

*ABI SUPERVISION, RISKS & PROFITABILITY 2024
IL RISCHIO DEI RISCHI: SIAMO FORMATI ABBASTANZA?*

*Nuovi rischi di conformità ed evoluzione delle
competenze della Compliance e degli strumenti di analisi
e controllo*

Francesco Martiniello
Chief Compliance & Anti-Financial Crime Officer
Illimity Bank S.p.A.

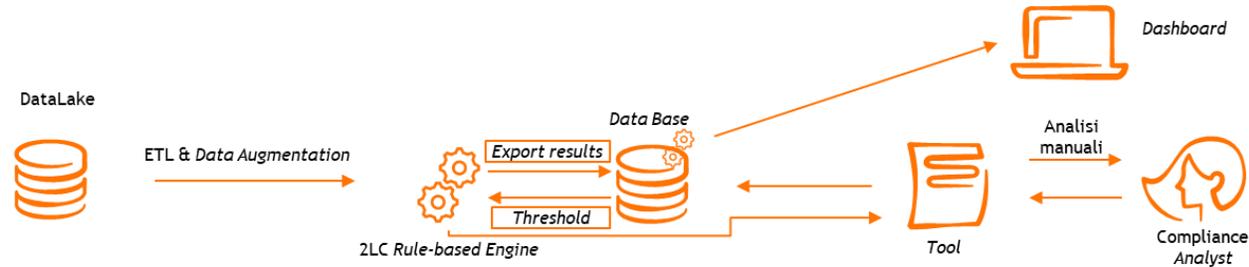
Milano, 8 marzo 2024

Sistema «C2L engine»

Nel biennio 2021-2022, è stata avviata una progettualità volta all'**automazione dei controlli** standardizzati su snodi di processo su cui insistono requisiti normativi al fine di rendere le attività di controllo di secondo livello:

- **efficienti**, attraverso verifiche massive (non più campionarie) sull'intera *customer base*, con risultati più rappresentativi e una minore frequenza di esecuzione;
- **data-driven**, contenendo il rischio di frammentazione delle fonti utilizzate per le verifiche;
- svolte per **step progressivi**, finalizzati a ricercare, senza l'intervento degli analisti, evidenze di anomalie o anche semplici 'indizi' delle stesse, la cui rilevanza (identificata al superamento di soglie predefinite di tolleranza) innesca la necessità di ulteriori analisi *human-based*.

L'attività di automazione ha portato alla realizzazione del motore dei controlli dedicato «C2L Engine»



Vantaggi derivanti dal nuovo paradigma di controllo



Creazione di una base dati unica e arricchita per l'esecuzione di controlli sulla maggior parte delle diverse aree di *business*



Efficientamento delle attività di controllo tramite logiche di automazione e regole prestabilite di valutazione dei risultati



Risparmio del tempo delle e risorse impiegate per i controlli *ex post*, a beneficio di un maggior presidio delle attività *ex ante*

Per il controllo **semi-automatico** avente come obiettivo la verifica che gli **incident ICT** che non sono stati segnalati al **Data Protection Officer** come **data breach** non abbiano effettivamente impattato dati personali, è stato definito un algoritmo che sulla base delle parole contenute nei **ticket** aperti dalle strutture segnalanti valuta la probabilità che l'evento segnalato abbia coinvolto dati personali e produce automaticamente un **ranking**. L'analista verifica quindi il contenuto dei singoli **ticket** presenti in tale **ranking** per accertare se gli **incident** segnalati hanno o meno coinvolto dati personali.

Esemplificazione: controllo antiusura

CONTROLLO TRADIZIONALE

Verifica **manuale** della corretta imputazione sugli applicativi antiusura dei tassi soglia definiti trimestralmente dal Ministero dell'Economia e delle Finanze.

CONTROLLO AUTOMATIZZATO

VS.

Verifica **automatica** della corretta imputazione negli applicativi dei tassi soglia usura di riferimento rispetto alla categoria di volta in volta rilevante per ciascun cliente che abbia ottenuto un finanziamento nel periodo di riferimento.

RISULTANZE DEL CONTROLLO

Visibilità dagli esiti dei singoli sottocontrolli che lo compongono, così da consentire una percezione immediata del collocamento delle eventuali anomalie.

INFORMAZIONI_CONTROLLO		DC	GC	FD	BILTY	
DESCRIZIONE	PERIODO	TOTALE	TOTALE	TOTALE	TOTALE	COMPLESSIVO
SOTTOCONTROLLO						
AUS_3_A	Clienti con finanziamenti (H2O) per i quali la soglia di usura censita a sistema non risulta in linea con quanto pubblicato da Banca d'Italia	2023-04-01 - 2023-06-30	0.0000%	0.0000%	0.0000%	0.0000%
AUS_3_B	Clienti con finanziamenti (PANDA) per i quali la soglia di usura censita a sistema non risulta in linea con quanto pubblicato da Banca d'Italia	2023-04-01 - 2023-06-30	0.0000%	0.0000%	0.0000%	0.0000%
AUS_3	Clienti con finanziamenti (PANDA) per i quali la soglia di usura censita a sistema non risulta in linea con quanto pubblicato da Banca d'Italia	2023-04-01 - 2023-06-30	0.0000%	0.0000%	0.0000%	0.0000%
AUS_3	AUS_3 - TOTALE KO	2023-04-01 - 2023-06-30	0	0	0	0
AUS_3	AUS_3 - PERIMETRO	2023-04-01 - 2023-06-30	84	245	24	1
AUS_3	AUS_3 - ESITO	2023-04-01 - 2023-06-30	NON SIGN	NON SIGN	NON SIGN	NON SIGN



CONTROLLO	PERIODO DI RIFERIMENTO	ESITO	CARENZE
AUS_3	2023-04-01 - 2023-06-30	NON SIGNIFICATIVO	0

ESITO FINALE DEL CONTROLLO

Derivante dalla combinazione degli esiti dei singoli sottocontrolli.

Cruscotto per esecuzione e gestione dei controlli di secondo livello

1

La barra del Menu contiene il pulsante per creare nuovi item/controlli, i 3 cataloghi principali ed un catalogo per gli oggetti archiviati.

Code	Description	Version	Lifecycle phase	Status	Sotto-catalogo	Modalità	Ambito
MAR_T_1_4Q2023	MAR_T_1_4Q2023	V1	Validazione - Completed	Live	Controllo tematico	Manuale	Market Abuse
PRU_25	PRU_25	V1	Compilazione - In Progress	Not Live	Controllo permanente	Manuale	Normativa Prudenziale
PRU_24	PRU_24	V1	Compilazione - In Progress	Not Live	Controllo permanente	Manuale	Normativa Prudenziale
PRU_23	PRU_23	V1	Validazione - Completed	Live	Controllo permanente	Manuale	Normativa Prudenziale
EX_PSD2_1Q2023_2	EX_PSD2_1Q2023_2	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Servizi di Pagamento
EX_PSD2_1Q2023_1	EX_PSD2_1Q2023_1	V2	Compilazione - In Progress	Live	Controllo ex-ante	Manuale	Servizi di Pagamento
EX_PSD2_1Q2023_1	EX_PSD2_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Servizi di Pagamento
EX_TSP_1Q2023_4	EX_TSP_1Q2023_4	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Trasparenza
EX_TSP_1Q2023_3	EX_TSP_1Q2023_3	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Trasparenza
EX_TSP_1Q2023_2	EX_TSP_1Q2023_2	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Trasparenza
EX_ASS_1Q2023_1	EX_ASS_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Distribuzione Assicurativa
EX_TSP_1Q2023_1	EX_TSP_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Trasparenza
EX_PRU_1Q2023_1	EX_PRU_1Q2023_1	V1	Compilazione - In Progress	Live	Controllo ex-ante	Manuale	Normativa Prudenziale
EX_AUS_1Q2023_1	EX_AUS_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Antiusura
EX_PVY_1Q2023_1	EX_PVY_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	Privacy
EX_MIF_1Q2023_2	EX_MIF_1Q2023_2	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	MIFID
EX_MAR_1Q2023_1	EX_MAR_1Q2023_1	V1	Validazione - Completed	Live	Controllo ex-ante	Manuale	EMIR

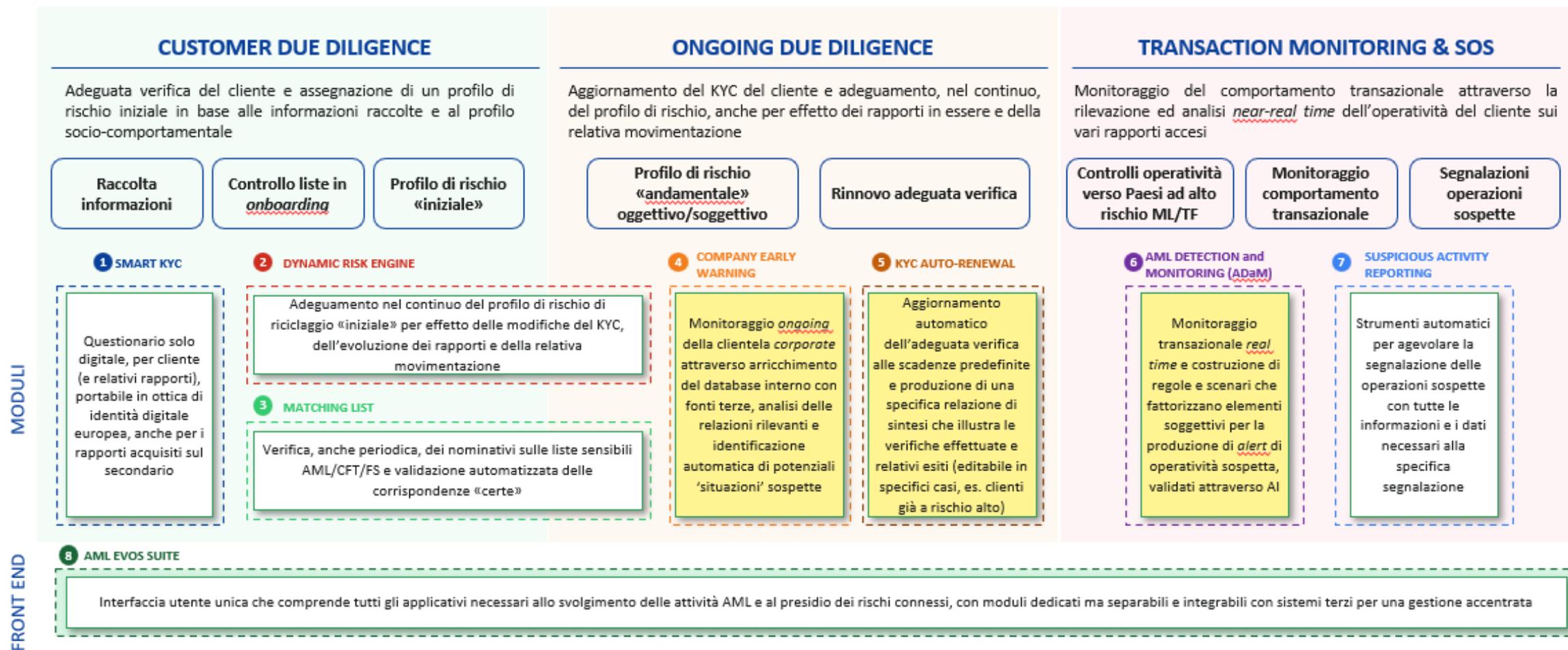
2

In alto a destra, viene mostrato lo user ed il ruolo con cui si sta navigando sul Gestionale.

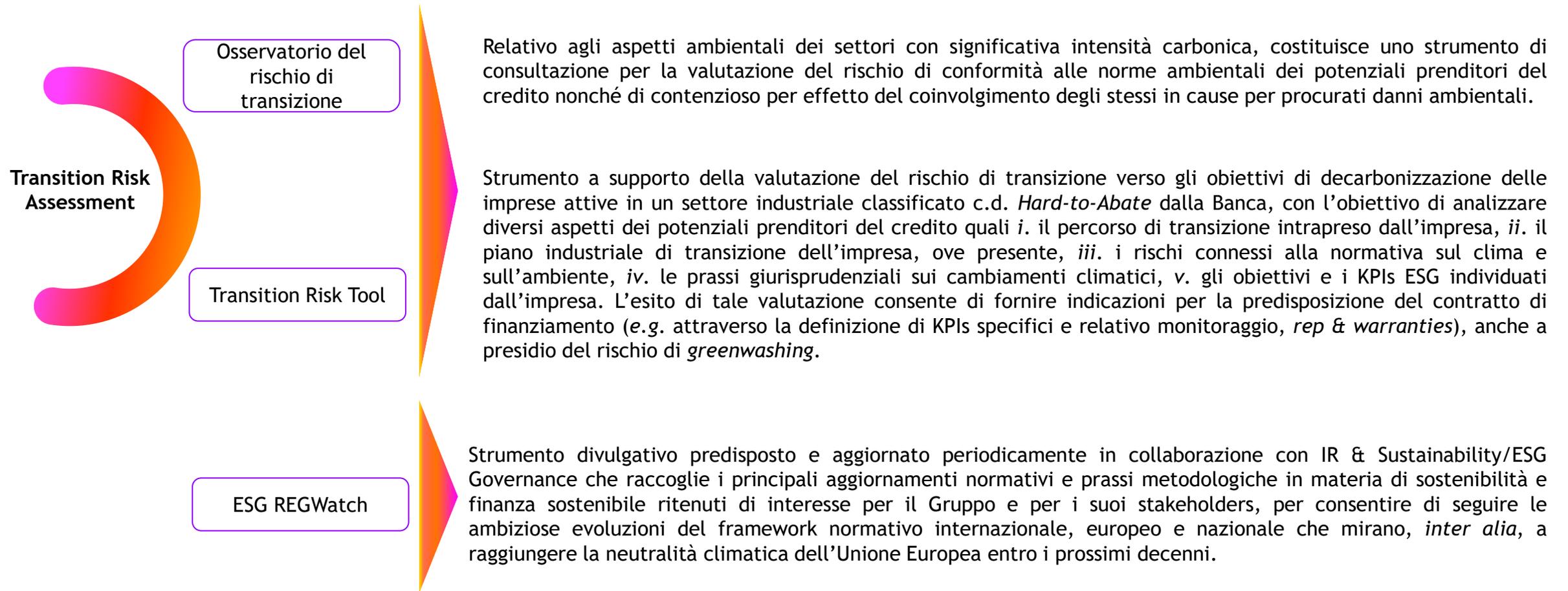
3

Riquadro che comprende l'elenco degli *item*/controlli che sono contenuti nel catalogo selezionato.

AML Evolving Suite - «AML EvoS»



ESG Compliance



Altre attività di ESG Compliance sono la valutazione di conformità o di corretta classificazione di prodotti rilevanti (e.g. *Green Loan*, *Sustainability-linked Loan*), il *compliance assessment* della normativa ESG, la formazione dedicata e il processo (in via di definizione) creditizio rafforzato per la valutazione del rischio di transizione dei prenditori operanti nei settori *Hard-to-Abate*, volto all'introduzione dei necessari meccanismi contrattuali a presidio del rischio di *greenwashing*.

ICT & Security Compliance

Nell'ambito delle attività di adeguamento al 40° Aggiornamento della Circolare 285 di Banca d'Italia, sono stati ripartiti i compiti di monitoraggio e controllo dei rischi ICT e di Sicurezza tra Risk Management e Compliance in base ai rispettivi ambiti di competenza. In particolare, la Compliance ha il compito di:

-  Effettuare controlli di secondo livello a presidio dei rischi ICT e di sicurezza, con inclusione di verifiche sui soggetti terzi rilevanti a tali fini (*i.e. outsourcer* e fornitori ICT, anche quando nominati responsabili esterni dei trattamenti privacy)
-  Valutare *ex ante* la conformità normativa in chiave di *compliance by design* dei progetti di acquisizione e sviluppo/modifica sostanziale/*change* dei sistemi ICT della Banca e del Gruppo o di progetti aventi un potenziale impatto su tali sistemi
-  Partecipare, unitamente alle strutture della Competence Line Digital e alla Competence Line Risk, al Comitato di Gestione dei Progetti e dei Cambiamenti ICT, con possibilità di richiedere *escalation* agli Organi
-  Supportare le strutture responsabili nelle valutazioni preliminari di rischio e nel monitoraggio degli accordi di esternalizzazione ICT della Banca
-  Verificare la capacità del sistema informativo di registrare, conservare e rappresentare correttamente i fatti di gestione e gli eventi rilevanti per le finalità previste dalla normativa esterna e interna
-  Verificare la corretta definizione e trasmissione di flussi informativi adeguati e tempestivi su qualsiasi attività o evento che influenzi in modo rilevante il profilo di rischio della Banca, ivi inclusi gli incidenti operativi o di sicurezza significativi nonché qualsiasi modifica sostanziale ai sistemi e ai processi ICT
-  Verificare *ex ante* la conformità della normativa interna in ambito ICT & Security in occasione di redazione e aggiornamento della stessa, altresì concorrendo alla definizione della policy di sicurezza dell'informazione
-  Fornire supporto alla Funzione Antiriciclaggio nell'effettuazione e documentazione dei *test* per la valutazione dei rischi di frode, furto d'identità e altri rischi ICT e di sicurezza afferenti ai processi antiriciclaggio rilevanti