

Outsourcing e copertura terze parti ICT

Informativa privacy

* 1. Informativa ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (GDPR).

Per leggere l'informativa completa [clicca qui](#).

☐ Dichiaro di aver letto e compreso l'informativa sul trattamento dei dati personali.

Outsourcing e copertura terze parti ICT

Domande anagrafiche e generali

* 2. **A quale tipologia di istituto finanziario appartiene l'entità per cui stai compilando questo questionario?**

- ☐ Società finanziaria non bancaria (incluso leasing, factoring, intermediari in cambi, ecc.)
- ☐ Istituto bancario o creditizio
- ☐ Intermediario finanziario (SIM - SGR - SICAV - IMEL, ecc.)
- ☐ Altre istituzioni finanziarie (es. Borsa Italiana, Monte Titoli ecc.)

* 3. **Quante società appartenenti al Gruppo per conto del quale stai completando il questionario sono consolidate nel ROI?**

- ☐ 1
- ☐ Da 2 a 5
- ☐ Da 6 a 10
- ☐ Oltre 10

* 4. **Quanti Auditor lavorano nell'istituto finanziario per il quale stai completando il questionario?**

- ☐ Fino a 20
- ☐ Da 21 a 50
- ☐ Da 51 a 100
- ☐ Da 101 a 200
- ☐ Oltre 200

*** 5. Qual è il numero di Auditor dedicati (FTE) a Audit sulle terze parti nell'istituto finanziario per il quale stai completando il questionario?**

- ☐ Meno di 1 FTE
- ☐ Da 1 a 5 FTE
- ☐ Da 6 a 10 FTE
- ☐ Da 11 a 20 FTE
- ☐ Oltre 20 FTE

*** 6. Quali altre funzioni aziendali specialistiche svolgono verifiche dirette sulle terze parti, oltre all'Internal Audit (es. I° e/o II° livello, anche on site)? (Risposta multipla)**

- ☐ DPO
- ☐ Risk Management
- ☐ Sicurezza Informatica
- ☐ Compliance
- ☐ Altro - Specificare

*** 7. In quale funzione aziendale è collocato il governo del processo di gestione delle terze parti?**

- ☐ Procurement
- ☐ Organizzazione
- ☐ Funzione IT
- ☐ Altro - Specificare



Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

*** 8. Sono stati definiti dei criteri per distinguere in modo univoco i servizi ICT dai servizi non-ICT nei casi ibridi (es. servizi di back-office con forte componente tecnologica)?**

- ☐ Sì
- ☐ No
- ☐ Non valutato



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

9. Se presenti, quali criteri sono utilizzati?



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

* 10. Sono presenti servizi nel ROI valutati anche come non-ICT ai sensi EBA 2019 ma inseriti in ragione della "materialità" dei rischi ICT sottostanti?

- ☐ Sì
- ☐ No
- ☐ Non valutato



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

11. Se presenti, per quali ragioni?



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

*** 12. Viceversa, ci sono servizi ICT nel registro EBA 2019 che non sono stati inclusi nel ROI?**

- ☐ Sì
- ☐ No
- ☐ Non valutato



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

13. Se presenti, per quali ragioni?



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

*** 14. Considerando il medesimo servizio, la classificazione FEI nel registro EBA 2019 e CIF nel ROI è sempre coerente?**

- ☐ Sì
- ☐ No
- ☐ Non valutato



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Classificazione delle terze parti

15. Se non è coerente, per quali ragioni?



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Audit Universe

* 16. Quale approccio viene adottato per la mappatura della terza parte nell'Audit Universe?

- ☐ Servizio
- ☐ Contratto
- ☐ Fornitore
- ☐ Altro - Specificare



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Audit Universe

* 17. In relazione alla domanda precedente nella tua organizzazione, il servizio/contratto/fornitore è considerato:

- ☐ Un elemento autonomo dell'Audit Universe
- ☐ Un attributo di un altro elemento dell'Audit Universe (es. un processo)
- ☐ Entrambi
- ☐ Altro (specificare)



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Audit Universe

*** 18. Nell'Audit Universe vengono inseriti tutti i servizi/contratti/fornitori o viene adottato un approccio risk based?**

- ☐ Tutti
- ☐ Risk Based



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Audit Universe

19. Specificare secondo quali criteri



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Audit Universe

*** 20. Quali sono le "Golden Source" utilizzate per alimentare l'Audit Universe?
(Risposta multipla)**

- ☐ Registro EBA
- ☐ Registro ROI
- ☐ Procurement tool
- ☐ Registro asset IT - CMDB
- ☐ Risk Management tool
- ☐ Altro - Specificare

*** 21. Con quale frequenza è previsto un Audit sulla governance delle terze parti per verificare aspetti come la qualità dei dati, la corretta classificazione e la conformità del processo?**

- ☐ Annuale
- ☐ Biennale
- ☐ Triennale
- ☐ Altro - Specificare



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla mappatura

Con riferimento al ROI a marzo 2026 (dati al 31/12/2025)

*** 22. Qual è il livello di granularità adottato per la compilazione del ROI richiesto da DORA?**

- ☐ Accordo Quadro
- ☐ Contratto
- ☐ Servizio
- ☐ Ordine d'acquisto
- ☐ Altro - Specificare

*** 23. Con quanti fornitori ICT e non-ICT collaborano le società del Gruppo che contribuiscono al ROI?**

- ☐ Meno di 100
- ☐ Tra 101 e 200
- ☐ Tra 201 e 300
- ☐ Tra 301 e 400
- ☐ Tra 401 e 500
- ☐ Più di 500

*** 24. Quanti fornitori ICT sono inclusi nel ROI?**

- ☐ Meno di 100
- ☐ Tra 101 e 200
- ☐ Tra 201 e 300
- ☐ Tra 301 e 400
- ☐ Tra 401 e 500
- ☐ Più di 500

*** 25. Quanti record sono inclusi nel ROI?**

- ☐ Meno di 100
- ☐ Tra 101 e 200
- ☐ Tra 201 e 300
- ☐ Tra 301 e 400
- ☐ Tra 401 e 500
- ☐ Più di 500

*** 26. Quanti record sono censiti nel registro EBA delle esternalizzazioni (rif. Linee Guida 2019)?**

- ☐ Meno di 100
- ☐ Tra 101 e 200
- ☐ Tra 201 e 300
- ☐ Tra 301 e 400
- ☐ Tra 401 e 500
- ☐ Più di 500

*** 27. Quanti dei record individuati nel ROI sono classificati come servizi a supporto di CIF?**

- ☐ Meno di 100
- ☐ Tra 101 e 200
- ☐ Tra 201 e 300
- ☐ Tra 301 e 400
- ☐ Tra 401 e 500
- ☐ Più di 500

*** 28. Nella compilazione del ROI i contratti/servizi infragruppo vengono inclusi con gli stessi criteri di selezione di quelli extra gruppo?**

- ☐ Sì
- ☐ No
- ☐ Non valutato

*** 29. Quali parametri vengono utilizzati per definire una fornitura come "continuativa e ricorrente" e pertanto includerla all'interno del ROI, escludendo così i contratti one-off? (Risposta multipla)**

- ☐ Durata temporale
- ☐ Continuità del servizio (tenendo conto dei rinnovi periodici)
- ☐ Opex vs Capex
- ☐ Dipendenza operativa
- ☐ Valore economico
- ☐ Altro - Specificare



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sul Risk Assessment

*** 30. La tua organizzazione ha un processo formalizzato per stabilire quali servizi/contratti/fornitori sottoporre ad attività di Audit?**

- ☐ Sì
- ☐ No

*** 31. Qual è il livello di granularità sul quale viene effettuato il Risk Assessment delle terze parti?**

- ☐ Fornitore
- ☐ Contratto
- ☐ Servizio
- ☐ Processo aziendale
- ☐ Altro - Specificare

* 32. **Il Risk Assessment viene eseguito su:**

- ☐ Tutte le terze parti
- ☐ Un sottoinsieme di terze parti selezionate tramite criteri preliminari
- ☐ Solo fornitori di servizi critici/regolamentati
- ☐ Altro - Specificare

* 33. **Quali output prodotti da altre funzioni aziendali vengono utilizzati come input del Risk Assessment, per prioritizzare le attività di Audit sulle terze parti? (Risposta multipla)**

- ☐ Valutazioni della Prima Linea di Difesa (es. due diligence, vendor assessment, monitoraggio fornitore)
- ☐ Valutazioni della Seconda Linea di Difesa (es. Risk Management, Compliance, ICT/Cyber Risk)
- ☐ Attestazioni o assessment indipendenti (es. SOC report, certificazioni, Audit esterni)
- ☐ Audit precedenti / Gap aperti
- ☐ Non vengono utilizzate valutazioni effettuate da altre funzioni
- ☐ Altro - Specificare

* 34. **Come viene utilizzato l'output del Risk Assessment? (Risposta multipla)**

- ☐ Prioritizzazione degli Audit
- ☐ Definizione della copertura
- ☐ Valutazione degli elementi dell'Audit Universe
- ☐ Supporto al professional judgment
- ☐ Decisioni gestionali
- ☐ Altro - Specificare

* 35. **Nel processo di Risk Assessment vengono considerati anche i subfornitori (sub-outsourcer)?**

- ☐ Sì
- ☐ Solo in alcuni casi
- ☐ No
- ☐ Non applicabile

* 36. **Le informazioni necessarie sono facilmente accessibili e correlate tra loro?**

- ☐ Sì
- ☐ Parzialmente
- ☐ No



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sul Risk Assessment

37. Se sì/parzialmente, come vengono gestite le correlazioni?



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sul Risk Assessment

38. Specificare eventuali criticità



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sul Risk Assessment

*** 39. Quali sono i principali fattori che dovrebbero essere considerati per determinare il livello di rischio della terza parte ai fini della prioritizzazione delle attività di Audit? (Risposta multipla, fino a un massimo di 7)**

- ☐ Criticità/importanza del servizio (i.e. supporto a CIF/Critical Business Services)
- ☐ Numerosità delle LE del gruppo servite
- ☐ Tipologia e sensibilità dei dati trattati
- ☐ Tecnologia utilizzata nella fornitura del servizio (es. IA, Cloud)
- ☐ Dipendenza dal fornitore
- ☐ Concentrazione del rischio
- ☐ Localizzazione geografica
- ☐ Rilevanza ICT/Cyber
- ☐ Incidenti rilevati
- ☐ Esiti di Audit precedenti / Gap aperti
- ☐ Valore economico del contratto
- ☐ Performance del fornitore
- ☐ Altre remediation aperte (es. gap ICT/security)
- ☐ Catena di subfornitura
- ☐ Valutazioni della Prima Linea
- ☐ Valutazioni della Seconda Linea
- ☐ Altro - Specificare

*** 40. Quale output ti aspetti da un Risk Assessment delle terze parti/contratti/servizi?**

- ☐ Ranking puntuale delle terze parti/contratti/servizi
- ☐ Cluster delle terze parti/contratti/servizi (gruppi di priorità es. L ML MH H)
- ☐ Altro - Specificare



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla copertura

*** 41. Quali sono le principali modalità di copertura e monitoraggio delle terze parti ICT adottate? (Risposta multipla - selezionare tutte quelle applicabili)**

- ☐ Audit standard
- ☐ Audit Lean (approccio di Audit risk-based e proporzionato per fornitori ICT con profilo di rischio contenuto, caratterizzato da un utilizzo estensivo delle informazioni già disponibili, assessment mirati e verifiche focalizzate)
- ☐ Audit in pool
- ☐ Attestazioni esterne indipendenti
- ☐ Continuous auditing/assurance
- ☐ Altro - Specificare
-

*** 42. Avete previsto o adottate un approccio che combina diverse modalità di copertura delle terze parti ICT?**

- ☐ Sì
- ☐ No



Outsourcing e copertura terze parti ICT

Domande sulla copertura

43. In caso affermativo, specificare quali approcci

*** 44. In caso affermativo, quali sono i principali criteri che determinano la scelta? (1= per nulla rilevante; 5=determinante/fattore decisivo)**

	1	2	3	4	5
Criticità del servizio	☐	☐	☐	☐	☐
Rischio ICT	☐	☐	☐	☐	☐
Cyber Risk	☐	☐	☐	☐	☐
DORA	☐	☐	☐	☐	☐
Esiti di Audit precedenti	☐	☐	☐	☐	☐
Incident	☐	☐	☐	☐	☐
Performance del fornitore	☐	☐	☐	☐	☐
Rating del fornitore	☐	☐	☐	☐	☐

Outsourcing e copertura terze parti ICT

Domande sulla copertura

*** 45. Con quale frequenza vengono rivalutate le modalità di copertura delle terze parti ICT rispetto alle modalità identificate?**

- ☐ Annualmente
- ☐ Ogni due anni
- ☐ Solo al rinnovo contrattuale
- ☐ Event-driven
- ☐ Altro - Specificare

*** 46. Avete partecipato ad iniziative di Pool audit o Audit congiunti nei confronti di terze parti ICT?**

- ☐ Sì
- ☐ No

Outsourcing e copertura terze parti ICT

Domande sulla copertura

*** 47. In caso affermativo, relativamente alla fase di esecuzione di un Audit svolto in pool, quali ritenete siano gli svantaggi più rilevanti? (Risposta multipla)**

- ☐ Complessità nel coordinamento tra diverse entità partecipanti con metodologie diverse.
- ☐ Difficoltà nel garantire l'assenza di conflitti di interesse tra gli auditor del pool.
- ☐ Potenziale limitazione nell'ispezionare aree specifiche di interesse esclusivo della nostra entità.
- ☐ Gestione della riservatezza dei dati e delle informazioni sensibili scambiate nel pool.
- ☐ Costi elevati
- ☐ Altro - Specificare

*** 48. In caso affermativo, relativamente alla fase di esecuzione di un Audit svolto in pool, quali ritenete siano i vantaggi più rilevanti? (Risposta multipla)**

- ☐ Facilità di "accesso" a Player Globali
- ☐ Knowledge sharing tra i partecipanti
- ☐ Team di Audit ben strutturati con presenza di elevati skill
- ☐ Costi suddivisi tra i partecipanti
- ☐ Ottimizzazione tempi e risorse
- ☐ Altro - Specificare



Associazione Italiana
Internal Auditors

Outsourcing e copertura terze parti ICT

Domande sulla copertura

*** 49. Quale modalità di copertura prevedete di incrementare nei prossimi 2-3 anni? (Risposta multipla)**

- ☐ Audit standard
- ☐ Audit Lean
- ☐ Audit in pool
- ☐ Attestazioni esterne indipendenti
- ☐ Continuous auditing/assurance

50. Rispetto alle 5 tipologie di Audit, qual è il livello di maturità della tua organizzazione? (1=Initial; 5= Optimized)

	1	2	3	4	5
Audit standard	☐	☐	☐	☐	☐
Audit Lean	☐	☐	☐	☐	☐
Audit in pool	☐	☐	☐	☐	☐
Attestazioni esterne indipendenti	☐	☐	☐	☐	☐
Continuous auditing/assurance	☐	☐	☐	☐	☐

51. Rispetto alle 5 tipologie di Audit, qual è il livello di efficacia che attribuite a ciascuna tipologia? (1=Initial; 5= Optimized)

	1	2	3	4	5
Audit standard	☐	☐	☐	☐	☐
Audit Lean	☐	☐	☐	☐	☐
Audit in pool	☐	☐	☐	☐	☐
Attestazioni esterne indipendenti	☐	☐	☐	☐	☐
Continuous auditing/assurance	☐	☐	☐	☐	☐

*** 52. In che misura fate affidamento sulle attestazioni esterne indipendenti?**

- ☐ Sempre
- ☐ Spesso
- ☐ Raramente

53. Elencare quali sono le attestazioni principali a cui fate riferimento

*** 54. Nel caso di Audit diretto presso una terza parte, condividete con il fornitore la documentazione e/o il report che riporta gli esiti della verifica?**

- ☐ Sì
- ☐ No

*** 55. Quanti Audit vengono fatti ogni anno sulle terze parti?**

- ☐ Meno di 5 Audit
- ☐ Tra 5 e 10 Audit
- ☐ Più di 10 Audit

56. Il Campo del ROI "Ultimo Audit fatto" b_07.01.0070 viene compilato sulla base di:

- ☐ Qualsiasi Audit fatto sul fornitore
- ☐ Un Audit a copertura totale sul servizio specifico
- ☐ Un Audit a copertura parziale sul servizio specifico
- ☐ Altro - Specificare

*** 57. La funzione Internal Audit esegue anche Audit che coprono processi critici, senza coprire eventuali fornitori di quei processi?**

- ☐ Sì
- ☐ No

*** 58. Quali sono i punti minimi per i quali si ritiene coperto un fornitore? (Risposta multipla)**

- ☐ Analisi dei controlli precontrattuali (es. classificazione, due diligence, risk assessment, ecc.)
- ☐ Analisi del contratto (es. clausole di sub-fornitura, access & audit rights, clausole di exit, ecc)
- ☐ Monitoraggio nel continuo del fornitore (KPI e attività in caso di violazioni)
- ☐ Analisi piani di Business Continuity
- ☐ Analisi delle attività che vengono svolte dal fornitore, come parte di un Audit di processo
- ☐ Altro