Accordo tra

la Commissione Nazionale per le Società e la Borsa in Italia e

il Public Company Accounting Oversight Board negli Stati Uniti d'America sul Trasferimento di Certi Dati Personali

La Commissione Nazionale per le Società e la Borsa in Italia (CONSOB)

e

il Public Company Accounting Oversight Board (PCAOB),

ciascuna una "Parte", congiuntamente le "Parti",

agendo in buona fede, applicheranno le garanzie specificate nel presente accordo per la protezione dei dati ("Accordo") relativamente al trasferimento di dati personali;

riconoscendo l'importanza della protezione dei dati personali e di porre in atto solidi regimi per la protezione dei dati personali,

considerato l'Articolo 46(3) (b) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati" o "GDPR"),

considerate le funzioni e i poteri della CONSOB ai sensi del Decreto Legislativo n. 58/1998, del Decreto Legislativo n. 39/2010, del Regolamento (UE) n. 537/2014 del Parlamento europeo e del Consiglio del 16 aprile 2014 sui requisiti specifici relativi alla revisione legale dei conti di enti di interesse pubblico e che abroga la Decisione 2005/909/CE della Commissione, nonché l'Articolo 47 della Direttiva 2006/43/CE del Parlamento europeo e del Consiglio e la Decisione di esecuzione della Commissione sull'adeguatezza delle autorità competenti degli Stati Uniti d'America in conformità all'art. 47 paragrafo 3 della Direttiva 2006/43/CE,

considerate le funzioni e i poteri del PCAOB ai sensi del Sarbanes-Oxley Act del 2002, come modificato (il "Sarbanes-Oxley Act"),

considerato il pertinente quadro giuridico per la protezione dei dati personali nella giurisdizione delle Parti e riconoscendo l'importanza di un dialogo regolare tra le Parti,

considerata la necessità di trattare dati personali per svolgere il mandato pubblico ed esercitare i pubblici poteri di cui sono investite le Parti, e

considerata la necessità di assicurare una cooperazione internazionale efficiente tra le Parti che agiscono in conformità ai rispettivi mandati come definiti dalle leggi applicabili,

hanno raggiunto la seguente intesa:

ARTICOLO I- DEFINIZIONI

Ai fini del presente Accordo si applicano le seguenti definizioni:

(a) "Dati Personali": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come un nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

(b) "Trattamento di Dati Personali" ("**Trattamento**"): qualsiasi operazione o insieme di operazioni compiuti su Dati Personali o insiemi di Dati Personali, con o senza l'ausilio di processi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(c) "L'Autorità italiana per la Protezione dei Dati": il Garante per la protezione dei dati personali di cui all'Articolo 2-*bis* del Codice italiano in materia di protezione dei dati personali;

(d) "Comunicazione di Dati Personali": comunicazione di Dati Personali da una Parte ricevente a un terzo nel proprio paese in conformità all'Articolo VIII del SOP;

(e) "Categorie particolari di Dati Personali/Dati Sensibili": dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona e dati relativi a condanne penali e a reati o a connesse misure di sicurezza in base agli Articoli 9(1) e 10 del GDPR in relazione a persone fisiche;

(f) Il **"Codice italiano in materia di protezione dei dati personali"**: il Decreto Legislativo n. 196 del 30 giugno 1996, come successivamente modificato;

(g) "SOP" o "Accordo di Cooperazione": l'Accordo di Cooperazione (Statement of Protocol) tra il PCAOB e la CONSOB per agevolare la cooperazione e lo scambio di informazioni;

(h) "Violazione di Dati Personali": una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a Dati Personali trasmessi, conservati o comunque trattati;

(i) "Profilazione": qualsiasi forma di trattamento automatizzato di Dati Personali consistente nell'utilizzo di Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o predire aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o i movimenti di tale persona fisica;

(j) "Diritti degli Interessati": nel presente Accordo si intendono i seguenti[1]:

- “Diritto di non essere sottoposto a decisioni automatizzate, compresa la profilazione”: diritto dell’Interessato a non essere sottoposto a decisioni, basate esclusivamente su un trattamento automatizzato, che producano effetti giuridici che lo riguardano;

- “Diritto di Accesso”: diritto dell’Interessato di ottenere da una Parte la conferma che sia, o meno, in corso un trattamento di Dati Personali che lo riguardano e, in tal caso, di ottenere l’accesso ai Dati Personali;

- “Diritto di Cancellazione”: il diritto dell’Interessato di ottenere da una Parte la cancellazione dei suoi Dati Personali quando i Dati Personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, o quando i dati sono stati raccolti o trattati illecitamente;

- “Diritto d’Informazione”: il Diritto dell’Interessato di ricevere informazioni sul trattamento di Dati personali che lo riguardano in forma concisa, trasparente, intellegibile e facilmente accessibile;

- “Diritto di Opposizione”: il diritto dell’Interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento da una Parte di Dati Personali che lo riguardano, salvi i casi in cui esistano motivi legittimi cogenti per il trattamento che prevalgono sugli interessi avanzati dall’Interessato o per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria;

- “Diritto di Rettifica”: diritto dell’Interessato di ottenere da una Parte la rettifica o integrazione dei Dati Personali inesatti dell’Interessato, senza ingiustificato ritardo;

- “Diritto di Limitazione di Trattamento”: diritto dell’Interessato a limitazioni di trattamento dei Dati Personali dell’Interessato quando i Dati Personali sono inesatti, il trattamento è illecito, una Parte non necessita più dei Dati Personali rispetto alle finalità per le quali furono raccolti o i Dati Personali non possono essere cancellati.

ARTICOLO II- FINALITA’ E AMBITO DI APPLICAZIONE DELL’ACCORDO

La finalità del presente Accordo è di fornire appropriate garanzie con riguardo ai Dati Personali trasferiti dalla CONSOB al PCAOB in conformità all’art. 46(3)(b) del GDPR e nella prestazione della cooperazione ai sensi del SOP. Le Parti concordano che il trasferimento di Dati Personali dalla CONSOB al PCAOB deve essere disciplinato dalle disposizioni del presente Accordo e si impegnano ad adottare le garanzie ivi indicate per il Trattamento di Dati Personali nell’esercizio dei rispettivi mandati e funzioni. Il presente Accordo è destinato ad integrare il SOP tra le Parti.

Ciascuna Parte conferma che può agire compatibilmente con il presente Accordo e che non ha motivo di ritenere che gli attuali requisiti di legge applicabili le impediscano di farlo.

Il presente Accordo non crea alcun obbligo giuridicamente vincolante, non conferisce alcun diritto giuridicamente vincolante, né sostituisce il diritto nazionale. Le Parti hanno attuato, nell’ambito delle rispettive giurisdizioni, le garanzie indicate nel presente Accordo in conformità ai requisiti di legge applicabili. Le Parti forniscono garanzie per proteggere i Dati Personali attraverso una combinazione di leggi, di regolamenti e di loro politiche e procedure interne.

[1] Questi diritti sono riconosciuti dal GDPR (cfr. Capitolo III del GDPR).

ARTICOLO III – PRINCIPI RELATIVI AL TRATTAMENTO DEI DATI

1. Limitazione della finalità: I Dati Personali trasferiti dalla CONSOB al PCAOB possono essere trattati dal PCAOB solo per supportare le sue funzioni di vigilanza in materia di revisione contabile ai sensi del Sarbanes-Oxley Act, cioè per finalità di vigilanza sui revisori, ispezioni e indagini su imprese di revisione contabile registrate e relative persone associate soggette alla giurisdizione del PCAOB e della CONSOB. La successiva Comunicazione di tali dati da parte del PCAOB, compresa la finalità di tale Comunicazione, sarà coerente con il Sarbanes-Oxley Act, ed è disciplinata dal successivo paragrafo 7. Il PCAOB non tratterà Dati Personali ricevuti dalla CONSOB per finalità diverse da quelle indicate nel presente Accordo.

2. Qualità dei dati e proporzionalità: I Dati Personali trasferiti dal PCAOB devono essere accurati e adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trasferiti e ulteriormente trattati. CONSOB trasferirà al PCAOB documenti contenenti dati personali solo su richiesta e solo se, ove richiesto, il PCAOB indichi le ragioni per le quali necessita di accedere a tali documenti. CONSOB valuterà tali richieste, restando inteso che il PCAOB utilizzerà i dati personali in conformità all'Articolo II e all'Articolo III paragrafo 1 del presente Accordo.

Una Parte informerà l'altra Parte ove venga a conoscenza del fatto che informazioni previamente trasmesse, o ricevute, sono inesatte e/o necessitano di essere aggiornate. In tal caso, le Parti apporteranno le opportune correzioni ai rispettivi *files*, tenuto conto delle finalità per le quali i Dati Personali sono stati trasferiti, anche integrando, cancellando, limitando il trattamento, correggendo o rettificando in altro modo i Dati Personali, come opportuno.

Le Parti riconoscono che il PCAOB ricerca principalmente i nomi e le informazioni relative alle attività professionali delle singole persone fisiche che erano responsabili o che hanno partecipato agli incarichi di revisione selezionati per controlli durante un'ispezione o un'indagine, o aventi un ruolo rilevante nella gestione e nel controllo di qualità della società. Queste informazioni verrebbero utilizzate dal PCAOB al fine di valutare il grado di ottemperanza delle società di revisione iscritte e delle loro persone associate al Sarbanes-Oxley Act, alle leggi in materia di titoli relative alla preparazione ed emissione di relazioni di revisione, alle regole del PCAOB, alle regole della SEC e agli standard professionali pertinenti in relazione allo svolgimento di attività di revisione, all'emissione di relazioni di revisione e questioni collegate che riguardino gli emittenti (come definiti nel Sarbanes-Oxley Act).

I Dati Personali devono essere conservati in un modo da permettere l'identificazione degli Interessati per un arco di tempo non superiore a quello necessario per le finalità per le quali i dati sono stati raccolti o per le quali sono ulteriormente Trattati, o per il tempo richiesto dalle leggi, norme e regolamenti applicabili. Le Parti devono avere in essere appropriate procedure di eliminazione per tutte le informazioni ricevute ai sensi del presente Accordo.

3. Trasparenza: Entrambe le Parti forniranno un'informativa generale attraverso la pubblicazione del presente Accordo sul proprio sito web. La CONSOB fornirà altresì agli Interessati informazioni relative al trasferimento e successivo Trattamento di Dati Personali. La CONSOB fornirà, in linea di principio, un'informativa generale agli Interessati riguardo a: (a) come e perché può Trattare e trasferire Dati Personali; (b) il tipo di entità cui tali dati possono essere trasferiti; (c) i diritti di cui dispongono gli Interessati ai sensi dei requisiti legali applicabili, ivi incluse le modalità di esercizio di tali diritti; (d) informazioni relative a eventuali ritardi o restrizioni applicabili con riguardo all'esercizio di tali diritti, ivi incluse le restrizioni applicabili nel caso di trasferimenti di Dati Personali all'estero; e (e) i recapiti per la presentazione di controversie o reclami.

Questa informativa sarà effettuata attraverso la pubblicazione di queste informazioni da parte della CONSOB sul proprio sito web, unitamente al presente Accordo. Anche il PCAOB pubblicherà sul proprio sito web informazioni appropriate relative al proprio trattamento di Dati Personali, ivi incluse le informazioni sopra indicate, come descritto nel presente Accordo.

La CONSOB fornirà un'informativa individuale agli Interessati in conformità ai requisiti di notifica e alle esenzioni e limitazioni applicabili ai sensi del GDPR (come stabilito dagli Articoli 14 e 23 del GDPR) e del Codice italiano in materia di protezione dei dati personali. Se dopo aver considerato ogni esenzione applicabile in merito all'informativa individuale e alla luce di discussioni con il PCAOB, la CONSOB conclude che è necessario ai sensi del GDPR informare l'Interessato del trasferimento dei suoi Dati Personali al PCAOB, la CONSOB notificherà il PCAOB prima di effettuare tale informativa individuale.

4. Sicurezza e riservatezza: Le Parti riconoscono che nell'**Allegato I** il PCAOB ha fornito informazioni che descrivono le proprie misure tecniche e organizzative di sicurezza ritenute adeguate dalla CONSOB al fine di prevenire la distruzione, la perdita, l'alterazione, la divulgazione di, o l'accesso ai, Dati Personali accidentale o illegale. Il PCAOB accetta di notificare alla CONSOB ogni modifica delle misure tecniche e organizzative di sicurezza che comporti un pregiudizio al livello di protezione dei Dati Personali riconosciuto dal presente Accordo e aggiornerà le informazioni di cui all'**Allegato I** in conformità all'Articolo VII, comma B.3 del SOP nel caso in cui tali modifiche vengano effettuate. Nel caso in cui il PCAOB effettui una tale notifica alla CONSOB, quest'ultima notificherà l'Autorità italiana per la Protezione dei Dati con riguardo a tali modifiche.

Il PCAOB ha fornito alla CONSOB una descrizione delle proprie leggi applicabili e/o regole relative alla riservatezza e alle conseguenze di ogni divulgazione illegale di informazioni non pubbliche o riservate o di sospette violazioni di tali leggi e/o norme.

Nel caso in cui una Parte ricevente venga a conoscenza di una Violazione di Dati Personali relativa a Dati Personali trasmessi ai sensi del presente Accordo, essa senza ingiustificato ritardo, e, ove possibile, non più tardi di 24 ore dal momento in cui è venuta a conoscenza del fatto che riguarda tali Dati Personali, notificherà l'altra Parte della Violazione di Dati Personali. Inoltre, la Parte notificatrice, appena possibile, utilizzerà mezzi ragionevoli e appropriati per porre rimedio alla Violazione di Dati Personali e minimizzare i potenziali effetti negativi.

5. Diritti degli Interessati: l'Interessato i cui Dati Personali siano stati trasferiti al PCAOB può esercitare i propri Diritti degli Interessati come definiti dall'Articolo I(j), anche richiedendo alla CONSOB di identificare ogni Dato Personale trasferito al PCAOB e richiedendo che la Consob confermi con il PCAOB che i propri Dati Personali siano completi, accurati e, se del caso, aggiornati e che il Trattamento avvenga in conformità ai principi di Trattamento dei Dati Personali del presente Accordo. L'Interessato può esercitare i propri Diritti degli Interessati formulando una richiesta diretta alla CONSOB.

Recapiti della CONSOB:

- via posta certificata a: consob@pec.consob.it;

- via e-mail a: protocollo@consob.it;

- via posta ordinaria a: Consob, Commissione Nazionale per le Società e la Borsa, via G.B. Martini n. 3 – 00198 Roma.

Il Responsabile della Protezione dei Dati della CONSOB può essere contattato presso la CONSOB (mail: responsabileprotezionedati@consob.it). Il PCAOB affronterà ogni richiesta pervenuta dalla CONSOB relativa a Dati Personali trasferiti dalla CONSOB al PCAOB in modo ragionevole e tempestivo. Ciascuna delle Parti può adottare misure appropriate, come l'addebito di spese ragionevoli per coprire i costi amministrativi o il rifiuto di dare corso alla richiesta in caso di una richiesta dell'Interessato manifestamente infondata o eccessiva.

Ove l'Interessato voglia contattare il PCAOB, egli/ella può inviare una mail a: personaldata@pcaobus.org.

Le garanzie riguardanti i Diritti degli Interessati sono soggette all'obbligo di legge di una delle Parti di non divulgare informazioni riservate in virtù del segreto professionale o altri obblighi giuridici. Queste garanzie possono essere limitate al fine di prevenire un pregiudizio o un danno alle funzioni di vigilanza o enforcement delle Parti che operano nell'esercizio dei pubblici poteri loro conferiti, come per la vigilanza o l'accertamento dell'ottemperanza alla normativa applicabile nella giurisdizione della Parte o la prevenzione o l'indagine su presunti violazioni; per importanti obiettivi di interesse pubblico generale, come riconosciuti negli Stati Uniti e in Italia o nell'Unione europea, incluso nello spirito di reciprocità proprio della cooperazione internazionale; o per la vigilanza di entità e soggetti regolamentati. La limitazione dovrebbe essere necessaria e prevista dalla legge, e seguiterà ad applicarsi solo finché la ragione della limitazione continua ad esistere.

La CONSOB fornirà all'Interessato informazioni sulle azioni intraprese riguardo a una richiesta ai sensi degli Articoli da 15 a 22 del GDPR senza ingiustificato ritardo e in ogni caso entro un mese dal ricevimento della richiesta. Ove necessario, tale periodo può essere esteso di due ulteriori mesi ove necessario, tenuto conto della complessità e del numero delle richieste. La CONSOB informerà l'Interessato di tale estensione entro un mese dal ricevimento della richiesta. Se la CONSOB e/o il PCAOB non intraprendono alcuna azione relativamente alla richiesta dell'Interessato, la CONSOB informerà l'Interessato, senza indugio e al più tardi entro un mese dal ricevimento della richiesta, circa le ragioni dell'inazione e sulla possibilità di presentare un reclamo all'Autorità italiana per la Protezione dei Dati e di proporre un ricorso giurisdizionale o davanti al meccanismo di reclamo stabilito presso il PCAOB. Ogni controversia o reclamo proposto da un Interessato relativamente al trattamento dei propri Dati Personali ai sensi del presente Accordo può essere presentato dinanzi alla CONSOB, al PCAOB o a entrambi, come applicabile e come stabilito nella Sezione 8.

Il PCAOB accetta di non assumere decisioni legali relative ad un Interessato basate esclusivamente sul trattamento automatizzato di Dati Personali, inclusa la Profilazione, senza il coinvolgimento umano.

6. Categorie particolari di Dati Personali/Dati Sensibili: le categorie particolari di Dati Personali/Dati Sensibili, come definiti nella clausola I(e), non saranno trasferiti dalla CONSOB al PCAOB.

7. Successiva Comunicazione di Dati Personali: Il PCAOB Comunicherà Dati Personali ricevuti dalla CONSOB esclusivamente con le entità identificate nell'Articolo VIII, commi C ed E.2 del SOP.[2] Nell'eventualità che il PCAOB intenda Comunicare Dati Personali con una terza parte identificata nell'Articolo VIII, paragrafi C e E.2 del SOP, diversa dalla U.S. Securities and Exchange Commission, il PCAOB dovrà richiedere il preventivo

[2] Le entità con le quali il PCAOB è autorizzato dalla legge statunitense a condividere informazioni riservate sono descritte nell'**Allegato II**.

consenso scritto alla CONSOB e Comunicherà tali Dati Personali solamente se la terza parte fornirà adeguate garanzie coerenti con quelle stabilite dal presente Accordo. Nel richiedere tale preventivo consenso scritto, il PCAOB dovrebbe indicare il tipo di dato personale che intende Comunicare e le ragioni e le finalità per le quali il PCAOB intende Comunicare i Dati Personali. Se la CONSOB non fornisce il proprio consenso scritto a tale Comunicazione in un tempo ragionevole, che non eccede i dieci giorni, il PCAOB consulterà la CONSOB e considererà ogni obiezione di quest'ultima. Ove il PCAOB decida di Comunicare i Dati Personali senza il consenso scritto della CONSOB, il PCAOB notificherà la CONSOB della propria intenzione. La CONSOB può quindi decidere se sospendere il trasferimento di Dati Personali e, nella misura in cui decida di sospendere tali trasferimenti, informerà di conseguenza l'Autorità italiana per la Protezione dei Dati. Qualora le adeguate garanzie sopra menzionate non possano essere fornite dalla terza parte, i Dati Personali possono essere Comunicati con la terza parte in casi eccezionali se la comunicazione dei Dati Personali sia per importanti motivi di interesse pubblico, come riconosciuti negli Stati Uniti e in Italia o nell'Unione europea, incluso nello spirito di reciprocità della cooperazione internazionale, o se la comunicazione è necessaria per far valere, esercitare o difendere un diritto in sede giudiziaria.

Prima di Comunicare Dati Personali alla U.S. Securities and Exchange Commission, il PCAOB otterrà dalla U.S. Securities and Exchange Commission adeguate garanzie in coerenza con quelle stabilite dal presente Accordo. In aggiunta, se il PCAOB ha condiviso Dati Personali soggetti al presente Accordo con la U.S Securities and Exchange Commission, il PCAOB informerà periodicamente la CONSOB circa la natura dei Dati Personali Comunicati e le ragioni per la Comunicazione, se fornendo tali informazioni non rischi di compromettere un'indagine in corso. Una tale limitazione riguardante informazioni relative a un'indagine in corso seguiterà ad applicarsi solo finché la ragione della limitazione continuerà ad esistere.

Un Interessato può richiedere alla CONSOB talune informazioni concernenti i propri Dati Personali che sono stati trasferiti dalla CONSOB al PCAOB nel corso della cooperazione ai sensi del SOP. Sarà responsabilità della CONSOB fornire tali informazioni all'Interessato in conformità ai requisiti legali applicabili ai sensi del GDPR e del Codice italiano in materia di protezione dei dati personali. Fermo restando il precedente paragrafo, a fronte della ricezione di una richiesta di un Interessato, la Consob può richiedere al PCAOB informazioni relative alla Comunicazione successiva di tali Dati Personali al fine di ottemperare agli obblighi di comunicazione all'Interessato ai sensi del GDPR e del Codice italiano in materia di protezione dei dati personali. A fronte della ricezione di una tale richiesta dalla CONSOB, il PCAOB fornirà alla CONSOB ogni informazione resa disponibile al PCAOB relativa al trattamento di tali Dati Personali da una terza parte alla quale il PCAOB ha Comunicato detti Dati Personali.

8. Ricorso: Ogni controversia o reclamo proposto da un Interessato relativo al trattamento dei propri Dati Personali ai sensi del presente Accordo può essere presentato dinanzi alla CONSOB, al PCAOB o a entrambi, come applicabile. Ciascuna Parte informerà l'altra Parte su ognuna di queste controversie o reclami, e si adopererà per risolvere amichevolmente la controversia o il reclamo in modo tempestivo.

Ogni segnalazione o reclamo relativo al trattamento di Dati Personali da parte del PCAOB può essere presentato direttamente al PCAOB Center for Enforcement Tips, Referrals, Complaints and Other Information, specificatamente attraverso il Tips & Referral Center, dove le informazioni possono essere fornite a mezzo di un modulo online sul sito internet, via posta elettronica, lettera o telefono, o, in alternativa può essere fornito alla CONSOB inviando tali informazioni ai recapiti indicati al paragrafo 5. Il PCAOB informerà la CONSOB sulle segnalazioni ricevute dagli Interessati sul trattamento dei loro Dati Personali che il PCAOB abbia ricevuto dalla CONSOB e consulterà la CONSOB per una risposta alla questione.

Se una Parte o le Parti non è/sono in grado di risolvere una segnalazione o un reclamo presentato da un Interessato relativamente al trattamento di Dati Personali da parte del PCAOB ricevuto tramite il Tips & Referral Center e la segnalazione o reclamo dell'Interessato non è manifestamente infondato o eccessivo, l'Interessato, la Parte o le Parti possono fare uso di un appropriato meccanismo di risoluzione delle controversie guidato da una funzione indipendente all'interno del PCAOB.

La decisione raggiunta attraverso questo meccanismo di risoluzione delle controversie può essere sottoposta ad un secondo esame indipendente, che dovrebbe essere condotto da una funzione indipendente separata. Il meccanismo di risoluzione delle controversie e il procedimento per il secondo esame sono descritti nell'**Allegato III** al presente Accordo. Ai sensi del presente Accordo, l'Interessato può esercitare i propri diritti per un ricorso giurisdizionale o amministrativo (compresi i danni) secondo la normativa italiana sulla protezione dei dati. In situazioni nelle quali la Consob sia del parere che il PCAOB non abbia agito in coerenza con le garanzie stabilite nel presente Accordo, la CONSOB può sospendere il trasferimento di Dati Personali ai sensi del presente Accordo fintantoché la questione non sia affrontata in modo soddisfacente dal PCAOB e può informare di ciò l'Interessato. Prima di sospendere i trasferimenti, la CONSOB discuterà la questione con il PCAOB e il PCAOB risponderà senza ingiustificato ritardo.

9. Vigilanza: Ciascuna Parte condurrà verifiche periodiche delle proprie politiche e procedure per l'implementazione delle garanzie sui Dati Personali descritte nell'Accordo. Su ragionevole richiesta di una Parte, l'altra Parte riesaminerà le proprie politiche e procedure al fine di accertare e confermare che le garanzie specificate nel presente Accordo siano implementate efficacemente and invierà una sintesi del riesame all'altra Parte.

Alla richiesta di CONSOB di condurre un esame indipendente sull'ottemperanza alle garanzie stabilite nell'Accordo, il PCAOB notificherà l'Office of Internal Oversight and Performance Assurance ("IOPA"), un ufficio indipendente del PCAOB, perché esso conduca un esame al fine di accertare e confermare che le garanzie del presente Accordo siano implementate efficacemente. Lo IOPA condurrà l'esame secondo le procedure e gli standard stabiliti e utilizzati da IOPA per eseguire il suo mandato usuale, come ulteriormente descritto nell'**Allegato IV** del presente Accordo. Ai fini del proprio esame indipendente, lo IOPA sarà informato di ogni controversia o reclamo proposto da un Interessato circa il trattamento dei propri Dati Personali ai sensi della sezione 8 del presente Articolo, ivi incluse le azioni intraprese dallo staff del PCAOB allo scopo di implementare decisioni risultanti da un meccanismo di risoluzione delle controversie. Lo IOPA fornirà una sintesi degli esiti del proprio esame alla CONSOB una volta che il Consiglio direttivo del PCAOB abbia approvato la comunicazione della sintesi alla CONSOB.

Qualora la CONSOB non abbia ricevuto gli esiti dell'esame dello IOPA e ritenga che il PCAOB non abbia agito in coerenza con le garanzie specifiche relative ai suoi obblighi ai sensi del presente Accordo, la CONSOB può sospendere il trasferimento di Dati Personali al PCAOB ai sensi del presente Accordo fintantoché la questione non sia affrontata in modo soddisfacente dal PCAOB. Prima di sospendere i trasferimenti, la CONSOB discuterà la questione con il PCAOB e il PCAOB risponderà senza ingiustificato ritardo. Nell'eventualità in cui la CONSOB sospenda il trasferimento di Dati Personali al PCAOB, o riavvii i trasferimenti dopo ognuna di tali sospensioni, la CONSOB informerà tempestivamente l'Autorità italiana per la Protezione dei Dati.

ARTICLE IV- ENTRATA IN VIGORE E CESSAZIONE

Il presente Accordo entra in vigore dalla data di sottoscrizione e resterà in vigore soltanto durante la vigenza del SOP. Le Parti hanno facoltà di consultarsi e rivedere i termini del presente Accordo secondo le condizioni stabilite all'Articolo X, paragrafo B del SOP.

Il presente Accordo può essere risolto da ciascuna delle Parti in qualsiasi momento. Dopo la cessazione del presente Accordo, le Parti continueranno a mantenere riservate, in conformità agli Articoli VII e VIII del SOP, tutte le informazioni ricevute ai sensi del SOP. Dopo la cessazione del presente Accordo, tutti i Dati Personali precedentemente trasferiti ai sensi del presente Accordo continueranno ad essere gestiti dal PCAOB secondo le garanzie stabilite dal presente Accordo. Le Parti riconoscono che, ai sensi della Sezione 105(b)(5) del Sarbanes-Oxley Act, la cessazione del presente Accordo e del SOP limiterebbe la capacità del PCAOB di condividere informazioni riservate con la CONSOB in relazione all'applicazione delle pertinenti garanzie stabilite dal presente accordo.

CONSOB informerà tempestivamente l'Autorità italiana per la Protezione dei Dati circa ogni modifica o cessazione del presente Accordo.

Allegati all'accordo tra la Commissione Nazionale per le Società e la Borsa in Italia e il Public Company Accounting Oversight Board negli Stati Uniti d'America sul trasferimento di alcuni dati personali

Allegato I: Descrizione dei sistemi/controlli informatici del PCAOB [RISERVATO]

Appendice II: Elenco delle entità alle quali il PCAOB è autorizzato a inoltrare informazioni riservate

Allegato III: Descrizione delle procedure applicabili di risoluzione delle controversie (ricorso)

Allegato IV: Descrizione del controllo da parte del PCAOB sull'attuazione della garanzia prevista dall'Accordo sulla protezione dei dati

Allegato I

Descrizione dei sistemi informatici/controlli del PCAOB – Marzo 2021

[RISERVATO]

Nel presente documento si fornisce una descrizione della metodologia adottata dal PCAOB rispetto alle misure di sicurezza e organizzative attuate per proteggere i dati personali e le informazioni non pubbliche. Uno dei modi più efficaci per risolvere i pericoli per la sicurezza è tenere conto degli standard del settore e delle *best practices*. Questi standard sono consultabili in molte fonti, tra cui organizzazioni governative e non governative, e spaziano in una vasta gamma di argomenti. Detti standard sono elaborati basandosi su un'ampia ricerca ed esperienza nel campo della sicurezza delle informazioni. Individuare e fare propri standard adeguati di sicurezza delle informazioni è una componente fondamentale di un efficace programma di sicurezza delle informazioni. Le pratiche di sicurezza dell'Office of Data, Security and Technology (ODST) del PCAOB tengono conto dei seguenti standard di settore e *best practices*: Standard di sicurezza del NIST, come lo SP800-53 *Controlli di sicurezza raccomandati per i sistemi e le organizzazioni informatiche federali* (*Recommended Security Controls for Federal Information Systems and Organizations)* e il Quadro di riferimento per il rafforzamento della sicurezza informatica delle infrastrutture critiche, versione 1.1 (Cybersecurity Framework o CSF), nonché i 20 principali controlli del Center for Internet Security (CIS).

Personale

Il PCAOB svolge le funzioni di sicurezza principalmente tramite un team di sicurezza appartenente all'Office of Data, Security and Technology. Il team di sicurezza comprende tecnici specialisti della *cyber security*, con molti anni di esperienza nel campo della sicurezza informatica. Il compito principale del team è salvaguardare la sicurezza mantenendo una ragionevole comodità d'uso dell'utente.

Durante la procedura di assunzione, il PCAOB effettua controlli sui precedenti di tutti i candidati dipendenti. Tale procedura è concepita per garantire, ad esempio, che i dipendenti del PCAOB non abbiano precedenti penali tali da comportare potenziali rischi per la sicurezza. Dopo l'assunzione, tutti i nuovi dipendenti del PCAOB frequentano una sessione di orientamento, in cui, tra l'altro, sono istruiti sulle regole di sicurezza ed etica del PCAOB e sugli obblighi loro imposti da queste norme. Inoltre tutti i dipendenti sono tenuti a frequentare una formazione etica e a confermare annualmente il loro costante rispetto del codice etico del PCAOB.

Sicurezza fisica

L'accesso fisico agli uffici del PCAOB è controllato tramite un sistema di sicurezza operato dal personale del PCAOB. Possono accedere ai locali del PCAOB solo i visitatori e i dipendenti muniti di un apposito contrassegno. I visitatori del PCAOB devono essere accompagnati in ogni momento della loro permanenza nei locali del PCAOB. L'accesso alle sale dei server e ai centri dati è limitato a un numero ristretto di persone. L'accesso agli uffici del PCAOB è protetto da appositi lettori di tessere ubicati agli ingressi dell'area. Inoltre l'accesso alle aree comuni del PCAOB è monitorato da impianti di videosorveglianza.

Tecnologia e processi del PCAOB

Ai fini della presentazione, la descrizione delle misure di sicurezza IT del PCAOB si articola nei 20 principali controlli critici del CIS. Nel prospetto 1 seguente si descrivono i 20 principali controlli del CIS e la tecnologia e i processi del PCAOB relativi ai controlli. Il prospetto 2 riporta la definizione del CIS per ciascuno dei 20 controlli principali.

Prospetto 1. Tecnologia e processi del PCAOB relativi ai 20 principali controlli del CIS

Controllo	Tecnologia	Processo
1. Inventario dei dispositivi autorizzati e non autorizzati	Il PCAOB impiega sistemi di prevenzione e di rilevamento delle intrusioni che monitorano il traffico di rete per bloccare possibili attacchi. Gli allarmi sono analizzati dagli addetti alla sicurezza, che intervengono quando necessario. Il PCAOB esegue analisi periodiche delle vulnerabilità di tutti i dispositivi connessi alla propria rete. Ad esempio, i computer portatili e fissi sono analizzati settimanalmente.	Il PCAOB implementa svariati controlli di sicurezza per garantire che l'accesso ai propri dati e all'infrastruttura sia consentito solo ai propri dispositivi e alle soluzioni tecnologiche autorizzate. Ad esempio, possono connettersi alla rete Wi-Fi del PCAOB solo i computer portatili muniti di certificati di sicurezza del PCAOB.[3] L'accesso remoto alla rete del PCAOB richiede l'autenticazione multifattoriale.
2. Inventario dei software autorizzati e non autorizzati	Il PCAOB esegue analisi settimanali delle vulnerabilità dei dispositivi connessi alla propria rete. Ad esempio, il server è analizzato settimanalmente. Il PCAOB opera i software del client e del server tramite un sistema centralizzato di gestione dei dispositivi.	La gestione dei software installati in computer portatili e fissi è centralizzata. Qualsiasi nuovo software richiesto attraversa gli appropriati canali interni del PCAOB, compresa un'analisi della sicurezza per garantire che nell'ambiente del PCAOB non si introducano nuovi rischi inaccettabili.
3. Configurazioni sicure per hardware e software nei computer portatili e fissi, nelle postazioni di lavoro e nei server	Per proteggersi dagli attacchi dei malware, i computer portatili e fissi del PCAOB adottano misure di sicurezza più rigorose (impostazioni di sicurezza concepite per ridurre al minimo i rischi per i computer). Ad esempio, gli utenti non possono accedere come amministratori ai propri computer e pertanto non possono disabilitare i controlli di sicurezza, essendo i loro diritti limitati ai dati a cui sono autorizzati ad accedere.	I server, i computer portatili e fissi e i dispositivi mobili del PCAOB possono essere utilizzati dal suo personale solo dopo un rafforzamento della sicurezza.
4. Valutazione e contrasto costante delle vulnerabilità	Il PCAOB utilizza sistemi e tecnologie interni ed esterni per eseguire analisi della sicurezza dei propri sistemi. Il PCAOB impiega sistemi di prevenzione e di rilevamento delle intrusioni che monitorano il traffico di rete per bloccare possibili	Il PCAOB segue precise procedure per la sicurezza delle applicazioni, la gestione delle patch, le valutazioni dei fornitori esterni nonché le analisi e gli esami delle vulnerabilità. Ad esempio, le patch dei software dei client e dei server sono implementate con cadenza mensile,

[3] Il PCAOB permette l'accesso Wi-Fi agli ospiti tramite un'apposita rete isolata da un firewall.

	attacchi. Gli addetti alla sicurezza esaminano gli allarmi e gestiscono le modalità di intervento dopo gli incidenti. Il PCAOB analizza periodicamente le vulnerabilità dei dispositivi connessi alla propria rete. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali. Il PCAOB opera i software del client e del server tramite un sistema centralizzato di gestione dei dispositivi.	generalmente entro breve tempo dalla loro pubblicazione.
5. Difese contro i malware	Il PCAOB utilizza la tecnologia per filtrare il traffico nel cloud, in rete e nella posta elettronica alla ricerca di malware e di altri tipi di contenuti indesiderati. I computer portatili e fissi e i server del PCAOB sono preconfigurati con un software anti-malware, aggiornato continuamente con nuovi supplementi.	La gestione dei software installati in computer portatili e fissi è centralizzata. Qualsiasi nuovo software richiesto attraversa gli appropriati canali interni del PCAOB, compresa un'analisi della sicurezza per garantire che nell'ambiente del PCAOB non si introducano nuovi rischi inaccettabili.
6. Sicurezza dei software applicativi	Il PCAOB ricorre a una serie di tecnologie di sicurezza delle applicazioni per implementare misure che riducano al minimo i rischi per la sicurezza. Queste misure comprendono i firewall delle applicazioni web, gli analizzatori delle applicazioni web, l'analisi del codice SAST e il monitoraggio delle problematiche.	Il PCAOB segue precise procedure per la sicurezza delle applicazioni, la gestione delle patch, le valutazioni dei fornitori esterni nonché le analisi e gli esami delle vulnerabilità. Il PCAOB esegue rassegne della sicurezza delle applicazioni nei sistemi sviluppati sia internamente che da fornitori esterni.
7. Controllo dei dispositivi wireless	Il PCAOB impiega firewall e tecnologie di sicurezza wireless nei punti di ingresso dell'infrastruttura IT. Il PCAOB limita l'accesso alla propria rete Wi-Fi solo ai propri dispositivi da esso stesso certificati.[4]	Il PCAOB implementa svariati controlli di sicurezza per garantire che l'accesso ai propri dati e all'infrastruttura sia consentito solo ai propri dispositivi e alle soluzioni tecnologiche autorizzate. Ad esempio, possono connettersi alla rete Wi-Fi del PCAOB solo i computer portatili muniti di certificati di sicurezza del PCAOB. [2]
8. Capacità di recupero dei dati	Il PCAOB utilizza tecnologie forensi per recuperare i dati e per le eventuali indagini.	Il PCAOB effettua copie di riserva di tutti i sistemi seguendo la consueta procedura documentata. Le copie di riserva di alcuni sistemi si effettuano di

[4] Il PCAOB permette l'accesso Wi-Fi agli ospiti tramite un'apposita rete isolata da un firewall.

		notte, mentre altre si eseguono in orari diversi.
9. Valutazione delle competenze in materia di sicurezza e formazione adeguata per colmare le lacune	Il PCAOB dispone di un team specializzato nella sicurezza, della quale vanta una profonda e ampia conoscenza. Gli addetti alla sicurezza possiedono numerose certificazioni di sicurezza informatica riconosciute a livello internazionale.	I dipendenti del PCAOB sono tenuti a frequentare annualmente un corso di formazione e sensibilizzazione alla sicurezza. Gli addetti alla sicurezza del PCAOB frequentano annualmente un opportuno corso di formazione.
10. Configurazioni sicure per i dispositivi di rete: firewall, router e switch	Il PCAOB verifica periodicamente le configurazioni dei dispositivi dell'infrastruttura critica per ridurre al minimo i rischi per la sicurezza e valutarne l'aderenza alle *best practices* del settore. Ad esempio, ogni settimana si esegue un'analisi delle vulnerabilità per accertarsi della corretta e sicura configurazione dei dispositivi.	Il PCAOB effettua analisi periodiche delle vulnerabilità dei dispositivi di rete e di sicurezza nonché dei server. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali.
11. Limitazione e controllo delle porte, dei protocolli e dei servizi di rete	Il PCAOB impiega firewall nei punti di ingresso dell'infrastruttura IT. Inoltre i computer portatili del PCAOB sono preconfigurati con firewall basato su host e software anti-malware, per garantire che solo i software autorizzati possano comunicare all'esterno del PCAOB. Il PCAOB impiega sistemi di prevenzione e di rilevamento delle intrusioni che monitorano il traffico di rete per bloccare possibili attacchi. Gli allarmi sono analizzati dagli addetti alla sicurezza, che intervengono quando necessario. Il PCAOB analizza periodicamente le vulnerabilità dei dispositivi connessi alla propria rete. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali. Il PCAOB opera i software del client e del server tramite un sistema centralizzato di gestione dei dispositivi.	Il PCAOB effettua analisi periodiche delle vulnerabilità dei dispositivi di rete e di sicurezza nonché dei server. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali.

	Il PCAOB limita l'accesso alla propria rete Wi-Fi solo ai propri dispositivi da esso stesso certificati.[5]	
12. Controllo dell'uso dei privilegi di amministratore	Per proteggersi dagli attacchi dei malware, i computer portatili e fissi del PCAOB adottano misure di sicurezza più rigorose (impostazioni di sicurezza concepite per ridurre al minimo i rischi per i computer). Ad esempio, gli utenti non possono accedere come amministratori ai propri computer e pertanto non possono disabilitare i controlli di sicurezza, essendo i loro diritti limitati ai dati a cui sono autorizzati ad accedere.	Il PCAOB segue una precisa procedura di gestione dei privilegi di amministratore applicati nella propria infrastruttura. Ad esempio, i privilegi di amministratore per i server devono essere approvati dal controllore del sistema.
13. Difesa del perimetro	Il PCAOB impiega sistemi di prevenzione e di rilevamento delle intrusioni che monitorano il traffico di rete per bloccare possibili attacchi. Gli allarmi sono analizzati dagli addetti alla sicurezza, che intervengono quando necessario. Il PCAOB esegue analisi periodiche delle vulnerabilità di tutti i dispositivi connessi alla propria rete. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali. Per proteggersi dagli attacchi dei malware, i computer portatili e fissi del PCAOB adottano misure di sicurezza più rigorose (impostazioni di sicurezza concepite per ridurre al minimo i rischi per i computer). Ad esempio, gli utenti non possono accedere come amministratori ai propri computer e pertanto non possono disabilitare i controlli di sicurezza, essendo i loro diritti limitati ai dati a cui sono autorizzati ad accedere. Il PCAOB protegge con firewall i punti di accesso all'infrastruttura IT. Il PCAOB limita l'accesso alla propria rete Wi-Fi solo ai propri dispositivi	Il PCAOB effettua analisi periodiche delle vulnerabilità dei dispositivi di rete e di sicurezza nonché dei server. Settimanalmente si analizzano le macchine dei client e i server.

[5] Il PCAOB permette agli ospiti l'accesso al Wi-Fi tramite una rete appositamente isolata.

	da esso stesso certificati. Il PCAOB permette agli ospiti l'accesso al Wi-Fi tramite una rete appositamente isolata.	
14. Aggiornamento, monitoraggio e analisi dei registri di controllo	Il PCAOB si avvale del SIEM (Security Information and Events Management) per garantire il corretto monitoraggio e la corretta analisi dei registri.	Il PCAOB attua un processo di risposta agli incidenti per risolvere gli allarmi sulla sicurezza.
15. Controllo degli accessi per esigenze professionali	Il PCAOB utilizza un ampio ventaglio di tecnologie di sicurezza per attuare i controlli degli accessi ai propri sistemi.	Il PCAOB applica una politica di controllo degli accessi. Detta politica descrive le procedure di concessione e revoca degli accessi degli utenti alle risorse del PCAOB. Le autorizzazioni agli accessi degli utenti si limitano alle esigenze professionali. La politica delle password seguita dal PCAOB per regolare gli account di accesso alla rete richiede password complesse e modificate frequentemente. Tutte le autorizzazioni di accesso dei dipendenti licenziati o dimissionari sono revocate.
16. Monitoraggio e controllo degli account	Il PCAOB impiega un ampio ventaglio di tecnologie di sicurezza per monitorare gli account di utenti e macchinari e applicare i controlli di sicurezza. Ad esempio, il PCAOB verifica mensilmente la active directory per accertarsi della corretta creazione e chiusura degli account.	Per garantire la corretta creazione ed eliminazione degli account, il PCAOB segue un processo documentato di *provisioning* degli utenti (processo di creazione e gestione dell'accesso alle risorse in un sistema IT) e di *de-provisioning*.
17. Classificazione e sicurezza dei dati	I computer portatili del PCAOB eseguono la crittografia integrale del disco rigido per proteggersi da possibili perdite o furti di dati. Si ricorre ad un software di prevenzione delle perdite di dati per proteggersi dall'esfiltrazione di informazioni e di dati classificati come sensibili.	Per securizzare i dati il PCAOB, segue una politica di classificazione della sensibilità delle informazioni. Il PCAOB applica una politica di controllo degli accessi. Detta politica descrive le procedure di concessione e revoca degli accessi degli utenti alle risorse del PCAOB. Le autorizzazioni agli accessi degli utenti si limitano alle esigenze professionali. La politica delle password seguita dal PCAOB per regolare gli account di accesso alla rete richiede password complesse e modificate frequentemente. Tutte le autorizzazioni

		di accesso dei dipendenti licenziati o dimissionari sono revocate.
18. Risposta e gestione degli incidenti	Il PCAOB utilizza un ampio ventaglio di tecnologie di sicurezza per monitorare e gestire gli incidenti di sicurezza.	Il PCAOB gestisce gli incidenti di sicurezza applicando un processo definito e documentato. Il piano di risposta agli incidenti e le relative procedure sono chiaramente definiti. Il PCAOB attua le funzioni di sicurezza principalmente tramite un team di sicurezza informatica appartenente al proprio Office of Data, Security and Technology. I responsabili della risposta agli incidenti nell'ambito del team di sicurezza vantano molti anni di esperienza nel campo della sicurezza informatica.
19. Ingegneria delle reti sicure	Il PCAOB opera i software del client e del server tramite un sistema centralizzato di gestione dei dispositivi. Il PCAOB impiega sistemi di rilevamento delle intrusioni che monitorano il traffico di rete contro potenziali attacchi. Gli allarmi sono analizzati dagli addetti alla sicurezza, che intervengono quando necessario. Il PCAOB esegue analisi periodiche delle vulnerabilità di tutti i dispositivi connessi alla propria rete. Ad esempio, i computer portatili e fissi e i server sono soggetti ad analisi settimanali. Per proteggersi dagli attacchi dei malware, i computer portatili e fissi del PCAOB adottano misure di sicurezza più rigorose (impostazioni di sicurezza concepite per ridurre al minimo i rischi per i computer). Ad esempio, gli utenti non possono accedere come amministratori ai propri computer e pertanto non possono disabilitare i controlli di sicurezza, essendo i loro diritti limitati ai dati a cui sono autorizzati ad accedere.	I controlli svolti annualmente dal PCAOB comprendono una revisione delle architetture di rete e di sicurezza. Le raccomandazioni sono implementate ogni qualvolta sia possibile.

	Il PCAOB limita l'accesso alla propria rete Wi-Fi solo ai propri dispositivi da esso stesso certificati.[6] Il PCAOB protegge con firewall i punti di accesso all'infrastruttura IT. Inoltre i computer portatili del PCAOB sono preconfigurati con firewall basato su host e con software anti-malware, per garantire che solo i software autorizzati possano comunicare da e verso gli ambienti esterni.	
20. Test di penetrazione ed esercitazioni del Red Team	Il PCAOB esegue test di penetrazione nell'ambito delle analisi della sicurezza dei pacchetti software applicativi e commerciali. Il test comprende metodi manuali e automatizzati con strumenti di sicurezza. Con il supporto di fornitori esterni di servizi di sicurezza, il PCAOB conduce dei test esaustivi di penetrazione ed esercitazioni del Red Team.	Il PCAOB segue precise procedure per la sicurezza delle applicazioni, la gestione delle patch, le valutazioni dei fornitori esterni nonché le analisi e gli esami delle vulnerabilità. Il PCAOB esegue rassegne della sicurezza delle applicazioni nei sistemi sviluppati sia internamente che da fornitori esterni. Il PCAOB effettua analisi periodiche delle vulnerabilità dei dispositivi di rete e di sicurezza nonché dei server. I computer portatili e fissi e i server sono soggetti ad analisi settimanali. I controlli svolti annualmente dal PCAOB comprendono una revisione delle architetture di rete e di sicurezza. Le raccomandazioni sono implementate ogni qualvolta sia possibile.

Prospetto 2. 20 principali controlli del CIS

Nome del controllo	**Descrizione**
1. Inventario dei dispositivi autorizzati e non autorizzati	*I processi e gli strumenti utilizzati per gestire attivamente (inventariare, sorvegliare e correggere) tutti i dispositivi hardware operanti in rete, affinché solo i dispositivi autorizzati possano accedervi e siano individuati i dispositivi non autorizzati e non gestiti impedendone l'accesso.*
2. Inventario dei software autorizzati e non autorizzati	*I processi e gli strumenti utilizzati per gestire attivamente (inventariare, sorvegliare e correggere) tutti i software in rete, in modo da poter installare ed eseguire solo quelli autorizzati, individuando quelli non autorizzati e non gestiti impedendone l'installazione o l'esecuzione.*

[6] Il PCAOB permette l'accesso Wi-Fi agli ospiti tramite un'apposita rete isolata da un firewall.

3. Configurazioni sicure per hardware e software nei computer portatili e fissi, nelle postazioni di lavoro e nei server	*I processi e gli strumenti utilizzati per stabilire, implementare e gestire attivamente (sorvegliare, segnalare, correggere) la configurazione della sicurezza in computer portatili, server e postazioni di lavoro tramite un rigoroso processo di gestione della configurazione e di controllo delle modifiche, per impedire agli aggressori di sfruttare le vulnerabilità dei servizi e delle impostazioni.*
4. Valutazione e contrasto costante delle vulnerabilità	*I processi e gli strumenti utilizzati per acquisire e valutare costantemente nuove informazioni e agire di conseguenza, per individuare e contrastare le vulnerabilità e ridurre al minimo la finestra di opportunità degli aggressori.*
5. Difese contro i malware	*I processi e gli strumenti utilizzati per controllare l'installazione, il contagio e l'esecuzione di un codice dannoso in più punti dell'azienda, ottimizzando il ricorso all'automazione per consentire un rapido aggiornamento della difesa, la raccolta dei dati e gli interventi correttivi.*
6. Sicurezza dei software applicativi	*I processi e gli strumenti utilizzati per gestire il ciclo di vita della sicurezza di tutti i software sviluppati internamente e acquisiti, per prevenire, rilevare e correggere i punti deboli della sicurezza.*
7. Controllo dei dispositivi wireless	*I processi e gli strumenti utilizzati per sorvegliare/controllare/prevenire/correggere l'uso in sicurezza di reti locali wireless (LAN), punti di accesso e sistemi di client wireless.*
8. Capacità di recupero dei dati	*I processi e gli strumenti utilizzati per eseguire correttamente e con una metodologia collaudata copie di sicurezza per il ripristino tempestivo delle informazioni critiche.*
9. Valutazione delle competenze in materia di sicurezza e formazione adeguata per colmare le lacune	*I processi e gli strumenti utilizzati per individuare le conoscenze, le competenze e le capacità specifiche necessarie per supportare la difesa dell'azienda; sviluppare ed eseguire un piano integrato di valutazione e individuazione delle lacune e porvi rimedio tramite politiche, pianificazione organizzativa e programmi di formazione e sensibilizzazione.*
10. Configurazioni sicure per i dispositivi di rete: firewall, router e switch	*I processi e gli strumenti utilizzati per stabilire, implementare e gestire attivamente (sorvegliare, segnalare, correggere) la configurazione della sicurezza dei dispositivi dell'infrastruttura di rete utilizzando un rigoroso processo di gestione della configurazione e di controllo delle modifiche, per impedire agli aggressori di approfittare delle vulnerabilità di servizi e impostazioni.*
11. Limitazione e controllo delle porte, dei protocolli e dei servizi di rete	*I processi e gli strumenti utilizzati per gestire (sorvegliare/controllare/correggere) l'operatività corrente di porte, protocolli e servizi nei dispositivi in rete, per ridurre al minimo le finestre di vulnerabilità sfruttabili dagli aggressori.*

12. Controllo dell'uso dei privilegi di amministratore	*I processi e gli strumenti utilizzati per sorvegliare/controllare/prevenire/correggere l'uso, l'assegnazione e la configurazione dei privilegi di amministratore in computer, reti e applicazioni.*
13. Difesa del perimetro	*I processi e gli strumenti utilizzati per rilevare/prevenire/correggere il flusso di informazioni tra reti con livelli diversi di fiducia, dedicando particolare attenzione ai dati dannosi per la sicurezza.*
14. Aggiornamento, monitoraggio e analisi dei registri di controllo	*I processi e gli strumenti utilizzati per raccogliere, gestire e analizzare i registri di controllo degli eventi, che possano contribuire a rilevare e comprendere un attacco o a effettuare il successivo ripristino.*
15. Controllo degli accessi per esigenze professionali	*I processi e gli strumenti utilizzati per sorvegliare/controllare/prevenire/correggere l'accesso sicuro alle informazioni determinando formalmente quali persone, computer e applicazioni abbiano la necessità e il diritto di accedere alle informazioni in base a una classificazione approvata*
16. Monitoraggio e controllo degli account	*I processi e gli strumenti utilizzati per gestire attivamente il ciclo di vita degli account di sistema e delle applicazioni (creazione, utilizzo, dormienza, eliminazione) e ridurre al minimo la possibilità che gli aggressori li sfruttino.*
17. Protezione dei dati	*I processi e gli strumenti utilizzati per prevenire l'esfiltrazione dei dati, attenuare le conseguenze dell'esfiltrazione e garantire la riservatezza e l'integrità delle informazioni sensibili.*
18. Risposta e gestione degli incidenti	*Il processo e gli strumenti utilizzati per proteggere le informazioni dell'organizzazione, nonché la sua reputazione, sviluppando e implementando un'infrastruttura di risposta agli incidenti (ad esempio piani, definizione dei ruoli, formazione, comunicazioni, vigilanza sulla gestione) per scoprire tempestivamente gli attacchi e così contenere efficacemente i danni, eradicando la presenza dell'aggressore e ripristinando l'integrità della rete e dei sistemi.*
19. Ingegneria delle reti sicure	*Il processo e gli strumenti utilizzati per fare della sicurezza un attributo intrinseco dell'azienda specificando, progettando e implementando funzionalità che garantiscano un'alta affidabilità operativa dei sistemi impedendo o riducendo al minimo le opportunità per gli aggressori.*
20. Test di penetrazione ed esercitazioni del Red Team	*Il processo e gli strumenti utilizzati per testare la solidità complessiva delle difese di un'organizzazione (tecnologia, processi e dipendenti) simulando gli obiettivi e le azioni di un aggressore.*

Allegato II

Elenco delle entità alle quali il PCAOB è autorizzato a inoltrare informazioni riservate

I terzi ai quali il PCAOB può inoltrare i dati personali citati nell'articolo III, comma 7, dell'Accordo sulla protezione dei dati, sono elencati nell'articolo 105(b)(5)(B) della Legge Sarbanes-Oxley Act del 2002 e successive modifiche, che stabilisce:

> (B) Disponibilità per le agenzie governative.- Senza perdere il loro status confidenziale e privilegiato quando sono in possesso del Board, tutte le informazioni di cui alla lettera (A) [dell'articolo 105(b)(5)] possono:
>
> (i) essere rese note alla [Securities and Exchange Commission]; e
>
> (ii) a discrezione del Board, ove quest'ultimo lo ritenga necessario per realizzare le finalità della presente Legge o per tutelare gli investitori, essere rese note:
>
> (I) al Procuratore Generale degli Stati Uniti;
>
> (II) all'ente regolatore funzionale federale competente[7] [come definito nell'articolo 509 della Legge Gramm-Leach-Bliley Act (15 U.S.C. 6809)], diverso dalla [Securities and Exchange Commission], e al Direttore della Federal Housing Finance Agency, nell'ambito di una relazione di controllo di qualità di un istituto soggetto alla giurisdizione di tale ente di regolazione;
>
> (III) i Procuratori generali dello Stato nell'ambito di un'indagine penale;

[7] L'espressione "Ente regolatore funzionale federale" nel succitato articolo (B)(ii)(II) è definita in 15 U.S.C. § 6809, includendovi:

- il Consiglio dei Governatori del Federal Reserve System,
- l'Ufficio del Comptroller of the Currency,
  il Consiglio d'amministrazione della Federal Deposit Insurance Corporation,
- il Direttore dell'Ufficio del Thrift Supervision,
- il Consiglio della National Credit Union Administration, e
- la Securities and Exchange Commission.

Oltre alla SEC, sono questi i vari enti regolatori degli istituti finanziari negli Stati Uniti.

(IV) qualsiasi autorità di regolazione statale competente[8]; e

(V) un organismo di autoregolazione, nell'ambito di una relazione di controllo di qualità su un intermediario o un operatore soggetto alla giurisdizione di tale organismo di autoregolazione,

ognuno dei quali manterrà riservate e privilegiate tali informazioni.

[8] L'espressione "autorità di regolazione statale" prevista dalla Norma 1001(a)(xi) del PCAOB designa "l'Agenzia statale o un'altra autorità competente per il rilascio di licenze o l'emissione di altri regolamenti della professione contabile nello Stato o negli Stati esercenti la giurisdizione su una società di contabilità pubblica registrata o su soggetti ad essa correlati..." Sostanzialmente sarebbero questi i Consigli statali di contabilità (State Boards of Accountancy) negli Stati Uniti.

Allegato III

Descrizione delle procedure applicabili di risoluzione delle controversie (ricorso)

Il meccanismo di ricorso del PCAOB citato nell'Accordo sulla protezione dei dati (DPA) consente a un interessato di presentare ricorso per reclami o controversie rimasti irrisolti e concernenti il trattamento dei suoi dati personali da parte del PCAOB nell'ambito del DPA. Il meccanismo di ricorso si articola in due gradi di esame. Come descritto nel DPA, il primo grado di esame si svolgerà dinanzi a una funzione indipendente interna al PCAOB (il "PCAOB's Hearing Officer" o Funzionario giudicante del PCAOB); il secondo grado di esame si terrà dinanzi a una funzione indipendente incaricata dal PCAOB (un *hearing officer* o funzionario giudicante proveniente da un'entità esterna).

1. Ricorso di primo grado – Funzionario giudicante del PCAOB

Il Funzionario giudicante del PCAOB funge da esaminatore indipendente e imparziale dei fatti in un procedimento amministrativo formale che richiede una decisione autorevole. Il Funzionario giudicante del PCAOB è un avvocato alle dipendenze del PCAOB ed è soggetto al Codice etico del PCAOB nonché alle restrizioni previste dall'articolo 105(b)(5) della Legge Sarbanes-Oxley Act (la Legge), compresa la gestione di informazioni riservate e non pubbliche, ma è indipendente da tutte le Divisioni e gli Uffici del PCAOB competenti per la richiesta ed il trattamento dei dati personali nell'ambito delle attività di sorveglianza del PCAOB. Il Funzionario giudicante del PCAOB è tenuto ad agire con onore e onestà, affinché tutte le delibere, le decisioni, le conclusioni e i verdetti emessi nell'esercizio delle sue funzioni siano equi e imparziali. Tali requisiti fondamentali di necessaria e appropriata autorità, indipendenza, obiettività, imparzialità ed equità sono applicabili al meccanismo di ricorso.

Le seguenti caratteristiche dell'Ufficio del Funzionario giudicante del PCAOB e il regolamento del PCAOB sono finalizzati a garantire l'indipendenza del Funzionario giudicante del PCAOB:

- L'Ufficio del Funzionario giudicante del PCAOB assume e conferma il proprio personale; il Funzionario giudicante del PCAOB ed i suoi collaboratori sono tenuti fisicamente separati dal restante personale del PCAOB. Il PCAOB è tenuto a dotare di fondi e risorse adeguati l'Ufficio del Funzionario giudicante del PCAOB.
- Ai membri del Consiglio ed al personale del PCAOB è esplicitamente vietato tentare di influenzare impropriamente le decisioni del Funzionario giudicante del PCAOB (durante l'esame di un contenzioso il personale può sottoporre prove e argomentazioni solo dandone preavviso e purché le tutte le parti possano intervenirvi). Il Codice Etico di PCAOB stabilisce provvedimenti disciplinari a carico del personale che violi tale obbligo.
- Un Funzionario giudicante del PCAOB non può essere revocato o destituito da un procedimento per influenzarne l'esito; in ogni caso la revoca di un Funzionario giudicante del PCAOB deve essere approvata dalla Securities and Exchange Commission statunitense.
- Tutte le decisioni concernenti le prestazioni e la remunerazione del Funzionario giudicante del PCAOB possono non tenere conto dell'esito del procedimento.

Il Funzionario giudicante del PCAOB dovrà esaminare imparzialmente il merito di un reclamo formale per accertare se durante il trattamento dei dati personali dell'interessato il personale del PCAOB abbia rispettato le garanzie stabilite nel DPA, ed esprimere una decisione autorevole in tempi ragionevoli.

In un ricorso di primo grado un interessato dovrà presentare un reclamo formale all'Ufficio del Funzionario giudicante del PCAOB, descrivendo dettagliatamente le proprie richieste o lagnanze riguardo al trattamento dei propri dati personali effettuato dal PCAOB. Il personale del PCAOB partecipante al trattamento dei dati personali dell'interessato dovrà presentare una risposta al reclamo e la controparte del PCAOB nel DPA potrà inviare una risposta descrivendo la propria partecipazione nell'ambito del trattamento e del trasferimento dei dati personali in esame. L'interessato dovrà ricevere una copia di tutte le risposte inviate al Funzionario giudicante del PCAOB, da cui però dovranno essere espunte tutte le informazioni considerate riservate dall'articolo 105(b)(5) della Legge. Il Funzionario giudicante del PCAOB dovrà esaminare il reclamo formale e le risposte ed emanare una decisione autorevole su qualsiasi circostanza esposta nella contestazione, ossia se nel trattamento dei dati personali in esame il personale del PCAOB abbia rispettato le garanzie descritte nel DPA.

Il ricorso di primo grado si concluderà quando il Funzionario giudicante del PCAOB emetterà una decisione scritta riguardo al reclamo dell'interessato. Se il funzionario giudicante del PCAOB concluderà che il personale del PCAOB non ha rispettato le garanzie previste nel DPA e oggetto del reclamo, il Funzionario giudicante del PCAOB ingiungerà al personale del PCAOB di rispettare le garanzie in questione. La decisione del Funzionario giudicante del PCAOB favorevole all'interessato sarà vincolante per il personale del PCAOB, e il PCAOB o il suo personale non potranno chiedere un ulteriore esame della decisione del Funzionario giudicante del PCAOB. Tutte le parti coinvolte riceveranno l'esito del procedimento amministrativo e l'interessato apprenderà la decisione formale tramite un documento redatto conformemente agli obblighi di riservatezza previsti dall'articolo 105(b)(5) della Legge. Dopo avere appreso la decisione del Funzionario giudicante del PCAOB l'interessato riceverà anche un'informativa sul ricorso di secondo grado descritto qui di seguito, nonché informazioni sulle modalità di avvio di tale ricorso di secondo grado. Ricorso di secondo grado – Funzionario giudicante proveniente da un'entità esterna.

2.

Il ricorso di secondo grado stabilito dal PCAOB conferirà all'interessato la possibilità di chiedere un esame della decisione formale emessa dal Funzionario giudicante del PCAOB. Il PCAOB ricorrerà ai servizi di un'entità esterna in passato già ingaggiata del PCAOB per servizi analoghi,[9] ossia l'invio di un funzionario giudicante per dirimere il ricorso di secondo grado. Tali funzionari giudicanti sono avvocati esperti, che durante la prestazione al PCAOB dei servizi previsti dall'accordo devono attenersi alle regole del PCAOB, compresi il Codice etico del PCAOB e le norme di indipendenza e imparzialità stabilite dal regolamento di giudizio del PCAOB. A richiesta del PCAOB, come stabilito in un contratto l'entità esterna invierà uno dei suoi funzionari giudicanti a presiedere con indipendenza e imparzialità un ricorso su una controversia. Un funzionario giudicante incaricato di presiedere il ricorso di secondo grado sarà denominato "revisore del ricorso" e firmerà con il PCAOB un impegno cogente di non divulgazione, in cui il funzionario giudicante ingaggiato confermerà di attenersi agli obblighi di riservatezza descritti nell'articolo 105(b)(5) della Legge durante l'esame delle informazioni riservate apprese nella procedura di ricorso.

Per avviare un ricorso di secondo grado l'interessato dovrà presentare un'istanza all'Ufficio di Segreteria del PCAOB entro 30 giorni dalla notifica della decisione del funzionario giudicante del PCAOB. Nell'istanza dovranno essere precisati i presunti errori o lacune della decisione emessa dal funzionario giudicante del PCAOB nel ricorso

[9] Non essendosi il PCAOB finora avvalso di più di un funzionario giudicante, il PCAOB ha stipulato un contratto con un altro organo di regolazione per potersi servire dei loro funzionari giudicanti. Quando si sono resi necessari più funzionari giudicanti, i loro funzionari giudicanti hanno operato come consulenti o appaltatori esterni del PCAOB e hanno presieduto alcuni procedimenti disciplinari. Il ricorso di secondo grado sarà condotto da uno di questi funzionari giudicanti, o in base a un accordo analogo.

di primo grado. Il Segretario del PCAOB emetterà rapidamente (entro 30 giorni) un ordine di assegnazione della controversia all'entità esterna, che designerà un funzionario giudicante a fungere da revisore del ricorso.

Il revisore del ricorso riceverà da ciascuna delle parti in causa (tra cui l'interessato, la controparte del PCAOB nel DPA e il personale del PCAOB) le argomentazioni e l'eventuale ulteriore documentazione a sostegno delle rispettive tesi. Come nel ricorso di primo grado l'interessato riceverà una copia di tutte le risposte presentate al revisore del ricorso, da cui però saranno espunte tutte le informazioni considerate riservate dall'articolo 105(b)(5) della Legge.

Basandosi sulle osservazioni presentate dalle parti e sul relativo verbale, il revisore del ricorso valuterà se i riscontri e le conclusioni del Funzionario giudicante del PCAOB siano stati arbitrari e immotivati, o comunque non conformi al DPA. Al termine dell'esame ed entro un termine ragionevole il revisore del ricorso esprimerà una decisione scritta che analizza le contestazioni mosse dall'interessato alla decisione precedente. Se nella decisione si concluderà che il personale del PCAOB non aveva rispettato le garanzie stabilite dal DPA, il revisore del ricorso ingiungerà al personale del PCAOB di rispettare le relative garanzie. La decisione del revisore del ricorso costituirà la determinazione definitiva sulla controversia.

Allegato IV

Vigilanza sull'attuazione delle garanzie del DPA da parte del PCAOB

Il DPA stabilisce che il controllo indipendente sulla conformità del PCAOB alle garanzie stabilite dal DPA sia effettuato dall'Office of Internal Oversight and Performance Assurance del PCAOB (di seguito "lo IOPA" o "l'Ufficio").[10]

Lo IOPA è un ufficio indipendente interno del PCAOB, che ha il compito di "effettuare un esame interno dei programmi e delle operazioni del PCAOB per contribuire a garantire l'efficienza, l'integrità e l'efficacia interne di tali programmi e operazioni. L'assicurazione fornita dall'Ufficio intende promuovere la fiducia del pubblico, della Securities and Exchange Commission e del Congresso nell'integrità dei programmi e delle operazioni del PCAOB."[11]

Per adempiere il compito affidatogli, tra le altre azioni lo IOPA dovrà individuare i rischi per l'efficienza, l'onorabilità e l'efficacia dei programmi e delle operazioni del PCAOB, e basandosi sulla propria valutazione del rischio eseguire esami, controlli di qualità e indagini sulle prestazioni e sull'assicurazione della qualità per rilevare e impedire sprechi, frodi, abusi e cattive gestioni dei programmi e delle operazioni del PCAOB; e raccomandare interventi costruttivi, che ove implementati riducano o eliminino i rischi individuati e promuovano la conformità alle leggi, ai regolamenti nonché alle norme ed alle politiche vigenti del PCAOB.

Le attività dello IOPA comprendono tra l'altro:

- Fornire una garanzia di qualità costante della concezione e dell'efficacia operativa dei programmi del PCAOB;
- Svolgere indagini sui programmi e sulle operazioni del PCAOB; e
- Ricevere ed esaminare le accuse di irregolarità presentate contro il personale del PCAOB, nonché i suggerimenti e i reclami su potenziali sprechi, frodi, abusi o cattiva gestione dei programmi o delle operazioni del PCAOB.

Per svolgere il loro lavoro come previsto dal Carta dello IOPA, il Direttore e il personale dello IOPA devono "essere esenti, sia di fatto che nell'apparenza, da impedimenti personali, esterni ed organizzativi che ne condizionino l'indipendenza". Al fine di promuovere tale indipendenza, a differenza di altri dipendenti di PCAOB (che generalmente rispondono a una sola persona all'interno del PCAOB), il Direttore risponde direttamente a tutti e cinque i membri del Consiglio del PCAOB. Come stabilito dalla Carta dello IOPA, il "giudizio sulle prestazioni del Direttore e la determinazione del suo corrispettivo si baseranno sulla gestione dell'Ufficio da parte del Direttore, sull'effettiva esecuzione del lavoro dell'Ufficio, ... ma non si baseranno sulla natura dei risultati degli esami, dei controlli di qualità e delle indagini dell'Ufficio". Inoltre l'indipendenza dello IOPA è rafforzata dalla durata dell'incarico del Direttore, limitata a un solo mandato quinquennale, e dalla soggezione dello stesso IOPA ad un esame periodico esterno dell'assicurazione della qualità. Inoltre lo IOPA può riferire al Consulente legale del PCAOB, compreso il Responsabile etico, in merito al proprio lavoro, tra cui gli esiti di indagini su denunce, reclami e/o accuse di cattiva condotta professionale o etica. Infine, lo IOPA ha diritto di accesso illimitato a tutto il

[10] L'articolo 9 del DPA stabilisce che, previa richiesta della controparte del PCAOB nel DPA di eseguire un esame indipendente della conformità con le garanzie previste nel DPA, il PCAOB notificherà allo IOPA di effettuare un esame per accertare e confermare l'effettiva attuazione delle garanzie previste dal DPA.

[11] Cfr. la Carta dello IOPA, consultabile nel sito web del PCAOB.

personale ed ai registri, alle relazioni, ai controlli di qualità, alle verifiche, ai documenti, ai carteggi, alle raccomandazioni o ad altri materiali del PCAOB.

Qualora lo IOPA apprendesse "problemi, abusi o carenze particolarmente gravi o flagranti, concernenti la gestione di programmi e operazioni del PCAOB e tali da richiedere un'attenzione immediata ... del Consiglio", lo IOPA dovrà immediatamente segnalare queste informazioni al Consiglio del PCAOB ed entro sette giorni di calendario anche alla SEC.

Al fine di svolgere il proprio lavoro, lo IOPA rispetta i principi e i requisiti accettati. Questi ultimi comprendono le istruzioni imperative dell'Institute of Internal Auditors, come (i) i Criteri Internazionali per la Pratica Professionale della Revisione Interna, (ii) i Principi fondamentali per la Pratica Professionale della Revisione Interna, (iii) la Definizione di Revisione Interna e (iv) il Codice Etico.

Riguardo al DPA, lo IOPA ha la capacità di condurre un esame della conformità del PCAOB alle pertinenti garanzie di protezione dei dati:

- Su iniziativa dello IOPA, ad esempio sulla base della propria valutazione dei rischi per i programmi e le operazioni del PCAOB;
- In risposta a denunce, reclami e/o accuse di cattiva condotta professionale o etica; o
- Su richiesta del Consiglio del PCAOB (ad esempio per adempiere il requisito, previsto dal DPA, che il PCAOB solleciti allo IOPA un esame a seguito di una richiesta).

Al fine di condurre tale esame, come precedentemente osservato, lo IOPA usufruirà dell'accesso illimitato a tutta la documentazione del PCAOB relativa alle pertinenti attività del PCAOB.

Lo IOPA eseguirà l'esame attenendosi al proprio processo di revisione standard e seguendo i Principi internazionali dell'Institute of Internal Auditors, articolati nelle fasi seguenti.

Pianificazione – Determinare gli obiettivi del controllo di qualità e i criteri di controllo della qualità appropriati. (I criteri del controllo di qualità si baseranno sulle clausole di garanzia descritte nell'accordo sulla protezione dei dati.) Inoltre, effettuare una valutazione preliminare del rischio assunto per realizzare gli obiettivi della direzione e individuare i controlli in atto per attenuare i rischi. Determinare l'ambito appropriato del controllo di qualità in relazione ai processi ed alle procedure di controllo da esaminare e verificare. Ideare le prove di conformità sostanziali da eseguire per valutare l'efficacia concettuale e operativa delle garanzie stabilite per la protezione dei dati.

Esecuzione – A seguito del programma documentato di controllo di qualità, eseguire il lavoro di verifica. Il lavoro di verifica generalmente consisterà nell'esame delle politiche e delle procedure e nelle descrizioni dei flussi di processo del sistema informatico; in colloqui con i titolari dei processi e dei controlli; in descrizioni/dimostrazioni delle garanzie e dei relativi controlli; nella riesecuzione da parte del revisore di alcune salvaguardie e controlli; nella verifica da parte del revisore di garanzie e controlli sulla base di selezioni di campioni rappresentativi e nell'esame della documentazione di accompagnamento attestante la progettazione e il funzionamento dei controlli.

Esame della qualità – La direzione dello IOPA supervisionerà il lavoro in corso ed esaminerà e approverà il prodotto del lavoro realizzato dal personale. La direzione dello IOPA determinerà la correttezza di eventuali problematiche del controllo di qualità evidenziate e l'adeguatezza delle prove addotte a conferma.

Resoconti – Lo IOPA redigerà un rapporto in cui renderà noto l'esito del suo esame. Saranno formulate raccomandazioni per risolvere le problematiche rilevate. Il rapporto comprenderà la risposta scritta del personale del PCAOB, precisando la concordanza con le osservazioni rilevate nel controllo di qualità, le azioni correttive intraprese o programmate e le date previste per il completamento. I rapporti saranno esaminati dal Consiglio direttivo del PCAOB e saranno comunicati alla controparte del PCAOB nel DPA dopo che il Consiglio direttivo del PCAOB avrà approvato la comunicazione non pubblica del rapporto a tale controparte. L'approvazione del Consiglio è richiesta solo per la comunicazione non pubblica delle conclusioni dello IOPA, come richiesto dal Codice etico del PCAOB, e non comprende il coinvolgimento del Consiglio nella redazione dei contenuti del rapporto dello IOPA, compresi i risultati dell'esame.

Monitoraggio – Al momento opportuno lo IOPA esaminerà gli interventi correttivi attuati dal personale del PCAOB per verificare che siano state ultimati in modo soddisfacente.