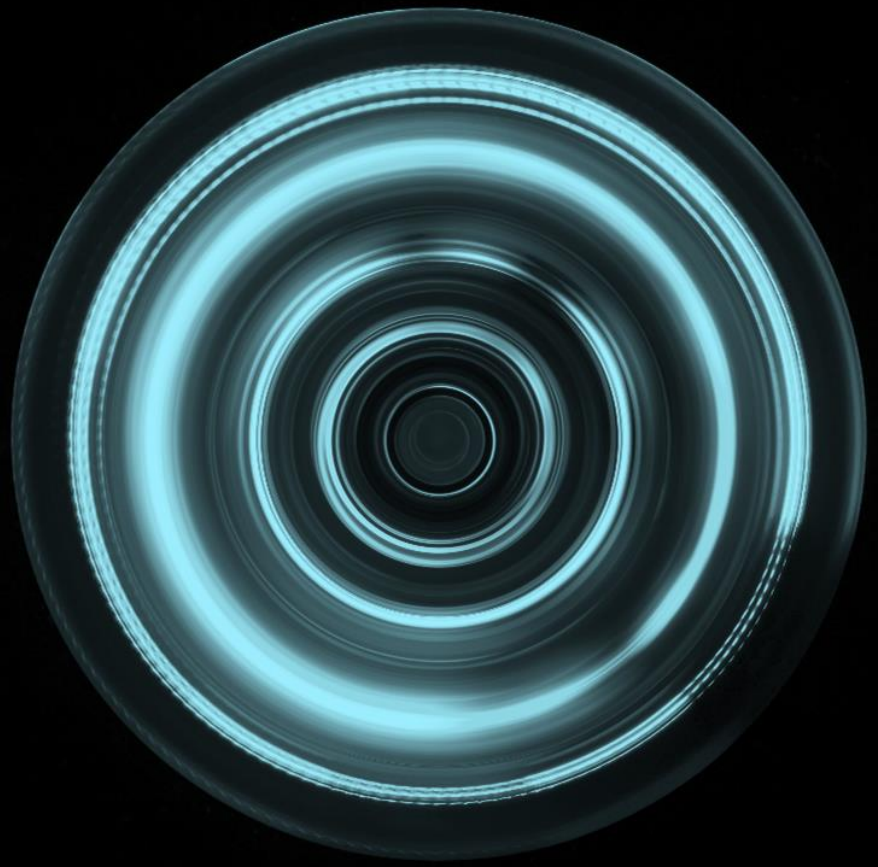
Deloitte.

ASSOCIAZIONE COMPLIANCE OFFICER RESPONSABILI ANTIRICICLAGGIO



Next Generation AML: nuove sfide e trend evolutivi in ambito Antiriciclaggio e Financial Crime

Secondo Webinar

17 Novembre 2021

Relatori:

Gianfranco Tessitore | Domenico Farina

gtessitore@deloitte.it dofarina@deloitte.it

Agenda

Dettaglio dei contenuti previsti

Di cosa parleremo..

Primo Webinar

1 Contesto e nuovi trend di tipo normativo e di tipo evolutivo

- **Pressione regolamentare** e **convergenza** della **regolamentazione** e della vigilanza a livello comunitario
- **Nuove minacce** e nuove fattispecie di rischio con focus su rischi derivanti dall'emergenza Covid-19
- **Nuove opportunità** derivanti dai processi di digitalizzazione dell'offerta dei servizi finanziari e dall'evoluzione tecnologica
- Le nuove opportunità derivanti dai **processi di digitalizzazione dell'offerta dei servizi finanziari** e dall'evoluzione tecnologica (introduzione)

2 La centralità dell'approccio basato sul rischio: dall'autovalutazione dei rischi alla profilatura del cliente

- **La centralità dell'Autovalutazione**: requisiti normativi, best practices di sistema e linee evolutive
- **Nuovi trend** e soluzioni a supporto della **profilatura** della clientela e nuovi approcci alla corretta **graduazione degli obblighi di adeguata verifica** sulla base dei «rischi reali»
- Evoluzione dei **modelli di training** e awareness secondo logiche risk based

Secondo Webinar

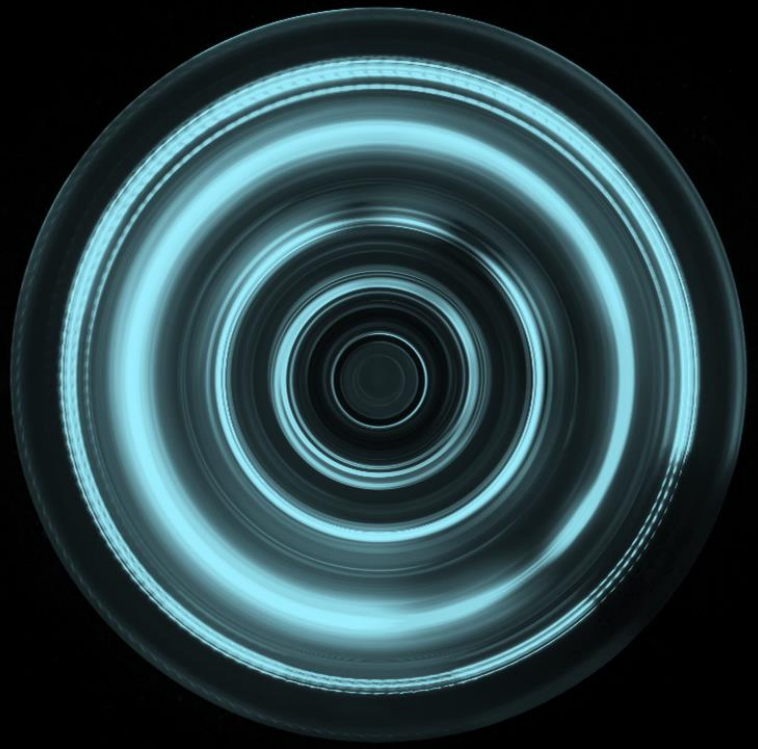
3 La rivoluzione digitale e gli impatti sul framework AML

- Nuovi approcci al **riconoscimento della clientela**, digital onboarding e opportunità derivanti dal Decreto Semplificazioni e dalla rivoluzione delle identità digitali SPID
- **Evoluzione tecnologica** a supporto dei processi AML e delle attività di controllo
- **La sfida dell'efficienza e dell'efficacia**
- Focus su tecniche di **AI/ML** applicate ai processi AML: **best practices & case study**

4 Verso un approccio olistico alla gestione dei «Financial Crime»

- Come approcciare in **modo sinergico** le diverse tipologie di «Financial Crime», Money Laundering, Fraud, Cyber crime, Corruption, etc.: framework organizzativi e soluzioni operative integrate

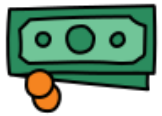
AGENDA



Nuovi approcci al riconoscimento della clientela, digital onboarding e opportunità derivanti dal Decreto Semplificazioni e dalla rivoluzione delle identità digitali SPID

Le nuove opportunità derivanti dall'evoluzione tecnologica

I processi di onboarding digitale della clientela sono accompagnati da una pluralità di requirements normativi

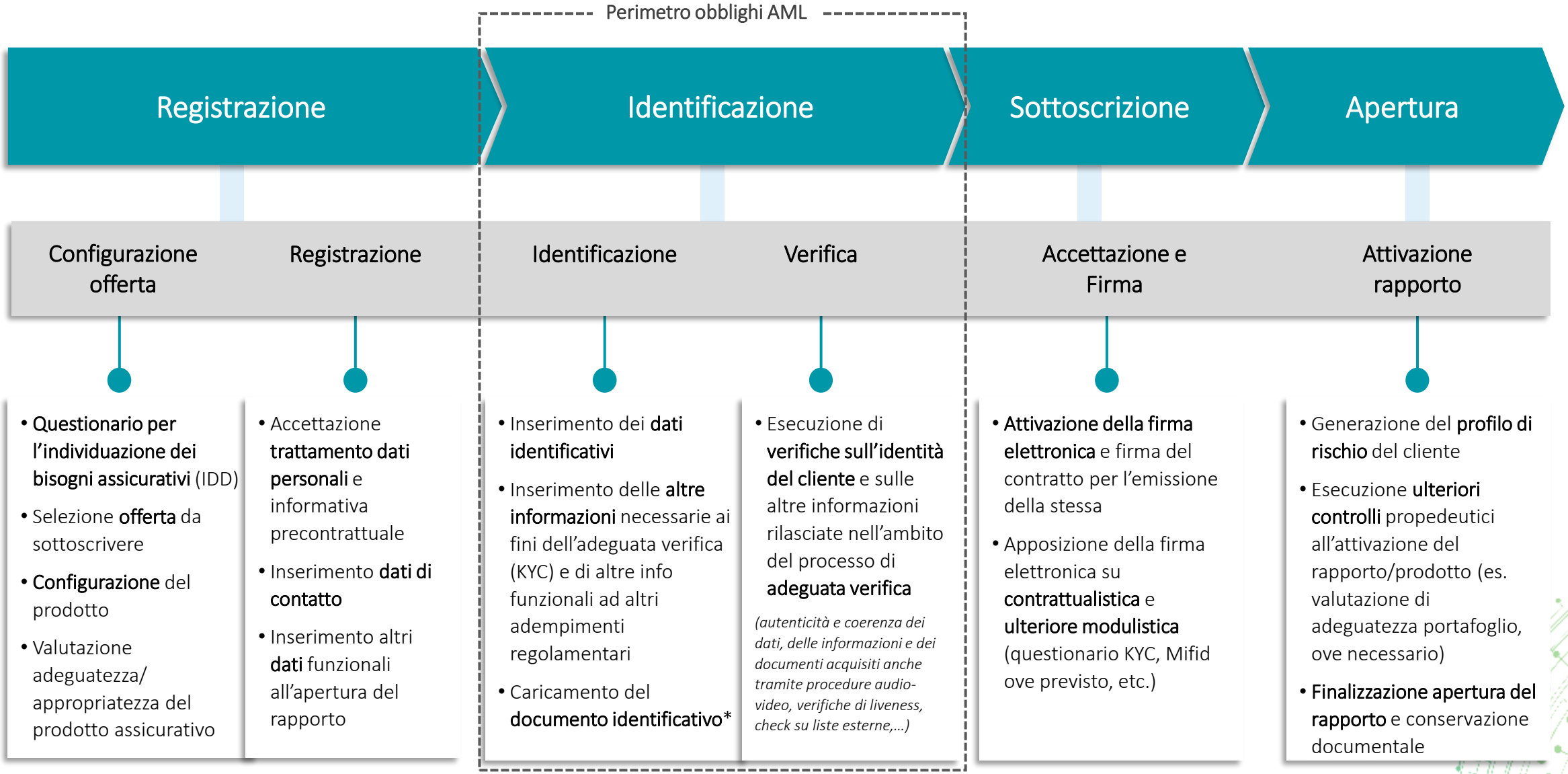
Dominio	Principali norme	Abstract
 AML	▪ IV e V Direttiva AML ▪ Decreto Antiriciclaggio ▪ Lettere al Mercato IVASS e Reg. IVASS n° 44/2019 ▪ Linee guida ESAs soluzioni innovative nei processi di adeguata verifica	Prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo
 Identità digitali e firme elettroniche	▪ Codice dell'amministrazione digitale ▪ Linee Guida Agid ▪ Misure urgenti per la semplificazione e l'innovazione digitale	Disciplina delle identità digitali e della firma elettronica
 Data Protection	▪ GDPR ▪ Codice Privacy ▪ Linee guida e Provvedimenti Autorità Garante (es. Provvedimento biometria)	Protezione delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati
 Trasparenza	▪ Codice delle assicurazioni private ▪ Regolamento IVASS n° 41 del 2 agosto 2018	Correttezza delle relazioni tra intermediari e clienti e obblighi di informativa, pubblicità e realizzazione dei prodotti assicurativi

Ulteriori normative devono essere considerate in relazione al cliente servito / prodotto offerto / area geografica interessata (ad es. normativa in ambito IDD, MiFID, FATCA / CRS)

Le nuove opportunità derivanti dall'evoluzione tecnologica

ESEMPLIFICATIVO

Il processo di onboarding digitale e i presidi minimi da garantire



*Alcune novità introdotte dal cd. «Decreto semplificazioni»

Le nuove opportunità derivanti dall'evoluzione tecnologica

Un focus sul processo di identificazione

La **normativa Antiriciclaggio** prevede diverse modalità per assolvere agli obblighi di **identificazione della clientela** (cliente/esecutore)

Gli intermediari pongono particolare attenzione all'operatività a distanza, in considerazione **dell'assenza di un contatto diretto** con il cliente e tengono conto del rischio di **frodi connesse al furto di identità**

L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente/esecutore, mediante

Valida anche per identificazione de visu

1 IDENTITA' DIGITALE

Possesso da parte del cliente/esecutore di una identità digitale di **livello significativo*** o di un certificato per la generazione di firma digitale

2 PROCEDURA DI VIDEO-IDENTIFICAZIONE

Identificazione da remoto effettuata mediante una specifica procedura di video-identificazione (disciplinata dall'art. 39 del Reg. IVASS 44 del 12 feb. 2019)

3 ALTRE SOLUZIONI E TECNOLOGIE INNOVATIVE

Utilizzo di **procedure flessibili** che prevedono, oltre **all'acquisizione dei dati identificativi del cliente** (es. attraverso i sistemi di comunicazione informatica), **meccanismi di "verifica ulteriore"** (anche in ottica risk-based)

IN VIA GENERALE, GLI INTERMEDIARI

- acquisiscono i dati identificativi e ne effettuano il riscontro su una copia – ottenuta tramite fax, posta, in formato elettronico o con modalità analoghe – di un valido documento di identità
- effettuano riscontri ulteriori rispetto a quelli previsti nel casi di identificazione de visu secondo un approccio risk based
- formalizzano le scelte compiute nell'ambito del documento di Policy Antiriciclaggio

Novità introdotta dal Decreto Semplificazioni

Le nuove opportunità derivanti dall'evoluzione tecnologica

Classificazione delle modalità di identificazione in uso

		MAIN USE CASES	DESCRIZIONE	PROs	CONs
Diretti	1	Video identificazione senza operatore	**Video identificazione effettuata direttamente da una macchina** in cui il cliente esegue alcune azioni (per escludere la presenza di un robot) e **fornisce il proprio documento di identità** (OCR) Verifica corrispondenza tramite **strumenti di riconoscimento facciale** tra immagine video e foto del documento	▪ Esperienza digitale avanzata ▪ 24X7 ▪ Pieno utilizzo di soluzioni tecnologiche avanzate (OCR + AI)	▪ Non adatto a clienti con scarsa attitudine al digitale ▪ Non in tempo reale*
	2	Video identificazione con operatore	**Video identificazione svolta tramite un operatore** che raccoglie i dati personali e la foto del documento di identità del cliente e svolge verifiche per escludere la presenza di un robot e per confermare l'identità del cliente in conformità ai requisiti della procedura di video identificazione disciplinati da Banca d'Italia	▪ Processo in tempo reale, al netto di verifiche e riscontri successivi ▪ Supporto costante al cliente	▪ Disponibile solo in determinati momenti (non 24X7) ▪ Esperienza digitale basica
Indiretti	3	Certificazione da fonte terza attendibile	È il primo metodo di identificazione a distanza utilizzato e **consiste, ad esempio, nel far disporre al cliente un bonifico (SCT) attraverso un intermediario bancario e finanziario** con sede in Italia o in un paese comunitario al fine di **verificare che il cliente esiste ed è già stato identificato da un intermediario**	▪ Bassi costi di implementazione per gli intermediari	▪ Bassa esperienza digitale ▪ Tempo necessario per l'allineamento SCT
	4	Identità digitale	**Consentire al cliente di utilizzare un'identità digitale** autogestita o gestita da una terza parte (ecosistemi privati o pubblici, come SPID) per essere identificati. Con questo metodo **l'identificazione ai fini dell'adeguata verifica del cliente viene acquisita da un ecosistema esterno tramite un soggetto che svolge il ruolo di Identity Provider (IdP)**	▪ Esperienza digitale avanzata ▪ Disponibilità 24X7 ▪ Ogni fase dell'identificazione è svolta dall'intermediario ▪ Time to serve ▪ Alto e massimo livello di sicurezza	▪ Maturità degli ecosistemi non ancora elevata ▪ Costi di implementazione per gli intermediari

In fase di diffusione a seguito del Decreto Semplificazioni

* É generalmente richiesto un supporto da parte del Back Office dell'intermediario

Le nuove opportunità derivanti dall'evoluzione tecnologica

Le novità introdotte dal Decreto Semplificazioni

Le misure introdotte dal Decreto Semplificazioni vanno nella direzione di **semplificare l'accesso ai servizi finanziari** con rilevanti benefici in termini di speditezza e sicurezza delle procedure di onboarding online della clientela da parte degli operatori bancari e degli intermediari

Novità in materia di identificazione della clientela

Revisione della disciplina in materia di identificazione della clientela (secondo la normativa Antiriciclaggio) con un maggiore incentivo **all'utilizzo di SPID**

Novità in materia di firma dei documenti

Estensione e semplificazione delle **modalità di identificazione** della clientela funzionali al rilascio della c.d. **firma elettronica avanzata** che potrà avvenire mediante le seguenti modalità:

1. **Identificazione tramite credenziali di strong authentication**
   Solo se l'utente è già stato oggetto di precedente identificazione ed è munito di credenziali di strong authentication
2. **Identificazione tramite SPID**
   Possibilità di essere identificati per l'ottenimento della firma elettronica avanzata mediante le credenziali SPID di livello 2 (basate su due fattori)
3. **Identificazione tramite CIE e sistemi di identificazione notificati**
   Identificazione attraverso identità digitali eventualmente rilasciate in altri Stati membri dell'Unione Europea o a mezzo di una Carta di identità elettronica

Le nuove opportunità derivanti dall'evoluzione tecnologica

Decreto Semplificazioni e le novità in materia di identificazione a distanza della clientela

PRIMA

D. LGS. 231/2007 PRE-MODIFICHE DECRETO SEMPLIFICAZIONI

Art. 19 – Modalità adempimento obblighi di adeguata verifica

[…] L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente: 1) […]

2) Per clienti ***in possesso di un'identità digitale****, di* ***livello massimo*** *di sicurezza, (…) o di un certificato per la generazione di firma digitale*

DOPO

DECRETO SEMPLIFICAZIONI - MISURE PER LA SEMPLIFICAZIONE E LA DIFFUSIONE DELLA FIRMA ELETTRONICA AVANZATA E DELL'IDENTITÀ DIGITALE

[…] si può procedere alla verifica dell'identità dell'utente anche tramite uno dei seguenti processi: […] processi di identificazione elettronica e di autenticazione informatica, a due fattori, basati su credenziali già rilasciate all'utente nell'ambito del ***Sistema Pubblico per la gestione dell'Identità Digitale*** *[…] processi di identificazione elettronica e di autenticazione informatica, basati su* ***credenziali di livello almeno "significativo"***

Criticità

- ***Scarsa diffusione di SPID con livello di sicurezza massimo*** *dato che la quasi totalità delle SPID rilasciate in Italia hanno, ad oggi, un livello di sicurezza significativo o non elevato*
- ***Controversa formulazione normativa*** *poiché la firma digitale è definita solo in Italia come particolare tipologia di firma elettronica qualificata ed anche perché essa non rientra nei sistemi di identificazione digitale notificati dal Regolamento eIDAS, bensì è autonomamente disciplinata dal medesimo regolamento quale servizio fiduciario*

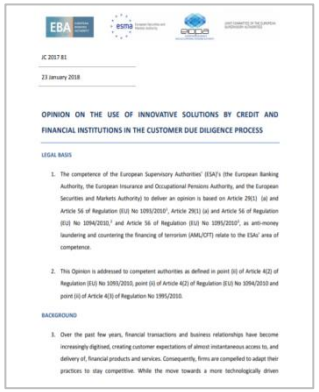
Opportunità

- *Possibilità di identificare il cliente utilizzando le* ***numerose identità digitali SPID già diffuse sul territorio (di livello significativo)*** *o certificati qualificati associati alle firme elettroniche con cui possono essere sottoscritti i contratti*
- *Possibilità di far leva su una* ***modalità di riconoscimento sicura e generalmente accettata***

È stato inoltre soppresso l'obbligo di acquisizione di un documento identificativo del cliente, così evitando la trasmissione online di copia dei documenti e lasciando l'intermediario libero di effettuare il riscontro dell'identità del cliente tramite fonti affidabili ed indipendenti

Le nuove opportunità derivanti dall'evoluzione tecnologica

Le altre modalità di identificazione «a distanza»: Le Linee Guida ESAs sull'utilizzo di soluzioni innovative nel processo di Adeguata Verifica



JC 2017 81

23 January 2018

OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS

LEGAL BASIS

1. The competence of the European Supervisory Authorities' (ESA's) (the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority) to deliver an opinion is based on Article 29(1) (a) and Article 56 of Regulation (EU) No 1093/2010[1], Article 29(1) (a) and Article 56 of Regulation (EU) No 1094/2010,[2] and Article 56 of Regulation (EU) No 1095/2010[3], as anti-money laundering and countering the financing of terrorism (AML/CFT) relate to the ESAs' area of competence.

2. This Opinion is addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010, point (ii) of Article 4(2) of Regulation (EU) No 1094/2010 and point (ii) of Article 4(3) of Regulation No 1095/2010.

BACKGROUND

3. Over the past few years, financial transactions and business relationships have become increasingly digitised, creating customer expectations of almost instantaneous access to, and delivery of, financial products and services. Consequently, firms are compelled to adapt their practices to stay competitive. While the move towards a more technologically driven

Le Linee Guida pubblicate dall'ESAs forniscono importanti indicazioni circa le valutazioni che gli intermediari dovrebbero compiere preventivamente **all'utilizzo di soluzioni tecnologiche innovative** nel processo di adeguata verifica della clientela

1 MECCASNISMI DI SUPERVISIONE E CONTROLLO

- Conduzione analisi preventiva
- Adeguati accordi con i provider
- Meccanismi di monitoraggio continuo della soluzione
- Meccanismi di conservazione dei dati
- Presidi in materia di protezione dei dati personali
- Controlli volti a garantire il rispetto dei requisiti in materia IT & Data Security
- Formazione del personale coinvolto
- Piani di continuità operativa

2 QUALITÀ E ADEGUATEZZA DELLE MISURE DI ADEGUATA VERIFICA

- Controlli su adeguato e corretto espletamento delle Misure di AV
- Meccanismi volti a garantire continuo updating dei dati e informazioni
- Integrazione della soluzione con workflow e sistemi di legacy
- soluzioni che abilitino la detection di transazioni potenzialmente sospette o inusuali

3 AFFIDABILITÀ DELLE MISURE DI ADEGUATA VERIFICA

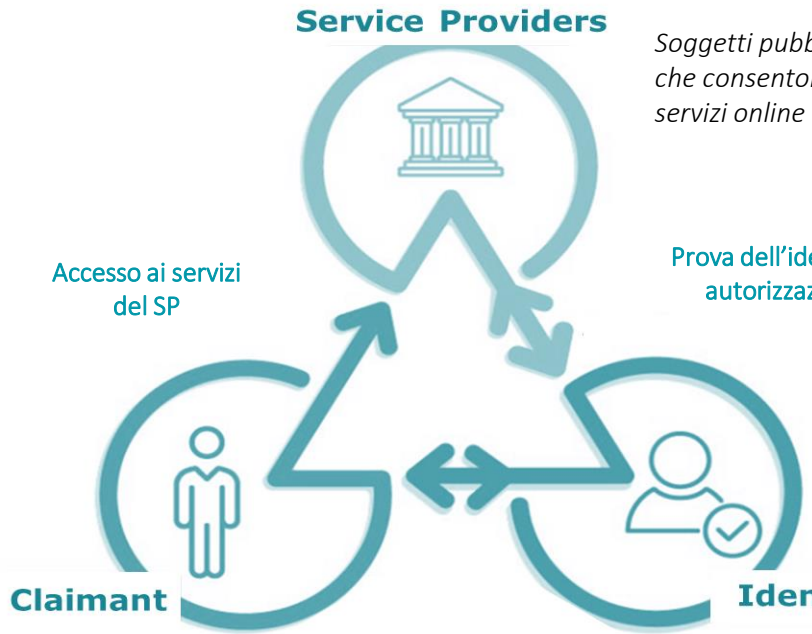
- Presidi volti a evitare il rischio di manomissione dell'immagine del cliente durante la trasmissione
- Presidi volti a evitare il rischio di alterazione/contraffazione/riciclo dei documenti di identità e di identificare le discrepanze di identità
- Adozione di sistemi volti a valutare la qualità degli output e degli alert generati dalla soluzione

4 RISCHI CONNESSI A CANALI DISTRIBUTIVI E AREA GEOGRAFICA

- Presidi volti a evitare l'uso fraudolento dei dati
- Presidi volti ad evitare rischi di coercizione
- Sistemi di rilevazione della posizione del cliente
- Meccanismi volti a valutare i motivi per cui i clienti stanno utilizzando i servizi di un intermediario da altre giurisdizioni

Le nuove opportunità derivanti dall'evoluzione tecnologica

Il sistema pubblico di identità digitale (SPID)



*Soggetti pubblici (9.081) e privati (**59**) che consentono l'accesso ai propri servizi online tramite SPID*

Persone fisiche e giuridiche che possiedono un'identità SPID per l'accesso ai servizi pubblici e privati

*Gestori di identità digitali **(9)** che rilasciano identità digitali con 3 livelli di garanzia*

Sicurezza	Descrizione
Basso	• Permette di accedere ai servizi on line attraverso nome utente e una password scelti dall'utente
Significativo	• Permette di accedere ai servizi on line attraverso nome utente e una password scelti dall'utente; la generazione di un codice temporaneo di accesso (one time password) o l'uso di un'APP, fruibile attraverso un dispositivo (es. smartphone)
Elevato	• Oltre le modalità di accesso ai servizi previsti per i livelli di sicurezza 1) e 2), richiede l'utilizzo di ulteriori soluzioni di sicurezza e dispositivi fisici (es. smart card) erogati dal gestore dell'identità

26.269.008
Identità erogate al 7 novembre 2021

143.872.687
di accessi in tutto il 2020

58.805.432
di accessi nel solo mese di ottobre 2021

Le nuove opportunità derivanti dall'evoluzione tecnologica

Implementazione di SPID nell'ambito di un processo di «credito al consumo»

Intermediario come Service Provider

È l'intermediario a ricoprire il ruolo di Service Provider, vale a dire di soggetto che consente l'accesso ai propri servizi online tramite SPID

Necessario attivare una procedura amministrativa per la sottoscrizione con Agid della Convenzione SPID

Necessario attivare una procedura tecnica secondo le Regole Tecniche di Agid per implementare il sistema SPID utlizzando lo standard SAML2 e ricevere il metadata per la configurazione dei propri servizi presso gli Identity Provider

Possibilità di rilasciare tramite SPID la firma elettronica avanzata per la sottoscrizione dei contratti coi clienti o di utilizzare SPID per la sottoscrizione degli stessi

VS

Certification Authority come Service Provider

È la Certification Authority a ricoprire il ruolo di Service Provider, vale a dire di soggetto che consente l'accesso ai propri servizi online tramite SPID tra cui il rilascio delle firme elettroniche qualificate e dei relativi certificati

L'intermediario indirizza il cliente sul portale della CA e in quel momento effettua l'accesso tramite SPID per accedere ai suoi servizi

La CA, al termine delle proprie attività di verifica, rilascia la firma elettronica qualificata e il relativo certificato

Il certificato di firma elettronica qualificata viene rilasciato dalla CA viene utilizzato dall'intermediario per assolvere gli obblighi di adeguata verifica AML

FOCUS ON NEXT SLIDES

Le nuove opportunità derivanti dall'evoluzione tecnologica

Implementazione di SPID nell'ambito di un processo di «credito al consumo»: le analisi condotte

Autovalutazione AML

Identificazione rischio inerente

- Operatività
- Canali distributivi
- Clientela
- Rischiosità prodotti/servizi
- Rischiosità Area Geografica

Analisi delle vulnerabilità

- Processi e strategie
- Policy e procedure
- Reporting
- Organizzazione e personale
- Controlli e metodologie
- Sistemi informativi

Rischio inerente	Liv. Vulnerabilità
Basso	Non significativo

Rischio residuo
Non significativo

Framework di analisi


EBA esma EIOPA

JC 2017 81

23 January 2018

OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS

LEGAL BASIS

1. The competence of the European Supervisory Authorities' (ESAs') (the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority) to deliver an opinion is based on Article 29(1) (a) and Article 56 of Regulation (EU) No 1093/2010[1], Article 29(1) (a) and Article 56 of Regulation (EU) No 1094/2010,[2] and Article 56 of Regulation (EU) No 1095/2010[3], as anti-money laundering and countering the financing of terrorism (AML/CFT) relate to the ESAs' area of competence.

2. This Opinion is addressed to competent authorities as defined in point (ii) of Article 4(2) of Regulation (EU) No 1093/2010, point (ii) of Article 4(2) of Regulation (EU) No 1094/2010 and point (ii) of Article 4(3) of Regulation No 1095/2010.

BACKGROUND

3. Over the past few years, financial transactions and business relationships have become increasingly digitised, creating customer expectations of almost instantaneous access to, and delivery of, financial products and services. Consequently, firms are compelled to adapt their practices to stay competitive. While the move towards a more technologically driven

1. MECCANISMI DI SUPERVISIONE E CONTROLLO
2. QUALITÀ E ADEGUATEZZA DELLE MISURE DI ADEGUATA VERIFICA
3. AFFIDABILITÀ DELLE MISURE DI ADEGUATA VERIFICA
4. RISCHI CONNESSI A CANALI DISTRIBUTIVI E AREA GEOGRAFICA

Esiti delle analisi

Valutazione dell'adeguatezza e robustezza dei presidi in essere

Identificazione dei presidi ulteriori da adottare per rafforzare il processo, quali, a titolo esemplificativo:

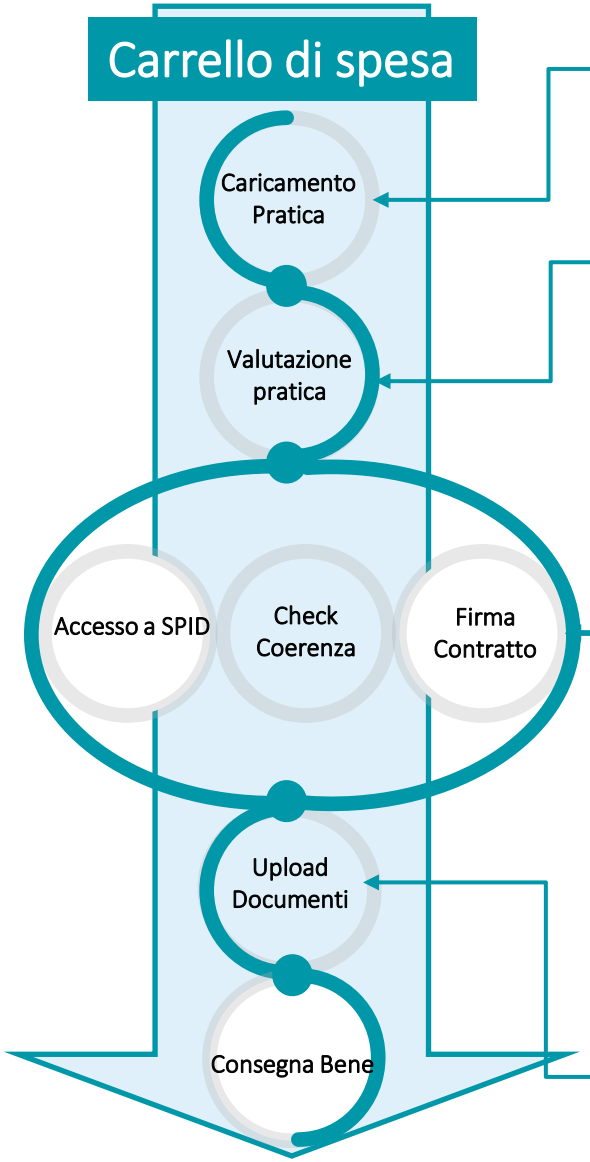
- Rafforzamento presidi contrattuali e monitoraggio outsourcer con SLA specifici
- Raccolta dati ulteriori dal sistema SPID (interrogazione in modalità «Registrazione»)
- Mantenimento controlli Scipafi
- Reperforming controlli liste in caso di sovrascrittura dati esistenti con quelli raccolti da SPID

Identificazione della soluzione target per l'implementazione del sistema SPID

Il framework di analisi è composto da una serie di requisiti e di ambiti di intervento attivati prendendo in considerazione il framework normativo di riferimento, con particolare attenzione alle Linee Guida ESAs. Sono stati identificati 16 requisiti sui quali è stata impostata una valutazione di conformità e di esposizione ai rischi, che tiene conto anche della soluzione di integrazione ipotizzata e conseguentemente individuati dei suggerimenti che possano mitigare il rischio potenziale e aumentare l'adeguatezza dei presidi.

Le nuove opportunità derivanti dall'evoluzione tecnologica

Implementazione di SPID nell'ambito di un processo di «credito al consumo»: Processo e-commerce con SPID



Caricamento Pratica

Il caricamento della pratica avrà 2 novità rispetto al processo AS IS:

1. Un' Informativa Privacy ad hoc
2. Esenzione dal fornire degli estremi del documento di identità

Valutazione Pratica

- I controlli previsti per la richiesta di finanziamento saranno i medesimi di oggi ma saranno effettuati senza gli estremi del documento di identità:
  - istruttoria della pratica e valutazione del merito creditizio
  - Screening liste con profilatura AML tramite apposito tool e controlli antifrode e di prevenzione del furto di identità

Accesso a SPID

- Sarà messa a disposizione del cliente una pagina per la scelta della modalità di identificazione. Potrà procedere con il processo SPID solo chi sia già in possesso dell'identità digitale, gli altri clienti verranno indirizzati sul processo AS IS con verifica dell'identità tramite allineamento SDD.
- Una volta scelta la modalità SPID il cliente sarà reindirizzato sulla pagina di scelta del proprio Identity Provider gestita da InfoCert

Check coerenza

- I dati restituiti dall'interrogazione al sistema SPID e restituiti dalla CA sono:

  Dati anagrafici: Nome, Cognome, Luogo e data di nascita, Provincia, Sesso, CF

  Dati Extra Anagrafici: Estremi del documento di identità, cellulare, email, domicilio fisico, data scadenza identità digitale, PEC, identificativo digitale.
- Su cui vengono effettuati i seguenti controlli:
  1. Check coerenza CF se KO ci sarà un reindirizzamento su processo SDD (a carico della CA)
  2. Check coerenza Dati Anagrafici se KO ci sarà un reindirizzamento su processo SDD (a carico di dell'intermediario)
  3. Check coerenza Dati Extra Anagrafici se KO i dati non coerenti saranno sovrascritti e verranno effettuati nuovamente i controlli di Valutazione pratica (a carico dell'intermediario)

Firma Contratto

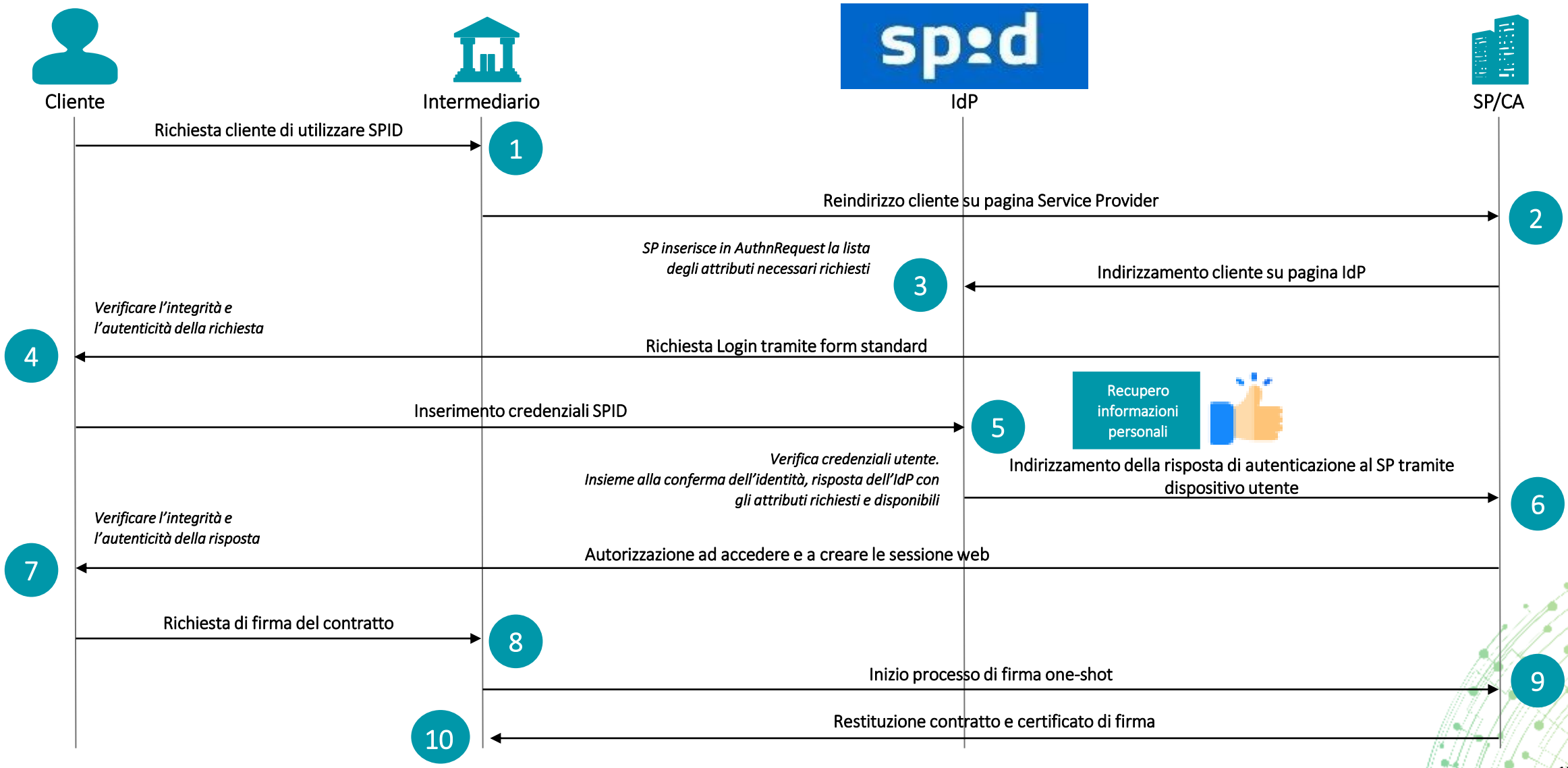
- Emissione certificato di firma e sottoscrizione del contratto

Upload documenti

- Non viene richiesto l'upload del documento di identità al cliente in caso di processo SPID
- Nei casi in cui il cliente sarà reindirizzato su processo SDD sarà richiesto l'upload del documento di identità per i controlli previsti
- Viene richiesto l'Upload dei documenti TS e documenti di reddito solamente per le pratiche di importo superiore a una determinata soglia parametrizzata

Le nuove opportunità derivanti dall'evoluzione tecnologica

Implementazione di SPID nell'ambito di un processo di «credito al consumo»: Il flusso tra intermediario e CA



Le nuove opportunità derivanti dall'evoluzione tecnologica

Implementazione di SPID nell'ambito di un processo di «credito al consumo»: Sintesi della soluzione adottata

Highlights della nuova soluzione

- Individuazione del fornitore della soluzione quale FOI che assume il ruolo, nell'ambito del sistema SPID, di Service Provider
- Non viene richiesto l'upload da parte del cliente del proprio documento di identità
- Il riconoscimento tramite SPID propedeutico al rilascio da della CA del certificato di firma digitale a sua volta acquisito per adempiere agli obblighi di adeguata verifica AML
- Possibilità per il cliente di utilizzare la propria identità SPID di livello 2 (significativo) ai fini dell'identificazione
- Non viene richiesta l'acquisizione degli estremi identificativi del documento dal cliente
- Interrogazione ad AGID, tramite CA, con la modalità «Registrazione» che consente di ottenere, oltre ai dati identificativi, gli estremi del documento identificativo, cellulare, e-mail, domicilio fisico, data scadenza SPID

Principali benefici

IDENTITA' SPID IN CONTINUA CRESCITA

La registrazione di una identità digitale SPID è sempre più diffusa nei servizi di pubblica amministrazione e privati. Al momento della sua adozione erano circa 18,6 Milioni di identità

AZZERAMENTO TEMPI DI VERIFICA IDENTITA' DEL CLIENTE

Attualmente la verifica dell'identità viene effettuata tramite Allineamento SDD e tale controllo richiede in media 6/7 giorni.

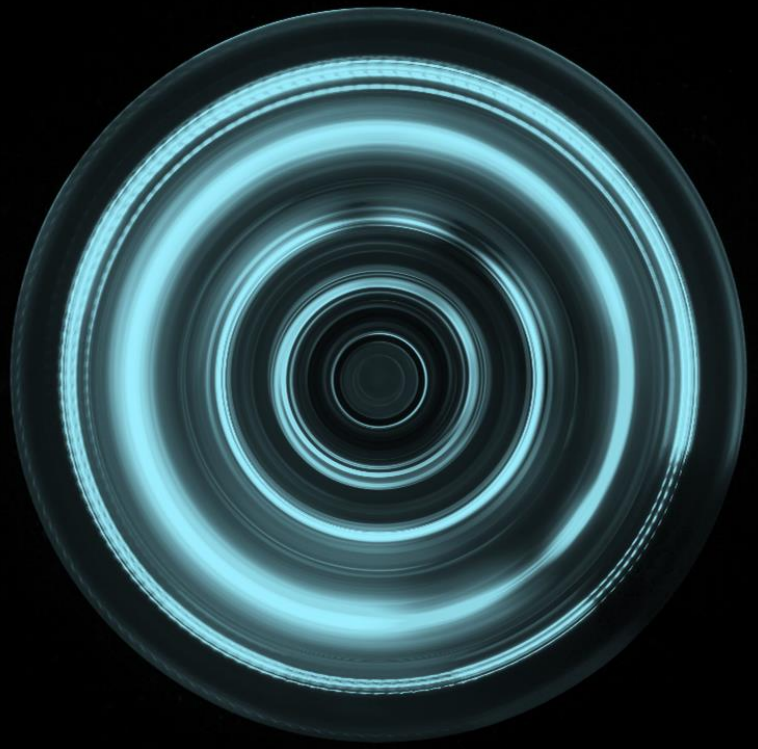
NUOVA OPERATIVITA' CLIENTE: SEMPLIFICAZIONE UX

Semplificazione della User Experience per i clienti non richiedendo più il caricamento del documento di identità

AUTOMATIZZARE APPROVAZIONE PRATICA e SAVING FTE INTERNI

Automatizzare, ove consentito, l'approvazione delle pratiche al fine di ottenere dei saving in termini di FTE interni

AGENDA



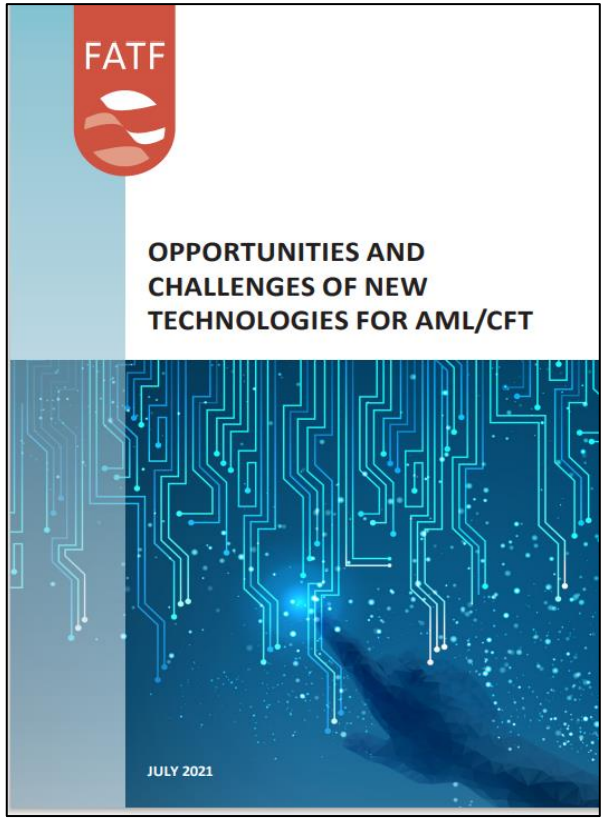
Evoluzione tecnologica a supporto dei processi AML e delle attività di controllo

Contesto di riferimento

Il GAFI ha recentemente tracciato lo stato dell'arte sull'applicazione di nuove soluzioni tecnologiche ai processi AML/CFT

Report GAFI

Il Gruppo di azione finanziaria internazionale (GAFI) è l'organismo intergovernativo indipendente che sviluppa e promuove politiche per proteggere il sistema finanziario globale dal riciclaggio di denaro, dal finanziamento del terrorismo. Le sue raccomandazioni vengono riconosciute come lo standard globale antiriciclaggio (AML) e antifinanziamento del terrorismo (CFT).



Overview

Nuove tecnologie per AML/CFT:

- Le nuove tecnologie permettono di rendere più veloci, economiche ed efficaci le misure antiriciclaggio (AML) e antifinanziamento del terrorismo (CFT).

Opportunità derivanti dalle nuove tecnologie per AML/CFT:

- Il GAFI è fortemente impegnato ad aggiornarsi sulle tecnologie ed i modelli di business innovativi adottati all'interno del settore finanziario, in modo tale da emanare standard globali aggiornati e consentire una regolamentazione affronti i rischi emergenti e promuova l'innovazione. A tal proposito, vengono esaminate le opportunità delle nuove tecnologie AML/CFT.

Le sfide derivanti dall'implementazione delle nuove tecnologie per AML/CFT:

- Il GAFI ha inoltre esaminato le sfide e gli ostacoli connessi all'implementazione di queste tecnologie e le modalità per attenuarli. Molte di queste sfide sono dovute a vincoli operativi e normativi eccezionali, come i sistemi di conformità AML/CFT legacy e i quadri normativi tradizionali e i meccanismi di supervisione.

Creazione ambiente armonico per l'utilizzo di nuove tecnologie in AML/CFT:

- Il GAFI propone di combinare l'efficienza e l'accuratezza delle soluzioni digitali con le conoscenze e le capacità analitiche degli esperti «umani» al fine di produrre sistemi più robusti in grado di rispondere efficacemente ai requisiti AML / CFT in modo pienamente «verificabile» e responsabile.

Contesto di riferimento

Le nuove soluzioni tecnologiche possono supportare numerosi stakeholder, sia interni che esterni, con molteplici benefici

Report GAFI

L'incremento dei controlli e delle sanzioni da parte delle Autorità preposte per contrastare il riciclaggio di denaro ed il finanziamento del terrorismo sta spingendo gli enti finanziari a dotarsi di processi e soluzioni tecnologiche volte a tutelare se stessi e la propria reputazione.

Gli utilizzatori delle nuove tecnologie

1. Istituzioni finanziarie multinazionali
2. Aziende Internet-based (Fintech o altre)
3. Banche retail e commerciali
4. FinTech
5. Autorità di Vigilanza

Benefici legati all'utilizzo delle nuove tecnologie

Il settore privato ha la capacità di:

- Identificare, valutare e gestire i rischi ML/TF
- Elaborare e analizzare grandi set di dati velocemente ed in modo accurato
- Migliorare la qualità delle segnalazioni di operazioni sospette alle autorità
- Ridurre i costi e ottimizzare l'impiego di risorse nelle aree più complesse dei processi AML/CFT
- Migliorare l'accuratezza dei risultati
- Migliore la gestione delle risorse umane

Le autorità di vigilanza riescono a:

Supervisionare un maggior numero di soggetti, identificare i rischi associati ai singoli settori, monitorare la conformità agli standard AML/CFT, archiviare, elaborare e riferire ampi insiemi di dati, scambiare informazioni con altre autorità competenti

Contesto di riferimento

Survey: lo stato di applicazione delle tecnologie evolute all'ambito AML nel contesto italiano*

Survey Crime & Tech

Campione dell'indagine

L'indagine è stata condotta nel gennaio 2021 e ha coinvolto categorie di soggetti obbligati quali banche e poste, altre istituzioni finanziarie indicate dalla normativa antiriciclaggio e gestori di case da gioco e operatori che offrono tramite a rete giochi, scommesse o concorsi con vincite in denaro. Sono stati contattati più di 100 professionisti con un tasso di risposta del 41%. Il totale dei rispondenti corrisponde al 46% del totale attivo del settore finanziario e di quello relativo al «gaming» in Italia.

Perimetro dell'indagine

Ai soggetti è stato somministrato un questionario finalizzato a comprendere il modus operandi con riferimento a:

- Analizzare e valutare il livello di adozione di strumenti di big data analytics e intelligenza artificiale nei settori regolamentati AML/CFT
- Esaminare come questi strumenti, quali ad esempio l'onboarding o il transaction monitoring, vengono utilizzati

Prime evidenze

In Italia il 53% dei soggetti obbligati che ha risposto al questionario utilizza soluzioni tecnologiche avanzate

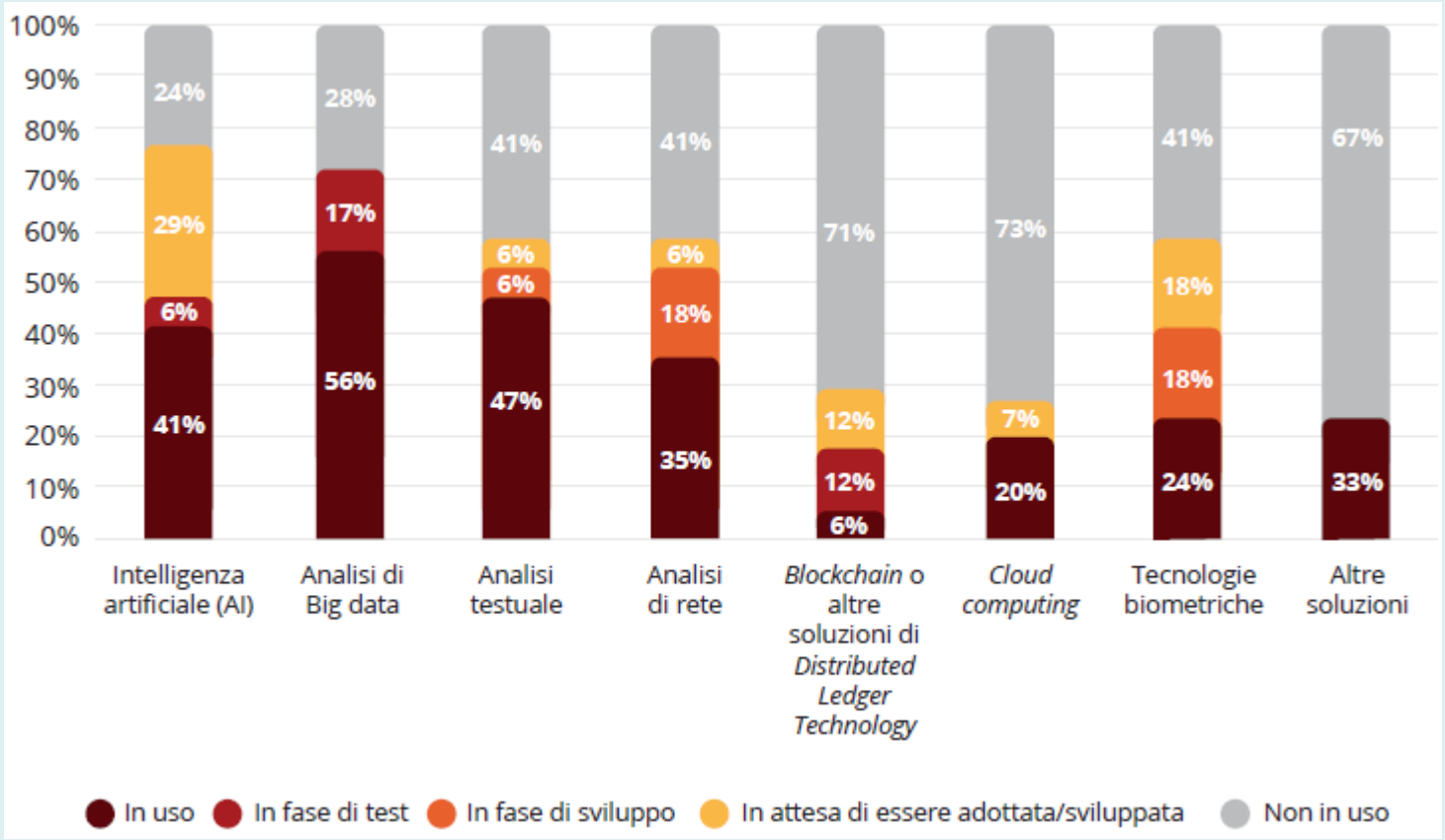
Le organizzazioni più grandi hanno più risorse da impiegare nell'acquisto o nello sviluppo di soluzioni tecnologiche e contestualmente hanno l'esigenza di ricorrere a strumenti più evoluti per gestire un volume più ingente di dati su transazioni e clienti

** Fonte: Crime&Tech (spin-off company dell'Università Cattolica del Sacro Cuore Transcrime) e SAS*

Contesto di riferimento

Survey: soluzioni tecnologiche adottate

Grafico 1: Tipo di soluzioni tecnologiche avanzate e livello di adozione



Intelligenza artificiale, analisi dei big data e analisi testuale sono le soluzioni avanzate più diffuse

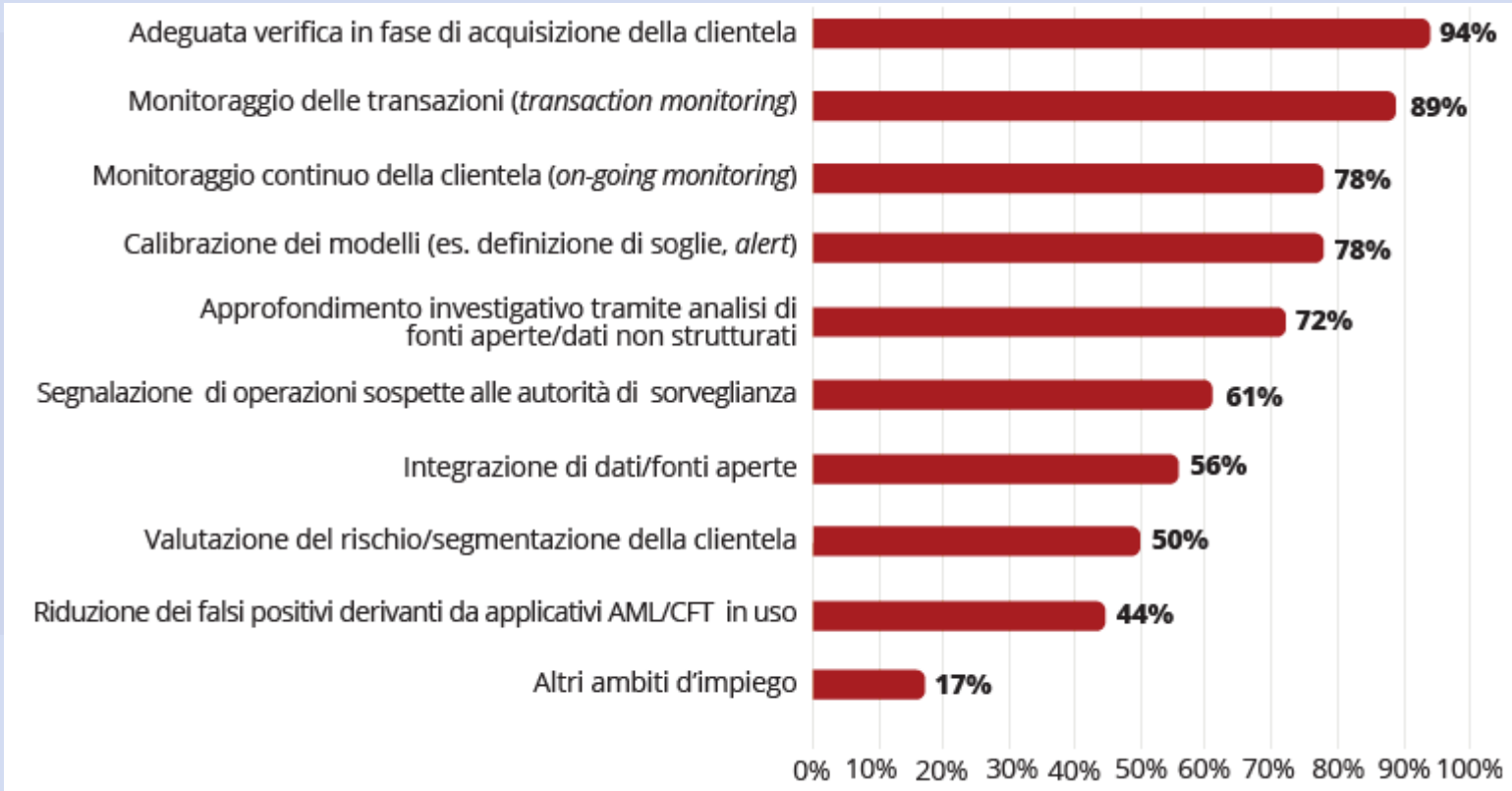
Il 20% del campione intervistato in fase di sviluppo/test di almeno una soluzione avanzata

Il 44% del campione ha in programma di adottare almeno una soluzione avanzata

Contesto di riferimento

Survey: Ambiti AML/CFT di impiego delle soluzioni tecnologiche avanzate

Grafico 2: Ambiti AML/CFT di impiego delle soluzioni tecnologiche avanzate.
Percentuale di rispondenti che adotta almeno una soluzione avanzata



Un impiego così importante delle tecnologie per la fase di on-boarding è conseguente ad una maggior digitalizzazione dei processi durante la pandemia ed alle recenti disposizioni legislative che prevedono la facilitazione dell'operatività a distanza (Decreto Semplificazioni)

Contesto di riferimento

Benefici e rischi

Emerge come l'impiego in soluzioni tecnologiche per l'AML/CFT sia un fenomeno in rapida evoluzione: per quanto questi strumenti evoluti siano adottati solo dal 53% del campione intervistato, l'84% dei rispondenti ha intenzione di investire nel prossimo futuro

Emerge come l'impiego di queste soluzioni possa portare:

- Migliorare l'individuazione dei comportamenti anomali e degli schemi emergenti di riciclaggio
- Ridurre il numero ancora elevato di falsi positivi nell'identificazione delle operazioni sospette
- Sfruttare il numero elevato di informazioni a disposizione dei soggetti obbligati, o acquisite da fonti terze
- Aumentare l'efficienza e il livello di automazione di molti dei processi AML/CFT, attualmente gestiti ancora manualmente, riducendo gli errori connessi alle attività manuali

Rimangono degli ostacoli da superare:

- Elevati costi per l'adozione di nuove soluzioni, ai quali si vanno a sommare costi aggiuntivi, in conseguenza alle difficoltà di integrazione con i sistemi AML/CFT già in uso, e le difficoltà di personalizzazione
- Difficoltà percepita nel gestire e interpretare le potenzialità e i risultati di questi strumenti evoluti e scarse capacità in tema di data analytics del personale addetto AML/CFT
- La sostituzione dei sistemi legacy con i nuovi strumenti, spesso particolarmente complessa, lunga e non diretta agli attori giusti
- 'Resistenza culturale' verso nuove soluzioni e attitudine ad affidarsi a soluzioni già collaudate ma meno efficaci nell'individuare i rischi di riciclaggio e, nel lungo periodo, più dispendiose

Risulta importante l'investimento nelle risorse umane per prevedere una nuova cultura e nuove competenze, incluse matematico-statistiche e informatiche, che consentano di individuare qualora dietro un'anomalia, identificata da una macchina intelligente, si nasconda una frode o un comportamento criminale

L’intelligenza artificiale a supporto dei processi antiriciclaggio

Occorre partire dalle peculiarità e problematiche che caratterizzano i processi AML

L’evoluzione tecnologica dei processi AML e CFT ha l’obiettivo di migliorare/risolvere alcuni punti critici generalmente riconosciuti:

Profilatura e adeguata verifica

- **Sistemi di profilatura meccanicistici** e non in grado di intercettare i rischi reali e di consentire una modulazione efficace delle misure di adeguata verifica
- **Ritardi** nel completamento delle informazioni su adeguata verifica e clienti privi di **questionario di AV**
- Rilevanti **stock di posizioni** da sottoporre ad analisi e lavorazione
- Opportunità di migliorare lo **standard qualitativo** e l’**omogeneità d’approccio** nelle attività di due diligence e rivalutazione della clientela

Monitoraggio operatività sospetta

- Elevato numero di **falsi positivi** generati dai sistemi tradizionali di monitoraggio basati su modelli deterministici
- Concertazione degli alert su pochi indicatori e derivanti da **regole semplici, di frequenza perlopiù giornaliera**
- Lunghe **tempistiche di segnalazione** anche in ragione dell’utilizzo dell’AUI quale sistema alimentante delle attuali soluzioni informatiche
- Necessità di potenziare i processi e gli strumenti di monitoraggio su ambiti a maggior rischio e **schemi di anomalia complessi**
- **Ritardi** nella lavorazione delle pratiche e accumulo di **stock di posizioni da valutare**

Controlli di secondo livello

- Necessità di **rafforzare alcuni ambiti di controllo** (es. clientela ad alto rischio, PEP, movimenti in contanti, clienti con carenze di info raccolte in fase di AV, ecc.) nonché i controlli **sull’operatività del primo livello**
- Necessità di ampliare il **numero** e la **frequenza** dei controlli di secondo livello attualmente svolti, nonché di ampliare i **campioni analizzati**
- Opportunità di migliorare i **supporti informatici** per la conduzione e storicizzazione dei controlli nonché per il **collegamento automatico all’esercizio di autovalutazione**
- Carenze, in termini di **completezza** ed **efficacia** della reportistica prodotta dalla Funzione

Processi operativi manuali e ripetitivi, con elevato numero di posizioni giornaliere da processare e rilevante esposizione a rischi di natura operativa. Forte concentrazione dell’impegno delle risorse coinvolte (circa 80%) nel processo di raccolta delle informazioni e solamente in modo residuale sulle analisi e valutazioni

L’intelligenza artificiale a supporto dei processi antiriciclaggio

Un focus sulle criticità degli attuali processi di transaction monitoring*

I Punti di attenzione delle attuali soluzioni di transaction monitoring…in pochi numeri

99%

…di falsi positivi

Gli attuali sistemi producono attualmente un **numero molto elevato di alert** (con rilevanti impatti sull’effort di **lavorazione**). Tuttavia solo una piccola parte di questi **(circa 1%)** diviene, a seguito di analisi e valutazione, una SOS.

55%

…di SOS derivanti dai medesimi indicatori

La maggior parte delle **SOS** (circa il 55%) origina da un numero limitato di indicatori di anomalia (**operazioni in contanti e bonifici Italia/Estero)**. Ci sono pertanto margini per ampliare il perimetro di analisi in linea con quanto peraltro richiesto dalla nuova normativa

40%

…di SOS derivanti da regole semplici

Le segnalazioni derivano da **regole semplici**, di frequenza giornaliera . I modelli di scoring si concentrano infatti su singoli soggetti e sui relativi legami statici.

Lunghe tempistiche di segnalazione

Le **tempistiche** di segnalazione risultano particolarmente elevate anche in ragione dell’utilizzo dell’AUI quale sistema alimentante dell’attuale soluzione di transaction monitoring

Root causes

Conoscenza a priori:

Individuazione delle regole e degli schemi di anomalia da monitorare, sulla base di esperienza utente o segnalazioni interne

Staticità dei controlli:

Gli algoritmi che descrivono le regole deterministiche di rappresentazione della fattispecie anomala sono alert statici nel tempo

Necessità di un costante aggiornamento delle regole:

In seguito all’attivazione dei presidi, è probabile che i comportamenti di rischio si modifichino nel tempo, generandone di nuovi. Per tale motivo è spesso necessario cercare, esplorare e individuare nuovi schemi

** Fonte: Benchmark Deloitte 2019*

L’intelligenza artificiale a supporto dei processi antiriciclaggio

Prima di approcciare ad un programma strutturato di applicazione di nuove tecnologie di analisi ai processi di controllo e mitigazione dei rischi è opportuno fare chiarezza sui concetti base

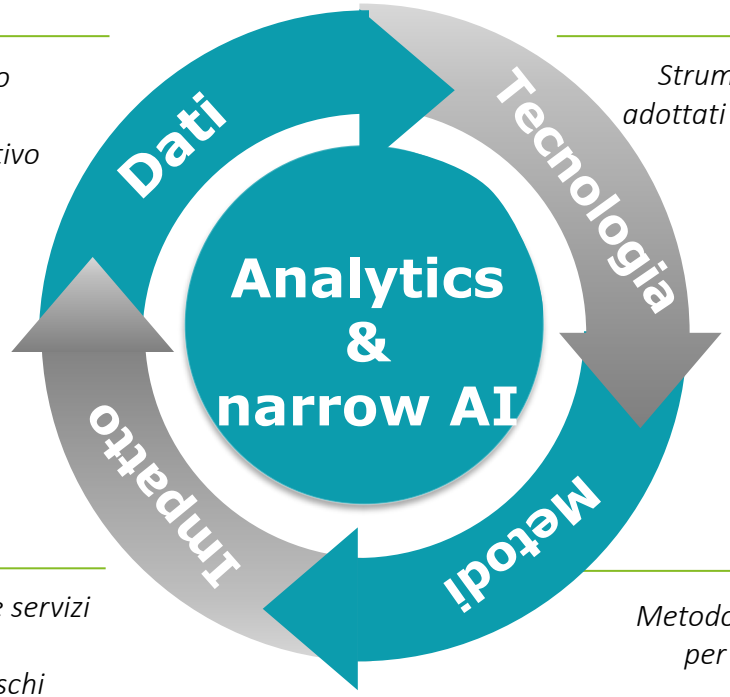
Un **modello** che può sintetizzare correttamente l’ambito di applicazione dei **tecnologie avanzate di analisi dei dati**, si articola in **4 fasi**:

1

Dati organizzati allo scopo di estrarre il contenuto informativo

2

Strumenti informatici adottati per l’utilizzo dei dati



4

Impatto sui prodotti e servizi e sulla creazione del valore/gestione dei rischi

3

Metodologie analitiche per l’analisi dei dati

Focus on machine learning

Le tecniche di Machine Learning si basano su un cambiamento del tipico paradigma di programmazione

Approccio tradizionale alla programmazione

Approccio del machine learning

L’intelligenza artificiale a supporto dei processi antiriciclaggio

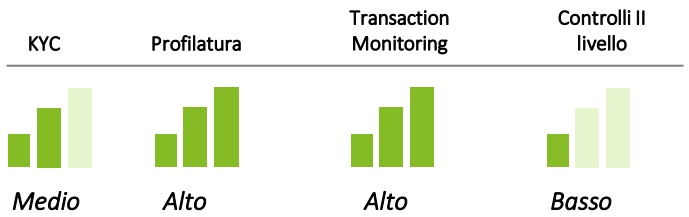
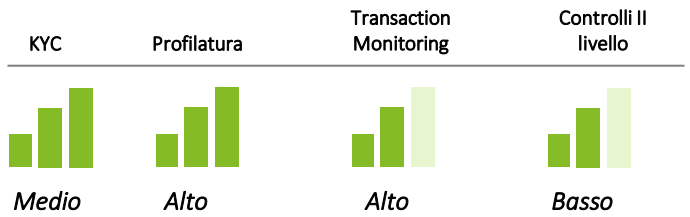
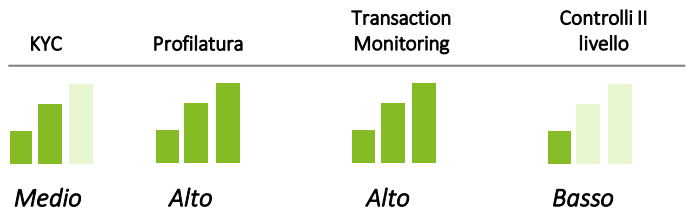
Caratteristiche e benefici derivanti dall’applicazione di tecniche di data analytics e machine learning ai processi AML

	Valutazione cliente (KYC)	Profilatura	Monitoraggio operatività sospetta	Controlli di secondo livello
1 Informazioni	• Dati anagrafici • Dati operatività transazionale • Dati da fonti esterne	• Dati anagrafici e operatività transazionale • Dati da fonti esterne • Dati da monitoraggio operatività sospetta	• Dati anagrafici e operatività transazionale • Dati profilatura	• Tutti i precedenti dati
2 Tecnologia	• Piattaforma analisi dati (es. R/Python, SAS, KNIME,…) • Work flow (possibile utilizzo WF esistenti)	• Piattaforma analisi dati (es. R/Python, SAS, KNIME…) • Work flow (possibile utilizzo WF esistenti)	• Piattaforma analisi dati (es. R/Python, SAS, KNIME…) • Work flow (possibile utilizzo WF esistenti)	• Piattaforma analisi dati (es. R/Python, SAS, KNIME…) • Piattaforma data visualization (es. Qlik, Power BI, Spotfire)
3 Metodo	• Data analytics • Machine learning • Predictive analysis	• Data analytics • Machine learning • Predictive analysis	• Data analytics • Machine learning • Predictive analysis	• Data analytics • Machine learning • Predictive analysis
4 Impatti	• Miglioramento dei processi di adeguata verifica e screening della clientela • Lettura documentale e identificazione delle informazioni mancanti/non corrette e «data enrichment»	• Evoluzione dei criteri di profilatura della clientela sulla base di elementi di rischio reale (da un approccio deterministico a un approccio probabilistico) • Aggiornamento dei profili di rischio in base all’operatività transazionale della clientela	• Apprendimento dei comportamenti del cliente considerati ‘normali’ e identificazione delle fattispecie sospette • Visual link analysis e scenario analysis • Riduzione del numero di falsi positivi e prioritizzazione degli alert prodotti dalle procedure di transaction monitoring	• Aumento del numero e della frequenza dei controlli • Ampliamento dei campioni analizzati • Scoring automatico degli esiti dei controlli • Tracciatura e storicizzazione dei controlli svolti

L’intelligenza artificiale a supporto dei processi antiriciclaggio

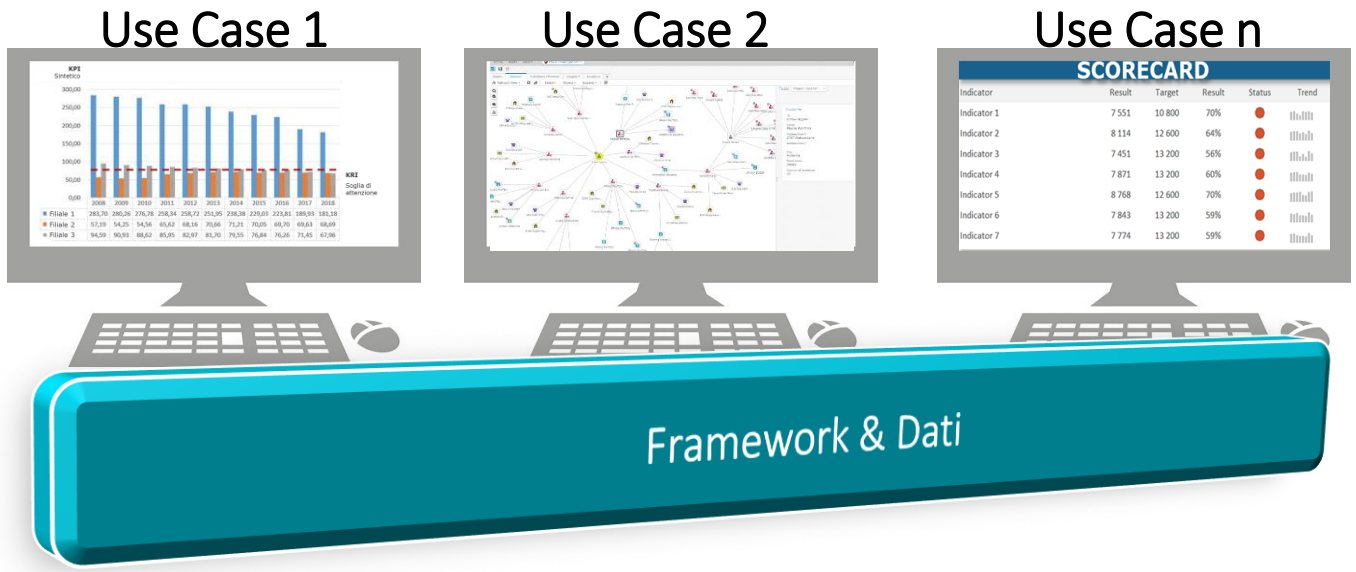
In particolare l’analisi predittiva e le tecniche di machine learning se applicate ad alcuni processi AML consentono di rendere più sofisticati ed efficaci gli attuali strumenti di detection

L'utilizzo dei Data Analytics nei processi AML è finalizzato all'individuazione, attraverso modelli econometrico/statistici, dei principali fattori che aumentano o diminuiscono la probabilità dei clienti di essere coinvolti in episodi di riciclaggio e finanziamento del terrorismo (e quindi segnalati alla UIF)

	Apprendimento supervisionato (supervised learning)	Apprendimento non supervisionato (unsupervised learning)	Apprendimento con rinforzo (reinforcement learning)
	«Riconosco connessioni che legano i dati in input a una colonna obiettivo» L’algoritmo impara mediante l’osservazione di esempi passati, ovvero i dati muniti di risultati (es. inattesi effettivamente divenuti SOS). Gli algoritmi di apprendimento supervisionato si propongono di «scovare» e riprodurre (con un certo grado di approssimazione) la regola che lega i dati di input al target (es. scenario di operatività sospetta). La condizione fondamentale per l’utilizzo di questo approccio è la disponibilità di dei dati e dei risultati relativi al dataset oggetto di analisi.	***«Riconosco strutture nei dati»*** La macchina riconosce alcuni aspetti della struttura dei dati in input, senza avere a disposizione un risultato passato (ovvero una colonna target). L’applicazione più comune dell’apprendimento supervisionato è quella del *clustering*, ovvero l’analisi dei gruppi (es. cluster di clienti omogenei per profilo di rischio)	***«Faccio tentativi e imparo dagli errori»*** La macchina interagisce con l’ambiente interno e impara dai suoi stessi errori mettendo in pratica ciò che ha imparato, valutando il corretto funzionamento del modello sulla base del c.d. meccanismo di ricompense e rinforzando la sua conoscenza attraverso questa nuova esperienza.
Scenario	Regressione (l’obiettivo è un numero) Classificazione (l’obiettivo è una categoria)	Clustering (raggruppamento in cluster omogenei) Riduzione della dimensione (screening dati)	Agente autonomo (imparare le risposte in base alle variazioni dell’ambiente)
Es. Algoritmo	Linear/logistic regression | Decision tree | Random forest | Neural network	K-means | Hierarchical clustering | Latent Direchlet Allocation (LDA) | Principal Component Analysis (PCA) | Singular Value Decomposition (SVD)	Q-Learning | Monte Carlo
Applicazione AML			

L’intelligenza artificiale a supporto dei processi antiriciclaggio

L’approccio prevalente prevede l’applicazione di modelli e tecniche di Narrow AI (Machine Learning) partendo dall’identificazione di specifici Use Case finalizzati a fornire risposte concrete e immediate a specifiche esigenze funzionali



ALCUNI ESEMPI

Focus slide successive

1. **Visualizzazione razionalizzata delle informazioni**
   Predisposizione di una visualizzazione aggregata delle informazioni sul Cliente rilevanti ai fini delle valutazioni AML, con conseguente saving di tempo per la rete in fase di data collection e valutazione e migliore conoscenza del Cliente

2. **Scoring Inattesi**
   Modello che, sulla base di un **AML probability index**, consente di attribuire un livello di priorità agli alert prodotti dai tradizionali sistemi di transaction monitoring (es. inattesi Gianos) al fine di prioritizzare e/o scremare gli alert da valutare

3. **Controlli Hub To Spoke**
   Controlli di secondo livello sul corretto operato delle strutture di primo livello e sulla rete distributiva, con particolare riferimento al monitoraggio dell’operatività sospetta

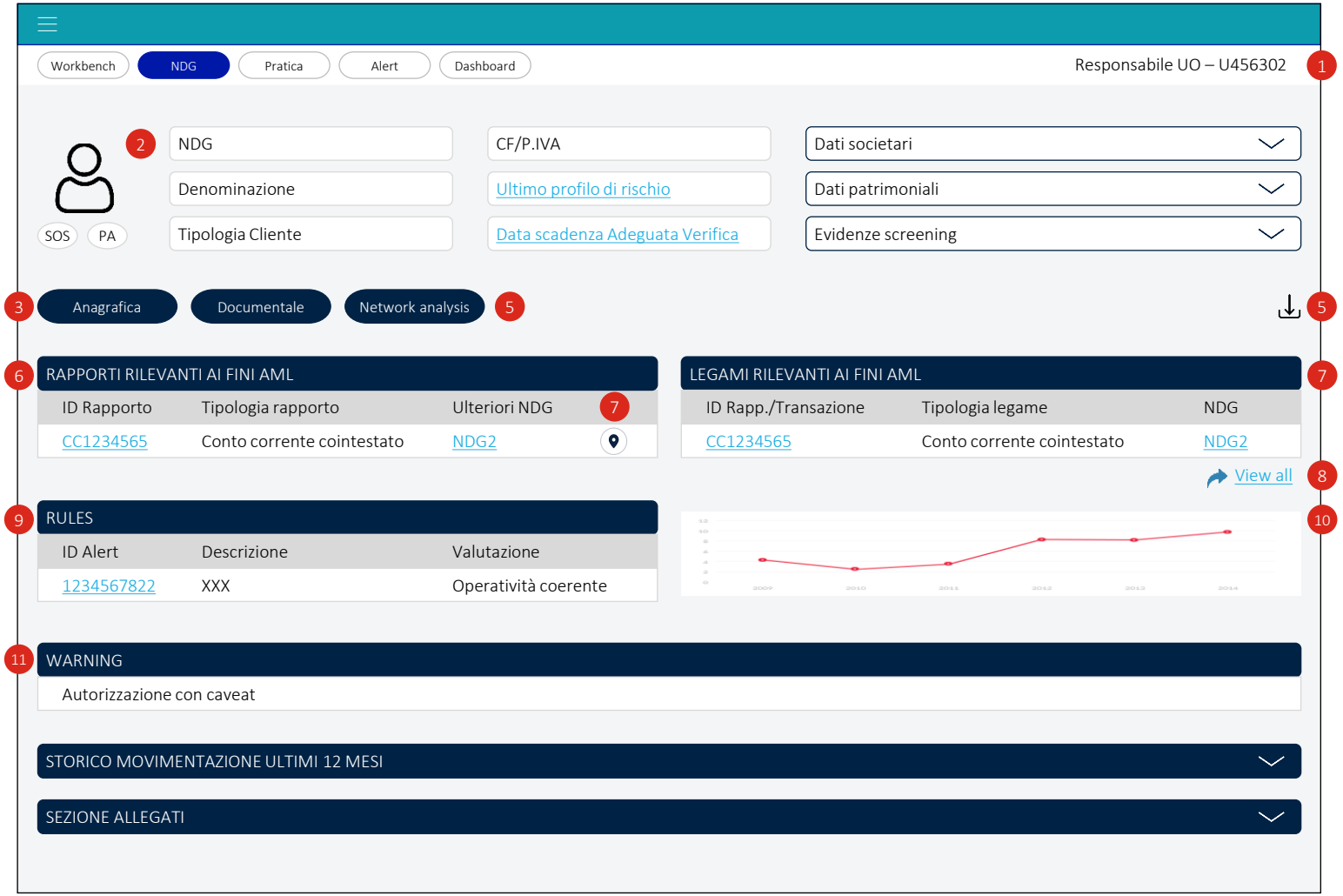
4. **High Risk Topics advanced detection**
   Utilizzo di tecniche innovative di detection (AI) su pattern di rischio anomali con specifiche riferimento a specifici ambiti ad elevato rischio e utilizzando altresì tecniche di **network analysis** (analisi delle connessioni tra entità correlate)

5. **Revisione Modelli di profilatura & Dinamic Risk Rating Engine**
   Utilizzo di modelli probabilistici e di una maggiore quantità di dati e informazioni con la finalità di determinare in modo più accurato il profilo di rischio del cliente

L’intelligenza artificiale a supporto dei processi antiriciclaggio

Visualizzazione razionalizzata delle informazioni

È possibile creare una pagina in cui aggregare tutte le informazioni rilevanti ai fini AML di un Cliente, completa di link ai gestionali e di grafici per l’analisi e la rielaborazione dai dati, di statistiche relative allo storico del cliente e di ulteriori elementi riportati in slide a titolo esemplificativo, personalizzabili in relazione delle esigenze dell’intermediario.



1. Profilazione delle informazioni a seconda dell’utente che accede in pagina
2. Informazioni anagrafiche, patrimoniali, evidenze da screening list, informazioni sul profilo di rischio e sull’ultima Adeguata Verifica eseguita
3. Accesso diretto a gestionali come ad es. Anagrafe, Documentale, Sezionale
4. Tasto di accesso diretto a gestionali come ad es. Anagrafe, Documentale, Sezionale o a Provider esterni per gestione delle bad news sul Cliente
5. Possibilità di scaricare tutte le informazioni in pagina
6. Elenco dei rapporti attivi rilevanti ai fini AML con link diretti al Partitario e alle pagine NDG collegate
7. Elenco dei legami rilevanti del Cliente, sia a livello anagrafico, che transazionale
8. Possibilità di visualizzare in forma grafico la link analysis del Cliente, sia a livello anagrafico, che transazionale in logica «follow the money»
9. Elenco delle regole AML scattate per il Cliente con storico valutazioni e link diretto ai singoli alert (A/C)
10. Dashboard sintetica con storico valutazioni e comportamenti anomali del Cliente e trend andamentale
11. Elenco dei warning inseriti in fase di valutazione alert precedenti o core system

L'intelligenza artificiale a supporto dei processi antiriciclaggio

Sistema di alert scoring

Il Modello è finalizzato a valutare e discriminare gli alert prodotti dai sistemi tradizionali di transaction monitoring con la finalità di identificare potenziali SOS determinando un AML probability index:

- È principalmente utilizzato per discriminare gli alert in valutazione presso la Rete e le strutture centrali al fine da focalizzare le attività di indagine direttamente sulle transazioni potenzialmente sospette, anche quando scartate
- Può altresì essere utilizzato per identificare eventuali posizioni archiviate che invece presentano un'elevata probabilità di determinare una SOS
- Possibilità di utilizzare il probability index come elemento "correttivo" della profilatura dei clienti, fornendo l'indicazione, già prima della generazione di un inatteso, sulla probabilità che il cliente possa determinare una SOS

Il modello di funzionamento

Finalità del modello

A partire dallo storico delle segnalazioni si costruisce un modello predittivo che, una volta addestrato, verrà applicato ai «nuovi» dati per **stimare** la probabilità di generazione di un falso positivo

Dimensioni di analisi

- **Unità statistiche** di riferimento:
  - Cliente
- **Variabili** di addestramento/profilo:
  - Anagrafiche | Movimentazioni | Indicatori
- **Classe**:
  - Status Inattesi

Step

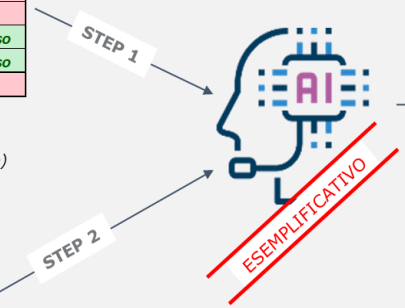
1. Data **selection**
2. Data **cleaning** – **transformation**
3. Feature **selection**
4. Model **selection**
5. Model **validation**
6. Interpret the **results**

Tab. 1 – *Dati per creazione modello predittivo (dati storici)*

ID	Utente	Provincia	Età	...	Ammontare Complessivo	...	Status
1	Marco Rossi	Genova	20	...	10.000,00 €	...	*Inatteso*
2	Matteo Bianchi	Milano	45	...	250.000,00 €	...	*SOS*
3	Nilde Loggia	Roma	70	...	3.000.000,00 €	...	*Inatteso*
4	Dalia Marino	Torino	34	...	340.000,00 €	...	*SOS*
...	...	...	...	...	...	...	*SOS*
12	Simone Verdi	Bologna	54	...	2.310.000,00 €	...	*Inatteso*
...	...	...	...	...	...	...	*Inatteso*
30	Elisa Greco	Verona	67	...	12.000,00 €	...	*SOS*

Tab. 2 – *Dati sui quali si vuole ottenere una previsione (periodo corrente)*

ID	Utente	Provincia	Età	...	Ammontare Complessivo
12	Rosa Bianchi	Catania	34	...	390.000,00 €
23	Gino Rossi	Napoli	56	...	23.500,00 €
35	Lara Piazza	Venezia	78	...	1.200.000,00 €
41	Tiziano Barese	Roma	23	...	300.000,00 €
...	...	...	...	...	...
57	Viola Lombardi	Bari	33	...	54.000,00 €
...	...	...	...	...	...
89	Marco De Luca	Parma	45	...	345.000,00 €



Tab. 3 – *Output / Predizione del modello*

ID	Utente	Status Pred.	SOS Prob.
12	Rosa Bianchi	*SOS*	90%
23	Gino Rossi	*Inatteso*	20%
35	Lara Piazza	*SOS*	51%
41	Tiziano Barese	*Inatteso*	49%
...	...	*Inatteso*	30%
57	Viola Lombardi	*SOS*	76%
...	...	*SOS*	64%
89	Marco De Luca	*Inatteso*	12%

Focus sul modello di alert scoring nelle slide successive

L'intelligenza artificiale a supporto dei processi antiriciclaggio

Controlli Hub To Spoke: la struttura del Modello

Il modello di profilatura delle singole filiali/agenzie è basato su 4 componenti di seguito rappresentate. Le stesse prevedono livelli di complessità differenti e possono essere implementate anche in modo autonomo preservando la consistenza del modello complessivo:

	1	2	3	4
	Indicatori di rischiosità inerente (KRI)	**Indicatori di natura organizzativa**	**Indicatori di performance (KPI)**	**Indicatore di natura probabilistica**
Overview	Indicatori che danno evidenza della rischiosità potenziale di ciascuna filiale sulla base di fattori rischio afferenti a: operatività, prodotti/servizi, tipologia clienti, aree geografiche di riferimento. Trattasi di fattori che partono da quelli solitamente utilizzati nell'ambito dell'esercizio di autovalutazione	Indicatori che tengono conto delle caratteristiche di natura organizzativa delle singole filiali e che possono rappresentare un primo mitigant rispetto ai profili di rischiosità potenziale identificati. Gli stessi sono rilevati mediante specifici «questionari»	Indicatori che danno evidenza delle performance di ciascuna filiale in relazione ai diversi domini di cui si compone il processo AML: adeguata verifica, segnalazione operazioni sospette, conservazione dati/documenti, trattamento del contante, antiterrorismo	Trattasi di un unico indicatore che da evidenza di quante operazioni ritenute potenzialmente sospette da un modello supervisionato di machine learning sono state invece ritenute non sospette dalla singola filiale in esame
	Complessità realizzativa: Bassa Peso della componente nel Modello: Basso – Alto	Complessità realizzativa: Bassa Peso della componente nel Modello: Basso – Alto	Complessità realizzativa: Media Peso della componente nel Modello: Basso – Alto	Complessità realizzativa: Alta Peso della componente nel Modello: Basso – Alto
Esempi	❑ Operatività in contante reale ❑ Rischiosità prodotti offerti dalle filiale ❑ Clienti a rischio alto ❑ Clienti PEP ❑ Clienti non natura di trust/fiduciaria ❑ Area geografica in cui opera la filiale e relativi clienti ❑ Ecc.	❑ Dimensione della filiale ❑ Eventuali gap aperti sulla filiale ❑ Ecc.	❑ Stock pratiche di AV da valutare ❑ Stock pratiche SOS da valutare ❑ Tempi medi di indagine ❑ Richieste di assistenza/consulenza alla Funzione AML ❑ Training erogato/fruito ❑ Indicatori semantici note di archiviazione SOS ❑ Ecc.	❑ Concentrazione di alert considerati ad alto rischio dal modello di machine learning ma che risultano essere stati archiviati dalla filiale come «da non segnalare»

L'intelligenza artificiale a supporto dei processi antiriciclaggio

Use Case

Controlli Hub To Spoke: output del modello di profilatura delle filiali

La media ponderata della valutazione espressa per i singoli indicatori determina il profilo di rischio per singola filiale:

Scorecard Filiali/Agenzie

Filiale	Ind. 1	Ind. 2	Ind. n	Score (RI)	Trend
Filiale Roma 1	7.454	6.433	…		
Agenzia Milano 2	8.145	3.498	…		
Filiale Genova 1	3.456	3.786	…		
Filiale Bolzano 3	5.123	2.123	…		
….	…	…	…	…	…

$$RI = \sum_{1}^{n} (K_i \cdot \alpha_i)$$

Dove:
RI=valutazione di rischio filiale
K=valutazione di rischio singolo KRI/KPI
α = fattore di ponderazione singolo KRI/KPI

Dossier Filiale/Agenzia

Possibilità di **deep-dive** sulla singola filiale al fine di analizzare i singoli indicatori che hanno determinato il profilo di rischio complessivo

A seconda del profilo di rischio possono essere adottati percorsi di controllo differenziati e opportunamente codificati nelle procedure interne:

- ☑ Frequenza e profondità delle **ispezioni in loco**
- ☑ **Ampiezza dei campioni** di analisi su cui si basano le attività di controllo a distanza
- ☑ **Approfondimenti** e **richiesta documentale** con perimetro e ampiezza differenziata
- ☑ Previsione di **percorsi formativi mirati/differenziati**
- ☑ Comminazione di **provvedimenti disciplinari**

L'intelligenza artificiale a supporto dei processi antiriciclaggio

High Risk Topics advanced detection: il framework di riferimento

Lo sviluppo dei modelli di rischio basati su algoritmi predittivi si basa sull'identificazione di specifici use case nell'ambito di un framework distinto nelle aree di rischio sottostanti (riciclaggio, finanziamento del terrorismo e corruzione, etc.)

L'identificazione dei modelli di rischio da sviluppare in riposta a specifici use case è il frutto di un'analisi preliminare volta a rilevare gli ambiti di maggior rischio

Il processo di identificazione dei modelli di rischio da sviluppare

1. Analisi del modello di business e operativo della Banca
2. Analisi caratteristiche della customer base e della composizione delle SOS
3. Rilevazione degli ambiti di maggior rischio
4. Declinazione degli use case e dei modelli di rischio da sviluppare

Framework di riferimento

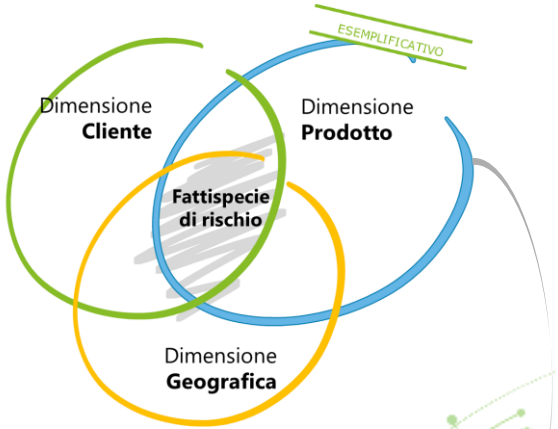
Riciclaggio
- Contante
- Prepagate
- Valute virtuali
- ....

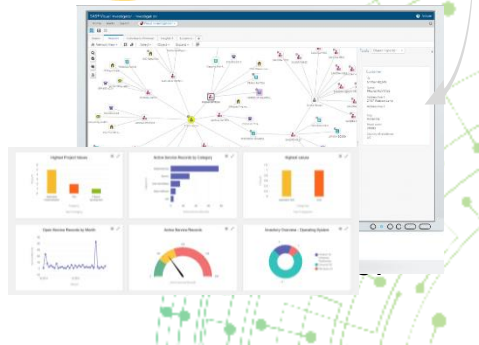
Finanziam. al terrorismo
- Fondazioni islamiche
- Hawalla
- ....

Corruzione
- Dipendenti delle PA in posizioni decisionali
- Concessione di appalti
- ....

New

Nuovi rischi Covid
- Truffe legate ai prodotti sanitari
- Fenomeni usurari e criminalità organizzata
- Accesso illecito a risorse pubbliche
- Frodi on line





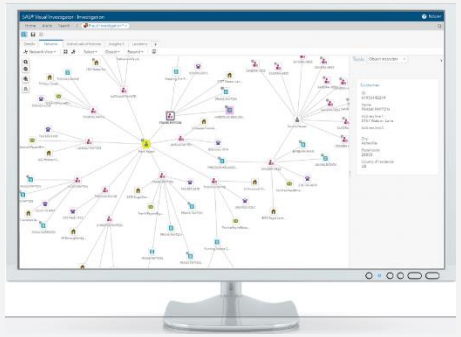
L'intelligenza artificiale a supporto dei processi antiriciclaggio

High Risk Topics advanced detection: utilizzo delle tecniche di network analysis

"Un cambio di prospettiva"

Le attuali soluzioni in uso si basano su modelli di scoring che si concentrano su singoli soggetti e sui relativi **legami statici**

- Attribuzione di un determinato profilo di rischio alla clientela sulla base dei dati raccolti in fase di adeguata verifica e del punteggio calcolato. Trattasi della **somma dei punteggi assegnati** a ciascuna delle informazioni fornite dal cliente e/o acquisite da fonti esterne
- Anche la rideterminazione periodica del punteggio avviene mediante le medesime regole
- **L'individuazione** delle **operazioni potenzialmente sospette** avviene utilizzando gli indicatori di anomalia **sempre ex-post** (a operazione avvenuta)



Le nuove soluzioni si basano su modelli probabilistici in grado di concentrarsi su diversi soggetti caratterizzati da **legami statici** (es. cointestazioni) e **lagami dinamici** (o secondari)

- ✓ L'analisi dei fenomeni rischiosi viene condotta mediante la formulazione di una **serie di distribuzioni** a priori che esprimono una determinata probabilità di accadimento di un evento rischioso e che nel tempo «insegnano al modello come comportarsi»
- ✓ Oltre ad elementi probabilistici sono utilizzati anche **variabili deterministiche** (es. qualifica di PEP)
- ✓ Il mix di tali variabili determina una **valutazione di rischio «reale»** correlata (e determinata) non solo al soggetto ma a tutti i soggetti che intrattengono con lo stesso legami statici e dinamici (c.d. piazza)

L'intelligenza artificiale a supporto dei processi antiriciclaggio

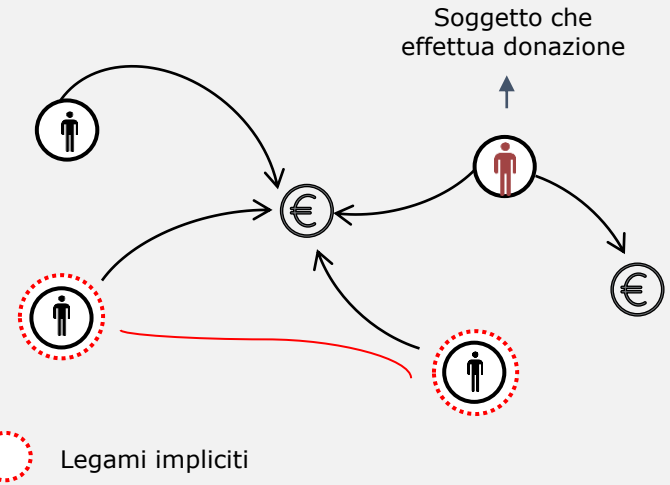
High Risk Topics advanced detection: utilizzo delle tecniche di network analysis

Caso 1: Finanziamento al terrorismo

…cosa accade?

Persona fisica effettua donazioni ad una associazione islamica

…cosa consente di fare il modello?



Al centro dell'analisi vi è l'evento anomalo. Nel caso in cui l'algoritmo evidenzia un' operazione sospetta il software consente di mostrare graficamente le transazioni ed i relativi importi effettuate dalla persona fisica, ed i legami secondari (es. bonifici effettuati verso l'associazione islamica da parte di altri clienti della banca) permettendo una visione di insieme sintetica ed immediata.

…su quali basi si poggia la regola dello strumento?

Indicatori di anomalia (cfr. Provvedimento della Banca d'Italia recante gli indicatori di anomalia per gli intermediari):

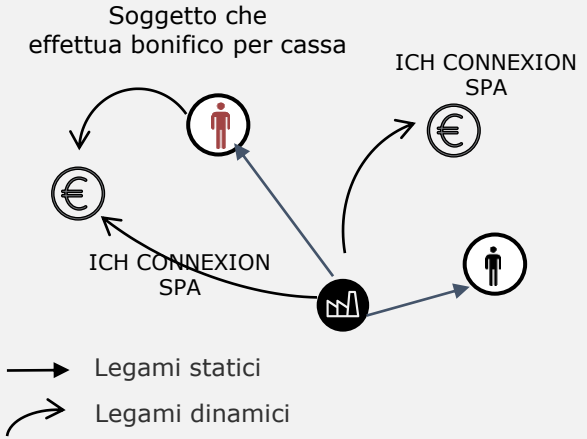
- ✓ 21.3 Ripetuti accrediti su conti intestati ad associazioni e fondazioni, a titolo di donazione, raccolte o simili, di ammontare complessivo consistente e non adeguatamente giustificato…

Caso 2: Riciclaggio

…cosa accade?

Persona fisica effettua bonifici per cassa per importi ingenti.

…cosa consente di fare il modello?



Il soggetto è una persona fisica e bonifica per cassa per importi ingenti, poi bonifica anche dall'azienda di cui è titolare effettiva, ICH CONNEXION SPA, società di gambling di Roma, versando un importo quasi simile a quello bonificato.
Il software mostrando i diversi nodi consente di analizzare e comprendere le anomalie e le diverse casistiche con efficacia ed una riduzione sostanziale delle tempistiche.

…su quali basi si poggia la regola dello strumento?

Provvedimento recante gli indicatori di anomalia per gli intermediari del 30 gennaio 2013:

- ✓ Schemi rappresentativi di comportamenti anomali su giochi e scommesse : profili oggettivi

L'intelligenza artificiale a supporto dei processi antiriciclaggio

Possibile applicabilità dell'AI in fase di calibrazione dei trigger o di definizione delle variabili deterministiche

MODELLO BASATO SU TRIGGER/EVENTI

Da attività stand-alone applicata ad un perimetro di Clienti definito ad approccio strutturato Risk Based

EVENT DRIVEN REVIEW (EDR)

Possono essere identificati dei Key Risk Factors (on top rispetto alle fasce di rischio) sulla base dei quali anticipare la scadenza della review e dell'acquisizione del questionario definendo altresì processi differenziati. Essi possono considerare quelli giù utilizzati in sede di profilatura ed integrarne altri con diverso livello di complessità

Indicatori «semplici»

- Assunzione qualifica PEP
- Residenza in Paese ad Alto Rischio
- Scadenza documento identificativo
- Richiesta info da Autorità (UIF per SOS)
- Riattivazione conto inattivo
- Cambio compagine societaria
- Modifica SAE e ATECO ad alto rischio
- Richiesta prodotti ad alto rischio
- Aumenta ricchezza significativo
- Adverse/bad news

Indicatori «complessi»

- Indicatori basati su modelli predittivi di AI costruiti internamente (es. AML Probability Index)
- Informazioni ed indici acquisiti da fonti esterne affidabili (es. indici infiltrazioni criminali)

Logiche per efficientare la review

Ferma restando l'attivazione della review al cambiamento della fascia di rischio, è possibile introdurre processi che vanno ad eliminare possibili inefficienze della EDR:

- Grace period[1];
- Regole di coda[2].

AUTOMATIC REVIEW (AR)

Identificati dei criteri (opportunamente calibrati in relazione al modello di business/operativo) al verificarsi dei quali è possibile procedere alla review automatica e all'aggiornamento della data di scadenza. Tali fattori possono riguardare le seguenti categorie: Fascia di rischio; Tipologia clientela; Tipologia rapporti continuativi attivi; Operatività nel periodo di tempo, etc.

Esemplificativo variabili deterministiche che, se simultaneamente verificate, possono autorizzare la review automatica[3]:

- Operazioni in contante < XX, per un importo complessivo < XX.XXX €;
- Bonifici ricevuti/disposti < XX, per un importo complessivo < XX.XXX €;
- Ritorni di insoluti < XX% dell'importo delle presentazioni;
- Operazioni extra conto < XX, per un importo complessivo < X.XXX €;
- Nessun alert di TxM;
- Documento d'identità valido;
- Questionario KYC valido almeno per uno dei rapporti in essere;
- Nessuna hit da screening list;
- Etc.

È possibile inoltre sofisticare il modello mediante l'utilizzo degli indicatori complessi (on top alle variabili deterministiche o ad integrazione delle stesse)

Es. Se AML Probability Index < XX (soglia di rilevanza del rischio), allora rinnovo automaticamente le info e definisco nuova data scadenza Questionario;

Possibilità di escludere fasce basse/irrilevante da review periodica «a scadenza» e attivazione solo legata ai trigger

1. EDR attiva la review solo se l'ultima review è precedente a XX giorni (l'EDR viene «spento») 2. Se la review è stata completata da meno di XX giorni, perché una nuova review venga avviata è necessaria l'attivazione di X EDR (l'EDR viene messo in «stand-by») 3. Due opzioni: a) il sistema procede al rinnovo automatico; b) il business visualizza le richieste di rinnovo automatico (report/alerting) ed autorizza i singoli rinnovi

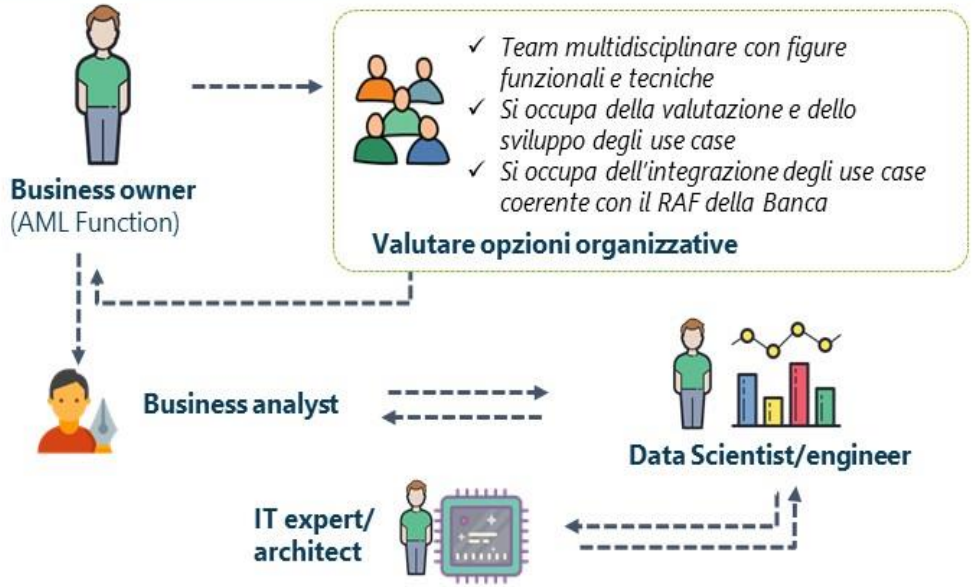
L’intelligenza artificiale a supporto dei processi antiriciclaggio

Le implicazioni di carattere organizzativo derivanti dall’applicazione dei modelli di AI ai procesi AML

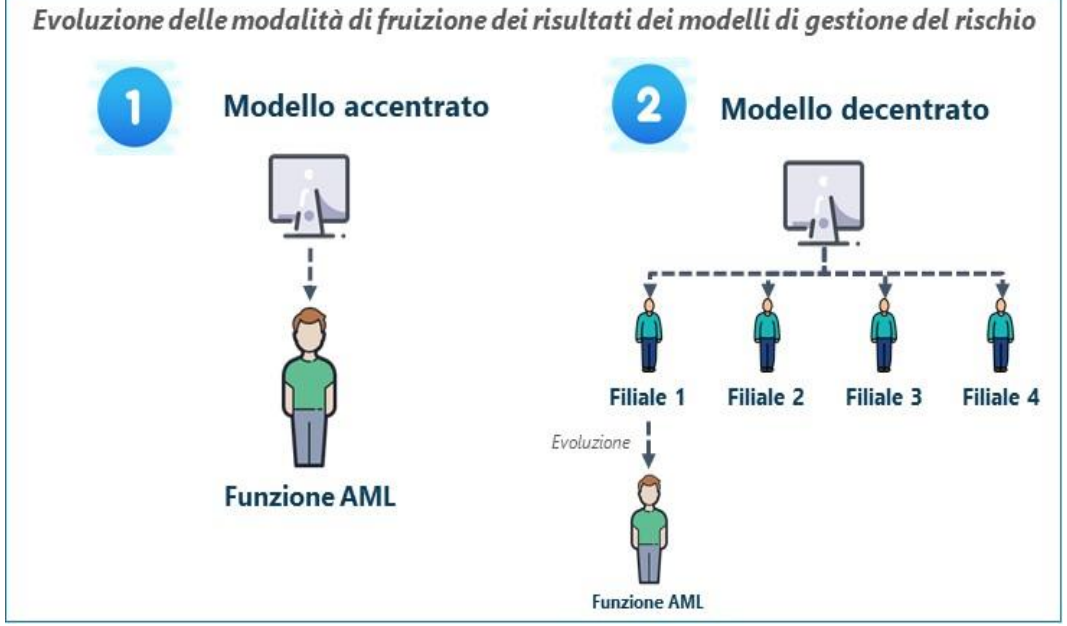
L’adozione di soluzioni di intelligenza artificiale e machine learning a supporto dei processi AML ed in particolare di risk profiling e detection dell’operatività sospetta comporta anche valutazioni di carattere organizzativo, sia nella fase di impianto e di manutenzione dei modelli, sia nella fase di consumo degli stessi:

Organizzazione e responsabilità

Impianto e manutenzione del modelli AI/ML



Consumo dei modelli (processi di monitoraggio/controllo)



System integration

Architettura target (applicativa e di gestione dei dati)

Una recente esperienza condotta presso un Gruppo Bancario Significant

Focus sul Modello di alert scoring: gli step seguiti per lo sviluppo del Modello

Use Case

1 Patrimonio informativo

- ✓ Predisposizione dati
- ✓ Definizione logicadegli indicatori
- ✓ Definizione dell'evento target (Output)

2 Analisi Esplorative

- ✓ Sviluppo DataFrame
- ✓ Features engineering
- ✓ Analisi di correlazione

3 Sviluppodel modello

- ✓ Imputazione e trasformazione delle variabili
- ✓ Scelta *champion model* e validazione delle statistiche di FIT e performance
- ✓ Analisi degli output e validazione dei risultati

Una recente esperienza condotta presso un Gruppo Bancario Significant

Use Case

Focus sul Modello di alert scoring: approccio di sviluppo adottato

L'applicazione di tecniche di AI deve essere chiaramente guidata dagli **obiettivi di business** ed allo stesso tempo dalla **disponibilità** e **qualità dei dati** opportunamente manipolati dagli algoritmi di **Machine Learning**. I modelli, interpretando i dati ed i loro collegamenti, supportano nell'individuazione di **fattispecie di rischio** anche non conosciute a priori e assegnando una valutazione *ad hoc*.

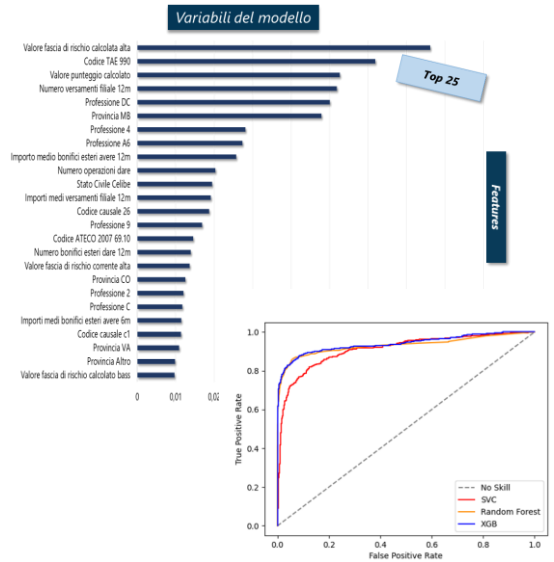
Caratteristiche del Modello di alert scoring

1	Informazioni	• Dati operatività transazionale e dati anagrafici • Dati indagini effettuate e dati filiale • AUI • …
2	Tecnologia	• Piattaforma analisi dati (Python) • Data visualization (Qlik,) • Work flow (utilizzo WF esistenti)
3	Metodo	• Data analytics • Text Analysis • Machine Learning
4	Benefici	• Identificazione delle potenziali SOS nell'ambito degli alert rilevati dalla soluzione in uso di transaction monitoring e riduzione del numero di falsi positivi mediante uno screening degli stessi • Efficientamento delle attività di valutazione e analisi dell'operatività sospetta mediante l'interfaccia di data visualization e l'analisi mediante il grafo • A tendere i modelli identificati **assimileranno** gli indicatori di anomalie di Banca d'Italia, monitorati dagli strumenti tradizionali

A Apprendimento non supervisionato (unsupervised learning)

«Riconosco strutture nei dati»

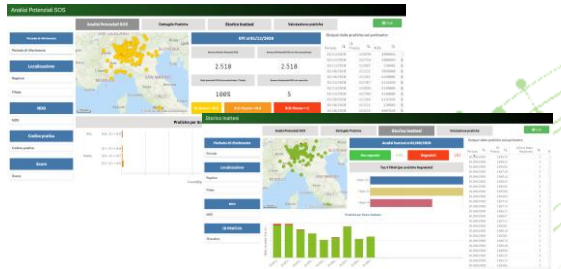
Applicazione del *clustering*, con l'obiettivo di **raggruppare** entità con caratteristiche **simili** all'interno dello stesso cluster. Schemi comuni si addenseranno al centro del cluster mentre, le **osservazioni anomale** (dette **outlier**) saranno più distanti andando a individuare delle eccezioni rispetto agli schemi ricorrenti. Il modello determinerà, sulla base del contenuto informativo analizzato, le **dimensioni** che caratterizzano i fenomeni AML e nell'**intersezione** che si creerà vi saranno le fattispecie atipiche su cui impostare determinati **gradi di rischio**.



B Apprendimento supervisionato (supervised learning)

«Riconosco connessioni che legano i dati rispetto ad uno specifico risultato»

L'algoritmo **apprende** mediante l'osservazione di fattispecie rilevate in passato e di effettive operazioni sospette: utilizzando dati storici "impara" a **valutare la potenziale rischiosità** di transazioni **future** assegnando *score* probabilistici e migliorando, di volta in volta, la capacità discriminatoria dell'intero modello



Una recente esperienza condotta presso un Gruppo Bancario Significant

Focus sul Modello di alert scoring: il patrimonio informativo considerato

1 Use Case

Partendo dai dati raccolti sull'operatività dei clienti e tenuto conto delle fattispecie ritenute più rischiose da parte della Funzione AML sono state identificate specifiche ***features*** opportunamente clusterizzate in **5** categorie, e delle quali si riportano alcuni esempi:

Categoria Features	*Dettaglio Esemplificativo Features*	*Totale feature*
Anagrafica cliente	*Sesso, Nazionalità, Data di Nascita, Stato Civile, Professione, Codice ATECO, etc..*	XX
Dettaglio Operazioni	*Importo totale, Causale, Codice Stato, Codice Divisa, Natura pratica, Importo totale contate, Tipologia soggetto, etc..*	XXX
Dettagli di natura finanziaria	*Importo Totale Bonifici Esteri, Numero Bonifici Esteri Dare a 3 mesi, Numero Prelievi, Importo Totale Versamenti, etc..*	XXX
Atri elementi di rischio	*Livello di Rischio Corrente, Tipologia PEP*	X
Variabile obiettivo	*Segnalato / da non segnalare*	1

l'attività di feature selection svolta ha mantenuto **1XX feature delle XXX feature totali**

- *Le variabili ottenute analiticamente dall'analisi del perimetro informativo sono state elaborate da un «**modello non supervisionato**», ovvero privo della variabile di output, al fine di suddividere il perimetro di soggetti in raggruppamenti omogeni*
- *Tramite questo processo si è ottenuta una nuova features, «**Cluster soggetti**», che sarà propedeutica all'analisi della popolazione, in quanto ogni gruppo fornirà un'indicazione del livello di rischio del soggetto che vi appartiene*

Ipotesi di analisi

- *Analisi dei gruppi finalizzata all'individuazione delle principali caratteristiche dei soggetti di appartenenza*
- *Attribuzione di un livello di Rischio a ciascun gruppo di soggetti*

Una recente esperienza condotta presso un Gruppo Bancario Significant

2 Use Case

Focus sul Modello di alert scoring: analisi esplorative (processo di individuazione delle principali variabili con particolare impatto sulla predizione dell'evento target)

Imputazione Missing Values

Sostituzione di valori *Missing* nella base dati:

- Interpretando da un punto di vista funzionale il significato della presenza di valori *missing*

Feature Selection

Selezione variabili significative da inserire nel modello finale, tramite due step:

- *Feature Selection* Iniziale:

Eliminazione delle variabili:
1. Duplicate
2. Collineari
3. Con bassa varianza

→ 1XX variabili selezionate

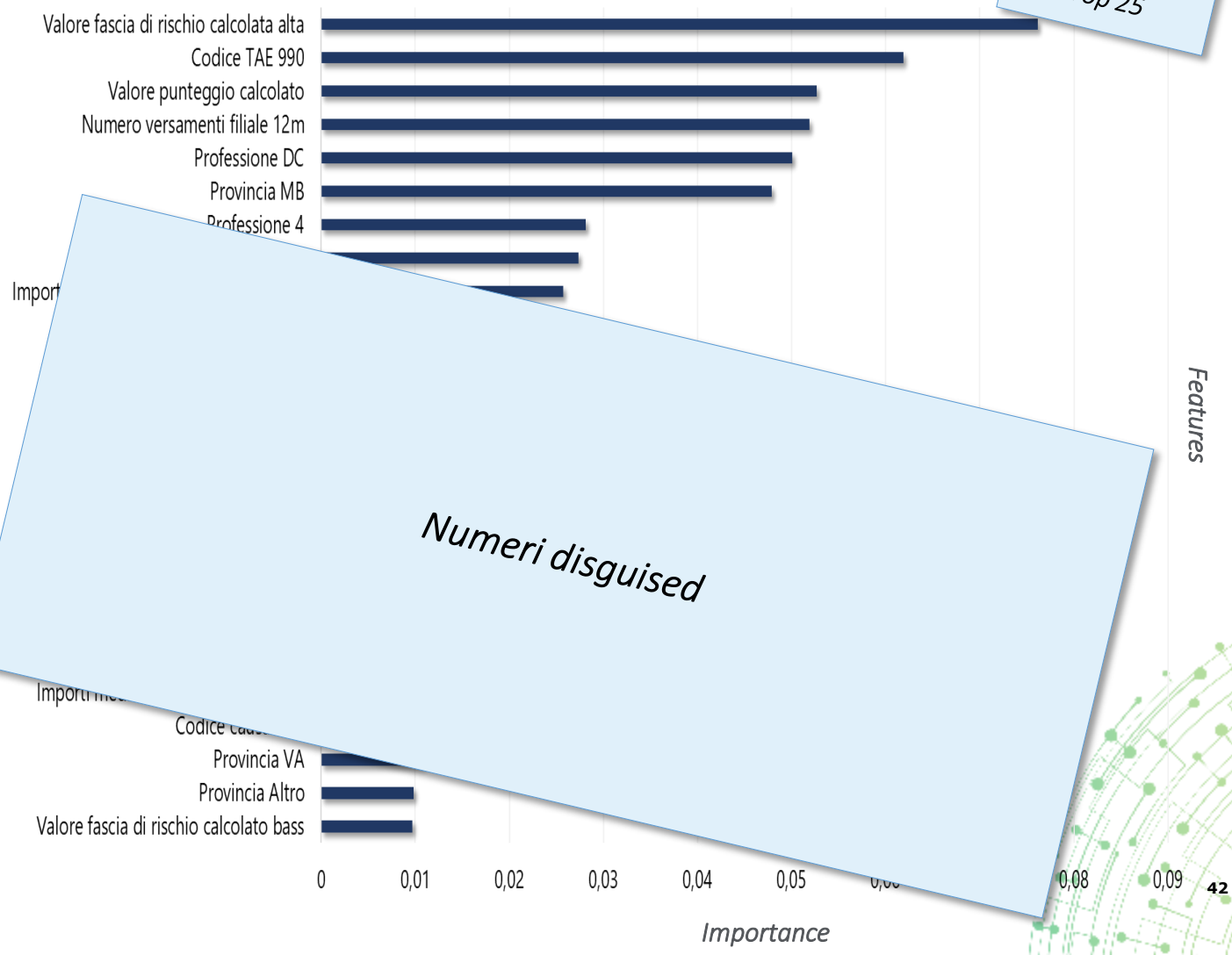
- *Feature Selection* basata su test univariati, in relazione alla variabile obiettivo

Processo implementato:
ANOVA per variabili quantitative
V di Cramer per variabili qualitative

→ XX variabili selezionate

Principali variabili del modello

Top 25



Numeri disguised

Una recente esperienza condotta presso un Gruppo Bancario Significant

Focus sul Modello di alert scoring: lo sviluppo del modello (approccio adottato e champion model)

Training & Testing del Modello

Perimetro temporale	
Periodo di osservazione	3 anni
Periodo di previsione	2 anni

Perimetro pratiche inattesi	
Pratiche segnalate	c.a. X %
Pratiche non segnalate	c.a. YY%
Pratiche totali	**100%**

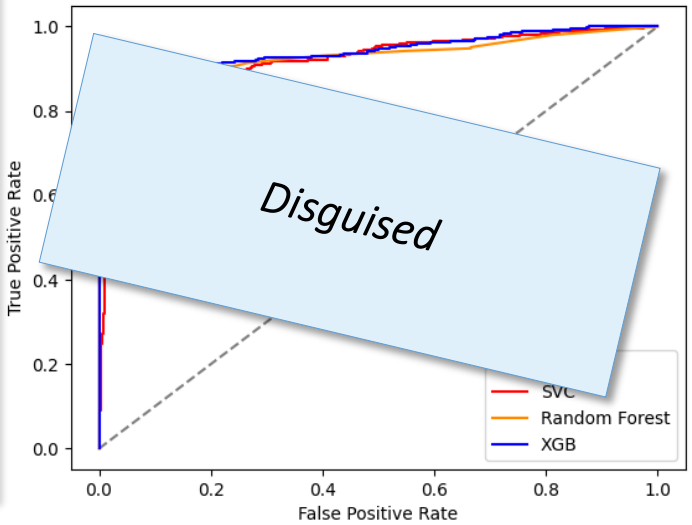
Suddivisione popolazione pratiche	
Popolazione pratiche in fase di training del modello	70%
Popolazione pratiche in fase di testing del modello	30%

Risultati applicazione modello

Algoritmi di machine learning utilizzati nell'analisi		
Support Vector Machine	Random Forest	XGBoost

Caratteristiche del champion model

Ensemble *(SVM, Random Forest e XGBoost)*
Accuratezza*: XX,yyy%*
Area under the ROC curve *(AUC): 0,yyy*
F1 Score*: 0,zzzz*



La ***curva ROC,*** descrive la capacità del modello di discriminare la classe delle pratiche positive, ovvero da segnalare, da quella negative, da non segnalare. L'area sottostante la curva idealmente dovrebbe essere pari a 1 per un modello perfettamente funzionante, quindi si può ritenere soddisfacente il valore di ***0,zzz*** ottenuto.

Una recente esperienza condotta presso un Gruppo Bancario Significant

Focus sul Modello di alert scoring: lo sviluppo del modello (risultanze finali)

3 Use Case

Si riportano di seguito gli ***score*** predetti dal modello sull'analisi degli inattesi svolta in fase di *testing* del modello

Livello di Rischio	Range di Probabilità	Numero di inattesi
Alto	Pr.> 80%	Z%
Medio	0,5 < Pr. < 0,8	X,Y%
Basso	Pr.< 0,5	+90%

Matrice di confusione

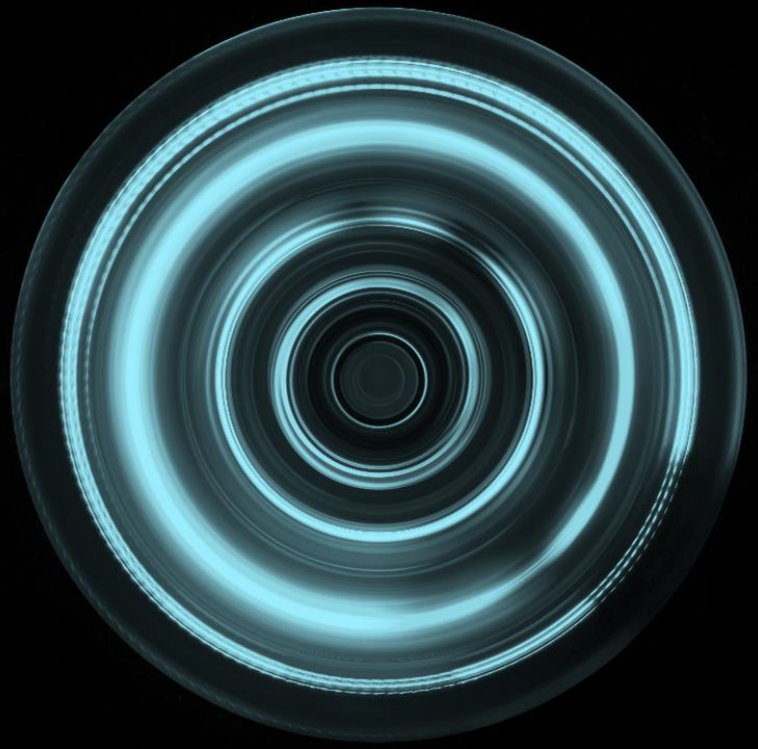
Etichetta prevista \ Etichetta effettiva	0	1
0	+90%	X%
1	Y%	Z%

Legenda

1- Inattesi diventati SOS

0 – Inattesi non segnalati

AGENDA



Evoluzione tecnologica a supporto dei processi AML e delle attività di controllo

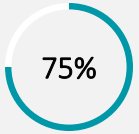
Verso un approccio olistico alle gestione dei «financial crime»

La fattispecie di rischio Antiriciclaggio rientra nella più ampia categoria dei rischi di Financial Crime

Fattispecie di rischio riconducibili nel perimetro del «Financial Crime»

Frode

Crimini, quali falsificazione, truffa di credito, che implichino il **raggiro** del **personale finanziario** o dei **servizi** al fine di commettere un **furto**

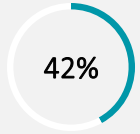


Evasione fiscale

Comportamenti attraverso i quali, vengono **violate norme** di legge allo **scopo** di eludere i propri obblighi, **non pagando** o **pagando meno tasse**

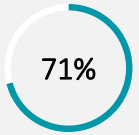
Finanziamento del terrorismo

Attività diretta alla **raccolta**, intermediazione, deposito, di **risorse economiche** per **finanziare** e sostenere **azioni** con finalità di **terrorismo**



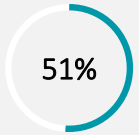
AML

Operazioni poste in essere al fine di **ostacolare** l'**identificazione** della **provenienza** di **denaro**, beni e altre utilità di **origine illecita**



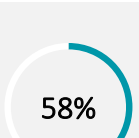
Furto

Attività finalizzate all'**impossessamento** di **beni** mobili **altrui** al fine di **trarne profitto**, quali utilizzo indebito di strumenti di pagamento



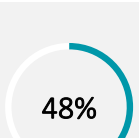
Corruzione

Accordi tra **soggetti**, tali per cui **un soggetto**, in **cambio** di **denaro** e/o **altri vantaggi agisce contro** i propri **doveri** e **obblighi**



Cyber-crime

Attività criminose caratterizzate dell'**abuso** di **componenti** della **tecnologia dell'informazione** – sia hardware che software –



*Fonte: "Innovation and the fight against Financial Crime", Refinitiv Report, 2019 - Appartenenza delle fattispecie di rischio al perimetro del financial crime per % di rispondenti -

Verso un approccio olistico alle gestione dei «financial crime»

Le Frodi, gli attacchi cyber ed altre tipologie di crimini finanziari sono favoriti da strumenti più accessibili che consentono attacchi sofisticati

Le diverse fattispecie di FC stanno evolvendo…

Crescente maturità del business criminale, con elevata disponibilità di armi informatiche all'avanguardia, muovendosi sempre di più verso un modello di crime-as-a-service

Aumento della complessità degli attacchi di financial crime, estendendosi a ed oltrepassando più domini, funzioni aziendali, organizzazioni e confini

Impatto dei singoli attacchi sempre più significativo, con elevate perdite finanziarie e di clientela, nonché notevoli conseguenze reputazionali, minacciando la fiducia vs istituzioni finanziarie

…come dimostrano alcuni dati relativi al settore FSI

~200 € Tariffa giornaliera per assumere un hacker	**~10 €** Costo di una carta di credito individuale
#177 Numero medio di gg per identificare un data breach	**#56** Numero medio di gg per contenere un data breach
0.5 Bln€ Costo max di fraud management tra le grandi banche UK	**4.6 Tln€** Costo stimato delle frodi a livello globale

Verso un approccio olistico alle gestione dei «financial crime»

L'esigenza di un approccio operativo olistico: i driver di evoluzione

- Il settore bancario ha l'esigenza di allontanarsi dai **tradizionali silos** che storicamente sono alla base di molte organizzazioni e di concentrarsi sull'adozione di un modello convergente che fornisca un approccio più efficace e integrato per proteggere, rilevare e rispondere alle moderne attività di criminalità finanziaria giornaliera

TECHNOLOGY DRIVEN	DATA CAPITALIZATION	SKILLS SINERGYES	PREDICTIVE INTELLIGENCE
			
Soluzioni che consentono la **ottimizzare i costi** attraverso l'**automazione** di **attività** , cercando al contempo modi per essere più **efficaci.** **Possibilità di sfruttare le medesime tecnologie nell'ambito del complessivo presidio dei finanziale crime**	**Sfruttamento di dati comuni** al fine di consentire una **visione globale del rischio** e un' affidabile **visione d'insieme** a **supporto** alle **strategie aziendali**, attraverso un **allineamento** con gli **obiettivi di performance aziendale**	**Sfruttamento di skills e competenze sinergiche** nell'ambito dell'**organizzazione aziendale**	Avere una **visione olistica** del **rischio** antiriciclaggio e della **compliance** utilizzando **analisi predittive** e **tecniche di apprendimento** per **identificare** e **prevenire tempestivamente** i **problemi** ed essere **efficaci** nelle **attività** di **monitoraggio continuo**

Rimuovere le barriere tra le funzioni aziendali coinvolte nella protezione dai crimini informatici e finanziari

Verso un approccio olistico alle gestione dei «financial crime»

I cambiamenti a livello di settore stanno affermando un approccio olistico, in grado di ottimizzare la gestione di attacchi cyber e di altri Financial Crime

As is

Responsabilità e competenze

- La responsabilità del rilevamento e della gestione degli attacchi è ripartita su diverse unità (Fraud, Cyber, AML, IA ...), ciascuna coinvolta in linea con le proprie competenze
- Assenza di flussi informativi e meccanismi di coronamento
- Carenza di skills analitici (AI, ML, ecc.)

Data & Tecnology

- I dati e le competenze necessarie per gestire i financial crime sono frammentati tra le diverse unità e entità legali all'interno del Gruppo
- Anche le tecnologie di risk profiling e di detection variano tra i diversi sylos e si basano su logiche diverse

Approcci

- Gli approcci di gestione dei financial crime sono differenziati all'interno della Banca, a seconda delle diverse attività delle Funzioni di Controllo
- Tali approcci seguono nella maggior parte approcci deterministici e logiche di controllo ex post

To be

1
- Sviluppo di **modelli organizzativi integrati** mediante l'accentramento di responsabilità o creazione di flussi informativi e meccanismi di coordinamento
- Far convergere **competenze eterogenee ma complementari**
- Sviluppare **centri operativi congiunti** per abilitare team integrati e aumentare l'efficacia nella gestione cross unit
- Focalizzarsi sulle giuste risorse integrando nell'organizzazione **data scientist** e specialisti in tecniche di machine learning e predictive analysis

2
- **Centralizzare la gestione dei dati** creando un unico luogo che agevoli l'identificazione di interconnessioni tra gli stessi
- Utilizzo delle **nuove tecnologie** e investimento in soluzioni innovative per automatizzare il rilevamento e la risposta agli attacchi financial crime
- Creare **sinergie di costo** nell'utilizzo delle medesime tecnologie tra le diverse unità

3
- Adottare tecniche di **advanced analytics e machine learning** per analizzare i dati in tempo reale e cercare relazioni non palesi con la finalità di aumentare la capacità di **rilevamento tempestivo di attacchi fraudolenti**
- Avviare **modelli di convergenza** più ampi attraverso Cyber-Fraud-AML

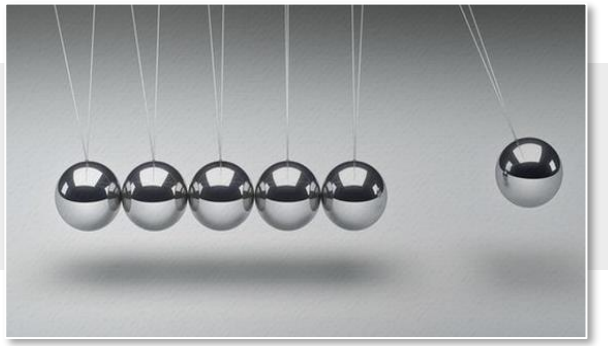
Verso un approccio olistico alle gestione dei «financial crime»

La maggior sfida è quella di integrare il proprio modello di presidi AML con un approccio predittivo, in grado di anticipare i Financial Crime

OGGI

Da un approccio stratificato e reattivo…

Reazione



- Catturare le perdite e identifica eventi passati quasi persi
- Sviluppare informazioni di base per quantificare l'impatto delle perdite dovute agli eventi
- Pianificare un report sullo stato dei rischi attuali e azioni correttive

DOMANI

…ad un approccio olistico e proattivo

Predizione

- Accumulare dati interni ed esterni in data lake condivisi per fornire avvisi di reporting quasi in tempo reale
- Utilizzare input reattivi e integrati per generare insight predittivi con metodologie di Advanced Analytics
- Consentire una descrizione accurata dell'esposizione fornendo una visione olistica dell'intera organizzazione, aumentando la collaborazione durante l'esecuzione di processi diversi

VANTAGGI

- Minimizzazione degli attacchi "riusciti“
- Risposte più rapide agli attacchi
- Riduzione delle perdite
- Modello di governance omni-globale
- Dati unificati disponibili per l'intera organizzazione
- Efficienza operativa e di processo

Un possibile approccio alla creazione di un framework olistico alla gestione dei financial crime

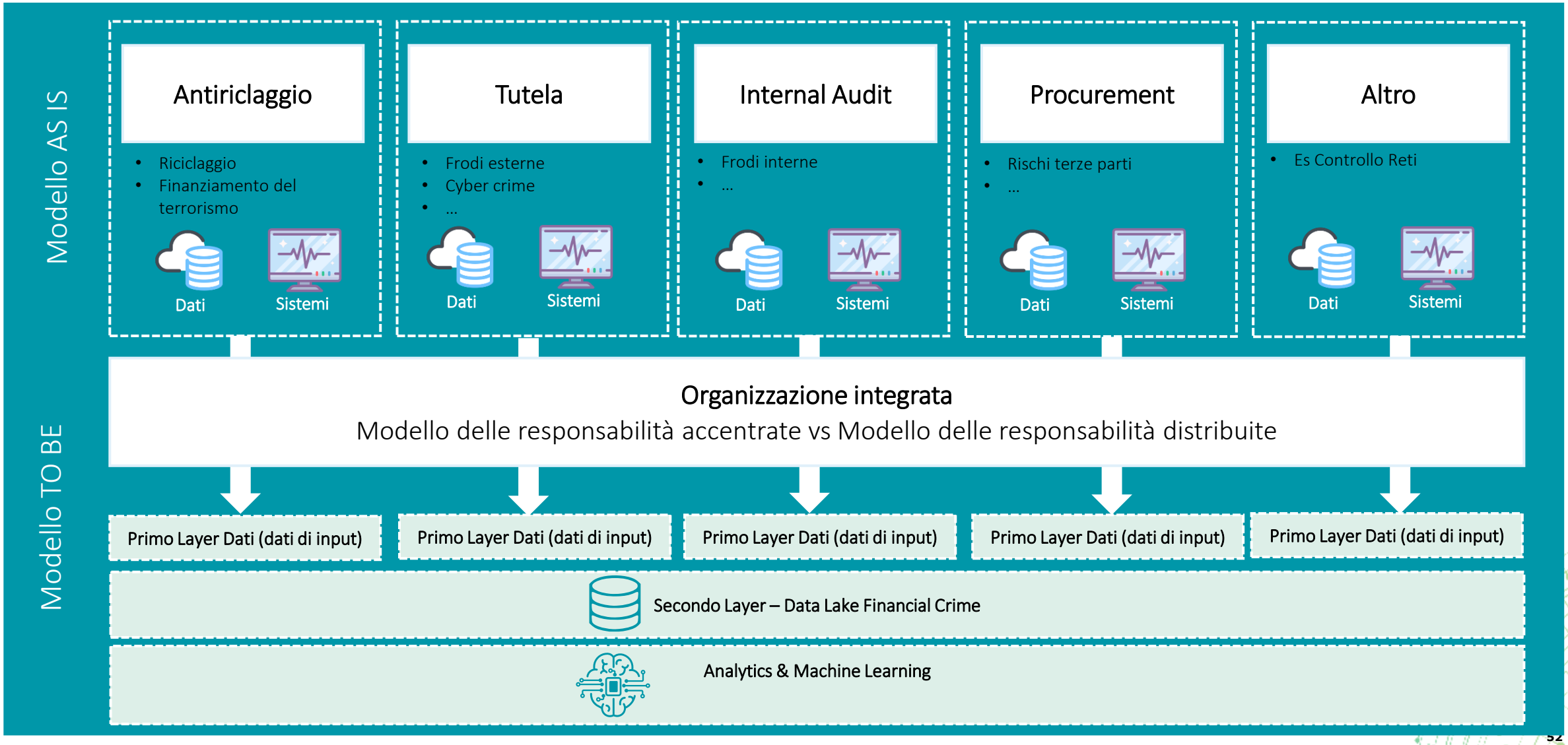
La vista complessiva sul percorso ipotizzato

	FASE 1 *Assessment funzionale e tecnologico*	*FASE 2* *Prima applicazione del modello olistico*	*FASE 3* *Estensione del modello olistico ed entrata a regime*
Obiettivi	Analizzare gli attuali assetti organizzativi operativi e tecnologici relativi ai «financial crime»	Prima applicazione in logica «laboratorio» dell'approccio olistico ad un ambito predefinito dei financial crime mediante lo sviluppo di un modello di Machine Learning	Estensione graduale del modello a tutte le altre fattispecie dei financial
Elapsed	~ 1,5 mesi	~ 2 mesi	*Variabile in base la perimetro ed estensione del Modello*
Macro-attività	• Identificazione fattispecie Financial Crime Gruppo Credem e creazione di una **tassonomia unica e condivisa** • Rilevazione Modello organizzativo/operativo AS IS: ✓ Ruoli e responsabilità delle diverse Funzioni tenute al presidio FC (AML, Tutela, IA, etc.); ✓ Processi operativi in essere ✓ Framework dati e soluzioni IT adottate da ciascuna Funzione • Definizione **linee guida modello TO BE e analisi costi benefici**: ✓ Modello organizzativo integrato ✓ Processi operativi integrati ✓ Modalità di integrazione framework dati (es. costruzione Data Lake Financial Crime) • Definizione **Execution Plan** per l'adozione graduale del Modello Olistico alla gestione dei Financial Crime	• Identificazione di **un ambito specifico dei Financial Crime** su cui implementare – secondo una logica di laboratorio – l'applicazione del Modello Olistico (es. frodi on line vs AML) • **Identificazione del patrimonio informativo e analisi esplorative**: predisposizione dati, sviluppo dataframe, feature engneering e feature selection, analisi di correlazione • **Sviluppo modello di machine learing:** Imputazione e trasformazione delle variabili; identificazione dei possibili modelli da utilizzare e training, scelta *champion model* e validazione delle statistiche e performance; Analisi degli output, testing del modello e validazione dei risultati *Il Modello di ML sarà in grado di identificare secondo logiche predittive fattispecie di rischio «comuni» mettendo a fattor comune analisi e a dati provenienti da diversi comparti*	• **Messa a terra del Modello organizzativo, operativo e del framework integrato dati e tecnologico** disegnato nella prima fase progettuale • Sulla base della **Road Map definita** graduale sviluppo dei Modelli di intelligenza artificiale in grado di estendere il modello di detection di tipo olistico a tutte le fattispecie dei Financial Crime

Un possibile approccio alla creazione di un framework olistico alla gestione dei financial crime

Prime considerazioni sulla configurazione del Modello olistico del Gruppo Credem

Illustrativo



Deloitte.