**REPORT SULL'EFFICACIA DEI CONTROLLI ESISTENTI: ANALISI DELLE MISURE DI MITIGAZIONE E IDENTIFICAZIONE DEI GAP DI SICUREZZA (2023-2024)**

**REPORT ANALITICO AZIENDALE**

Report ID: RPT-20251121\_131051  
Data di Generazione: 21 November 2025  
Classificazione: Interno - Riservato

**INDICE**

1. Sezione 1 – Sintesi esecutiva ............................ 1

2. Sezione 2 – Mappatura e copertura dei controlli .......... 3

3. Sezione 3 – Efficacia delle verifiche di conformità e distribuzione delle valutazioni 5

4. Sezione 4 – Non conformità e stato delle azioni di remediation 7

5. Sezione 5 – Rischio residuo, gap prioritari e sintesi dei gap di sicurezza 9

6. Sezione 6 – Conclusioni operative (sintesi) .............. 11

**SEZIONE 1 – SINTESI ESECUTIVA**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Breve valutazione dell'efficacia complessiva dei controlli esistenti nel periodo 2023–2024, con evidenza delle aree con controllo insufficiente, non conformità rilevate e rischi residui significativi. Il report integra dati di mappatura controllo-rischio, risultati delle verifiche di conformità, non conformità rilevate e valutazioni di rischio residuo per identificare gap prioritari.

**SEZIONE 2 – MAPPATURA E COPERTURA DEI CONTROLLI**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2.1 Mappatura Controlli Vs Eventi Di Rischio**

Sezione 2.1 — Mappatura controlli vs eventi di rischio

Sintesi esecutiva

La mappatura dei controlli rispetto agli eventi di rischio si basa su 54 record presenti nella tabella RM04RiskMControlloRischioEvento. L’analisi documenta un catalogo ampio e granulare di controlli (54 descrizioni di ControlloAudit), una predominanza di controlli automatizzati e una concentrazione delle misure sui rischi di cybersecurity e continuità operativa. Questi elementi guidano le priorità operative e le raccomandazioni di razionalizzazione dei target.

Dimensione e granularità del catalogo controlli

Il dataset contiene 54 voci distinte di Controllo\_Audit: ogni voce rappresenta circa l’1,85% del totale, a indicare un elevato livello di dettaglio e pochi raggruppamenti aggregati. La granularità è utile per l’operatività ma comporta complessità di governance e di monitoraggio se non accompagnata da una tassonomia di aggregazione/ KPI.

Distribuzione per categoria di rischio

La distribuzione per Categoria\_Rischio evidenzia le priorità di rischio:

* Cybersecurity: 20 record (37,04%)
* Continuità Operativa: 14 record (25,93%)
* Conformità: 6 record (11,11%)
* Change Management: 4 record (7,41%)
* Cloud / Terze Parti: 3 record (5,56%)
* Access Management: 3 record (5,56%)
* Adeguatezza e Capacity del Personale: 2 record (3,70%)
* Sicurezza: 2 record (3,70%)

Insight: il 63,0% delle voci (Cybersecurity + Continuità Operativa) concentra la maggior parte dei controlli; ciò impone investimenti prioritari in strumenti, automazione e test per questi ambiti.

Tipologia dei controlli

La ripartizione per Tipo\_Controllo mostra un netto orientamento all’automazione:

* Automatizzato: 37 record (68,52%)
* Procedurale: 14 record (25,93%)
* Organizzativo: 3 record (5,56%)

Insight: oltre due terzi dei controlli sono automatizzati, suggerendo buone possibilità di raccolta dati e misurabilità. Tuttavia, la componente procedurale e organizzativa (circa 31,5%) richiede attenzione su formazione, responsabilità e processi di verifica manuale.

Target di risultato (Soglia\_Target) e misurabilità

I target associati ai controlli mostrano una forte propensione a soglie elevate:

* = 95%: 25 record (46,30%)
* 100%: 10 record (18,52%)
* = 99%: 6 record (11,11%)
* = 98%: 5 record (9,26%)
* = 90%: 4 record (7,41%)

Altre soglie specifiche (ad es. remediation entro 30 gg) compaiono in misura residuale (ciascuna 1,85%).

Insight: il 46,3% dei controlli adotta una soglia di successo =95% e quasi il 29,6% mira a soglie ≥99% (100% o 99%). Obiettivi di questo livello possono essere appropriati per controlli automatizzati ad alta affidabilità, mentre per controlli procedurali o dipendenti da fornitori esterni tali soglie possono risultare irrealistiche senza investimenti aggiuntivi.

Meccanismi di controllo e metriche associate

Le metriche (colonna Metrica) sono ampiamente specifiche e, nella maggior parte dei casi, associate in modo diretto a singole voci di controllo (ogni coppia Metrica–Soglia\_Target è generalmente univoca nel dataset). Questo facilita la tracciabilità dei KPI ma accresce il numero di indicatori da monitorare operationalmente.

Rischi operativi e possibili inefficienze rilevate

- Elevata frammentazione: 54 controlli distinti aumentano il costo di governance e il rischio di sovrapposizioni funzionali.

- Soglie uniformemente elevate: obiettivi al 95–100% possono creare falsi allarmi o richiedere sforzi non proporzionati per controlli a bassa materialità.

- Dipendenza dall’automazione: il 68,5% di controlli automatizzati richiede attendibilità degli strumenti e pipeline di dati robuste; mancanze di integrazione possono degradare l’efficacia complessiva.

Raccomandazioni operative

1. Prioritizzazione rischi-controlli: concentrare revisioni e investimenti su Cybersecurity (37,04% delle voci) e Continuità Operativa (25,93%) per coprire il 63% del rischio mappato.

2. Raggruppamento e semplificazione: definire una tassonomia a livelli per aggregare i 54 controlli in macro-controlli operativi (es. Vulnerability Management, Identity Management, Backup & Recovery) per ridurre il numero di KPI da governare e migliorare l’efficienza del reporting.

3. Revisione dei target: valutare la sostenibilità delle soglie 95–100% in funzione del Tipo\_Controllo; applicare target differenziati per controlli automatizzati vs procedurali e inserire SLO di remediation (es. % remediation entro 30 gg) dove rilevante.

4. Misurazione della copertura di automazione: monitorare la percentuale di controlli automatizzati efficaci (attualmente 68,52%) e definire obiettivi di incremento per ridurre attività manuali ripetitive.

5. Programma di consolidamento metriche: stabilire un set di KPI consolidati (max 10–15) derivati dalle metriche esistenti per reporting executive, mantenendo il dettaglio operativo a supporto dei team.

Conclusione

La mappatura evidenzia un inventario completo e dettagliato di controlli con una forte focalizzazione su cybersecurity e continuità operativa, una prevalenza di controlli automatizzati (68,52%) e target frequentemente molto ambiziosi (46,30% a =95% e 18,52% a 100%). L’organizzazione trae valore da una razionalizzazione delle metriche, dalla definizione di una tassonomia di aggregazione e da un approccio differenziato ai target in funzione del tipo di controllo, per migliorare efficacia, efficienza e governance del rischio.

**2.2 Copertura Dei Controlli Per Asset E Fattori Di Rischio**

Sezione 2.2 — Copertura dei controlli per asset e fattori di rischio

Panoramica del dataset

Il dataset analizzato contiene 81 record relativi all’associazione tra asset, fattori di rischio e controlli di audit. La misura complessiva del peso attribuito ai controlli (PesoControlloAudit) presenta una media di 0,54321, con un valore minimo registrato di 0,1 e un massimo di 1,0; la somma aggregata dei pesi è pari a 44,0. L’efficacia media dichiarata dei controlli (EfficaciaControlloAudit) è 0,52593, con valori compresi tra 0,3 e 0,8 e somma aggregata 42,6. Questi indicatori forniscono un punto di riferimento per valutare l’adeguatezza della copertura dei controlli rispetto ai rischi censiti.

Copertura per asset

La distribuzione per asset mostra concentrazioni significative: il top asset è "Cluster 7- Workplace" con 9 record (11,11% del dataset), seguito da tre asset a 7 record ciascuno — "cluster 1- host legacy", "CB Payments" e "cluster 5- Data Farm Oracle" — ciascuno con il 8,64% dei casi. Dal punto di vista qualitativo, alcuni asset evidenziano pesi medi di controllo più elevati: ad esempio "cluster 5- Data Farm Oracle" registra un peso medio 0,8000 e un’efficacia media 0,5571; "CB Payments" mostra peso medio 0,6571 ed efficacia 0,5429. Al contrario, "cluster 1- host legacy" presenta un peso medio inferiore a 0,3286 ed efficacia media 0,4714, indicando potenziale under‑coverage sui sistemi legacy.

Copertura per fattore di rischio

Il fattore di rischio più frequente è "Incidenti non gestiti in tempo" con 18 occorrenze (22,22% del totale), media del peso controllo 0,6000 ed efficacia media 0,5056. Seguono "Gestione non documentata modifiche" con 10 casi (12,35%, peso medio 0,3900, efficacia 0,5600) e "Gestione inadeguata delle credenziali" con 9 casi (11,11%, peso medio 0,5889, efficacia 0,5000). La concentrazione del rischio sugli incidenti ritrae una priorità operativa rilevante: il fattore più presente (22,22%) mostra un’efficacia media dei controlli leggermente inferiore alla media complessiva (0,5056 vs 0,5259), segnalando margini di miglioramento nell’efficacia delle misure attuate.

Analisi dei controlli di audit

I controlli più frequentemente citati sono: "Calcolo MTTR (Mean Time To Resolution)", "Riesame registro incidenti" e "Verifica escalation", ciascuno con 6 record (7,41% del dataset). "Calcolo MTTR" presenta peso medio 0,5667 ed efficacia 0,5333; "Riesame registro incidenti" peso medio 0,5500 ed efficacia 0,5000; "Verifica escalation" peso medio 0,6833 ed efficacia 0,4833. Alcuni controlli mostrano forte peso ma efficacia variabile: ad esempio "Audit IAM/PAM" ha peso medio 0,8667 ed efficacia 0,6000 (evidenza di investimento mirato con buona efficacia), mentre "Campionamento account orfani" mostra efficacia molto bassa (0,3000) nonostante un peso medio moderato (0,4667).

Confronti e gap operativi

Confrontando medie e frequenze emergono due gap principali. Primo, il fattore dominante ("Incidenti non gestiti in tempo") registra un’efficacia media (0,5056) inferiore alla media complessiva (0,5259) nonostante un peso moderato (0,6000), indicando che le misure esistenti non riducono sufficientemente il rischio. Secondo, gli asset legacy presentano pesi medi di controllo inferiori (es. cluster 1: peso 0,3286) e talvolta efficacia sotto soglia (0,4714), esponendo elementi obsoleti a rischio elevato senza adeguata mitigazione. Infine, alcuni controlli con elevato peso risultano poco efficaci in pratica (es. "Verifica escalation" efficacia 0,4833), suggerendo necessità di revisione delle modalità di esecuzione o di rafforzamento operativo.

Raccomandazioni operative

- **Prioritizzare interventi su "Incidenti non gestiti in tempo":** incrementare monitoraggio del MTTR, formalizzare playbook di escalation e re‑designare le verifiche di escalation per innalzare l’efficacia oltre la media attuale di 0,5056.

- **Rinforzare la copertura sui sistemi legacy:** rivedere i pesi di controllo per "cluster 1- host legacy" (peso medio 0,3286) e allocare controlli a maggiore impatto per portare efficacia verso la media aziendale.

- **Ricalibrare controlli con basso rendimento**: analizzare i processi relativi a controlli con efficacia <0,4 (es. "Campionamento account orfani" efficacia 0,3000) per determinare se rinforzarli, riprogettare l’approccio o sostituirli con controlli alternativi più efficaci.

- **Consolidare best practice su controlli ad alto impatto**: formalizzare l’approccio di controlli con efficacia superiore (es. "Audit IAM/PAM" efficacia 0,6000) e replicarne elementi sui controlli critici per aumentare efficacia complessiva.

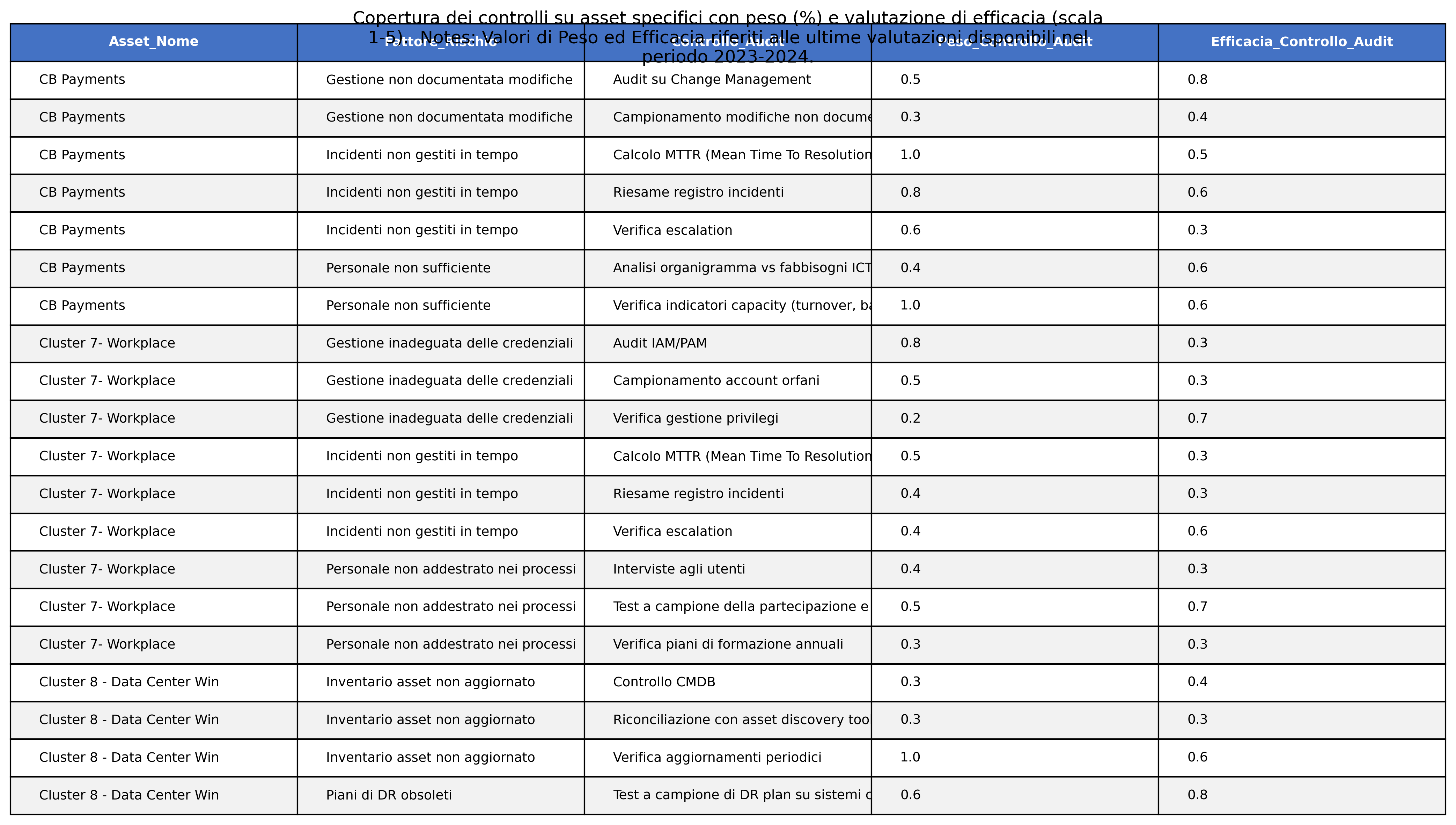
Sintesi esecutiva

L’analisi su 81 record evidenzia concentrazione dei rischi sugli incidenti temporali (22,22% dei casi) e varianza nella qualità dei controlli: peso medio 0,54321 ed efficacia media 0,52593. Le evidenze quantitative indicano focali operative chiare su asset legacy e su controlli relativi alla gestione degli incidenti. Interventi mirati su priorità, riallocazione del peso dei controlli e revisione delle pratiche operative possono aumentare l’efficacia di mitigazione e ridurre l’esposizione complessiva.

**VISUALIZZAZIONI**



*Figura: table\_20251121\_124037*



*Figura: table\_20251121\_124223*

**SEZIONE 3 – EFFICACIA DELLE VERIFICHE DI CONFORMITÀ E DISTRIBUZIONE DELLE VALUTAZIONI**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.1 Punteggi Delle Verifiche Per Area Normativa (Trend 2023-2024)**

3.1 Punteggi delle verifiche per area normativa (trend 2023–2024)

Sintesi dei dati analizzati

- L’analisi utilizza la tabella CR05ComplianceArNormVerifNormPlan, che contiene 149 record complessivi.

- Nel periodo considerato per il trend (anni 2023–2024) risultano registrati solo 2 verifiche, pari al 1,34% del totale (2/149).

- L’intervallo di punteggio rilevato nella tabella è 0–2; la somma totale dei punteggi è 2 e la media aritmetica sull’intero dataset è 0,0134 (2/149 ≈ 0,01342).

Trend 2023–2024 per Area\_Normativa

* Nel 2024 si registrano due verifiche, ciascuna appartenente a una diversa Area\_Normativa:

- "LA GESTIONE DEI PROGETTI E DEI CAMBIAMENTI ICT": 1 verifica (2024), punteggio medio 0.

- "GOVERNO, ORGANIZZAZIONE E CONTROLLI DEL SISTEMA INFORMATIVO": 1 verifica (2024), punteggio medio 2.

- Il punteggio medio aggregato per il biennio 2023–2024 è pari a 1,0 (somma punteggi 2 diviso 2 verifiche). Tuttavia, la base campionaria è estremamente limitata (n=2), pertanto qualsiasi interpretazione di trend risulta statisticamente fragile.

Distribuzione per area e osservazioni quantitative

- Nella fotografia complessiva (tutti gli anni presenti nella tabella) le aree normative con maggiore numero di verifiche sono:

* GESTIONE DEL RISCHIO ICT E DI SICUREZZA: 27 verifiche (18,12% del totale)
* GESTIONE DELLA SICUREZZA DELL’INFORMAZIONE E DELLE OPERAZIONI ICT: 24 verifiche (16,11%)

- L’ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO E IL RICORSO A SOGGETTI TERZI PER LA PRESTAZIONE DI SERVIZI ICT: 21 verifiche (14,09%)

* LA CONTINUITÀ OPERATIVA: 18 verifiche (12,08%)
* LA GESTIONE DEI PROGETTI E DEI CAMBIAMENTI ICT: 17 verifiche (11,41%)

- Per le prime 9 aree più frequenti, il punteggio medio calcolato su tutti i record risulta pari a 0. In pratica, su 149 verifiche totali la somma dei punteggi è pari a 2, il che indica che quasi tutte le registrazioni riportano punteggio nullo o non assegnato.

Interpretazione e impatto operativo

- La disponibilità di soli 2 record per il periodo 2023–2024 impedisce la definizione di un trend affidabile a livello annuale o semestrale. L’apparente variabilità (0 vs 2) riflette un campione troppo esiguo per inferenze robuste.

- La quasi totalità dei record con punteggio medio pari a 0 indica un problema di copertura o di popolamento del campo VerificationScore15: può trattarsi di punteggi non assegnati, di un’interpretazione diversa del campo oppure di un processo di tracciamento incompleto.

- Dal punto di vista del rischio e del reporting, l’assenza di dati aggregati significativi riduce la capacità di monitorare l’efficacia dei controlli per area normativa, di confrontare performance tra aree e di individuare regressioni o miglioramenti nel tempo.

Raccomandazioni operative e visualizzazione

- Nonostante la limitazione dei dati, si raccomanda la visualizzazione mediante un bar chart che riporti, per ciascuna Area\_Normativa, il punteggio medio 2023–2024 con etichettatura del numero di osservazioni (n). Tale grafico evidenzia immediatamente la scarsità delle osservazioni per il biennio e permette di segnalare le aree con punteggio non nullo.

* Azioni prioritarie per migliorare la qualità del trend reporting:

1. Standardizzare e rendere obbligatorio il campo VerificationScore15 al momento della registrazione della verifica, con controlli di qualità sui valori accettati.

2. Incrementare la copertura temporale: mirare a raccogliere almeno 20–30 verifiche per anno nel perimetro di controllo per ottenere trend confrontabili (valore indicativo da adeguare alla dimensione operativa).

3. Introdurre KPI di data quality: percentuale di verifiche con punteggio assegnato per anno (obiettivo iniziale > 90%).

4. Effettuare una revisione retrospettiva dei record esistenti per mappare punteggi eventualmente non registrati o memorizzati in documenti allegati.

- A medio termine, una reportistica affidabile richiede sia maggiore numerosità delle verifiche recenti sia uniformità nella codifica del punteggio. Solo con una base dati più consistente diventa possibile implementare bar chart comparativi per area e analisi di trend 2023 vs 2024 con significatività statistica.

Conclusione sintetica

- I dati attuali mostrano 149 record complessivi ma soltanto 2 rilevazioni riferite al periodo 2023–2024 (1,34% del totale) e una somma complessiva dei punteggi pari a 2. La limitata numerosità e l’elevata prevalenza di punteggi nulli impediscono di trarre conclusioni robuste sul trend dei punteggi per area normativa. Si suggerisce di intervenire prioritariamente sulla qualità e sulla completezza della raccolta dei punteggi prima di avviare analisi comparative strutturate.

**3.2 Distribuzione Dell'Efficacia Dei Controlli Per Asset**

3.2 Distribuzione dell'efficacia dei controlli per asset

Sintesi dei dati e ambito dell’analisi

L’analisi si basa sulla tabella RM05RiskMAssetRischioEventoContr, che contiene 121 record riferiti a 16 asset distinti. La metrica impiegata è EfficaciaControlloAudit, con valori osservati nell’intervallo 0,30–0,80 (30%–80%). La media complessiva osservata per tutti i record è 0,536 (53,6%), mentre la media degli average per asset è 0,5371 (53,71%). Questi valori costituiscono la base per la valutazione comparativa dell’efficacia dei controlli per singolo asset.

Risultati principali per asset (medie e volumi)

La distribuzione delle medie per asset mostra differenze significative tra i gruppi:

- Asset con le medie più alte: "Cluster 7- Workplace" presenta la media più elevata pari a 0,6375 (63,75%) con 8 record; "Finance" riporta una media di 0,6286 (62,86%) su 7 record; "cluster 5- Data Farm Oracle" ha media 0,6250 (62,50%) su 8 record.

- Asset con le medie più basse: "Multichannel" riporta la media più bassa pari a 0,4250 (42,50%) con 8 record; "CB Payments" ha media 0,4571 (45,71%) su 7 record; sia "Management Systems" sia "Security App" presentano medie di circa 0,4857 (48,57%) su 7 record ciascuno.

Per contestualizzare la rappresentatività: i 10 asset principali per frequenza coprono ciascuno tra il 5,79% e il 7,44% del totale dei record (ad esempio "cluster 1- host legacy" e "cluster 4 - Server Farm Linux" rappresentano ciascuno il 7,44% dei record).

Dispersione e variabilità dell’efficacia

La variabilità interna agli asset (misurata tramite deviazione standard) varia in modo significativo: la deviazione standard degli asset oscilla tra circa 0,1035 (10,35 punti percentuali) e 0,2360 (23,60 punti percentuali). Gli asset con maggiore variabilità includono "Cluster 8 - Data Center Win" (stddev = 0,2360, media 57,14%) e "cluster 2 - App Server Farm Windows" (stddev = 0,2116, media 58,57%). L’elevata dispersione indica applicazione non uniforme dei controlli o presenza di casi anomali che aumentano la variabilità. Al contrario, asset come "Multichannel" mostrano media bassa (42,5%) con deviazione standard relativamente contenuta (≈0,128), segnalando una debolezza dei controlli consistente e diffusa piuttosto che episodi isolati.

Osservazioni operative e implicazioni per il rischio

- Quattro asset su sedici (25%) hanno una media di efficacia inferiore al 50% (Multichannel, CB Payments, Management Systems, Security App). Ciò identifica un cluster di asset con controlli sistematicamente insufficienti che richiede intervento prioritario.

- Gli asset con media relativamente alta (>60%) rappresentano buone pratiche locali (ad es. Cluster 7- Workplace, Finance), che possono costituire riferimento per misure di rimedio e standardizzazione.

- Asset con elevata deviazione standard (es. Cluster 8 - Data Center Win) evidenziano incoerenze operative: è opportuno approfondire le cause di variabilità (diverse tipologie di controllo, esecuzione irregolare, o campionamento eterogeneo) e ridurne la dispersione tramite processi e controlli più omogenei.

Raccomandazione sulla visualizzazione (box plot) e linee di intervento

Per comunicare efficacemente la distribuzione per asset, si raccomanda la rappresentazione tramite box plot per ciascun asset (ordinati per mediana o media). Il box plot mette in evidenza mediana, IQR (interquartile range) e outlier, facilitando l’identificazione di:

- asset con mediane sotto la soglia di accettabilità (es. <50%),

* asset con IQR ampio (controlli non coerenti),
* outlier che richiedono approfondimento puntuale.

Azioni operative suggerite

1. Prioritizzare interventi correttivi sugli asset con media <50% (4 asset, 25% del totale): definire piani di miglioramento, responsabilità e tempistiche.

2. Indagare asset con elevata variabilità (stddev > 0,20): eseguire root-cause analysis per identificare cause di applicazione disomogenea dei controlli.

3. Standardizzare e documentare le procedure di controllo negli asset con performance elevate per favorire trasferimento di best practice.

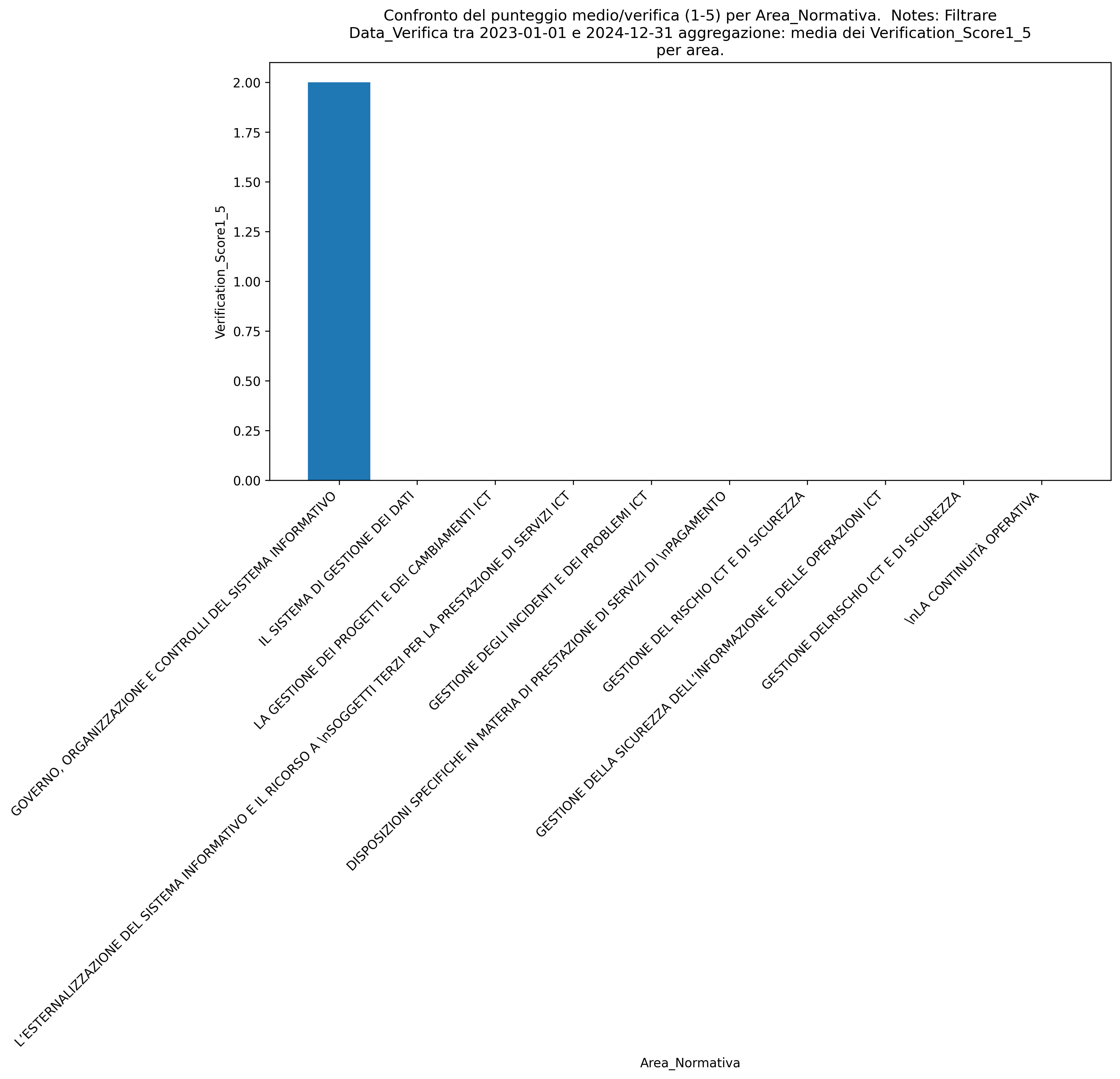
4. Definire soglie target (es. obiettivo operativo iniziale 70% di efficacia media per asset) e istituire monitoraggio continuo con reporting trimestrale.

5. Utilizzare box plot come visualizzazione principale nel reporting esecutivo per mostrare rapidamente mediane, IQR e outlier per ciascun asset.

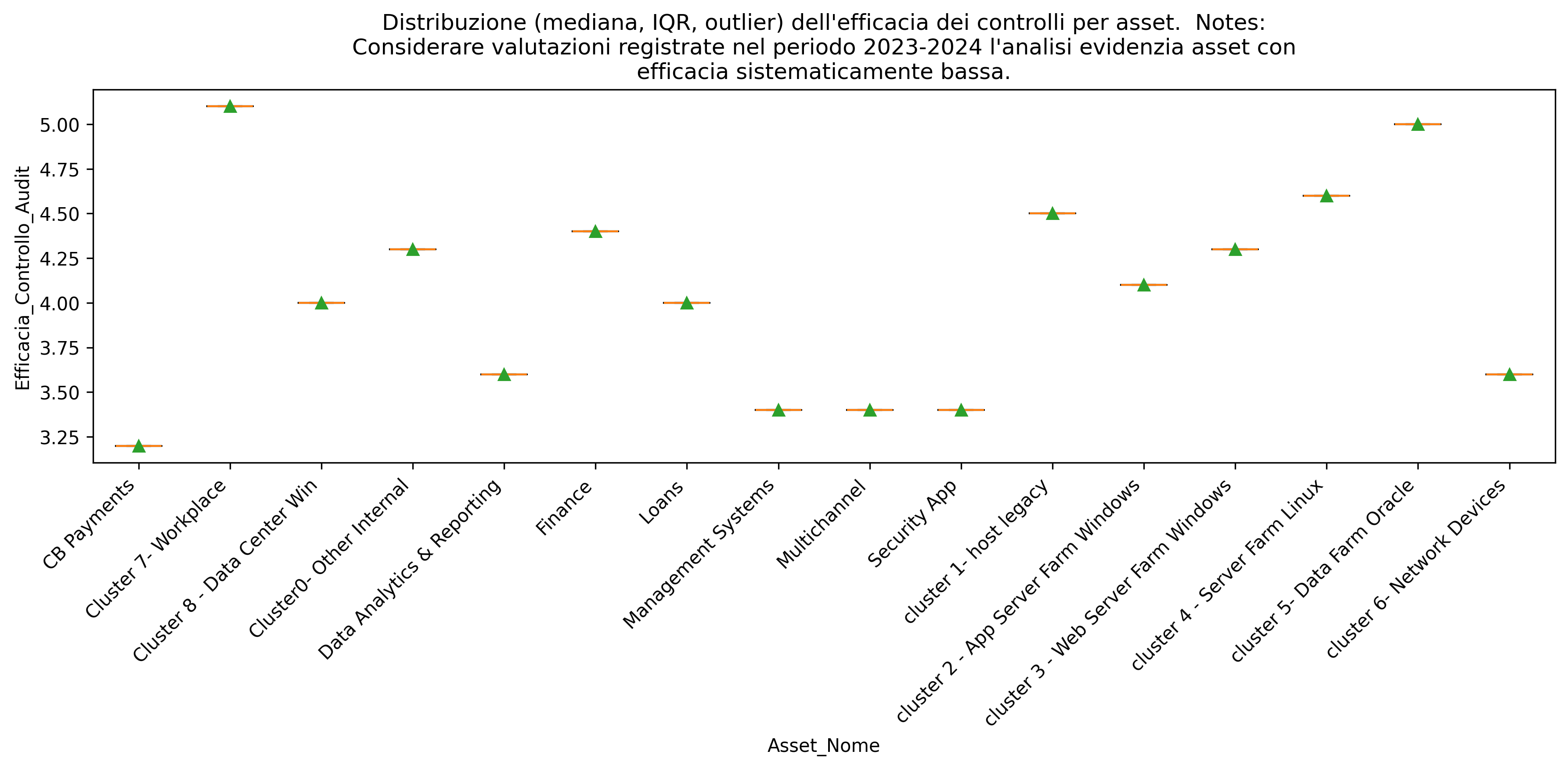
Conclusione

L’analisi quantitativa evidenzia una media complessiva di efficacia dei controlli pari a 53,6% su 121 osservazioni e differenze sostanziali tra asset (medie per asset da 42,5% a 63,75%). Il 25% degli asset mostra efficacia media sotto il 50% e circa il 12–13% degli asset (2 asset) manifesta elevata variabilità (>0,21 stddev). Il box plot per asset costituisce lo strumento più efficace per la comunicazione e la prioritizzazione degli interventi: consente di distinguere rapidamente tra problemi sistemici (bassa media e bassa variabilità) e problemi di coerenza applicativa (alta variabilità), orientando così le azioni di remediation e controllo.

**VISUALIZZAZIONI**



*Figura: bar\_chart\_20251121\_124508*



*Figura: box\_plot\_20251121\_124838*

**SEZIONE 4 – NON CONFORMITÀ E STATO DELLE AZIONI DI REMEDIATION**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.1 Elenco Non Conformità Rilevate E Stato Di Chiusura**

Sezione 4.1 — Elenco non conformità rilevate e stato di chiusura

Sintesi esecutiva

Il dataset analizzato contiene 16 non conformità registrate nella tabella CR06ComplianceElencononConformita. Tutte le 16 segnalazioni risultano chiuse al momento dell’analisi, corrispondendo a un tasso di chiusura del 100,0%. Le rilevazioni sono concentrate nel periodo di marzo 2023 (prima rilevazione 2023-03-01, ultima 2023-03-31) mentre le chiusure si estendono tra il 2023-06-14 e il 2024-02-12. Il tempo medio di chiusura è pari a 205 giorni, con un minimo registrato di 85 giorni e un massimo di 335 giorni.

Distribuzione per Area Normativa

La quota maggiore di non conformità si concentra nell’area “GESTIONE DELLA SICUREZZA DELL’INFORMAZIONE E DELLE OPERAZIONI ICT”, che rappresenta 7 casi su 16 (43,75%). Seguono “GESTIONE DEL RISCHIO ICT E DI SICUREZZA” e “LA CONTINUITÀ OPERATIVA”, ciascuna con 3 casi (18,75% ciascuna). L’area “IL SISTEMA DI GESTIONE DEI DATI” include 2 segnalazioni (12,50%) e “GESTIONE DEGLI INCIDENTI E DEI PROBLEMI ICT” risulta con 1 caso (6,25%). Questa concentrazione indica una prevalenza di criticità legate alla sicurezza informativa e alla gestione operativa ICT, con impatti potenziali su riservatezza, disponibilità e integrità dei servizi digitali.

Origine delle segnalazioni e quadro regolamentare

La fonte prevalente delle non conformità è la Funzione Audit, responsabile del 50,0% dei casi (8 su 16). Le ispezioni della BCE costituiscono il 31,25% (5 casi) mentre la Funzione Compliance contribuisce per il 18,75% (3 casi). Dal punto di vista normativo, i casi sono distribuiti su tre regimi principali: GDPR con 6 casi (37,50%), una categoria identificata come “285” con 5 casi (31,25%) e DORA con 5 casi (31,25%). La sovrapposizione tra aree di rischio tecnologico e requisiti normativi (GDPR e DORA) evidenzia la necessità di approcci integrati tra privacy, resilienza operativa e sicurezza ICT.

Tempi di rilevazione e chiusura

Tutte le non conformità sono state rilevate nell’arco di un mese (marzo 2023) e la finestra di chiusura si estende su circa otto mesi fino a febbraio 2024. Il tempo medio di 205 giorni per la risoluzione indica processi di remediation che richiedono sforzi sostenuti e coordinamento tra funzioni tecniche e di governance. La variabilità (minimo 85 giorni, massimo 335 giorni) suggerisce che alcune pratiche sono chiuse con efficienza mentre altre richiedono interventi complessi e prolungati, probabilmente per l’implementazione di misure strutturali (es. piani di resilienza, adeguamenti contrattuali con fornitori, implementazioni tecnologiche rilevanti).

Osservazioni operative e raccomandazioni

- Prioritizzazione: l’azienda deve focalizzare risorse e governance sulle aree con maggiore concentrazione di non conformità (sicurezza informativa e gestione rischio ICT). Interventi mirati su questi 7 elementi possono ridurre sostanzialmente il rischio complessivo.

- Riduzione dei tempi di chiusura: con un tempo medio di 205 giorni, è opportuno definire KPI target (es. ridurre il tempo medio a <120 giorni) e introdurre checkpoint di avanzamento per accelerare remediation critiche.

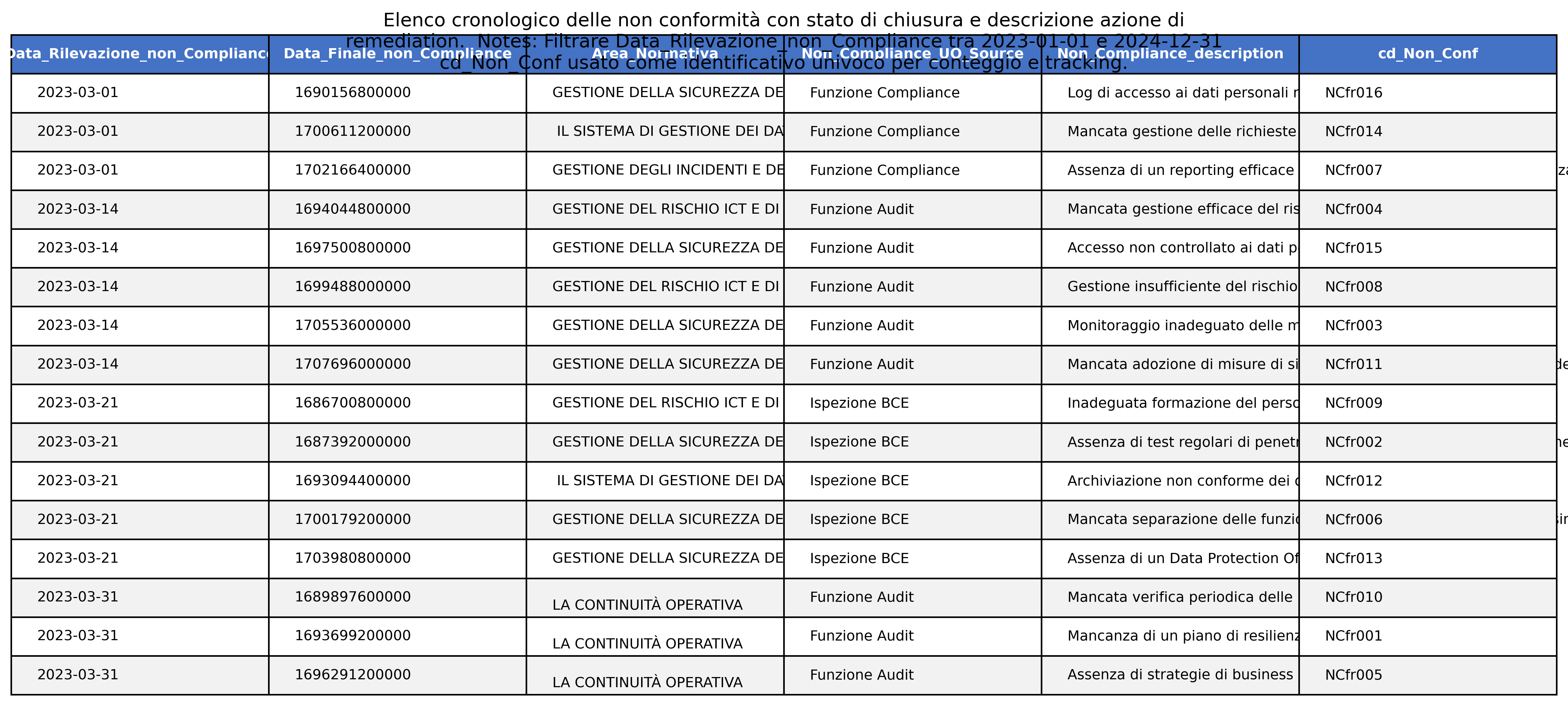
- Allineamento regolamentare: la presenza simultanea di GDPR, DORA e altre normative richiede un framework di compliance integrato che evidenzi obblighi trasversali e mitigazioni condivise (policy, controlli tecnici, formazione).

- Rafforzamento del monitoraggio post-chiusura: pur avendo il 100% di casi chiusi, è consigliabile formalizzare controlli di efficacia a 3-6 mesi dopo la chiusura per verificare che le misure implementate mantengano il rischio entro soglie accettabili.

Conclusioni

L’analisi fornisce una fotografia completa: 16 non conformità, tutte chiuse, con concentrazione nel dominio della sicurezza informativa e tempi di rimedio mediamente lunghi (205 giorni). Il quadro indica capacità di chiusura delle segnalazioni ma evidenzia margini di miglioramento nella rapidità di intervento e nella governance integrata tra funzioni operative, audit e compliance, soprattutto per conformarsi efficacemente a GDPR e DORA. Implementare azioni prioritarie e KPI di tempo di chiusura risulta essenziale per ridurre il rischio operativo e regulatorio.

**VISUALIZZAZIONI**



*Figura: table\_20251121\_125017*

**SEZIONE 5 – RISCHIO RESIDUO, GAP PRIORITARI E SINTESI DEI GAP DI SICUREZZA**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5.1 Rischio Residuo Per Asset (Prioritizzazione)**

5.1 Rischio residuo per asset (prioritizzazione)

Sintesi dei dati e dimensione del campione

La tabella RM11RiskMValutazioneRischioEvento contiene 48 record relativi alla valutazione del rischio evento. Le osservazioni sono raggruppate su 16 asset distinti (media pari a 3 valutazioni per asset). Il RischioResiduo presenta un valore minimo registrato di 1,2, un valore massimo di 17,5 e una media complessiva pari a 6,3229 (totale Rischio\_Residuo = 303,5). L’efficacia media dei controlli è 0,4708 (≈47,08%), indicativa di un’efficacia parziale degli interventi di mitigazione attuali.

Distribuzione per tipologia e criticità

Gli asset si distribuiscono per tipo con 27 record relativi ad Infrastruttura (56,25%) e 21 ad Applicazione (43,75%). Le valutazioni sono prevalentemente classificate come “Critico”: 39 record (81,25%) vs 9 record (18,75%) classificati “Importante”. Questa concentrazione di criticità richiede attenzione immediata nella prioritizzazione degli interventi.

Cluster di rischio residuo e soglie operative

Per agevolare la prioritizzazione si definiscono tre bucket operativi basati sul Rischio\_Residuo:

* Alto (>= 10): 12 record, pari al 25,0% del totale;
* Medio (5–9,99): 14 record, pari al 29,17% del totale;

- Basso (< 5): 22 record, pari al 45,83% del totale.

Questa suddivisione mostra che il 54,17% delle osservazioni supera la soglia di rischio basso (Rischio\_Residuo >= 5), mentre il 25% richiede attenzione prioritaria immediata (>= 10).

Asset con priorità più elevate

Analisi degli indicatori per asset evidenzia i seguenti elementi prioritari (ordinati per media Rischio\_Residuo decrescente):

* Management Systems — cnt=3, media Rischio\_Residuo = 11,433 (max 17,5)
* cluster 5 - Data Farm Oracle — cnt=3, media = 8,233 (max 10,5)
* Security App — cnt=3, media = 8,233 (max 11,2)
* cluster 2 - App Server Farm Windows — cnt=3, media = 8,167 (max 17,5)
* Cluster 8 - Data Center Win — cnt=3, media = 8,000 (max 10,5)

Inoltre, i singoli record con Rischio\_Residuo massimo (valore 17,5) riguardano asset quali “cluster 2 - App Server Farm Windows” e “Management Systems”, rendendoli punti chiave per interventi correttivi urgenti.

Interpretazione e implicazioni operative

- Priorità immediata: il 25% dei record (12 su 48) con Rischio\_Residuo >= 10 rappresenta il primo ambito di intervento. Questi casi combinano spesso alta probabilità e impatto, non completamente mitigati dai controlli correnti (efficacia media controllo ≈ 47%).

- Focus per tipologia: sia Infrastruttura che Applicazione mostrano livelli medi di rischio residuo simili (media Applicazione = 6,4429 vs Infrastruttura = 6,2296), pertanto le azioni devono coprire entrambe le categorie senza privilegiare esclusivamente una tipologia.

- Asset strategici: Management Systems e i cluster server appaiono come punti critici per l’operatività e devono entrare nelle prime azioni correttive per ridurre l’esposizione complessiva.

Raccomandazioni di prioritizzazione e azione

1. Esecuzione di interventi correttivi immediati sugli asset con Rischio\_Residuo >= 10 (12 record, 25%): patching urgente, rafforzamento controlli di accesso, e verifica delle configurazioni di sicurezza sui server identificati.

2. Piano trimestrale per ridurre del 50% il numero di record con RischioResiduo >= 10 entro 6 mesi, misurando l’efficacia tramite diminuzione della media RischioResiduo e aumento di Efficacia\_Controlli.

3. Monitoraggio continuo e revisione delle misure di controllo sugli asset con media Rischio\_Residuo >= 8 (top 5 elencati): assegnare risorse dedicate e fissare KPI operativi (riduzione media per asset, tempo di remediation medio).

4. Consolidamento del reporting di rischio con bar chart settoriale: visualizzare la media di RischioResiduo per AssetNome ordinata discendentemente, includendo linee soglia a 5 e 10 e indicatore di Efficacia\_Controlli. Questo grafico barre facilita decisioni rapide di allocazione risorse e comunicazione verso il Board.

Proposta di visualizzazione (bar chart)

Si raccomanda un bar chart con:

* Asse X: AssetNome (ordinati per media RischioResiduo decrescente)
* Asse Y: media Rischio\_Residuo (valore numerico)

- Annotazioni: numero di record per asset (cnt), linea di soglia a 5 (rischio medio) e a 10 (rischio alto), colore delle barre differenziato per Asset\_Tipo (Applicazione vs Infrastruttura).

Questo grafico evidenzia chiaramente le priorità operative e supporta il monitoraggio dell’efficacia degli interventi.

Conclusione

La valutazione mostra una concentrazione significativa di rischi residui su un sottoinsieme di asset: 25% delle osservazioni necessita di azioni prioritarie e il 54,17% supera la soglia operativa di attenzione (Rischio\_Residuo >= 5). L’insieme di raccomandazioni proposte consente di tradurre l’analisi quantitativa in un piano operativo misurabile, con obiettivi temporali e KPI per ridurre rapidamente l’esposizione più critica.

**5.2 Asset Con Gap Evidenti (Bassa Efficacia + Alto Rischio Residuo)**

Sezione 5.2 — Asset con gap evidenti (bassa efficacia + alto rischio residuo)

Sintesi quantitativa

- Il set di dati analizzato contiene 48 record totali nella tabella RM11RiskMValutazione\_RischioEvento.

- La media complessiva di EfficaciaControlli è pari a 0,4708; la media complessiva di RischioResiduo è pari a 6,3229.

- Sono 20 i record (41,67% del totale) con Efficacia\_Controlli <= 0,4, categoria definita come “bassa efficacia”.

- Tra tutti i record, 11 record (22,92% del totale) presentano contemporaneamente EfficaciaControlli <= 0,4 e RischioResiduo >= media complessiva (>= 6,3229): si tratta dei casi di gap più critici sul piano operativo e di rischio residuo.

- A livello di aggregazione per asset, sono 8 asset distinti che mostrano media di RischioResiduo pari o superiore alla media complessiva e contemporaneamente media di EfficaciaControlli bassa (<= 0,4).

Asset con priorità di intervento

L’analisi identifica gli asset su cui concentrare le azioni correttive per ridurre il rischio residuo e aumentare l’efficacia dei controlli. I principali asset con gap evidenti (ordinati per Rischio\_Residuo medio decrescente) sono:

- cluster 2 - App Server Farm Windows: 1 record, EfficaciaControlli media 0,3, RischioResiduo medio 17,5 (valore massimo osservato).

- Management Systems: 3 record, EfficaciaControlli media 0,3, RischioResiduo medio 11,4333.

- Security App: 2 record, EfficaciaControlli media 0,3, RischioResiduo medio 10,85.

- Cluster 8 - Data Center Win: 1 record, EfficaciaControlli media 0,3, RischioResiduo medio 10,5.

- CB Payments: 2 record, EfficaciaControlli media 0,3, RischioResiduo medio 8,05.

- cluster 5 - Data Farm Oracle: 2 record, EfficaciaControlli media 0,3, RischioResiduo medio 7,35.

- Data Analytics & Reporting: 2 record, EfficaciaControlli media 0,3, RischioResiduo medio 7,00.

- Finance: 1 record, EfficaciaControlli media 0,3, RischioResiduo medio 7,00.

Osservazioni di contesto

- La concentrazione di record con criticità è significativa: il 81,25% dei record totali è classificato come “Critico” per criticità di rischio evento, suggerendo che la maggior parte delle registrazioni riguarda scenari ad alto potenziale impatto.

- La tipologia degli asset coinvolti comprende sia infrastrutture (56,25% dei record) sia applicazioni (43,75%), pertanto le misure correttive devono includere interventi tecnici su infrastrutture e processi/controlli applicativi.

- La bassa variabilità dell’indicatore Efficacia\_Controlli all’interno del sottoinsieme critico (valori medi ricorrenti a 0,3) indica che molte controlli segnalati come attivi risultano uniformemente poco efficaci e richiedono una revisione omogenea delle misure di mitigazione.

Implicazioni operative e di rischio

- Gli asset indicati con RischioResiduo superiore alla media e con EfficaciaControlli bassa rappresentano esposizioni immediate: il caso più urgente (cluster 2 - App Server Farm Windows) presenta Rischio\_Residuo 17,5, oltre il doppio della media complessiva.

- Questi gap aumentano la probabilità di incidenti con impatti rilevanti sui processi core e sui dati sensibili. La presenza di più record critici su Management Systems e Security App evidenzia rischi trasversali che possono impattare più ambiti aziendali.

Raccomandazioni prioritarie

1. Prioritizzazione tripartita: assegnare priorità immediata agli asset con RischioResiduo > 10 e EfficaciaControlli <= 0,4 (es. cluster 2, Management Systems, Security App, Cluster 8), con interventi di remediation entro il prossimo trimestre.

2. Revisione e rafforzamento controlli: rivedere le misure preventive e detective esistenti (configurazioni, patch management, monitoraggio dei log, controlli di accesso) per aumentare l’Efficacia\_Controlli target almeno a 0,6 su asset critici.

3. Misure compensative a breve termine: introdurre controlli compensativi (monitoraggio continuo, segmentazione, controlli d’accesso rafforzati, detection rules) dove la mitigazione strutturale richiede più tempo.

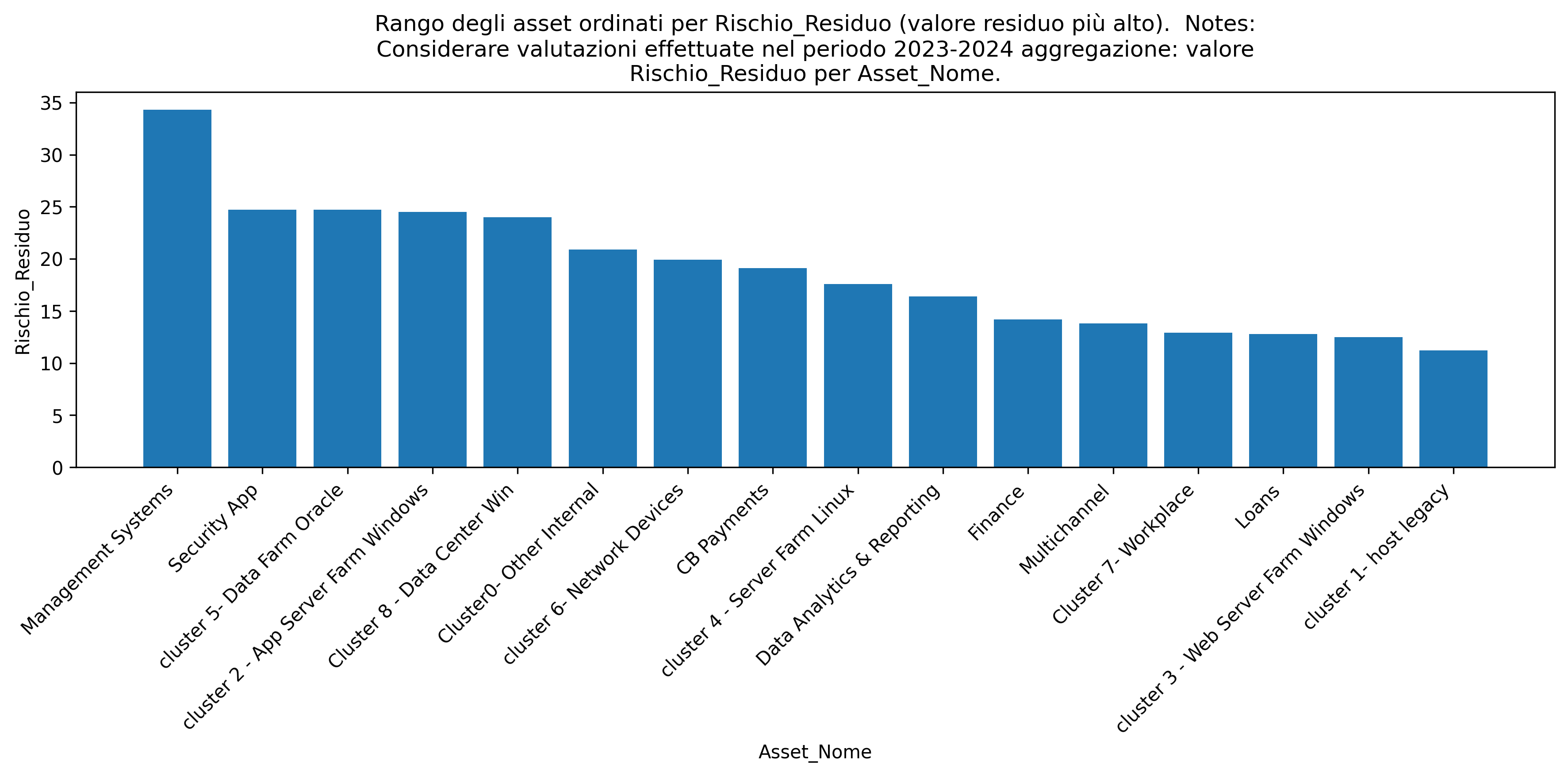
4. Verifica post-intervento: definire KPIs di verifica (EfficaciaControlli obiettivo, riduzione RischioResiduo target) e rieseguire la valutazione entro 3 mesi per validare la riduzione del rischio residuo.

5. Governance e reporting: includere gli 8 asset identificati in un piano di escalation al Comitato di Rischio con report mensile sullo stato di avanzamento delle azioni correttive.

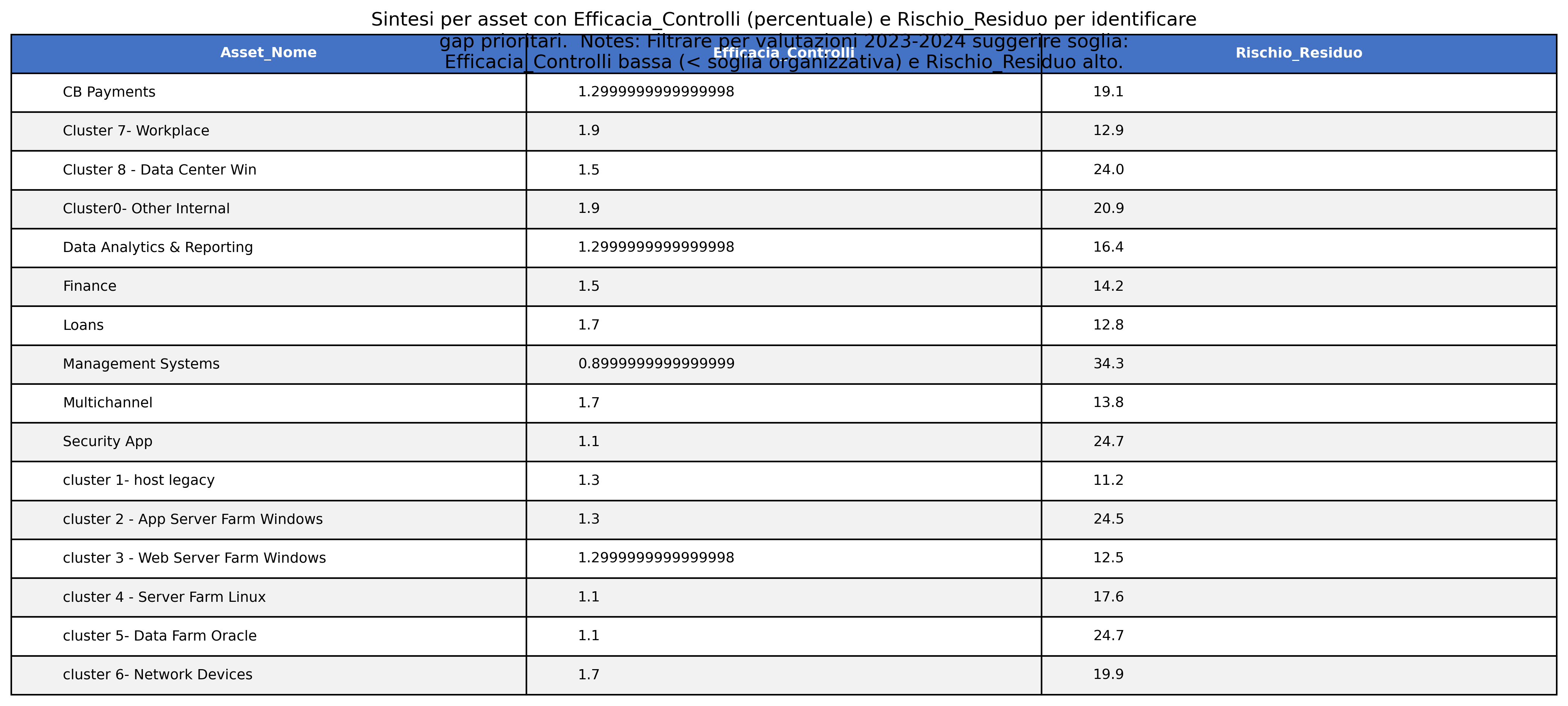
Conclusione

L’analisi evidenzia un cluster rilevante di 20 record con controlli a bassa efficacia e 11 record con congiunta esposizione a rischio residuo elevato. Otto asset distinti presentano una combinazione di controllo debole e rischio residuo superiore alla media; questi asset costituiscono la prima linea di intervento per ridurre rapidamente l’esposizione complessiva. L’implementazione di interventi prioritari, controlli compensativi e un ciclo di verifica definito consente di ridurre il rischio residuo e migliorare l’efficacia operativa delle misure di controllo.

**VISUALIZZAZIONI**



*Figura: bar\_chart\_20251121\_125252*



*Figura: table\_20251121\_125417*

**SEZIONE 6 – CONCLUSIONI OPERATIVE (SINTESI)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Breve chiusura con i principali gap identificati (es.: aree normative con punteggi di verifica bassi, asset con alta esposizione residua e controlli con efficacia insufficiente) e le priorità suggerite (interventi tecnico-organizzativi su asset prioritari, rafforzamento controlli dove la copertura è scarsa, chiusura delle non conformità aperte 2023-2024).

Nota finale: tutti i filtri temporali indicati (2023-2024) devono essere applicati alle colonne data disponibili (es. DataVerifica, DataRilevazionenonCompliance). Per le tabelle senza colonne data, utilizzare le valutazioni/registrazioni più recenti acquisite nel periodo 2023-2024.