EBA/GL/2017/05

11/09/2017

Orientamenti

Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)

1. Conformità e obblighi di comunicazione

Status giuridico degli orientamenti

1. Il presente documento contiene orientamenti emanati in applicazione dell'articolo 16 del regolamento (UE) n. 1093/20101. Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano la posizione dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione in un particolare settore. Ai sensi dell'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010, le autorità competenti sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di comunicazione

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono comunicare all'ABE entro 13.11.2017 se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento "EBA/GL/2017/05" da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le comunicazioni sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

1 Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

2. Oggetto, ambito di applicazione e definizioni

Oggetto e ambito di applicazione

5. I presenti orientamenti, redatti in conformità dell'articolo 107, paragrafo 3, della direttiva 2013/36/UE[2], mirano a garantire la convergenza delle pratiche di vigilanza per la valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT), a norma del processo di revisione e valutazione prudenziale (SREP) di cui all'articolo 97 della direttiva 2013/36/UE e ulteriormente illustrato negli Orientamenti dell'ABE sulle procedure e sulle metodologie comuni per il processo di revisione e valutazione prudenziale (SREP)[3]. In particolare, i presenti orientamenti specificano i criteri di valutazione che le autorità competenti dovrebbero applicare durante la valutazione prudenziale della governance e della strategia degli enti in materia di ICT e durante la valutazione prudenziale dell'esposizione ai rischi e del controllo dei rischi ICT degli enti. I presenti orientamenti sono parte integrante degli Orientamenti dell'ABE sullo SREP.

6. Le autorità competenti dovrebbero attenersi ai presenti orientamenti conformemente al livello di applicazione dello SREP stabilito negli Orientamenti dell'ABE sullo SREP, nonché al modello di impegno minimo e ai requisiti di proporzionalità in essi stabiliti.

Destinatari

7. I presenti orientamenti sono rivolti alle autorità competenti di cui all'articolo 4, paragrafo 2, punto i), del regolamento (UE) n. 1093/2010.

Definizioni

8. Se non diversamente specificato, i termini utilizzati e definiti nella direttiva 2013/36/UE, nel regolamento (UE) n. 575/2013 e nelle definizioni di cui agli Orientamenti dell'ABE sullo SREP hanno il medesimo significato nei presenti orientamenti. In aggiunta, ai fini dei presenti orientamenti, si applicano le seguenti definizioni:

[2] Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (1) - GU L 176 del 27.6.2013.

[3] ABE/GL/2014/13

Sistemi ICT	Tecnologie dell'informazione e della comunicazione adottate come parte di un meccanismo o di una rete di interconnessione a supporto delle operazioni di un ente.
Servizi ICT	I servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono ad esempio: servizi di alimentazione, archiviazione, elaborazione e comunicazione dei dati, ma anche servizi di monitoraggio, di supporto all'azienda e al processo decisionale.
Rischio di disponibilità e continuità ICT	Il rischio che le prestazioni e la disponibilità dei sistemi e dei dati ICT siano influenzati negativamente, incluso il rischio di incapacità di ripristinare tempestivamente i servizi dell'ente a causa di un guasto delle componenti ICT hardware o software; debolezze nella gestione dei sistemi ICT; o qualsiasi altro evento, come ulteriormente esposto nell'allegato.
Rischio di sicurezza ICT	Il rischio di accesso non autorizzato ai sistemi e ai dati dei sistemi ICT dell'ente, dall'interno o dall'esterno (ad esempio nel caso di attacchi informatici), come ulteriormente esposto nell'allegato.
Rischio relativo ai cambiamenti ICT	Il rischio derivante dall'incapacità dell'ente di gestire i cambiamenti dei sistemi ICT in modo tempestivo e controllato, in particolare per quanto concerne programmi di modifica complessi e di grandi dimensioni, come ulteriormente esposto nell'allegato.
Rischio di integrità dei dati ICT	Il rischio che i dati archiviati ed elaborati dai sistemi ICT siano incompleti, inesatti o incoerenti nei vari sistemi, in seguito, ad esempio, a controlli ICT carenti o assenti durante le varie fasi del ciclo di vita dei dati ICT (vale a dire, progettazione dell'architettura dei dati, costruzione del modello e/o dei dizionari di dati, verifica degli inserimenti dei dati, controllo delle estrazioni, dei trasferimenti e delle elaborazioni dei dati, inclusi i risultati forniti), tali da compromettere la capacità di un ente di fornire servizi e di produrre le informazioni finanziarie e relative alla gestione (del rischio) in modo corretto e tempestivo come ulteriormente esposto nell'allegato.
Rischio di esternalizzazione ICT	Il rischio che il ricorso a una terza parte o a un'altra entità del gruppo (esternalizzazione intra-gruppo), per la fornitura di sistemi ICT o servizi connessi incida negativamente sulle prestazioni e sulla gestione del rischio dell'ente, come ulteriormente esposto nell'allegato.

3. Attuazione

Data di applicazione

9. I presenti orientamenti si applicano a partire dal 1° gennaio 2018.

4. Requisiti in materia di valutazione dei rischi ICT

Titolo 1 - Disposizioni generali

10. Le autorità competenti dovrebbero effettuare la valutazione dei rischi ICT, della governance e della strategia relativa all'ICT come parte del processo SREP, in conformità del modello di impegno minimo e dei criteri di proporzionalità di cui al titolo 2 degli Orientamenti dell'ABE sullo SREP. In particolare, ciò significa che:

    a. la frequenza della valutazione dei rischi ICT dipenderà dal modello di impegno minimo stabilito in base alla categoria SREP assegnata all'ente, nonché al suo programma di revisione prudenziale; e

    b. la profondità, il livello di dettaglio e l'intensità della valutazione dell'ICT dovrebbero essere proporzionati a dimensione, struttura e contesto operativo dell'ente, nonché alla natura, ampiezza e complessità delle sue attività.

11. Nei presenti orientamenti, il principio di proporzionalità si applica all'ambito di applicazione, alla frequenza e all'intensità dell'impegno e del dialogo di vigilanza con un ente, nonché alle aspettative di vigilanza sugli standard che l'ente dovrebbe soddisfare.

12. Le autorità competenti possono prendere in considerazione il lavoro svolto in precedenza dall'ente o dalle autorità competenti stesse nell'ambito delle valutazioni di altri rischi o elementi legati allo SREP, e basarsi su di esso per aggiornare la valutazione. In particolare, durante l'esecuzione delle valutazioni specificate nei presenti orientamenti, le autorità competenti dovrebbero scegliere l'approccio e la metodologia di valutazione prudenziale più appropriati e proporzionalmente adeguati all'ente e dovrebbero altresì utilizzare la documentazione esistente disponibile (ad es. relazioni e altri documenti pertinenti, assemblee dei dirigenti (incaricati della gestione dei rischi), risultati delle ispezioni in loco) per formare la propria valutazione.

13. Le autorità competenti dovrebbero riassumere i risultati delle valutazioni dei criteri specificati nei presenti orientamenti e utilizzarli per trarre debite conclusioni sulla valutazione degli elementi dello SREP, come specificato negli Orientamenti dell'ABE sullo SREP.

14. In particolare, i risultati della valutazione della governance e della strategia riguardante l'ICT, effettuata in conformità del Titolo 2 dei presenti orientamenti dovrebbero riflettersi nel riepilogo dei risultati della valutazione dell'elemento dello SREP relativo alla governance e ai controlli interni a livello aziendale, come specificato nel titolo 5 degli Orientamenti dell'ABE sullo SREP, ed essere rispecchiati dal rispettivo punteggio di tale elemento dello SREP. Inoltre, le autorità competenti dovrebbero considerare che

qualsiasi impatto negativo significativo della valutazione della strategia ICT sulla strategia aziendale dell'ente, o qualsiasi preoccupazione relativa al fatto che l'ente non abbia sufficienti risorse e capacità ICT per effettuare e sostenere importanti cambiamenti strategici pianificati, dovrebbero contribuire all'analisi del modello imprenditoriale eseguita in conformità del titolo 4 degli Orientamenti dell'ABE sullo SREP.

15. L'esito della valutazione dei rischi ICT, come specificato nel titolo 3 dei presenti orientamenti, dovrebbe influenzare i risultati della valutazione del rischio operativo e dovrebbe incidere sul pertinente punteggio, come specificato nel titolo 6.4 degli Orientamenti dell'ABE sullo SREP.

16. Si noti che, mentre in generale le autorità competenti dovrebbero valutare le sottocategorie dei rischi come parte delle categorie principali (ad es. il rischio ICT dovrebbe essere valutato come parte del rischio operativo), laddove le autorità competenti ritengano che alcune sottocategorie siano rilevanti, potranno decidere di valutarle individualmente. A tal fine, laddove l'autorità competente identifichi un rischio ICT come rilevante, i presenti orientamenti riportano una tabella di punteggio (tabella 1) da utilizzare per assegnare un punteggio individuale alla sottocategoria di rischio ICT, in linea con l'approccio generale, contenuto negli Orientamenti dell'ABE sullo SREP, per l'assegnazione di punteggio ai rischi che impattano sul capitale.

17. Per decidere quando il rischio ICT sia da considerare rilevante e, di conseguenza, se vi sia la possibilità di valutare e assegnare un punteggio a detto rischio considerandolo come una sottocategoria distinta del rischio operativo, le autorità competenti possono fare riferimento ai criteri di cui alla sezione 6.1 degli Orientamenti dell'ABE sullo SREP.

18. Nell'applicazione dei presenti orientamenti, le autorità competenti dovrebbero, se del caso, riferirsi all'elenco non esaustivo delle sottocategorie e degli scenari di rischio ICT definiti nell'allegato, tenendo presente che l'allegato si incentra sui rischi ICT che possono causare gravi perdite. Le autorità competenti possono escludere taluni rischi ICT presenti nella classificazione, se non pertinenti alla loro valutazione. Gli enti sono tenuti a mantenere le proprie classificazioni di rischio anziché utilizzare la classificazione dei rischi ICT di cui all'allegato.

19. Laddove i presenti orientamenti si applichino ai gruppi bancari transfrontalieri e alle loro entità e nel caso in cui sia stato istituito un collegio delle autorità di vigilanza, le autorità competenti dovrebbero, in virtù della collaborazione ai fini della valutazione SREP, in conformità della sezione 11.1 degli Orientamenti dell'ABE sullo SREP, coordinare il più possibile l'ambito di applicazione preciso e dettagliato di ciascuna informazione in modo uniforme per tutte le entità del gruppo.

Titolo 2 - Valutazione della governance e della strategia degli enti in materia di ICT

2.1 Principi generali

20. Le autorità competenti dovrebbero valutare se i sistemi di governance e di controllo interno dell'ente coprano adeguatamente i sistemi ICT e i rischi ad essi correlati e se l'organo di amministrazione tratti adeguatamente tali aspetti, poiché l'ICT è fondamentale per il corretto funzionamento di un ente.

21. Durante l'esecuzione di tale valutazione, le autorità competenti dovrebbero fare riferimento ai requisiti e agli standard di organizzazione interna e di controllo dei rischi, come specificato negli Orientamenti ABE sull'organizzazione interna (GL 44)[4] e nelle linee guida internazionali relative a tale ambito, nella misura in cui applicabili data la specificità dei sistemi e dei rischi ICT.

22. La valutazione di cui al presente titolo non copre gli elementi specifici della governance, della gestione e del controllo dei sistemi ICT che riguardano i rischi ICT specifici trattati nel titolo 3 dei presenti orientamenti, ma si concentra sulle seguenti aree:

    a. strategia ICT – se l'ente dispone di una strategia ICT che è adeguatamente gestita ed è in linea con la strategia aziendale dell'ente;

    b. governance generale – se l'organizzazione interna generale dell'ente è adeguata rispetto ai sistemi ICT dello stesso; e

    c. rischio ICT nel sistema di gestione dei rischi dell'ente – se il sistema di gestione dei rischi e di controllo interno dell'ente protegge adeguatamente i sistemi ICT dello stesso.

23. Il punto a) di cui al paragrafo 22, pur fornendo informazioni sugli elementi relativi alla governance dell'ente, dovrebbe contribuire principalmente alla valutazione del modello imprenditoriale, di cui al titolo 4 degli Orientamenti dell'ABE sullo SREP. I punti b) e c) completano ulteriormente le valutazioni relative ai temi di cui al titolo 5 degli Orientamenti dell'ABE sullo SREP e la valutazione descritta nei presenti orientamenti dovrebbe contribuire alle rispettive valutazioni di cui al titolo 5 degli Orientamenti dell'ABE sullo SREP.

24. L'esito della presente valutazione dovrebbe incidere, se del caso, sulla valutazione della gestione e controllo dei rischi di cui al titolo 3 dei presenti orientamenti.

2.2 Strategia ICT

25. In conformità della presente sezione, le autorità competenti dovrebbero valutare se l'ente disponga di una strategia ICT soggetta a un'adeguata sorveglianza da parte dell'organo di amministrazione dell'ente,

[4] Orientamenti ABE sull'organizzazione interna (GL 44), del 27 settembre 2011.

coerente con la strategia aziendale, specialmente per quanto concerne l'aggiornamento dei propri sistemi ICT e la pianificazione o attuazione di importanti e complesse modifiche alle stesse, e che supporti il modello imprenditoriale dell'ente.

2.2.1 Sviluppo e adeguatezza della strategia ICT

26. Le autorità competenti dovrebbero verificare che l'ente disponga di un framework per la preparazione e lo sviluppo della strategia ICT, proporzionato alla natura, ampiezza e complessità delle sue attività in materia di ICT. Nell'esecuzione delle valutazioni, le autorità competenti dovrebbero considerare se:

    a. l'alta dirigenza[5] della/e linea/e di business sia adeguatamente coinvolta nella definizione delle priorità strategiche delle ICT dell'ente e, parallelamente, l'alta dirigenza della funzione ICT sia al corrente dello sviluppo, della progettazione e dell'avvio delle principali strategie e iniziative aziendali al fine di garantire il costante allineamento tra i sistemi, i servizi e la funzione ICT (ossia, i responsabili della realizzazione e gestione di tali sistemi e servizi) e la strategia aziendale dell'ente, e che l'ICT sia adeguatamente aggiornato;

    b. la strategia ICT sia documentata e supportata da piani di attuazione concreti, in particolar modo riguardanti le tappe principali e la pianificazione delle risorse (comprese quelle finanziarie e umane) per garantire che siano realistici e consentano l'attuazione della strategia ICT;

    c. l'ente aggiorni periodicamente la strategia ICT, in particolare laddove si modifichi la strategia aziendale, per assicurare un allineamento costante tra l'ICT e gli obiettivi, i piani e le attività aziendali a medio e lungo termine;

    d. l'organo di amministrazione approvi la strategia ICT e i piani di attuazione e monitori la loro attuazione.

2.2.2 Attuazione della strategia ICT

27. Laddove la strategia ICT dell'ente richieda l'attuazione di modifiche all'ICT importanti e complesse, o che comportino implicazioni significative per il modello imprenditoriale dell'ente, le autorità competenti dovrebbero valutare se l'ente disponga di un sistema di controllo adeguato rispetto a dimensioni, attività ICT e livello delle modifiche, per supportare la corretta attuazione della strategia ICT dell'ente. Nell'esecuzione delle valutazioni, le autorità competenti dovrebbero considerare se il sistema dei controlli:

    a. includa processi di governance (ad es. monitoraggio e reporting dello stato di avanzamento e del budget) e organi competenti (ad es. una struttura di gestione dei progetti (project management office - PMO), un gruppo direttivo responsabile dell'ICT o equivalente) per sostenere in modo efficace l'attuazione dei programmi strategici ICT;

    b. abbia definito e assegnato i ruoli e le responsabilità per l'attuazione dei programmi strategici dell'ICT, prestando particolare attenzione all'esperienza dei principali soggetti interessati

[5] Per i termini "alta dirigenza" e "organo di gestione" sono applicabili le definizioni di cui all'articolo 3, paragrafo 7 (organo di gestione), e all'articolo 3, paragrafo 9 (alta dirigenza), della direttiva 2013/36/UE del 26 giugno 2013.

nell'organizzazione, nella direzione e nel monitoraggio di importanti e complesse modifiche apportate all'ICT e nella gestione dei più ampi impatti organizzativi e umani (ad es. gestione della resistenza al cambiamento, formazione, comunicazione);

c. coinvolga le funzioni di controllo indipendenti e di audit interno per assicurare che i rischi connessi all'attuazione della strategia ICT siano stati individuati, valutati ed efficacemente mitigati e che il sistema di governance previsto per l'attuazione di detta strategia ICT sia efficace;

d. comprenda un processo di pianificazione e revisione della pianificazione sufficientemente flessibile per far fronte a eventuali problemi importanti riscontrati (ad es. problemi o ritardi nell'attuazione) o sviluppi esterni (ad es. cambiamenti significativi nel contesto aziendale, problematiche tecnologiche o innovazioni), allo scopo di garantire un adeguamento tempestivo del piano strategico di attuazione.

2.3 Governance generale

28. In conformità del titolo 5 degli Orientamenti dell'ABE sullo SREP, le autorità competenti dovrebbero valutare se l'ente disponga di una struttura societaria adeguata e trasparente che sia "adatta allo scopo" e abbia messo in atto adeguati meccanismi di governance. Per quanto riguarda in particolare i sistemi ICT, e in linea con gli Orientamenti ABE sull'organizzazione interna, tale valutazione dovrebbe verificare che l'ente disponga di:

    a. una struttura organizzativa solida e trasparente, con responsabilità relative all'ICT definite in modo chiaro, comprendente l'organo di amministrazione e i relativi comitati, ove i responsabili dell'ICT(ad es. il direttore informatico (CIO), il direttore operativo (COO) o una posizione equivalente) dispongano di un adeguato accesso indiretto o diretto all'organo di amministrazione, affinché le informazioni e le questioni importanti in materia di ICT siano adeguatamente riportate, discusse e decise a livello dell'organo di amministrazione;

    b. un organo di amministrazione che conosca e tenga in debito conto i rischi associati all'ICT.

29. In conformità della sezione 5.2 degli Orientamenti dell'ABE sullo SREP, le autorità competenti dovrebbero altresì valutare se la politica e la strategia di esternalizzazione dell'ente in materia di ICT tenga in considerazione, se del caso, l'impatto dell'esternalizzazione dell'ICT sulle attività dell'ente e sul suo modello imprenditoriale.

2.4 Rischi ICT nel sistema di gestione del rischio

30. Nel valutare la gestione dei rischi e dei controlli interni dell'ente, come previsto dal titolo 5 degli Orientamenti dell'ABE sullo SREP, le autorità competenti dovrebbero valutare se il sistema di gestione dei rischi e dei controlli interni dell'ente protegga adeguatamente i sistemi ICT dell'ente, in modo proporzionato alla dimensione e all'attività dell'ente e al suo profilo di rischio ICT, come definito nel titolo 3. In particolare, le autorità competenti dovrebbero determinare se:

    a. la propensione al rischio e il processo di valutazione dell'adeguatezza del capitale interno (ICAAP) coprono i rischi ICT, nell'ambito della categoria più ampia del rischio operativo, per la definizione della strategia globale del rischio e la determinazione del capitale interno;

    b. i rischi ICT rientrano nell'ambito di applicazione dei sistemi a livello aziendale di gestione del rischio e dei controlli interni dell'ente.

31. Le autorità competenti dovrebbero effettuare la valutazione di cui al precedente punto a) tenendo in considerazione sia gli scenari attesi che quelli avversi, ad esempio quelli inclusi nelle prove di stress specifiche per l'ente o di vigilanza.

32. Con particolare riguardo al punto b), le autorità competenti dovrebbero valutare se le funzioni di controllo indipendenti e di audit interno, come specificato nel paragrafo 104, lettere a) e d) e nel paragrafo 105, lettere a) e c) degli Orientamenti dell'ABE sullo SREP, siano idonee a garantire un livello sufficiente di indipendenza tra la funzione ICT e le funzioni di controllo e audit, tenendo in considerazione la dimensione e il profilo di rischio ICT dell'ente.

2.5 Sintesi dei risultati

33. Tali risultati dovrebbero riflettersi in un riepilogo dei rilievi, ai sensi del titolo 5 degli Orientamenti dell'ABE sullo SREP, e dovrebbero essere inclusi nel rispettivo punteggio, in linea con le considerazioni di cui alla tabella 3 degli Orientamenti dell'ABE sullo SREP.

34. Per concludere la suddetta valutazione, i seguenti punti dovrebbero essere considerati ai fini della valutazione della strategia ICT:

    a. se le autorità competenti giungono alla conclusione che il sistema di governance dell'ente è inadeguato per sviluppare e attuare la strategia ICT dell'ente, a norma del punto 2.2, ciò dovrebbe influire sulla valutazione della governance dell'ente di cui al titolo 5, punto 87, lettera a), degli Orientamenti dell'ABE sullo SREP;

    b. se, in virtù delle valutazioni di cui al punto 2.2, le autorità competenti giungono alla conclusione che si verificherebbe un disallineamento significativo tra la strategia ICT e la strategia aziendale, che potrebbe avere un significativo impatto negativo sugli obiettivi aziendali e/o finanziari a lungo termine, sulla sostenibilità e/o sul modello imprenditoriale o sulle aree/linee di business dell'ente identificate come le più rilevanti nel paragrafo 62, lettera a), degli Orientamenti dell'ABE sullo SREP, ciò dovrebbe contribuire a formare la valutazione del modello imprenditoriale di cui al titolo 4, punto 70, lettere b) e c); e

c. se, in virtù delle valutazioni di cui al punto 2.2, le autorità competenti giungono alla conclusione che l'ente non dispone di sufficienti risorse ICT e capacità di realizzazione dell'ICT per eseguire e sostenere importanti cambiamenti strategici pianificati, ciò dovrebbe contribuire a formare la valutazione del modello imprenditoriale di cui al titolo 4, punto 70, lettera b), degli Orientamenti dell'ABE sullo SREP.

Titolo 3 - Valutazione dell'esposizione ai rischi ICT e dei relativi controlli degli enti

3.1 Considerazioni generali

35. Le autorità competenti dovrebbero valutare se l'ente abbia adeguatamente individuato, valutato e mitigato i propri rischi ICT. Questo processo dovrebbe essere parte del sistema di gestione del rischio operativo ed essere coerente con l'approccio applicato al rischio operativo.

36. Le autorità competenti dovrebbero innanzitutto individuare i rischi ICT intrinseci rilevanti a cui l'ente è, o potrebbe essere, esposto, ed effettuare una valutazione dell'efficacia del sistema di gestione dei rischi ICT degli enti, nonché delle procedure e dei controlli per ridurre tali rischi. L'esito della valutazione dovrebbe riflettersi in una sintesi dei risultati che viene inclusa nel punteggio di rischio operativo di cui agli Orientamenti sullo SREP. Quando il rischio ICT è considerato significativo e le autorità competenti desiderano assegnare un punteggio individuale, la Tabella 1 deve essere utilizzata per assegnare un punteggio in quanto sottocategoria del rischio operativo.

37. Durante la valutazione di cui al presente titolo, le autorità competenti dovrebbero utilizzare tutte le fonti informative disponibili, come stabilito nel titolo 6, paragrafo 127, degli Orientamenti dell'ABE sullo SREP, ad esempio le attività di gestione dei rischi dell'ente, le relazioni e gli esiti, come base per l'individuazione delle loro priorità di valutazione prudenziale. Le autorità competenti dovrebbero altresì utilizzare altre fonti di informazione per effettuare tale valutazione, tra cui, se del caso:

    a. le autovalutazioni dei rischi e dei controlli ICT (se incluse nelle informazioni ICAAP);
    b. le informazioni di gestione (Management Information - MI) correlate al rischio ICT presentate all'organo di amministrazione dell'ente, ad esempio la reportistica dei rischi ICT periodica e a seguito di incidente (compreso il database delle perdite operative), i dati relativi all'esposizione ai rischi ICT da parte della funzione di gestione del rischio dell'ente;
    c. i rilievi degli audit interni ed esterni relativi all'ICT segnalati al comitato per l'audit interno dell'ente.

3.2 Identificazione dei rischi ICT rilevanti

38. Le autorità competenti dovrebbero identificare i rischi ICT rilevanti a cui l'ente è o potrebbe essere esposto osservando i passaggi indicati di seguito.

3.2.1 Analisi del profilo di rischio ICT dell'ente

39. Durante la revisione del profilo di rischio ICT dell'ente, le autorità competenti dovrebbero prendere in considerazione tutte le informazioni pertinenti riguardanti le esposizioni ai rischi ICT dell'ente, comprese le informazioni di cui al paragrafo 37, e le carenze o debolezze rilevanti individuate nell'organizzazione

ICT e nei controlli a livello aziendale di cui al titolo 2 dei presenti Orientamenti e, se del caso, esaminare tali informazioni in modo appropriato. Nell'ambito della presente revisione, le autorità competenti dovrebbero considerare quanto segue:

a. il potenziale impatto di una interruzione significativa del funzionamento dei sistemi ICT dell'ente sul sistema finanziario, a livello nazionale o internazionale;
b. se l'ente possa essere soggetto a rischi di sicurezza ICT o a rischi di disponibilità e continuità ICT dovuti alla dipendenza da Internet, all'elevato utilizzo di soluzioni ICT innovative o ad altri canali di distribuzione aziendale che potrebbero rendere l'ente un possibile obiettivo di attacchi informatici;
c. se l'ente possa essere maggiormente esposto a rischi di sicurezza ICT , rischi di disponibilità e continuità ICT , rischi di integrità dei dati ICT o rischi relativi ai cambiamenti ICT dovuti alla complessità (ad esempio, derivante da fusioni o acquisizioni) o all'obsolescenza dei suoi sistemi ICT;
d. se l'ente stia attuando cambiamenti sostanziali ai propri sistemi ICT e/o alla funzione ICT (ad esempio, a seguito di fusioni, acquisizioni, dismissioni o sostituzione dei principali sistemi ICT) che possono avere effetti negativi sulla stabilità o sul regolare funzionamento dei sistemi ICT e comportare rischi ICT rilevanti di disponibilità e continuità, di sicurezza, relativi ai cambiamenti o di integrità dei dati;
e. se l'ente abbia esternalizzato i servizi o i sistemi ICT, all'interno o all'esterno del gruppo, e se pertanto possa essere esposto a rischi di esternalizzazione ICT rilevanti ;
f. se l'ente stia attuando misure aggressive di riduzione dei costi delle ICT che possano portare alla riduzione di investimenti in ICT, risorse e competenze informatiche necessari e possano aumentare l'esposizione a tutti i tipi di rischi ICT illustrati nella classificazione;
g. se l'ubicazione di importanti centri operativi/dati ICT (ad es. regioni, paesi) possa esporre l'ente a catastrofi naturali (ad es. inondazioni, terremoti), instabilità politica o conflitti sindacali e disordini civili che possano portare ad un aumento significativo dei rischi di disponibilità e continuità e di sicurezza ICT.

3.2.2 Analisi dei sistemi e dei servizi ICT critici

40. Nell'ambito del processo di identificazione dei rischi ICT che possano avere un potenziale impatto prudenziale significativo sull'ente, le autorità competenti dovrebbero esaminare la documentazione dell'ente e formulare un parere indicando quali sistemi e servizi ICT sono critici per l'adeguata operatività, disponibilità e continuità e per la sicurezza delle attività essenziali dell'ente.

41. A tal fine, le autorità competenti dovrebbero esaminare la metodologia e i processi applicati dall'ente per identificare sistemi e servizi ICT critici, considerando che alcuni di questi possono essere considerati critici da parte dell'ente dal punto di vista della continuità e della disponibilità operativa, della sicurezza (ad es. la prevenzione delle frodi) e/o della riservatezza (ad es. dati riservati). Durante la revisione, le autorità competenti dovrebbero considerare che i sistemi e servizi ICT critici devono soddisfare almeno una delle seguenti condizioni:

a. supportare le principali operazioni di business e i principali canali di distribuzione (ad es. bancomat, Internet e mobile banking) dell'ente;

b. supportare i processi fondamentali di governance e le funzioni aziendali, compresa la gestione dei rischi (ad es. sistemi di gestione dei rischi e della tesoreria);

c. rispondere a requisiti legali o regolamentari specifici (se del caso) che impongono maggiori requisiti di disponibilità, resilienza, riservatezza o sicurezza (ad es. legislazione in materia di protezione dei dati o eventuali obiettivi in materia di tempi di ripristino (Recovery Time Objectives - RTO - tempo massimo entro il quale deve essere ripristinato un sistema o un processo dopo un incidente) e obiettivi in materia di punti di ripristino (Recovery Point Objective - RPO - periodo di tempo massimo durante il quale i dati possono essere persi in caso di incidente) per alcuni servizi di importanza sistemica (laddove applicabili);

d. elaborare o conservare dati riservati o sensibili per i quali l'accesso non autorizzato potrebbe avere un impatto significativo sulla reputazione dell'ente, sui risultati finanziari o sulla solidità e continuità della propria attività (ad es. database contenente dati sensibili del cliente);

e. fornire funzionalità di base fondamentali per il corretto funzionamento dell'ente (ad es. servizi di telecomunicazione e connettività, sicurezza ICT e cyber).

3.2.3 Identificazione dei rischi rilevanti relativi ai sistemi e ai servizi ICT critici

42. Tenendo conto delle analisi condotte sul profilo di rischio ICT dell'ente e dei sistemi e servizi ICT critici sopra esposti, le autorità competenti dovrebbero formulare un parere sui rischi ICT rilevanti che, secondo la loro valutazione prudenziale, possono avere un impatto prudenziale significativo sui sistemi e servizi ICT critici.

43. Per la valutazione dell'impatto potenziale dei rischi ICT sui sistemi e sui servizi ICT critici di un ente, le autorità competenti dovrebbero considerare:

a. l'impatto finanziario, compresi (ma non limitatamente a) la perdita di fondi o attività, la possibile compensazione del cliente, i costi legali e di riparazione, i danni contrattuali, i mancati profitti;

b. il potenziale impatto per l'interruzione dell'operatività, considerando (ma non limitatamente a) la criticità dei servizi finanziari interessati, il numero di clienti e/o filiali e dipendenti potenzialmente interessati;

c. il potenziale impatto sulla reputazione dell'ente, sulla base dell'importanza del servizio bancario o dell'attività operativa interessata (ad es., furto di dati dei clienti); il profilo esterno/la visibilità dei sistemi ICT e dei servizi interessati (ad es. sistemi di mobile banking o online banking, punti vendita, bancomat o sistemi di pagamento);

d. l'impatto normativo, comprese la possibile censura pubblica da parte del regolatore, multe o addirittura modifica delle autorizzazioni.

e. L'impatto strategico sull'ente, ad esempio se i piani strategici di prodotto o quelli operativi vengono compromessi o sottratti.

44. Le autorità competenti dovrebbero pertanto effettuare una mappatura dei rischi ICT considerati rilevanti nelle seguenti categorie di rischio, per le quali ulteriori descrizioni ed esempi dei rischi sono

riportati nell'allegato. Le autorità competenti dovrebbero considerare i rischi ICT di cui all'allegato nell'ambito della valutazione di cui al titolo 3:

a. rischio di disponibilità e continuità ICT
b. rischio di sicurezza ICT
c. rischio relativo ai cambiamenti ICT
d. rischio di integrità dei dati ICT
e. rischio di esternalizzazione ICT

La mappatura aiuta le autorità competenti a determinare quali rischi sono rilevanti (se presenti) e dovrebbero quindi essere oggetto di un'analisi più dettagliata e/o approfondita secondo le seguenti fasi di valutazione.

3.3 Valutazione dei controlli per mitigare i rischi ICT rilevanti

45. Per valutare l'esposizione residua ai rischi ICT dell'ente, le autorità competenti dovrebbero esaminare il modo in cui l'ente identifica, monitora, valuta e mitiga i rischi rilevanti individuati dalle autorità competenti nella valutazione di cui sopra.

46. A tal fine, per i rischi ICT rilevanti identificati, le autorità competenti dovrebbero esaminare i seguenti elementi ove applicabili:

    a. le politiche e i processi di gestione dei rischi ICT e le relative soglie di tolleranza;
    b. i sistemi di gestione organizzativa e di controllo;
    c. la copertura delle attività dell'audit interno e le relative risultanze;
    d. i controlli sui rischi ICT, specifici per i rischi ICT rilevanti identificati.

47. La valutazione dovrebbe tenere in considerazione l'esito dell'analisi del sistema di gestione dei rischi e dei controlli interni di cui al titolo 5 degli Orientamenti dell'ABE sullo SREP, nonché della governance e della strategia dell'ente di cui al titolo 2 dei presenti orientamenti, poiché le carenze significative individuate in questi settori possono influenzare la capacità dell'ente di gestire e mitigare la propria esposizione ai rischi ICT. Se del caso, le autorità competenti dovrebbero altresì utilizzare le fonti d'informazione di cui al paragrafo 37 dei presenti orientamenti.

48. Le autorità competenti dovrebbero svolgere le seguenti fasi di valutazione in modo proporzionato alla natura, all'ampiezza e alla complessità delle attività dell'ente e applicando un livello di revisione prudenziale adeguato al profilo di rischio ICT dell'ente.

3.3.1 Politiche di gestione dei rischi ICT, dei processi e delle soglie di tolleranza

49. Le autorità competenti dovrebbero verificare se l'ente disponga di politiche, processi, e soglie di tolleranza adeguati per la gestione dei rischi ICT rilevanti identificati. Questi possono fare parte del sistema di gestione dei rischi operativi o di un documento separato. Ai fini della valutazione, le autorità competenti dovrebbero considerare se:

    a. la politica di gestione dei rischi è formalizzata e approvata dall'organo di amministrazione e fornisce linee guida sufficienti sulla propensione al rischio ICT dell'ente e sui principali obiettivi di gestione dei rischi ICT e/o sulle relative soglie di tolleranza applicate. Inoltre, la politica di gestione dei rischi ICT dovrebbe essere comunicata a tutte le parti interessate;
    b. la suddetta politica copre tutti gli elementi significativi per la gestione dei rischi ICT rilevanti individuati;
    c. l'ente ha attuato un processo e procedure sottostanti per l'identificazione (ad es. autovalutazioni del controllo dei rischi (RCSA), analisi dello scenario di rischio) e il monitoraggio dei rischi ICT rilevanti;
    d. l'ente dispone di una reportistica relativa alla gestione dei rischi ICT che fornisce informazioni tempestive all'alta dirigenza e all'organo di amministrazione e che permette all'alta dirigenza e/o all'organo di amministrazione di valutare e monitorare se i piani e le misure di mitigazione dei rischi ICT degli enti siano coerenti con la propensione al rischio approvata e/o con le soglie di tolleranza (laddove pertinenti) e di monitorare i cambiamenti dei rischi ICT rilevanti.

3.3.2 Sistema di gestione organizzativa e controllo

50. Le autorità competenti dovrebbero valutare come i ruoli e le responsabilità relativi alla gestione dei rischi siano incorporati e integrati nell'organizzazione interna per gestire e controllare i rischi ICT rilevanti identificati. A questo proposito, le autorità competenti dovrebbero valutare se l'ente dimostri:

    a. ruoli e responsabilità definiti chiaramente per quanto concerne l'identificazione, la valutazione, il monitoraggio, la mitigazione, la segnalazione e il controllo dei rischi ICT rilevanti in questione;
    b. che responsabilità e ruoli relativi ai rischi siano chiaramente comunicati, assegnati e incorporati in tutte le aree pertinenti (ad es. linee di business, IT) e nei processi dell'organizzazione, inclusi i ruoli e le responsabilità per la raccolta e l'aggregazione delle informazioni sui rischi e la segnalazione delle stesse all'alta dirigenza e/o all'organo di amministrazione;
    c. che le attività di gestione dei rischi ICT siano eseguite con risorse umane e tecniche sufficienti e qualitativamente appropriate. Per valutare la credibilità dei piani di attenuazione del rischio, le autorità competenti dovrebbero inoltre valutare se l'ente abbia stanziato sufficienti risorse finanziare e/o altre risorse necessarie per la loro attuazione;
    d. un adeguato follow-up e un intervento dell'organo di amministrazione in merito a importanti rilievi da parte delle funzioni di controllo indipendenti riguardanti i rischi ICT, considerando l'eventuale delega di alcuni aspetti a un comitato, laddove presente;

e. che le eccezioni alle norme e alle politiche in materia di ICT in vigore siano registrate e soggette a una revisione e segnalazione documentata da parte della funzione di controllo indipendente, con particolare attenzione ai rischi correlati.

3.3.3 Copertura dell'audit interno e relative risultanze

51. Le autorità competenti dovrebbero valutare se la funzione di audit interno svolga in modo efficace gli audit relativi al framework applicabile di controllo dei rischi ICT, valutando se:

a. il framework di controllo dei rischi ICT è sottoposto a revisione con il livello di qualità, dettaglio e frequenza richiesto e in modo proporzionato alle dimensioni, alle attività e al profilo di rischio ICT dell'ente;

b. il piano di audit include controlli sui rischi ICT critici individuati dall'ente;

c. le principali risultanze di audit sull'ICT, incluse le azioni concordate, sono segnalati all'organo di amministrazione; e

d. le risultanze degli audit sull'ICT, incluse le azioni concordate, sono monitorate e le relazioni relative ai progressi sono periodicamente riesaminate dall'alta dirigenza e/o dal comitato per il controllo interno.

3.3.4 Controlli sui rischi ICT, specifici per i rischi ICT rilevanti identificati

52. Le autorità competenti dovrebbero valutare se l'ente disponga di specifici controlli per gestire i rischi ICT rilevanti identificati. Le sezioni che seguono forniscono un elenco non esaustivo dei controlli specifici da prendere in considerazione durante la valutazione dei rischi rilevanti di cui al punto 3.2.3 che sono stati connessi alle seguenti categorie di rischio ICT:

a. Rischi di disponibilità e continuità ICT;
b. rischi di sicurezza ICT;
c. rischi relativi ai cambiamenti ICT;
d. rischi di integrità dei dati ICT;
e. rischi di esternalizzazione ICT.

(a) Controlli per la gestione dei rischi ICT rilevanti di disponibilità e continuità ICT

53. Oltre ai requisiti di cui agli Orientamenti dell'ABE sullo SREP (paragrafi 279-281), le autorità competenti dovrebbero valutare se l'ente disponga di un framework adeguato per individuare, comprendere, misurare e mitigare i rischi di disponibilità e continuità ICT.

54. Per questa valutazione, le autorità competenti dovrebbero, in particolar modo, considerare se il framework:

a. individui i processi critici dell'ICT i relativi sistemi ICT di supporto che dovrebbero far parte del piano di resilienza e continuità aziendale mediante:

i. un'analisi completa della relazione di dipendenza tra i processi aziendali critici e i sistemi di supporto;

ii. la determinazione degli obiettivi di ripristino per i sistemi ICT di supporto (ad esempio generalmente determinati dalle attività aziendali e/o dai regolamenti in termini di RTO e RPO);

iii. adeguati piani di emergenza per consentire la disponibilità, la continuità e il ripristino di sistemi e servizi ICT critici al fine di ridurre le interruzioni delle operazioni di un ente entro limiti accettabili.

b. disponga di resilienza aziendale, standard e politiche ambientali di controllo della continuità e controlli operativi che includano:

i. misure per evitare che un singolo scenario, incidente o disastro possa avere un impatto sia sui sistemi ICT di produzione che su quelli di ripristino;

ii. procedure di backup e ripristino dei sistemi ICT per software e dati critici, che assicurino che tali backup siano memorizzati in una posizione sicura e sufficientemente remota in modo che non possano essere distrutti o corrotti in caso di incidente o disastro;

iii. soluzioni di monitoraggio per la rilevazione tempestiva degli incidenti legati alla disponibilità o continuità delle ICT;

iv. un processo documentato di gestione e di escalation, che fornisca inoltre indicazioni sui diversi ruoli e responsabilità di gestione e di escalation degli incidenti, sui membri del/dei comitato/i di crisi e sulla catena di comando in caso di emergenza;

v. misure fisiche per proteggere le infrastrutture ICT critiche dell'ente (ad es. centri dati) da rischi ambientali (ad es. allagamenti e altri disastri naturali) e garantire un ambiente operativo appropriato per i sistemi ICT (ad es. aria condizionata);

vi. processi, ruoli e responsabilità per garantire che anche i sistemi e i servizi ICT esternalizzati siano coperti da adeguati piani e soluzioni di resilienza aziendale e di continuità;

vii. soluzioni di pianificazione e monitoraggio delle prestazioni e della capacità dei sistemi e servizi ICT critici, con requisiti di disponibilità definiti, per individuare tempestivamente importanti limitazioni a prestazioni e capacità;

viii. soluzioni per proteggere attività o servizi Internet critici (ad es. servizi di e-banking), ove necessario e appropriato, da attacchi "denial of service" e da altri attacchi informatici provenienti da Internet mirati a impedire o disturbare l'accesso a tali attività e servizi.

c. testi le soluzioni di disponibilità e continuità delle risorse ICT, ipotizzando una gamma di scenari realistici che includano attacchi informatici e test di fail-over e backup per software e dati critici che:

i. siano pianificati, formalizzati e documentati e i cui risultati vengano utilizzati per rafforzare l'efficacia delle soluzioni di disponibilità e continuità delle risorse ICT;

ii. includano le parti interessate e le funzioni interne all'organizzazione, quali i responsabili delle linee di business, compresi i team responsabili della continuità aziendale, degli incidenti e gestione delle crisi, nonché le parti interessate esterne, appartenenti all'ecosistema;

iii. coinvolgano adeguatamente l'organo di amministrazione e l'alta dirigenza (ad esempio, in quanto parte dei team di gestione delle crisi), che vengono informati dei risultati dei test.

(b) Controlli per la gestione dei rischi rilevanti di sicurezza ICT

55. Le autorità competenti dovrebbero valutare se l'ente disponga di un framework efficace per individuare, comprendere, misurare e mitigare il rischio di sicurezza ICT. Per questa valutazione, le autorità competenti dovrebbero, in particolar modo, considerare se il framework tenga conto di:

a. ruoli e responsabilità definiti in modo chiaro per quanto riguarda:
   i. le persone e/o i comitati responsabili della gestione quotidiana della sicurezza ICT e dell'elaborazione delle politiche generali di sicurezza ICT, prestando particolare attenzione alla loro necessaria indipendenza;
   ii. la progettazione, attuazione, gestione e monitoraggio dei controlli di sicurezza ICT;
   iii. la protezione di sistemi e servizi ICT critici, mediante, ad esempio, un processo di valutazione delle vulnerabilità, la gestione di patch di software, la protezione degli end-point (ad es. virus malware), strumenti per la rilevazione e la protezione da intrusioni;
   iv. il monitoraggio, la classificazione e la gestione degli incidenti di sicurezza ICT, esterni o interni; tra cui l'intervento in caso di incidenti e la ripresa e il ripristino dei sistemi e dei servizi ICT;
   v. valutazioni periodiche e proattive delle minacce per mantenere adeguati controlli di sicurezza.

b. una politica di sicurezza ICT che prenda in considerazione e, laddove appropriato, sia conforme a standard e norme di sicurezza in materia di ICT riconosciute a livello internazionale (ad esempio il "principio del privilegio minimo", ovvero limitare l'accesso al livello minimo, che consenta il normale funzionamento per la gestione dei diritti di accesso, e il principio della "difesa in profondità", ovvero meccanismi di sicurezza a più livelli che aumentano la sicurezza del sistema nel suo insieme per la progettazione di un'architettura di sicurezza);

c. un processo per identificare sistemi e servizi ICT e requisiti di sicurezza adeguati che riflettano il potenziale rischio di frode e/o possibili usi impropri e/o abusi di dati riservati, nonché i presidi di sicurezza documentate da adottare per tali sistemi, servizi e dati ICT identificati, in linea con la tolleranza del rischio dell'ente e la cui corretta attuazione viene costantemente monitorata;

d. un processo documentato di gestione e di escalation degli incidenti di sicurezza, che fornisca indicazioni sui diversi ruoli e responsabilità di gestione e di escalation degli incidenti, sui membri del/dei comitato/i di crisi e sulla catena di comando in caso di emergenze relative alla sicurezza;

e. registrazione delle attività degli utenti e degli amministratori (logging) per consentire un monitoraggio efficace, la rilevazione e l'intervento tempestivo in caso di attività non autorizzate e per assistere o condurre indagini forensi sugli incidenti relativi alla sicurezza. L'ente dovrebbe disporre di politiche di registrazione che definiscano i tipi appropriati di registrazioni (logs) da custodire e il loro periodo di conservazione;

f. azioni o iniziative informative e di sensibilizzazione per informare tutti i livelli organizzativi dell'ente circa l'utilizzo sicuro e la protezione dei sistemi ICT dell'ente, il loro ruolo nel mitigare le violazioni della sicurezza, nonché i principali rischi per la sicurezza ICT (e altri) di cui devono essere consapevoli, in particolare per ciò che concerne le minacce informatiche esistenti e in evoluzione (ad es. virus informatici, possibili abusi o attacchi interni o esterni, attacchi informatici);

g. adeguate misure di sicurezza fisiche (ad es. telecamere a circuito chiuso, allarmi antifurto, porte di sicurezza) per impedire l'accesso fisico non autorizzato ai sistemi ICT critici e sensibili (ad es. centri dati);

h. misure per proteggere i sistemi ICT da attacchi provenienti da Internet (ovvero attacchi informatici) o da altre reti esterne (ad es. connessioni di telecomunicazioni tradizionali o connessioni con partner di fiducia). Le autorità competenti dovrebbero valutare se il framework dell'ente consideri:

   i. un processo e soluzioni per la conservazione di un inventario completo e aggiornato e una panoramica di tutti i punti di connessione di rete verso l'esterno (ad es. siti web, applicazioni Internet, WIFI, accesso remoto) attraverso i quali terze parti potrebbero infiltrarsi nei sistemi ICT interni;

   ii. misure di sicurezza monitorate e gestite attentamente (ad es. firewall, server proxy, mail relay, antivirus e scanner per i contenuti) per rendere sicuro il traffico di rete in entrata e in uscita (ad es. posta elettronica) e le connessioni di rete verso l'esterno attraverso le quali terze parti potrebbero infiltrarsi nei sistemi ICT interni;

   iii. processi e soluzioni per proteggere siti web e applicazioni che possono essere direttamente attaccate da Internet e/o dall'esterno, che possono servire da punto di ingresso nei sistemi ICT interni. In generale, questi comprendono una combinazione di pratiche riconosciute di sviluppo sicuro, pratiche di hardening ed esame delle vulnerabilità dei sistemi ICT e/o l'attuazione di soluzioni di sicurezza aggiuntive come, ad esempio, firewall applicativi e/o sistemi di rilevamento delle intrusioni (IDS) e/o sistemi di prevenzione delle intrusioni (IPS);

   iv. periodici penetration test per valutare l'efficacia delle misure e dei processi di sicurezza ICT realizzati internamente e a difesa da attacchi esterni. Questi test dovrebbero essere eseguiti da personale e/o esperti esterni aventi le competenze necessarie; i risultati di tali test dovrebbero essere documentati e le conclusioni presentate all'alta dirigenza e/o all'organo di amministrazione. Laddove necessario e applicabile, questi test dovrebbero essere utilizzati dall'ente per capire dove è necessario perfezionare i controlli e i processi di sicurezza e/o dove ottenere maggiori garanzie sulla loro efficacia.

(c) Controlli per la gestione dei rischi rilevanti relativi ai cambiamenti ICT

56. Le autorità competenti dovrebbero valutare se l'ente disponga di un framework efficace per individuare, comprendere, misurare e mitigare il rischio di cambiamento ICT, proporzionato alla natura, all'ampiezza e alla complessità delle attività dell'ente e al profilo di rischio ICT dell'ente. Il framework dell'ente dovrebbe coprire i rischi connessi allo sviluppo, al collaudo e all'approvazione dei cambiamenti dei sistemi ICT, compreso lo sviluppo o il cambiamento del software, prima che questi vengano migrati nell'ambiente di produzione, e garantire un'adeguata gestione del ciclo di vita dell'ICT. Per questa

valutazione, le autorità competenti dovrebbero, in particolar modo, considerare se il framework tenga conto di:

a. processi documentati per la gestione e il controllo dei cambiamenti dei sistemi ICT (ad es. configurazione e gestione delle patch) e dei dati (ad es. correzione di bug o dati), assicurando l'adeguato coinvolgimento dei responsabili della gestione dei rischi ICT per importanti cambiamenti in materia di ICT che possano avere un impatto significativo sul profilo di rischio o sull'esposizione al rischio dell'ente;

b. specifiche relative alla necessaria separazione dei compiti durante le varie fasi dei processi di cambiamento ICT realizzati (ad es. progettazione e sviluppo di soluzioni, test e approvazione di nuovi software e/o modifiche, migrazione e attuazione nell'ambiente di produzione e correzione dei bug), con particolare attenzione alle soluzioni attuate e alla separazione dei compiti per gestire e controllare i cambiamenti relativi ai sistemi ICT di produzione e ai dati da parte del personale responsabile ICT (ad es. sviluppatori, amministratori di sistemi ICT, amministratori di database) o da qualsivoglia altro soggetto (ad es. utenti aziendali, fornitori di servizi);

c. ambienti di test che riflettano adeguatamente gli ambienti di produzione;

d. un inventario delle attività delle applicazioni e dei sistemi ICT presenti nell'ambiente di produzione, nonché nell'ambiente di test e sviluppo, affinché i cambiamenti necessari (ad es. aggiornamenti della versione, patch di sistemi, modifiche di configurazione) possano essere correttamente gestiti, eseguiti e monitorati per i sistemi ICT interessati;

e. un processo di monitoraggio e gestione del ciclo di vita dei sistemi ICT utilizzati, per garantire che continuino a soddisfare e supportare i requisiti effettivi di gestione aziendale e dei rischi, per assicurare che le soluzioni e i sistemi ICT utilizzati siano ancora supportati dai fornitori e che ciò sia correlato da procedure adeguate per il ciclo di vita di sviluppo software (SDLC);

f. un sistema di controllo del codice sorgente del software e procedure appropriate per impedire modifiche non autorizzate al codice sorgente del software sviluppato internamente;

g. un processo per condurre uno screening di sicurezza e di vulnerabilità di sistemi e software ICT nuovi o sottoposti a cambiamenti sostanziali, prima che vengano messi in produzione ed esposti a eventuali attacchi informatici;

h. un processo e soluzioni per prevenire la diffusione non autorizzata o non intenzionale di dati riservati durante la sostituzione, l'archiviazione, l'eliminazione o la distruzione di sistemi ICT;

i. un processo indipendente di revisione e validazione per ridurre i rischi generati da errori umani durante l'applicazione di cambiamenti ai sistemi ICT che possano avere un importante effetto negativo su disponibilità, continuità o sicurezza dell'ente (ad es. importanti modifiche alla configurazione del firewall) o sulla sicurezza dell'ente (ad es. cambiamenti nei firewall).

(d) Controlli per la gestione dei rischi rilevanti di integrità dei dati ICT

57. Le autorità competenti dovrebbero valutare se l'ente disponga di un framework efficace per individuare, comprendere, misurare e mitigare il rischio di integrità dei dati ICT, proporzionato alla natura, all'ampiezza e alla complessità delle attività dell'ente e al profilo di rischio ICT dell'ente. Il framework dell'ente dovrebbe considerare i rischi connessi al mantenimento dell'integrità dei dati archiviati e

trattati dai sistemi ICT. Per questa valutazione, le autorità competenti dovrebbero, in particolar modo, considerare se il framework tenga conto di:

a. una politica che definisca i ruoli e le responsabilità per la gestione dell'integrità dei dati nei sistemi ICT (ad es. architetto dati, responsabili dati[6], depositari dei dati[7], proprietari/gestori dei dati[8]) e indichi quali dati sono fondamentali dal punto di vista dell'integrità e debbano pertanto essere sottoposti a specifici controlli ICT (ad es. controlli di convalida degli input automatici, controlli di trasferimento dati, riconciliazioni, ecc.) o a revisioni (ad es. un controllo di compatibilità con l'architettura dei dati) nelle varie fasi del ciclo di vita dei dati ;

b. un'architettura dei dati, un modello e/o un dizionario dati documentati, convalidati dai soggetti aziendali e IT interessati per supportare la necessaria coerenza dei dati nei sistemi ICT e per far sì che l'architettura dei dati, il modello e/o il dizionario dati siano conformi alle esigenze aziendali e di gestione dei rischi;

c. una politica volta a delineare in quali casi è consentito l'utilizzo di strumenti di End User Computing e il grado di affidamento attribuibile in particolare per quanto riguarda l'identificazione, la registrazione e la documentazione di importanti soluzioni di End User Computing (ad es. quando sono elaborati dati importanti), e i livelli di sicurezza attesi per prevenire modifiche non autorizzate, sia all'interno dello strumento stesso, sia per i dati in esso archiviati;

d. processi documentati di gestione delle eccezioni per risolvere problematiche identificate legate all'integrità dei dati ICT, in linea con la loro importanza e livello di riservatezza.

58. Per gli enti sottoposti a vigilanza che rientrano nel campo di applicazione dei "Principi in materia di efficace aggregazione e reportistica dei dati di rischio" BCBS 239[9], le autorità competenti dovrebbero verificare che l'analisi dei rischi dell'ente relativa alle sue capacità di aggregazione e reportistica dei dati di rischio sia in linea con i principi e la documentazione a riguardo, tenendo conto della tempistica di attuazione e delle disposizioni transitorie disciplinati negli stessi Principi.

(e) Controlli per la gestione dei rischi rilevanti di esternalizzazione dei sistemi ICT

59. Le autorità competenti dovrebbero valutare se la strategia di esternalizzazione dell'ente, in linea con i requisiti di cui agli orientamenti del CEBS sull'esternalizzazione [Guidelines on outsourcing del CEBS (2006)] e l'obbligo di cui al paragrafo 85, lettera d), degli Orientamenti dell'ABE sullo SREP, si applichi adeguatamente all'esternalizzazione ICT, compreso il caso di esternalizzazione intra-gruppo che prevede una fornitura di servizi ICT all'interno del gruppo. Nel valutare i rischi di esternalizzazione dei sistemi ICT, le autorità competenti dovrebbero tenere conto del fatto che tali rischi possono essere trattati anche nell'ambito della valutazione dei rischi operativi intrinseci, ai sensi del paragrafo 239, lettera j), degli Orientamenti dell'ABE sullo SREP, così da evitare di svolgere lo stesso lavoro o conteggio due volte.

[6] Il responsabile dati si occupa di utilizzo e trattamento dati.

[7] Il depositario dei dati è responsabile della custodia, del trasporto e della conservazione in sicurezza dei dati.

[8] Il gestore dei dati è responsabile della gestione e dell'adeguatezza dei dati (sia a livello di contenuto, sia di metadati).

[9] Comitato di Basilea per la vigilanza bancaria, Principi per un'efficace aggregazione e reportistica dei dati di rischio, gennaio 2013, disponibile online: http://www.bis.org/publ/bcbs239.pdf.

60. In particolare, le autorità competenti dovrebbero valutare se l'ente disponga di un framework efficace per individuare, comprendere e misurare il rischio di esternalizzazione dei sistemi ICT e, in particolare, se disponga di controlli e di un ambiente di controllo per mitigare i rischi connessi ai servizi ICT esternalizzati, proporzionati alle dimensioni, all'attività e al profilo di rischio ICT dell'ente e che comprendano:

   a. una valutazione dell'impatto dell'esternalizzazione dei sistemi ICT sulla gestione dei rischi dell'ente in relazione all'utilizzo di fornitori di servizi (ad es. i fornitori di servizi cloud) e dei loro servizi durante la procedura di appalto, che sia documentata e presa in considerazione dall'alta dirigenza o dall'organo di amministrazione per la decisione di esternalizzare o meno i servizi. L'ente dovrebbe esaminare le politiche di gestione dei rischi relativi alle ICT e i controlli e l'ambiente di controllo delle ICT del fornitore di servizi per garantire che soddisfino gli obiettivi di gestione dei rischi interni e la propensione al rischio dell'ente. Tale revisione dovrebbe essere periodicamente aggiornata durante il periodo di esternalizzazione contrattuale, tenendo conto delle caratteristiche dei servizi esternalizzati;

   b. un monitoraggio dei rischi ICT dei servizi esternalizzati durante il periodo contrattuale di esternalizzazione, nell'ambito della gestione dei rischi dell'ente, che si integri nella reportistica relativa alla gestione dei rischi ICT dell'ente (ad es. reportistica relativa alla continuità aziendale, alla sicurezza);

   c. un monitoraggio e un confronto dei livelli di servizio ricevuti con quelli stabiliti nel contratto che dovrebbero far parte del contratto di esternalizzazione o dell'accordo sul livello dei servizi (SLA);

   d. personale, risorse e competenze adeguati per monitorare e gestire i rischi ICT relativi ai servizi esternalizzati.

3.4 Sintesi dei risultati e punteggio

61. A seguito della valutazione di cui sopra, le autorità competenti dovrebbero formulare un parere sul rischio ICT dell'ente. Detto parere dovrebbe riflettersi in una sintesi dei risultati che le autorità competenti dovrebbero prendere in considerazione al momento dell'assegnazione di un punteggio per il rischio operativo di cui alla tabella 6 degli Orientamenti dell'ABE sullo SREP. Le autorità competenti dovrebbero basare il proprio parere sui rischi ICT rilevanti, tenendo conto delle considerazioni che seguono per contribuire alla valutazione dei rischi operativi:

   a. Considerazioni in materia di rischi

      i. esposizione ai rischi e profilo di rischio ICT dell'ente;
      ii. sistemi e servizi ICT critici identificati; e
      iii. livello di rilevanza dei rischi ICT in relazione ai sistemi ICT critici.

   b. Considerazioni in materia di gestione e controlli

      i. se la politica e la strategia di gestione dei rischi ICT dell'ente siano coerenti con la sua strategia generale e la propensione al rischio;

ii. se il framework organizzativo per la gestione dei rischi ICT sia solido, con responsabilità definite chiaramente e una netta separazione dei compiti tra i responsabili dei rischi e le funzioni di gestione e controllo;
iii. se i sistemi di misurazione, monitoraggio e segnalazione dei rischi ICT siano adeguati; e
iv. se i framework di controllo per i rischi ICT rilevanti siano solidi.

62. Se le autorità competenti ritengono che il rischio ICT sia rilevante e l'autorità competente decide di valutare e assegnare un punteggio a tale rischio in quanto sottocategoria del rischio operativo, la tabella riportata di seguito (tabella 1) riporta le considerazioni relative al punteggio di rischio ICT.

Tabella 1: Considerazioni prudenziali per l'assegnazione del punteggio di rischio ICT

Punteggio del rischio	Giudizio di vigilanza	Considerazioni relative al rischio intrinseco	Considerazioni per una gestione e controllo adeguati
1	Non si rileva alcun rischio di impatto prudenziale significativo sull'ente considerando il livello di rischio intrinseco, la gestione e i controlli.	• Le fonti di informazione da considerare ai sensi del paragrafo 37 non mostrano alcuna esposizione significativa al rischio ICT. • La natura del profilo di rischio ICT dell'ente, unitamente alla revisione dei sistemi ICT critici e dei rischi ICT rilevanti per i sistemi e i servizi ICT, non mostrano alcun rischio ICT rilevante.	• La politica e la strategia in materia di rischi ICT sono adeguate alla strategia e alla propensione al rischio generali. • Il framework organizzativo dei rischi ICT è solido, con responsabilità definite in modo chiaro e una netta separazione dei compiti tra i responsabili dei rischi e le funzioni di gestione e controllo. • I sistemi di misurazione, monitoraggio e
2	Si rileva un basso rischio di impatto prudenziale significativo sull'ente considerando il livello di rischio intrinseco, la gestione e i controlli.	• Le fonti di informazione da considerare ai sensi del paragrafo 37 non mostrano alcuna esposizione significativa al rischio ICT. • La natura del profilo di rischio ICT dell'ente, unitamente alla revisione dei sistemi ICT critici e dei rischi ICT rilevanti per i sistemi e i servizi ICT, mostrano una lieve esposizione al rischio ICT(ad es. non più di 2 punti su 5 nelle categorie di rischio ICT predefinite).	
3	Si rileva un rischio medio di impatto prudenziale significativo	• Le fonti di informazione da considerare ai sensi del paragrafo 37 mostrano segni di una possibile esposizione significativa	

	sull'ente considerando il livello di rischio intrinseco, la gestione e i controlli.	al rischio ICT. • La natura del profilo di rischio ICT dell'ente, unitamente alla revisione dei sistemi ICT critici e dei rischi ICT rilevanti per i sistemi e i servizi ICT, mostrano un'accentuata esposizione al rischio ICT (ad es. 3 punti, o più, su 5 nelle categorie di rischio ICT predefinite).	segnalazione dei rischi ICT sono appropriati. • Il framework di controllo per i rischi ICT è solido.
4	Si rileva un alto rischio di impatto prudenziale significativo sull'ente considerando il livello di rischio intrinseco, la gestione e i controlli.	• Le fonti di informazione da considerare ai sensi del paragrafo 37 mostrano diverse indicazioni di esposizione significativa al rischio ICT. • La natura del profilo di rischio ICT dell'ente, unitamente alla revisione dei sistemi ICT critici e dei rischi ICT rilevanti per i sistemi e i servizi ICT, mostrano un'alta esposizione al rischio ICT (ad es. 4 o 5 punti su 5 nelle categorie di rischio ICT predefinite).	

Allegato – Classificazione dei rischi ICT

5 categorie di rischi ICT, corredate da un elenco non esaustivo dei rischi ICT di elevata gravità e/o impatto operativo, reputazionale o finanziario

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
Rischi di disponibilità e continuità ICT	Inadeguata gestione della capacità	La mancanza di risorse (ad es. hardware, software, personale, fornitori di servizi) può comportare un'incapacità di offrire un servizio che soddisfi esigenze aziendali, interruzioni di sistema, degrado di servizio e/o errori operativi.	• La mancanza di capacità può influenzare la velocità di trasmissione e la disponibilità della rete (Internet) per servizi come l'Internet banking. • La mancanza di personale (interno o esterno) può comportare interruzioni di sistema e/o errori operativi.
	Guasti dei sistemi ICT	Perdita di disponibilità a causa di guasti hardware.	• Guasti/malfunzionamento di dispositivi di archiviazione (hard disk), server o altre apparecchiature ICT, causati, ad esempio, da mancanza di manutenzione.
		Perdita di disponibilità a causa di malfunzionamenti software e bug.	• Loop infinito nel software applicativo che impedisce l'esecuzione delle operazioni. • Interruzioni dovute all'uso continuo di sistemi e soluzioni ICT obsoleti che non soddisfano più i requisiti attuali di disponibilità e resilienza e/o che non sono più supportati dai loro fornitori.
	Inadeguatezza dei piani di ripristino in caso di disastro e della continuità dei sistemi ICT	Inefficienza delle soluzioni pianificate per la disponibilità e/o di continuità ICT e/o del piano di ripristino in caso di disastro (ad es. centri dati di ripristino alternativi) quando attivato per intervenire in caso di incidente.	• Le differenze di configurazione tra il centro dati primario e quello secondario possono causare l'incapacità del centro dati alternativo di fornire la continuità di servizio prevista.
	Attacchi	Attacchi per scopi diversi (ad es. movimenti militanti,	• Gli attacchi di tipo DDOS (Distributed Denial of

[10] I rischi ICT sono elencati nella categoria di rischio sulla quale hanno un impatto maggiore, ma potrebbero influenzare anche altre categorie di rischio

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
	informatici dirompenti e distruttivi	ricatto) che comportano un sovraccarico dei sistemi e della rete, impedendo agli utenti legittimi di accedere ai servizi informatici online.	Service) hanno l'intento di interrompere il servizio e vengono eseguiti tramite una moltitudine di sistemi informatici su Internet controllati da un hacker, che invia a servizi Internet una grande quantità di richieste di servizio apparentemente legittime (ad es. servizi di e-banking).
Rischi di sicurezza ICT	Attacchi informatici e altri attacchi esterni ICT	Attacchi eseguiti attraverso Internet o da reti esterne per scopi diversi (ad es. frode, spionaggio, movimenti militanti /sabotaggio, terrorismo informatico) utilizzando una gamma di tecniche (ad es. social engineering, tentativi di intrusione attraverso lo sfruttamento delle vulnerabilità, utilizzo di software malevoli) per ottenere il controllo dei sistemi ICT interni.	Diversi tipi di attacchi: • Attacchi mirati e persistenti (APT, Advanced Persistent Threat) per ottenere il controllo dei sistemi interni o rubare informazioni (ad es. informazioni relative all'identità, informazioni su carte di credito). • Software malevolo (ad es. ransomware) che crittografa i dati allo scopo di ricatto. • Contagio dei sistemi ICT interni mediante software trojan per commettere azioni malevole sui sistemi in modo celato. • Sfruttamento delle vulnerabilità di sistemi ICT e/o applicazioni (web), come SQL injection, per accedere al sistema ICT interno.
		Esecuzione di operazioni di pagamento fraudolente da parte di hacker attraverso l'accesso non autorizzato o l'elusione della sicurezza dei servizi di e-banking e di pagamento e/o attaccando e sfruttando le vulnerabilità di sicurezza dei sistemi di pagamento interni dell'ente.	• Attacchi a servizi di e-banking o di pagamento, con l'obiettivo di effettuare operazioni non autorizzate. • Creazione e invio di transazioni di pagamento fraudolente da parte dei sistemi di pagamento interni dell'ente (ad es. messaggi SWIFT fraudolenti).
		Esecuzione di operazioni in titoli fraudolente da parte di hacker attraverso l'accesso non autorizzato o l'elusione della sicurezza dei servizi di e-banking che forniscono anche l'accesso ai conti dei titoli dei clienti.	• Attacchi pump & dump tramite cui gli hacker ottengono l'accesso ai conti titoli e-banking dei clienti ed effettuano acquisti o vendite fraudolenti per influenzare il prezzo di mercato e/o ottenere guadagni in base a posizioni in titoli

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
			precedentemente stabilite.
		Attacchi su connessioni di comunicazione e conversazioni di tutti i tipi o sistemi ICT con l'obiettivo di raccogliere informazioni e/o commettere frodi.	• Intercettazione della trasmissione non protetta dei dati di autenticazione codificati in testo non crittografato.
	Insufficiente sicurezza interna delle ICT	Accesso non autorizzato dall'interno dell'ente a sistemi ICT critici per scopi diversi (ad es. frode, esecuzione e occultamento di attività commerciali illecite, furto di dati, attivismo/sabotaggio) mediante una varietà di tecniche (ad es. abusi e/o sfruttamento di privilegi, furto d'identità, ingegneria sociale, sfruttamento delle vulnerabilità dei sistemi ICT, utilizzo di software malevoli).	• Installazione di keylogger per rubare ID utente e password e ottenere l'accesso non autorizzato a dati riservati e/o commettere frodi. • Decifrare/indovinare password deboli per ottenere diritti di accesso illegittimi o elevati. • L'amministratore di sistema utilizza sistemi operativi o servizi di database (per modifiche dirette del database) per commettere frodi.
		Utilizzi non autorizzati dell'ICT dovuti a procedure e pratiche di gestione degli accessi inadeguate.	• Mancata disattivazione o eliminazione di account non necessari, ad esempio di membri del personale che hanno cambiato funzione e/o hanno lasciato l'ente, inclusi ospiti o fornitori che non hanno più bisogno di accesso, che dà luogo all'accesso non autorizzato ai sistemi ICT. • Concessione di diritti e privilegi di accesso eccessivi, consentendo accessi non autorizzati e/o di celare attività illecite.
		Minacce alla sicurezza dovute alla mancanza di responsabilizzazione in materia di sicurezza per cui i dipendenti non comprendono, trascurano o non rispettano le politiche e le procedure di sicurezza ICT.	• Dipendenti raggirati e portati a fornire assistenza per un attacco (ad es. ingegneria sociale). • Cattive pratiche relative alle credenziali: condivisione di password, utilizzo di password "facili" da indovinare, stessa password per diversi scopi, ecc. • Archiviazione di dati riservati non crittografati su computer portatili (laptop) e dispositivi portatili di archiviazione dati (ad es. chiavette USB) che possono essere persi o rubati.

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
		Archiviazione o trasferimento non autorizzato di informazioni riservate all'esterno dell'ente.	• Persone che ottengono indebitamente, comunicano deliberatamente o forniscono illegalmente informazioni riservate a persone non autorizzate o al pubblico.
	Insufficiente sicurezza fisica ICT	Uso improprio o furto di componenti ICT tramite accesso fisico che provochi danni, perdita di beni o dati o altre possibili minacce.	• Irruzione fisica in uffici e/o centri dati per appropriarsi indebitamente delle apparecchiature ICT (ad es. computer, computer portatili, soluzioni di archiviazione) e/o per copiare dati accedendo fisicamente ai sistemi ICT.
		Eventuali danni materiali alle componenti ICT, accidentali o volontari, causati da terrorismo, incidenti o manomissioni fatali/erronee da parte del personale dell'ente e/o di terzi (fornitori, personale della manutenzione).	• Terrorismo (ad es. bombe terroristiche) o sabotaggio di beni ICT. • Distruzione del centro dati in seguito a incendi, perdite d'acqua o altri fattori.
		Protezione fisica insufficiente contro le catastrofi naturali risultante nella distruzione parziale o totale di sistemi ICT /centri dati a seguito di catastrofi naturali.	• Terremoti, calore estremo, tempeste di vento, forti tempeste di neve, inondazioni, incendi, fulmini.
Rischi relativi ai cambiamenti ICT	Controlli inadeguati rispetto a cambiamenti dei sistemi ICT e sviluppo di ICT	Incidenti causati da errori o vulnerabilità non rilevati a seguito di un cambiamento di, ad esempio, software, sistemi e dati ICT (ad es. effetti imprevisti di un cambiamento o di un cambiamento gestito in modo errato a causa di mancanza di test o di pratiche di gestione del cambiamento improprie).	• Messa in produzione di software insufficientemente testati o modifiche di configurazione con effetti negativi imprevisti sui dati (ad es. corruzione, cancellazione) e/o sulle prestazioni del sistema ICT (ad es. guasto, degrado delle prestazioni). • Cambiamenti incontrollati dei sistemi ICT o dei dati nell'ambiente di produzione. • Messa in produzione di sistemi informatici e applicazioni Internet non sicuri, che creano opportunità per gli hacker di attaccare i servizi Internet forniti e/o di violare i sistemi ICT interni. • Cambiamenti incontrollati del codice sorgente del software sviluppato internamente. • Test insufficienti a causa dell'assenza di ambienti di

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
			prova adeguati.
	Architettura ICT inadeguata	Una debole gestione delle architetture ICT in fase di progettazione, costruzione e manutenzione dei sistemi ICT (ad es. software, hardware, dati) può portare, nel tempo, a sistemi ICT poco flessibili e complessi, difficili e costosi in termini di gestione, che non sono più sufficientemente allineati alle esigenze aziendali e ai requisiti di gestione dei rischi in vigore.	• Modifiche a sistemi, software e/o dati ICT gestite in modo inadeguato per un lungo periodo di tempo, che portano a sistemi e architetture ICT poco flessibili e complessi, eterogenei e difficili da gestire, causando impatti negativi sulle attività aziendali e sulla gestione del rischio (ad es. mancanza di flessibilità e agilità, incidenti e guasti ICT, costi operativi elevati, indebolimento di sicurezza e resilienza ICT, riduzione della qualità dei dati e capacità di segnalazione). • Eccessiva personalizzazione ed estensione dei pacchetti software commerciali con software sviluppato internamente, che impedisce di utilizzare versioni successive e aggiornamenti del software commerciale, generando il rischio di non essere più supportati dal fornitore.
	Gestione inadeguata del ciclo di vita e delle patch	Mancanza di un adeguato inventario di tutti i beni ICT a supporto di (e unitamente alle) pratiche di gestione del ciclo di vita e della corretta gestione delle patch. Ciò porta a sistemi ICT con patch insufficienti (e quindi più vulnerabili) e obsoleti che potrebbero non supportare le esigenze aziendali e di gestione dei rischi.	• Sistemi informatici non aggiornati e obsoleti che possono causare impatti negativi sulle attività aziendali e sulla gestione del rischio (ad es. mancanza di flessibilità e agilità, interruzioni ICT, indebolimento di sicurezza e resilienza ICT).
Rischi di integrità dei dati ICT	Trattamento o gestione inadeguati dei dati ICT	A causa di errori o guasti di sistema, di comunicazione e/o di applicazione o errori di estrazione, trasferimento e caricamento (ETL) di dati, questi potrebbero essere danneggiati o persi.	• Errore del sistema IT nel trattamento dei batch, che genera saldi non corretti nei conti bancari dei clienti. • Query eseguite in modo errato. • Perdita di dati dovuta all'errore di replica (backup) dei dati.
	Controlli di validazione dei	Errori causati da mancanti o inefficaci controlli automatizzati di alimentazione e di accettazione dei	• Formattazione/convalida insufficiente o invalida degli input dei dati nelle applicazioni e/o nelle

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
	dati progettati in modo inadeguato per i sistemi ICT	dati (ad es. dati utilizzati da terze parti), di trasferimento, di elaborazione e output di dati nei sistemi ICT (ad es. controlli di validità degli input, riconciliazione dei dati).	interfacce utente. • Assenza di controlli di riconciliazione dei dati sugli output • Assenza di controlli sui processi di estrazione dei dati eseguiti (ad es. query di database) che generano dati errati. • Utilizzo di dati esterni difettosi.
	Modifiche dei dati non adeguatamente controllate nei sistemi ICT in produzione	Errori sui dati causati dalla mancanza di controlli sulla correttezza e sulla legittimità delle manipolazioni dei dati in produzione nei sistemi ICT.	• Sviluppatori o amministratori di database che accedono e modificano i dati direttamente nei sistemi ICT di produzione in modo non controllato, ad esempio nel caso di un incidente ICT.
	Architettura di dati, flussi di dati, modelli di dati o dizionari di dati progettati e/o gestiti in modo inadeguato	Le architetture, i modelli, i flussi o i dizionari di dati gestiti in modo inadeguato possono creare più versioni degli stessi dati nei sistemi ICT che non sono più coerenti a causa di modelli di dati o definizioni dei dati applicati in modo diverso e/o delle differenze nel processo di generazione e modifica dei dati sottostanti.	• Esistenza di diversi database clienti per ogni prodotto o unità di business con diverse definizioni e campi di dati, che genera dati dei clienti inadeguati e difficili da confrontare e integrare a livello globale dell'ente o del gruppo finanziario.
Rischi di esternalizzazione ICT	Resilienza insufficiente di servizi di terzi o di altri enti del gruppo	La mancata disponibilità di servizi ICT critici esternalizzati, servizi di telecomunicazione e utenze. Perdita o corruzione di dati fondamentali/sensibili affidati al fornitore di servizi	• Mancata disponibilità dei servizi di base a causa di errori in sistemi o applicazioni ICT (esternalizzati) dei fornitori. • Interruzione dei collegamenti di telecomunicazione. • Interruzione dell'alimentazione elettrica.
	Organizzazione inadeguata dell'esternalizzazione	Grave degrado o interruzione dei servizi dovuti a processi di preparazione o di controllo inefficienti da parte del fornitore dei servizi esternalizzati. Un'inefficace organizzazione dell'esternalizzazione può provocare una mancanza di adeguate competenze e capacità per identificare, valutare, mitigare e	• Procedure inadeguate di gestione degli incidenti, meccanismi di controllo contrattuali e garanzie integrate nell'accordo per la fornitura dei servizi che aumentano la dipendenza da terzi e fornitori. • Controlli di gestione del cambiamento inadeguati relativi all'ambiente ICT del fornitore di servizi

Categorie dei rischi ICT	Rischi relativi ICT (elenco non esaustivo[10])	Descrizione del rischio	Esempi
		monitorare completamente i rischi ICT e può limitare le capacità operative degli enti.	possono causare un degrado o un'interruzione del servizio.
	Insufficiente sicurezza di terzi o altri enti del gruppo	L'attacco informatico ai sistemi ICT dei fornitori di servizi, con un impatto diretto sui servizi esternalizzati o sui dati fondamentali/riservati archiviati presso il fornitore del servizio. Personale del fornitore di servizi che ha ottenuto l'accesso non autorizzato a dati fondamentali/sensibili memorizzati presso il fornitore di servizi.	• L'attacco informatico ai fornitori di servizi da parte di criminali o terroristi, come punto di accesso ai sistemi ICT degli enti o per accedere/distruggere i dati fondamentali o sensibili archiviati presso il fornitore dei servizi. • Soggetti malintenzionati, operanti presso il fornitore di servizi, tentano di appropriarsi indebitamente e vendere dati sensibili.