L'EVOLUZIONE DEI RISCHI DIGITALI TRA ECB STRESS TESTING E AI ACT: COSA CAMBIA NELLA GESTIONE DEI RISCHI

Nicasio Muscia, Managing Director
Accenture Strategy & Consulting

Martina Pettazzi, Manager
Accenture Strategy & Consulting

13 giugno 2024

accenture **RAIGHT** | Accenture for Responsible AI

AGENDA

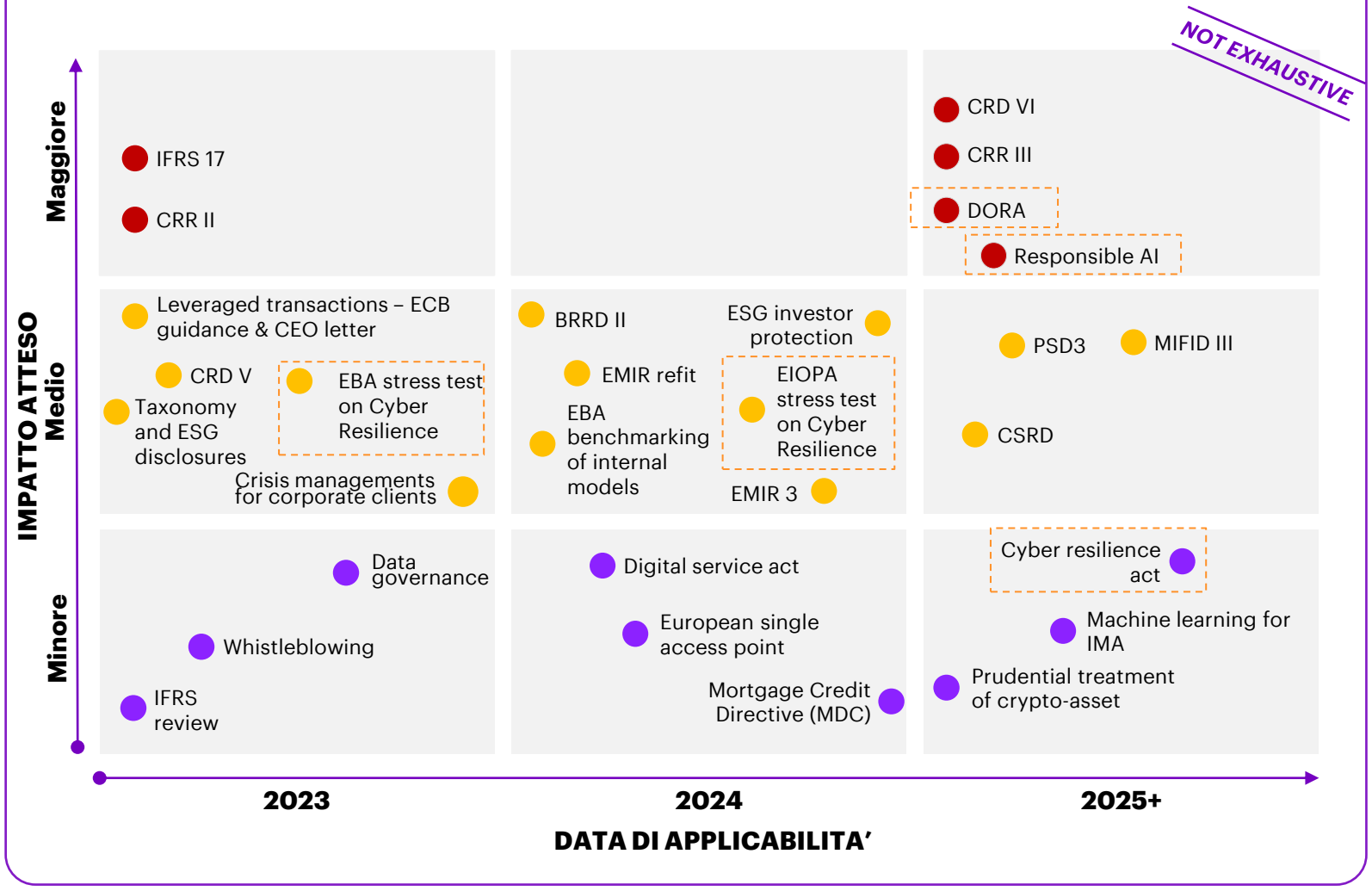
01 Contesto dei rischi digitali e le implicazioni dello stress test

02 L'evoluzione dei rischi alla luce del Regolamento sull'Intelligenza Artificiale

CONTESTO DEI RISCHI DIGITALI E LE IMPLICAZIONI DELLO STRESS TEST

PANORAMICA REGOLAMENTARE SEMPRE PIÙ SFIDANTE

REGOLAMENTAZIONI



PRINCIPALI TEMATICHE IN AMBITO DIGITAL RISK

- **DIGITAL OPERATIONAL RESILIENCE** (e.g., DORA)
- **RESPONSIBLE AI** (e.g., AI ACT)
- **THIRD-PARTY RISK MANAGEMENT** (e.g., DORA)
- **BCE STRESS TEST ON CYBER RESILIENCE**
- **EIOPA STRESS TEST ON CYBER RESILIENCE**

IMPATTO Maggiore Medio Minore

Rilevanti ai fini del Digital risk

CONTESTO DEI RISCHI DIGITALI E LE IMPLICAZIONI DELLO STRESS TEST
LA NORMATIVA E LE PRINCIPALI AREE DI IMPATTO

RUOLI E RESPONSABILITÀ — A

La normativa di riferimento porta alla necessità di **ripensare ai propri modelli di governance** e di **ridefinire i compiti** degli organi aziendali e i relativi profili di responsabilità. **In particolare:**

- Viene designata una **funzione ad Hoc** per la **gestione dei rischi digitali** all'interno della
- **Rafforzamento del ruolo** della funzione **Digital Risk** Management

Circ. 285 | ECB Stress Test | DORA | EIOPA Stress Test | AI Act

RISK APPETITE FRAMEWORK — B

La gestione del rischio digitale deve essere effettuata in **linea con la propensione al rischio** dell'Organizzazione. In tale contesto la normativa delinea i seguenti requisiti:

- **definire gli obiettivi di controllo ICT e di sicurezza**
- **sviluppare specifiche metriche di KRI e KPI**
- **monitorare gli indicatori** sulla base di specifiche soglie in concerto con la propria **propensione al rischio**

Circ. 285 | ECB Stress Test | DORA | EIOPA Stress Test | AI Act

QUANTIFICAZIONE DEL RISCHIO DIGITALE (CYBER & ICT) — C

La normativa di riferimento richiede una **valutazione del rischio digitale** basata su una serie di scenari che possano misurare e valutare la **resilienza operativa dell'Organizzazione**. In tale contesto:

- È necessario **sviluppare un modello di quantificazione *scenario-based*** del rischio digitale (Cyber e ICT)
- **Aggiornare periodicamente le valutazioni** in caso di ogni cambiamento ICT significativo
- Definire una corretta ed esaustiva **reportistica**

Circ. 285 | ECB Stress Test | DORA | EIOPA Stress Test | AI Act

INTELLIGENZA ARTIFICIALE RESPONSABILE — D

Il nuovo Regolamento sull'IA prevede una **classificazione dei Sistemi di IA** sulla base del rischio **e relativi requisiti e obblighi** per accedere al mercato dell'UE. In tale contesto è necessario:

- Definire la **Governance dell'AI** (ruoli e responsabilità)
- Mappare e **censire i Sistemi di IA**
- **Classificare** i Sistemi di AI **ed effettuare il Risk Assessment**
- **Definire regole e strumenti** per una IA responsabile (trasparenza, *fairness,* spiegabilità e sorveglianza umana)
- Sviluppare un framework di **controlli di I e II livello**

Circ. 285 | ECB Stress Test | DORA | EIOPA Stress Test | AI Act

CONTESTO DEI RISCHI DIGITALI E LE IMPLICAZIONI DELLO STRESS TEST

ECB STRESS TEST – STUDIO ACCENTURE

VARIABILI E CATEGORIE D'IMPATTO ECONOMICO

SCENARIO ECB

La BCE ha fornito uno scenario fittizio per cui l'integrità del database del sistema bancario principale è stata violata. Tutte le **misure preventive** sono state **eluse** o hanno fallito. Il **recupero dei dati** è necessario. Ad ogni modo non è stata ricevuta alcuna richiesta di riscatto

STORYLINE

L'attacco è perpretrato da un **dipendente** dell'Organizzazione che imposta una **chiave di crittografia** sul DB del sistema Core della Banca. Quetso porta ad un fallimento del **sistema di autenticazione** agli account dell' amministratore nel DB. Ad ogno modo viene confermato che i DB sono attivi e funzionanti. Una notizia relativa agli incidenti di sicurezza informatica è pubblicata su media affidabili

VARIABILI DRIVER

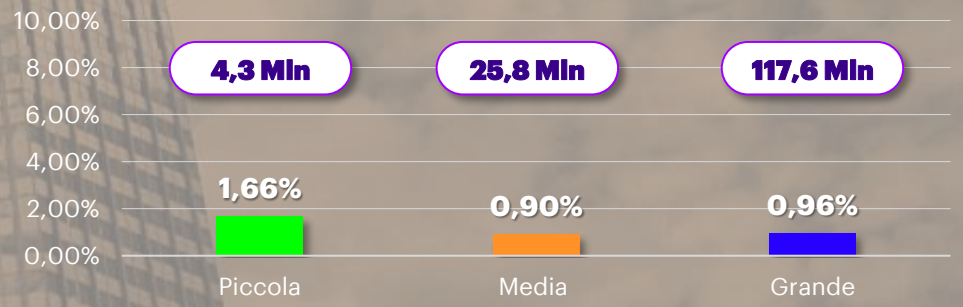
- **Banca di PICCOLE DIMENSIONI :**
  +1,9 Mln numero di clienti
  +260 Mln di Risultato Operativo
- **Banca di MEDIE DIMENSIONI:**
  +5 Mln numero di clienti
  +1,76 B di Risultato Operativo
- **Banca e di GRANDI DIMENSIONI:**
  +10,3 Mln numero di clienti
  +12,2 B di Risultato Operativo

CATEGORIE D' IMPATTO ECONOMICO ANALIZZATE

- AZIONE LEGALE
- SANZIONI
- ASSET REMEDIATION E COSTI OPERATIVI
- RIMBORSO AI CLIENTI
- PERDITA NUOVO BUSINESS
- DANNI REPUTAZIONALI SUI RICAVI
- STRATEGIA DI RECUPERO REPUTAZIONALE

RISULTATI

Esposizione ECB / Risultato Operativo



Esposizione ECB / N° Clienti

Dal rapporto tra l'esposizione al rischio cyber emerge che le banche, a parità di condizioni di business, risultano avere proporzionalmente alla loro dimensione un esposizione al rischio pressoché simile in termini di scenario ECB stress test. Dall'altro canto, si nota una riduzione dell'impatto in funzione alla dimensione dell'organizzazione (per effetto della riduzione dei costi variabili su grande scala)

CONTESTO DEI RISCHI DIGITALI E LE IMPLICAZIONI DELLO STRESS TEST

PRINCIPALI SFIDE E PUNTI DI ATTENZIONE EMERSI SULL'UTILIZZO DI MODELLI QUANTITATIVI

PRINCIPALI SFIDE & PUNTI DI ATTENZIONE

- NECESSITA' DI EVOLVERE MODELLI QUALITATIVI VERSO APPROCCI QUANTITATIVI IN GRADO DI FORNIRE INFORMAZIONI UTILI A PRIORITIZZARE SCELTE STRATEGICHE E DI BUSINESS
- DIFFICOLTA' OGGETTIVA NEL REPERIRE E AD ACCEDERE AI DATI NECESSARIE ALLA MISURAZIONE DEL RISCHIO (E.G., INCIDENTI, CLIENTI IMPATTATI, COSTI LEGALI,..)
- COMPLESSITA' NELL'AVERE UNA VISIONE OLISTICA DEL RISCHIO DIGITALE PROVENIENTE DA DIVERSE FONTI (E.G., CLOUD, ARTIFICIAL INTELLIGENCE…)
- NECESSITA' DI SVILUPPARE TOOL E SISTEMI CHE POSSANO SUPPORTARE L'ORGANIZZAZIONE NEL MONITORAGGIO 'REAL TIME' DEL RISCHIO

L'EVOLUZIONE DEI RISCHI ALLA LUCE DELL'AI ACT
IL REGOLAMENTO IN SINTESI

L'AI Act disciplina l'IA sviluppata o impiegata nell'UE, e i diritti e i doveri dei principali player internazionali

Timeline:

- **8 Dicembre, 2023**
  Accordo politico sulle questioni aperte
- **11 Dicembre, 2023 - Gennaio 2024**
  Incontri tecnici per finalizzare il testo
- **13 Marzo 2024**
  Testo finale votato dal Parlamento Europeo
- **21 Maggio 2024**
  Via libera definitivo da Commissione UE
- **Dicembre 2024 - Giugno 2026***
  Il Regolamento viene applicato sul mercato

**June 2027 for Medical Devices*

Sintesi

Categoria di rischio	Esempi illustrativi	Obblighi	Tempi di applicazione	Sanzioni
Inaccettabile	• Social scoring • Identificaz. biometrica real-time • Riconoscimento delle emozioni in ambito educativo e lavorativo (con eccezioni	Vietato	**6 mesi**	35 milioni di euro o il 7% del fatturato annuo globale
Alto Rischio	• Credit scoring • Sistemi di sicurezza energetica • Modelli di previsione delle malattie • Quantificazione delle immagini mediche • Sicurezza dei prodotti (ad es. giocattoli, aviazione, dispositivi medici e veicoli) • Gestione del capitale umano (incluso il reclutamento) • Modello di fondazione/GPAI con formazione > 10^25 FLOP	• Valutazione dell'impatto e della conformità dei diritti fondamentali • Sistema di gestione del rischio e della qualità • Registrazione nel database pubblico • Trasparenza, supervisione umana, accuratezza, robustezza e sicurezza informatica • Governance dei dati • Documentazione e conservazione dei dati	**24 mesi** **12 mesi** per l'uso Generico di AI**	15 milioni di euro o il 3% del fatturato annuo globale
Rischio Limitato	• Motore per il suggerimento di prodotti e servizi • Chatbot per i clienti • Modelli di fondazione / GPAI con formazione < 10^25 FLOP	• Avvisi di trasparenza		7,5 milioni di euro o l'1,5% del fatturato globale annuo
Rischio Minimo	• Filtri antispam per le e-mail • Videogiochi abilitati all'intelligenza artificiale	• Codice di condotta volontario		

** La legge si concentra sui casi d'uso, ma l'IA per «General Purpose» e i Foundation Model ad alta potenza di calcolo saranno considerati «modelli GPAI ad alto impatto con rischio sistemico» e avranno obblighi simili a quelli dei sistemi ad alto rischio, con una tempistica di applicazione accelerata di 12 mesi..

INIZIATIVE E STANDARDS

AI-PACT, la **comunità europea** degli attori chiave, mira a condividere le *best practice* e ad **aumentare la consapevolezza** sui principi dell'IA.

Standard ISO per **certificare la conformità della gestione dei sistemi di intelligenza artificiale.**

L'EVOLUZIONE DEI RISCHI ALLA LUCE DELL'AI ACT
VALUTAZIONE DEL RISCHIO DURANTE IL TUTTO IL CICLO DI VITA DEL SISTEMA DI IA

Definizione libreria dei Rischi

- Definizione/ integrazione della **Libreria dei Rischi** in modo da tenere conto dei **rischi specifici legati ai Sistemi di Intelligenza Artificiale** (es. rischio di mancata trasparenza, spiegabilità, equità, etc.)

AI Risk Assessment

- Conduzione dell'**AI Risk Assessment** con l'obiettivo di valutare la rischiosità del Sistema di Intelligenza Artificiale
- Conduzione di **analisi di scenario** per consolidamento impatti

Monitoraggio nel continuo

- **Monitoraggio nel continuo successivo all'entrata in produzione** del Sistema di Intelligenza Artificiale con opportuni KRI e relative metriche

L'EVOLUZIONE DEI RISCHI ALLA LUCE DELL'AI ACT
LIBRERIA DEI RISCHI (1/2)

Il sistema di AI deve essere analizzato tenendo in considerazione tutti i rischi collegati, contenuti in normative e standard di riferimento (*CoSO framework, ISO/ IEC 42001, ISO 23894 IT — AI — Guidance on risk management*)

ENTERPRISE RISK MAP

ILLUSTRATIVE

BUSINESS CONTINUITY

STRATEGIC RISK

STRATEGY

- Strategic Planning
- Misalignment Between Internal Functions
- M&A valuation and pricing
- Investor & Business Relations
- Image and brand reputation
- New products development
- Competition and demand

GOVERNANCE & ORGANIZATION

- Organizational structure
- Project Management
- Reporting Reliability
- Employee Relations
- Control & Supervision
- Management Performance

FINANCIAL RISK

MARKET RISK

- Commodity/ CO2 Price Risk
- Financial Instruments
- Interest rate volatility
- Equity Risk
- Foreign Currency Volatility

LIQUIDITY

- Liquidity management
- Funding/ Debit
- Counterparty solvency
- Cash management

CREDIT RISK

- Counterparty Risk

OPERATIONAL RISK

OPERATION RISKS

- Production Risk
- Sales Process Risk
- Distribution Risk
- Supply Chain Risk
- Sourcing Risk
- IT Systems Risk
- Security Risk
- Industrial Accident
- Health & People Risks
- Information Security Risk

EXTERNAL RISK

- Country / Area Risk
- Environment & Natural Disaster
- Industrial Disaster
- External Fraud

COMPLIANCE RISK

LEGAL & COMPLIANCE RISKS

- Intellectual Property protection
- Product Liability
- Pricing of products/ services provided
- Contracts Management
- Internal Procedures Violation

EXTERNAL REGULATION

- Country/state/local regulation
- Industry specific regulation
- Market regulation

Rischi legati all'AI

L'EVOLUZIONE DEI RISCHI ALLA LUCE DELL'AI ACT
LIBRERIA DEI RISCHI (2/2)

ILLUSTRATIVE

Possibile riconduzione del CoSO framework con rischi complessivi AI definiti in standard ISO

Fonte: **CoSO framework**			Fonte: **ISO 23894** (IT — AI — Guidance on risk management)
Level 1	**Level 2**	**Level 3**	**Level 4**
Rischio strategico	Strategic	Image and brand reputation risk	ENVIRONMENTAL IMPACT
	Governance and organization	Organisational structure risk	ACCOUNTABILITY
		Control and supervision risk	HUMAN OVERSIGHT
			MANTAINABILITY
Rischio Operativo	Operation risk	IT system risk	SECURITY
			ROBUSTNESS
		Health & people risk	FAIRNESS
			SAFETY
		Information security risk	TRASPARENCY & EXPLAINABILITY
			AVAILABILITY AND QUALITY OF TRAINING AND TEST DATA
		Business Continuity	AI EXPERTISE
Rischio di Compliance	Legal & Compliance risk	Intellectual Property protection	PRIVACY
		Contracts Management	
	External regulation	Country/state/local regulation	

L'EVOLUZIONE DEI RISCHI ALLA LUCE DELL'AI ACT
AI GOVERNANCE: PANORAMICA DI PROCESSO

È necessario definire un **sistema di governance con ruoli e responsabilità chiari**, regolati da specifici meccanismi di *escalation* sia a livello di Gruppo che di Paese, al fine di definire, coordinare e monitorare l'implementazione dei requisiti

GOVERNANCE

Team Centrale

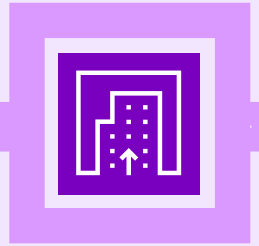
- Supervisiona la **definizione e l'implementazione del modello** di governance dell'IA
- Definisce, **guida e aggiorna il modello di governance dell'IA**
- Supporta e supervisiona l'implementazione del modello di governance dell'IA **monitorandone le prestazioni**

Business Units

- **Implementa, guida, coordina e monitora il modello di governance dell'IA locale** definito dal Team Centrale per raggiungere gli obiettivi di performance stabiliti
- **Garantisce la conformità al modello di governance dell'IA** nel suo dominio funzionale
- **Fornisce al Team Centrale informazioni, evidenze e documenti esaustivi e tempestivi** richiesti dalla regolamentazione interna per tutte le iniziative di IA nel suo perimetro

PROCESSO

AI IMPLEMENTATION ASSESSMENT



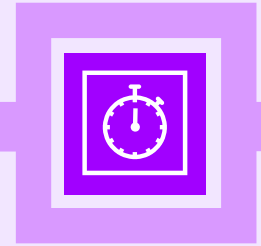
Valutazione della corretta implementazione di ogni iniziative AI

AI RISKS ASSESSMENT

Focus Next Slide

Esecuzione di una valutazione dedicata dei rischi dell'IA per ciascuna iniziativa di IA

AI MONITORING SYSTEM



Monitoraggio delle iniziative e relativi processi

L'intero processo di Governance dell'IA si basa su un **Inventario degli Asset** che consente il corretto monitoraggio di tutte le iniziative di IA e delle relative prestazioni

REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE (AI ACT)
ESEMPIO CO-PILOT

CONTESTO

1. In corso **progetto pilota per l'utilizzo di Co-pilot**
2. Effettuata **informativa preventiva** verso il sindacato
3. Valutato che il ricorso a Microsoft rappresenta un'**esternalizzazione di Funzione Essenziale o Importante** (FEI), con approvazione in capo al Consiglio di Amministrazione (pratica considerata OMR – Operazione di Maggior Rilievo)
4. Coinvolte tutte le strutture validatrici nella creazione del **parere finale** su utilizzo di Co-pilot (Risk, Privacy, Compliance, Legal, Cybersecurity)

...PRINCIPALI EVIDENZE EMERSE

CLASSIFICAZIONE

- Co-pilot è classificato:
  - in base all'**AI Act**, come sistema di AI **non ad alto rischio, con obblighi di informativa**;
  - in base al **risk assessment**, con **rischio potenziale alto**

AZIONI DI MITIGAZIONE

- Individuate diverse **azioni di mitigazione del rischio**:
  - Riduzione del rischio di produzione di informazioni errate, fuorvianti, improprie grazie al fatto che il patrimonio informativo di riferimento per l'AI è circoscritto alla knowledge base dell'Organizzazione, senza possibilità di interazione (in entrata ed in uscita) con basi informative esterne;
  - Riduzione del rischio legato all'utilizzo non consapevole dell'AI, grazie all'attivazione dei servizi di AI non automatica, ma solo su richiesta dell'utente
  - Riduzione del rischio di utilizzo improprio dei risultati prodotti, grazie all'introduzione del principio «Human in the Loop»: i risultati prodotti dall'AI non possono essere trasmessi direttamente all'esterno dell'Organizzazione; è in capo agli utenti della Banca una valutazione critica dei risultati generati dall'AI (appropriatezza, pertinenza, coerenza).- cd. «accountability»