Supply chain: gestire i rischi con strumenti di IA gratuita

di Giancarlo Butti

Supply chain: gestire i rischi con strumenti di IA gratuita

EDITORE

ITER S.r.l.
Piazzetta Guastalla, 11
20122 Milano (MI)
www.iterdigital.it

ISBN: 9791298583313

STAMPA

Digital Book S.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

Prima edizione Novembre 2025

Copyright ITER S.r.l. *(www.iterdigital.it)*

Tutti i diritti sono riservati a norma di legge e a norma delle convenzioni internazionali.
Nessuna parte di questa pubblicazione può essere riprodotta con sistemi elettronici, meccanici o altri, senza l'autorizzazione scritta dell'editore.
Tutti i marchi citati sono registrati dai rispettivi proprietari.
Gli eventuali testi delle normative e di altri documenti riportati nel libro hanno solo finalità indicativa e non hanno alcun valore ufficiale.
Gli unici testi ufficiali delle normative sono quelli riportati sulle pubblicazioni ufficiali dei vari enti emittenti che prevalgono in caso di discordanza.
L'applicazione pratica delle soluzioni proposte deve essere valutata da ogni singola organizza-zione in considerazione delle sue specificità.
I testi tratti da pubblicazioni di ENISA sono soggetti al copyright originale (a seconda dei casi libera riproduzione citando la fonte o https://creativecommons.org/licenses/by/4.0/).
Alcune parti del testo sono state realizzate con l'ausilio di strumenti di IA.

Ad Andrea, Attilio, Francesca V., Francesca G., Raffaella

A mia moglie ed a Jenny, Dalia, Luna, Hope, Teddy, Swan

Giancarlo

Giancarlo Butti

Master in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.

Si occupa di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni.

Come divulgatore ha all'attivo:

- oltre 800 articoli su 40 diverse testate
- 30 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
- 31 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT sulla sicurezza ICT in Italia
- relatore in oltre 170 eventi presso ABI, ISACA/AIEA, AIIA, ORACLE, CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, TECNA, UNISEF, PARADIGMA…
- già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer
- docente in master e corsi di perfezionamento post-universitario in diversi atenei:
    - Master di II livello in "Data Protection Officer e Diritto della privacy" dell'Università degli Studi Suor Orsola Benincasa - Napoli
    - Corso di Perfezionamento in Data Protection e Data Governance dell'Università degli Studi di Milano
    - Percorso di Alta Formazione Data Protection Officer del Cefriel
    - Master di Specializzazione per Responsabili della Protezione dei Dati Personali dell'UNISEF
    - Percorso DPO e dell'Osservatorio Information Security & Privacy del Politecnico di Milano
    - Master Risk management, internal audit & frodi della Ca Foscari Challenge School
    - Analisi e gestione del rischio all'Università Statale di Milano.

Socio e già proboviro di ISACA-AIEA (www.aiea.it), socio del CLUSIT (www.clusit.it), di DFA (perfezionisti.it), di BCI (www.thebci.org) e di ACFE (https://www.acfecentral.it/).

Partecipa a diversi gruppi di lavoro di ABI LAB, di ISACA-AIEA, del CLUSIT…

Ha acquisito le certificazioni/qualificazioni LA ISO 20000-1, LA ISO/IEC 42001, LA BS7799, LA ISO/IEC 27001:2005/2013/2022, LA ISO/IEC 22301, CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.

Contatti: *giancarlo.butti@promo.it, gbutti@clusit.it*

INDICE

Sommario

GUIDA ALLA LETTURA ix
L'uso degli strumenti di AI nel testo ix
LA GESTIONE DEI FORNITORI 1
L'uso degli strumenti di AI per la classificazione dei fornitori 4
Normative di riferimento 6
DORA (Digital Operational Resilience Act) 6
Ambito di applicazione 8
LA GOVERNANCE DELLA GESTIONE FORNITORI 11
Uso dell'AI per la gestione della governance dei fornitori 11
Normativa di riferimento 13
Elementi chiave della governance 19
Uso dell'AI per la creazione di una politica per la gestione dei fornitori 21
FASI DELLA GESTIONE DELLA RELAZIONE CON I FORNITORI 26
I RISCHI DEI FORNITORI 34
Normativa 34
La valutazione del rischio di concentrazione 38
Tipologie dei rischi di fornitura 39
Uso dell'AI per la gestione dei rischi 40
Il rischio informatico del fornitore 47
Valutazione di specifici aspetti di sicurezza di un fornitore 54
Attacchi alla catena di fornitura 58
LA VALUTAZIONE PRELIMINARE 62
Normativa 62
Due Diligence 65
L'uso dell'AI per l'esecuzione della due diligence 68
Strumenti per la valutazione dei rischi informatici 83
La valutazione del fornitore da parte di enti Ufficiali 94
I market place 97
La scelta del fornitore 99

Confrontare le offerte 100
Gli obblighi dei fornitori: la normativa NIS2 103
L'uso dell'AI per confrontare i fornitori 103
FASE DI CONTRATTUALIZZAZIONE 107
Gli aspetti contrattuali 107
Normativa 107
Analisi delle normative 119
I termini di un contratto 121
L'uso dell'IA per la fase di contrattualizzazione 122
Ricontrattualizzare un contratto 134
L'uso dell'AI per la gestione delle clausole per la subfornitura 135
Esempi di contratto 139
GLI ASPETTI PRIVACY NELLA GESTIONE DELLE FORNITURE 143
Ambito di applicazione della normativa 143
Il ruolo del fornitore 148
Amministratori di sistema 150
Adempimenti conseguenti al trattamento di dati personali 154
Trasferimento di dati verso paesi terzi o organizzazioni internazionali 154
Rischi derivanti dal trattamento di dati personali 157
Documenti di supporto 158
FASE DI MONITORAGGIO E CONTROLLO 163
Normativa 163
L'uso dell'AI per il monitoraggio della catena di fornitura 165
KPI per il Monitoraggio dei Fornitori 169
L'uso dell'AI per la gestione di parametri per il monitoraggio 169
Metriche e misure e loro caratteristiche 177
Lead e Lag indicators 179
Il monitoraggio nell'ambito delle misure di sicurezza 180
Tipologia di misure di sicurezza 181
Monitoraggio degli SLA 184
ATTIVITÀ DI AUDIT 187

Normativa 187
L'attività di audit interna 197
L'uso dell'AI per lo svolgimento delle attività di audit interno 198
L'attività di audit sui fornitori: la valutazione volontaria 211
Checklist per audit sui fornitori 213
L'uso dell'AI per le attività di audit sui fornitori 214
La certificazione del personale in ambito audit 224
LA CHIUSURA DEL RAPPORTO DI FORNITURA 228
Normativa 228
L'uso dell'AI nella gestione della chiusura del rapporto di fornitura 231
EXIT STRATEGY ED EXIT PLAN 235
Normativa 235
Procedura di Exit Strategy da un Fornitore 242
Uso di strumenti di AI per un Exit Plan Finalizzato al rientro 243
Uso di strumenti di AI per un Exit Plan Finalizzato al passaggio ad un altro fornitore 252
STANDARD E CODICI DI CONDOTTA 268
Standard 268
Codici di condotta 269
CLOUD 271
I fornitori in ambito cloud 271
L'uso dell'AI per la gestione del passaggio alle soluzioni Cloud 274
Ripartizione di responsabilità cliente - fornitore nei modelli Cloud 277
L'impatto del Data Act sui servizi in Cloud 279
ALLEGATI 285
PROCESSI E FUNZIONI ESSENZIALI 287
I processi 287
Cataloghi di processi 293
La rilevazione dei flussi documentali 295
Strumenti 297
Le funzioni operative importanti 299
GLOSSARIO 302

GUIDA ALLA LETTURA

La stesura di questo testo è stata particolarmente lunga e complessa. Soltanto nel mese di giugno 2025 è stato infatti pubblicato il regolamento delegato relativo alle subforniture, ultimo tassello normativo che completa il quadro delineato dal Regolamento DORA.

Poiché il presente volume si fonda principalmente su tali disposizioni, è stato necessario attendere la disponibilità anche di questo regolamento.

DORA rappresenta infatti, ad oggi, il quadro normativo più articolato in materia di presidio esteso del rischio informatico, con un'attenzione specifica alla gestione della catena di fornitura.

Durante la redazione sono state sperimentate diverse tecniche di utilizzo di strumenti di intelligenza artificiale generativa, adottati esclusivamente nelle loro versioni gratuite. Le esperienze maturate in tale ambito sono già state oggetto di trattazione nei miei precedenti volumi:

- *IA e Audit*, ITER, 2024
- *Compliance 4.0*, ITER, 2025.

In misura minore, tali esperienze vengono richiamate anche in questo testo, che si concentra principalmente su due aspetti:

- la gestione dei rischi della supply chain
- l'utilizzo di strumenti di intelligenza artificiale generativa, nelle loro versioni gratuite, a supporto di tali attività.

Per quanto riguarda l'impiego di questi strumenti, la quasi totalità dei risultati è stata ottenuta tramite *NoteBook LM* di Google. La scelta è motivata dal fatto che tale applicazione basa le proprie analisi soprattutto sui documenti forniti direttamente dall'utente, riducendo così il rischio di fenomeni di "allucinazione" e aumentando il livello di affidabilità delle risposte generate.

Considerata la duplice finalità di questo volume, le risposte fornite dall'intelligenza artificiale non sono state modificate, salvo in casi eccezionali. Per lo stesso motivo, sebbene il contenuto delle risposte fornite dai sistemi di AI sia stato in linea generale verificato, esso potrebbe comunque includere informazioni non corrette. È pertanto necessario, prima di utilizzarlo, procedere a un'attenta verifica della loro accuratezza, così da valutarne la validità.

L'USO DEGLI STRUMENTI DI AI NEL TESTO

La struttura grafica che verrà utilizzata nel libro, quando si utilizzeranno questi strumenti, è la seguente:

Prompt
descrizione del prompt utilizzato in grassetto corsivo

NOME DELLO STRUMENTO UTILIZZATO IN MAIUSCOLO CORSIVO

Risposta dello strumento in un riquadro

In alcuni casi, il prompt non verrà utilizzato direttamente nello strumento che dovrà generare la risposta, ma nello strumento https://console.anthropic.com/ di Anthropic.

Tale strumento genera, a partire dal prompt inserito, un prompt molto più completo ed articolato, che verrà utilizzato per l'interrogazione vera e propria.

Il prompt generato da https://console.anthropic.com/ non è un mero arrichimento del prompt iniziale, ma contiene già elementi di risposta. In particolare contiene, di norma, un indice dettagliato della risposta che deve essere fornita dallo strumento di AI prescelto.

LA GESTIONE DEI FORNITORI

Il ricorso a un fornitore e/o a un outsourcer introduce una serie di rischi specifici che devono essere adeguatamente valutati e gestiti.
In questo testo, con il termine fornitori si intendono sia quelli di servizi e lavorazioni, sia quelli di prodotti fisici, che si tratti di prodotti finiti, semilavorati o materie prime.

Per garantire la sicurezza di un'organizzazione (intendendo con tale termine qualunque tipo di azienda, ente o associazione) è necessario valutare con particolare attenzione la capacità della catena di fornitura di resistere a un attacco o a qualsiasi altro evento avverso, doloso o accidentale.

Infatti, anche se il livello di sicurezza di un'organizzazione è estremamente elevato, quando i suoi dati (personali o meno) e i suoi asset di altra natura, sono presenti presso soggetti terzi, o quando tali soggetti rivestono un ruolo rilevante per l'organizzazione stessa, è indispensabile valutarne i presidi di sicurezza.

Non sono infatti rari i casi in cui i danni a un'organizzazione siano stati causati da un attacco rivolto a un suo fornitore.

Qualora il fornitore tratti dati personali per conto dell'organizzazione (circostanza che si verifica nella quasi totalità dei casi di fornitori di servizi), la responsabilità per un'eventuale violazione resta in capo all'organizzazione cliente, quale Titolare del trattamento, e solo in parte grava sul fornitore, in quanto Responsabile.

Va inoltre ricordato che spesso anche un fornitore si avvale a sua volta di altri fornitori (subfornitori), e che la catena può estendersi a tal punto da rendere impossibile per l'organizzazione cliente un presidio effettivo dell'intera filiera di un prodotto o servizio.
In questo contesto, una tutela puramente contrattuale non può considerarsi sufficiente ed è pertanto opportuno effettuare:

- una valutazione ex ante di tutti i componenti della catena
- un monitoraggio continuo degli stessi
- puntuali verifiche periodiche, possibilmente in loco.

La valutazione ex ante del fornitore deve essere condotta sotto diversi profili:

- la capacità di garantire un livello di sicurezza adeguato
- la capacità di garantire adeguata resilienza e capacità di recupero
- la classificazione in merito alla sostituibilità, ossia la possibilità di rimpiazzarlo qualora, ad esempio:
    - non soddisfi le aspettative sotto vari aspetti
    - non sia in grado di proseguire nell'erogazione del servizio a causa di eventi endo- o eso-aziendali, dall'attacco informatico al fallimento.

La reale sostituibilità di un fornitore (che comprende anche la possibilità di reinternalizzare la lavorazione) è determinata da diversi fattori, quali ad esempio:

- il numero di fornitori disponibili per quello specifico prodotto o servizio (alcuni servizi sono offerti da pochissimi attori o da un unico soggetto)

- il numero di fornitori alternativi che presentano caratteristiche compatibili con i requisiti dell'organizzazione (ad esempio, possono esistere fornitori alternativi, ma che trattano i dati personali nei loro data center collocati al di fuori dell'UE)
- la reale capacità dell'organizzazione di gestire in autonomia il prodotto o servizio
- la facilità con cui sia possibile sostituire il fornitore, sia tramite un altro soggetto sia tramite internalizzazione;
- l'economicità del processo di sostituzione;
- …

Se la strategia di uscita prevede il passaggio a un altro fornitore, occorre verificare se tale opzione sia concretamente attuabile. Alcuni fornitori operano infatti in regime di monopolio e non è realisticamente ipotizzabile sostituirli. In altri casi, pur esistendo fornitori alternativi, i costi o i tempi richiesti per la sostituzione non risultano compatibili con le esigenze dell'organizzazione.

Le problematiche sopra evidenziate non riguardano esclusivamente i fornitori di servizi: anche i fornitori di materie prime, semilavorati o componenti costituiscono un potenziale punto di vulnerabilità se non adeguatamente valutati e presidiati. La guerra in Ucraina, ad esempio, ha messo in difficoltà diverse aziende italiane che avevano come unico fornitore un produttore collocato in quello Stato.

Per tali motivi, il processo di gestione dei fornitori è particolarmente complesso e comprende diverse fasi:

- la definizione dei requisiti del prodotto/servizio richiesto
- la valutazione sull'opportunità o necessità di ricorrere a un fornitore esterno
- la valutazione del fornitore (o dei fornitori) e degli eventuali subfornitori
- la formalizzazione dei rapporti mediante un contratto adeguato ed esaustivo
- il monitoraggio continuo delle prestazioni del fornitore
- la verifica periodica, ad esempio tramite audit e test mirati, delle effettive capacità del fornitore di adempiere a quanto stabilito contrattualmente
- la definizione di una exit strategy e di un exit plan
- il test periodico dell'exit plan.

Il ricorso sempre più frequente a fornitori e outsourcer ha spinto il legislatore (o, più precisamente, diversi legislatori e autorità di controllo) a intervenire, in particolare nei settori maggiormente esposti come la finanza e la pubblica amministrazione, con normative primarie e con atti di regolamentazione dettagliata degli ambiti citati.

Tali normative o atti includono:

- una descrizione del processo sopra indicato in forma anche molto analitica
- la predisposizione di contratti standard
- la predisposizione di check list di valutazione.

Specie nel settore della pubblica amministrazione sono stati definiti criteri formali non solo per la selezione dei fornitori, ma anche per la loro preventiva qualificazione, effettuata da enti appositamente incaricati. Gli esiti di tali valutazioni sono pubblici e consentono di individuare prodotti e fornitori qualificati, che possono essere utilizzati dalle amministrazioni. Tale qualificazione risulta ovviamente utile anche alle

organizzazioni private, che possono così avvalersi di un parco di fornitori e prodotti già selezionati secondo criteri trasparenti e ripetibili.

Va inoltre precisato:

- che i fornitori presentano rischi intrinseci aggiuntivi rispetto a quelli propri di un'organizzazione;
- che la capacità effettiva di un'organizzazione di valutare le caratteristiche di un fornitore, ad esempio mediante audit, può incontrare difficoltà oggettive in particolari situazioni, sempre più frequenti nell'erogazione di servizi, come l'impiego di componenti in cloud.

Per tale motivo, la normativa europea più recente in materia di resilienza operativa digitale per il settore finanziario, Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i Regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, meglio noto come Regolamento DORA, ha introdotto la possibilità che i controlli sui fornitori particolarmente significativi (definiti "critici") siano affidati a un'autorità di vigilanza pubblica.

Inoltre, ESMA (European Securities and Markets Authority), EBA (European Banking Authority) ed EIOPA (European Insurance and Occupational Pensions Authority) hanno ciascuna emanato linee guida in materia di gestione dei fornitori, che costituiscono un valido riferimento per qualunque tipologia di fornitura e sono applicabili alla maggior parte dei settori, in particolare quelli legati ai servizi:

- **ESMA – Orientamenti sull'esternalizzazione a fornitori di servizi cloud;**
- **EBA/GL/2019/02 – Orientamenti in materia di esternalizzazione (25 febbraio 2019);**
- **EIOPA-BoS-20-002 – Orientamenti sull'esternalizzazione a fornitori di servizi cloud;**
- **BCE – Guida sull'esternalizzazione di servizi cloud a fornitori di servizi cloud.**

Nel prosieguo del capitolo si farà riferimento in particolare alla normativa EBA, in quanto relativa a qualunque tipo di esternalizzazione, e al Regolamento DORA.

Per quanto riguarda altri aspetti, va considerato che il ricorso a servizi in cloud introduce ulteriori complessità, per cui si farà riferimento specifico alle normative dedicate a tale modalità di erogazione.

Per i fornitori che non erogano servizi, ma forniscono materie prime o semilavorati, alcune delle considerazioni contenute in questo capitolo devono essere adattate al contesto specifico. È evidente, infatti, che la mancanza di materie prime o semilavorati può compromettere o interrompere il funzionamento di un'organizzazione e che la predisposizione di opportuni presidi per garantire resilienza e capacità di recupero è indispensabile ed è spesso molto più difficile da implementare rispetto all'ambito dei servizi.

Vengono infatti coinvolte le capacità e flessibilità degli impianti produttivi, la logistica, lo stoccaggio dei materiali, tutti elementi per lo più assenti nell'ambito della fornitura di servizi e con costi potenzialmente rilevanti.

Il rapporto con i fornitori è inoltre regolato da normative trasversali che incidono su diversi aspetti, e che variano da Stato a Stato quali ad esempio:

- la normativa sulla protezione dei dati personali (privacy)
- il codice civile, per quanto riguarda la formalizzazione dei contratti
- la normativa in materia di safety, relativa alla sicurezza degli ambienti di lavoro
- …

Esistono infine normative specifiche di settore, come quelle già citate, o altre di più ampia portata, quali la Direttiva (UE) 2022/2555 (NIS2), che si applica a un numero di settori più ampio rispetto al Regolamento DORA.

L'USO DEGLI STRUMENTI DI AI PER LA CLASSIFICAZIONE DEI FORNITORI

In questo paragrafo viene rappresentato un primo semplice esempio di uso degli strumenti di AI.

Nel proseguo del libro tali strumenti verranno utilizzati per finalità molto più impegnative e non sarò limitato alla semplice creazione di un testo descrittivo.

Prompt

quali sono i metodi (vedi matrice di Kraljic) per classificare in classi omogenee i fornitori

Per raggruppare i fornitori in categorie omogenee, esistono diverse metodologie che variano in complessità e focus, ma che generalmente mirano a segmentare il portafoglio di fornitori per applicare strategie di gestione più mirate. La **matrice di Kraljic** è un esempio di metodologia ampiamente riconosciuta.

Ecco le metodologie normalmente utilizzate, con un focus sulle matrici e sugli strumenti quantitativi e qualitativi:

1. Metodologie Basate su Matrici di Portfolio

Questi approcci mirano a segmentare i fornitori (o i prodotti/servizi che offrono) in categorie, spesso basate su due dimensioni principali:

Matrice del portafoglio d'acquisto (Kraljic Purchasing Portfolio):

Il Dr. Peter Kraljic di McKinsey ha proposto che non esiste un unico approccio migliore per la gestione degli acquisti in tutte le circostanze.

La sua matrice categorizza tutti i prodotti acquistati (e, per estensione, i relativi fornitori) in due dimensioni principali:

Rischio di fornitura dal mercato (Supply Risk).

Impatto finanziario del materiale acquistato (Financial Impact).

Da queste due dimensioni emergono quattro categorie di prodotti acquistati, per ciascuna delle quali viene proposta una strategia di acquisto ottimale. Ad esempio, per i "prodotti di routine", che presentano grandi varietà e alta complessità logistica, Kraljic suggerisce una strategia di contrattazione di sistema e soluzioni di e-commerce, evitando le offerte competitive a causa del basso costo e della complessità delle varietà.

Un approccio simile, la **Matrice del portafoglio d'acquisto** più generale, segmenta i fornitori basandosi sulla **forza dell'azienda acquirente** nella relazione e sul **numero di fornitori disponibili** a fornire un prodotto a breve termine. Per gli "articoli strategici", dove l'acquirente ha forza ma ci sono pochi fornitori, l'ufficio acquisti dovrebbe usare la propria forza con attenzione per coinvolgere i fornitori in una relazione che assicuri la fornitura a lungo termine.

Matrici di valutazione/analisi:

Matrice di Criticità (Criticality Matrix): Utilizzata per classificare i prodotti in base alla loro importanza e differenziare il modo in cui vengono gestiti. Anche se si riferisce ai prodotti,

l'applicazione di diversi livelli di servizio a prodotti critici rispetto a quelli non critici ha un impatto diretto sulla relazione e la categorizzazione dei fornitori.

Matrice delle preferenze (Preference Matrix): Permette di valutare alternative (inclusi i fornitori) in base a diversi criteri di performance, sia quantitativi che qualitativi. A ciascun criterio viene assegnato un peso che riflette la sua importanza, e a ciascun fornitore un punteggio per ogni criterio. Il punteggio totale ponderato aiuta a classificare i fornitori. Boston Scientific utilizza una **Matrice di Distribuzione del Rischio** per mappare la probabilità di rischio del fornitore rispetto all'impatto potenziale sui ricavi.

Matrice di Classificazione del Rischio (Risk Classification Matrix): Usata per integrare la gestione del rischio nelle aree di produzione interne, classificando i rischi in base al loro impatto e localizzando le aree causative. Questo può indirettamente categorizzare i fornitori in base ai rischi che introducono nella catena di fornitura.

Matrice degli attributi di stoccaggio (Storage Attributes Matrix): Sebbene non direttamente sui fornitori, questo tipo di matrice aiuta a identificare i sistemi di stoccaggio più adatti alle esigenze di magazzino. Il principio di classificare basandosi su attributi specifici può essere esteso ai fornitori.

Matrice del processo prodotto (Product-Process Matrix): Mette in relazione il volume, la personalizzazione del prodotto e le caratteristiche del processo di produzione. La posizione di un'azienda su questa matrice può influenzare il tipo di fornitori di cui ha bisogno (es. per alta personalizzazione vs. alta produzione di massa).

2. Strumenti Quantitativi per la Selezione e Valutazione dei Fornitori (che portano a categorizzazione implicita)

Questi strumenti supportano un processo di selezione più razionale e possono portare a una categorizzazione dei fornitori basata sulle loro performance o caratteristiche:

Metodo Categoriale (Categorical Method): Si definiscono criteri di selezione (es. qualità, consegna, servizio) e si assegnano giudizi (es. buono (+), insoddisfacente (-), neutro (0)) per ogni fornitore. La somma dei giudizi fornisce un punteggio totale, permettendo una classificazione semplice ma soggettiva. È consigliato l'uso di un team multifunzionale per ridurre i bias.

Metodo del Rapporto di Costo (Cost Ratio Method): Utilizza dati storici sulle performance (es. qualità, servizio, affidabilità di consegna) per stabilire "costi di penalità". I prezzi unitari quotati vengono quindi aggiustati per ottenere costi netti, che possono alterare la selezione del fornitore più conveniente e, di fatto, categorizzarli per efficienza di costo totale.

Analisi ABC / Analisi di Pareto: Questo è un metodo fondamentale in logistica e gestione della supply chain per identificare gli elementi più importanti (ad esempio, prodotti, clienti, o anche fornitori). Si basa sulla "regola 80/20", secondo cui una piccola percentuale di elementi rappresenta una grande percentuale del valore o del throughput. Applicata ai fornitori, può identificarne un numero limitato che sono i più importanti per il business, consentendo di concentrare l'analisi e la gestione su di essi.

Analisi XYZ: Classifica gli articoli in base alla volatilità e frequenza della domanda (es. Classe X: domanda costante; Classe Y: domanda fluttuante; Classe Z: domanda sporadica). Questa categorizzazione dei prodotti può influenzare le strategie di rifornimento e, di conseguenza, la categorizzazione dei fornitori che li riforniscono.

3. Altre Metodologie di Classificazione/Segmentazione

Clustering di materiali o servizi: Un passo strategico nella definizione di una strategia di sourcing è la creazione di profili per categorie di materiali o servizi (es. carta, metallo, gomma o sedili, ruote, lampade) e il loro raggruppamento per identificare modelli di sourcing ripetitivi. Questo porta indirettamente a una categorizzazione dei fornitori specializzati in tali gruppi.

Gruppi di prodotti (Product Groups): La categorizzazione dei prodotti (es. per settore come beni per la casa, industriali, di consumo; o per tipo come hardware, software, ricambi) implica una categorizzazione dei fornitori che li offrono.

Requisiti di servizio al cliente / Tipo di ordine / Tipo di canale: Questi fattori possono influenzare la strategia di sourcing e la conseguente segmentazione dei fornitori.

Classificazione basata su normative (es. NAICS codes): Le agenzie governative utilizzano sistemi come il North American Industry Classification System (NAICS) per classificare le industrie. Questo può essere una base per categorizzare i fornitori in base al loro settore industriale.

Classificazione per rischi: Nel contesto della gestione del rischio della supply chain, le aziende possono classificare i fornitori in base alla loro conformità agli standard (es. ISO 31000) e feedback su criteri come qualità del servizio, salute finanziaria e incidenti legali. Le tassonomie di rischio operazionale possono categorizzare i rischi (e quindi i fornitori che li introducono) in base a fattori come materie prime, processi di produzione, ecc..

Segmentazione per caratteristiche di domanda e offerta: Classificare gli ambienti operativi in base alle caratteristiche di domanda e offerta, che poi influenzano le strategie logistiche (ad esempio, prodotti "A" più standardizzati per approcci lean, prodotti "B" più variabili per approcci agili). Anche questo può guidare la categorizzazione dei fornitori.

In sintesi, le metodologie per raggruppare i fornitori in categorie omogenee spaziano da approcci strategici basati su matrici (come Kraljic) che considerano rischio e impatto, a strumenti di valutazione quantitativi che classificano i fornitori in base alle loro performance e costo totale, fino a classificazioni basate su caratteristiche di prodotto, servizio o rischio. Tutte queste metodologie mirano a fornire trasparenza e a guidare decisioni di sourcing più efficaci.

NORMATIVE DI RIFERIMENTO

Tutti i capitoli del libro partono con una rassegna di alcune normative di riferimento.
Le normative citate sono principalmente dell'ambito finanziario ed in particolare:

- **EBA – Orientamenti in materia di esternalizzazione**
- **EBA – Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza**
- **BCE - Guida della BCE sull'esternalizzazione di servizi cloud a fornitori di servizi cloud**
- **Regolamento DORA** e relativi regolamenti delegati
- **Direttiva NIS2** compresa la normativa italiana di recepimento e il relativo **Regolamento di esecuzione.**

Il riferimento a normative del settore finanziario non è casuale e non è legato al fatto che questo testo sia dedicato ad un particolare settore.

Il settore finanziario è uno di quelli maggiormente regolamentati, sia dal punto di vista della sicurezza, sia dal punto di vista della gestione delle forniture esterne e delle esternalizzazioni.

Inoltre, a differenza di altre tipologie di documenti, quali potrebbero essere framework o standard di riferimento, le normative del settore finanziario sono molto pratiche ed analitiche e quindi, possono essere utilizzate come buoni esempi di implementazione dei principi teorici legati, come in questo caso, alla gestione dei fornitori.

In particolare la normativa in ambito bancario, emessa da EBA, e quella rivolta alle entità finanziarie nel loro complesso, con particolare riferimento al regolamento DORA, sono molto analitiche nel descrivere i requisiti da implementare.

DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

In questo paragrafo verrà illustrato brevemente il Regolamento DORA, emesso nel dicembre del 2022 e che è diventato pienamente operativo nel gennaio del 2025.

Viene data larga enfasi a questa normativa in quanto da un peso molto rilevante alla regolamentazione dei rapporti fra le entità finanziarie (principali destinatarie della normativa) e i loro fornitori (anche se limitatamente ai fornitori ICT) ed impone alle prime un controllo sulla intera catena di fornitura.

Inoltre, sebbene in forma molto limitata, è probabilmente la prima normativa che si applica non solo ai soggetti direttamente destinatari della stessa (le entità finanziarie), ma anche ai loro fornitori.

Da ultimo, DORA introduce un controllo diretto da parte delle Autorità di Vigilanza su un ristretto numero di fornitori ICT considerati critici.

DORA

«fornitore terzo critico di servizi TIC»: un fornitore terzo di servizi TIC designato come critico in conformità dell'articolo 31;

DORA è nato per rispondere ad una serie di problemi legati al quadro normativo preesistente che si possono così riassumere:

- l'insufficiente risposta della normativa all'aumento dei livelli di rischio in ambito ICT, (la normativa utilizza la dizione TIC - tecnologie dell'informazione e della comunicazione)
- una visione incompleta sulla frequenza e sulla importanza degli incidenti in ambito ICT
- l'esistenza di molteplici obblighi di segnalazione degli incidenti
- l'insufficiente condivisione di informazioni sulle minacce tra gli istituti finanziari
- il mancato riconoscimento transfrontaliero dei test di resilienza
- l'insufficiente valutazione delle capacità preventive e di resilienza
- il mancato monitoraggio dei rischi dei fornitori ICT.

"DORA mira a creare un quadro normativo sulla resilienza operativa digitale grazie a cui tutte le imprese garantiscono di poter far fronte a tutti i tipi di malfunzionamenti e minacce connessi alle TIC, al fine di prevenire e mitigare le minacce informatiche."[1]

Le aree di intervento di DORA sono ben espresse dall'art.1 del Regolamento:

ARTICOLO 1
OGGETTO
1. Al fine di conseguire un livello comune elevato di resilienza operativa digitale, il presente regolamento stabilisce i seguenti obblighi uniformi in relazione alla

[1] *https://www.consilium.europa.eu/it/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/*

sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie:

a) obblighi applicabili alle entità finanziarie in materia di:

i) gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);

ii) segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;

iii) segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;

iv) test di resilienza operativa digitale;

v) condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;

vi) misure relative alla solida gestione dei rischi informatici derivanti da terzi;

b) obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie;

c) norme per l'istituzione e l'attuazione di un quadro di sorveglianza per i fornitori terzi critici di servizi TIC, allorché forniscono i loro servizi a entità finanziarie;

d) norme sulla cooperazione tra autorità competenti e norme sulla vigilanza e l'applicazione da parte delle autorità competenti in relazione a tutte le materie trattate dal presente regolamento.

2. Quanto alle entità finanziarie identificate come soggetti essenziali o importanti ai sensi delle norme nazionali che recepiscono l'articolo 3 della direttiva 2022/2555, il presente regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 4 di tale direttiva.

3. 3. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri per quanto riguarda le funzioni essenziali dello Stato concernenti la sicurezza pubblica, la difesa e la sicurezza nazionale conformemente al diritto dell'Unione.

In sintesi quindi DORA regolamenta i seguenti aspetti:

- gestione del rischio TIC
- segnalazione degli incidenti connessi alle TIC
- test di resilienza operativa digitale
- rischi relativi alle TIC derivanti da terzi
- condivisione delle informazioni
- predisposizione di un Quadro per il coordinamento fra le varie autorità.

AMBITO DI APPLICAZIONE

DORA ha un perimetro molto ampio di applicazione che comprende 2 grandi macrocategorie di soggetti:

- le entità finanziarie, così come elencate all'art. 2, che comprende 20 diverse categorie di soggetti
- i fornitori terzi di servizi TIC.

Tuttavia a questi ultimi è richiesto, come unico requisito normativo, l'obbligo di formalizzare il loro rapporto contrattuale con le entità finanziarie, mediante un atto scritto.

LA GOVERNANCE DELLA GESTIONE FORNITORI

Una possibile definizione di governance, derivante da una sintesi ottenuta dai risultati di una ricerca è la seguente:

"la governance della catena di fornitura è l'insieme strutturato di regole, procedure e relazioni che coordinano le attività e le connessioni tra i vari partecipanti della supply chain. Questo sistema integrato ha l'obiettivo di migliorare l'efficienza complessiva, ridurre i rischi e assicurare il rispetto delle normative applicabili, contribuendo così a generare valore sostenibile per l'intera azienda."

Alcuni obiettivi della governance della gestione dei fornitori

Obiettivo	Spiegazione
Efficienza operativa	Implementare processi agili e ottimizzati consente di ridurre costi e tempi, aumentando la produttività complessiva dell'organizzazione.
Reattività ai cambiamenti	Potenziare la capacità di risposta a evoluzioni del mercato, innovazioni o eventi imprevisti migliora l'adattabilità dell'impresa.
Sostenibilità integrata	Adottare pratiche ambientali e socialmente responsabili promuove uno sviluppo equilibrato e duraturo.
Conformità normativa	Mantenere un allineamento costante alle disposizioni di legge riduce i rischi legali e contribuisce a consolidare l'affidabilità dell'impresa.
Relazioni con i partner	Stabilire rapporti solidi e trasparenti con fornitori e partner assicura continuità operativa e qualità nei servizi o prodotti.
Ottimizzazione dei costi	Ridurre sprechi e spese lungo l'intera catena del valore permette un uso più efficiente delle risorse.
Miglioramento continuo	Promuovere una cultura orientata al progresso costante consente di soddisfare, e in alcuni casi superare, le aspettative del cliente.
Trasparenza e tracciabilità	Monitorare e documentare processi e decisioni favorisce la fiducia degli stakeholder e la conformità ai requisiti normativi.
Equità nelle relazioni	Collaborare nel rispetto dei diritti umani e dei principi etici rafforza la responsabilità sociale dell'organizzazione.
Resilienza operativa	Rafforzare la capacità di risposta a eventi critici garantisce la continuità delle operazioni in situazioni straordinarie.
Incremento della competitività	L'adozione di tecnologie innovative migliora l'efficienza e la qualità, accrescendo la capacità di distinguersi sul mercato.
Reputazione aziendale	Comunicare in modo chiaro l'impegno verso l'etica e la sostenibilità migliora l'immagine pubblica e la fiducia degli stakeholder.

USO DELL'AI PER LA GESTIONE DELLA GOVERNANCE DEI FORNITORI

Elementi Utili alla Governance della Supply Chain

Prompt

la governance della catena di fornitura è l'insieme strutturato di regole, procedure e relazioni che coordinano le attività e le connessioni tra i vari partecipanti della supply chain. Questo sistema integrato ha l'obiettivo di migliorare l'efficienza complessiva, ridurre i rischi e assicurare il rispetto delle normative applicabili, contribuendo così a generare valore sostenibile per l'intera azienda.

NOTEBOOK

La governance, definita come l'approccio complessivo attraverso cui i dirigenti senior dirigono e controllano l'intera organizzazione utilizzando informazioni gestionali e strutture di controllo gerarchiche, è essenziale per la supply chain.
Gli elementi chiave per una governance efficace includono:

1. **Allineamento Strategico**: La strategia della supply chain deve essere allineata e supportare la strategia aziendale complessiva. Deve essere **resiliente** per gestire e mitigare i rischi, **responsabile** per promuovere il benessere sociale e ambientale, e **adattabile** per rispondere a un ambiente aziendale in evoluzione. L'integrazione della strategia di gestione del rischio dovrebbe diventare una considerazione incorporata nello sviluppo delle strategie della supply chain e delle strategie aziendali.
2. **Gestione del Rischio (Supply Chain Risk Management - SCRM)**: È un processo sistematico per gestire l'esposizione ai rischi lungo l'intera supply chain.
    - La governance definisce le **strutture e i modelli operativi** di SCRM, stabilendo le ipotesi su minacce, vulnerabilità, impatto e probabilità dei rischi.
    - Include l'**identificazione precoce delle vulnerabilità e dei rischi** e l'implementazione di misure preventive. Il rischio nella supply chain è definito come un danno valutato con la sua probabilità di accadimento, che interessa più di un'azienda della supply chain e la cui causa può risiedere all'interno di un'azienda, della sua supply chain o nel suo ambiente.
    - Dovrebbe essere integrato nei processi di acquisizione e nei processi aziendali e di missione.
    - Standard come **ISO 28000** e **ISO 28002** offrono linee guida per sistemi di gestione della sicurezza della supply chain e lo sviluppo della resilienza.
    - La resilienza implica la capacità di un sistema di tornare al suo stato originale o desiderato dopo essere stato disturbato, e processi resilienti sono flessibili e agili.
3. **Informazione e Tecnologia (IT)**: L'informazione è la "linfa vitale" di un sistema logistico e di distribuzione.
    - L'IT è cruciale per la gestione di **enormi quantità di dati** in modo rapido e preciso.
    - I sistemi di gestione della supply chain (SCM-Systeme) sono sempre più utilizzati per gestire e proteggere la crescente complessità delle supply chain globali.
    - Devono supportare la **trasparenza** e il **flusso continuo e senza errori delle informazioni** lungo la supply chain.
    - Strumenti come **Hardware Bill of Materials (HBOMs)** e **Software Bill of Materials (SBOMs)** sono importanti per la gestione del rischio e la tracciabilità dei componenti.
    - Sistemi avanzati come gli **Advanced Planning Systems (APS)** consentono una pianificazione integrata e la simulazione di scenari.
    - La visibilità delle informazioni basata sulla collaborazione stretta con clienti e fornitori è fondamentale.
4. **Definizione di Ruoli e Responsabilità**: È cruciale definire chiaramente ruoli e responsabilità per i senior leader coinvolti nelle attività della supply chain. Le organizzazioni più lungimiranti hanno riconosciuto la necessità di ripensare l'organizzazione delle operazioni logistiche, passando da strutture funzionali a **strutture orientate ai processi**.
5. **Politiche e Procedure**: Le **politiche C-SCRM** indirizzano l'implementazione della strategia C-SCRM, definendo i punti di integrazione con i processi di gestione del rischio e specificando ruoli e responsabilità a un livello più granulare.
    - Devono coprire la gestione della configurazione, la sicurezza fisica, l'accesso e l'autenticazione, la protezione dal codice malevolo e la gestione degli incidenti.
    - **Codici di Condotta (CoC)** e audit sono strumenti per verificare l'implementazione di procedure e politiche lungo la supply chain, inclusa la formazione del personale e l'aderenza a regolamenti internazionali e locali.
6. **Misurazione delle Performance**:
    - Le **KPI (Key Performance Indicators)** sono centrali per una strategia di supply chain efficace.

- Il modello SCOR® offre un repertorio comune di termini e un set di strumenti standard per misurare le performance e confrontarle con quelle di altre aziende del settore. Le metriche sono organizzate per attributi di performance e processi, gerarchicamente strutturate da strategiche a diagnostiche e causali.
- La gestione della performance nella supply chain implica la definizione di obiettivi all'interno e tra le funzioni, che porteranno ai risultati desiderati in modo equilibrato e senza conflitti.

7. **Gestione dei Fornitori (Supplier Management)**: Implica l'identificazione, la valutazione, la selezione e lo sviluppo dei fornitori. Include la revisione e l'auditing periodico dei fornitori per valutarne la qualità e il rischio. Programmi di certificazione dei fornitori aiutano i nuovi fornitori a soddisfare gli standard del settore, costruendo fiducia e affidabilità.
8. **Gestione Contrattuale**: I contratti devono includere una **specifica completa dei servizi, tariffe associate e obblighi delle parti**. L'obiettivo è allineare gli incentivi tra i partecipanti della supply chain per massimizzare la redditività totale.
9. **Collaborazione e Coordinamento**: La gestione della supply chain si concentra sulla **cooperazione e la fiducia** tra le parti, riconoscendo che "il tutto può essere maggiore della somma delle sue parti". Una scarsa coordinazione può portare a conseguenze negative come costi di inventario più elevati, tempi di consegna più lunghi e servizio clienti inferiore. Strumenti come il **Collaborative Planning, Forecasting, and Replenishment (CPFR)** sono approcci basati sulla partnership che migliorano il coordinamento attraverso la condivisione di informazioni e la creazione di piani e previsioni congiunte.
10. **Sostenibilità**: Integrare le considerazioni ambientali e sociali nelle decisioni della supply chain. Questo include la gestione dei rifiuti, l'efficienza energetica, la minimizzazione dei rischi per la salute e la sicurezza, e l'innovazione di prodotti e processi per supportare le responsabilità finanziarie, ambientali e sociali.

In conclusione, la governance della supply chain è un approccio olistico che permea ogni livello e funzione, trasformando la supply chain da una serie di attività frammentate a una rete sinergica. Richiede un impegno costante nell'allineamento strategico, nella gestione proattiva del rischio, nell'adozione di tecnologie avanzate, nella definizione chiara delle responsabilità, nella misurazione continua delle performance e nella promozione di una cultura di collaborazione e fiducia tra tutti i partner.

NORMATIVA DI RIFERIMENTO

Le normative qui rappresentate sono relative unicamente alle forniture ICT, ma i principi che sono presi in considerazione, possono essere applicati in generale alla fornitura di servizi e, con qualche adattamento, alle forniture in generale.

DORA

ARTICOLO 28

PRINCIPI GENERALI

1. Le entità finanziarie gestiscono i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi di cui all'articolo 6, paragrafo 1, e conformemente ai principi indicati di seguito:

a) le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla normativa applicabile in materia di servizi finanziari;

b) la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie si svolge nel rispetto del principio di proporzionalità, tenendo conto:

i) della natura, della portata, della complessità e dell'importanza delle dipendenze connesse alle TIC;

ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la disponibilità delle attività e dei servizi finanziari a livello individuale e di gruppo.

2. Nel contesto del quadro per la gestione dei rischi informatici TIC, le entità finanziarie diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese adottano e riesaminano periodicamente una strategia per i rischi informatici derivanti da terzi, tenendo conto della strategia basata su una varietà di fornitori di cui all'articolo 6, paragrafo 9, ove applicabile. Tale strategia comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi e si applica su base individuale e, se del caso, su base subconsolidata e consolidata. Sulla base di una valutazione del profilo di rischio complessivo dell'entità finanziaria e della portata e della complessità dei servizi operativi, l'organo di gestione riesamina periodicamente i rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti.

3. Nel contesto del quadro per la gestione dei rischi informatici, le entità finanziarie mantengono e aggiornano a livello di entità, e su base subconsolidata e consolidata, un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi.

Gli accordi contrattuali di cui al primo comma sono opportunamente documentati, distinguendo quelli che si riferiscono a servizi TIC a supporto di funzioni essenziali o importanti dagli altri.

Le entità finanziarie comunicano almeno una volta all'anno alle autorità competenti il numero di nuovi accordi per l'utilizzo di servizi TIC, le categorie di fornitori terzi di servizi TIC, il tipo di accordi contrattuali e le funzioni e i servizi TIC forniti.

Su richiesta, le entità finanziarie mettono a disposizione dell'autorità competente il registro delle informazioni completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

Le entità finanziarie informano tempestivamente l'autorità competente in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti, nonché del momento in cui una funzione diventa essenziale o importante.

4.Prima di stipulare un accordo contrattuale per l'utilizzo di servizi TIC, le entità finanziarie:

a) valutano se l'accordo contrattuale riguardi l'utilizzo di servizi TIC a supporto di una funzione essenziale o importante;

b) verificano se siano soddisfatte le condizioni di vigilanza per la conclusione del contratto;

c) identificano e valutano tutti i rischi pertinenti relativi all'accordo contrattuale, compresa la possibilità che tale accordo contrattuale possa aggravare il rischio di concentrazione delle TIC di cui all'articolo 29;

d) effettuano controlli di dovuta diligenza (due diligence) sui potenziali fornitori terzi di servizi TIC e ne garantiscono l'idoneità lungo tutto il processo di selezione e valutazione;

e) individuano e valutano i conflitti d'interessi che possano derivare dall'accordo contrattuale.

5. Le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi TIC che soddisfano standard appropriati in materia di sicurezza delle informazioni. Laddove tali accordi contrattuali riguardino funzioni essenziali o importanti, le entità finanziarie, prima di concludere detti accordi, prendono in debita considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli standard di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni.

6. Nell'esercizio dei diritti di accesso, ispezione e audit nei confronti del fornitore terzo di servizi TIC, le entità finanziarie predeterminano, sulla base di un approccio basato sul rischio, la frequenza delle verifiche di audit e delle ispezioni nonché i settori da sottoporre ad audit, aderendo a standard di audit comunemente accettate in conformità di eventuali indicazioni di vigilanza sull'uso e l'integrazione di tali standard di audit.

Laddove gli accordi contrattuali conclusi con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, l'entità finanziaria verifica che i revisori, indipendentemente dal fatto che siano revisori interni o esterni o siano un gruppo di revisori, possiedano competenze e conoscenze adeguate per svolgere efficacemente gli audit e le valutazioni del caso.

7. Le entità finanziarie stabiliscono clausole che consentano la risoluzione degli accordi contrattuali per l'utilizzo di servizi TIC in una qualsiasi delle circostanze seguenti:

a) rilevante violazione, da parte del fornitore terzo di servizi TIC, di leggi, regolamenti o condizioni contrattuali applicabili;

b) circostanze, identificate nel corso del monitoraggio dei rischi informatici derivanti da terzi, ritenute suscettibili di alterare l'esercizio delle funzioni previsto a norma dell'accordo contrattuale, tra cui modifiche di rilievo che incidano sull'accordo o sulla situazione del fornitore terzo di servizi TIC;

c) punti deboli del fornitore terzo di servizi TIC emersi riguardo alla sua gestione complessiva dei rischi informatici e, in particolare, nel modo in cui il fornitore garantisce la disponibilità, autenticità, integrità e riservatezza dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali;

d) laddove l'autorità competente non sia più in grado di vigilare efficacemente sull'entità finanziaria per via delle condizioni dell'accordo contrattuale in questione o delle circostanze ivi afferenti.

8. Per i servizi TIC a supporto di funzioni essenziali o importanti, le entità finanziarie predispongono strategie di uscita. Tali strategie tengono conto dei rischi che possono emergere a livello dei fornitori terzi di servizi TIC, in particolare possibili disfunzioni dei

fornitori stessi, il deterioramento della qualità dei servizi TIC forniti, una perturbazione dell'attività commerciale conseguente a una fornitura di servizi TIC inadeguata o carente, oppure gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio del rispettivo servizio TIC oppure la risoluzione di accordi contrattuali con fornitori terzi di servizi TIC in una delle circostanze di cui al paragrafo 7.

Le entità finanziarie garantiscono di poter porre termine agli accordi contrattuali senza:

a) perturbare le proprie attività commerciali;

b) limitare il rispetto dei requisiti normativi;

c) pregiudicare la continuità e la qualità dei servizi forniti ai clienti.

I piani di uscita sono esaustivi, documentati e, conformemente ai criteri di cui all'articolo 4, paragrafo 2, sottoposti a test adeguati e riesaminati periodicamente.

Le entità finanziarie identificano soluzioni alternative ed elaborano piani di transizione che consentano loro di trasferire i servizi TIC previsti dal contratto e i relativi dati dal fornitore terzo di servizi TIC, in maniera sicura e nella loro interezza, a fornitori alternativi oppure reintegrarli al proprio interno.

Le entità finanziarie dispongono di misure di emergenza idonee per mantenere la continuità operativa qualora si verifichino le circostanze di cui al primo comma.

…

REGOLAMENTO DELEGATO (UE) 2024/1773 DELLA COMMISSIONE del 13 marzo 2024[2]

ARTICOLO 3

MECCANISMI DI GOVERNANCE

1. L'organo di gestione riesamina la politica almeno una volta all'anno e la aggiorna se necessario. Le modifiche apportate alla politica sono attuate in modo tempestivo e non appena possibile nell'ambito degli accordi contrattuali pertinenti. L'entità finanziaria documenta la tempistica prevista per l'attuazione.

2. La politica stabilisce o fa riferimento a una metodologia per determinare quali sono i servizi TIC a supporto di funzioni essenziali o importanti. La politica specifica inoltre quando tale valutazione deve essere condotta e riesaminata.

3. La politica assegna chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione dei pertinenti accordi contrattuali e assicura che all'interno dell'entità finanziaria siano mantenute le competenze, l'esperienza e le conoscenze adeguate a supervisionare efficacemente i pertinenti accordi contrattuali, compresi i servizi TIC forniti nell'ambito di tali accordi.

4. Fatta salva la responsabilità finale dell'entità finanziaria di supervisionare efficacemente gli accordi contrattuali pertinenti, la politica impone di valutare se il fornitore terzo di servizi TIC dispone di risorse sufficienti a garantire il rispetto da

[2] REGOLAMENTO DELEGATO (UE) 2024/1773 DELLA COMMISSIONE del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC (Testo rilevante ai fini del SEE)

parte dell'entità finanziaria di tutti i requisiti di natura legale e regolamentare relativi ai servizi TIC a supporto di funzioni essenziali o importanti che sono prestati.

5. La politica individua chiaramente il ruolo o il dirigente di rango elevato responsabile del monitoraggio degli accordi contrattuali pertinenti. La politica specifica le modalità di collaborazione tra il ruolo o il dirigente di rango elevato e le funzioni di controllo, salvo nel caso in cui ne faccia parte, e definisce le linee gerarchiche di comunicazione all'organo di gestione, compresi la natura delle informazioni da comunicare e i documenti da fornire. Essa stabilisce altresì la frequenza di tale comunicazione.

6. La politica garantisce che gli accordi contrattuali siano coerenti con:

a) il quadro per la gestione dei rischi informatici di cui all'articolo 6 del regolamento (UE) 2022/2554;

b) la politica di sicurezza dell'informazione di cui all'articolo 9, paragrafo 4, del regolamento (UE) 2022/2554;

c) la politica di continuità operativa delle TIC di cui all'articolo 11 del regolamento (UE) 2022/2554;

d) gli obblighi di segnalazione degli incidenti di cui all'articolo 19 del regolamento (UE) 2022/2554.

7. La politica impone che i servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC siano soggetti a un riesame indipendente e siano inclusi nel piano di audit.

8. La politica specifica esplicitamente che gli accordi contrattuali:

a) non sollevano l'entità finanziaria e il suo organo di gestione dagli obblighi regolamentari e dalle responsabilità nei confronti dei clienti;

b) non devono impedire l'efficace vigilanza dell'entità finanziaria e non devono contravvenire a eventuali restrizioni di vigilanza sui servizi e sulle attività;

c) devono prescrivere che i fornitori terzi di servizi TIC collaborino con le autorità competenti;

d) devono prescrivere che l'entità finanziaria, i suoi revisori e le autorità competenti abbiano effettivo accesso ai dati e ai locali connessi all'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti.

EBA - Orientamenti in materia di esternalizzazione

6 Solidi dispositivi di governance ed esternalizzazione

35. L'esternalizzazione di funzioni non può comportare la delega delle responsabilità dell'organo di amministrazione. Gli enti e gli istituti di pagamento restano pienamente responsabili del rispetto di tutti i loro obblighi normativi, compresa la capacità di vigilare sull'esternalizzazione di funzioni essenziali o importanti.

36. L'organo di amministrazione è in ogni momento pienamente responsabile almeno:

a. di assicurare che l'ente o l'istituto di pagamento soddisfi costantemente le condizioni che è tenuto a rispettare per mantenere l'autorizzazione, comprese eventuali condizioni imposte dall'autorità competente;

b. dell'organizzazione interna dell'ente o dell'istituto di pagamento;

c. di individuare, valutare e gestire i conflitti di interesse;

d. di definire le strategie e le politiche dell'ente o dell'istituto di pagamento (ad esempio, il modello di business, la propensione al rischio, il quadro di gestione dei rischi);

e. di vigilare sulla gestione quotidiana dell'ente o dell'istituto di pagamento, compresa la gestione di tutti i rischi associati all'esternalizzazione;

f. di svolgere il ruolo di supervisione dell'organo di amministrazione nella sua funzione di supervisione strategica, compresi il monitoraggio e il controllo sul processo decisionale dell'amministrazione.

37. L'esternalizzazione non dovrebbe abbassare i requisiti di idoneità applicati ai membri dell'organo di amministrazione di un ente, ai direttori e alle persone responsabili della gestione dell'istituto di pagamento e il personale che riveste ruoli chiave. Gli enti e gli istituti di pagamento dovrebbero avere competenze adeguate e risorse sufficienti e debitamente qualificate per assicurare un'adeguata gestione e supervisione degli accordi di esternalizzazione.

38. Gli enti e gli istituti di pagamento dovrebbero:

a. attribuire in modo chiaro le responsabilità per le attività di documentazione, gestione e controllo degli accordi di esternalizzazione;

b. stanziare risorse sufficienti per assicurare il rispetto di tutte le previsioni di legge e di tutti gli obblighi normativi, compresi i presenti orientamenti e la documentazione e il monitoraggio di tutti gli accordi di esternalizzazione;

c. tenendo conto della sezione 1 dei presenti orientamenti, istituire una funzione di esternalizzazione o designare un membro del personale di grado superiore (senior staff member) che risponda direttamente all'organo di amministrazione (ad esempio, una persona che riveste un ruolo chiave nell'ambito di una funzione di controllo) e che sia responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni dell'ente e della supervisione della documentazione degli accordi di esternalizzazione. Gli enti o gli istituti di pagamento di piccole dimensioni e minore complessità dovrebbero almeno assicurare una chiara divisione dei compiti e delle responsabilità relative alla gestione e al controllo degli accordi di esternalizzazione, e possono assegnare questa funzione in materia di esternalizzazione a un membro dell'organo di amministrazione dell'ente o dell'istituto di pagamento.

39. Gli enti e gli istituti di pagamento dovrebbero mantenere in ogni momento un'operatività sostanziale, evitando di diventare cosiddette «empty shells» o «letter-box entities». A tal fine essi dovrebbero:

a. soddisfare in ogni momento tutte le condizioni della loro autorizzazione, tra cui assicurare che l'organo di amministrazione eserciti effettivamente le responsabilità di cui al paragrafo 36 dei presenti orientamenti;

b. mantenere una struttura e un quadro organizzativo chiari e trasparenti, che consentano loro di assicurare il rispetto delle previsioni di legge e degli obblighi normativi;

c. se i compiti operativi delle funzioni di controllo interno sono esternalizzati (ad esempio, in caso di esternalizzazione infragruppo o di esternalizzazione nell'ambito di sistemi di tutela istituzionale), esercitare un controllo adeguato ed essere in grado di gestire i rischi generati dall'esternalizzazione di funzioni essenziali o importanti;

d. disporre di risorse e abilità sufficienti per assicurare l'osservanza delle lettere da a) a c).

40. In caso di esternalizzazione, gli enti e gli istituti di pagamento dovrebbero almeno assicurare di:

a. poter prendere e attuare decisioni in relazione alle proprie attività operative e alle funzioni essenziali o importanti, incluse quelle esternalizzate;

b. mantenere l'ordinato svolgimento delle proprie attività e dei servizi bancari e di pagamento che forniscono;

c. individuare, valutare, gestire e attenuare in maniera adeguata i rischi connessi agli accordi di esternalizzazione esistenti e a quelli futuri, compresi i rischi ICT e quelli legati alla tecnologia finanziaria (fintech);

d. porre in essere disposizioni adeguate in materia di riservatezza dei dati e di altre informazioni;

e. mantenere un adeguato flusso di informazioni con i fornitori di servizi;

f. poter intraprendere in tempi adeguati almeno una delle seguenti azioni con riferimento all'esternalizzazione di funzioni essenziali o importanti:

i. trasferire la funzione a fornitori di servizi alternativi;

ii. reintegrare la funzione; oppure iii. interrompere le attività operative che dipendono dalla funzione.

g. attuare misure adeguate e trattare i dati in conformità del regolamento (UE) 2016/679 nel caso in cui i dati personali siano trattati da fornitori di servizi situati nell'UE e/o in paesi terzi.

ELEMENTI CHIAVE DELLA GOVERNANCE

Politica di gestione dei fornitori

EBA - Orientamenti in materia di esternalizzazione

7 Politica di esternalizzazione

41. L'organo di amministrazione di un ente o istituto di pagamento che ha in essere o che prevede di concludere accordi di esternalizzazione dovrebbe approvare, rivedere e aggiornare periodicamente una politica di esternalizzazione redatta in forma scritta e assicurarne l'attuazione, ove opportuno, a livello individuale, subconsolidato e consolidato. Per gli enti, la politica di esternalizzazione dovrebbe essere conforme alla sezione 8 degli orientamenti dell'ABE sulla governance interna e, in particolare, dovrebbe tenere conto dei requisiti di cui alla sezione 18 (nuovi prodotti e modifiche significative) di tali orientamenti. Anche gli istituti di

pagamento possono armonizzare le proprie politiche con le sezioni 8 e 18 degli orientamenti dell'ABE sulla governance interna.

42. La politica dovrebbe includere le fasi principali del ciclo di vita degli accordi di esternalizzazione e definire i principi, le responsabilità e i processi in relazione all'esternalizzazione. In particolare, la politica dovrebbe riguardare almeno:

a. le responsabilità dell'organo di amministrazione in linea con il paragrafo 36, compreso il suo coinvolgimento, se del caso, nel processo decisionale relativo all'esternalizzazione di funzioni essenziali o importanti;

b. il coinvolgimento delle linee di business, delle funzioni di controllo interno e di altri soggetti con riferimento agli accordi di esternalizzazione;

c. la pianificazione degli accordi di esternalizzazione, che include:

i. la definizione dei requisiti operativi relativi agli accordi di esternalizzazione;

ii. i criteri, compresi quelli di cui alla sezione 4, e i processi per l'individuazione delle funzioni essenziali o importanti;

iii. l'individuazione, la valutazione e la gestione dei rischi conformemente alla sezione 12.2;

iv. i controlli di due diligence sui potenziali fornitori di servizi, comprese le misure di cui alla sezione 12.3;

v. le procedure per l'individuazione, la valutazione, la gestione e l'attenuazione dei potenziali conflitti di interesse, conformemente alla sezione 8;

vi. la pianificazione della continuità operativa in linea con quanto indicato nella sezione 9; vii. il processo di approvazione di nuovi accordi di esternalizzazione;

d. l'attuazione, il monitoraggio e la gestione degli accordi di esternalizzazione, compresi:

i. la continua valutazione della performance del fornitore di servizi in linea con la sezione 14;

ii. le procedure di notifica e di reazione alle modifiche riguardanti un accordo di esternalizzazione o un fornitore di servizi (ad esempio, la sua posizione finanziaria, la sua struttura organizzativa o proprietaria, la subesternalizzazione);

iii. la revisione e verifiche di audit indipendenti sulla conformità alle alle previsioni di legge, agli obblighi normativi e alle politiche; iv. i processi di rinnovo;

e. la documentazione e la tenuta dei registri, in considerazione dei requisiti di cui alla sezione 11;

f. le strategie di uscita (exit strategies) e i processi per porre termine all'accordo, compresa la richiesta di un piano di uscita (exit plan) documentato per ogni funzione essenziale o importante da esternalizzare, qualora tale uscita sia considerata praticabile alla luce delle possibili interruzioni del servizio o della cessazione inattesa di un accordo di esternalizzazione.

43. La politica di esternalizzazione dovrebbe distinguere tra:

a. l'esternalizzazione di funzioni essenziali o importanti e altri accordi di esternalizzazione;

b. l'esternalizzazione a fornitori di servizi autorizzati da un'autorità competente e a fornitori di servizi che non lo sono;