



21-24 NOVEMBRE 2023

AREZZO FIERE E CONGRESSI

21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI

18

18

 *Avv. Massimiliano*
Parla

LA SANITÀ TECNOLOGICA E LA COMPLIANCE NORMATIVA

AREZZO FORUM RISK 2023

#ForumRisk18



www.forumriskmanagement.it

#ForumRisk18

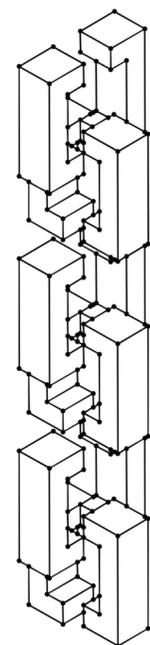
Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001



www.forumriskmanagement.it

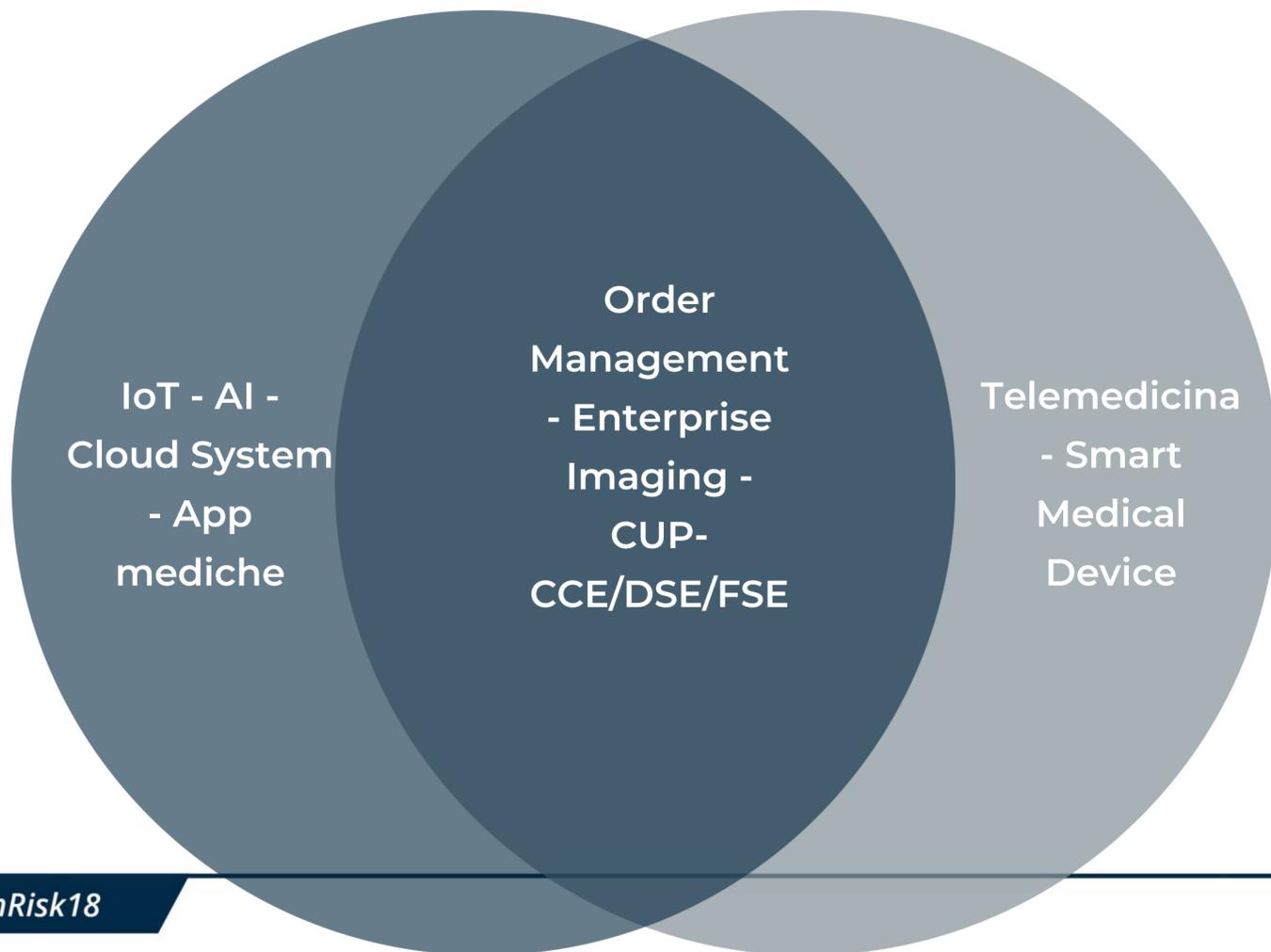
La Sanità Tecnologica e la Gestione del Rischio in Sanità non possono **oggi** non prendere in considerazione la necessaria compliance normativa in tema Cyber Security

- 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



#ForumRisk18

MATRIX OF APPLICABILITY

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

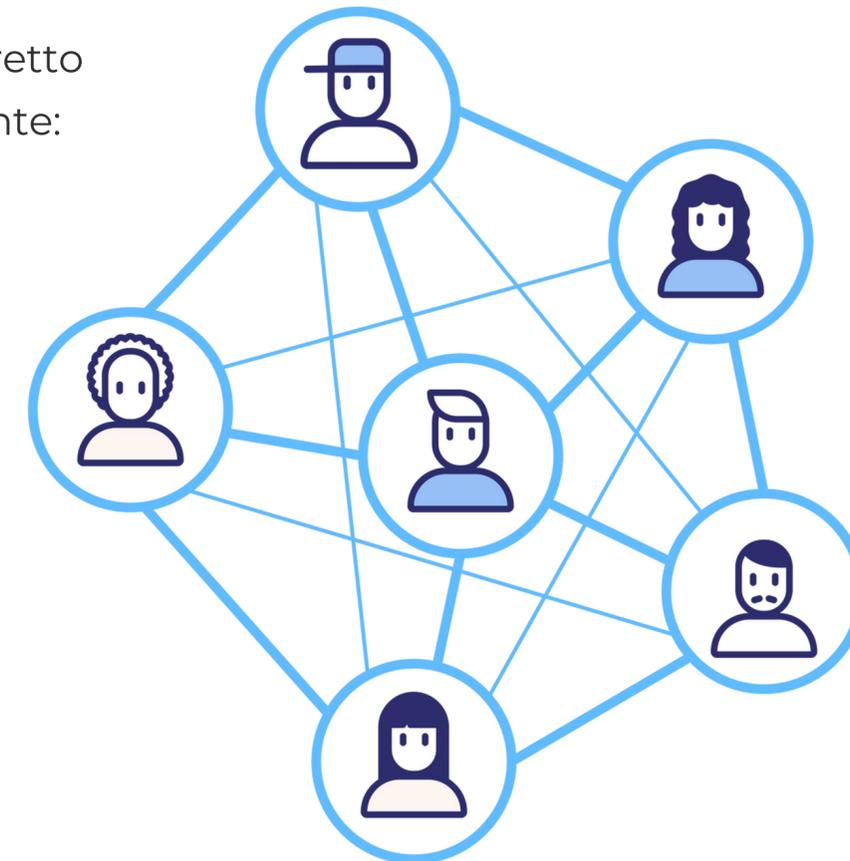
- Definizione del **contesto interno ed esterno** con individuazione della c.d. **Supply Chain**;
- Valutazione del **rischio** aziendale;
- **Sicurezza Asset** e Infrastrutture Strategiche



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 conegunte:

-  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'erogazione 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 <i>governance</i> di <i>alert</i> 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 <i>policy</i> contenente i più recenti aggiornamenti sul tema	Revisione della procedura alla luce delle più recenti linee guida	xx/xx/xxxx	4	1	4



21-24 NOVEMBRE 2023

AREZZO FIERE E CONGRESSI

21-24 NOVEMBRE 2023
AREZZO FIERE E CONGRESSI

18

18

 *Avv. Massimiliano
Parla*

GRAZIE PER L'ATTENZIONE

AREZZO FORUM RISK 2023

#ForumRisk18



www.forumriskmanagement.it

#ForumRisk18

Del presente documento è severamente vietata ogni abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico, ai sensi della Legge n. 633/1941 e dell'Art. 25-novies, D.Lgs. n. 231/2001



www.forumriskmanagement.it

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

[Torna all'inizio](#)