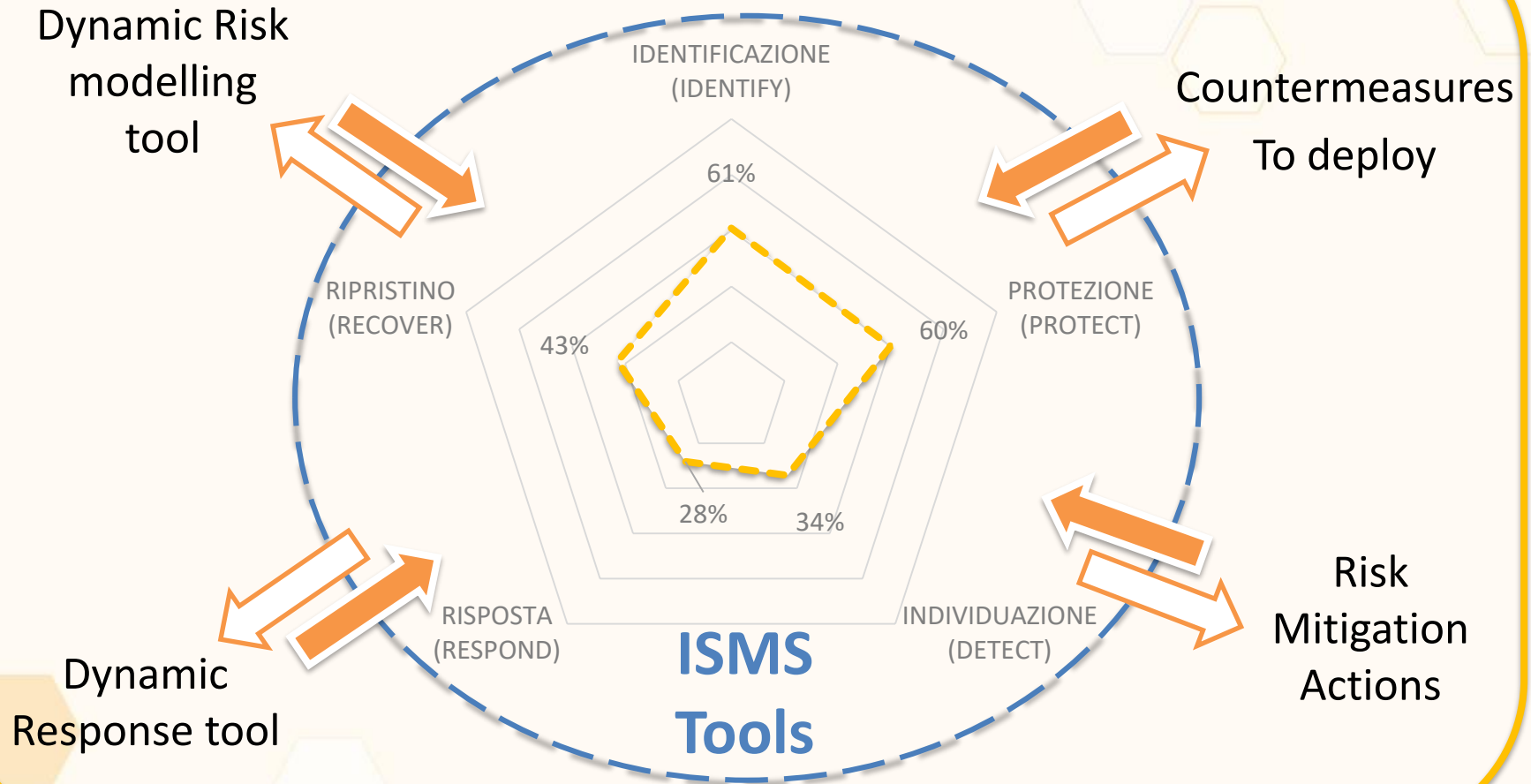
Overview of the Cyber Security Governance

ISMS Deep analysis (detailed gaps per Categories)

Prioritization according to the best Standards

Cybersecurity Governance Tool in PANACEA

PANACEA FRAMEWORK





THANK YOU!

Raniero Rapone

Aon Hewitt Cyber Risk Unit Team Manager

Contacts:

Email: Raniero.Rapone@aon.it

Linkedin : <https://www.linkedin.com/in/raniero-rapone-5740298/>

Funded by the European Commission
Horizon 2020 – Grant # 740129

