MANAGEMENT

Audit e GDPR

Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)

NUOVA EDIZIONE

Giancarlo Butti, Maria Roberta Perugini

FRANCOANGELI

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

Am - La prima collana di management in Italia

Testi advanced, approfonditi e originali, sulle esperienze più innovative
in tutte le aree della consulenza manageriale,
organizzativa, strategica, di marketing, di comunicazione,
per la pubblica amministrazione, il non profit...

Giancarlo Butti,
Maria Roberta Perugini

Audit e GDPR

Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)

NUOVA EDIZIONE

FRANCOANGELI

Isbn: 9788835157939

A Bob (Penna Bianca)

A Carlo, che ha saputo unire genialità,
simpatia e altruismo

A mia moglie
Alle mie bimbe (Lara, Hope, Chery)
e ai miei bimbi (River, Book, Eros)
Giancarlo

Indice

Introduzione

Dopo oltre un anno dall'entrata in vigore del GDPR (Regolamento (UE) 2016/679)[1] e del relativo adeguamento della normativa italiana sulla protezione dei dati personali, si deve affrontare il tema delle verifiche:

- delle azioni intraprese al fine di garantire la conformità alla normativa;
- del fatto che le policy, le procedure, le misure di sicurezza definite, siano effettivamente implementate e rispettate.

Gli attori coinvolti in tali attività sono:

- il titolare, *cioè la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali...*;
- il responsabile, *cioè la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*;
- il DPO *(Data Protection Officer – Responsabili della protezione dei dati personali), designato ai sensi degli artt. 37-39 del GDPR*.

Le attività di verifica sono svolte di norma da auditor professionisti, siano essi interni o esterni all'azienda, risorse particolamente specializzate e rare.

Nondimeno il compito di sorvegliare il rispetto della normativa è un obbligo dei DPO, che nella maggior parte dei casi si trova ad affrontare questa attività per la prima volta e non dispone, di norma, di adeguati strumenti e competenze per svolgerla.

1. 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).

Ecco quindi l'idea di questo libro, il cui obiettivo di è quello di consentire:

- sia ad "auditor" professionisti, sia a soggetti che conoscono la normativa privacy, ma che hanno poca dimestichezza con le attività di verifica di:
  - svolgere un assessment in ambito privacy;
  - definire un piano di audit;
  - definire un programma di audit;
  - creare check list;
  - raccogliere evidenze;
  - valutare le risultanze dell'audit;
  - stilare un verbale di audit;
  - …

  al fine di verificare il livello di conformità della organizzazione sottoposta a verifica;
- ai titolari e responsabili, di saper valutare:
  - quali tipi di verifica meglio siano rispondenti alle loro esigenze;
  - le offerte su attività di verifica, distinguendo in particolare fra quelle che si limitano a considerare gli aspetti formali da quelle che effettuano un riscontro oggettivo su come opera l'organizzazione.

Il libro inoltre, anche se limitatamente ai casi trattati, fornisce dettagli sulle implementazioni richieste per garantire la conformità alla normativa.

Gli autori, un auditor professionista con competenze in ambito ICT, organizzativo, legale ed un avvocato con oltre 25 anni di esperienza in ambito privacy, sviluppano i vari temi legati alle verifiche in ambito privacy nelle due parti in cui è organizzato il testo.

Nella prima parte viene affrontato il tema di come impostare un'attività di verifica in generale e più specificatamente in ambito organizzativo e tecnico, mentre nella seconda parte vengono affrontati temi prettamente legali.

Molti degli esempi sono tratti dai miei articoli su Toolnews, e di questo ringrazio Alessandro Giacchino. Un ringraziamento particolare al prof. Fabio Maccaferri, per il suo contributo sul rischio di audit.

Gli eventuali testi delle normative e di altri documenti riportati nel libro hanno solo finalità indicativa e non hanno alcun valore ufficiale.

Gli unici testi ufficiali delle normative sono quelli pubblicati sulla Gazzetta Ufficiale della Repubblica Italiana e Gazzetta Ufficiale dell'Unione Europea che prevalgono in caso di discordanza.

Grazie anche a Leonardo, il Nasci, Deborah e Mario, attenti lettori e suggeritori e soprattutto a Francesca, che ha da subito creduto in quest'opera.

Parte prima

di *Giancarlo Butti*

1 Le verifiche in ambito privacy

Si è volutamente utilizzato il termine verifiche e non audit in quanto non tutte le verifiche sono necessariamente strutturate sotto forma di audit; la normativa privacy, infatti, non prescrive alcuna regola in merito alle modalità con cui effettuare le verifiche.

Spetta quindi al singolo titolare o responsabile del trattamento di dati personali (nel seguito per semplificare si utilizzerà solo il termine titolare anche se quanto esposto riguarda sia i titolari, sia i responsabili, salvo che diversamente specificato) determinare quali siano le modalità con cui vuole effettuare delle verifiche.

Analoga responsabilità investe il DPO, che fra i suoi compiti deve:

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

Nel complesso le attività di verifica possono riguardare:

- l'autovalutazione della conformità agli adempimenti prevista dalla normativa effettuati dal titolare tramite strutture interne (audit/compliance) o esterne;
- la valutazione della conformità agli adempimenti prevista dalla normativa effettuati dal DPO anche per il tramite di strutture interne (audit/compliance) o esterne;
- la valutazione effettuata da un titolare sugli adempimenti contrattuali del responsabile;
- la valutazione effettuata da un titolare sugli adempimenti messi realmente in atto dal DPO, rispetto a quanto formalizzato nel suo atto di designazione;
- la valutazione effettuata da un titolare sulle caratteristiche di un DPO, rispetto a quanto previsto dalla normativa.

Le attività di verifica non sono codificate in modo puntuale nella normativa e quindi possono essere svolte con una certa libertà di metodo; è tuttavia consigliabile, nel caso si svolgano attività classificabili come audit, utilizzare linee guida e standard codificati da associazioni di settore riconosciute o da organismi di normazione.

Le verifiche possono essere classificate come:

- assessment di carattere generale;
- ricognizioni che portino a formulare suggerimenti in luogo di rilievi[1];
- audit veri e propri;
- verifiche di carattere tecnico;
- verifiche nell'ambito della sicurezza tramite vulnerability assessment e penetration test;

e possono variare in funzione del perimetro sottoposta a verifica:

- processi;
- requisiti normativi;
- …

e della profondità:

- verifiche dei soli aspetti formali (verifica di impianto);
- verifiche della reale operatività messa in atto dall'organizzazione sottoposta a verifica (verifica di funzionamento).

1. Chi effettua le verifiche

L'attività di verifica può essere svolta da personale interno o esterno alla struttura verificata, purché tale personale:

- abbia le necessarie competenze tecnico/giuridiche e conosca i processi ed i trattamenti in essere presso la struttura da verificare;
- non operi in conflitto di interessi, andando a verificare processi o ambiti nei quali è intervenuto lui stesso in fase di implementazione;
- sia adeguatamente supportato nella sua attività di verifica;
- non debba verificare, se interno, una struttura dalla quale dipende gerarchicamente;
- non subisca delle ritorsioni in conseguenza delle sue attività di verifica.

Leggendo queste indicazioni non può mancare un accostamento alle analoghe caratteristiche che deve avere un DPO, ed in effetti la figura del DPO e quella dell'auditor hanno diversi punti in comune.

1. Con il termine rilievo in questo libro si intende il dare evidenza di una differenza fra quanto si è riscontrato in sede di verifica e quanto ci si attendeva.

Nel caso in cui esista un DPO le attività di verifica possono essere svolte direttamente da lui medesimo, in quanto compiere verifiche come abbiamo visto sopra è uno dei suoi compiti (la capacità di svolgere attività di verifica è una delle competenze che il DPO deve possedere).

Nondimeno un titolare potrebbe non avere l'obbligo di designare un DPO, ma disporre di strutture interne dedicate alle attività di verifica.

Tale situazione si presenta comunque molto raramente e riguarda strutture molto grandi e nella maggior parte dei casi specificatamente regolamentate in questo ambito.

Un ottimo esempio di questo caso è l'ambito bancario (dove è anche obbligatoria la presenza di un DPO), che utilizzeremo più volte nel corso del testo.

Non può svolgere attività di verifica un consulente o un'azienda di consulenza che abbia partecipato all'attività di implementazione del modello privacy dell'organizzazione.

Vi sarebbe altrimenti un palese conflitto di interessi.

Nel caso in cui l'attività sia svolta da parte di una società di consulenza, vi è conflitto di interessi anche nel caso in cui chi svolge le attività di verifica sia una persona che non ha partecipato alle attività di consulenza (si troverebbe nella scomoda posizione di dover valutare l'operato dei colleghi).

Un comportamento difforme da qunto appena descritto:

- è eticamente scorretto;
- pone dei rischi per la conformità del titolare, che deve essere in grado di dimostrare il motivo delle sue scelte;
- pone dei rischi operativi per il titolare, in quanto difficilmente chi ha implementato un modello privacy secondo i propri criteri ne evidenzierà i limiti in sede di verifica.

2. Le caratteristiche di chi svolge le verifiche

Vari istituti, tra cui, *in primis*, The Institute of Internal Auditors e ISACA, hanno emesso delle linee guida e degli standard per lo svolgimento delle attività di audit e indicato le caratteristiche che devono avere i soggetti che svolgono tale attività[2].

Ad esempio gli Standard Internazionali dell'Internal Auditing e le Guide Interpretative per la Pratica Professionale, la cui traduzione italiana è curata dall'AIIA (Associazione Italiana Internal Auditor) elenca i seguenti standard di connotazione:

1100 – Indipendenza e Obiettività;

2. Per approfondimenti su questo tema e sugli standard relativi alle attività di audit si rimanda alle pubblicazioni delle citate istituzioni.

1110 – Indipendenza Organizzativa;
1120 – Obiettività Individuale;
1130 – Condizionamenti pregiudizievoli all'Indipendenza e all'Obiettività
1200 – Competenza e Diligenza professionale;
1210 – Competenze;
1220 – Diligenza Professionale;
1230 – Aggiornamento Professionale Continuo;

In particolare la **Guida Interpretativa 1210-1 Competenze** recita:

Gli internal auditor devono possedere le conoscenze, capacità e competenze necessarie all'adempimento delle loro responsabilità individuali.

L'attività di Internal Auditing nel suo insieme deve possedere o procurarsi tutte le conoscenze, capacità e competenze necessarie all'adempimento delle sue responsabilità.

1. Ciascun Internal Auditor deve possedere determinate conoscenze, competenze e capacità. In particolare:

- *padronanza nell'applicazione di standard, procedure e tecniche di Internal Auditing è richiesta a tutti. Padronanza significa la capacità di gestire problemi di normale entità, senza prevalente ricorso al supporto e all'assistenza specialistica;*
- *padronanza in materia di principi e tecniche contabili è richiesta agli auditor impegnati nella verifica di scritture e rendiconti finanziari;*
- *conoscenza dei principi di management è richiesta a tutti, per poter riconoscere l'esistenza e valutare l'entità di deviazioni dalle regole della sana gestione. Conoscenza significa la capacità di utilizzare, in specifiche situazioni reali, il proprio bagaglio professionale per identificare deviazioni significative ed effettuare le necessarie ricerche al fine di pervenire a soluzioni accettabili;*
- *cognizioni di base di contabilità, economia, diritto commerciale, legislazione fiscale, finanza, analisi quantitative e sistemi informativi costituiscono infine il bagaglio dell'internal auditor. Cognizione di base significa la capacità di percepire la presenza di problemi e di determinare la necessità di ulteriori approfondimenti o l'assistenza da richiedere.*

2. Gli internal auditor devono possedere capacità di relazione e saper comunicare efficacemente. Devono comprendere le relazioni interpersonali e mantenere buoni rapporti con le loro controparti.

3. Gli internal auditor devono avere una buona capacità di esposizione sia in forma scritta sia orale, così da poter comunicare chiaramente ed efficacemente obiettivi, valutazioni, conclusioni e raccomandazioni.

4. Il responsabile Internal Auditing deve definire i requisiti di preparazione ed esperienza necessari per ricoprire le diverse posizioni, tenendo conto della complessità del lavoro e del livello di responsabilità. Il livello di formazione e competenza di ciascuna persona da inserire nell'Internal Auditing deve essere ragionevolmente verificato.

5. L'organico dell'Internal Auditing deve collettivamente possedere le conoscenze e le capacità necessarie all'esercizio della pratica professionale in seno all'organizzazione.

Annualmente è necessario svolgere un esame delle conoscenze e delle capacità presenti per individuare aree di opportunità sulle quali indirizzare l'Aggiornamento Professionale Continuo, l'attività di selezione o il ricorso a fornitori di servizi esterni.

6. L'Aggiornamento Professionale Continuo è fondamentale per garantire il mantenimento di un'elevata competenza professionale. Per i dettagli relativi all'Aggiornamento Professionale Continuo, consultare la Guida Interpretativa 1230-1.

7. Al fine di supportare e integrare le aree dove le competenze dello staff risultano non interamente adeguate, il responsabile Internal Auditing deve ottenere assistenza da esperti esterni alla funzione Internal Auditing.

Per maggiori dettagli relativi all'acquisizione di servizi a supporto e integrazione dell'Internal Auditing, consultare la Guida Interpretativa 1210.A1-1.

3. Le qualifiche del personale che effettua le verifiche

Le verifiche inerenti alla privacy riguardano diversi aspetti: dal semplice riscontro formale tra quanto richiesto dalla normativa e quanto riportato in un documento redatto dal titolare (come, ad esempio, una informativa) alla dettagliata analisi delle implementazioni tecniche messe in atto per garantire la cancellazione dei dati personali al termine del relativo periodo di conservazione.

Le competenze dei soggetti che svolgono le verifiche (difficilmente una sola figura è in grado di svolgere verifiche sia in ambito normativo, sia in ambito tecnologico) possono trovare un riconoscimento in una o più attestazioni/qualificazioni/certificazioni professionali, che in molti casi possono essere conseguite solo dopo anni di comprovata esperienza nel ruolo e da un esame a volte preceduto obbligatoriamente da un corso.

Inoltre il mantenimento della certificazione è condizionato da un sistema di crediti formativi che testimoniamo l'obbligo di aggiornamento continuo da parte dei soggetti certificati.

Questo ad ulteriore garanzia del committente.

Al riguardo è utile considerare soprattutto le certificazioni di auditor (rilasciate in particolare dal The Institute of Internal Auditors), che comprendono CIA, CCSA, CFSA, CRMA, o quelle di ICT Auditor (rilasciate in particolare da ISACA, associazione internazionale degli IT Auditor) che comprendono CISA, CISM, CRISC, CGEIT.

Specificatamente in ambito privacy vanno inoltre considerate le certificazioni rilasciate dalla IAPP (International Association of Privacy Professionals), anche se non specificatamente dedicate all'attività di audit.

Esistono inoltre numerose certificazioni nell'ambito dei sistemi di gestione della sicurezza (Lead auditor ISO/IEC 27001, Lead auditor ISO 22301 Business continuity management, Lead auditor ISO/IEC 20000-1, CBCI, AMBCI, SBCI, MBCI, FBCI ecc.) e nell'ambito tecnico/organizzativo legato alla sicurezza (CISSP, OPSA, CHFI ecc.).

Tali certificazioni, salvo quelle nelle quali è distintamente indicato il termine auditor, qualificano delle competenze, ma non necessariamente la capacità di svolgere attività di verifica in modo autonomo.

Tuttavia tali figure esperte possono essere impiegate nel team di verifica in particolare là dove solo figure altamente qualificate possono svolgere adeguatamente l'attività.

Competenze specifiche nell'ambito delle verifiche della privacy sono inoltre presenti ad esempio dalla norma UNI 11697, di recente istituzione, relativa alle figure Professionali Privacy.

La norma prevede quattro diverse figure certificabili in ambito privacy, fra le quali quella specifica del Valutatore privacy, e quella del DPO, che come più sopra ricordato, comprende fra le sue capacità anche quella di svolgere delle attività di verifica.

Al riguardo è anche disponibile la certificazione della Autorità Garante spagnola (AEPD) che comprende nelle competenze richieste per ottenere la certificazione la capacità di:

- Data protection audits;
- Information Systems Audit;

oltre che:

- Analysis and management of personal data processing risks;
- Risk analysis and management methodologies;
- Information security;
- Data Protection Impact Assessment "DPIA".

Analoga certificazione è stata proposta dall'Autorità Garante francese (CNIL) anche se non sono così dettagliatamente espresse le competenze richieste nell'ambito delle verifiche.

Tutte queste certificazioni (al di là del fatto che chi sia certificato svolga effettivamente un'attività di audit), qualificano le competenze professionali di chi ne è in possesso, e quindi sono uno strumento di valutazione utile alle aziende per la selezione sia di eventuali fornitori, sia di potenziali candidati.

4. Le strutture che effettuano le verifiche

Le organizzazioni sono spesso dotate di strutture il cui compito è quello di effettuare dei controlli sul corretto operato dell'organizzazione stessa.

In alcuni casi tali strutture sono volontarie (come gli Organismi di Vigilanza ai sensi della legge 231/2001) in altri sono obbligatorie (come il Collegio Sindacale in alcune categorie di aziende, o l'audit e la Compliance nelle banche).

Sebbene nessuna di queste strutture sia specificatamente dedicata a svolgere attività di verifica in ambito privacy è opportuno che l'insieme delle strutture di controllo si coordino fra loro per garantire un presidio anche su questa tematica ed evitare inutili sovrapposizioni.

Va inoltre ricordato che le strutture di controllo la cui titolarità dei trattamenti è in carico al titolare, quali l'audit o la Compliance, trattano un rilevante numero di dati personali, molto spesso dati particolari. Potrebbero quindi essere oggetto di verifica su tali trattamenti da parte del DPO.

Altre strutture, come gli OdV, presidiano dei reati quali quelli informatici, che hanno in parte una sovrapposizione con i requisiti di sicurezza richiesta dalla normativa privacy e quindi, anche in questo caso, è opportuno un coordinamento. Analoghe tematiche privacy si pongono nella gestione dei controlli messi in atto per garantire il presidio del modello organizzativo che l'organizzazione si è data ai sensi della citata legge 231/2001.

5. Il sistema dei controlli interni

Come indicato in precedenza è possibile utilizzare il modello dei controlli interni che la normativa impone alle banche al fine di organizzare il proprio.

L'uso di altre normative emesse da enti autorevoli, di standard emessi da enti di certificazione, di documenti prodotti da una delle Autorità Garanti è una tecnica che in questo libro verrà ripresa più volte.

Là dove la normativa privacy non specifica dettagliatamente i comportamenti che devono essere messi in atto dal titolare per essere conforme, l'uso di metodi e modelli emessi da enti autorevoli è ampiamente consigliabile rispetto all'uso di metodi auto prodotti o suggeriti da qualche consulente anche qualificato.

La Circolare 285 di Banca d'Italia, che è liberamente consultabile sul sito della stessa, costituisce un'ottima guida alla costruzione di un adeguato sistema di controlli interni, adottabile come punto di riferimento dalle aziende di una certa dimensione e complessità.

La Circolare definisce come:

- *"funzioni di controllo": l'insieme delle funzioni che per disposizione legislativa, regolamentare, statutaria o di autoregolamentazione hanno compiti di controllo;*
- *"funzioni aziendali di controllo": la funzione di conformità alle norme (compliance), la funzione di controllo dei rischi (risk management function) e la funzione di revisione interna (internal audit).*

La Circolare declina nel dettaglio quelli che sono l'architettura ed i compiti di un sistema di controllo interno:

Il sistema dei controlli interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- *verifica dell'attuazione delle strategie e delle politiche aziendali;*
- *contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (Risk Appetite Framework – RAF);*
- *salvaguardia del valore delle attività e protezione dalle perdite;*
- *efficacia ed efficienza dei processi aziendali;*
- *affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;*
- *prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo);*
- *conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.*

L'approccio basato sul rischio suggerito dalla Circolare è analogo, per altro, a quello del GDPR e, a parte alcuni temi specifici del mondo bancario quali usura o riciclaggio, è applicabile a tutte le organizzazioni.

Per ottenere i risultati desiderati il sistema dei controlli interni proposto deve:

- *assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia), l'affidabilità del processo di gestione dei rischi e la sua coerenza con il RAF;*
- *prevedere attività di controllo diffuse a ogni segmento operativo e livello gerarchico;*
- *garantire che le anomalie riscontrate siano tempestivamente portate a conoscenza di livelli appropriati dell'impresa (agli organi aziendali, se significative) in grado di attivare tempestivamente gli opportuni interventi correttivi;*
- *incorporare specifiche procedure per far fronte all'eventuale violazione di limiti operativi.*

Oltre alla funzione di audit (revisione interna) Banca d'Italia declina strutture di controllo specialistiche e definisce una gerarchia nei controlli:

- di primo livello – controlli di linea;
- di secondo livello – controlli sui rischi (Risk) e sulla conformità (Compliance);
- di terzo livello – revisione interna (Audit).

Più dettagliatamente la normativa definisce:

- ***controlli di linea (c.d. "controlli di primo livello"),*** *diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del back office; per quanto possibile, essi sono incorporati nelle procedure informatiche. Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi;*
- ***controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello"),*** *che hanno l'obiettivo di assicurare, tra l'altro:*
  - *la corretta attuazione del processo di gestione dei rischi;*
  - *il rispetto dei limiti operativi assegnati alle varie funzioni;*
  - *la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.*

  Le funzioni preposte a tali controlli sono distinte da quelle produttive; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi;
- ***revisione interna (c.d. "controlli di terzo livello"),*** *volta a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi. La funzione di revisione interna è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali.*

6. Le attività di audit

Le attività di audit in senso stretto sono regolamentate da vari modelli proprietari (quali, ad esempio, i modelli dei citati **The Institute of Internal**

Auditors o **ISACA)** o, per alcune tipologie di audit, anche da standard internazionali (come, ad esempio, nel caso degli audit dei sistemi di gestione sulla qualità o sulla sicurezza, che sono normati dalla **ISO 19011).**

Si ricorda che, in astratto, gli audit possono essere raggruppati in due grandi categorie e precisamente:

- i *"compliance audit"* che riguardano, ad esempio, la verifica dei requisiti di una normativa;
- gli *"audit di buona gestione"* o *"management audit"*.

Gli audit in ambito qualità, sicurezza ecc., rientrano nella seconda categoria e, pertanto, agli stessi sono applicabili le indicazioni previste dalla ISO 19011.

In realtà, soprattutto in seguito all'entrata in vigore del GDPR, qualsiasi verifica in ambito privacy necessita di una **metodologia mista**; ciò in quanto il rispetto di detta normativa prevede da un lato, regole ben precise e definite, dall'altro, l'implementazione in alcuni ambiti di un vero e proprio sistema di gestione (ad esempio nell'ambito delle misure di sicurezza).

È evidente che non esiste alcuna prescrizione normativa che imponga a un titolare la modalità con cui eseguire un audit in ambito privacy ma, come già detto, il ricorrere a standard consolidati è altamente consigliabile.

Ad esempio la ISO 19011 utilizza le seguenti definizioni:

- *audit (audit), verifica ispettiva, processo sistematico, indipendente e documentato per ottenere evidenze dell'audit e valutare con obiettività, al fine di stabilire in quale misura i criteri dell'audit sono stati soddisfatti.*

Vengono definite due diverse tipologie di audit:

- *gli audit interni, a volte denominati "audit di prima parte", sono effettuati, per il riesame da parte della direzione e per altri fini interni, dall'organizzazione stessa, o per suo conto, e possono costituire la base per una autodichiarazione di conformità da parte dell'organizzazione. In molti casi, particolarmente nelle organizzazioni più piccole, l'indipendenza può essere dimostrata con l'assenza di responsabilità per l'attività oggetto dell'audit;*
- *gli audit esterni comprendono quelli che sono generalmente denominati "audit di seconda parte" e di "terza parte". Gli audit di seconda parte sono effettuati da chi ha un interesse nell'organizzazione, quali i clienti, o da altre persone per conto degli stessi. Gli audit di terza parte sono effettuati da organismi di audit esterni indipendenti, quali quelli che rilasciano certificazioni di conformità ai requisiti della ISO 9001 e della ISO 14001.*

Ulteriori definizioni significative sono le seguenti:

- *criteri dell'audit (audit criteria), insieme di politiche, procedure o requisiti;*

- *evidenze dell'audit (audit evidence), registrazioni, dichiarazioni di fatti o altre informazioni, che sono pertinenti ai criteri dell'audit e verificabili;*
- *risultanze dell'audit (audit findings), risultati della valutazione delle evidenze dell'audit raccolte rispetto ai criteri dell'audit;*
- *conclusioni dell'audit (audit conclusion), esito di un audit fornito dal gruppo di audit dopo aver preso in esame gli obiettivi dell'audit e tutte le risultanze dell'audit.*

Inoltre per quanto riguarda i soggetti che svolgono le attività di audit la ISO 19011 introduce le seguenti definizioni:

- *auditor (auditor), valutatore, persona che ha la competenza per effettuare un audit;*
- *gruppo di audit (audit team), uno o più auditor che eseguono un audit, supportati, se richiesto, da esperti tecnici;*
- *esperto tecnico (technical expert), Persona che fornisce conoscenze o competenze specifiche al gruppo di audit.*

Relativamente a quest'ultima figura la ISO 19011 introduce due diverse precisazioni:

- *la conoscenza o competenza specifica sono riferite all'organizzazione, al processo o all'attività da sottoporre ad audit, alla lingua o alla cultura;*
- *un esperto tecnico non può agire come auditor nel gruppo di audit.*

7. I rischi delle attività di audit[3]

L'attività di audit comporta una serie di rischi, come tutte le attività investigative.

In particolare vi è il rischio di non rilevare elementi di non conformità, di effettuare campionamenti[4] errati, di considerare attendibili informazioni errate, di basare il giudizio su percezioni piuttosto che su elementi oggettivi.

Al riguardo valgono le seguenti definizioni.

7.1. Rischio inerente

È il rischio che un'evidenza viziata da errori significativi intervenga nella formulazione di un'asserzione in ipotesi di assenza di controllo interno. Questa tipologia di rischio è condizionata da:

- contesto aziendale complessivo (supporto del management, autorevolezza degli auditor, cultura e atteggiamento nei confronti dell'audit ecc.);

3. Questo paragrafo è stato realizzato con il contributo del prof. Fabio Maccaferri.
4. Il tema verrà trattato in uno specifico paragrafo.

- caratteristiche del perimetro dell'audit (complessità, ampiezza, documentabilità, disponibilità di documentazione ecc.);
- caratteristiche del "momento" in cui viene effettuato l'audit (ambiente esterno, situazione economico/finanziaria, clima aziendale ecc.).

Il rischio inerente è maggiore là dove peggiori sono le condizioni che si riscontrano:

- difficoltà ad accedere alla documentazione;
- complessità nell'interpretazione delle evidenze;
- limitata disponibilità alle interviste;
- lacune nelle spiegazioni;
- …

7.2. Rischio di controllo

È il rischio che un errore significativo non sia intercettato dal sistema dei controlli interni. Questa tipologia di rischio è condizionata da:

- contesto del sistema organizzativo (partecipazione del management, chiarezza dei ruoli, responsabilizzazione e delega, fiducia nell'audit, investimenti nel sistema dei controlli ecc.);
- caratteristiche del sistema operativo (complessità dei processi, parcellizzazione – anche geografica, livello di automazione ecc.);
- "posizionamento" dei controlli nella scala delle priorità.

Il rischio di controllo è maggiore dove maggiore è la complessità:

- permeabilità dei controlli a causa della parcellizzazione dei processi e dei ruoli;
- carenza di responsabilizzazione diretta;
- aggiornamento e miglioramento continuo del sistema dei controlli;
- …

7.3. Rischio di rilevazione

È il rischio che le procedure di audit portino ad affermare che un'evidenza viziata da errori significativi sia corretta quando in realtà non lo è. Questa tipologia di rischio è condizionata da:

- competenza dell'auditor (conoscenza della materia, conoscenza dell'azienda, predisposizione personale, capacità organizzativa, "sesto senso", esperienza ecc.);
- autorevolezza dell'auditor (capacità di relazione ad alto livello aziendale, sintesi, "incondizionabilità", capacità espressiva, un pò di "cattiveria", sapersi imporre quando è il caso, capacità di discernimento – ad esempio selezionare gli aspetti rilevanti rispetto a quelli di minore impatto ecc.).

Il rischio di rilevazione è minore dove maggiore è la competenza e autorevolezza dell'auditor il quale:

- va a fondo nelle questioni rilevanti senza farsi condizionare dal contesto e dal livello degli interlocutori;
- rischia professionalmente: non scende a compromessi e non cede al buonismo;
- "sente" quando qualcosa "non va";
- …

Il rischio di rilevazione è l'elemento più pertinente per gli audit di conformità; gli auditor lavorano inevitabilmente su campioni, raramente sull'intera popolazione di evidenze.

Questo comporta il rischio che l'auditor sia esposto a potenziali critiche.

7.4. Strumenti per la riduzione dei rischi

È possibile utilizzare alcuni strumenti per ridurre i rischi:

- con la statistica si possono offrire rappresentazioni delle risultanze;
- con la probabilità si possono determinare il livello di significatività[5] e rischio dell'audit specifico;
- con le tecniche di campionamento è possibile determinare il campione adeguato a:
  - quantificare e massimizzare la significatività;
  - quantificare e ridurre il rischio;
- con le tecniche di monitoraggio andamentale si possono verificare e rappresentare i miglioramenti (o peggioramenti) rilevati tramite audit ripetuti.

7.5. Statistica

Grazie alla **statistica** è possibile:

- rappresentare l'andamento di un fenomeno nel passato o nel presente:
  - per informare;
  - per capire se si sta lavorando bene;
- confrontare l'andamento di un fenomeno nel passato rispetto al presente:
  - per informare;
  - per capire se si sta migliorando o peggiorando.

Non c'è rischio o errore di modello: è ciò che è avvenuto e che avviene, è assodato. Non c'è errore: si riportano solo i fatti che si rilevano sui dati di cui si dispone.

5. Il termine verrà chiarito nei paragrafi successivi.

Ma al di fuori di quanto sopra, non è possibile fare alcuna affermazione.

STATISTICA DESCRITTIVA	STATISTICA INFERENZIALE
• dispone dei dati per l'intera "popolazione" (con "popolazione" si intende un gruppo omogeneo, finito e completo di eventi, fenomeni ecc.); • fornisce tecniche per elaborare i dati, raccoglierli, analizzarli e desumere caratteristiche e trend.	• dispone di informazioni parziali sulla popolazione, spesso neppure il numero di elementi che la compongono. Si ha a disposizione, in altri termini, un campione; • fornisce tecniche per individuare caratteristiche e trend e prendere decisioni sulla base di poche e incomplete informazioni, accettando un margine di incertezza (rischio di sbagliare). È MOLTO meglio che decidere su supposizioni che per quanto possano essere giuste, non sono suffragate da metodi scientifici.

7.6. Probabilità

Grazie alla **probabilità** è possibile:

- capire il comportamento di un fenomeno nel futuro:
  - per informare;
  - per capire quanto si sta lavorando bene;
- quando si desidera capire il rischio derivante dal formulare le affermazioni su un numero limitato di riscontri, o di avere sbagliato:
  - per informare;
  - per decidere.

C'è errore (possibile), c'è rischio. Meno informazioni si hanno, maggiore è la possibilità di errore. Va valutato e dichiarato.

7.7. Campionamento

Il mondo reale, per costi, disponibilità di informazioni, certezza delle informazioni, elementi imponderabili che intervengono nei processi… non sempre offre una visione completa ed esaustiva dei fenomeni. L'auditor non può "andare a vedere tutto" e anche se potesse, non può essere certo che sia tutto o che gli sia stato nascosto qualcosa.

L'audit lavora principalmente "a campione":

- sulle evidenze;
- sulle persone da intervistare;
- sulle attività da verificare.

Lavorando "a campione", le rilevazioni sono inevitabilmente su una parte della popolazione interessata, quindi c'è altrettanto inevitabilmente un'incer-