La Comunicazione - Note, Recensioni e Notizie n. 67
Anno 2023

I rischi della supply chain[1]

Supply chain risks

Giancarlo Butti♦

♦ ISACA MILANO

Sommario

Il sempre maggior ricorso a fornitori ed outsourcers, anche nell'ambito ICT, aumenta i rischi ai quali è esposta un'organizzazione.

Anche in questo campo, le normative in ambito finanziario offrono una serie di interessanti spunti pure per gli altri settori.

Abstract

The increasing use of suppliers and outsourcers, also in the ICT area, rises the risks to which an organisation is exposed.

Also in this field, regulations in the financial sector offer a number of interesting suggestions for other sectors.

Keyword

Outsourcing, exit strategy, exit plan, cloud, risk

1 - Introduzione

Sempre più aziende ed enti di ogni dimensione fanno ricorso a fornitori ed outsourcers per l'acquisizione di servizi che comportano il trasferimento e il trattamento di informazioni spesso riservate o che comprendono dati personali, anche particolari.

Le ragioni di una tale scelta sono soprattutto di natura economica. Le organizzazioni sperano da un lato di ottimizzare i costi di gestione, sfruttando l'economia di scala determinata dal

[1] Alcune parti del testo di questo articolo sono tratte dal volume ***G. Butti – Manuale di resilienza, ITER***, 2023

fatto che i fornitori sono in grado di erogare i loro servizi con costi nettamente inferiori a quelli derivanti da una lavorazione interna di analoga qualità.
Secondariamente, le organizzazioni desiderano concentrare la loro attenzione solo sulle attività core, evitando investimenti e gestione di quelle che sono considerate attività accessorie per le quali non è opportuno effettuare rischiosi investimenti.
Il modello di erogazione di tali servizi in modalità cloud, offerto da molti fornitori, aggiunge inoltre il vantaggio della flessibilità della fruizione che consente di passare da costi fissi a costi legati all'effettivo uso del servizio stesso.
I fornitori sono anche in grado di offrire livelli di sicurezza e capacità di continuità operativa che difficilmente un'organizzazione sarebbe in grado di sostenere senza elevati investimenti.
Tutto questo almeno in teoria.

2 – Valutare l'esternalizzazione

Decidere se esternalizzare sia effettivamente una buona scelta comporta un'analisi molto articolata, che comprende aspetti legali, una valutazione dei rischi, una valutazione di opportunità oltre che, ovviamente, considerazioni di natura economica.
Da quest'ultimo punto di vista, i presunti risparmi potrebbero non rilevarsi tali se si effettuano le corrette valutazioni e si passa da una miope valutazione per cassa ad una più attenta valutazione che prenda in considerazione il valore di asset, come il know how aziendale, il quale viene perso nel caso in cui si dia seguito ad un'esternalizzazione.
Il ricorso a fornitori ed outsourcers introduce una serie di rischi non indifferenti che devono essere attentamente valutati poiché i fornitori non sono tutti uguali.
In particolare, è necessario valutare la capacità di un fornitore di resistere ad un attacco. Anche se il livello di sicurezza di un'organizzazione può essere estremamente elevato, quando i suoi dati sono presenti anche presso soggetti terzi, deve essere valutato il loro livello di sicurezza.
Non sono infatti rari i casi di danni provocati ad un'organizzazione a causa di un attacco attuato nei confronti di un suo fornitore.

Nel caso in cui il fornitore tratti anche dei dati personali per conto dell'organizzazione (situazione che si presenta nella quasi totalità delle situazioni), la responsabilità di una eventuale violazione di dati personali ricade comunque sull'organizzazione in quanto Titolare del trattamento (e solo in parte sul fornitore in quanto Responsabile[2]).

Va inoltre ricordato che spesso anche un fornitore si avvale a sua volta di altri fornitori (sub fornitori) e tale catena può estendersi a tal punto da non consentire un reale presidio da parte dell'organizzazione sulla catena di fornitura di un prodotto/servizio.

Si evidenzia che una tutela puramente contrattuale non è sicuramente sufficiente e quindi è necessaria sia una valutazione ex ante di tutti i componenti della catena di fornitura, sia un monitoraggio nel continuo del suo reale livello di sicurezza.

La valutazione ex-ante del fornitore dovrà avvenire da diversi punti di vista:

- la sua capacità di garantire un livello di sicurezza adeguato
- la sua capacità di garantire un livello di resilienza e recovery adeguato
- la sua classificazione in merito alla facilità con cui lo stesso possa essere sostituito nel caso in cui ad esempio:
    - non si dimostri all'altezza delle aspettative
    - non sia in grado di proseguire nell'erogazione del servizio in conseguenza di eventi endo o eso aziendali di qualunque tipo, dall'attacco informatico al fallimento.

[2] Il ruolo assunto da fornitore deve essere valutato da caso a caso; non è possibile generalizzare.

Al riguardo, la reale sostituibilità di un fornitore (la sostituibilità comprende anche la possibilità della reinternalizzazione della lavorazione) è determinata da diversi fattori, quali ad esempio:

- il numero di fornitori che erogano quel prodotto/servizio (alcuni servizi sono erogati da pochi o da un solo fornitore)
- il numero di fornitori che erogano il servizio e che hanno caratteristiche compatibili con i requisiti dell'organizzazione (ad esempio esistono fornitori alternativi a quello utilizzato, ma trattano i dati personali nei loro data center negli USA)
- la reale capacità dell'organizzazione di gestire in autonomia il servizio/prodotto
- la facilità di sostituzione
- l'economicità della attività di sostituzione
- le tempistiche richieste per la sostituzione….

Per quanto sopra evidenziato, il processo di gestione di un fornitore è particolarmente complesso e comprende diverse fasi:

- la valutazione sulla opportunità/necessità di ricorrere ad un fornitore esterno
- la valutazione del fornitore (o possibilmente dei fornitori) e degli eventuali sub fornitori
- la formalizzazione dei rapporti con il fornitore mediante un adeguato ed esaustivo contratto
- il monitoraggio nel continuo del fornitore
- la verifica periodica, ad esempio tramite audit mirati e test, delle reali capacità del fornitore di adempiere a quanto definito 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 ed outsourcers ha spinto il legislatore a intervenire, in particolare nei settori più esposti come quelli della finanza e della pubblica amministrazione, sia con normative primarie, sia con altre tipologie di atti per regolamentare dettagliatamente ogni ambito prima citato.

Tali normative o atti comprendono:

- una descrizione del processo esposto al punto precedente in una forma anche molto analitica
- la predisposizione di contratti standard
- la predisposizione di check list di valutazione.

Va precisato inoltre:

- che i fornitori presentano una serie di rischi intrinsechi che si aggiungono a quelli che un'organizzazione deve valutare come propri
- che la reale capacità di un'organizzazione di valutare le caratteristiche di un fornitore, ad esempio mediante il ricorso ad un'attività di audit, può presentare delle oggettive difficoltà in particolari situazioni (sempre più frequenti), quali il ricorso a una componente in cloud nella fornitura del servizio stesso.

Anche per tale motivo, la recedente normativa europea (DORA - Digital Operational Resilience Act) ha introdotto la possibilità che tali controlli, per fornitori particolarmente significativi (sebbene limitati all'ambito finanziario), sia affidata ad un'autorità di controllo pubblica (nel caso in specie ad EBA, ESMA o EIOPA).

Le tre autorità pubbliche citate hanno emesso singolarmente delle normative relativamente alla gestione dei fornitori che possono costituire un valido riferimento per qualunque tipo di fornitura ed applicarsi alla maggior parte dei settori:

- **ESMA - Orientamenti in materia di esternalizzazione a fornitori di servizi cloud**
- **EBA/GL/2019/02 - 25 febbraio 2019 - Orientamenti in materia di esternalizzazione**
- **EIOPA-BoS-20-002 - Orientamenti in materia di esternalizzazione a fornitori di servizi cloud**

3 – I rischi dei fornitori

La normativa EBA elenca fra i possibili rischi dei fornitori che un'organizzazione deve valutare:

- i rischi di concentrazione, compresi quelli derivanti:
  - dall'esternalizzazione a un fornitore di servizi prevalente e non facilmente sostituibile
  - da molteplici accordi di esternalizzazione con lo stesso fornitore di servizi o con fornitori di servizi strettamente connessi
- i rischi aggregati derivanti dall'esternalizzazione di diverse funzioni al livello dell'ente o dell'istituto di pagamento e, nel caso di gruppi di enti o di sistemi di tutela istituzionale, i rischi aggregati a livello consolidato o del sistema di tutela istituzionale
- nel caso di enti significativi, il rischio di intervento («step-in risk»), ossia il rischio che potrebbe derivare dalla necessità di fornire sostegno finanziario a un fornitore di servizi in difficoltà o di subentrargli nelle sue attività operative

è inoltre opportuno:

- considerare le implicazioni del luogo in cui ha sede il fornitore di servizi (all'interno o all'esterno dell'UE)
- esaminare la stabilità politica e la situazione della sicurezza dei paesi in questione, tra cui:
  - la legislazione vigente, compresa quella sulla protezione dei dati
  - le previsioni vigenti per l'applicazione della legislazione
  - le previsioni del diritto fallimentare applicabili in caso di dissesto di un fornitore di servizi e le eventuali restrizioni che potrebbero insorgere specialmente in riferimento al recupero urgente dei dati dell'ente o dell'istituto di pagamento
- definire e stabilire un adeguato livello di protezione della riservatezza dei dati, di continuità delle attività esternalizzate nonché di integrità e tracciabilità dei dati e dei sistemi nell'ambito della prevista esternalizzazione. Gli enti e gli istituti di pagamento dovrebbero altresì prendere in considerazione, ove necessario, misure specifiche per i dati in transito, memorizzati e a riposo, come l'utilizzo di tecniche di cifratura in combinazione con un'adeguata architettura di gestione delle chiavi.

Ai rischi sopra elencati, si aggiungono quelli derivanti dalle sub esternalizzazioni:

- se l'accordo di esternalizzazione prevede la possibilità che il fornitore di servizi subesternalizzi funzioni essenziali o importanti ad altri fornitori di servizi, gli enti e gli istituti di pagamento dovrebbero tener conto di quanto segue:
  - i rischi associati alla subesternalizzazione, compresi i rischi aggiuntivi che possono sorgere se il subcontraente ha sede in un paese terzo o in un paese diverso da quello del fornitore di servizi;
  - il rischio che lunghe e complesse catene di subesternalizzazione riducano la capacità degli enti o degli istituti di pagamento di vigilare sulla funzione essenziale o importante esternalizzata e la capacità delle autorità competenti di esercitare una efficace vigilanza su essi.

4 – La scelta del fornitore

L'azienda, che desidera acquisire un prodotto/servizio o implementare una soluzione, dovrebbe mettere in atto un processo di valutazione dei fornitori basato su criteri oggettivi e su un'adeguata analisi dei rischi relativamente alle varie alternative possibili.

Una modalità sufficientemente oggettiva per effettuare una scelta fra le soluzioni offerte da più fornitori è quella di definire una serie di parametri che si considerano particolarmente significativi.

Tali parametri devono valutare:

- il prodotto/servizio/soluzione
- il fornitore.

Ad esempio, nel caso della valutazione di una soluzione software si dovrebbe tenere conto:

- degli aspetti tecnici di carattere generale, cioè indipendenti dallo specifico servizio/prodotto quali ad esempio:
  - completezza delle funzionalità rispetto alle esigenze
  - diffusione
  - maturità
  - qualità della documentazione
  - tipologia di assistenza
  - livello di parametrizzazione
  - …
- degli aspetti tecnici legati allo specifico servizio/prodotto
- di quelli più legati al fornitore in quanto tale:
  - i rischi, secondo i parametri prima elencati
  - l'affidabilità del fornitore
  - la dipendenza dal fornitore per le attività di gestione ordinaria e straordinaria
  - il livello di servizio garantito dal fornitore
  - …

Ulteriori elementi da considerare sono i costi, che comprendono:

- il costo di acquisizione/noleggio
- il modello di crescita del costo in funzione della quantità (ad esempio licenze per utenze…)
- il costo di gestione
- i costi collegati
- il costo di esternalizzazione
- il costo della strategia di uscita
- il costo di passaggio ad altro fornitore o di reinternalizzazione.

Un confronto fra più soluzioni si può ottenere componendo, con le voci prescelte, una tabella nella quale viene assegnato un peso alle singole voci e dando poi un punteggio ad ogni singolo prodotto/fornitore per ognuna delle voci.

Tabella 1. Stralcio di tabella per la valutazione di un prodotto.

Valutazione del prodotto				
Caratteristiche generali - prodotti software	**Peso**	**Prodotto 1**	**Prodotto 2**	**Prodotto 3**
Aspetti tecnici generali				
• Completezza funzionalità rispetto alle esigenze	10	8	9	7
• Diffusione del prodotto	8	7	9	7
• Maturità del prodotto	8	9	8	6

Sommando i valori così ottenuti, si ottiene una stima quali/quantitativa delle varie possibili soluzioni.

Tabella 2. Stralcio di tabella per la valutazione di un fornitore e valutazione complessiva.

Valutazione del fornitore	**Peso**	**Fornitore 1**	**Fornitore 2**	**Fornitore 3**
• Dimensioni	8	9	7	7
• Maturità	9	7	9	8
• Diffusione sul territorio	8	9	6	6
• Esperienza nel settore	10	8	10	9
• Referenze	10	8	10	9
• Tipologia di assistenza	10	9	9	9
• Capacità di assistenza	10	9	9	9
• …				
• ,,,				
TOTALE		**547**	**565**	**536**
Caratteristiche generali - prodotti software		1360	1375	1335
Caratteristiche specifiche - prodotto		2156	2151	2134
Valutazione del fornitore		…	…	…
TOTALE		…	…	…

Nella valutazione rivestono particolare rilievo, solitamente erroneamente trascurati, tutti i costi legati alla gestione della strategia di uscita; creare delle dipendenze irreversibili o comunque difficili da gestire verso un unico fornitore (o verso un unico cliente, ma tale tema non è oggetto di trattazione in questo articolo) riduce la resilienza di un'azienda e la sua reale capacità di sopravvivenza.

Anche recentemente, il conflitto russo ucraino ha messo in gravi difficoltà aziende che basavano la loro produzione sulla fornitura di materie prime provenienti da questi paesi.
È evidente che tali situazioni si sono create per diversi motivi:

- il ricorso ad un unico fornitore senza aver predisposto adeguati piani di continuità operativa
- la mancata attività di intelligence verso il rischio paese, che in realtà era di pubblico dominio da tempo.

La scarsa attenzione delle aziende verso queste tematiche le rende vulnerabili rispetto a scenari di rischio che potrebbero essere sempre più frequenti.
Le strategie di uscita non sono da confondersi con i piani di continuità operativa e con le misure di resilienza, ma tutti questi aspetti dovrebbero essere presi in considerazioni da un management illuminato e previdente che raramente è presente nelle aziende.
Anche per tale motivo, le normative prima citate e DORA introducono come obbligatoria la predisposizione di exit strategy ed exit plan.
Inoltre, DORA introduce anche l'obbligo, così come già in essere per i piani di continuità operativa, di testare tali piani.

Per meglio comprendere di cosa stiamo parlando, utili definizioni sono quelle riportate nel documento dell'**European Banking Federation AISBL**, denominato **Cloud exit strategy – testing of exit plans**:

Exit strategy	A high-level description of an institution's ultimate risk mitigation strategy when dealing with a failing cloud provider or when terminating the outsourcing. This might include exit and transition of outsourced functions and data to an alternative provider (in part or completely), the return of these functions on-premises, or even discontinuation of the process.
Exit plan	An underlying element to the exit strategy. A high-level document describing how to implement the exit strategy including a description of all its phases, involved roles and responsibilities and various plan features such as the ones mentioned in the EBA Guidelines para. 108 (see also figure 2). A plan is to be enacted in case of pre-defined events following a long-term strategy approach. It does not include short-term incident management, since the business implications of enacting an exit plan can be considered severe. The exit plan ensures business continuity in case of the pre-defined events, aiming at response times appropriate to the severity of the triggering event.
Testing of an exit plan	Activities to be performed to ensure that an exit plan is well documented and actionable when necessary. A table-top exit plan test involves a 'paper evaluation' to ensure that the exit plan is fully documented, understood by stakeholders, realistic and achievable in line with business and regulatory requirements. This includes checking on the availability of resources identified in the plan.

La definizione di tali soluzioni può essere molto impegnativa sia in termini di risorse sia in termini economici, in particolare se si pensa ad una reinternalizzazione in quanto non sono ipotizzabili fornitori alternativi.

Nel caso, ad esempio, di esternalizzazione di servizi informatici è necessario che siano mantenute o ripristinabili:

- l'infrastruttura e le applicazioni informatiche:
  - riacquisendole, se possibile
  - pagando le relative licenze anche se non sono utilizzate
- le competenze necessarie per svolgere l'attività che viene esternalizzata.

Il tutto può avere un costo non indifferente, costo che deve essere aggiunto:

- a quello dell'iniziale progetto di esternalizzazione
- al progetto di reinternalizzazione.

L'organizzazione dovrebbe anche definire come mantenere le adeguate competenze e le risorse umane necessarie per una successiva reinternalizzazione, risorse che nel frattempo sono state riallocate per svolgere altre attività e che possono avere avuto un percorso di carriera in altri ambiti aziendali o che sono uscite dall'azienda.

Va inoltre considerato che le condizioni fra il momento della esternalizzazione e quello della successiva possibile reinternalizzazione possono variare; ad esempio possono essere intervenute modifiche alla normativa che hanno comportato un adeguamento delle applicazioni software che supportano il processo esternalizzato.

Ne consegue che è necessario effettuare periodicamente una revisione del piano di uscita al fine di mantenerlo in linea con la reale situazione presente presso il fornitore e riaddestrare il personale coinvolto.

Anche questa attività deve essere quantificata in termini economici per avere una valutazione economica complessiva della esternalizzazione.

Complessivamente si dovranno considerare almeno le seguenti voci:

- il costo di esternalizzazione
- il canone periodico del fornitore
- il costo del mantenimento della infrastruttura
- il costo del mantenimento delle competenze delle risorse umane
- il costo delle revisioni periodiche dei piani
- il costo degli eventuali aggiornamenti periodici delle infrastrutture
- il costo degli eventuali aggiornamenti periodici delle risorse umane
- il costo di reinternalizzazione.

Se il motivo originario della scelta di esternalizzare era di natura economica, le valutazioni di cui sopra potrebbero cambiare notevolmente i costi da prendere in considerazione e influire sulla scelta stessa.

5 – Monitorare il fornitore

Quali sono gli strumenti che un'organizzazione ha a disposizione per controllare un proprio fornitore, ad esempio dal punto di vista della sicurezza?

Le soluzioni sono molteplici.

Molte aziende ricorrono alla somministrazione di check list con le quali il fornitore effettua un assessment la cui valenza non può, tuttavia, ritenersi esaustiva.

La soluzione dovrebbe consistere in un'attività di reale verifica presso lo stesso fornitore, ma questo tipo di azione, anche se prevista contrattualmente, non sempre è agevole e possibile.

I motivi sono molteplici e possono andare dalla collocazione geografica del fornitore alla complessità di effettuare un audit su architetture complesse, nella maggior parte dei casi condivise con altri clienti, che porterebbero a risultati soddisfacenti solo se adeguatamente prolungate nel tempo.

Per contro, la prospettiva di avere decine di auditor di clienti diversi che svolgono la loro attività di verifica contemporaneamente con possibili interferenze sulla erogazione dei servizi non è piacevole per un fornitore e in realtà rischia di compromettere proprio la sicurezza delle attività.

Per tale motivo, le aziende possono avvalersi di altri strumenti che sono stati predisposti nel corso degli ultimi anni.

Sono infatti disponibili:

- aziende specializzate che rilasciano indicazioni sulla postura di sicurezza dei fornitori periodicamente aggiornate
- enti preposti alla valutazione dei fornitori, soprattutto in ambito cloud, allorquando questi desiderino erogare i loro servizi per conto della pubblica amministrazione; in particolare, oltre alla italiana AGID, di notevole interesse è la statunitense FedRAMP. Quest'ultima rende disponibili sia le check list, utilizzate per la valutazione, sia l'elenco dei servizi/fornitori valutati. Appare evidente il fatto che si tratti di un ente statunitense è irrilevante, considerando il carattere internazionale di una fornitura in modalità cloud; unico vincolo per un'azienda europea è verificare se il fornitore prescelto abbia la possibilità di erogare il servizio da datacenter collocati nell'UE
- iniziative da parte di associazioni di fornitori, come la CSA (Cloud Security Alliance), che rende disponibile l'elenco di prodotti/fornitori che hanno effettuato un autovalutazione rispetto a parametri di sicurezza e privacy, ovvero che abbiano chiesto un audit da parte di terzi indipendenti; le autovalutazioni o i report di audit sono disponibili sul portale della CSA

- audit e certificazioni di terze parte che i singoli fornitori rendono disponibili sui propri siti. È frequente, in particolare per i fornitori di servizi o applicazioni in ambito cloud, rendere disponibili tali documenti realizzati secondo lo standard SOC, (standard realizzato dell'AICPA, Association of International Certified Professional Accountants), ovvero della Cloud Computing Compliance Criteria Catalogue – C5:2020, realizzato dalla tedesca BSI.
- Esclusivamente per quelli che verranno considerati fornitori critici nel mondo finanziario ed assicurativo (perimetro di applicazione del Regolamento DORA), la verifica sarà effettuata direttamente dalle autorità di vigilanza europea.

6 – Gli aspetti contrattuali

Gli elementi che dovrebbero regolamentare a livello contrattuale il rapporto con il fornitore sono ampiamente descritti nelle tre normative sopra citate.

A titolo esemplificativo, si riportano alcuni punti tratti dalla normativa EBA che prevede che il contratto contenga almeno le seguenti clausole:

- una descrizione chiara della funzione esternalizzata che deve essere svolta
- la data di inizio e, ove applicabile, la data di fine dell'accordo
- i termini di preavviso per il fornitore di servizi e per l'ente o l'istituto di pagamento
- la normativa che disciplina il contratto
- gli obblighi finanziari delle parti
- una clausola che indichi se è consentita la subesternalizzazione
- le condizioni alle quali la subesternalizzazione è soggetta
- i luoghi (regioni o paesi) in cui sarà svolta la funzione essenziale o importante
- il diritto di monitoraggio costante della performance del fornitore di servizi
- i livelli di servizio concordati

- gli obblighi di reportistica del fornitore
- una clausola che indichi se il fornitore di servizi debba stipulare un'assicurazione obbligatoria contro determinati rischi
- i requisiti per l'attuazione e la verifica dei piani di emergenza dell'impresa (business contingency plans)
- disposizioni che assicurino l'accesso ai dati in caso di insolvenza, risoluzione o cessazione dell'attività del fornitore di servizi
- l'obbligo del fornitore di servizi di cooperare con le autorità
- il diritto illimitato di ispezionare e sottoporre a verifiche di audit il fornitore di servizi
- i diritti di cessazione.

Ulteriori clausole sono specificatamente trattate per i seguenti ambiti:

- subesternalizzazione di funzioni essenziali o importanti
- sicurezza dei dati e dei sistemi
- diritti di accesso, di informazione e di audit
- diritti di cessazione.

7 – Conclusioni

Anche per quanto attiene la gestione di fornitori ed outsourcer, la normativa realizzata per il mondo finanziario e assicurativo può costituire un punto di riferimento ed un esempio di buona pratica valido anche per molti altri settori.

Le aziende che appartengono a settori non specificatamente normati possono quindi trarre vantaggio dalla loro consultazione.

Grazie a DORA, anche le aziende che non appartengono al settore finanziario, ma che utilizzano fornitori sottoposti alle autorità di vigilanza, avranno la certezza dell'alto livello di qualità e sicurezza dei fornitori vigilati.

8 - Bibliografia

[1] ESMA - ESMA50-164-4285 IT “Orientamenti in materia di esternalizzazione a fornitori di servizi cloud”, 2021

[2] EBA/GL/2019/02 - “Orientamenti in materia di esternalizzazione”, 2019

[3] EIOPA - EIOPA-BoS-20-002 - “Orientamenti in materia di esternalizzazione a fornitori di servizi cloud”, 2020

[4] Parlamento Europeo, “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 (Testo rilevante ai fini del SEE)”, 2022

[5] Banca d’Italia, “Circolare 285”, 2013

[6] Butti G., “Aziende resilienti”, La Comunicazione N.R.&N., 2019

[7] Butti G., “Dalla business continuity alla resilienza operativa”, La Comunicazione N.R.&N., 2022

[8] Butti G., “Manuale di resilienza”, ITER, 2023