

1

Le dimensioni del controllo dei rischi IT

Il tema del **controllo sull'attività IT** è sempre più attuale a seguito degli sviluppi tecnologici in atto e delle **rischiosità collegate**.

La pervasività delle tecnologie informatiche sui processi di business impongono un **presidio attento e costantemente aggiornato**.

Legislatori, regolatori e gli stessi mercati sono oggi particolarmente attenti a monitorare gli impatti e a stabilire regole di prevenzione dei **rischi sui dati e sulle elaborazioni**.

Rischi	Principali riferimenti normativi	Principali Impatti
Rischi ICT e di Sicurezza	Circolare 285/13 Banca d'Italia - 40° aggiornamento	- Funzione dedicata controllo 2° livello sul rischio IT - Metodologia Controllo di 2° livello su analisi di rischio IT
Rischi sulla Qualità dei Dati	Data Quality Guidelines (Unione Europea)	- KQI di Qualità dei dati
Rischi Cyber	Direttiva UE NIS2 Regolamento DORA (Digital Operational Resilience Act)	- Attivazione di un presidio Cyber DORA-Compliant - Certificazione adeguatezza
Rischi Artificial Intelligence	Proposta di Regolamento per regole armonizzate sull'intelligenza artificiale (Commissione Europea) Report on big data and Advanced analytics (EBA)	- Sviluppo dell'AI rispettando gli standard etici - Controlli sulla piena applicazione degli standard etici di Intelligenza Artificiale

Il **sistema dei controlli** è tipicamente articolato in 4 fasi, di cui la prima è insita nel processo operativo stesso (controlli di linea) e altre 3 sono eseguite lateralmente al processo e coinvolgono strutture dedicate e specializzate.

Controlli di 1° livello o di linea

Sono attività di controllo eseguite **contestualmente alle elaborazioni** e sono finalizzate ad assicurare nell'immediato la correttezza dei dati inseriti o delle scelte funzionali effettuate. Riguardano prevalentemente le verifiche formali (controlli formali), ma possono valutare anche il merito delle operazioni (controlli di merito). Le attività di controllo **sono svolte a posteriori** al fine di assicurare che la processazione effettuata sia stata eseguita correttamente. In tal caso hanno prevalentemente un ruolo di assicurazione del merito, ma non sono escluse verifiche formali.

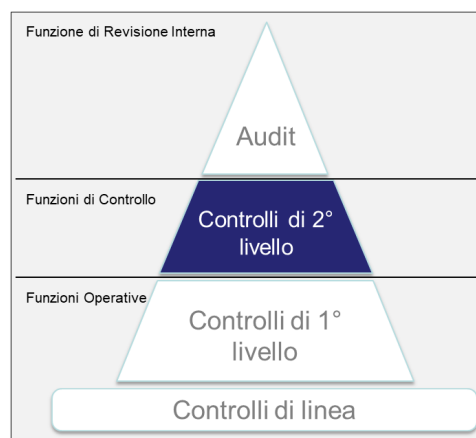
Controlli di 2° livello

Verificano e assicurano in merito alla adeguatezza ed effettività delle attività di controllo (controlli di linea e di 1° livello). Si riferiscono sia al **controllo di conformità delle operazioni IT** che al **controllo delle rischiosità IT**. Esprimono una valutazione del sistema di controllo operativo, utilizzata a sua volta per migliorare robustezza ed efficacia del sistema di controllo stesso. Opportuni Key Quality Indicators (KQI) sono solitamente utilizzati per il monitoraggio direzionale.

Controlli di 3° livello

Sono le attività di **revisione interna** e costituiscono l'ultima barriera di controllo delle attività IT e sono finalizzate a monitorare la tenuta del sistema di controllo complessivo ai fini della assicurazione e rendicontazione diretta agli Organi Aziendali. I controlli di auditing non hanno i caratteri della sistematicità e quindi non possono avere un ruolo operativo.

La Piramide del controllo



Se i controlli di livello operativo e di revisione interna sono storicamente diffusi e sistematicamente eseguiti all'interno delle aziende, i **controlli di 2° livello iniziano ora ad essere definiti, applicati e rendicontati**, sotto la spinta di regolatori e legislatori.

Le caratteristiche tipiche di un Sistema di Controllo sono applicate anche ai Sistemi di Controllo IT

COMPLETEZZA

- La completezza rappresenta la capacità del Sistema dei Controlli Interni di presidiare l'intero perimetro delle rischiosità aziendali

ADEGUATEZZA

- L'adeguatezza si riferisce al corretto disegno del Sistema dei Controlli Interni rispetto alle rischiosità da presidiare

AFFIDABILITA'

- L'affidabilità del Sistema dei Controlli si riferisce alla sua capacità di operare in maniera sistematica e ricorrente nel tempo

FUNZIONALITA'

- La funzionalità si riferisce alla capacità del Sistema dei Controlli di fronteggiare i rischi (efficacia) e di farlo ad un costo ragionevole (efficienza) in relazione agli impatti dei rischi stessi

Analogamente agli altri ambiti di Rischio, anche il Sistema di Controllo è soggetto a valutazione di 2° livello.

STRUTTURA ORGANIZZATIVA

Le indicazioni regolamentari (es. 285/13) richiedono strutture organizzative:



- Dedicate
- Esenti da ruoli operativi
- Indipendenti
- Competenti
- Adeguatamente dimensionate

METODOLOGIE

Le attività di controllo devono essere svolte sulla base di metodologie di lavoro strutturate e consolidate



- Analisi preliminari di focalizzazione
- Tempistiche ricorrenti
- Check-list
- Criteri di valutazione omogenei

STRUMENTI DI SUPPORTO

Le attività di controllo devono beneficiare di strumenti di supporto che ne facilitano lo svolgimento e la ren-

- Gestione delle attività di verifica
- Capacità di elaborazione per supportare i controlli (es. anomaly detection sui dati)



- Produzione sistematica di reporting
- Indicatori di misura e valutazione (KQI)
- Strumenti di controllo

L'esecuzione strutturata dei **controlli dei rischi di 2° livello** richiede una struttura organizzativa specializzata, un metodo di lavoro consolidato, strumenti di supporto robusti.

Rischio ICT e di Sicurezza

Analisi del Rischio IT vs Controlli sul Rischio IT

Analisi e valutazione del Rischio IT e Controlli sul Rischio IT sono attività distinte che non devono essere confuse, anche se entrambe sono affidate dai Regulatori alla supervisione da parte di una **medesima struttura di Controllo**.

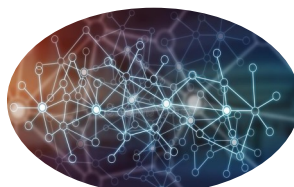
L'**Analisi e la Valutazione del Rischio IT** possono essere efficacemente svolte da strutture operative, che dispongono peraltro di competenze tecniche approfondite ed aggiornate dato il quotidiano operare sulle medesime tecnologie. Tali strutture sono in grado infatti di definire e attuare efficaci controlli di linea o di 1° livello sull'impianto IT e sui rischi corrispondenti.

Il **Controllo su tali attività** e conseguentemente la **valutazione Sistema di Controllo del Rischio IT** è bene che sia svolto in modalità autonoma da una **struttura di 2° livello**, che opera con metodologie, tecniche ed esperienze proprie ed autonome

Hardware



Reti



Basi Dati



Applicazioni



Dati



► Rischio ICT: approccio strutturato esteso a tutte le industries e sulla base di una configurazione a livelli



✓ Solida e comprovata metodologia

E' fondamentale l'utilizzo di metodologie di controllo consolidate e riconosciute, che siano tenute costantemente aggiornate, in grado di supportare una affidabile VALUTAZIONE del livello di sicurezza dei sistemi esaminati

✓ Stumenti di supporto alle attività di controllo

L'attività di controllo deve disporre di strumenti di supporto adeguati a sostenere la complessità del lavoro, quali ad esempio check-list costruite sull'esperienza, competenze che indirizzino le verifiche sulle aree più promettenti, confronti con altre realtà, standard di documentazione e certificazione dei risultati



Check-list metodologiche



Guida all'analisi preliminare del rischio



Strumenti di Benchmarking



Standard di Reporting



✓ Esperienza e competenza delle persone

L'analisi e il controllo sul rischio IT richiede esperienza maturata sul campo e competenze robuste costruite attraverso un aggiornamento continuo delle innovazioni tecnologiche e delle vulnerabilità corrispondenti. Richiede inoltre un sano scetticismo e scaltrezza nella previsione dei rischi

✓ Commitment della Direzione

L'attività di controllo è efficace se è adeguatamente sostenuta da un pieno e convinto commitment della Direzione. Le valutazioni emerse dall'attività di controllo, talvolta dolorose, sono accettate e fatte proprie dalla struttura solo a fronte di un deciso coinvolgimento della Direzione aziendale



Strumenti ed attività sono propedeutici alla produzione **sistematica** di una **reportistica direzionale** corredata di opportuni **indicatori** idonei a misurare nel tempo lo **stato del presidio**

3

Rischi connessi con la Qualità dei Dati

Qualità dei dati: un obiettivo cruciale

Le aziende sono costantemente impegnate a misurare e rappresentare se stesse: attraverso i loro dati, capiscono dove sono e cosa stanno facendo.

Attraverso i dati le aziende determinano e guidano il proprio futuro.

E tramite i dati che presentano esse sono valutate, apprezzate e autorizzate ad operare.

La qualità dei dati è quindi essenziale, oggi più che mai.

Volumi elevati di dati e tecnologie avanzate di elaborazione

Con l'aumento esponenziale della quantità di dati gestiti, delle possibilità di utilizzo di tali dati, degli strumenti di processazione disponibili, nonché delle occasioni di malversazione, la conservazione di una adeguata qualità nei dati aziendali è un'attività esteremamente onerosa e difficile.

Machine Learning & Artificial Intelligence

A ciò, si sono aggiunti negli ultimi anni i nuovi paradigmi di elaborazione basati su Machine Learning e Artificial Intelligence che hanno reso ulteriormente complicato assicurare l'attendibilità e la validità di una determinata informazione.

Il tema del controllo sul processo di produzione e gestione dei dati e la **verifica costante della loro qualità** sta diventando un **obiettivo irrinunciabile**, al quale sono dedicati **risorse, strumenti, investimenti** sempre più rilevanti.

► Il presidio sulla Data Quality

KQI e Anomaly detection sono le chiavi vincenti per la Data Quality

I controlli ordinari (di linea e di 1° livello) sulla qualità dei dati sono consolidati nelle aziende e consentono di assicurare un discreto presidio sulla qualità per le attività meno critiche.

Il problema sorge sulle attività critiche, per le quali l'attendibilità del dato è cruciale (es. esposizione ai regolatori, supporti interni alle decisioni, mansioni critiche).

Oggi si sta affermando l'attività di controllo di 2° livello sulla qualità dei dati, finalizzata a verificare la tenuta dello stesso presidio sulla qualità dei dati (1° livello), nonché la qualità dei processi di produzione e gestione delle informazioni.



Misurare la Qualità dei Dati: i KQI

Innanzitutto è necessario poter misurare la qualità dei dati attraverso un adeguato insieme di indicatori in grado di fornire un'istantanea sulla reale situazione della qualità e indicare le eventuali direzioni di intervento



Anomaly Detection e Reperforming

E' indispensabile poi poter svolgere delle verifiche autonome ed indipendenti dall'operatività al fine di identificare situazioni di degrado o carenza della qualità dei dati (anomaly detection) e di errori di processazione (reperforming).

I grandi volumi di dati oggi e la complessità degli algoritmi da "certificare" richiedono strumenti avanzati, basati su tecnologie di Machine Learning e di Artificial Intelligence, che consentono di ridurre l'impiego delle risorse umane, per concentrarle invece sulle attività realmente "intelligence consuming"



Remediation

Una volta identificate le anomalie o gli errori, deve essere definito un piano di intervento per conseguire la bonifica dei dati e approntato un monitoraggio continuo finalizzato alla sua risoluzione

Gli **indicatori** di qualità e l'andamento delle attività di **remediation** intraprese meritano di essere **riportati sistematicamente agli Organi Aziendali** per rappresentare nel tempo lo **stato del presidio sulla qualità dei dati**

4 Cyber Risk

CYBER: un rischio incalzante

Il rischio Cyber è diventato attuale in tutti gli ambiti di business, veicolato dalla complessità raggiunta dai sistemi informatici e tecnologici e dalla loro pervasività nei processi operativi.

Ma i sistemi informatici sono diventati fondamentali anche per gli stessi processi di governo di tutte le organizzazioni, non solo aziendali, ma anche statali e sovranazionali.

Da qui l'esigenza di protezione sempre più spinta contro i possibili attacchi a scopi di frode, terrorismo, spionaggio.

DORA, NIS2 e gli altri

Gli stessi Regolatori nazionali e sovranazionali hanno iniziato a definire protocolli di **gestione** e **certificazione** della sicurezza dei sistemi informatici (Regolamento DORA, Tallinn 2.0, NIS2, ecc.).

E infatti le organizzazioni sono costantemente impegnate a presidiare in maniera operativa il rischio Cyber con investimenti sempre più rilevanti in termini di competenze e strumenti.

Indotte dagli stessi Regolatori, le organizzazioni stanno attivando **nuovi processi e nuove strutture organizzative** finalizzate alle attività di **controllo sulla effettiva attuazione ed efficacia delle misure di presidio definite o richieste**.

Spinte dai regolatori, le organizzazioni aziendali stanno rapidamente **attivando il controllo di 2° livello sul Rischio Cyber**

► Chiari indirizzi dai Regolatori per la sicurezza e la cybersicurezza dei settori di business critici

Il Parlamento Europeo ha espresso chiaramente, attraverso specifici e mirati provvedimenti, la propria strategia finalizzata a rendere robusto e reattivo il sistema produttivo e finanziario dell'Europa a fronte di eventi avversi di cybersecurity.

E' stato recentemente aggiornato il Regolamento NIS2 (Reg. 2022/2555) in merito alle misure comuni di cybersicurezza e sono state attivate l'agenzia ENISA ed il Gruppo Europeo di Certificazione sulla Cybersecurity (ECCG), quest'ultimo incaricato di definire il framework di riferimento per la Certificazione di Cybersicurezza.

Al contempo, è entrato in vigore il nuovo Regolamento DORA (2022/2554 - Digital Operational Resilience Act) che a partire da gennaio 2025 obbligherà le imprese finanziarie e i rispettivi fornitori critici al rispetto di precisi requisiti di sicurezza informatica e resilienza.

Le organizzazioni aziendali rilevanti si sono attivate da tempo per presidiare la propria sicurezza e cybersicurezza e hanno ormai una storia di attivazione di sistemi coordinati di gestione delle minacce e degli incidenti ICT e di sicurezza informatica (es. SIEM/SOAR).

Ora la norma prevede un intervento più diffuso verso sicurezza e cybersicurezza, coinvolgendo anche le aziende di minori dimensioni ma non per questo meno critiche

Ma il vero problema è l'**applicazione effettiva ed efficace** delle tecnologie di protezione Cyber adottate, nonché la assicurazione sulla loro adeguatezza.

Riferimenti Normativi	Descrizione	Decorrenza	Principali impatti
Parlamento Europeo e Consiglio - 2019-881	Istituzione di ENISA e linee guida per la certificazione della cibersicurezza per le tecnologie ICT	28 Giugno 2021	Tutti i settori di business - ECCG (European Cybersecurity Certification Group) - Raccolta informativa incidenti - Standard di certificazione Cyber
Parlamento Europeo e Consiglio - 2022-2554	DORA Resilienza operativa digitale per il settore finanziario	17 Gennaio 2025	Intermediari finanziari
Banca d'Italia - Circolare 285 - 40° aggiornamento	Funzione dedicata di controllo di 2° livello sul Rischio Informatico e di Sicurezza, controllo sui fornitori terzi, controllo sui progetti ICT, Formazione	30 Giugno 2023	Intermediari finanziari
Parlamento Europeo e Consiglio - 2022-2555	NIS 2 Misure per un livello comune elevato di cibersicurezza nell'Unione	18 Ottobre 2024	Altri settori di business Essenziali, Importanti, Critici
Parlamento Europeo e Consiglio - 2022-2557	CER Resilienza dei soggetti critici	18 Ottobre 2024	Altri settori di business Critici
Parlamento Italiano legge n. 133/2019	Individuazione dei Soggetti del Perimetro di sicurezza cibernetica nazionale (art. 3 DPCM 131/2020)	immediata	Altri settori di business Critici
Parlamento Italiano legge n. 138/2024	Recepimento Direttiva 2022-2555 NIS2	Varie scadenze nel 2026	Altri settori di business Essenziali, Importanti, Critici

La verifica **analitica e indipendente** della **sussistenza delle misure di protezione Cyber** previste e il confronto con le **pratiche migliori** attuate in realtà similari aumentano il livello di sicurezza complessivo e forniscono una **rassicurazione** verso gli **Organi Aziendali e gli altri stakeholder** interessati

5

Ethical Standard in Artificial Intelligence

**ML&AI:
soluzioni
parzialmente
prevedibili**

La sempre maggiore diffusione delle nuove tecniche di elaborazione basate su **Machine Learning e Artificial Intelligence** unita alle **specifiche caratteristiche** di tali tecnologie portano a dover affrontare nuove problematiche particolarmente critiche.

A differenza delle tecniche tradizionali di elaborazione, in cui il comportamento del sistema **era rigorosamente previsto a priori** dal progetto del programmatore, i nuovi paradigmi di elaborazione basati sull'**apprendimento** producono **risultati** che sono solo **parzialmente prevedibili e certi**, in quanto basati sull'attendibilità degli esempi forniti al sistema, dall'accuratezza con cui è avvenuto l'addestramento.

Infatti, **attendibilità degli esempi e accuratezza dell'addestramento** sono grandezze difficilmente sistematizzabili e misurabili.

**Obbligo di
controllo sul
rispetto dei
Principi Etici**

Vista la rapida diffusione di tali tecnologie su **sistemi critici per la vita delle persone** (es.: valutazione di solvibilità di un creditore, guida autonoma di un'auto, scelta di un candidato), teorici dell'informatica, regolatori e legislatori hanno affrontato il tema dell'*Etica dell'Intelligenza Artificiale*, definendo i **principi comportamentali di base** per l'utilizzo di tali tecnologie informatiche.

Oltre a ciò, regolatori e legislatori prevedono specifiche attività di controllo sul rispetto di tali principi.

Anche per il **controllo** sulle soluzioni basate su **ML & AI** sono necessarie **competenze ed esperienze specifiche** sul tema

► Artificial Intelligence sotto controllo

La criticità dell' AI impone l'applicazione di stringenti regole etiche

La Commissione Europea già nel 2018 ha elaborato la propria strategia in merito all'AI e nel 2022 ha emanato una proposta di regolamento.

Altre istituzioni internazionali (es. EBA) hanno emanato linee guida effettive per assicurare un utilizzo adeguatamente gestito delle nuove tecnologie di analisi ed elaborazione.

Il Regolamento in approvazione prevede precise indicazioni sui principi etici a cui i sistemi di AI devono sottostare

Inoltre, il regolamento in approvazione prevede e identifica:

- Il perimetro di applicazione alle principali industry
- La definizione delle pratiche vietate
- L'identificazione dei sistemi AI ad alto rischio
- I requisiti per i sistemi AI
- Struttura della vigilanza e delle sanzioni
- Regole di convalida e test

In sostanza, ancora una volta viene rimarcata l'importanza del presidio di 2° livello da parte degli operatori del mercato sulle tecnologie dell'informazione.

E viene attribuito un ruolo di responsabilità agli Organi Aziendali in merito all'adeguata applicazione di tali tecnologie al business

ETHICS by design

Le applicazioni basate sull'AI devono essere concepite, progettate, realizzate e utilizzate aderendo a principi etici di rispetto nei confronti delle persone, di prevenzione dei danni, di equità e di trasparenza

Security

I rischi di sicurezza si realizzano secondo modalità non consuete. I tool di AI rischiano ad esempio di essere clonati nel loro funzionamento, sottoposti ad addestramenti fuorvianti, ingannati con falsi input, ecc.

Explainability & Interpretability

I sistemi di AI tendono a operare come black-box. Sono quindi necessarie tecniche di verifica che consentano di spiegare un certo risultato e le regole del loro funzionamento

Fairness & Avoidance of bias

Le AI si comportano per come sono state addestrate, cioè in base agli esempi ricevuti. L'addestramento deve quindi avvenire in maniera equa, senza discriminazioni e favori

Traceability & Auditability

Tutto il processo di sviluppo e addestramento deve essere tracciabile e verificabile, con adeguata documentazione. L'evoluzione dei modelli ML&AI deve essere monitorabile

Data Protection

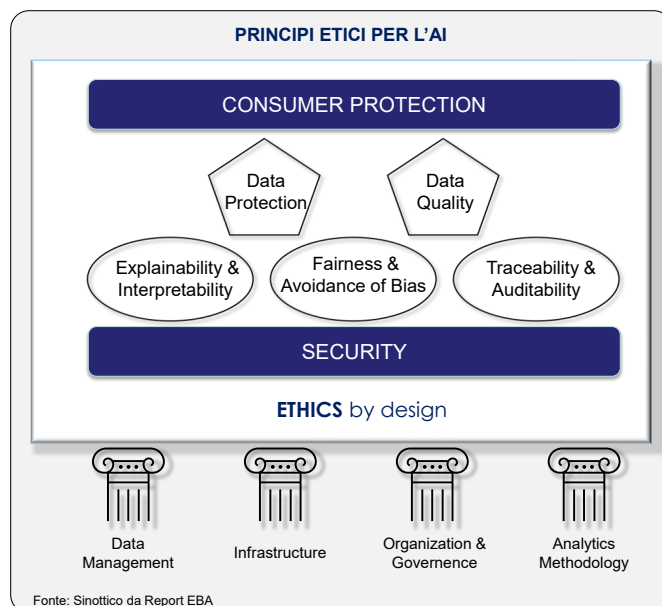
I dati, soprattutto quelli personali dei fruitori, devono essere protetti anche quando sono utilizzati per addestrare l'AI stessa, la quale deve assicurare la riservatezza

Data Quality

I risultati dell'applicazione dell'AI devono essere di qualità adeguata in modo da evitare risposte del sistema inadeguate o scorrette che possano fuorviare l'utente

Consumer Protection

La fiducia nell'AI si trasmette con il rispetto dei diritti dell'utilizzatore (es. consumatore) e nella salvaguardia dei suoi interessi



Le parole d'ordine dell'EU sono **"ECCELLENZA"** nell'implementazione e **"FIDUCIA"** da trasmettere ai cittadini e alle imprese riguardo al loro utilizzo. Sono quindi importanti il **CONTROLLO** e la **CERTIFICAZIONE** delle soluzioni AI.