

DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Rischi cyber e IA nella revisione dei contratti ICT

13 Novembre 2026

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper





Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Studio Legale Tributario Associato

DLA Piper

Le comunicazioni della BCE del 7 luglio 2026 e di Banca d'Italia e IVASS del 17 luglio richiamano l'adeguatezza dei contratti con i fornitori ICT. I modelli avanzati di intelligenza artificiale possono accelerare l'individuazione dei difetti di sicurezza e il loro sfruttamento, riducendo il tempo disponibile per intervenire. Banca d'Italia e IVASS chiedono adeguati requisiti contrattuali sul monitoraggio della sicurezza e sulla gestione degli aggiornamenti correttivi, o patch; la BCE collega ai contratti e ai livelli di servizio (SLA) la gestione delle modifiche urgenti.[1]

Per i dipartimenti legali di banche e assicurazioni, queste indicazioni rendono necessario verificare se i rapporti esistenti permettano all'ente di ottenere ciò che occorre durante un'emergenza. Un contratto può già prevedere obblighi di sicurezza e un addendum DORA, lasciando tuttavia incerti i tempi dell'allerta o chi debba applicare una correzione. Il rischio riguarda anche servizi che non utilizzano IA, perché gli strumenti dell'attaccante possono colpire software ordinario, infrastrutture cloud e assistenza remota. La revisione deve quindi considerare il portafoglio dei contratti ICT secondo l'esposizione e la rilevanza dei servizi, senza limitarsi agli acquisti di soluzioni di intelligenza artificiale.

Il quadro di riferimento resta DORA, che mantiene in capo all'entità finanziaria la responsabilità per i propri obblighi anche quando ricorre a terzi fornitori ICT. L'art. 30 distingue il contenuto contrattuale minimo comune dagli impegni aggiuntivi per i servizi a supporto di funzioni essenziali o importanti.[2] Le indicazioni della vigilanza richiedono di verificare quali clausole siano sufficienti e quali integrate. Le soluzioni negoziali esaminate di seguito sviluppano questa verifica: il loro contenuto deve essere proporzionato al servizio e rimane distinto da quanto direttamente imposto dalle fonti.

Impostare la revisione dei rapporti in essere

La prima attività consiste nel confrontare il contratto con la prestazione effettiva. Una clausola pensata per la licenza di un prodotto può essere inadeguata se il fornitore ha poi assunto la gestione dell'applicazione o ottenuto accessi remoti. Legale e procurement devono quindi ricostruire con le funzioni ICT e di sicurezza il perimetro del rapporto. L'analisi permette di formulare richieste attuabili, evitando

1 BCE, Addressing AI-enabled cybersecurity threats, 7 luglio 2026, Annex 1; comunicazioni di Banca d'Italia e IVASS del 17 luglio 2026 sulla resilienza operativa digitale e i modelli avanzati di IA.

2 Regolamento (UE) 2022/2554, artt. 28–31; regolamento delegato (UE) 2024/1774, titolo II, artt. 10 e 21.

vedi l'articolo online

obblighi riferiti ad attività che nessuna delle parti svolge.

Una struttura contrattuale utile combina disposizioni comuni con obblighi collegati all'esposizione. Se il fornitore accede ai sistemi dell'ente, rilevano il controllo delle credenziali e la possibilità di interrompere connessioni compromesse. Nei servizi cloud o esposti su internet, il contratto deve presidiare gli ambienti nei quali sono trattati i dati e garantita la continuità. Per il software installato presso l'ente, occorre coordinare patch, installazione e supporto della versione utilizzata. I profili possono sovrapporsi e vanno valutati insieme alla criticità delle funzioni servite.

Questa ricognizione può essere formalizzata in una scheda tecnica allegata al contratto, che assegni le attività e raccolga i parametri concordati. La scheda deve identificare le prestazioni e poter essere aggiornata con una procedura definita. Se il fornitore introduce un nuovo accesso amministrativo, l'ente deve esserne informato prima dell'attivazione per valutarne i presidi. Il perimetro iniziale perde utilità se le variazioni del servizio non comportano un riesame degli obblighi.

Nei rapporti esistenti, le priorità devono seguire il rischio e i tempi per correggere le carenze. La relazione con piano di lavoro richiesta da Banca d'Italia e IVASS entro il 31 dicembre 2026 può rappresentare anche gli interventi sui fornitori; la BCE ha fissato al 31 ottobre 2026 il piano delle istituzioni significative. Sono scadenze documentali, che tuttavia non differiscono le misure urgenti. I destinatari restano distinti: i chiarimenti Banca d'Italia del 14 ottobre riferiscono la relazione consolidata ai soggetti italiani direttamente vigilati, escludendo controllate estere e componenti assicurative; per queste ultime rileva separatamente la comunicazione IVASS.[3]

Integrare gli obblighi di informazione e di allerta

Il primo gruppo di clausole da riesaminare riguarda le informazioni che il fornitore deve mettere a disposizione. Un obbligo di comunicare soltanto gli incidenti può lasciare non presidiata la scoperta di una vulnerabilità ancora non sfruttata, quando vi è invece spazio per prevenire il danno. Il contratto dovrebbe distinguere le due situazioni e collegare a ciascuna un obbligo di collaborazione. Nel quadro ordinario di gestione del rischio ICT, l'art. 10 del regolamento delegato 2024/1774 richiede all'ente di verificare che i fornitori gestiscano le vulnerabilità dei servizi e segnalino tempestivamente almeno quelle critiche, insieme a statistiche e tendenze.[2]

Per consentire questa valutazione, la clausola deve precisare quali informazioni accompagnino l'allerta e da quando decorra il termine per inviarla. È utile riferirsi alla conoscenza acquisita dalle funzioni del fornitore che possono rilevare il problema, evitando che un passaggio interno ne rinvii la comunicazione. Anche una segnalazione attendibile dell'ente deve attivare la verifica. L'avviso iniziale può essere incompleto, purché indichi i servizi potenzialmente interessati, le precauzioni disponibili e il successivo aggiornamento. Attendere l'analisi definitiva potrebbe sottrarre all'ente il tempo necessario a proteggersi.

I tempi vanno concordati con le funzioni tecniche secondo l'esposizione e la reperibilità richiesta, prevedendo canali alternativi se quello ordinario non funziona. Occorre disciplinare gli aggiornamenti fino alla chiusura e la conferma dell'efficacia della correzione. Per una vulnerabilità diffusa, un riscontro espresso sull'eventuale coinvolgimento dei servizi evita che l'ente interpreti il silenzio come assenza di rischio. Sono obblighi negoziali: le comunicazioni della vigilanza non fissano un termine unico di allerta per tutti i fornitori.

Le informazioni sul software rendono più efficace questa verifica. Un'applicazione può incorporare una libreria di terzi che utilizza, a sua volta, un componente vulnerabile: l'ente potrebbe esserne esposto senza conoscerne il nome. La Software Bill of Materials, o SBOM, è una distinta dei componenti e delle loro relazioni che aiuta a individuarli. Il contratto può richiederne la consegna o l'accesso protetto, riferiti alla versione utilizzata e aggiornata quando cambia. Le indicazioni ENISA e CISA offrono riferimenti tecnici volontari per concordarne il contenuto.[4]

L'accesso va coordinato con la riservatezza del fornitore. Un estratto dell'inventario o una verifica indipendente possono essere soluzioni ragionevoli se permettono decisioni con dettaglio e tempi ade-

3 Banca d'Italia, chiarimenti del 14 ottobre 2026 sul seminario sulla resilienza operativa digitale. Per l'impostazione proporzionata, ESAs, JC 2026 25, 31 luglio 2026, parr. 5–8 e Annex.

4 ENISA, Technical Advisory for Software Bill of Materials, 22 ottobre 2026, §§ 1.2 e 2–4; CISA e partner, 2026 Minimum Elements for a Software Bill of Materials, 29 luglio 2026, v. 2.1.

guati. Un'attestazione annuale generica difficilmente consente di accertare subito la presenza di una libreria. Occorre anche permettere l'uso dei dati da parte delle funzioni competenti e degli incaricati, preservando i diritti di auditor e autorità secondo la normativa vigente. La negoziazione riguarda quindi l'utilizzabilità delle informazioni, oltre alla loro disponibilità.

Precisare responsabilità e tempi per le correzioni

La clausola che disciplinal e attività di manutenzione è spesso il punto nel quale l'impegno di sicurezza deve diventare una prestazione determinata. Espressioni come «applicare regolarmente gli aggiornamenti» o «rimediare tempestivamente» possono lasciare incerto il livello di servizio atteso e diventare fonte di contrasto proprio quando occorre intervenire. Va verificato anche se la manutenzione copra le vulnerabilità che non hanno ancora provocato un guasto. Il contratto dovrebbe disciplinarne la gestione, assegnando un termine massimo in funzione dell'urgenza e definendo quando inizia a decorrere.

Le classi di urgenza devono riflettere le condizioni del servizio, oltre al punteggio tecnico della vulnerabilità. Un difetto già sfruttato contro un'applicazione accessibile da internet può richiedere priorità rispetto a uno teoricamente grave in una funzione isolata. Il legale deve ottenere dalle funzioni competenti criteri utilizzabili nel contratto e una procedura di riesame, evitando che il dissenso sospenda le protezioni necessarie. Anche una promessa di monitoraggio continuo richiede perimetro e modalità verificabili, per evitare interpretazioni incompatibili con il servizio atteso.

Occorre poi distinguere le fasi dell'intervento. Il produttore sviluppa e rende disponibile la patch; chi gestisce l'ambiente ne verifica la compatibilità e organizza l'installazione, che può spettare a un altro manutentore o all'ente stesso. Una clausola che imponga a un solo soggetto di «correggere» il difetto può risultare difficile da applicare se quel soggetto non controlla l'intero processo. Il contratto deve assegnare le attività e coordinarne i tempi, chiarendo quali dipendenze richiedano la collaborazione del cliente. Il fornitore deve segnalarle tempestivamente e proseguire le attività eseguibili; eventuali proroghe richiedono condizioni definite, motivazione e accordo.

La disponibilità della patch può far decorrere il termine per installarla, ma resta da disciplinare il periodo precedente. Si immagini che il fornitore gestisca il portale della banca e utilizzi un prodotto di un terzo, per il quale la correzione non sia ancora pronta. L'ente ha interesse a ottenere subito una valutazione e misure temporanee, ad esempio una restrizione degli accessi o la disattivazione della funzione esposta. Il contratto dovrebbe obbligare il fornitore a coinvolgere il produttore, seguire il rilascio della correzione e adottare le protezioni nella propria disponibilità. La mancata consegna della patch da parte di un terzo non dovrebbe paralizzare queste attività.

Le misure temporanee comportano decisioni che devono rimanere governabili dall'ente. Disattivare una funzione può ridurre il rischio, ma anche impedire operazioni verso i clienti: la proposta del fornitore deve quindi chiarirne efficacia e impatto sul servizio. L'eventuale differimento della correzione definitiva richiede un'approvazione motivata, con scadenza e riesame, anziché conseguire automaticamente all'adozione di una protezione provvisoria. Se il contenimento è insufficiente, occorre poter sospendere soltanto il componente o la connessione interessati, coordinando la misura con la continuità delle attività dell'ente.

Quando la patch è disponibile, la procedura deve consentire autorizzazioni e test abbastanza rapidi senza compromettere la stabilità del servizio. Vanno definite le verifiche dopo l'installazione e le modalità di ripristino in caso di malfunzionamento, ricordando che il ritorno alla versione precedente può reintrodurre la vulnerabilità. Anche gli SLA richiedono un raccordo: le finestre di manutenzione o le esclusioni per attività programmate non dovrebbero autorizzare rinvii incompatibili con l'urgenza. L'ente deve poter distinguere una correzione soltanto messa a disposizione da una correzione installata e verificata nell'ambiente interessato.

La disciplina va completata con il supporto del prodotto. Una versione non più assistita può richiedere una migrazione per ottenere aggiornamenti di sicurezza. Il contratto dovrebbe indicare supporto garantito e preavviso di cessazione, collegandoli a un piano sostitutivo. Per il software installato, correzioni di sicurezza separate dagli aggiornamenti funzionali, ove fattibile, possono facilitare il collaudo. Vanno anche distinti i costi della manutenzione inclusa nel canone da quelli di una sostituzione o migrazione: lasciarli aperti rende più difficile intervenire nell'emergenza.

Rafforzare la sicurezza e verificarne l'attuazione

Le clausole di sicurezza devono considerare anche il fornitore come possibile punto d'ingresso dell'attacco. Se viene compromessa la postazione di chi svolge assistenza remota, la connessione autorizza-

ta può esporre i sistemi dell'ente. Occorre quindi delimitare gli accessi e i privilegi necessari, prevedere autenticazione robusta e accessi amministrativi temporanei, e disciplinare la revoca quando cessano le esigenze. La compromissione anche sospetta deve poter attivare una comunicazione rapida e la sospensione delle connessioni, mantenendo una modalità sicura di assistenza. L'efficacia di queste previsioni dipende dalla coerenza tra contratto, procedure del fornitore e controlli effettivamente esercitabili dall'ente.

L'obbligo di collaborazione durante un incidente deve poi coprire le informazioni necessarie a ricostruirlo. Le parti dovrebbero concordare conservazione e disponibilità tempestiva dei log, ossia delle registrazioni delle attività sui sistemi, e la preservazione delle evidenze pertinenti, tutelando i dati personali e le informazioni dei clienti. Il fornitore deve aggiornare l'ente senza attendere che quest'ultimo completi la classificazione regolamentare. I termini per le segnalazioni dell'ente alla vigilanza non vanno semplicemente riprodotti come tempi concessi al fornitore, perché occorre lasciare spazio alla valutazione e alla notifica.[5] L'art. 30, par. 2, lett. f), DORA richiede inoltre assistenza per gli incidenti relativi al servizio senza costi aggiuntivi o a costo stabilito ex ante: tale previsione va coordinata con le tariffe di assistenza e le eventuali esclusioni del contratto.

Gli impegni devono essere controllabili anche al di fuori dell'incidente. La reportistica dovrebbe consentire di comprendere quali vulnerabilità restino aperte, da quanto tempo e per quale ragione, rendendo visibili ritardi ed eccezioni. Frequenza e dettaglio possono essere graduati secondo il servizio, ferma l'esigenza di informazioni tempestive sui casi urgenti. Certificazioni e report indipendenti sono utili se il loro perimetro corrisponde alle attività affidate; le clausole devono consentire approfondimenti quando emergono esclusioni o rilievi. Per i servizi a supporto di funzioni essenziali o importanti, eventuali garanzie alternative devono preservare l'effettività dei diritti di accesso, ispezione e audit previsti da DORA.

I diritti di controllo comprendono anche test e piani di continuità. Occorre verificarne l'adeguatezza agli scenari attuali e la partecipazione del fornitore alle prove dell'ente secondo il quadro applicabile. Le regole di ingaggio devono consentire verifiche utili proteggendo servizio e altri clienti. Le prove dovrebbero includere attacchi assistiti dall'IA e compromissioni simultanee, verificando la capacità del fornitore di intervenire su più ambienti. Nei piani di disaster recovery va considerato che ambienti separati possono condividere componenti o sistemi di accesso. Le prove devono accertare la recuperabilità di dati e configurazioni anche con il percorso ordinario indisponibile, rispetto agli obiettivi concordati di ripristino e perdita tollerata dei dati.

Il funzionamento di questi obblighi dipende infine dalla supply chain. Un'allerta rapida del contraente principale è poco utile se il subfornitore gli comunica il problema giorni dopo. Occorre verificare che gli impegni assunti verso l'ente siano sostenuti da obblighi e flussi informativi compatibili lungo la catena. Per i servizi a supporto di funzioni essenziali o importanti, o parti significative di esse, il regolamento delegato 2025/532 disciplina responsabilità del fornitore, monitoraggio e condizioni della subfornitura. Le modifiche sostanziali richiedono preavviso e possibilità di approvazione od opposizione, con diritti di cessazione nei casi previsti.[6] La verifica deve comprendere anche le dipendenze tecniche rilevanti che non emergano dal solo elenco dei subfornitori.

Aggiornare requisiti e rimedi nei contratti esistenti

L'integrazione degli obblighi tecnici deve essere accompagnata da una procedura per mantenerli adeguati. Una clausola può riconoscere all'ente il diritto di chiedere nuove misure quando cambiano le indicazioni della vigilanza o l'esposizione del servizio. Occorre però chiarire come il fornitore debba valutarle e in quale termine le parti debbano concordarne l'attuazione. Il diritto di formulare una richiesta non equivale al potere di imporre unilateralmente la modifica. Le misure urgenti che possono essere attivate senza attendere una nuova negoziazione vanno quindi identificate in anticipo, insieme ai soggetti autorizzati e alle conseguenze sul servizio.

Anche la disciplina economica merita una scelta espressa. Le parti possono stabilire quali adeguamenti siano compresi nel corrispettivo, ad esempio perché necessari a mantenere il livello di sicurezza promesso, e quali modifiche ulteriori debbano essere valutate separatamente. Le comunicazioni della vigilanza non risolvono automaticamente la ripartizione dei costi tra cliente e fornitore. Se quest'ultimo

5 Regolamento delegato (UE) 2025/301, art. 5.

6 Regolamento delegato (UE) 2025/532, artt. 3-6.

vedi l'articolo online

non può attuare l'aggiornamento o manca un accordo entro il termine stabilito, il contratto deve offrire una soluzione praticabile, che può comprendere misure compensative o un diritto di uscita. L'accettazione del rischio residuo richiede una decisione consapevole dell'ente e un riesame, senza ridurre gli obblighi inderogabili.

Perché tali diritti siano utilizzabili, vanno coordinati con il regime generale dei rimedi. Un termine previsto per sanare un ordinario inadempimento può essere troppo lungo per una vulnerabilità sfruttata; la procedura urgente deve poter operare senza attenderne la scadenza. La sospensione mirata richiede condizioni chiare di attivazione e riattivazione, evitando che l'ente sia esposto a contestazioni per aver protetto i propri sistemi. Per carenze gravi o persistenti occorre verificare i diritti di risoluzione o recesso e la loro relazione con i piani correttivi. La legge applicabile e il testo complessivo del contratto restano determinanti per scegliere e rendere efficaci queste soluzioni.

La stessa lettura trasversale serve per la responsabilità. I service credits, ossia le riduzioni del corrispettivo per mancato rispetto degli SLA, possono risultare inadeguati se configurati come rimedio esclusivo anche per violazioni degli obblighi di sicurezza. Vanno inoltre esaminati esclusioni e massimali rispetto ai costi di contenimento e ripristino e chiarito se l'obbligo di prestare assistenza continui una volta raggiunto il limite risarcitorio. Un diritto di uscita «senza penali» deve essere coordinato con impegni minimi di spesa e costi di migrazione. Il piano di transizione deve rendere possibile il trasferimento del servizio, garantendo collaborazione e continuità per il periodo necessario secondo quanto pattuito.

Nel formalizzare l'accordo, occorre concordare la prevalenza dell'addendum sulle disposizioni incompatibili del contratto, compresi gli SLA e le condizioni standard richiamate online. Vanno inoltre identificate le versioni dei documenti incorporati e regolate le modifiche, perché il fornitore non possa svuotare gli impegni negoziati aggiornando una policy esterna. Se alcuni parametri sono rinviati alla scheda tecnica, devono essere completati e approvati entro termini coerenti con l'esposizione del servizio. La firma di un allegato con scadenze o attività ancora indeterminate rinvia il problema che l'integrazione avrebbe dovuto risolvere.

Il programma di revisione deve seguire l'esecuzione degli accordi. A ogni carenza vanno associati una richiesta al fornitore, un responsabile interno e un termine, documentando le misure temporanee e le decisioni sui punti aperti. Dopo la firma, legale e procurement verificano con i responsabili del servizio l'attivazione degli obblighi e i primi riscontri. Gli organi aziendali possono così conoscere l'avanzamento effettivo dell'adeguamento, distinguendo i contratti modificati dai presidi operativi e dalle esposizioni ancora da gestire.

vedi l'articolo online



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it