

Servizio di certificazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) Secondo gli standard UNI CEI ISO/IEC 27001:2013

Capitolato Tecnico

Sommario

1.	PREMESSE, ORGANIZZAZIONE E AMBITO DI CERTIFICAZIONE.....	3
2.	OGGETTO	6
3.	MODALITA' E TEMPI DI ESECUZIONE DELL'APPALTO	7
4.	REQUISITI DEL FORNITORE	8
5.	DURATA	8
6.	PENALI	9
7.	VALORE DELL'APPALTO, FATTURAZIONE E PAGAMENTI.....	9

1. PREMESSE, ORGANIZZAZIONE E AMBITO DI CERTIFICAZIONE

Agenzia delle entrate-Riscossione (di seguito, anche solo “AdeR” o “Ente”) è un Ente pubblico economico istituito ai sensi dell'articolo 1 del Decreto legge 22 ottobre 2016, n. 193, convertito con modificazioni dalla Legge 1 dicembre 2016 n. 225, e svolge le funzioni relative alla riscossione nazionale.

L'Ente è sottoposto all'indirizzo e alla vigilanza del Ministro dell'Economia e delle Finanze ed è strumentale all'Agenzia delle entrate a cui è attribuita la titolarità della riscossione nazionale ai sensi dell'articolo 3, comma 1, del Decreto legge 30 settembre 2005 n. 203, convertito con modificazioni dalla Legge 2 dicembre 2005, n. 248.

L'Ente opera attraverso la seguente struttura organizzativa articolata in:

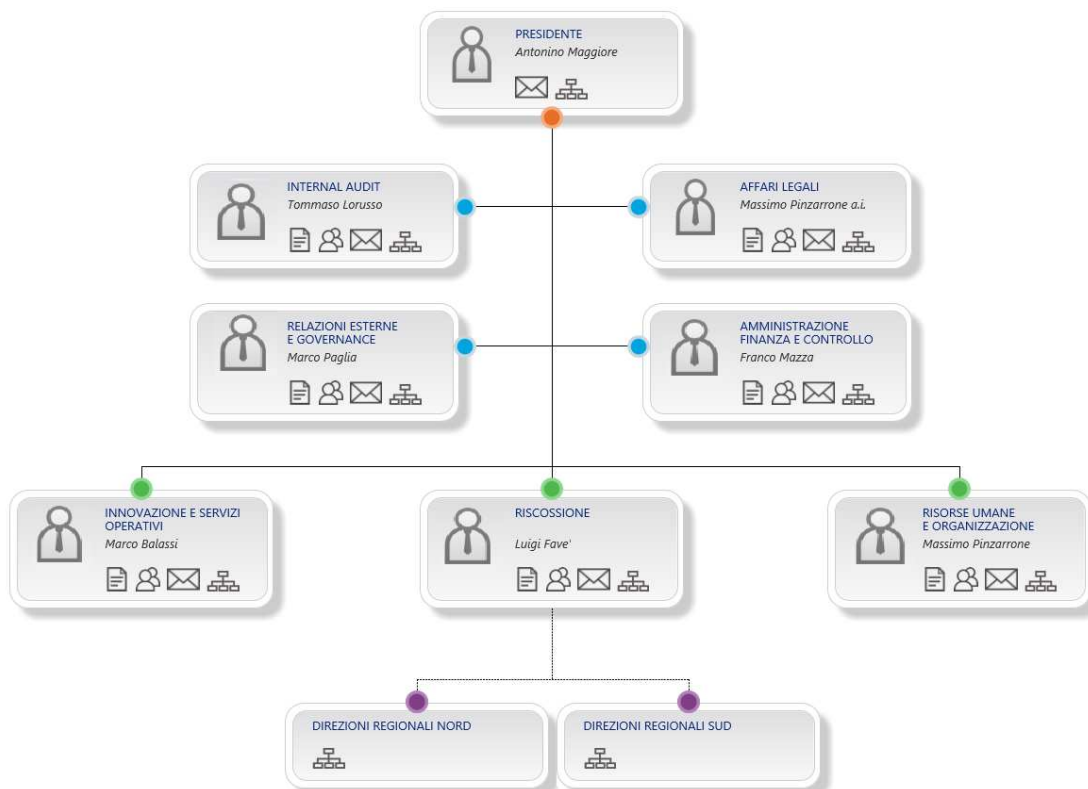
- 1 Direzione Generale con sede in Roma
- 18 Direzioni Regionali
- 61 Aree territoriali

AdeR, come Ente pubblico economico, ha autonomia organizzativa, patrimoniale, contabile e di gestione. Gli organi sociali di Agenzia delle entrate-Riscossione sono il Presidente, il Comitato di gestione e il Collegio dei revisori dei conti. Il Comitato di gestione è composto dal Direttore dell'Agenzia delle entrate in qualità di Presidente dell'Ente e da due componenti nominati dall'Agenzia medesima tra i propri dirigenti.

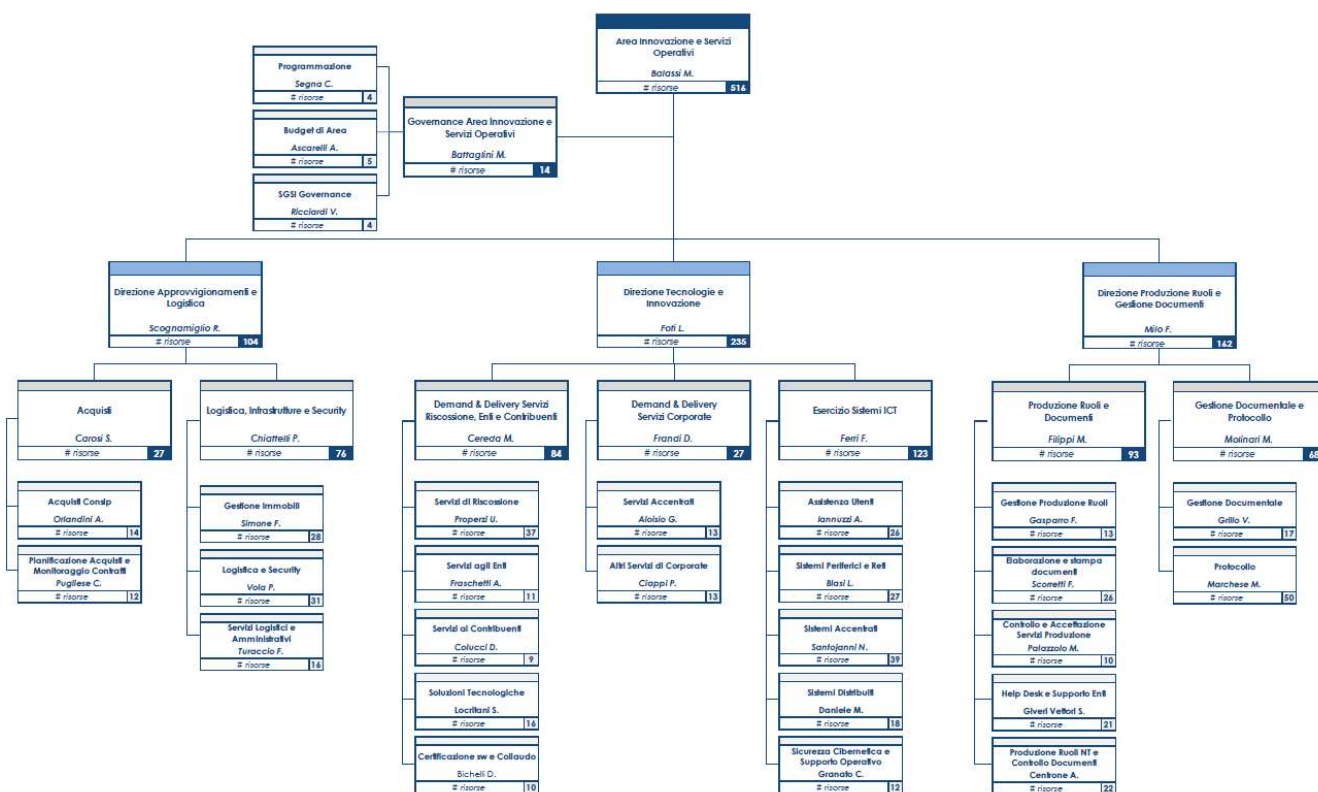
L'obiettivo dell'Agenzia delle entrate-Riscossione è di migliorare l'attività di riscossione nazionale mediante un approccio che garantisca economicità della gestione, soddisfazione dei contribuenti per i servizi prestati e aumento dei volumi di riscossione, anche mediante azioni di prevenzione e contrasto dell'evasione ed elusione fiscale.

Di seguito viene illustrato l'organigramma di AdeR con i riporti gerarchici di primo livello per ogni struttura evidenziata ed il dettaglio dell'organigramma dell'Area Innovazione e Servizi Operativi.

AdeR



Area Innovazione e Servizi Operativi



Il corretto esercizio delle attività istituzionali inerenti alla riscossione nazionale e l'amministrazione dei processi corporate da parte dell'Agenzia delle entrate-Riscossione è strettamente correlato alla disponibilità, all'integrità e alla riservatezza dei dati contenuti nel proprio sistema informativo.

AdeR, a tal riguardo, in considerazione di quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017 - 2019, emanato dall'Agenzia per l'Italia Digitale ha deciso di definire ed attuare un efficace Sistema di Gestione per la Sicurezza delle Informazioni (di seguito anche "SGSI"), a norma UNI EN ISO 27001:2013.

Il SGSI, che si innesta all'interno dei processi già presidiati dall'Ente in coerenza con il modello organizzativo ed il sistema delle responsabilità da quest'ultimo adottato, è gestito all'interno dell'Area Innovazione e Servizi Operativi dall'ufficio SGSI Governance.

Agenzia delle entrate-Riscossione ha intrapreso un percorso finalizzato all'adozione del SGSI per tutte le informazioni e i dati gestiti, sia nell'ambito delle attività di riscossione che nell'ambito dei processi amministrativi/corporate.

L'adozione del Sistema SGSI seguirà un approccio di tipo modulare, venendo via via implementato, a partire dalle informazioni e dai dati trattati nell'ambito del Data Center allocato presso le sedi di Roma e di Torino, fino ad estendersi progressivamente a tutti i dati e le informazioni dell'Ente.

2. OGGETTO

Agenzia delle entrate-Riscossione ha, l'obiettivo di conseguire entro il 2019 la certificazione UNI CEI/ISO 27001:2013 del proprio SGSI, con riferimento ai processi ed ai servizi gestiti da AdeR a partire da quelli erogati per la gestione del Data Center, allocato presso le sedi di Roma e di Torino.

Il servizio di certificazione, in relazione all'ambito poc'anzi indicato, ha ad oggetto le attività di Audit preliminare, Audit iniziale e sorveglianza per il rilascio ed il mantenimento della certificazione del Sistema di gestione per la sicurezza delle informazioni (SGSI) di AdeR in conformità alla norma UNI CEI ISO/IEC 27001:2013.

Le attività dovranno essere realizzate conformemente alle prescrizioni della normativa internazionale di riferimento.

Costituiscono oggetto del presente appalto tutte le prestazioni e le forniture necessarie per l'esecuzione del servizio così come descritto.

a) Attività di Audit preliminare

Scopo dell'attività di Audit preliminare (di natura documentale ed on-site presso il sito di Roma) sarà quella di valutare la completezza e la conformità del SGSI (documentazione di sistema, processi e procedure) ai requisiti della normativa di riferimento, la sua applicazione e, soprattutto, la coerenza dello stesso col perimetro individuato, al fine di ottenere il certificato attestante la conformità alla norma UNI CEI ISO/IEC 27001:2013.

Costituiscono oggetto delle attività di Audit preliminare tutte le prestazioni intellettuali svolte dal personale incaricato di tali attività, incluse, eventualmente, quelle svolte on-site presso il sito di Roma e la fornitura ad AdeR del, o dei, rapporti conclusivi.

Al termine delle attività di Audit preliminare, la cui finalità è di verificare lo stato di attuazione del SGSI, ovvero se è sufficientemente maturo per l'Audit di certificazione, il Fornitore dovrà redigere e rilasciare ad AdeR specifici rapporti che evidenzino:

- gli eventuali aspetti del SGSI non ancora attuati e necessari per l'audit di certificazione,

- le opportunità di miglioramento del SGSI in termini della qualità della documentazione, dell'organizzazione e dei processi.

Per ciascun aspetto che possa mettere a rischio il processo di certificazione è inoltre richiesto di specificare i requisiti della norma che risultano non attuati. Sarà cura del committente a fronte delle risultanze dell'audit preliminare predisporre ed attuare un piano di azioni correttive e migliorative.

b) Attività di Audit iniziale e sorveglianza

Scopo delle verifiche dell'Organismo di Certificazione (documentale, iniziale e di sorveglianza/mantenimento) è quello di valutare la completezza e la conformità del SGSI di AdeR (documentazione di sistema, processi e procedure) ai requisiti della normativa di riferimento, la sua effettiva applicazione e il mantenimento al fine di ottenere il certificato attestante la conformità del sistema alle prescrizioni della normativa.

Le verifiche per il rilascio della certificazione seguiranno il criterio del campionamento degli item da sottoporre ad audit iniziale e di sorveglianza.

Costituiscono oggetto delle attività di audit iniziale e di sorveglianza tutte le prestazioni intellettuali svolte dal personale incaricato delle attività di Audit preliminare, incluse quelle svolte on-site presso i 2 siti di Roma e di Torino.

3. MODALITA' E TEMPI DI ESECUZIONE DELL'APPALTO

Il fornitore si impegna a svolgere le attività relative all'Audit preliminare, al ciclo di certificazione ed al successivo mantenimento, articolate nelle fasi di seguito indicate:

1. audit preliminare;
2. audit iniziale;
3. 1° sorveglianza;
4. 2° sorveglianza.

Per l'esecuzione di ciascuna della attività elencate il fornitore dovrà indicare l'impegno espresso in giorni/uomo.

La fase di Audit preliminare dovrà essere effettuata successivamente alla stipula del contratto entro la data comunicata al Fornitore da AdeR, con un preavviso minimo di 10 (dieci) giorni, e comunque concludersi entro il mese di luglio del 2019.

La fase di Audit iniziale e rilascio del certificato dovrà essere effettuata trascorsi almeno 3 (tre) mesi successivamente alla conclusione della fase di Audit preliminare, entro la data comunicata al Fornitore da AdeR, con un preavviso minimo di 10 (dieci) giorni, e comunque concludersi entro 30 (trenta) giorni solari.

A seguito dell'esito positivo, il fornitore dovrà rilasciare il certificato entro 10 (dieci) giorni lavorativi dalla data del verbale di Audit.

Dalla data di rilascio del certificato di qualità da parte del Fornitore decorreranno i termini per l'effettuazione delle prestazioni relative alle successive fasi di sorveglianza.

4. REQUISITI DEL FORNITORE

Il Fornitore, che svolgerà il servizio, deve essere Organismo di certificazione per la norma **UNI CEI ISO/IEC 27001:2013** accreditato da Accredia, l'Ente Italiano di Accreditamento, ovvero da equivalenti enti certificatori esteri equiparati, per i settori di accreditamento IAF EA 33 (Tecnologia dell'informazione), EA 35 (altri Servizi) ed EA 36 (Pubblica amministrazione). Il Fornitore dovrà mantenere tale accreditamento per tutta la durata della certificazione.

Il Fornitore, nel pieno rispetto degli standard ISO e dei regolamenti di ACCREDIA, dovrà possedere organizzazione, mezzi e risorse idonee e adeguate, sia sotto il profilo dei requisiti normativi, sia sotto il profilo dei servizi professionali, ed essere in grado di offrire un servizio con elevato standard di qualità, alle condizioni previste dal presente capitolato d'appalto e dai documenti da esso richiamati.

Il servizio dovrà essere eseguito dal fornitore, con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di un'organizzazione efficiente, risorse e mezzi adeguati. Il fornitore, inoltre dovrà essere in regola con tutte le prescrizioni di legge attinenti ai servizi appaltati, gestiti a proprio esclusivo rischio e sotto la propria direzione, sorveglianza e diretta responsabilità.

Il fornitore si impegna, inoltre, a svolgere tutte le attività, anche non espressamente indicate negli atti della gara e nel contratto, che si rendessero necessarie per garantire l'efficiente svolgimento del servizio.

Il servizio deve essere organizzato e svolto con disponibilità di risorse umane e tecnologiche adeguate e a norma di legge rispetto alla consistenza qualitativa/quantitativa e all'osservanza dei parametri di sicurezza delle persone fisiche e delle strutture coinvolte.

5. DURATA

Il contratto avrà durata a decorrere dalla sottoscrizione del verbale di avvio dell'esecuzione dell'attività fino alla scadenza naturale del certificato emesso.

6. PENALI

Per ogni giorno di ritardo nell'esecuzione della singola prestazione e nella emissione del certificato rispetto ai termini di cui al precedente par. 3, AdeR potrà applicare direttamente sui corrispettivi maturati dall'appaltatore una penale di importo pari all'uno per mille del corrispettivo contrattuale.

Trascorsi 10 (dieci) giorni dalla scadenza del termine massimo fissato per il completamento delle attività in carico all'appaltatore, AdeR risolverà di diritto il contratto.

L'applicazione delle penali, di cui al presente articolo, non esonera in alcun caso l'appaltatore dall'adempimento dell'obbligazione per la quale si è reso inadempiente, che ha fatto scaturire l'obbligo di pagamento della medesima penale.

AdeR potrà applicare all'appaltatore penali sino alla misura massima del 10% (dieci per cento) del corrispettivo complessivo massimo del presente contratto, dopo di che la stessa potrà dichiarare la risoluzione di diritto del contratto.

L'applicazione delle penali previste dal presente articolo non preclude il diritto di AdeR di richiedere il risarcimento degli eventuali maggiori ed ulteriori danni.

7. VALORE DELL'APPALTO, FATTURAZIONE E PAGAMENTI

Il valore complessivo dell'appalto in oggetto sarà quello offerto dall'aggiudicatario della procedura. Nel valore offerto per l'appalto sono inclusi tutti gli oneri accessori (spese di trasferta, generali, etc.) che l'Ente di Certificazione dovrà sostenere per l'effettuazione delle verifiche.

Gli oneri della sicurezza per rischi interferenti sono pari a zero.

I Servizi forniti dal fornitore saranno oggetto di fatturazione da parte dello stesso, a seguito di ciascuna fase prevista ai fini del rispetto della normativa UNI CEI ISO/IEC 27001:2013 con le seguenti modalità:

Attività	Percentuale
----------	-------------

A seguito dell'effettuazione dell'Audit preliminare	17%
A seguito dell'effettuazione dell'Audit iniziale	49%
A seguito dell'effettuazione dell'Audit relativo alla 1° sorveglianza	17%
A seguito dell'effettuazione dell'Audit relativo alla 2° sorveglianza	17

Il Responsabile del
Procedimento
Valerio Ricciardi
(Firmato Digitalmente)