Avv. Massimiliano

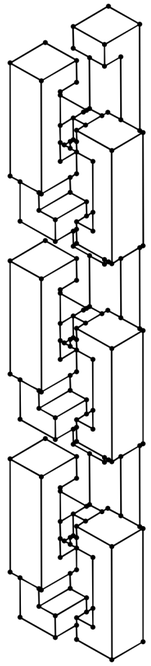
Parla

LA SANITÀ TECNOLOGICA E LA COMPLIANCE NORMATIVA

AREZZO FORUM RISK 2023

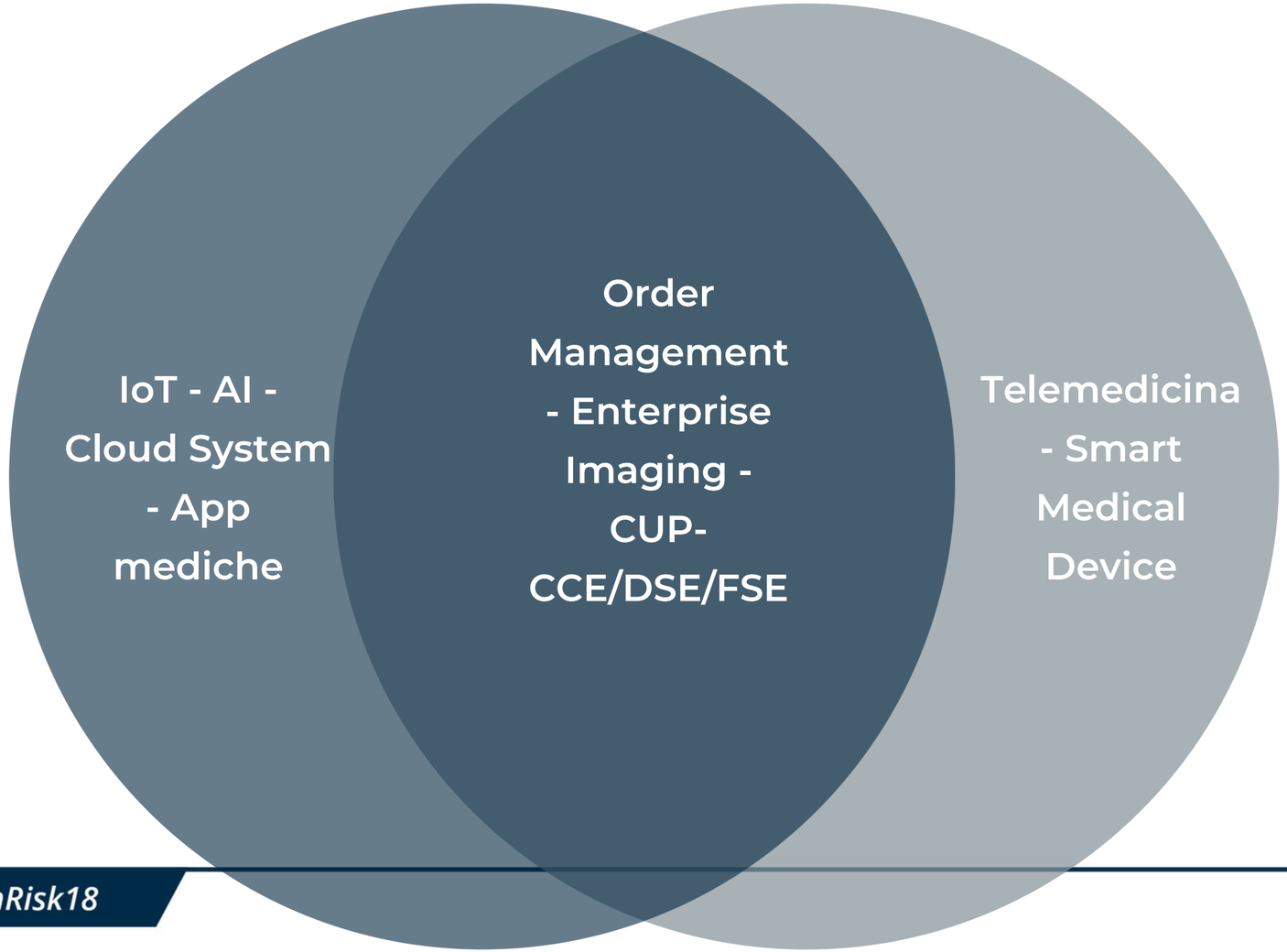
La Sanità Tecnologica e la Gestione del Rischio in Sanità non possono **oggi** non prendere in considerazione la necessaria compliance normativa in tema Cyber Security

- CAD 2005
- Linee Guida AgID
- DPCM 81/2021
- Framework ACN
- NIS 2 Directive
- GDPR
- ISO 27001 - 27701 - 17065
- Euro Privacy Certification



- Rating → GDPR / CYBER SECURITY
- Compliance integrata in ottica G-Core
- Auditing Supplier documentato
- Risk Analysis & Management

SANITÀ TECNOLOGICA & DATA ENTRY



L'applicazione tecnologica in Sanità deve passare per:

Progettazione di un perimetro by design per i dati personali G-Core

Implementazione di un perimetro di controlli e sicurezza informatica

Attuazione di politiche di valutazione e di gestione del rischio

The list of criteria, and checks and controls

- Homogeneous and consistent certifications
- Divers categories of data processing activities
- GDPR Core Criteria
- Contextual checks and controls
  - Complementary contextual checks and controls
  - Technical and Organisational Measures
  - National Obligations checks and controls

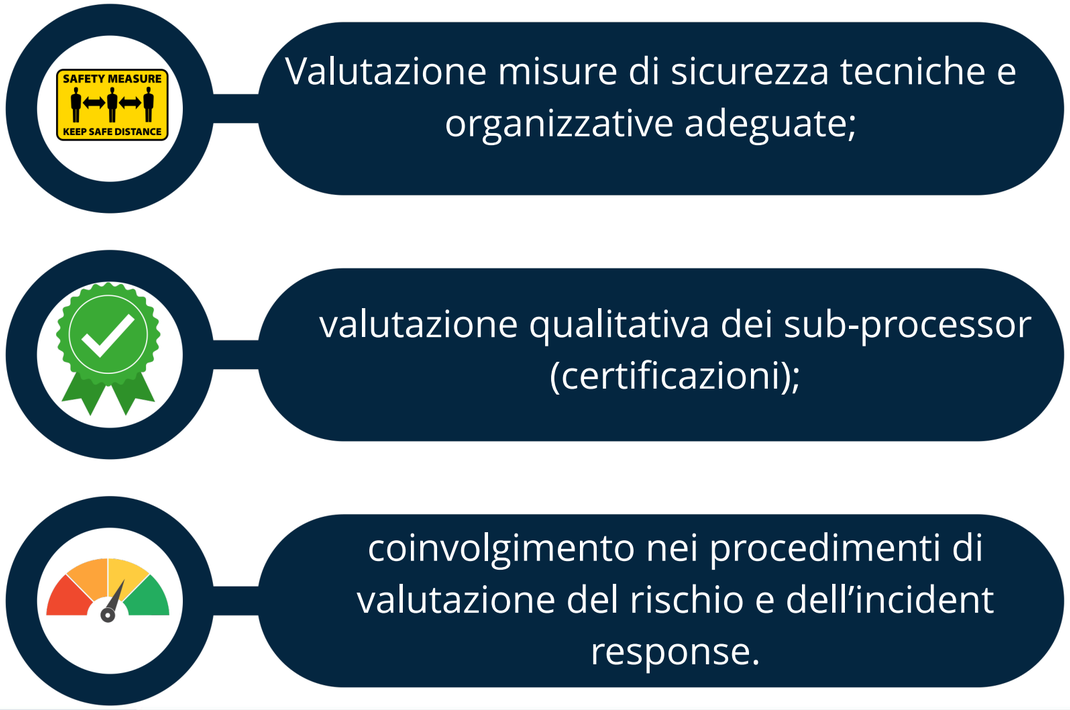
MATRIX OF APPLICABILITY

Integrazione di schemi normativi e di compliance in chiave multidisciplinare per rispondere a differenti esigenze di:

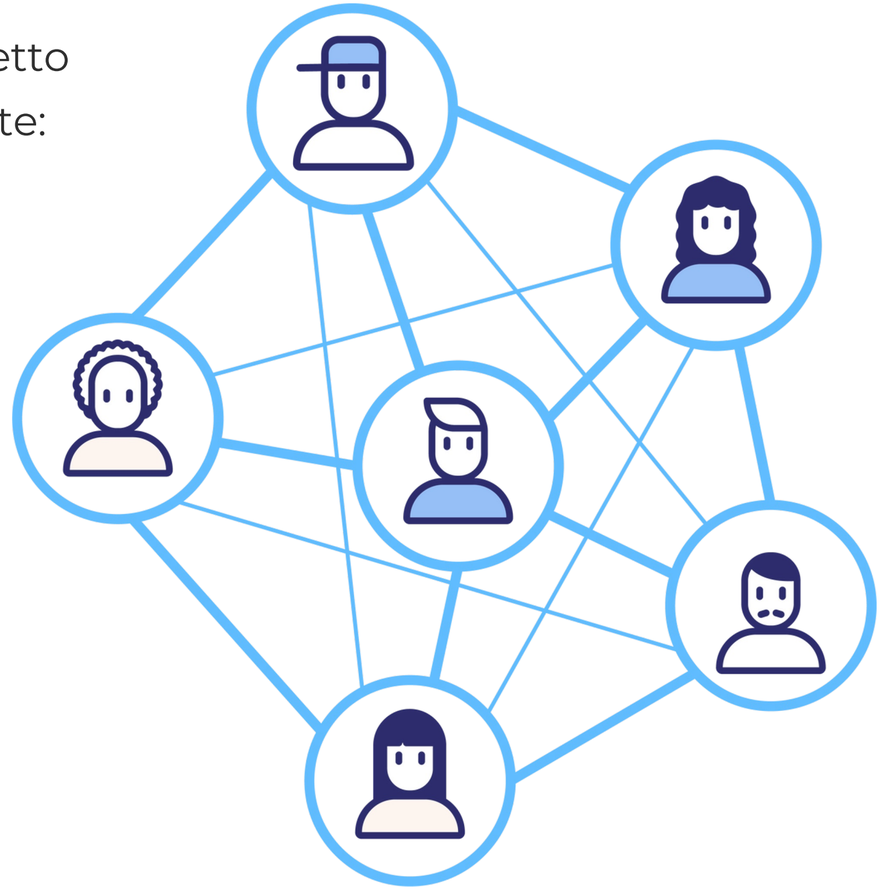
- Definizione del contesto interno ed esterno con individuazione della c.d. Supply Chain;
- Valutazione del rischio aziendale;
- Sicurezza Asset e Infrastrutture Strategiche

TECHNICAL & ORGANISATIONAL MEASURES (TOM) SUPPLIER AUDITING

Punto nodale e imprescindibile dell'avanzata della Sanità digitale è un corretto inquadramento dei primari Supplier tecnologici di riferimento, con coneguente:



- Valutazione misure di sicurezza tecniche e organizzative adeguate;
- valutazione qualitativa dei sub-processor (certificazioni);
- coinvolgimento nei procedimenti di valutazione del rischio e dell'incident response.



L'ANALISI E LA VALUTAZIONE DEL RISCHIO

Secondo i principi dettati dalla norme internazionali di riferimento

id	Processo / Funzione coinvolta e singola attività sensibile	Rischio	Causa della problematica *(perché potrebbe succedere...)*	Metodo di controllo attuale *(cosa si fa per evitare che il rischio si concretizzi)*	D	P	Indice Rischio effettivo
2	Sicurezza delle Informazioni/Informatica						
2.3	*Accesso alle immagini sistema RIS/PACS*	Violazione del principio RID con riguardo alle informazioni rilevanti dell'organizzazione	Mancata definizione di un perimetro di sicurezza informatica aziendale	Draft di disciplinare accessi gestionale RIS/PACS xxx - rev. x/xxxx	4	4	16
2.4	*Business Continuity per l'erogoazione del servizio CUP*	Interruzione nella continuità dell'attività dell'organizzazione	Incidenti di natura informatica che possono influire in merito alla corretta erogazione dei servizi istituzionali	Procedura operativa xxx - Business Continuity serv. CUP rev. x/xxxx	4	2	8

L'ANALISI E LA VALUTAZIONE DEL RISCHIO

Secondo i principi enucleati dalle norme internazionali di applicazione volontaria

id	Rilevazioni in merito ai controlli previsti (es. *mancata o incompleta attuazione che giustifica un indice di rischio alto*)	Azioni di *remediation* raccomandate	Azioni effettivamente attuate	Data di attuazione dell'azione	D	P	Indice Rischio residuo
2							
2.3	è stata rilevata, allo stato, la mancata adozione e diffusione ai dipendenti del disciplinare in parola.	Si consiglia l'implementazione e la formale adozione del disciplinare appositamente predisposto per il tema in parola con contestuale diffusione, pubblicazione sull'intranet e formazione degli utenti abilitati.	Trasmissione alla *governance* di *alert* relativo alla mancanza rilevata.	xx/xx/xxxx	4	4	16
2.4	è stata rilevato, allo stato, la puntuale attuazione della procedura in parola.	Si consiglia di calendarizzare periodicamente monitoraggi relativi alla concreta e di procedere a revisioni della *policy* contente i più recenti aggiornamenti sul terma	Revisione della procedura alla luce delle più recenti linee guida	xx/xx/xxxx	4	1	4

Avv. Massimiliano
Parla

GRAZIE PER L'ATTENZIONE

AREZZO FORUM RISK 2023