AI e Cyber Risk.
L'ORM è morto.
Lunga vita all'ORM

Le nuove sfide dell'Operational Risk Manager alla luce dei nuovi rischi AI e Cyber

Le richieste all'ORM sono tante e su vari ambiti

Rischio Frodi esterne

Rischio ESG

Rischi IT

Rischi da eventi esterni

Rischio Frodi interne

Rischio interruzioni dell'operatività

Rischi da prodotti e servizi effettuati

Rischio Esternalizzazioni

Rischio salute e sicurezza sul lavoro

Rischi reputazionali

Rischi GDPR

Rischio di processo

Rischi professionali verso clienti

Vediamo come si è trasformato adattandosi negli anni

1) Il ruolo

3) I sistemi

2) La metodologia

Ruolo

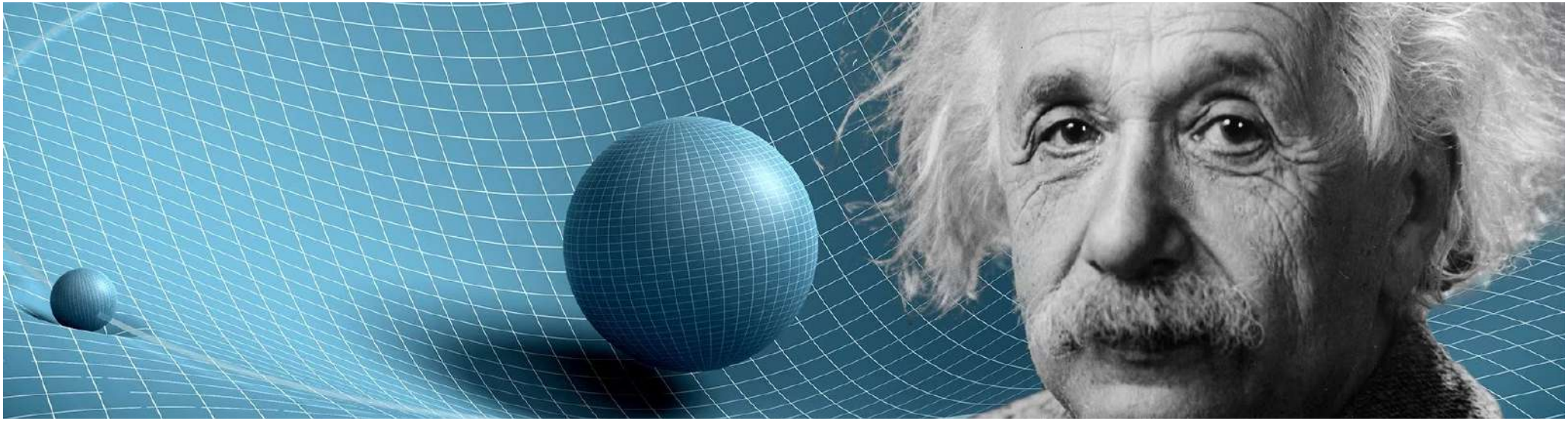
Da Specialista di uno specifico Rischio

Esperto nella gestione del Rischio Operativo per distinguersi dall' esperto nella gestione del Rischio di Credito o di Mercato

Tuttologo

Esperto nella gestione Rischi Operativi, Rischi Informatici, Varie normative, Data Protection, Rischi Reputazionali, ESG …

Ruolo



Da esperto in modelli statistici matematici

Analisi Quantitative e statistiche su serie di LDC, Quantili, Modello Montecarlo, analisi impatto economico.

A esperto di processi,, controlli e normative

Analisi qualitative, funzione di controllo, Risk Assessment, RAF, Pareri di impatto sui processi e sistemi, analisi normative specifiche …

Sistemi

Da Sistema per la gestione di LDC e ORSA

Sistema per la raccolta anche sofisticata di eventi di Perdita, categorizzazione rischi e workflow per determinazione impatto, Analisi statistiche e Risk Assessment.

A governance e integrazione rischi

Sistema per la governance di rischi diversi, Piani di azione, Cruscotti informativi, Integrazione analisi di rischi diversi.

Sistemi

Dalla fragilità di una gestione su Excel

Prassi flessibile e veloce della gestione su Excel per la raccolta di informazioni e reportistiche varie

A affidabilità di un Sistema di GRC

Sistema sicuro e affidabile, che permette la ricostruzione delle desioni, l'analisi di grandi moli di dati, la raccolta strutturata delle informazioni in workflow e assessment distribuiti

Metodologia

Dal Risk Assessment

Analisi statica della rischiosità di processi Ex-post. Focalizzazione sugli eventi storici e sugli assessment. Classificazione e mappatura sui processi. Valutazione efficacia dei controlli. Decisione su accettabilità del rischio.

Al Risk Management

Creazione di cruscotti di monitoraggio di indicatori di rischio predittivo KRI, Valutazione di soglie per far scattare allarmi. Analisi ex-ante. Individuazione e gestione dei piani di azione di mitigazione.

Metodologia

Dall’analisi degli impatti economici

Analisi di ogni singolo evento con particolare enfasi sugli impatti economici contabili e su classificazione e collocazione nei processi dell’evento.

All’analisi delle cause e integrazione con altri rischi

Focus su fattori di rischio e integrazione con altri ambiti di rischio (Asset IT, Adempimenti normative, Rischi reputazionali, Data Protection, Informazioni reclami)

Il Ruolo e la Metodologia RO vengono attaccati da molti fronti

Sembra che abbiano resistito. Si sono adattati, cambiano le armi e strategie ma il castello e le fondamenta reggono l'urto. Sono salvi. Ma …

Due nuovi guerrieri sembrano però dare il colpo di grazia al castello

Cyber risk

AI Act

Cyber Risk

Cyber Risk rientra a pieno titolo nell'ambito dell'ORM

Ruolo

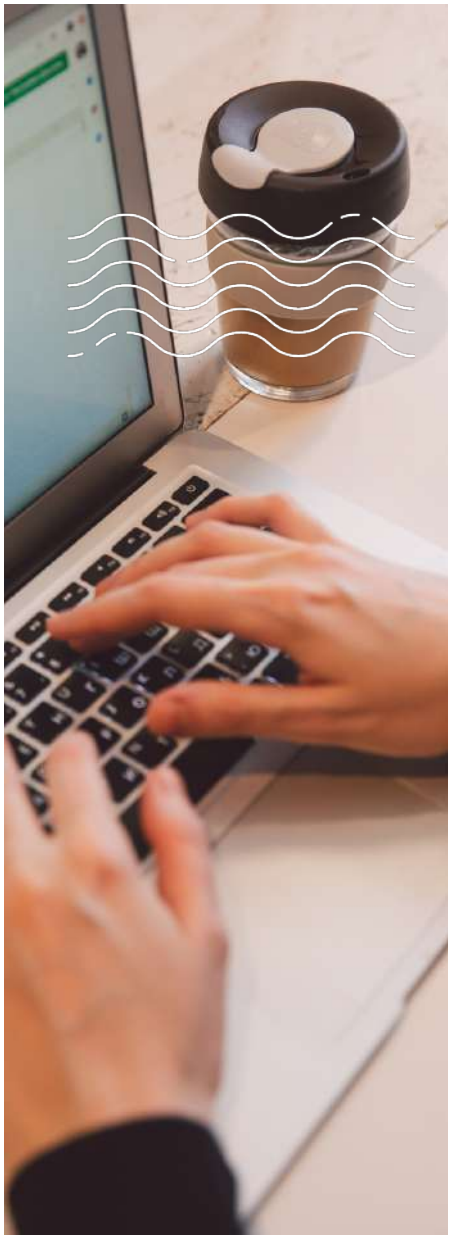
C'è un problema di formazione tecnica, di linguaggio, di esperienza. Difficile trovare e mantenere risorse tecniche formate

Sistemi

Sicuramente dà il colpo di grazia alla prassi di gestire I rischi IT con qualche Sistema semplice di Asset Catalog assieme a fogli excel.

Metodologia

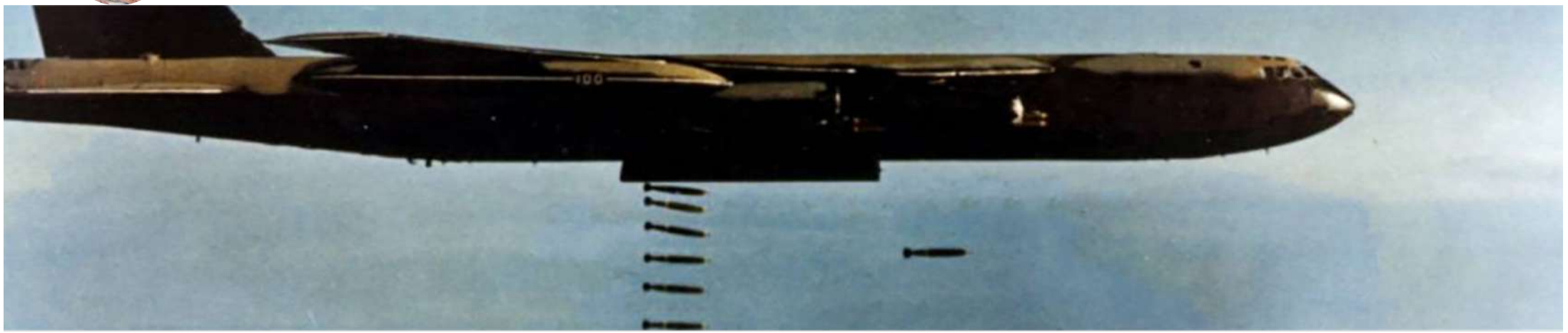
Da un punto di vista metodologico mette a dura prova I modelli di calcolo e di gestione dell'ORM



Nel modello Cyber ha ancora senso parlare di probabilità?

Se esiste una vulnerabilità dove credete che si concentrerà il nemico?

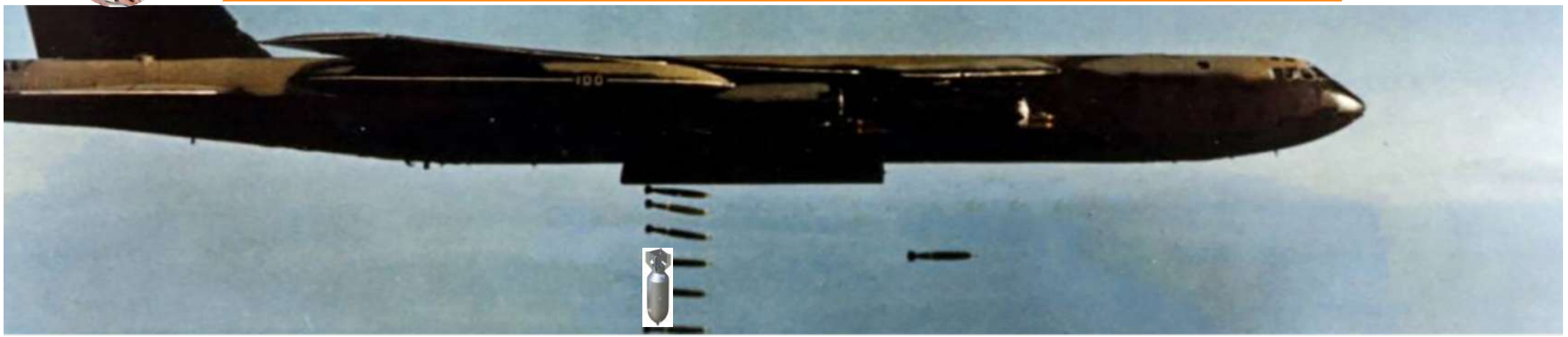
Metodologia



$$\text{Rischio(e)} = p(e) \times v.eco(e) \times (1 - Eff.Contr(e))$$

Augeos

Metodologia



cade l’attenzione sulla valutazione della probabilità di accadimento. Questo non è un fatto da poco se pensate all’enfasi data alle tecniche statistiche degli anni passati

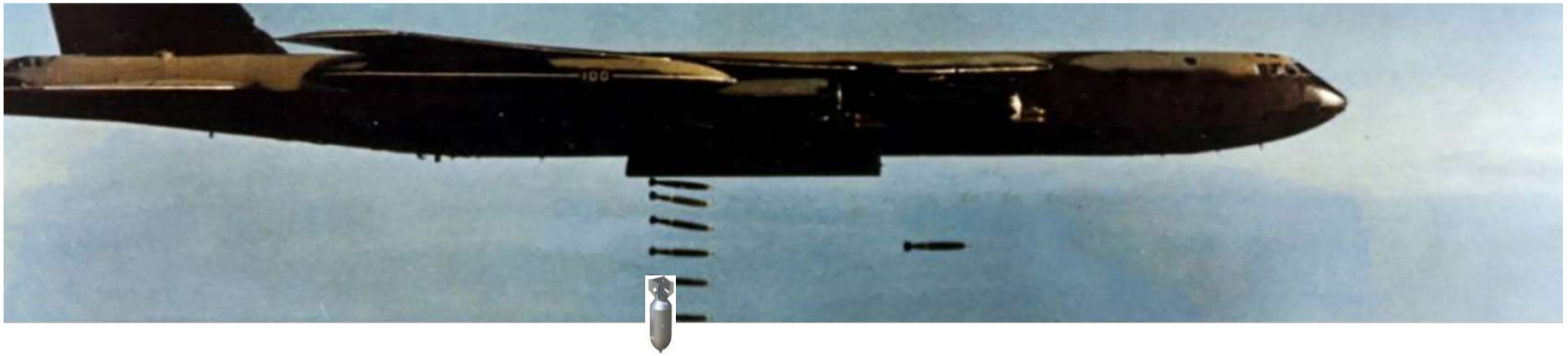
$$\text{Rischio(e)} = p(e) \times v.eco(e) \times (1 - Eff.Contr(e))$$

Augeos

In un evento di continuità operativa ha ancora senso parlare di valore economico?

Esiste un criterio di accettabilità stile RAF per eventi di continuità operativa?

Metodologia



Diminuisce l'attenzione sulla valutazione economica di un evento critico di continuità operativa a favore dell'impatto di business.

$$\text{Rischio(e)} = 1 \times v.econ(e) \times (1 - Eff.Contr(e))$$

Augeos

AI Act

I rischi AI rientrano a pieno titolo nell'ambito dell'ORM

Ruolo

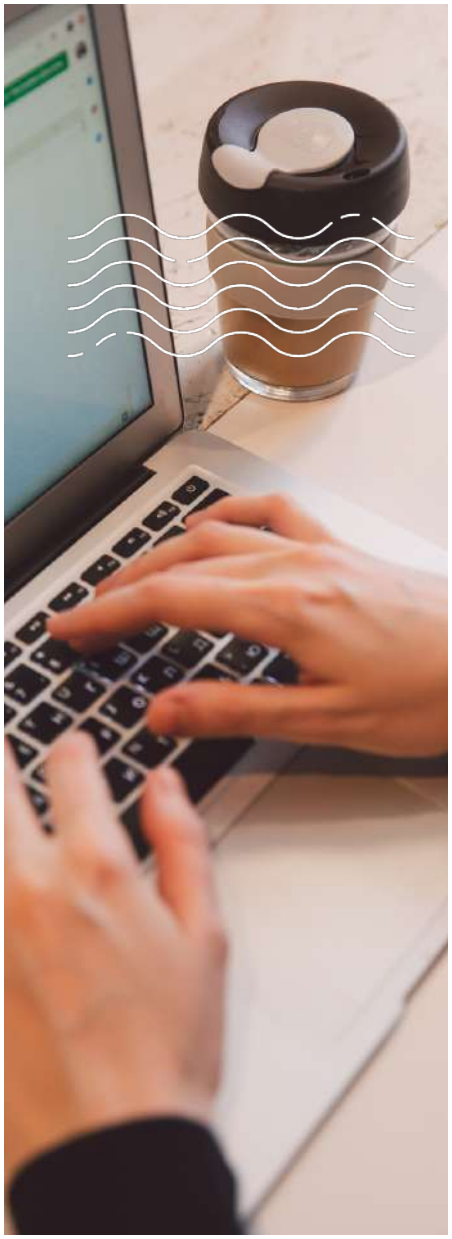
C'è un problema di formazione tecnica, di linguaggio, di esperienza ma anche di un cambio fondamentale nel ruolo organizzativo.

Sistemi

Analoghe considerazioni del Cyber Risk

Metodologia

Da un punto di vista metodologico il punto di attenzione è la focalizzazione sul rischio dei prodotti



AI Act

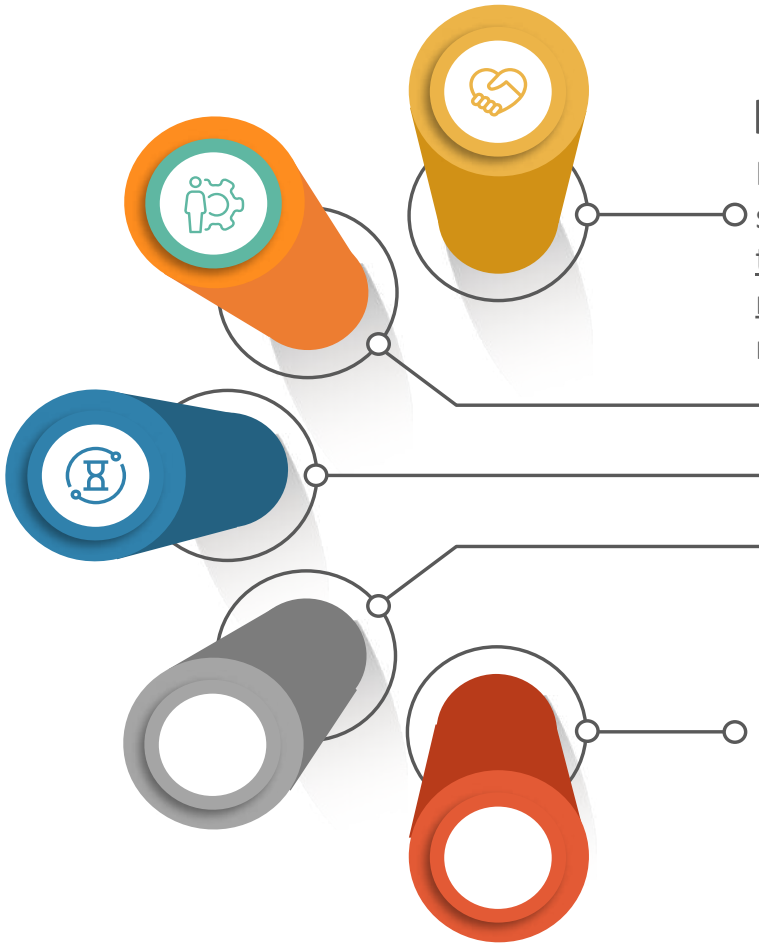
La specificità è che si pone **molto di più l'attenzione sul prodotto** che fa uso di sistemi AI ad alto rischio

Questo implica che le banche

- qualora sviluppino sistemi AI ad alto rischio devono avviare i processi usuali di governance interna tra cui quelli della valutazione dei rischi
- ma devono anche accertarsi che **ogni sistema ad alto rischio** (secondo la definizione dell'allegato alla norma) e quindi a titolo di esempio anche **i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito,** che decidono di immettere sul mercato risponda a tutti i requisiti previsti. Si può fare una analogia come avviene per altri prodotti armonizzati (quelli a marchio "CE"), come i giocattoli, i dispositivi medici, i prodotti connessi, eccetera.

Cosa resta dopo il bombardamento del ruolo del vecchio ORM

Si salvano alcune cose …



Integrazione rischi

Funzione di controllo trasversale su metodologie senza entrare nel tecnico Abitudine a integrare rischi e fattorini di rischio di natura diversa con i processi

Controlli e presidi

L'enfasi e l'esperienza nell'impostazione, valutazione e gestione di controlli e presidi

LDC

Abitudine a gestire, classificare, valutare e stimare serie storiche di eventi. Data cleaning.Analisi delle cause e degli effetti non solo economici e di bilancio

Sistemi

Sistemi affidabili per la raccolta, il trattamento e la gestione dei dati di rischio e l'abitudine all'accountability

Risk Self Assessment

La raccolta strutturata in workflow dei dati di rischio e l'abitudine a coinvolgere i presidi decentrati

Le nuove sfide dell’ORM

Mentalità sempre più da protezione civile

Investire in rete di intelligence interna e esterna per prevenire

Avere a disposizione tempestivamente dati e informazioni. Avere la capacità di leggere i dati e interpretarli, creare e gestire modelli di previsione

Respond: Agire prontamente quando si è sotto attacco o nell'emergenza

passare della logica zero risk ad **una logica del rischio inevitabile preventivamente studiato.** In modo che, **nel momento in cui succederà** (perchè succederà), con **piani di azione preordinati a tavolino**, piani di emergenza, strategie di controffensive (segregazioni, piani B, etc…) agire con prontezza ed efficacia per limitare i danni e ripristinare la normalità il prima possible.

Analizzare gli eventi e imparare dagli errori

Prevenzione

Formazione del team di ORM, delle altre funzioni di controllo e di tutte le figure decentrate che intervengono nella gestione dei rischi. In modo da avere un linguaggio comune, obiettivi e metodi condivisi, visione comune.

Test

Programmi periodici di test per verificare l’efficacia dei presidi, delle procedure di emergenza e per fare awareness

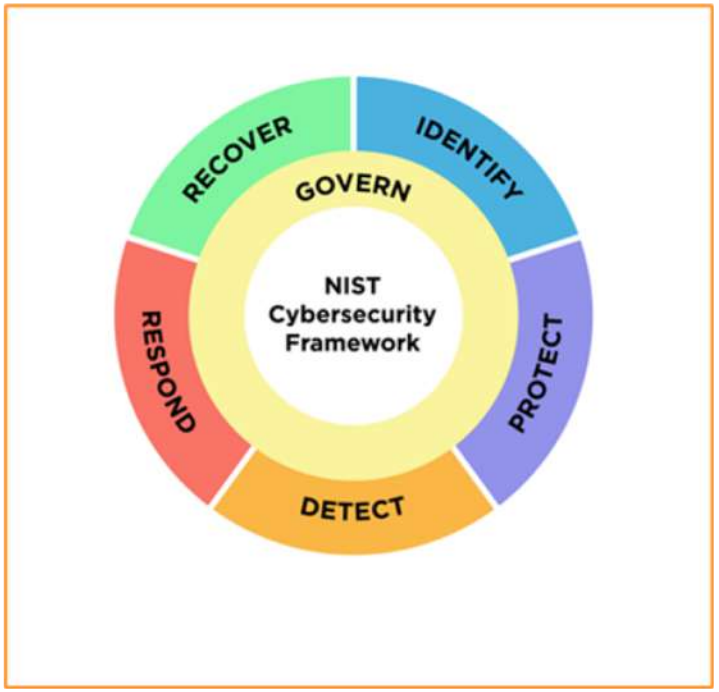
Fare Sistema con le terze parti

Far entrare all'interno del perimetro delle mura defensive presidiate anche i fornitori critici o importanti

Individuare, analizzare, gestire coadiuvare e controllare le terze parti e gli impegni reciproci contrattuali periodicamente in un'ottica Win-Win

Passare dai 5 passi lineari alla governance iterativa circolare

Focus su governance e applicazione della prassi delle **iterazioni successive** e **miglioramento continuo** per adattarsi progressivamente.



E’ il metodo migliore quando il contesto non è stabile e determinabile a priori.

E’ adattivo secondo il sano principio della proporzionalità. Scalabilità che è anche interna (team piccoli di incursori)

Conclusioni

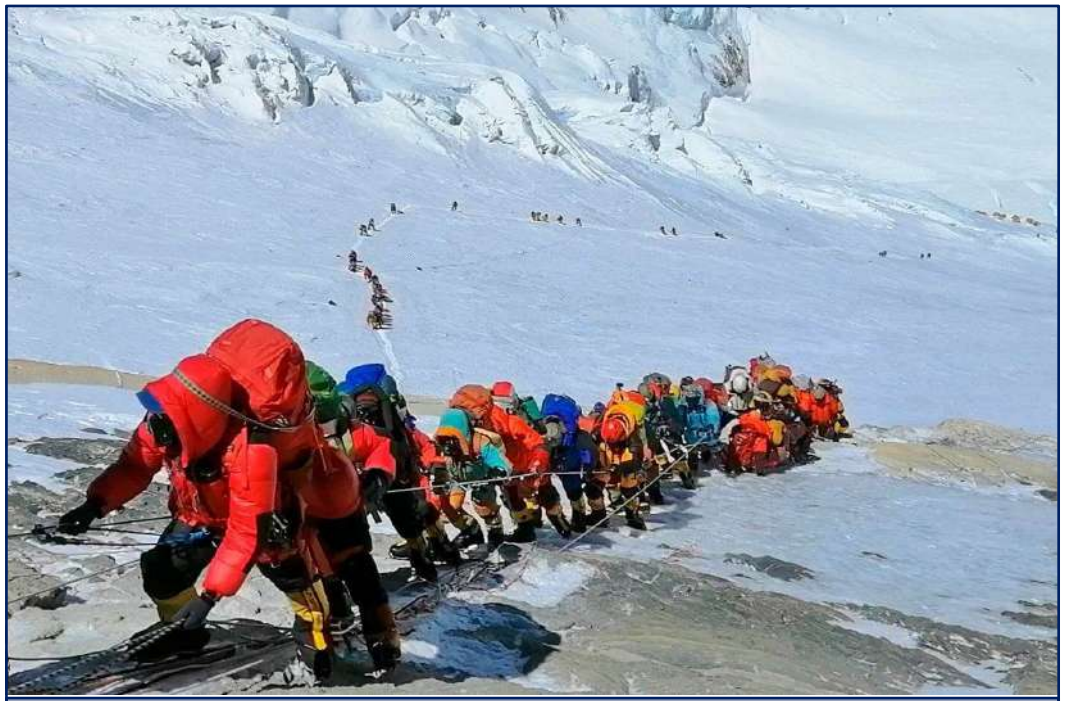
Alzare il livello stategico di azione dell'ORM, con una visione sempre più vicina ai ruoli apicali, CRO, Audit, Compliance, etc….

Coordinare e armonizzare le metodologie di tutti i non-financial risk, da un punto di vista di

- metodologie,
- sistemi SW,
- patrimonio informativo integrato dei dati,
- analisi e interazione tra rischi diversi.

Infatti ciascuna funzione di rischio vede una piccola fetta del problema ma solo il'ORM ha uno sguardo panoramico completo dall'alto.

Con Augeos verso una «Operational Risk Governance resiliente»



In questo contesto, appare rilevante la scelta di

- **farsi accompagnare da persone esperte**
- Investire e dotarsi di **strumenti operativi sw adeguati e proporzionati agli obiettivi**,

Venite a visitare il nostro blog
blog.augeos.it

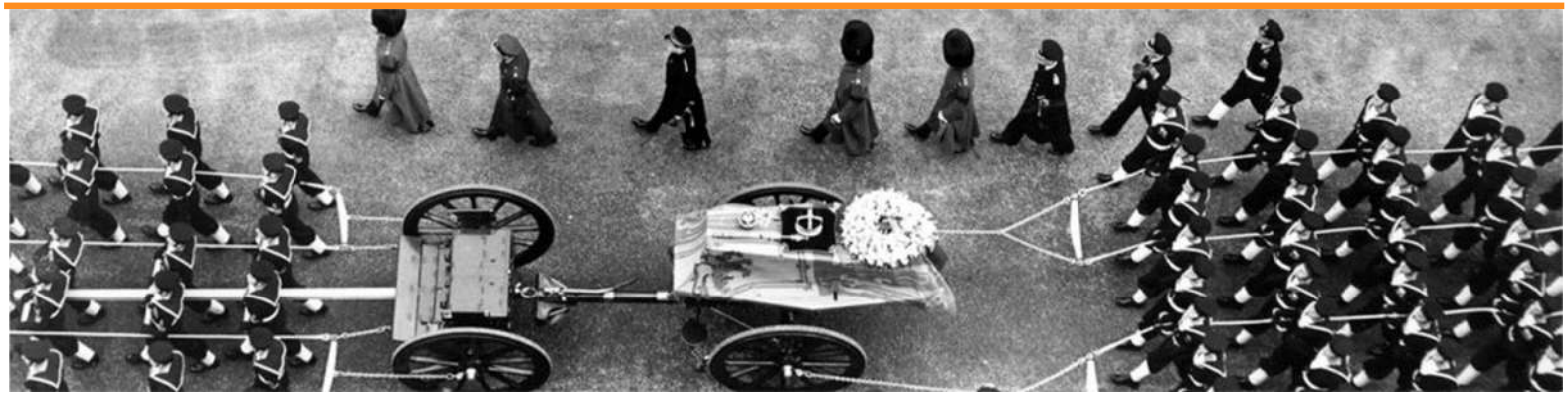
Docs Repo Augeos

Guild Documenti DORA

La documentazione di analisi del Regolamento DORA prodotta da Augeos

Documento Augeos	Link
Sito Web per la Consultazione Facilitata del Regolamento DORA	Clicca quì
White Paper **Guida Completa per la Conformità** al Regolamento DORA	Clicca quì
Checklist di Conformità al Regolamento DORA	Clicca quì
RTS DORA su Threat Led Penetration Test (**TLPT**)	Clicca quì
Linee Guida su **costi e perdite** derivanti da incidenti major legati a TIC	Clicca quì
RTS e ITS DORA sulla **segnalazione di incidenti** significativi	Clicca quì
RTS sul **Subappalto di servizi TIC** a supporto di Funzioni Essenziali o Importanti (FEI)	Clicca quì
RTS DORA sull'**Utilizzo dei servizi TIC** che supportano FEI prestate da fornitori terzi	Clicca quì
ITS Standardizzazione della **registrazione** delle informazioni relative agli **accordi** contrattuali	Clicca quì
RTS sulla **Gestione del rischio TIC Parte I**	Clicca quì
RTS sulla **Gestione del rischio TIC Parte II**	Clicca quì

E’ morto l’ORM



Lunga vita all’ORM

the art of creating innovative solutions

Thank You