

Linee Guida per la

Validazione dei Sistemi Software per l'adozione in contesti di Ricerca



Hanno partecipato al progetto:



POLICLINICO DI **SANT'ORSOLA**

Gruppo di Lavoro AISIS

COORDINATORI

Luca Capitani

CIO Azienda Ospedaliero Universitaria S. Orsola, IRCCS, Bologna

Marco Foracchia

CIO Azienda USL di Reggio Emilia, IRCCS

PARTECIPANTI

Antonia Bianchi, *Ospedale San Raffaele, IRCCS*

Maria Cammarota, *ASL BT*

Fabiola Casullo, *ASL Avellino*

Sara Cazzaniga, *IQVIA*

Fabio Collura, *ISMETT, IRCCS*

Lara D'Amico, *Azienda USL di Parma, Azienda Ospedaliero universitaria di Parma*

Francesca De Giorgi, *Istituto Neurologico "Carlo Besta" IRCCS*

Alice Dalla Torre, *Dedalus Italia S.p.A.*

Paola Falorio, *Azienda Ospedaliero Universitaria S. Orsola, IRCCS, Bologna*

Christian Fedeli, *IQVIA*

Martina Francesconi, *ESTAR, Toscana*

Giulio Gatti, *Azienda USL di Reggio Emilia, IRCCS*

Anna Giardini, *ICS Maugeri, IRCCS*

Roberta Lo Giudice, *Fondazione Toscana Gabriele Monasterio*

Maurizio Mangione, *Fondazione Toscana Gabriele Monasterio*

Monica Moz, *Dedalus Italia S.p.A.*

Andrea Nitrosi, *Azienda USL di Reggio Emilia, IRCCS*

Giuseppina Pagliarello, *Azienda USL di Parma, Azienda Ospedaliero universitaria di Parma*

Greta Perselli, *Fondazione Toscana Gabriele Monasterio*

AnnaRita Pettinato, *Azienda USL di Ferrara e Azienda Ospedaliero - Universitaria di Ferrara*

Donata Pezzuto, *Senior GxP Quality Advisor and Auditor, Qualified Person/PRRC*

Francesca Pierin, *Azienda USL di Ferrara e Azienda Ospedaliero - Universitaria di Ferrara*

Pierluigi Previtali, *Ospedale San Raffaele, IRCCS*

Laura Reiss, *Ospedale San Raffaele, IRCCS*

Ilaria Riela, *Centro Specialistico Ortopedico Traumatologico Gaetano Pini - CTO*

Marco Sergio, *ISMETT, IRCCS*

Alessandro Testa, *ASL Napoli 3 Sud*

Laura Verzellesi, *Azienda USL di Reggio Emilia, IRCCS*

0 _ Indice

1 _	Prefazione	5
2 _	Introduzione	7
3 _	Obiettivi	9
4 _	Metodologia Adottata	12
4.1 _	Limitazioni d'uso della metodologia	12
4.2 _	Limitazione nella Valutazione del Rischio	13
4.3 _	Qualificazione e Analisi del Processo	13
4.4 _	Parametrizzazione	14
5 _	Il Processo di Validazione dei Sistemi Software Clinici adottati per Attività di Ricerca	15
5.1 _	Identificazione dei Casi d'Uso – Use Case Definition	16
5.2 _	Identificazione e Classificazione dei Sistemi Software Coinvolti Software Ecosystem Definition	18
5.2.1 _	Criteri di inclusione/esclusione dalla compilazione della scheda di prodotto	18
5.3 _	Qualificazione del Produttore e del Sistema Software Manufacturer Qualification and System Qualification	18
5.4 _	Qualificazione del Contesto di Installazione Installation Site Qualification	20
5.5 _	Valutazione del Rischio dell'Ecosistema Software e Identificazione delle Azioni di Mitigazione del Rischio	22
6 _	Conclusione e Sviluppi Futuri	25
7 _	Riferimenti Normativi e Bibliografici	26
8 _	Acronimi	27
9 _	Appendice - Schema di Rilevazione	28
9.1 _	Identificazione del Caso d'uso e dell'Ecosistema Software	28
9.1.1 _	Parametrizzazione	30
9.1.2 _	Sistema di Calcolo	30
9.2 _	Qualificazione del Produttore e Sistema Software	31
9.3 _	Qualificazione del Sito di Installazione	35

1 _ Prefazione

Le linee guida e la metodologia presentate in questa pubblicazione di AISIS nascono da una esigenza espressa da molti operatori del settore ICT sanitario, associati e simpatizzanti.

La natura stessa del settore della Sanità Digitale, chiamato istituzionalmente a garantire la sicurezza delle cure e la protezione dei dati dei cittadini e degli assistiti, comporta da sempre la necessità di conformarsi a normative specifiche e di sottoporsi a verifiche da parte di enti di diversa natura e livello.

L'applicazione "by design" di requisiti normativi e indicazioni derivanti da linee guida rappresenta una prassi quotidiana per gli operatori del settore al fine di garantire la conformità ai principi stabiliti dai diversi livelli regolatori. Questo mandato di interpretazione e applicazione non riguarda solo i singoli sistemi, ma si estende altresì al complesso ecosistema derivante dalla integrazione di un numero anche significativo di componenti software e infrastrutturali.

Il ruolo dei nostri operatori va quindi oltre la semplice applicazione di normative, implicando sempre più spesso l'interpretazione, la declinazione e l'integrazione di più aspetti regolatori al fine di garantire la rispondenza senza però compromettere le destinazioni native e le funzionalità degli strumenti digitali a supporto dell'attività sanitaria.

Diventa quindi quotidianità lo sforzo sia metodologico che operativo di armonizzazione e convergenza di GDPR, NIS2, MDR, IVDR, Linee Guida Internazionali, Linee Guida e disposizioni nazionali e regionali.

Questo quadro regolatorio eterogeneo e molto articolato presenta il più delle volte elementi di ridondanza dei principi e delle modalità implementative, ma è doveroso sottolineare che non mancano, seppure minoritari, esempi di apparente incoerenza tra prescrizioni derivanti da contesti normativi differenti. Ne deriva quindi una necessità di interpretazione ma anche di definizione delle priorità di rispondenza, in carico al CIO o altre figure dirigenziali che, in ultima istanza, si assumono la responsabilità e l'onere della scelta tecnico-finanziaria di implementare le necessarie misure.

In questo quadro già molto complesso, le strutture sanitarie che hanno esteso o hanno nativamente nel loro mandato l'attività di ricerca clinica o clinico-organizzativa, si confrontano da sempre con ulteriori vincoli e prescrizioni derivanti dalla necessità di garantire ai promotori e agli enti regolatori dell'attività di ricerca una adeguata qualità sul trattamento del dato (ed anche la garanzia di tutela della salute del paziente oggetto di sperimentazione, seppure ridondante rispetto al mandato clinico-assistenziale). Questo ambito, spesso declinato in checklist prescrittive da applicare e verificare su singoli sistemi software o infrastrutture, ha in anni recenti visto una evoluzione verso un approccio più sistematico, inserito spesso all'interno del framework GAMP (Good Automated Manufacturing Practice, al momento nella sua versione 5), promosso e ora anche imposto formalmente da enti di alto livello quali EMA (European Medicines Agency, agenzia

con funzione regolatoria della EU) e FDA (Food and Drug Administration, ente regolatorio USA). L'esigenza emersa di **"Garantire un trattamento del dato orientato all'uso per contesti di ricerca, oltre alla sicurezza del paziente e alla tutela delle sue libertà personali"** diventa quindi un nuovo elemento da sistematizzare secondo un approccio "by design" nell'attività quotidiana di CIO, Responsabile Ingegneria Clinica ed altre figure dirigenziali correlate. Va inoltre evidenziato che l'evoluzione delle modalità di conduzione della ricerca clinica ha esteso studi e attività di ricerca praticamente a ogni contesto assistenziale, indipendentemente dalla dimensione o dalla vocazione originaria. Ne consegue che il tema oggetto delle presenti linee guida coinvolge sia strutture di grandi dimensioni quali strutture universitarie e IRCCS, ma anche strutture cliniche di dimensioni medio-piccole comunque coinvolte nella raccolta dati o partecipazione a studi multicentrici.

Come per ogni quadro di recente definizione, il confronto tra colleghi diventa la prima sorgente di supporto per interpretazioni e soluzioni implementative. Il passo successivo è la definizione di consensus che consentano una interpretazione uniforme e la messa a fattore comune delle soluzioni più efficaci ed anche, nella economia di riduzione dell'impatto, più efficienti. Da questa volontà di definire una modalità comune di interpretazione e gestione di queste nuove tematiche ed evoluzioni normative nasce questa iniziativa. Si tratta di un primo passo, destinato a ulteriori sviluppi e a una probabile convergenza con altre iniziative simili, nello spirito di miglioramento continuo che da sempre è parte integrante del nostro settore (e di AISIS), nonché della filosofia alla base del framework GAMP.

Altro elemento secondario, ma rilevante sul piano operativo, è la funzione "certificatoria" che deriva dalla metodologia proposta in questo lavoro. Quanto proposto è infatti principalmente uno strumento che guida gli operatori all'applicazione di processi e modalità di gestione che siano coerenti con i principi ispiratori definiti dagli enti regolatori, ma allo stesso tempo consenta di dichiarare e documentare in modo sistematico e oggettivo la rispondenza a tali principi. Obiettivo del gruppo di lavoro è infatti anche quello di supportare gli enti di verifica fornendo una modalità uniforme e "leggibile" di descrizione e attestazione della rispondenza ai requisiti.

Come in ogni gruppo di lavoro AISIS, il risultato non chiude un tema, ma lo apre a nuove riflessioni e ad un percorso di miglioramento. I momenti di confronto tra i colleghi che hanno contribuito a questo documento sono stati ricchi di punti di vista variegati, esperienze dirette di strutture di dimensioni e tipologia molto diversa e background multidisciplinari. Confidiamo che il risultato di questo confronto, riassunto in questa pubblicazione, aiuti colleghi nell'affrontare il tema e contribuisca alla ulteriore crescita del settore.

Per chiunque volesse in futuro contribuire alla evoluzione di questo lavoro o partecipare a nuove iniziative AISIS, vi invitiamo a contattarci (comitatoscientifico@aisis.it).

È importante riconoscere come contributo indiretto al lavoro del gruppo di lavoro AISIS l'apporto metodologico portato dal Prof. Gianfranco DeFeo, dell'Istituto Nazionale Tumori IRCCS Fondazione Pascale di Napoli. Per tramite di colleghi che hanno sperimentato la metodologia proposta dal suo gruppo per il medesimo contesto, questa ha fortemente influenzato la metodologia di valutazione del rischio finale adottata.

2 _ Introduzione

Le Linee Guida presentate nel documento sono derivate da un percorso di analisi del quadro regolatorio, di studio del framework GAMP (nella sua versione 5) dei principi ALCOA+, e dalla contemporanea applicazione del quadro regolatorio preesistente nel settore Sanità Digitale (in particolare GDPR (e sua declinazione nazionale italiana), MDR, IVDR, NIS2).

Il presente documento non si pone come obiettivo quello di trattare nel dettaglio sufficiente il framework GAMP o gli attuali riferimenti regolatori, di cui si consiglia una lettura a chi volesse affrontare il tema (in calce i riferimenti). Risulta a nostro avviso di particolare utilità, per chi volesse approfondire, un momento di confronto o di supporto da parte di operatori del settore ricerca dedicati al trattamento del dato. Seminari, conferenze e percorsi anche più strutturati sono disponibili sul panorama nazionale e consentono di meglio approfondire il quadro retrostante le presenti Linee Guida.

Il gruppo di lavoro si è avvalso dei preziosi contributi della Dott.ssa Donata Pezzuto e del Dott. Christian Fedeli (IQVIA), la cui competenza e contributo sono stati prova del fatto che anche in questo caso la definizione di un vocabolario e patrimonio di concetti comuni sono elemento fondamentale per una corretta interpretazione condivisa di esigenze e metodologie.

La metodologia proposta va letta in termini di:

- Elementi di attenzione / analisi: cosa considerare / analizzare / governare all'interno della propria organizzazione, sia relativamente ai sistemi software e infrastrutture che in termini di processi di gestione.
- Modalità di integrazione/aggregazione del complesso insieme di elementi di cui sopra allo scopo di valutare (e, perché no?... misurare) il generale livello di adeguatezza per il corretto trattamento dati a scopo di ricerca.

La metodologia non è esente da gradi di libertà nella definizione dei pesi dei vari fattori e limiti/declinazioni locali. Essendo una modalità nata da un lavoro precedente di sottogruppo AISIS, e applicata ad un numero limitato di casistiche (seppure oggetto di ispezione da parte di enti certificatori, tra cui AIFA), prevede ancora gradi di "contestualizzazione". Ogni realtà che volesse applicarla può quindi adottare la metodologia nella sua versione proposta, ma anche contestualizzarla. Sono chiaramente evidenziati parametri che consentono di modulare il risultato sulla base di sensibilità locali differenti. Elemento costante della metodologia proposta, che invitiamo gli utilizzatori a mantenere invariato, portando suggerimenti di evoluzione sul tavolo nazionale AISIS, è la definizione delle classi di elementi da considerare, e loro integrazione a comporre una valutazione congiunta.

Un elemento della metodologia proposta è anche la modularità degli step di valutazione e delle classi/categorie di elementi da valutare. Questo approccio nasce dalla necessità di portare a sistema la metodologia in modo efficiente, consentendo rilevazioni distribuite tra più team di

operatori, ed anche consentendo una condivisione di valutazioni tra centri che presentino ambiti comuni (es. stesso applicativo in uso presso più strutture; infrastruttura ospitante comune tra più applicativi/organizzazioni; modalità di gestione comuni a più applicativi/organizzazioni).

Allo scopo di valorizzare questa modularità, AISIS si farà promotore della raccolta e condivisione (volontaria) delle rilevazioni fatte sfruttando questa metodologia, sia come esempi che, appunto, per riutilizzo in contesti che condividano i medesimi elementi. Invitiamo i colleghi che in futuro dovessero adottare questa metodologia a trasmetterci le loro schede di rilevazione (comitatoscientifico@aisis.it), e soprattutto osservazioni e proposte di evoluzione che dovessero derivare dalla esperienza di applicazione.

Nota di Metodo: il template sviluppato per una fruizione diretta, e reso disponibile da AISIS, è stato redatto in lingua inglese. È infatti esperienza comune che questa metodologia e i relativi risultati siano in molti casi utilizzabili in contesti di studi internazionali.

3 _ Obiettivi

A seguito della pubblicazione delle Linee Guida di EMA e dell'accoglimento da parte di AIFA nel nostro Paese¹, il processo di validazione dei sistemi applicativi in ambito sperimentale ha avuto un accrescimento nella sua rilevanza per garantire che le sperimentazioni cliniche producano dati affidabili e utilizzabili secondo gli intendimenti regolatori. Il lavoro svolto dal gruppo di lavoro si innesta in questo contesto: il regolatore europeo – attraverso la Guideline on computerised systems and electronic data in clinical trials (EMA/226170/2021)² – ha formalizzato requisiti che spaziano dalla Data Governance, passando per la protezione dei dati, fino alla verifica della qualità del software, con pieno allineamento ai principi ALCOA++. Queste Linee Guida entrate in vigore a settembre 2023, richiedono che ogni sistema elettronico utilizzato in uno studio clinico sia “fit for purpose”, validato, documentato, e che il suo ciclo di vita sia gestito correttamente. Oltre all'EMA, anche l'Agenzia Italiana del Farmaco (AIFA) e diverse associazioni scientifiche hanno sottolineato la necessità di rendere i processi di gestione dei sistemi informatizzati più trasparenti e documentati. La coerenza con l'ICH E6(R3) e l'ICH Q9(R1) rende evidente che l'approccio non è più soltanto tecnologico, ma regolatorio e di qualità. Questo significa che la validazione di un sistema applicativo non può essere confinata al team IT, ma deve essere parte integrante del Quality Management System dello sponsor o del centro. L'armonizzazione europea si muove chiaramente verso un modello risk-based, in cui l'obiettivo non è la mera produzione di evidenze documentali, ma la dimostrazione che il sistema garantisce sicurezza e affidabilità in condizioni operative reali.

L'obiettivo del lavoro è duplice: da un lato definire e consolidare una metodologia strutturata di validazione applicativa in grado di soddisfare i requisiti normativi; dall'altro supportare Sponsor, CRO, centri sperimentali e fornitori software a implementare processi che permettano di superare le ispezioni e garantire la compliance. In particolare, si mira a sviluppare checklist, schede di qualifica prodotto, criteri di risk assesment che permettano di valutare efficacemente la criticità dei sistemi, determinare quali sistemi necessitano di una validazione più rigorosa e renderli pronti ad audit e ispezioni.

Nel lavoro si considera il concetto di “criticità” dei sistemi informatici, ossia quanto un sistema può impattare sull'integrità dei dati clinici, sulla sicurezza dei partecipanti, sulla trasparenza regolatoria. I sistemi che raccolgono dati di outcome primario, quelli che gestiscono rando-

¹ Agenzia Italiana del Farmaco (AIFA). Linee guida sull'utilizzo dei sistemi elettronici nelle sperimentazioni cliniche con medicinali. 2023. Available from: https://www.aifa.gov.it/documents/20142/847386/Utilizzo_sistemi_elettronici_sperimentazioni_cliniche_medicinali.pdf

² European Medicines Agency (EMA). Guideline on computerised systems and electronic data in clinical trials (EMA/226170/2021). 2023. Available from: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

mizzazione, blinding, firme elettroniche, auditable log, e quelli che interagiscono con sistemi di terze parti critiche, sono alla base di questa valutazione. Si introducono criteri di risk-based validation: non tutti i sistemi devono essere validati allo stesso modo, ma la profondità, la documentazione, la frequenza dei controlli, e delle revisioni deve essere proporzionata al rischio. Il ricorso a strumenti riconosciuti dall'ICH Q9, come FMEA (Failure Mode and Effects Analysis) o risk ranking and filtering, consente di attribuire un punteggio oggettivo a probabilità, severità e rilevanza di ciascun rischio. In questo modo il processo non è soggettivo, ma standardizzato e replicabile. Tale approccio, raccomandato anche dall'EMA, rafforza la capacità dell'organizzazione di dimostrare che le risorse sono state allocate in maniera coerente con il livello di rischio e impatto regolatorio.

Un altro obiettivo è quello di promuovere una cultura di collaborazione attiva tra gli attori coinvolti: fornitori software (vendors), team IT, staff clinico, qualità GCP. Le fonti che abbiamo esaminato – tra cui documenti di AIFA e comunicati di associazioni come AICRO³ – evidenziano che spesso nei centri clinici vi sono sistemi sviluppati internamente e non sempre validati, o sistemi la cui convalida è incompleta. La collaborazione è essenziale perché i fornitori possano fornire evidenza delle certificazioni, supporto tecnico, documentazione, mentre gli sponsor e gli sperimentatori devono garantire che queste evidenze siano acquisite, verificate e mantenute durante tutta la vita utile del sistema.

Infine, il lavoro si propone di rendere operativo il concetto di “audit readiness”: non solo validare, ma garantire che tutti gli elementi richiesti da EMA siano documentati e prontamente disponibili in sede di ispezione. Ciò significa che le schede di qualifica prodotto, le checklist fedeli a criteri ALCOA++, le evidenze di autenticazione, i log, le firme elettroniche, i piani di disaster recovery, le revisioni periodiche, i piani di gestione del cambiamento, devono essere predisposti, conservati e accessibili.

Il processo di validazione applicativa che il gruppo di lavoro AISIS ha definito punta quindi all'efficacia, alla robustezza, alla conformità regolatoria: un processo che non considera la validazione come un adempimento formale, ma come parte integrante della progettazione, implementazione, gestione operativa e chiusura di ogni sistema applicativo utilizzato in studi clinici, secondo gli standard EMA, ICH⁴ e le best practice internazionali. In prospettiva, il processo di validazione applicativa deve essere visto come parte di un percorso evolutivo che prepara il sistema sanitario e la ricerca clinica alle sfide future: l'uso di big data, l'introduzione di algoritmi di intelligenza artificiale, l'impiego di wearable devices e soluzioni decentralizzate. In tutti

³ Associazione Italiana Contract Research Organization (AICRO). Comunicato sulle linee guida EMA on computerised systems and electronic data in clinical trials. 2023.

Available from:

<https://www.datariver.health/aicro-comunicato-su-linee-guida-ema-on-computerised-systems-and-electronic-data-in-clinical-trials/>

⁴ International Council for Harmonisation (ICH). ICH E6(R3) Good Clinical Practice – Step 4 Guideline. 2025 Jan.

Available from:

https://database.ich.org/sites/default/files/E6-R3_Step4_2025_0106.pdf

International Council for Harmonisation (ICH). ICH Q9(R1) Quality Risk Management. Step 5 version. 2023 Jan.

Available from:

<https://database.ich.org/sites/default/files/Q9-R1-QRM-Step5-2023-01.pdf>

questi scenari, le regole definite da EMA e ICH continueranno a rappresentare il quadro di riferimento per garantire che innovazione e compliance procedano insieme. Il lavoro con AISIS, in questo senso, non si limita a rispondere a un requisito normativo attuale, ma si propone come base metodologica e culturale per affrontare la complessità crescente dei sistemi clinici digitali, mantenendo sempre al centro integrità, qualità e tutela del paziente. In prospettiva, il processo di validazione applicativa deve essere visto come parte di un percorso evolutivo che prepara il sistema sanitario e la ricerca clinica alle sfide future: l'uso di big data, l'introduzione di algoritmi di intelligenza artificiale, l'impiego di wearable devices e soluzioni decentralizzate. In tutti questi scenari, le regole definite da EMA e ICH continueranno a rappresentare il quadro di riferimento per garantire che innovazione e compliance procedano insieme. Il risultato del lavoro di gruppo, in questo senso, non si limita a rispondere a un requisito normativo attuale, ma si propone come base metodologica e culturale per affrontare la complessità crescente dei sistemi clinici digitali, mantenendo sempre al centro integrità, qualità e tutela del paziente.

4 _ Metodologia Adottata

La metodologia proposta nelle presenti Linee Guida prende ispirazione dal framework GAMP, dai principi ALCOA+ e dai riferimenti normativi conseguenti (in particolare le linee guida EMA). Questi riferimenti coprono il tema del trattamento del dato a scopo ricerca in tutte le sue declinazioni contestuali, dalla vera e propria progettazione e implementazione di software, fino alla adozione di sistemi software per l'elaborazione e l'analisi dei dati.

Le presenti linee guida definiscono un perimetro ristretto di applicazione della metodologia proposta, limitato ai contesti di pertinenza dei CIO e IT Manager delle strutture sanitarie.

4.1 _ Limitazioni d'uso della metodologia

Le presenti Linee Guida limitano l'interesse ai contesti clinici, quindi alle strutture sanitarie la cui operatività ordinaria sia di cura (e sue declinazioni di sanità territoriale). Questa limitazione nasce dalla natura e mandato di AISIS, ma anche dal fatto che la maggiore complessità risiede probabilmente nella declinazione in contesti di ricerca di sistemi software già esistenti la cui destinazione d'uso non sia nativamente quella di ricerca.

Sono quindi oggetto di applicazione della presente metodologia i processi di rilevazione ed elaborazione del dato a scopo di ricerca che coinvolgano sistemi di gestione clinica, quali ad esempio (elenco non esaustivo, a titolo esemplificativo):

- Software collegati o embedded in DM o IVD
- Middleware di Integrazione / ESB
- Software Dipartimentali Ancillari (LIS, RIS)
- MPI
- CDR
- EMR
- Patient Portal

Sono stati reputati di interesse per una inclusione nella metodologia anche sistemi software che, seppure destinati principalmente all'attività strettamente di ricerca (per rilevazione o elaborazione del dato), siano integrati con sistemi software di uso clinico.

Ad esempio, qualora piattaforme di eCRF o Portali Paziente destinati a contesti di ricerca siano integrati per rilevazione dati direttamente ai sistemi di uso clinico, questi di fatto costituiscono insieme ai sistemi clinici un sistema complesso / integrato, la cui valutazione complessiva dipende da elementi oggetti di qualificazione di tutti i componenti e metodologia di gestione generale.

4.2 _ Limitazione nella Valutazione del Rischio

La metodologia è orientata all'analisi del rischio, che si compone, come espresso dal framework GAMP in due tipologie:

- 1) Rischio per il paziente (inteso nel senso analogo a MDR e IVDR come rischio di compromissione della salute).
- 2) Rischio per il dato, da intendersi in due declinazioni:
 - a) rischio per le libertà fondamentali dell'individuo conseguente ad un non corretto trattamento del dato (inteso nel senso analogo a GDPR e complesso delle normative privacy);
 - b) rischio per il valore del dato nel contesto dell'attività di ricerca (elemento specifico e caratterizzante la validazione).**

Nella presente metodologia le prime due tipologie di rischio 1 e 2a non sono state considerate assumendo che, nell'ambito dei sistemi software e infrastrutture adottate nei contesti clinici, tali tipologie siano già coperte da vincoli normativi sovraordinati sia in termini di caratteristiche dei prodotti che dal punto di vista gestionale.

È infatti insito nella normativa vigente il fatto che qualsiasi sistema software e contesto organizzativo che contribuisca al trattamento di dati orientati alla cura del paziente o al trattamento di dati personali debbano sottostare alle prescrizioni previste da MDR, IVDR, GDPR e NIS2.

La metodologia prevede, a tale scopo, la valutazione, intesa come verifica vincolante, che una valutazione o certificazione di questi aspetti sia già stata svolta in sede preliminare.

La tipologia di rischio 2b è da intendersi come l'evenienza che comportamenti sistematici o imprevisti di un ecosistema software o modalità di gestione dell'ecosistema stesso compromettano il dato rendendolo non utilizzabile nel contesto di ricerca in termini di disponibilità, formato o attendibilità.

4.3 _ Qualificazione e Analisi del Processo

La metodologia proposta è basata su due diverse dimensioni di analisi:

- Analisi del singolo sistema software.
- Analisi dell'ecosistema software, come declinato rispetto ai casi d'uso specifici del contesto di ricerca oggetto di valutazione e validazione.

Le due dimensioni contribuiscono a valutare rispettivamente la componente di rischio sul trattamento da parte del singolo sistema, e il rischio risultante congiunto dal trattamento svolto dall'insieme dei sistemi software tra loro integrati.

Le analisi svolte sui singoli sistemi software sono strutturalmente suddivise in:

- 1) Elementi di Qualificazione: valutazione di elementi oggettivi sul sistema e suo contesto di fabbricazione.
- 2) Elementi di Processo Gestionale: valutazione di elementi oggettivi, ma inerenti processi gestionali interni all'organizzazione.

È importante sottolineare che la suddivisione in questi due elementi di valutazione è rilevante

anche nell'ottica di una corretta identificazione delle azioni di mitigazione che si rendessero necessarie come conseguenza di una valutazione di rischio complessiva. La possibilità di ricondurre il rischio risultante a elementi del tipo 1) o del tipo 2) implica infatti una significativa differenza in termini di potenziali azioni. Il tipo 1) è intrinsecamente più rigido, in quanto legato al processo produttivo del sistema, mentre la tipologia 2) è normalmente collegata a caratteristiche gestionali governabili dall'organizzazione, su cui quindi sono possibili azioni correttive.

4.4 _ Parametrizzazione

La metodologia risultante sulla base delle valutazioni derivanti dalla qualificazione dei sistemi software che compongono l'ecosistema software e dei loro produttori, e sulla base dalle valutazioni derivanti dai processi di gestione di questi sistemi, genera una valutazione quantitativa del rischio derivata tramite opportuna pesatura di tutti gli elementi.

La pesatura è, come per ogni metrica derivante da valutazioni empiriche/statistiche, oggetto di affinamento (processo di identificazione del modello) in studi successivi.

Tali parametri (pesi), sono presenti su più livelli del modello, e costituiscono una dimensione di configurabilità dello stesso che sarà oggetto di:

- Valutazioni di opportunità locale: ogni organizzazione può decidere di porre particolare peso/attenzione a elementi specifici sulla base del contesto complessivo (dell'attività di ricerca o della organizzazione).
- Affinamento su base statistica: correlando i risultati di rischio ottenuti col modello a valutazioni ottenute tramite altre metodologie di riferimento, modificando i parametri per ottenere uno scostamento minimo tra le due metodologie a confronto.

5 _ Il Processo di Validazione dei Sistemi Software Clinici adottati per Attività di Ricerca

Il processo di validazione proposto nella presente metodologia coinvolge principalmente due tipologie di attori:

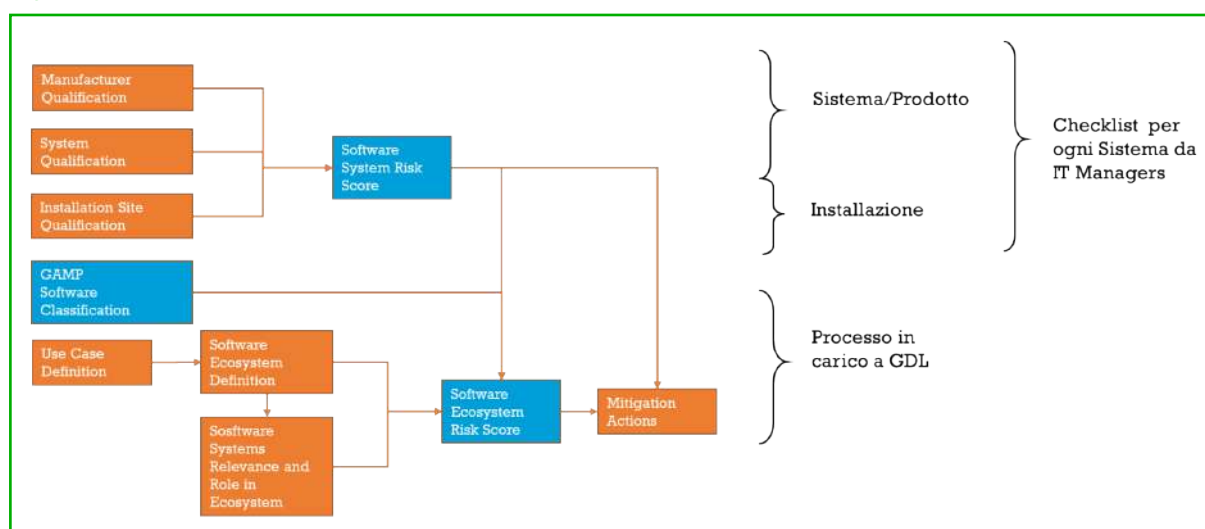
- Il **Team di gestione ICT (IT Managers)** a cui si assume siano affidate:
 - la rilevazione e gestione dell'inventario dei sistemi software in uso presso l'organizzazione che la gestione di tali sistemi (tramite processi formalizzati di gestione del parco IT e della infrastruttura di supporto.
- Un **Gruppo di Lavoro Multidisciplinare** la cui composizione comprenda professionisti le cui diverse sensibilità e competenze consentano di definire:
 - Il processo di trattamento del dato nello specifico contesto di ricerca oggetto di validazione.
 - L'insieme dei sistemi software che costituiscono l'ecosistema software.
 - Il ruolo che ciascuno dei sistemi software svolge nel processo di trattamento.
 - Il livello di accettabilità del rischio risultante dall'utilizzo dell'ecosistema software individuato per l'implementazione del processo di trattamento.
 - Le azioni di mitigazione opportune e accettabili per ridurre, qualora necessario, il rischio risultante.

Il processo di validazione si compone di tre fasi / linee di azione, affidate ai due attori sopra definiti:

1) Il carico al **Gruppo di Lavoro Multidisciplinare**:

- a) l'identificazione del caso d'uso oggetto di validazione (quindi il contesto specifico dello studio o ambito di ricerca)

Figura 1 - Processo di Validazione Proposto



- b) l'identificazione dell'ecosistema software, inteso come insieme dei sistemi software che contribuiscono al trattamento complessivo
- c) l'identificazione del ruolo di ciascuno sistema software all'interno dell'ecosistema
- 2) In carico al **Team di Gestione ICT**: la rilevazione/determinazione di elementi di qualificazione (quindi oggettivi) che determinano le variabili di base di valutazione del rischio sui singoli sistemi software che compongono l'ecosistema individuato
- 3) In carico al **Gruppo di Lavoro Multidisciplinare**:
 - a) La valutazione del rischio complessivo dell'ecosistema software.
 - b) La valutazione di accettabilità del rischio ottenuto.
 - c) L'identificazione (col supporto del Team di Gestione ICT) delle azioni di mitigazione del rischio necessarie.

Sulla base del ruolo che il Gruppo di Lavoro Multidisciplinare deve svolgere nel processo sopra descritto, è auspicabile che questo sia composto da:

- Ricercatori del settore disciplinare del caso d'uso oggetto di valutazione.
- Metodologi di gestione del rischio.
- Metodologi di biostatistica/analisi del dato.
- IT Managers.

5.1 _ Identificazione dei Casi d'Uso – Use Case Definition

L'identificazione dei casi d'uso, nell'ambito oggetto delle presenti linee guida, è opportuno che venga condotta dal punto di vista del percorso che i dati, di interesse per lo studio clinico, effettuano dal loro inserimento nei sistemi aziendali fino alla destinazione finale intesa come messa a disposizione del dato stesso per lo specifico studio clinico. Si tratta quindi di prendere in esame

Figura 2 - Dallo Studio Clinico alla definizione dell'Ecosistema Software



il **data journey**, dello studio clinico nel contesto specifico dell'azienda. Step iniziale fondamentale è l'individuazione del dataset (insieme di dati) coinvolti nello studio. A partire da questi sarà necessario e possibile individuare, inseguendone il data journey, l'insieme dei sistemi software che contribuiscono a vario titolo al trattamento di questi dati. Tale insieme di sistemi software è definito, per lo scopo del presente documento, come **ecosistema software**.

Tali sistemi saranno oggetto della compilazione delle checklist indicate nei paragrafi seguenti. Al fine della descrizione del caso d'uso per lo studio clinico risulta importante dare evidenza di come per questi dati venga tenuta traccia di eventuali modifiche e di come e dove vengano conservati (backup, sistema di disaster recovery, repository).

Se il dato oggetto di studio, dopo la sua raccolta su un sistema informatico viene inviato ad altri sistemi è necessario descrivere:

- eventuali sistemi di transito che non abbiano impatti significativi sul dato stesso (es. Order Entry, middleware);
- se il sistema di destinazione finale utilizza il dato per generare altri dati e/o informazioni, in questo caso anche questo sistema deve essere analizzato e descritto (es. Sistema LIS che riceve da CCE dati anamnestici utilizzati, insieme ad altri, per produrre un risultato di laboratorio).

Occorre infine descrivere come i dati oggetto dello studio vengano messi a disposizione per lo studio stesso e se vengano fatti ulteriori trattamenti (es. ricodifica dei dati come OMOP, LOINC, ...). Qualora questa eventuale operazione avvenga mediante sistemi software anche questi dovranno essere oggetto di analisi e compilazione delle checklist descritte nei paragrafi successivi.

Questa analisi sarà inevitabilmente studio-specifica e differenziata a seconda che sia stia affrontando uno studio retrospettivo, al fine della presente linea guida da intendersi come studio su dati già memorizzati su sistemi aziendali, e studi di tipo prospettico, al fine della presente linea guida da intendersi come nuova raccolta di dati e dove i sistemi software aziendali rappresentano il data source dello studio stesso.

Studio Prospettico:

Per ciascun dato, o gruppo di dati, dovrà essere indicato lo strumento informatico nel quale nascono i dati, tramite integrazione strumentale, inserimento manualmente da parte di clinici (source document) o dai pazienti stessi (Patient Reported Outcome – PRO).

Studio Retrospettivo:

In questo caso si assume che i dati siano conservati in sistemi aziendali e che quest'ultimi possano essere considerati come Source Document.

In questo caso, essendo il trattamento originale che ha alimentato il Source Document potenzialmente anche remoto nel tempo (e diversificato per la presenza nel tempo di sistemi diversi di raccolta), si ritiene opportuno non includere tale fase di trattamento nel data journey.

L'analisi si può quindi limitare a considerare i sistemi a partire dal sistema di origine del dato retrospettivo.

5.2 _ Identificazione e Classificazione dei Sistemi Software Coinvolti Software Ecosystem Definition

A partire dal Data Journey identificato per lo specifico caso d'uso (studio clinico o attività di ricerca), è possibile identificare l'ecosistema software, inteso come insieme dei sistemi software coinvolti, stratificati per il rispettivo ruolo.

Per ciascuno sistema software individuato, si ritiene opportuno individuare la rilevanza che assume all'interno dello studio. Questa valutazione è orientata a ridurre il contributo che sistemi coinvolti possano dare alla valutazione del rischio complessivo, questo soprattutto nell'ottica di ridurre l'impatto nella valutazione globale di sistemi coinvolti marginalmente (es. perché orientati alla rilevazione di dati di importanza secondaria).

Rilevanza / Relevance del sistema:

- Alto → Il sistema è direttamente coinvolto nella generazione, modifica o archiviazione di dati rilevanti ai fini regolatori.
- Medio → Il sistema supporta processi rilevanti ma non genera direttamente dati rilevanti per lo studio.
- Basso / Trascurabile → Il sistema ha impatto indiretto, è solo consultativo, o non è determinante per qualità/integrità dei dati rilevanti per lo studio.

5.2.1 Criteri di inclusione/esclusione dalla compilazione della scheda di prodotto

I sistemi coinvolti nel processo da includere nell'ecosistema software oggetto di analisi sono identificati secondo i seguenti criteri:

- consentono la generazione e la raccolta diretta di dati elettronici originali o trascritti;
- hanno impatto su randomizzazione, blinding, assegnazione di trattamento;
- svolgono funzione di controllo critico (monitoraggio, audit, notifiche);
- presentano componente regolatoria rilevante (firma elettronica, tracciamento, integrazione con altri sistemi).

Sono invece esclusi dall'ecosistema software i sistemi che:

- hanno funzione meramente documentale, con dati archiviati anche altrove in formato regolatorio (es. copie cartacee firmate);
- sono necessari alla gestione clinica del paziente ma che non influenzano i dati regolatori (es. sistemi di order entry);
- sono utilizzati per attività operative generiche (es. repository condivisi di file non strutturati) e non modificano o generano dati di interesse.

5.3 _ Qualificazione del Produttore e del Sistema Software Manufacturer Qualification and System Qualification

Per ogni sistema individuato come parte dell'Ecosistema Software derivato dal Caso d'Uso, è necessario determinare:

5 _ Il Processo di Validazione dei Sistemi Software Clinici adottati per Attività di Ricerca

- La classificazione GAMP.
- Il livello di Rischio intrinseco del sistema, dipendente dalle caratteristiche oggettive, oggetto di qualificazione, del produttore e del sistema.

La classificazione GAMP è riassumibile nei tre livelli:

- **1-OTS/Fixed:** software "Off the Shelf", distribuito commercialmente, che non presenta gradi di libertà in termini di configurazione/adattamento al contesto.
- **2-Configurable:** software che presenta livelli di configurabilità tali da poter essere adeguato a contesti di applicazione differenti.
- **3-Custom:** software oggetto di sviluppi/adequamenti atti a renderlo adeguato al contesto di applicazione.

Figura 3 - Esempio di valutazione di un ambito di rischio relativo al Produttore e Sistema

Attributable/Traceable	Reference	Yes/No	Comments	Weight	Score	Weighted Score
Does the system require user authentication?	EMA §4.2.1	Yes		1	1	1
Does authentication require password with complexity controlled by organization policies?	EMA §4.2.2	No		1	0	0
Does the system implement an automatic log-off?	EMA §4.2.2	Yes		1	1	1
Does the system block user after several failed attempts?	EMA §4.2.2	Yes		1	1	1
Does the site provide credentials to the monitor?	EMA §4.2.2	Yes		1	1	1
Does the system require electronic signatures?	EMA §4.5 / ICH §4.3.4(h)	No		1	0	0
If the system is opened, does the system include electronic signatures?		Yes		1	1	1
Do electronic signatures contain an automatically generated timestamp?	EMA §4.5 / ICH §4.3.4(f)	Yes		1	1	1
Does the system store authentication logs for auditing?	EMA Annex 4	Yes		1	1	1
Are all data modifications logged?	EMA Annex 4 / ICH §4.3.4(f)	No		1	0	0
Are all data modifications traced?	EMA Annex 4	Yes		1	1	1
Are all data modifications logged on a user-reference?	EMA Annex 1	No		1	0	0
Are all data modifications logged on a device/location-reference?	EMA Annex 4	Yes		1	1	1
Are logging/tracing information accessible by regular users?	EMA Annex 4	Yes		1	1	1
Are logging/tracing information NOT alterable by regular users?	EMA §4.3	No		1	0	0
Are logging/tracing information accessible by system administrators or superusers?	EMA Annex 4	Yes		1	1	1
Are logging/tracing information NOT alterable by system administrators or superusers?	EMA Annex 4 / ICH §4.3.4(g)	Yes		1	1	1
Is disabling logging/tracing prevented?	EMA Annex 4	No		1	0	0
Is the audit trail encrypted?	ICH §4.3.4(g)	Yes		1	1	1
Are critical data changes notified to supervisors?	EMA Annex 5	Yes		1	1	1
Is there a role-identity consistency control?	EMA §4.2 / ICH §4.3.4(a)	No		1	0	0
				21	14	14
						0,67

Figura 4 - Esempio di calcolo del Risk Score di Produttore e Sistema.

Si noti la combinazione pesata degli score derivati agli ambiti di valutazione

Section	Score	Weight	Weighted Score
Manufacturer Certification	0,00	1	0,00
System Certification	0,00	1	0,00
Attributable/Traceable	0,67	1	0,67
Legible/Available when needed	0,00	1	0,00
Contemporaneous	0,00	1	0,00
Original/Accurate/Endurable	0,00	1	0,00
Final Manufacturer and System Risk Score			89%

Allo scopo di definire uno Score di Rischio relativo all'insieme di produttore + sistema software, è applicata una metodologia basata sulla rilevazione di elementi che contribuiscono al rischio, suddivisi nei seguenti ambiti:

- **Tracciabilità/Riconducibilità all'Autore** (Attributable/Traceable).
- **Leggibile e Disponibile quando necessario** (Legible/Available When Needed).
- **Contemporaneo** (Contemporaneous).
- **Originale, Accurato, Persistente** (Original/Accurate/Endurable).

Ciascuno di questi ambiti definisce uno score di rischio, determinato come media pesata degli elementi identificati.

Firma Digitale

Un elemento inserito nelle caratteristiche di prodotto è l'adozione della firma digitale (sia in forma forte/qualificata che semplice). Tale elemento è inserito in quanto ritenuto elemento di garanzia di autenticità, integrità e la non ripudiabilità del dato/documento.

Tale modalità di firma viene ritenuta sicura in quanto i certificati vengono rilasciati da soggetti a vigilanza istituzionale, nel rispetto di regolamenti nazionali (AGID) ed europei (eIDAS), e l'operazione di firma avviene mediante dispositivi certificati.

Il rilascio delle firme digitali avviene mediante una procedura definita dall'ente accreditato AGID ed è effettuata in presenza congiunta dell'operatore addetto al riconoscimento e del personale sanitario. Ciò al fine di garantire la sicurezza della assegnazione del certificato di firma digitale all'operatore sanitario effettivamente operante nella Struttura.

È altresì importante indicare anche i casi in cui i dati sono 'firmati' con Firma Elettronica Semplice. La corretta gestione dei processi di autenticazione e abilitazione negli applicativi aziendali, anche con il semplice utilizzo di utente e password, permette di registrare nei rispettivi database i dati raccolti associandoli all'autore dell'inserimento, modifica o cancellazione del dato stesso. Tale modalità di firma ha valore legale, ma è un valore probatorio che deve essere valutato caso per caso dal giudice, non è automatico come per la firma elettronica qualificata o digitale.

5.4 _ Qualificazione del Contesto di Installazione Installation Site Qualification

La fase di Qualificazione del Contesto di Installazione (Installation Site Qualification) ha come obiettivo la rilevazione degli elementi che contraddistinguono i processi di gestione dei sistemi software all'interno della organizzazione che contribuiscono direttamente o indirettamente al trattamento del dato a scopo di ricerca.

È importante notare che in organizzazioni complesse è possibile che uno stesso processo di trattamento del dato a scopo di ricerca coinvolga nell'ecosistema software complessivo sistemi in gestione a teams differenti o collocati in contesti diversi.

Esempi: è possibile che sistemi differenti, tra loro integrati e interagenti nel caso d'uso in oggetto, siano:

5 _ Il Processo di Validazione dei Sistemi Software Clinici adottati per Attività di Ricerca

- in gestione a Servizi ICT e Servizi Ingegneria Clinica, che adottano metodologie di gestione differenti;
- collocati su siti di installazione differenti (es. in cloud e on premise) con conseguenti metodologie di gestione o soluzioni tecniche di infrastruttura differenti.

È quindi possibile che nel valutare il rischio legato al singolo sistema software questo dipenda da elementi di qualificazione del prodotto stesso e del suo produttore, combinati al sito di installazione specifico, mentre nel valutare il rischio complessivo dell'ecosistema software questo risulti dalla combinazione di elementi di qualificazione di prodotti diversi collocati su siti di installazione diversi.

Figura 5 - Esempio di rilevazione di elementi dell'ambito "Quality System" di qualificazione del Sito di Installazione. Si noti nelle colonne di destra il calcolo dello score pesato per ciascun elemento

Quality System	ALCOA+								Yes/No	Comments	Weight	Score	Weighted Score
	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available				
Are SOP for users management available and applied?										Yes		1	1
Are SOP for user authorizations management available and applied?										No		1	0
Are SOP for user support available and applied?										Yes		1	1
Are SOP for systems change request available and applied?										Yes		1	1

Figura 6 - Esempio di calcolo del Risk Score di Sito di Installazione. Si noti la combinazione pesata degli score derivati agli ambiti di valutazione

Section	Score	Weight	Weighted Score
Quality System	0,15	1	0,15
Documentation	0,43	1	0,43
Registries Inventories	0,00	1	0,00
Training	0,00	1	0,00
User Support	0,00	1	0,00
Data Quality Management	0,00	1	0,00
Data Integrity and Security	0,00	1	0,00
Authentication and Authorization	0,00	1	0,00
Final Site Installation Risk Score			93%

Le caratteristiche individuate per la qualificazione del sito di installazione sono state declinate in modo oggettivo (allo scopo di limitare la discrezionalità di valutazione) e suddivise nei seguenti ambiti:

- **Sistema Qualità (Quality System):** livello di formalizzazione e standardizzazione dei processi di gestione dei sistemi software (Nota: è richiesto di dichiarare la presenza di SOP formalizzate ed effettivamente attuate all'interno dell'organizzazione; non è quindi una mera verifica della sola presenza di documentazione di processo).
- **Documentazione (Documentation):** livello di disponibilità della documentazione descrittiva dell'ecosistema software, orientata sia ad una gestione che agli utenti finali.
- **Registri (Registries/Inventories):** livello di gestione della rilevazione strutturata degli asset ICT dell'organizzazione.
- **Training:** livello di formalizzazione e gestione dei processi di formazione a supporto della gestione e dell'uso dei sistemi software.
- **User Support:** livello di formalizzazione e gestione dei processi e servizi di supporto all'utenza.
- **Data Quality Management:** disponibilità di sistemi e processi a supporto della qualità del dato.
- **Data Integrity and Security:** livello di formalizzazione e gestione dei processi di protezione della integrità del dato e cyber-sicurezza.
- **Authentication, Authorization:** livello di formalizzazione e gestione dei processi di gestione delle utenze e della profilazione dei permessi.

La metodologia consente di determinare per ciascuno di questi ambiti uno score di settore/ambito (somma pesata degli elementi che lo compongono).

La combinazione degli score dei vari ambiti consente di determinare uno score generale del sito di installazione (somma pesata degli score di settore/ambito), da cui consegue (in modo complementare a 100%) lo score di rischio.

Nota di Metodo: suggeriamo di prendere familiarità con lo strumento simulando rilevazioni con i template Excel resi disponibili.

Allo scopo di consentire una migliore comprensione delle motivazioni per cui ogni elemento dei vari ambiti è oggetto di rilevazione, la metodologia proposta pone in evidenza l'insieme dei fattori ALCOA+ corrispondenti ad ogni rilevazione (Vedi Appendice e template Excel).

5.5 _ Valutazione del Rischio dell'Ecosistema Software e Identificazione delle Azioni di Mitigazione del Rischio

Gli step del processo descritti nei punti precedenti consentono di determinare:

- L'insieme dei sistemi software coinvolti (che compongono l'ecosistema software).
- Per ogni sistema Software.
 - ◇ Uno score di rischio.
 - ◇ Il sito in cui è installato e gestito.

5_ Il Processo di Validazione dei Sistemi Software Clinici adottati per Attività di Ricerca

- ◇ Una classificazione secondo GAMP della tipologia di sistema (Sistema Custom, Sistema Configurabile, Sistema Commerciale/Off The Shelf).
- Per ogni sito di installazione individuato.
 - ◇ Uno score di rischio.

Allo scopo di valutare uno score complessivo che rappresenti il livello di rischio congiunto conseguente al trattamento del dato attraverso tutti i sistemi individuati, la metodologia propone una composizione degli score dei singoli sistemi coinvolti, modulati sulla base dei seguenti elementi correttivi:

- **AUMENTANO** lo score di rischio:
 - ◇ **Utilizzo del sistema per inserimento manuale di dati:** si assume che ogni step di rilevazione manuale comporti un maggiore rischio di alterazione/errata rilevazione del dato (rispetto a sistemi basati su rilevazione strumentale o tramite integrazione).
 - ◇ **Applicazione di trasformazioni del dato:** ogni sistema che, nell'ecosistema complessivo, svolga un ruolo di trasformazione del dato (es. qualsiasi elaborazione che trasformi il dato in formato o valore) o generazione di dati rilevati (es. calcolo di ulteriori misure derivate).
 - ◇ **Assenza di storage:** si assume che ogni sistema che preveda archiviazione del dato.

Figura 7 - Esempio di Valutazione del Rischio di singoli sistemi di un ecosistema software

System	Installation Site	A: Manufacturer and Product Risk Score	B: Installation Site Risk Score	Base Risk Score	Used for Manual Input	Transit	Storage	Transform	Relevance of System in the Clinical Study	Final Score	GAMP Classification	Risk Level	Overall Score	Overall Risk Level
SystemA	SiteA	40%	10%	30%	Yes	No	Yes	Yes	High	44%	2-Configurable	M	32%	H
SystemB	SiteA	30%	10%	23%	No	Yes	No	No	Medium	21%	1-OTS/Fixed	L		
SystemC	SiteB	12%	20%	15%	No	Yes	No	No	Low	12%	1-OTS/Fixed	L		
SystemD	SiteB	50%	20%	40%	No	No	Yes	Yes	High	53%	3-Custom	H		

Figura 8 - Matrice di determinazione del livello di rischio (ispirata al modello Prof. DeFeo)

Scores Matrix			
3	M	H	H
2	L	M	H
1	L	L	M
	0,33	0,66	1

- **ATTENUANO** lo score di rischio:
 - ◇ **La presenza di solo transito dati sul sistema:** si assume che sistemi di solo trasporto (es. ESB) comportino un rischio minore di alterazione o compromissione del dato.
 - ◇ **L'assenza di archiviazione:** si assume che qualsiasi sistema stateless comporti un minore rischio per il trattamento del dato.

L'aumento o l'attenuazione del risk score è espresso in termini parametrici moltiplicativi.

Allo scopo di consentire una ulteriore pesatura del contributo dei singoli sistemi all'ecosistema software complessivo derivante dal diverso impatto sulle finalità di ricerca (es. sistemi deputati a rilevare o gestire misure/valori di minore o maggiore rilevanza per lo studio) è introdotto un parametro moltiplicativo ulteriore di **Rilevanza del Sistema per lo Studio Clinico**.

Adottando la metodologia proposta dal Prof. DeFeo, il livello di rischio risultante per ogni sistema software individuato è determinato combinando su una matrice 3x3 dalle due dimensioni:

- Lo **score di rischio del sistema**, risultante dalla metodologia sopra descritta, stratificato in tre fasce. Tale score è, riassumendo, una combinazione degli score risultanti dalle caratteristiche del prodotto software, del produttore e dei processi gestionali del sito di installazione; tale score è inoltre corretto rispetto ai fattori sopra descritti che ne determinano una amplificazione o attenuazione sulla base del ruolo svolto dal sistema nell'ecosistema rispetto alle modalità di trattamento e all'impatto del sistema sullo studio clinico oggetto di valutazione.
- La **classificazione GAMP del sistema**. Tale classificazione rappresenta il rischio intrinseco della tipologia di software, come suggerito dal framework GAMP.

Lo score risultante per ogni sistema è espresso in termini di livello **Alto (H)**, **Medio (M)** o **Basso (L)**. È importante ricordare che tale classificazione finale è il risultato di vari livelli di parametrizzazione, che devono essere oggetto di attenta valutazione metodologica a priori:

- Parametri di pesatura degli elementi e degli ambiti di qualificazione del prodotto / produttore.
- Parametri di pesature degli elementi e degli ambiti di qualificazione del sito di installazione.
- Parametri di pesatura dello score finale ottenuto come composizione degli score di cui sopra.
- Parametri di amplificazione / attenuazione dello score legati alle modalità di trattamento dati e rilevanza del sistema.
- Parametri di identificazione delle tre fasce di score di rischio per la determinazione dei livelli di rischio finale.

Dovendo giungere ad una valutazione congiunta finale del livello di rischio dell'ecosistema software complessivo, la disciplina della valutazione del rischio suggerisce una composizione cautelativa di **"massimo rischio degli elementi che compongono"**. Ne deriva una metodologia in cui, pur includendo elementi di attenuazione o amplificazione derivanti dal ruolo di ogni singolo sistema software, la presenza di un singolo elemento ad alto rischio comporta una valutazione complessiva di alto rischio.

Questa conseguenza appare però coerente con un approccio in cui un processo / filiera di trattamento del dato debba garantire affidabilità e correttezza del dato, e non un approccio di "compensazione" tra singoli sistemi che appare poco sensato a fronte del propagarsi di errori generati in un qualsiasi punto dell'ecosistema.

6 _ Conclusione e Sviluppi Futuri

Il tema trattato in questo documento si inserisce nel sempre più ampio tema della “accountability” delle metodologie e degli strumenti che compongono la Sanità Digitale. Gli operatori del settore IT sanitario, forse ripercorrendo una strada già aperta dai colleghi del settore Ingegneria Clinica, si trovano sempre più a dover documentare e validare modalità operative e scelte fatte, allo scopo di garantire a terze parti (in questo caso enti regolatori o promotori di attività di ricerca) che gli impianti software adottati e le loro modalità gestionali rispondono a caratteristiche che garantiscano una corretta disponibilità e qualità del dato.

Queste linee guida sono quindi uno strumento che viene incontro a questa duplice esigenza di documentare e validare.

L’auspicio del gruppo di lavoro che ha redatto le presenti Linee Guida e di AISIS è che quanto rappresentato in questo documento possa diventare un utile strumento di lavoro per tutti i colleghi delle aziende sanitarie, pubbliche e private, che si trovano a dover dare risposte su questo tema nelle proprie realtà.

Ci auguriamo che l’adozione di queste linee guida faciliti la compliance regolatoria e la “audit readiness”, e promuova anche una cultura della qualità e della responsabilità all’interno delle organizzazioni sanitarie. Il coinvolgimento in processi di validazione di tutti gli attori, dal CIO al personale clinico, dai fornitori ai responsabili qualità, come quello descritto in queste linee guida è fondamentale per garantire che i sistemi informativi siano realmente “fit for purpose” e pronti a sostenere la ricerca clinica in modo affidabile e sicuro.

Il suo utilizzo nella pratica quotidiana fornirà sicuramente nuovi spunti per migliorare ed arricchire questa prima versione delle linee guida che AISIS si impegnerà a revisionare e a condividere con tutti i colleghi.

Per questo motivo siete tutti invitati a condividerci le vostre riflessioni ed osservazioni scrivendoci a comitatoscientifico@aisis.it

7 _ Riferimenti Normativi e Bibliografici

GDPR – General Data Protection Regulation - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

MDR – Medical Device Regulation- Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017.

IVDR – In Vitro Diagnostic Medical Devices Regulation - Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio del 5 aprile 2017.

NIS2 – Direttiva sulla cybersicurezza - Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (recepita in Italia con D.Lgs. n. 138/2024).

8 _ Acronimi

ALCOA+: Attributable – Attribuibile: ogni dato deve essere collegato a chi lo ha generato. Legible – Leggibile: il dato deve essere chiaro e comprensibile. Contemporaneous – Contemporaneo: registrato al momento in cui si verifica. Original – Originale: deve essere la fonte primaria o una copia certificata. Accurate – Accurato: deve riflettere la realtà senza errori. Complete – Completo: nessuna informazione mancante. Consistent – Coerente: i dati devono seguire una sequenza logica. Enduring – Duraturo: i dati devono essere conservati nel tempo. Available – Disponibile: i dati devono essere accessibili per revisione e audit.

CDR: Clinical Data/Document Repository.

DM: Dispositivo Medico.

Ecosistema Software: insieme di sistemi software tra loro integrati che concorrono ad un trattamento organico e coordinato di un set di dati.

EMA: European Medicines Agency.

EMR: Electronic Medical Record (CCE, CCI, SCCI).

FDA: Food and Drug Administration.

GAMP: Good Automated Manufacturing Practice.

IVD: Dispositivo In Vitro.

MPI: Master Patient Index.

Sistema Software: Singola componente software, omogenea funzionalmente (singolo prodotto), per destinazione d'uso e produttore.

9 _ Appendice - Schema di Rilevazione

Lo schema di rilevazione presentato, fornito come template Excel a corredo della presente linea guida, svolge il duplice ruolo di:

- Sistema di rilevazione a scopo dichiarativo: gli elementi delle checklist e di rilevazione del processo di validazione costituiscono una rappresentazione grafica ordinata e standardizzata da proporre agli organi ispettivi.
- Sistema di calcolo degli score di rischio: la metodologia sopra descritta è stata implementata allo scopo di consentire sia un approccio di simulazione, che di calcolo effettivo durante la validazione. È inoltre stato introdotto un calcolo pre-post per consentire l'aspetto dichiarativo corrispondente alla situazione iniziale e post-mitigazione.

9.1 _ Identificazione del Caso d'uso e dell'Ecosistema Software

Ogni caso d'uso oggetto di validazione prevede la rilevazione di un a testata con informazioni di base:

Use Case Title / Study Code	
Institution/Organizzazione	
Use Case Title / Study Title	
Use Case / Study Starting Date	
Use Case / Study Duration+	
Use Case / Study Protocol Version	
Type of Study	
Target Population	
Use Case/ Study Description	

Associato al caso d'uso è prevista una scheda descrittiva del processo di validazione:

Software Ecosystem Validation Process	
Members of the IT Team	
Members of Multidisciplinary Teams	
Date of Validation Process Start	
Date of Finale Validation	
Initial Risk Level	
Risk Mitigation Strategies Applied	
Final Risk Level	

Al caso d'uso corrisponde la rilevazione dell'Ecosistema Software definito dalla sequenza di Sistemi Software coinvolti, loro relativo ruolo e Sito di Installazione del sistema. A ciascun sistema, come descritto in precedente sezione, è associato un indicatore di rilevanza, secondo i criteri definiti in metodologia. A ciascun sistema è inoltre associabile, secondo le definizioni GAMP, una classificazione della tipologia.

System	Installation Site	System Checklist Provided - Check	Installation Site Checklist Provided à - Check	Role in the Clinical Study	Relevance of System in the Clinical Study	GAMP Classification	Used for Manual Input	Transit	Storage	Transform
SystemA	SiteA	Yes	Yes	High	2-Configurable	Yes	No	Yes	Yes
SystemB	SiteA	Yes	Yes	Medium	1-OTS/Fixed	No	Yes	No	No
SystemC	SiteB	Yes	Yes	Low	1-OTS/Fixed	No	Yes	No	No
SystemD	SiteB	Yes	Yes	High	3-Custom	No	No	Yes	Yes

Dalla sequenza di sistemi e siti di installazione derivano (dalle corrispondenti schede, vedi sezioni successive) i relativi score di rischio.

La rilevazione degli ulteriori elementi di attenuazione o amplificazione del rischio, dipendenti dal ruolo di ogni sistema nell'ecosistema complessivo, contribuisce a determinare lo score di rischio finale, da cui deriva la classificazione in livello di rischio.

9.1.1 _ Parametrizzazione

Sono oggetto di parametrizzazione i pesi associati ai fattori di attenuazione/amplificazione dello score di rischio:

Data Transit Weight Score	0,9
Data Archive Weight Score	1
Data Transform Weight Score	1,2
Manual Input Weight Score	1,1
High Relevance Weight Score	1,1
Medium Relevance Weight Score	1
Low Relevance Weight Score	0,9

Ed è infine oggetto di parametrizzazione la matrice, e relative soglie sullo score di rischio, per la classificazione in livelli di rischio (ascisse: soglie per score di rischio; ordinate: classificazione GAMP):

Scores Matrix			
3	M	H	H
2	L	M	H
1	L	L	M
	0,33	0,66	1

9.1.2 _ Sistema di Calcolo

A partire dai dagli score di rischio corrispondenti al sistema e al sito, riportati per ogni sistema coinvolto, sono calcolati:

- Lo score di rischio base.
- Lo score di rischio a seguito delle azioni di attenuazione / amplificazione.
- Il livello di rischio risultante (Alto, Medio, Basso).

Questa metodologia di calcolo è applicata in due sezioni corrispondenti relativamente alla situazione originale/iniziale (pre-mitigazione), e alla situazione post-mitigazione. La possibilità di

rilevare entrambe le situazioni è stata introdotta per consentire un approccio documentativo delle azioni implementate, e conseguenti risultati sul livello di rischio finale.

La differenza nelle due rilevazioni si colloca sugli score di rischio di sistema e di sito di installazione, che corrispondono agli elementi di progetto e di gestione che sono controllabili, e quindi modulabili dall'organizzazione.

ORIGINAL					MITIGATED				
A: Manufacturer and Product Risk Score	B: Installation Site Risk Score	Base Risk Score	Final Score	Base Risk Level	A: Manufacturer and Product Risk Score - Mitigated	B: Installation Site Risk Score - Mitigated	Mitigated Risk Score	Mitigated Final Score	Mitigated Risk Level
40%	10%	30%	44%	M	10%	10%	10%	15%	L
30%	10%	23%	21%	L	30%	10%	23%	21%	L
12%	20%	15%	12%	L	12%	20%	15%	12%	L
50%	20%	40%	53%	H	20%	20%	20%	26%	M

9.2 _ Qualificazione del Produttore e Sistema Software

La scheda proposta per la qualificazione del produttore e prodotto svolge il ruolo dichiarativo garantendo che ogni sistema coinvolto nel caso d'uso sia corredato da sufficienti informazioni di base attestanti una gestione conforme a standard qualitativi minimi. La disponibilità di informazioni di tracciabilità sulle azioni di installazione, formazione e manutenzione è infatti da considerarsi prerequisito. L'assenza di queste informazioni implica una gestione del sistema software priva di metodologia, quindi fortemente a rischio di compromissione del dato.

9 _ Appendice - Schema di Rilevazione

System Name		Comments Refer to EMA/INS/GCP/112288/2023 E.g.: ISO 27001, ISO 13485, GAMP5 Assessment, FDA 21 CFR Part 11, EU Annex 11, MDR, IVDR
System Version		
System Intended Use		
System GAMP Classification		
System Certification		
Manufacturer Name		Comments If different from Manufacturer If different from Manufacturer
Manufacturer Address		
Vendor Name		
Vendor Address		
Manufacturer Process Certifications		
System		
Software Installation implemented by:		
Software Architecture Project provided by:		
Software Architecture Project approved by:		
Software Acceptance Tests performed by:		
Security Software Acceptance Tests performed by:		
System Installation		
System First Installation Date		
Installation performed by:		
Acceptance test performed by:		
System Last Major Update Date		
Installation performed by:		
Acceptance test performed by:		
System Integration		
List of Systems Integrated with:		System Name; Version; Manufacturer; Data flows implemented; Technology (e.g. HL7, SOAP, XML, etc.)
Integration Documentation available:		
Integration log and audit available:		
Training		
Initial Formal Training provided by:		
Number of Users Involved in Initial formal training:		
Retraining provided by:		
Frequency of retraining:		
Maintenance		
Systems Maintenance provided by:		Choose all that apply: Corrective, Regulatory, Proactive/Preemptive
Types of Maintenance provided:		
Are Service Level Agreements formalized for System Maintenance		
Is a Maintenance program set up for the system, including limits to system downtime?		
General Notes / Comments		

La rilevazione delle caratteristiche oggettive relative al sistema software è suddivisa nelle quattro sezioni descritte in sezioni precedenti. Lo schema di rilevazione ripropone, come referenza metodologia, le corrispondenti sezioni dei riferimenti normativi e istituzionali.

Attributable/Traceable	Reference
Does the system require user authentication?	EMA §4.2.1
Does authentication require password with complexity controlled by organization policies?	EMA §4.2.2
Does the system implement an automatic log-off?	EMA §4.2.2
Does the system block user after several failed attempts?	EMA §4.2.2
Does the site provide credentials to the monitor?	EMA §4.2.2
Does the system require electronic signatures?	EMA §4.5 / ICH §4.3.4(h)
If the system is opened, does the system include electronic signatures?	
Do electronic signatures contain an automatically generated timestamp?	EMA §4.5 / ICH §4.3.4(f)
Does the system store authentication logs for auditing?	EMA Annex 4
Are all data modifications logged?	EMA Annex 4 / ICH §4.3.4(f)
Are all data modifications traced?	EMA Annex 4
Are all data modifications logged on a user-reference?	EMA Annex 1
Are all data modifications logged on a device/location-reference?	EMA Annex 4
Are logging/tracing information accessible by regular users?	EMA Annex 4
Are logging/tracing information NOT alterable by regular users?	EMA §4.3
Are logging/tracing information accessible by system administrators or superusers?	EMA Annex 4
Are logging/tracing information NOT alterable by system administrators or superusers?	EMA Annex 4 / ICH §4.3.4(g)
Is disabling logging/tracing prevented?	EMA Annex 4
Is the audit trail encrypted?	ICH §4.3.4(g)
Are critical data changes notified to supervisors?	EMA Annex 5
Is there a role-identity consistency control?	EMA §4.2 / ICH §4.3.4(a)

Legible/Available When Needed	Reference
Are data stored in their original machine-readable format?	EMA §4.3 / ICH §4.3.4(i)
Can authorized users access data in original format?	EMA §4.3.4(i)
Does the system support export in a human-readable third-party format (e.g., PDF)?	EMA Annex 6
Is a long-term access interface or viewer available?	EMA Annex 6 / ICH §4.3.4(i)

Contemporaneous	Reference
Is the system synchronized with a centralized time source (e.g., NTP)?	EMA Annex 4
Does the system distinguish between clinical event time and data entry time?	EMA §4.3.4
Are timestamps tracked at field level (not just record)?	EMA Annex 2

Original/Accurate/Endurable	Reference
Is original data acquisition/storage protected from modification?	EMA §4.3.4(a)
Does the system prevent permanent overwriting (e.g., soft delete, versioning)?	EMA Annex 4
Is data readability ensured throughout the retention period?	ICH §4.3.4(i)

Ciascuna di queste sezioni è oggetto di calcolo di uno score relativo, dipendente da parametri associati a ciascun elemento della sezione:

Legible/Available When Needed	Reference	Yes/No	Comments	Weight	Score	Weighted Score
Are data stored in their original machine-readable format?	EMA §4.3 / ICH §4.3.4(i)	Yes		1	1	1
Can authorized users access data in original format?	EMA §4.3.4(i)	No		1	0	0
Does the system support export in a human-readable third-party format (e.g., PDF)?	EMA Annex 6	Yes		1	1	1
Is a long-term access interface or viewer available?	EMA Annex 6 / ICH §4.3.4(i)	Yes		1	1	1
				4	3	0,75

Gli score complessivi sono riportati in schema riassuntivo finale, da cui è dedotto lo score di rischio del sistema software:

Section	Score	Weight	Weighted Score
Manufacturer Certification	1,00	1	1,00
System Certification	0,00	1	0,00
Attributable/Traceable	0,86	1	0,86
Legible/Available when needed	0,75	1	0,75
Contemporaneous	1,00	1	1,00
Original/Accurate/Endurable	0,67	1	0,67
Final Manufacturer and System Risk Score			29%

9.3 _ Qualificazione del Sito di Installazione

La scheda proposta per la qualificazione del sito di installazione svolge il ruolo dichiarativo garantendo che ogni sito di installazione sia corredato da informazioni inerenti alle modalità di progettazione, validazione tecnica (acceptance) e manutenzione.

Installation Site:	
Infrastructure	
Main hardware infrastructure provided by:	
Type of hardware infrastructure	
Infrastructural Project provided by:	
Infrastructural Project approved by:	
Infrastructure acceptance test performed by:	
Infrastructure security acceptance test performed by:	
Infrastructural Maintenance provided by:	
Infrastructural maintenance approved by:	

Gli elementi oggetto di rilevazione puntuale che determinano lo score di rischio finale associato al sito di installazione sono suddivisi nelle sezioni indicate in sezione precedente. Ogni elemento è ricondotto ai principi ALCOA+ allo scopo di consentirne una riconducibilità metodologia al rischio sul dato.

Quality System	ALCOA+							
	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring + Available
Are SOP for users management available and applied?								
Are SOP for user authorizations management available and applied?								
Are SOP for user support available and applied?								
Are SOP for systems change request available and applied?								
Are SOP for system activation available and applied?								
Are SOP for system de-activation available and applied?								
Are SOP for systems Business Continuity available and applied?								
Are SOP for system Disaster Recovery available and applied?								
Are SOP for system Disaster Recovery application and regular tests available and applied?								
Are SOP for systems Data Backup available and applied?								
Are SOP for systems Data Restore available and applied?								
Are SOP for systems maintenance available and applied?								
Are SOP for systems testing available and applied?								
Are SOP for systems operational monitoring available and applied?								
Are SOP for systems integration maintenance available and applied?								
Are SOP for systems integration testing available and applied?								
Are SOP for systems integrations operational monitoring available and applied?								
Are SOP for systems data quality monitoring available and applied ?								
Are SOP for system de-commissioning available and in use, and do they specifically issue data retention policies?								
Are SOP for systems off-line archiving policies available and in use ?								

	ALCOA+								
Documentation	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Is official documentation regarding data retention time-limits available and enforced ?									
Is documentation stating the intended use of every system in the organization available ?									
Is documentation stating the general integration architecture in the organization available ?									
Is systems documentation stored and made available in a centralized repository?									
Does systems documentation include user documentation?									
Does systems documentation include installation and maintenance documentation?									
Does systems documentation include test documentation and logs?									

	ALCOA+								
Registries / Inventories	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Software Systems Inventory									
Hardware Systems Inventory									
Network Systems Inventory									
Incidents Registry									
Change Log Registry									
Change Requests Registry									
Issues Log Registry									
Users Registry									
Administrators Registry									
External Access Authorization Registry									

	ALCOA+								
Training	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Is user training on main software systems performed regularly?									
Is user training for information security performed regularly?									
Is user training for data protection performed regularly?									
Does the ICT team have a formalized training program?									
Does the ICT team have a formalized training program on GAMP or related methodologies ?									

	ALCOA+								
User Support	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Are systems users supported by a Help Desk Service ?									
Are system users supported by on line documentation ?									
Are system users supported by a Research-Activity informed/trained Help Desk service ?									
Are system users supported by Research Activity specific on line documentation ?									

	ALCOA+								
Data Quality Management	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Is a centralized repository for coding systems and nomenclatures available and in use ?									
Does the site guarantee a time-reference synchronization on all systems involved?									
Does the site guarantee a workstation/point of data capture identification for all systems involved?									
Does the site have automatic or semi-automatic (e.g. reporting systems) system to support data quality monitoring?									
Does the site provide a centralized long-term archiving system for digitally signed documents ?									

	ALCOA+								
Data Integrity and Security	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available
Is data backup performed?									
Is data backup stored in a remote location?									
Is data backup monitored?									
Are data restore tests performed regularly?									
Frequency of data backup >= daily									
Is anti-malware software active on client and server systems?									
Frequency of anti-malware software updates >= daily									
Does the organization manage or not allow the connection of external devices ? (BYOD)									
Does the organization detect and monitor the connection of external unauthorized devices?									

Authentication, Authorization, Log and Audit	ALCOA+							
	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring
Does the organization have a single authentication framework?								
Does user lifecycle include automatic activation and deactivation?								
Are all authentication and access operations logged and stored for auditing?								
Is user profiling subject to a workflow including at least two levels of authorization ?								
Do users with administrative roles have strong authentication criteria? (e.g. double factor)								
Is automatic analysis of audit trails for intrusion detection performed?								
Does the system or the site provide with automatic log-off functionality?								

9 _ Appendice - Schema di Rilevazione

Ogni sezione è associata ad uno schema di calcolo dello score corrispondente, comprendete i parametri di pesatura:

ALCOA+														
Documentation	Attributable	Legible	Contemporaneous	Original	Accurate	+ Complete	+ Coherent	+ Enduring	+ Available	Yes/No	Comments	Weight	Score	Weighted Score
Is official documentation regarding data retention time-limits available and enforced ?										Yes		1	1	1
Is documentation stating the intended use of every system in the organization available ?										No		1	0	0
Is documentation stating the general integration architecture in the organization available ?										Yes		1	1	1
Is systems documentation stored and made available in a centralized repository?										No		1	0	0
Does systems documentation include user documentation?										Yes		1	1	1
Does systems documentation include installation and maintenance documentation?										Yes		1	1	1
Does systems documentation include test documentation and logs?										Yes		1	1	1
												7	5	5
														0,71

La sintesi degli score corrispondenti alle diverse sezioni, e il relativo calcolo dello score di rischio del sito oggetto di qualificazione è resa disponibile:

Section	Score	Weight	Weighted Score
Quality System	0,85	1	0,85
Documentation	0,71	1	0,71
Registries Inventories	0,40	1	0,40
Training	0,60	1	0,60
User Support	0,75	1	0,75
Data Quality Management	0,80	1	0,80
Data Integrity and Security	0,89	1	0,89
Authentication and Authorization	0,86	1	0,86
Final Site Installation Risk Score			27%