

SGSI - Audit interni di primo livello

Agenzia delle entrate - Riscossione

Indice dei Contenuti

1	Introduzione.....	3
1.1	Scopo.....	3
1.2	Contenuto e destinatari	3
1.3	Acronimi	4
2	Gestione Audit interni di primo livello	5
2.1	Definizione del Programma di Audit	6
2.2	Pianificazione degli Audit.....	7
2.3	Preparazione degli Audit.....	7
2.4	Conduzione degli Audit.....	7
2.5	Chiusura degli Audit.....	8
2.6	Azioni successive agli Audit	9
2.7	Valutazione dei risultati	9
A.	Appendice – Linee guida per la qualificazione degli Auditor	11
B.	Appendice - Guida alla compilazione dei moduli di audit.....	12
B.1	Guida alla compilazione del modulo Programma di audit.....	12
B.2	Guida alla compilazione del modulo di Rapporto di Audit Interno	13

1 Introduzione

1.1 Scopo

Il presente documento illustra la procedura per la gestione e conduzione **degli Audit interni di primo livello** (di seguito anche semplicemente Audit) relativi alle attività inerenti:

- al Sistema di Gestione della Sicurezza delle Informazioni (SGSI);
- agli aspetti organizzativi documentati su: Manuale SGSI [4], Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni [5], Regolamenti interni, Codice Etico, Procedure, Piani ecc.

Le Norme, le leggi, i requisiti ed i regolamenti utilizzati come termini di confronto per le evidenze degli Audit, costituiscono i criteri di Audit, così come definiti dalla Norma UNI EN ISO 19011 [2].

Gli Audit sono svolti ad intervalli pianificati, al fine di stabilire se gli obiettivi di controllo, i controlli, i processi e le procedure inerenti alla sicurezza delle informazioni sono:

- conformi ai requisiti delle Normative di riferimento;
- conformi ai requisiti identificati per la sicurezza delle informazioni;
- realizzati, mantenuti ed aggiornati;
- efficaci ed efficienti rispetto alle attese.

Nel presente documento sono descritti i criteri e le modalità per definire, pianificare, condurre e documentare gli Audit interni di primo livello, in considerazione di quanto contenuto nella norma UNI EN ISO 19011 "Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale" [2].

I risultati degli Audit interni di primo livello saranno utilizzati per il riesame del SGSI al fine di individuare eventuali azioni di miglioramento da apportare al sistema.

Al fine di creare le opportune sinergie e coordinare eventuali azioni comuni tra le attività inerenti agli audit di primo e di secondo livello, l'Ufficio SGSI Governance informerà la Direzione Internal Audit dell'inizio delle proprie attività.

In ogni caso la documentazione relativa alle attività di audit di primo livello sarà resa disponibile alla Direzione Internal Audit.

1.2 Contenuto e destinatari

Il presente documento è aggiornato e revisionato a cura del Gestore SGSI. Le indicazioni contenute nel documento sono rivolte al personale coinvolto nella gestione degli audit di primo livello, appartenente all'ufficio SGSI Governance. Riferimenti normativi e documentali.

- [1] UNI CEI ISO/IEC 27001:2014 "Tecnologia delle Informazioni – Tecniche di sicurezza – Sistemi di gestione per la sicurezza delle informazioni - Requisiti"
- [2] UNI EN ISO 19011 "Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale"
- [3] PGS_SGSI_Gestione Non Conformità e Azioni Correttive
- [4] DIS_SGSI_Implementazione_SGSI "Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)"

[5] DIS_SGSI_MANUALE “Manuale per la sicurezza delle informazioni”

1.3 Acronimi

AISO – Area Innovazione e Servizi Operativi

NC1 - Non-Conformità di categoria 1

NC2 - Non-Conformità di categoria 2

OSS - Osservazione

RGA - Responsabile del Gruppo di Audit

SGSI – Sistema di Gestione per la Sicurezza dell'Informazione

2 Gestione Audit interni di primo livello

Gli Audit interni di primo livello sono svolti ad intervalli pianificati e sono costituiti da diverse fasi:

- definizione del Programma di Audit;
- pianificazione degli Audit;
- preparazione degli Audit;
- conduzione degli Audit;
- chiusura degli Audit;
- azioni successive agli Audit;
- valutazione dei risultati.

Gli attori coinvolti sono:

- gli *Auditor interni per il SGSI* che eseguono gli Audit. Fra i vari Auditor deve essere identificato da parte del *Gestore del SGSI* il *Responsabile del Gruppo di Auditor (RGA)*;
- le strutture sottoposte ad Audit;
- eventuali osservatori;
- il *Gestore del SGSI*;
- il *Responsabile del SGSI*.

Di seguito si riporta la mappa delle responsabilità, rappresentata attraverso la c.d. matrice RACI. Ogni attività viene dettagliata nei successivi paragrafi.

Di seguito viene illustrato il significato della notazione RACI:

R = Responsible: esegue l'attività e ne è responsabile; per la stessa attività è ammessa una responsabilità condivisa.

A = Accountable: coordina, supervisiona e approva i risultati dell'attività; è unico per l'attività.

C = Consulted: è consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.

I = Informed: è informato dei risultati dell'attività.

N°	Attività	Respons. Gruppo di Audit (RGA)	Auditor interni per il SGSI	Struttura soggetta ad Audit	Gestore del SGSI	Responsabile del SGSI
1	Definizione del Programma di Audit				R	A
2	Pianificazione degli Audit	R/A	C		I	
3	Preparazione degli Audit	R/A	C	C	I	
4	Conduzione degli Audit	R/A	C	C		

N°	Attività	Respons. Gruppo di Audit (RGA)	Auditor interni per il SGSI	Struttura soggetta ad Audit	Gestore del SGSI	Responsabile del SGSI
5	Chiusura degli Audit	R/A	C	C	I	
6	Azioni successive agli Audit	C	C	R	A	
7	Valutazione risultati	C	C	C	R	A

2.1 Definizione del Programma di Audit

Il Gestore SGSI produce annualmente il Programma di Audit interni di primo livello sulla base dello stato e dell'importanza dei processi e delle strutture da sottoporre ad Audit, anche in funzione dei risultati di Audit precedenti, delle indicazioni emerse in sede di Riesame del Vertice, delle eventuali evoluzioni o modifiche del Sistema di cui si ritiene opportuno verificarne l'applicazione.

Il Gestore del SGSI richiede l'approvazione del programma al Responsabile del SGSI e successivamente informa i Responsabili delle Strutture interessate e gli Auditor interni per il SGSI per avviare l'esecuzione del Programma di Audit interni di primo livello.

Il Programma di Audit viene aggiornato sulla base di:

- variazioni agli Audit già pianificati;
- risultati degli Audit effettuati nei mesi precedenti;
- aggiornamenti dei documenti di pianificazione.

Per il Programma di Audit interni di primo livello, viene compilato il modulo "Programma di Audit per la sicurezza ICT" (MGS_SGSI_Programma audit).

Il Programma contiene:

- anno di riferimento del Programma di Audit;
- emittente;
- numero degli Audit programmati.

Per ogni sessione di Audit prevista:

- processo/Struttura da sottoporre ad Audit;
- persona da contattare/Responsabile del Processo o struttura da sottoporre ad Audit;
- Auditor: Responsabile del Gruppo di Audit (RGA) e altri Auditor;
- Data prevista per l'Audit.

Il Gestore del SGSI, attraverso il Programma di Audit, assegna agli Auditor gli incarichi relativi agli Audit da effettuare, e nomina i Responsabili del Gruppo di Audit. (Nota: qualora vi sia un solo Auditor, egli svolge tutti i compiti affidati come Responsabile di un gruppo di Audit).

La scelta dell'Auditor viene effettuata coerentemente con la sua esperienza professionale e sulla base dell'oggetto dell'Audit da eseguire. In Appendice A sono riportati i criteri di qualificazione degli Auditor Interni. La scelta degli Auditor e la conduzione degli Audit assicurano l'obiettività e l'imparzialità del processo di Audit.

Il Gestore del SGSI può altresì avvalersi della collaborazione di personale esterno avente specifica competenza in materia di Audit.

Se non pienamente coperte dagli Auditor del gruppo di Audit, le conoscenze e le competenze necessarie per condurre l'Audit il Gestore del SGSI si può avvalere della collaborazione di esperti tecnici interni o personale esterno avente specifica competenza in materia di Audit.

La conduzione degli Audit interni può essere unificata ad altri Audit (es. Qualità) previste in AeR, in cui è coinvolto un team di Auditor appartenenti a varie strutture opportunamente formati e qualificati.

2.2 Pianificazione degli Audit

Ciascun Audit contenuto nel Programma viene pianificato e concordato con il Responsabile della struttura soggetta all'Audit. In particolare il Responsabile del Gruppo di Audit (RGA) concorda la data effettiva in maniera tale da non interferire con la normale attività lavorativa del personale coinvolto.

Il RGA invia al Responsabile della struttura soggetta ad Audit le informazioni sull'Audit pianificato comprendente l'ambito, l'identificativo, i criteri, l'oggetto, la data proposta o concordata, la durata prevista. La comunicazione dell'Audit viene inviata attraverso messaggio di posta elettronica al Responsabile della struttura soggetta ad Audit e per conoscenza al Gestore del SGSI. Qualora il Responsabile del Gruppo di Audit non riesca a fissare una data per l'intervista, deve darne comunicazione al Gestore SGSI.

2.3 Preparazione degli Audit

Gli Auditor che fanno parte del gruppo di Audit preparano i documenti necessari per le attività di Audit, tali documenti sono costituiti da:

- liste di riscontro (Check-List) inerenti alla tipologia ed alle caratteristiche dell'Audit da eseguire;
- moduli di registrazione delle evidenze, e registrazioni dell'Audit.

2.4 Conduzione degli Audit

La conduzione degli Audit è caratterizzata da interviste, esame dei documenti a campione, osservazioni sullo svolgimento delle attività.

Aspetti da prendere in considerazione nel corso degli Audit interni di primo livello sono:

- la conformità ai requisiti legali (cogenti);
- l'efficace e l'efficiente attuazione delle procedure SGSI;
- le opportunità per il miglioramento continuo;
- la capacità dei processi di soddisfare i requisiti delle norme prese a riferimento;
- l'utilizzazione efficace ed efficiente delle misure di processo e di sistema;
- l'utilizzazione efficace ed efficiente di tecnologie informatiche;
- l'efficace ed efficiente utilizzazione delle risorse;
- i risultati e le aspettative sulle prestazioni dei processi e dell'oggetto;
- le attività di miglioramento;
- i rapporti con le parti interessate.

Le attività svolte consistono quindi nella raccolta, esame e valutazione delle informazioni, dei dati e degli eventi. L'Auditor è tenuto a basare le proprie

considerazioni solo su fatti oggettivi, in modo da poter ricostruire con esattezza quanto rilevato.

Dagli Audit interni di primo livello possono emergere le seguenti tipologie di Non Conformità:

- Non-Conformità di categoria 1 (NC1): Anomalie che evidenziano gravi scostamenti e/o gravi carenze di controllo sull'oggetto esaminato, oppure una Non-Conformità di Categoria 2 che risulta persistere nel tempo.
- Non-Conformità di categoria 2 (NC2): Anomalie che evidenziano significativi scostamenti e/o significative carenze di controllo sull'oggetto esaminato, oppure una Osservazione che risulta persistere nel tempo.
- Osservazione (OSS): Anomalie di tipo formale/documentale e/o di tipo operativo.

Le Non Conformità riscontrate sono classificate in base a requisiti:

- normativi;
- di controllo (es. Piano di Trattamento del Rischio, Politiche e/o procedure di sicurezza).

2.5 Chiusura degli Audit

Entro i tempi prestabiliti e comunque nel termine dell'attività di Audit, il Responsabile del Gruppo di Audit espone al Responsabile dell'oggetto sottoposto ad Audit e ad eventuali altri attori coinvolti, le risultanze e le conclusioni dell'Audit, in maniera tale che queste siano conosciute e comprese da parte della Struttura sottoposta ad Audit, e, eventualmente, per convenire il periodo di tempo entro cui il Responsabile dell'oggetto sottoposto ad Audit può attuare le azioni per eliminare le eventuali non conformità individuate.

I risultati dell'Audit effettuato sono riportati nell'apposito modulo "*Rapporto di Audit Interno*" (MGS_SGSI_Rapporto di Audit Interno) a cura dell'Auditor con le seguenti informazioni:

- ambito dell'Audit, indicazione se si tratta di Sistema di gestione della Sicurezza delle informazioni o altri aspetti della sicurezza;
- identificativo dell'Audit;
- responsabile del Gruppo di Audit;
- data dell'esecuzione dell'Audit;
- oggetto dell'Audit;
- responsabile oggetto sottoposto ad Audit;
- struttura sottoposta ad Audit;
- criteri dell'Audit;
- riepilogo dell'Audit.

Eventuali Non Conformità rilevate nel corso dell'Audit vengono registrate da parte dell'Auditor sul modulo *Rapporto di Audit Interno* nel quale, per ogni singola Non Conformità riscontrata, va riportato:

- numero progressivo Non Conformità;
- tipo;
- riferimento;

- azioni da intraprendere.

Per fornire maggiori informazioni sulle Non Conformità si utilizzano i moduli "Segnalazione delle Non Conformità" (MGS_SGSI_Segnalazione Non Conformità), tanti quante sono le non conformità rilevate. Le modalità di compilazione del modulo sono indicate nel documento "Gestione delle non conformità e delle azioni correttive" (PGS_SGSI_Gestione Non Conformità e Azioni Correttive) [3].

Ulteriori informazioni contenute nel modulo Rapporto di Audit Interno sono:

- sintesi Audit;
- data di fine Audit;
- firma del Responsabile del Gruppo di Audit.

L'Audit è completato quando tutte le attività previste dal Piano di Audit sono state attuate e, sia il "Rapporto di Audit di primo livello", sia i moduli di "Segnalazione delle Non Conformità" sono stati consegnati al Gestore SGSI e quindi ai Responsabili delle strutture soggette a Audit.

2.6 Azioni successive agli Audit

Le eventuali Non Conformità vengono gestite in linea con la procedura illustrata nel documento "Gestione delle non conformità e delle azioni correttive" (PGS_SGSI_Gestione Non Conformità e Azioni Correttive) [3].

La Struttura che è stata sottoposta all'Audit, deve assicurare che tutte le azioni, per eliminare le Non Conformità individuate e le loro cause, siano intraprese senza ritardi in relazione al periodo di tempo convenuto.

Le conclusioni dell'Audit possono evidenziare l'esigenza di azioni di miglioramento. Tali azioni sono realizzate dalla Struttura sottoposta ad Audit. Sono pertanto decise ed effettuate nelle modalità e con le tempistiche concordate con il Responsabile del Gruppo di Audit.

La verifica dell'efficacia delle Azioni Correttive messe in atto può essere eseguita anche attraverso un Audit successivo (*Follow up*), secondo le modalità descritte nei paragrafi precedenti. Obiettivo del Follow up è la verifica dell'attuazione e dell'efficacia delle azioni correttive decise.

2.7 Valutazione dei risultati

Il Gestore del SGSI analizza i risultati di Audit, ed in particolare delle non conformità riscontrate, ed utilizza tali risultati come elementi in ingresso nell'ambito del riesame del SGSI.

Nel corso dell'arco temporale a cui si riferisce il Programma di Audit interni di primo livello, viene effettuato un monitoraggio da parte del Gestore del SGSI sulle registrazioni relative agli Audit effettuati, al fine di verificare:

- il rispetto della programmazione e l'efficacia del programma rispetto agli obiettivi prefissati;
- il rispetto della procedura di conduzione degli Audit;
- l'adeguatezza delle registrazioni, intesa come completezza, chiarezza, coerenza;
- l'efficacia delle prassi di conduzione dell'Audit (procedura).

I risultati degli Audit interni di primo livello sono argomento del riesame del SGSI per individuare eventuali azioni di miglioramento da apportare al sistema.

A. Appendice – Linee guida per la qualificazione degli Auditor

La fiducia e l'affidabilità accordata al processo di Audit dipende dalla competenza di coloro che effettuano l'Audit.

Gli Auditor sono scelti dal *Gestore del SGSI*, ovvero in eccezione, da altri soggetti Responsabili dell'audit, titolati a tale scelta. L'attribuzione dell'incarico viene effettuata per iscritto. Tale incarico può essere revocato.

La scelta degli Auditor interni si basa sulle indicazioni, di seguito riportate che abbracciano aspetti di esperienza, di istruzione, di competenza e di caratteristiche personali appartenenti dimostrate all'Auditor.

Competenza generale

Gli Auditor dovrebbero avere almeno il diploma di scuola media superiore.

Esperienza di lavoro

Gli Auditor dovrebbero avere esperienza pluriennale almeno in uno dei seguenti campi:

- pianificazione, analisi e sviluppo del software,
- erogazione di servizi informatici;
- controllo qualità;
- sicurezza delle informazioni.

Esperienza/Formazione specifica

Gli Auditor dovrebbero avere esperienza almeno in uno dei seguenti campi:

- partecipazione a gruppi di lavoro per la definizione di Sistemi di sicurezza;
- partecipazione ad un corso per Lead Auditor sulla Normativa di riferimento, con attestato di frequenza e valutazione finale positiva;
- partecipazione ad un corso per Auditor interno.

Caratteristiche personali

Gli Auditor dovrebbero aver dimostrato le seguenti caratteristiche personali:

- onestà intellettuale;
- capacità di analisi e sintesi;
- capacità ed indipendenza di giudizio;
- resistenza ai condizionamenti psicologici;
- capacità di pianificare e di adeguarsi a realtà complesse;
- capacità di comunicare e d'instaurare buoni rapporti interpersonali;
- capacità di dare la giusta importanza ai contenuti sostanziali ed agli aspetti formali.

B. Appendice - Guida alla compilazione dei moduli di audit

B.1 Guida alla compilazione del modulo Programma di audit

Il modulo viene utilizzato per programmare gli Audit interni di primo livello da eseguire da parte della struttura di SGSI Governance, relativi alle attività inerenti:

- il Sistema di Gestione della Sicurezza delle Informazioni (SGSI);
- aspetti di sicurezza documentati su: Politiche per la Sicurezza delle informazioni, Regolamenti interni, Codice Etico, Manuale della Sicurezza, Procedure, Piani di Sicurezza ecc.

Il Gestore SGSI, compila annualmente il Programma di Audit interni di primo livello sulla base dello stato e dell'importanza dei processi e delle strutture organizzative da sottoporre ad Audit.

Una prima parte del modulo riporta i dati relativi al Programma di Audit interni di primo livello; una seconda parte riporta il dettaglio degli Audit da eseguire. Il modulo può essere aggiornato periodicamente durante l'anno, in funzione degli Audit che si rendono necessari, e anche in relazione agli Audit relativi alla verifica di Azioni Correttive effettuate.

PRIMA PARTE

Anno: indicare l'anno di riferimento del Programma di Audit.

Emittente: SGSI Governance.

N° di Audit previsti: numero totale di Audit previsti nel Programma.

Firma: firma del Compilatore.

Data: indicare la data di compilazione.

SECONDA PARTE

Per ogni Audit previsto:

Identificativo di Audit: numero progressivo dell'Audit.

Processo/Struttura da sottoporre ad Audit: indicare la struttura da sottoporre ad Audit e il relativo responsabile.

Persona da contattare/Responsabile del Processo o struttura da sottoporre ad Audit: riportare in maniera sintetica una descrizione dell'oggetto da sottoporre ad Audit e il responsabile dell'oggetto da sottoporre ad Audit.

Auditor: indicare il nome del Responsabile del Gruppo di Audit (RGA) e Auditor (se presente).

Data prevista: Indicare il mese in cui sarà condotto l'Audit. Inserire, se necessario, una nota per motivare la cancellazione o la ripianificazione dell'Audit specificando la nuova data prevista.

B.2 Guida alla compilazione del modulo di Rapporto di Audit Interno

Il modulo è compilato a cura del Responsabile del Gruppo di Audit, al termine di ogni Audit, al fine di sintetizzare i risultati emersi. Il modulo si compone di due parti. Le informazioni che devono essere riportate sono le seguenti:

PRIMA PARTE

Ambito dell'Audit: indicare se si tratta di Sistema di Gestione della Sicurezza delle Informazioni (SGSI) o altri aspetti di sicurezza.

Identificativo Audit: riportare il numero univoco del singolo Audit.

Responsabile del Gruppo di Audit: indicare il nome del Responsabile incaricato dell'Audit.

Data: indicare la data effettiva in cui l'Audit ha avuto luogo.

Oggetto dell'Audit: riportare in maniera sintetica una descrizione dell'oggetto da sottoporre ad Audit.

Responsabile oggetto sottoposto ad Audit: indicare il nome del Responsabile dell'oggetto sottoposto ad Audit.

Struttura: indicare la Struttura sottoposta ad Audit.

Criteri dell'Audit: indicare le Norme, Leggi, Requisiti, Regolamenti utilizzati come riferimenti rispetto a cui si confrontano le evidenze degli Audit.

Riepilogo Audit: indicare la sintesi dell'Audit, segnalando per ogni Non Conformità riscontrata:

N.C.: numero progressivo della Non Conformità.

Tipo: indicare la tipologia di Non Conformità (NC1, NC2, OSS).

Riferimento: indicare il riferimento in relazione all'Audit seguito, se relativa ai requisiti in generale del SGSI (UNI EN ISO IEC 27001:2014) o specifica su alcuni controlli (es. rispetto delle tempistiche e delle attività indicate Piano di Trattamento del Rischio, rispetto di specifiche Politiche e/o procedure di sicurezza), o altre Normative di riferimento.

Inoltro al Responsabile SGSI: qualora si tratti di una Non Conformità, occorre scrivere "SI". Viceversa il campo viene lasciato in bianco.

Azioni da intraprendere: breve descrizione delle azioni da intraprendere

SECONDA PARTE

Sintesi dell'Audit: riportare una descrizione sintetica di quanto emerso durante l'Audit o fare riferimento all'eventuale verbale da allegare al rapporto.

Fine Audit: apporre la data e la firma del Responsabile del Gruppo di Audit.

Area Innovazione e Servizi Operativi

II DIRETTORE

Marco Balassi

(Firmato digitalmente)