Audit

Cesare Gallotti

Milano, 27 febbraio 2013

Privacy e verifiche

Verifiche al responsabile del trattamento

- Articolo 29, comma 5 del D. Lgs. 196 del 2003:

  Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Verifiche agli Amministratori di sistema

- Articolo 4.4, Provvedimento 27/11/2008 e aggiornato il 25/06/2009:

  L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Domande

- Come interpretare il termine «verifica»?
- Come effettuare le verifiche?

Definizioni e introduzione

Le definizioni base (ISO/IEC 17021)

- Audit: processo sistematico, indipendente e documentato per ottenere registrazioni, affermazioni o fatti o altre informazioni pertinenti e per valutarle con obiettività per determinare in quale misura i criteri specificati sono stati soddisfatti.
  - > Mentre «audit» si applica ai sistemi di gestione, «assessment» si applica alla valutazione di conformità degli organismi di certificazione e in modo più generale.
- Ispezione: esame di un progetto di prodotto, di un prodotto, di un processo di installazione e determinazione della sua conformità rispetto a requisiti specifici o, sulla base di un giudizio professionale, requisiti generali.
  - > L'ispezione di un processo può includere l'ispezione di persone, infrastrutture, tecnologie e metodologie
- Quali differenze?

Tre tipi di audit (ISO 19011)

- Audit interni (audit di prima parte): sono condotti dall'organizzazione stessa per un riesame da parte della Direzione o per altri fini (per esempio per avere conferma dell'efficacia di un sistema di gestione o per ottenere informazioni circa il suo miglioramento).
  - > Gli audit interni possono fornire gli elementi base per un'auto dichiarazione dell'organizzazione.
  - > In molti casi, in particolare nelle piccole organizzazioni, l'indipendenza dell'auditor può essere dimostrata dal suo non coinvolgimento nelle responsabilità dell'attività verificata o dalla mancanza di conflitti di interesse.
- Gli audit esterni includono gli audit di seconda e terza parte.
  - > Gli audit di seconda parte sono condotti da entità che hanno un interesse nell'organizzazione, per esempio i clienti.
  - > Gli audit di terza parte sono condotti da organizzazioni indipendenti, come organismi regolatori o di certificazione.

Criteri di audit

- Criteri di audit: insieme di politiche, procedure o requisiti utilizzati come riferimento per confrontare le evidenze di audit.
- Quali sono i criteri di audit di
  - prima parte (politiche e procedure)
  - seconda parte (requisiti contrattuali)
  - terza parte (standard internazionali, normative, specifiche condivise)

Chi fa cosa

- Committente dell'audit (audit client): Organizzazione o persona che richiede un audit
  - > Il committente può essere l'organizzazione oggetto dell'audit o qualsiasi altra organizzazione che abbia un diritto di richiedere un audit.
- Organizzazione oggetto dell'audit (auditee): Organizzazione sottoposta all'audit.
- Auditor (o valutatore): Persona che ha la competenza per effettuare un audit
- Gruppo di audit (audit team): Uno o più auditor che eseguono un audit
- Un auditor del gruppo di audit è nominato responsabile del gruppo (Lead Auditor).

Conformità e non conformità

- Conformità: soddisfacimento di un requisito
- Non conformità: mancato soddisfacimento di un requisito
- Azione correttiva: azione per eliminare la causa di una non conformità rilevata, o di altre situazioni indesiderabili rilevate.
  - > Una non conformità può dipendere da più cause.
  - > Correzione ed Azione Correttiva hanno significati diversi
- Azione preventiva: Azione per eliminare la causa di una non conformità potenziale o di altre situazioni potenziali indesiderabili.

Principi dell’audit

Comportamento etico

- Il fondamento della professionalità
- Onestà, diligenza, onestà
- Conformità ai requisiti legali
- Dimostrazione della competenza
- Imparzialità

Presentazione imparziale

- L'obbligo di riportare fedelmente e con precisione
- Le risultanze, le conclusioni ed i rapporti di audit riflettono fedelmente ed accuratamente le attività di audit. Vengono riportati gli ostacoli significativi incontrati durante l'audit e le opinioni divergenti non risolte tra il gruppo di audit e l'organizzazione oggetto dell'audit.

Adeguata professionalità

- L'applicazione di accuratezza e di discernimento nell'attività di audit
- Gli auditor pongono un'attenzione di livello adeguato all'importanza del compito che essi svolgono e alla fiducia riposta in loro dai committenti dell'audit e dalle altre parti interessate. È fondamentale che essi posseggano le competenze necessarie.

Riservatezza

- Sicurezza delle informazioni
- Gli auditor sono attenti nell'uso delle informazioni acquisite nel corso delle loro attività.
- Le informazioni acquisite non sono utilizzate non correttamente dagli auditor o dal committente per interessi personali, o comunque in modo che possa danneggiare gli interessi legittimi dell'auditee
- Questo concetto include le modalità di trattamento delle informazioni critiche o riservate

Indipendenza

- La base per l'imparzialità dell'audit e l'obiettività delle sue conclusioni
- Gli auditor sono indipendenti dall'attività oggetto dell'audit e sono liberi da pregiudizi e conflitto d'interesse. Gli auditor conservano uno stato di obiettività di pensiero durante il processo dell'audit per assicurare che le risultanze e le conclusioni dell'audit siano basate solo sulle evidenze dell'audit.

Approccio basato sull'evidenza

- Il metodo razionale per raggiungere conclusioni dell'audit affidabili e riproducibili in un processo dell'audit sistematico
- Le evidenze dell'audit sono verificabili. Esse si basano su campioni di informazioni disponibili, poiché un audit è effettuato in un periodo di tempo limitato e con risorse limitate. L'uso appropriato del campionamento è strettamente connesso con il livello di confidenza che può essere riposto sulle conclusioni dell'audit.

Il programma di audit

Il programma di audit

- Programma di audit (audit programme): Insieme di uno o più audit pianificati per un arco di tempo definito ed orientati verso uno scopo specifico.
  - > Un programma di audit comprende tutte le attività necessarie per pianificare, organizzare ed eseguire gli audit

Estensione di un programma di audit

- Punti da considerare:
  - il campo, l'obiettivo e la durata di ogni audit;
  - la frequenza degli audit;
  - il numero, l'importanza, la complessità, l'analogia e le localizzazioni delle attività da sottoporre ad audit;
  - le norme, le leggi, i requisiti regolamentati e contrattuali ed altri criteri dell'audit;
  - le caratteristiche dei processi, dei prodotti o servizi e dei progetti, il loro livello di maturità e le tecnologie adottate
  - i fornitori critici
  - le conclusioni di precedenti audit, incidenti o reclami;
  - la lingua, gli aspetti culturali e sociali;
  - i rischi delle parti interessate;
  - le modifiche significative dell'organizzazione o delle attività dell'auditee

Il processo di gestione del programma di audit

1. Stabilire le responsabilità per la gestione di un programma di audit
2. definire il programma di audit
3. attuare il programma di audit
4. monitorare e riesaminare il programma di audit
5. migliorare il programma di audit

- Il programma di audit deve permettere di:
  - organizzare le risorse e le persone, considerando il carico di lavoro su uno o più anni;
  - garantire la presenza di auditor adeguatamente competenti;
  - comprendere i criteri di scelta delle aree da verificare e la frequenza degli audit presso quelle aree.

I rischi dell'audit

- Pianificazione: mancata impostazione degli obiettivi
- Risorse: tempo insufficiente per sviluppare il programma o per condurre gli audit
- Selezione del gruppo di audit: inadeguata competenza degli auditor
- Attuazione: inefficace comunicazione del programma
- Registrazioni: mancata sicurezza delle registrazioni e conseguente non dimostrabilità dell'efficacia del programma di audit
- Controllo: inefficace controllo dei risultati del programma di audit
- Sicurezza del personale: non disponibilità di dispositivi di protezione individuale per gli auditor o incompetenza sulle modalità di comportamento in certi ambienti

Attuazione: comunicare all'auditee

- Le seguenti informazioni dovrebbero essere comunicate all'auditee con anticipo (con una procedura):
  - modalità di conduzione delle verifiche
  - modalità di classificazione delle non conformità
  - modalità di trattamento delle non conformità
  - modalità di emissione del rapporto
  - gestione dei fornitori dell'auditee
  - canali di comunicazione con il responsabile del programma dell'audit e con il committente dell'audit
  - modalità di contestazione
  - dichiarazione di riservatezza

Attuazione: le registrazioni

- Le registrazioni relative ai singoli audit, quali
  - i piani dell'audit,
  - i rapporti di audit,
  - i rapporti di non conformità,
  - i rapporti di azioni correttive e preventive,
  - i rapporti di azioni successive all'audit, se applicabili;
- i risultati del riesame del programma di audit;
- le registrazioni relative al personale coinvolto nell'audit:
  - la valutazione delle competenze e delle prestazioni dell'auditor,
  - la composizione del gruppo di audit,
  - il mantenimento ed il miglioramento delle competenze.
- Le registrazioni dovrebbero essere conservate e controllate con adeguata sicurezza.

Nota sul programma

- Il programma di audit non deve prevedere la verifica completa di tutte le attività dell'organizzazione in tempi brevi.
- In molti casi, il programma potrebbe o dovrebbe essere strutturato in modo da verificare tutte le aree (attività, processi, sedi) in un certo numero di anni (per esempio 3 o 5).
  - esempio: se le sedi sono 10, è possibile organizzare un programma triennale che prevede la verifica della sede centrale ogni anno e di altre 3 sedi periferiche all'anno)
- Le aree più critiche dovrebbero essere verificate almeno una volta all'anno.
- Alcune aree potrebbero non essere mai verificate (per esempio, alcuni fornitori o alcune sedi di sola rappresentanza)

In pratica

- Al termine di ogni audit (e, preferibilmente, anche con anticipo), bisogna:
  - verificare se il piano di audit è stato eseguito correttamente
  - gli auditor e gli esperti hanno dimostrato le competenze necessarie per condurre le attività loro assegnate
  - lasciare note per la pianificazione dell'audit successivo
    - tempi per condurre ogni attività
    - aspetti non adeguatamente verificati
    - progetti in corso
  - riesaminare i metodi e le tecniche utilizzate
- E' molto utile:
  - elaborare (o rielaborare) una pianificazione di massima per gli audit successivi
  - conservare un organigramma e le relazioni tra processi e funzioni dell'organizzazione

Un esempio di programmazione biennale

AREA	2014	2015	2016	Criteri
Fornitori				
Fornitore hosting – Milano	3 gu			Contratto
Fornitore hosting SAP – Roma		3 gu		
...				
Responsabili interni				
Area HR	2 gu			Procedura HR 01
Area clienti back office	2 gu			Procedura BO
Area clienti front office		3 gu		Procedura Gestione chiamate
...				
Amministratori di sistema				
AdS Windows	0,5 gu	2 gu		
AdS Unix	2 gu	0,5 gu		
AdS SQL Server	0,5 gu	2 gu		
AdS Oracle	2 gu	0,5 gu		
...				
TOT GIORNATE	12 gu	11 gu		

Attività di audit

Il piano dell’audit (1/4)

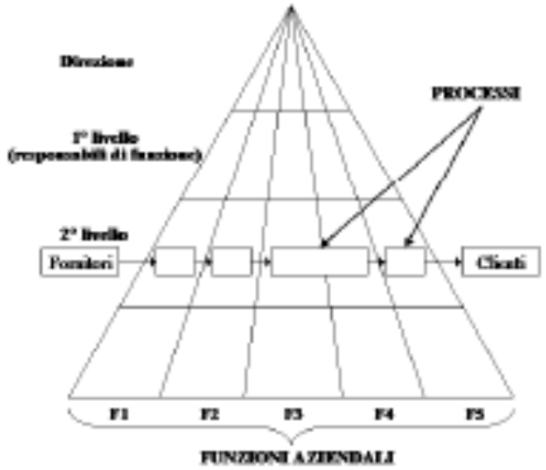
- Piano dell'audit (audit plan): Descrizione delle attività e delle disposizioni per la conduzione di un audit
- Il piano dell'audit dovrebbe essere sufficientemente flessibile da permettere modifiche, quali variazioni nel campo dell'audit, che possano diventare necessarie man mano che progrediscono le attività di audit.
- Il piano dell'audit dovrebbe comprendere quanto segue:
  - gli obiettivi dell'audit;
  - i criteri dell'audit e tutti i documenti di riferimento;
  - il campo dell'audit, compresa l'identificazione delle unità organizzative e funzionali e dei processi da sottoporre ad audit;
  - le date ed i luoghi ove si devono attuare le attività di audit sul posto;
  - la stima del tempo e della durata per le attività
  - i ruoli e le responsabilità dei membri del gruppo di audit e degli accompagnatori;
  - la lingua utilizzata nelle attività e nei rapporti di audit
  - le indicazioni per la logistica (spostamenti, sistemazioni sul posto, ecc.).

Il piano dell’audit (2/4)

- Il piano dovrebbe essere riesaminato ed accettato dal committente dell'audit e presentato all‘auditee prima (almeno 2 settimane, anche 3 mesi) che inizino le attività di audit sul posto:
  - per rispetto verso le persone da coinvolgere (auditee)
  - per rispettare i tempi (gli auditor devono chiudere un’intervista nei tempi previsti)
  - per la logistica (es. prenotazione biglietti e hotel)
  - per confermare la completezza dell’audit
- Il responsabile del gruppo di audit dovrebbe
  - assegnare a ciascun auditor specifici processi o attività
  - tener conto delle esigenze di indipendenza e di competenza
  - tener conto di un'utilizzazione efficiente delle risorse
- Man mano che l'audit progredisce possono essere effettuate delle modifiche alla assegnazione dei compiti.

Il piano dell'audit (3/4)

- Nota 1: Ricordarsi della riunione di apertura, del tempo di preparazione del rapporto e della riunione di chiusura (anche di ciascun giorno).
- Nota 2: è bene preparare il piano di audit con la collaborazione dei rappresentanti dell'auditee:
  - > si conferma la corretta comprensione dell'organizzazione da parte dell'auditor
  - > l'auditor non deve conservare organigrammi o altri documenti dell'auditee
- Nota 3: fare attenzione a come è realmente strutturata un'organizzazione
  - > per processi
  - > per funzioni



Il piano dell’audit (4/4)

Orario	Area
09:00-09:30	Riunione di Apertura
09.30 – 11.00	Analisi sicurezza fisica
11.00 - 13.00	Analisi controllo accessi
13.00 – 14.00	Pausa Pranzo
14.00 - 15.30	Analisi backup
15.30 - 17.00	Antivirus, eccetera
17.00 – 17.30	Riunione Gruppo di Verifica
17.30 - 18.00	Riunione di Chiusura

Documenti di lavoro

- Tali documenti di lavoro possono comprendere
  - > liste di riscontro e piani di campionamento dell'audit;
  - > moduli per registrare le informazioni
- L'utilizzazione di liste di riscontro e di moduli non dovrebbe limitare l'estensione delle attività di audit
- I documenti di lavoro dovrebbero essere conservati almeno fino al termine dell'audit.

Riunione di apertura

- Il Lead Auditor presiede la riunione di apertura:
  - presentazione dei partecipanti e dei loro ruoli;
  - la conferma degli obiettivi, dell'estensione e dei criteri di esecuzione dell'audit;
  - conferma del piano e della logistica;
  - i metodi e le procedure da utilizzare per condurre l'audit;
  - la conferma di canali di comunicazione formale fra il gruppo di audit e auditee
  - la conferma della lingua da utilizzare durante l'audit;
  - la conferma che, durante l'audit, l'auditee sarà tenuto informato del progresso
  - la conferma che siano disponibili le risorse e quanto necessario al gruppo di audit;
  - la conferma, per il gruppo di audit, di idonee condizioni di sicurezza sul lavoro,
  - la conferma della disponibilità, dei ruoli e dell'identità di eventuali guide;
  - il metodo di preparazione dei rapporti, comprese le eventuali classificazioni delle non conformità;
  - le informazioni riguardanti eventuali modalità di ricorso sulla conduzione o sulle conclusioni dell'audit.

Comunicazione durante l'audit

- Il gruppo di audit dovrebbe consultarsi periodicamente per scambiarsi informazioni, valutare il progresso dell'audit e riassegnare compiti tra gli auditor, se necessario.
- Durante l'audit, il responsabile del gruppo di audit dovrebbe comunicare periodicamente il progredire dell'audit ed eventuali problemi.
- Ove le evidenze dell'audit disponibili indichino che gli obiettivi dell'audit sono irraggiungibili, il responsabile del gruppo di audit dovrebbe riportarle al committente dell'audit ed all'auditee.

Raccolta e verifica informazioni (1/3)

- Interviste con impiegati e con altre persone;
- Osservazione delle attività e delle condizioni e dell'ambiente di lavoro;
- Documenti, quali politica, obiettivi, piani, procedure, norme, istruzioni, licenze e permessi, specifiche, disegni, contratti ed ordini;
- Registrazioni, come registrazioni di ispezioni, resoconti di riunioni, rapporti di audit, registrazioni di programmi di controllo e risultati di misurazioni;
- Riassunti di dati, analisi ed indicatori di prestazioni;
- Informazioni sui programmi di campionamento pertinenti dell'organizzazione oggetto dell'audit e sulle procedure per il controllo del campionamento e dei processi di misurazione;
- Rapporti da altre fonti, per esempio, informazioni di ritorno dal cliente, altre informazioni pertinenti da parti esterne e valutazioni di fornitori;
- Banche dati di computer esiti web.

Raccolta e verifica informazioni (2/3)

- Chiedere (vedere oltre)
- Osservare (che cosa succede nei reparti)
- Verificare (le dichiarazioni attraverso la documentazione)
  - > evitare di basare gli audit su interviste senza analizzare documenti o registrazioni (anche via IT)
  - > non rifiutare la documentazione in formato elettronico
  - > non pretendere firme olografe se non quando necessario
- Prendere nota (rispetto a cose osservate, per poter chiedere chiarimenti ad altre funzioni).
  - > non tutto può essere spiegato dall'intervistato (per esempio, un operatore dell'Ufficio Personale non potrà necessariamente spiegare perché sul suo pc non è installato un antivirus!)
  - > non tutto può o deve essere verificato dal responsabile (per verificare la presenza degli antivirus sui pc, non è sufficiente chiedere al responsabile IT)!

Raccolta e verifica informazioni (3/3)

- Per le interviste, considerare quanto segue:
  - le interviste dovrebbero essere rivolte a persone di opportuni livelli e funzioni che eseguono attività o compiti nell'ambito del campo dell'audit;
  - le interviste dovrebbero essere condotte durante l'orario normale di lavoro e, ove possibile, sul luogo di lavoro abituale della persona intervistata;
  - dovrebbe essere fatto ogni sforzo per mettere la persona che viene intervistata a proprio agio prima e durante l'intervista;
  - dovrebbero essere spiegate le ragioni dell'intervista e di ogni annotazione presa;
  - le interviste possono essere iniziate con la richiesta alle persone di descrivere il loro lavoro;
  - dovrebbero essere evitate le domande che possono influenzare le risposte (cioè le domande influenzanti) o le domande chiuse (sì/no);
  - non imporre o rifiutare una terminologia
  - i risultati delle interviste dovrebbero essere sintetizzati e riesaminati con la persona intervistata;
  - le persone intervistate dovrebbero essere ringraziate per la loro partecipazione e per la loro cooperazione.

Risultanze dell'audit (1/2)

- Ciò che è stato posto in evidenza dall'audit dovrebbe essere valutato a fronte dei relativi criteri per dar luogo alle risultanze dell'audit
- Classificazione
  - > Non conformità (vari livelli)
  - > Conformità
  - > Opportunità di miglioramento
- Le non conformtià dovrebbero essere riesaminate con l'organizzazione oggetto dell'audit.

Risultanze dell'audit (2/2)

- Le non conformità vanno descritte con:
  - evidenza
  - requisito
  - mancanza
- Esempi:
  - «Contrariamente a quanto previsto dal contratto stipulato in data xxx (requisito), si è verificato che non è disponibile uno strumento per la cancellazione sicura dei supporti di memorizzazione (evidenza + mancanza)»
  - «Contrariamente a quanto previsto dal contratto stipulato in data xxx (requisito), per la cancellazione sicura dei supporti di memorizzazione è utilizzata la formattazione (evidenza) e non uno strumento di sanitizzazione (mancanza)»

Esempio

- Procedura BKP1: “Per ogni sistema informatico, devono essere effettuati dei backup completi almeno una volta alla settimana”.
- Situazione sistemi:
  - sistema A: backup completo effettuato ogni sabato;
  - sistema B: backup completo effettuato ogni giorno;
  - sistema C: backup completo effettuato ogni 30 giorni;
  - sistema D: backup completo effettuato ogni domenica.
- C’è una non conformità?
  - Come scriverla?

Riunione di chiusura

- Al termine dell'audit, deve essere tenuta una riunione di chiusura, presieduta dal Lead Auditor, per
  - > presentare le risultanze e le conclusioni dell'audit in maniera tale che queste siano conosciute e comprese da parte dell'auditee
  - > concordare il periodo di tempo per presentare un piano di azioni correttive e preventive.

Rapporto di audit

- Il Lead Auditor ha la responsabilità della preparazione del rapporto di audit.
- Il rapporto di audit dovrebbe comprendere o far riferimento a:
  - gli obiettivi dell'audit;
  - il campo dell'audit;
  - l'identificazione del committente dell'audit;
  - l'identificazione del responsabile e dei membri del gruppo di audit;
  - le date e i luoghi dove sono state eseguite le attività di audit;
  - i criteri dell'audit;
  - le risultanze dell'audit;
  - le conclusioni dell'audit
  - il piano dell'audit;
  - l'elenco dei rappresentanti dell'auditee;
  - una sintesi del processo dell'audit;
  - eventuali aree non coperte, sebbene rientranti nel campo dell'audit;
  - eventuali opinioni divergenti non risolte tra il gruppo di audit e l'auditee;
  - i piani concordati delle azioni successive;
  - una dichiarazione sulla riservatezza dei contenuti;
  - la lista di distribuzione del rapporto di audit.

Chiusura dell'audit

- L’audit è completato quando tutte le attività descritte nel piano dell'audit sono state attuate ed il rapporto di audit approvato è stato distribuito.
- I documenti riguardanti l'audit dovrebbero essere conservati o distrutti a seguito di accordi fra le parti partecipanti e secondo le procedure del programma di audit.
- A meno che non sia richiesto per legge, il gruppo di audit ed i responsabili della gestione del programma di audit non dovrebbero divulgare i contenuti dei documenti, né eventuali altre informazioni raccolte nel corso dell'audit.
- Se è richiesta la divulgazione dei contenuti di un documento dell'audit, il committente dell'audit e l'organizzazione oggetto dell'audit dovrebbero esserne informati al più presto possibile.

Attuazione delle azioni successive

- Le conclusioni dell'audit possono indicare l'esigenza di azioni correttive, preventive e, se applicabile, di miglioramento.
- Tali azioni sono generalmente decise ed effettuate dall'organizzazione oggetto dell'audit secondo tempistiche concordate e non sono considerate come facenti parte dell'audit.
- Il completamento e l'efficacia delle azioni correttive dovrebbero essere verificati. Questa verifica può costituire oggetto di un audit successivo oppure di un audit straordinario (per esempio, in caso di NC gravi, se previsto dal regolamento condiviso)
- Il programma di audit può specificare azioni successive da parte dei membri del gruppo di audit, che sono considerati valore aggiunto in quanto utilizzano la loro competenza. In tali casi, dovrebbe essere prestata attenzione per mantenere l'indipendenza in successive attività di audit.

Grazie!

- Cesare Gallotti
  cesaregallotti@cesaregallotti.it
  PEC: cesaregallotti@mailcert.it
  http://www.cesaregallotti.it
  http://blog.cesaregallotti.it