REGOLAMENTO TECNICO PER LA CERTIFICAZIONE DEI CONSERVATORI A NORMA

Dasa - Rägister

INDICE

Dasa - Rägister

1. GENERALITA'

Il presente documento descrive le procedure applicate da Dasa-Rägister per la Certificazione dei Conservatori a Norma secondo le disposizioni dell'Agenzia per l'Italia Digitale (Lista di riscontro AgID) ed è da considerarsi supplementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Contrattuale".

L'Organizzazione richiedente la Certificazione deve:

- stabilire, documentare, attuare e mantenere un efficace processo di conservazione e aggiornarlo quando necessario in conformità ai requisiti della norma di riferimento;
- definire lo scopo e il campo di applicazione del processo di conservazione specificando i servizi ed i siti ai quali è indirizzato;
- assicurare che i pericoli che ci si può ragionevolmente aspettare che accadano in relazione ai servizi compresi nel campo di applicazione del processo di conservazione siano identificati, valutati e controllati;
- mantenere a disposizione di Dasa-Rägister le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti;
- mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili all'attività, processo, servizio, prodotto incluso nel campo di applicazione della Certificazione;
- essere in possesso della certificazione in conformità alla UNI CEI EN ISO/IEC 27001, rilasciata da un organismo accreditato a fronte del Regolamento UE 765/2008, per i servizi di conservazione a norma (il campo di applicazione deve riguardare tutti i servizi di conservazione, compresi i servizi "underpinning" affidati all'esterno, e tutti i siti interessati);
- disporre del Manuale Operativo per i servizi oggetto di certificazione.

Il Certificato è emesso a fronte del completamento, con esito positivo, dell'Audit Iniziale (Initial Audit), ha una durata biennale e la sua validità è subordinata al superamento di un Audit di Sorveglianza periodico (Surveillance Audit) e ad una completa rivalutazione (Re-Audit) entro il termine della scadenza. Il Programma di Certificazione, quindi, prevede una verifica iniziale, una sorveglianza annuale ed una verifica di rinnovo con cadenza biennale.

Qualora la richiesta di certificazione provenga da Organizzazioni già certificate da enti accreditati e con certificato in corso di validità, Dasa-Rägister subentra nelle attività in accordo con la pianificazione del precedente ente, recependo eventuali rilievi ed effettuando il relativo Audit secondo le modalità previste dal presente regolamento.

Prima dell'esecuzione di ogni Audit, Dasa-Rägister comunica all'Organizzazione i nomi dell'Audit Team che condurrà la valutazione e nello stesso momento indica l'eventuale documentazione che dovrà essere resa disponibile.

Per ogni Audit sono previste:

- una riunione iniziale tra l'Audit Team e il Organizzazione finalizzata alla presentazione delle parti e all'illustrazione delle procedure di Audit;
- la verifica in campo e a campione della conformità del Organizzazione ai requisiti della norma di riferimento e della presa in carico delle prescrizioni legali riferibili al campo di applicazione della Certificazione;
- la redazione della Lista di Riscontro AgID e del rapporto (Audit Report) con i risultati e le conclusioni dell'Audit e l'eventuale pianificazione delle attività successive;
- una riunione finale tra l'Audit Team e il Organizzazione per illustrare l'esito dell'Audit e consegnare l'Audit Report. In questa fase il Organizzazione può sollevare e formalizzare eventuali riserve.

In occasione di ogni Audit (iniziale, sorveglianza e rinnovo), sarà valutata la conformità a fronte dell'Art. 24 del Regolamento eIDASe ai requisiti individuati nella Lista di riscontro AgID per la certificazione dei conservatori.

In merito all'uso di infrastrutture "cloud", il Conservatore dovrà dare evidenza della capacità di reale "controllo operativo" di tali servizi e della adesione alle eventuali indicazioni di AgID in merito all'ubicazione dei server fisici e sui repository (sistemi di memorizzazione) nei quali avviene l'archiviazione dei dati/informazioni che costituiscono l'oggetto del processo di Conservazione. Inoltre, il Conservatore dovrà dare evidenza dell'esistenza e dell'efficacia dei controlli operativi, riferiti alla Norma UNI CEI EN ISO/IEC 27001, relativi ai processi di VA (Vulnerability Assessment) e PT (Penetration Test). Questi dovranno essere svolti da strutture interne o esterne al Conservatore, la cui qualificazione deve essere

Dasa - Rägister

basata, a partire dal 01 Giugno 2017, sulla Norma ISO/IEC 17025 e che, sin da subito, forniscano evidenza almeno:

- della chiara individuazione e diligente applicazione dei requisiti inerenti la metodologia di valutazione tecnica adottata, che richiami, preferibilmente, l'applicazione dei requisiti ISO/IEC 27008;
- della competenza formale (qualifiche, da chi rilasciate, quale esperienza nel settore) delle risorse umane addette a tali test;
- della qualifica (certificazione in gergo IT) dei SW utilizzati (almeno la garanzia che le versioni siano compatibili e aggiornate ai rilasci dei SO e delle applicazioni da analizzare del Conservatore).

La sussistenza dei suddetti requisiti, ove il Laboratorio di test sia scelto dal Conservatore è di pertinenza dello stesso Conservatore e sarà oggetto di valutazione nell'ambito del processo di audit. Diversamente, se il Laboratorio sarà stato scelto da Dasa-Rägister, si applicheranno le regole di qualifica previste dalla Norma di accreditamento 17065. Dal 01 Giungo 2018, gli Operatori che effettueranno tali attività di PT e VA dovranno essere accreditati secondo la ISO/IEC 17025:2005.

Gli Audit potranno essere condotti sia in presenza che a distanza (modalità “da remoto”) così come in forma mista.

2. PRE-AUDIT

È possibile effettuare un Audit preliminare (Pre-Audit) prima dell’Audit Iniziale (Pre-Audit) con lo scopo di individuare il grado di preparazione dell'Organizzazione in relazione ai requisiti della norma e di identificare quelle situazioni che potrebbero compromettere il buon esito dell’Initial Audit.

Può essere condotto un solo Pre-Audit per ogni Richiesta di Certificazione.

3. AUDIT INIZIALE (INITIAL AUDIT)

L’Audit Iniziale ha luogo presso l’Organizzazione ed eventuali altri siti in cui si svolgono attività e processi connessi alle attività oggetto di certificazione, mediante osservazione diretta delle attività, interviste al personale, esame delle registrazioni attestanti il rispetto sistematico, da almeno tre mesi, dei requisiti della norma di riferimento.

Eventuali Non Conformità che dovessero emergere al termine dell’Initial Audit devono essere prese in carico dall’Organizzazione e la loro gestione comunicata a Dasa-Rägister (tramite le modalità indicate nell'Audit Report). Per poter proseguire con le successive fasi del processo di Certificazione, le modalità di trattamento e le eventuali Azioni Correttive definite dall’Organizzazione devono essere approvate dal Lead Auditor.

In caso In caso di Non Conformità Maggiori è necessario verificare l’efficacia del trattamento e delle eventuali Azioni Correttive, che deve avvenire entro sei mesi dalla data dell’Initial Audit altrimenti quest'ultimo deve essere ripetuto. La valutazione può avvenire su base documentale o tramite un Follow-Up Audit (par. 5.). In assenza di tale verifica non è possibile proseguire con la fase di Delibera.

3.1. RILASCIO DELLA CERTIFICAZIONE

La Certificazione viene rilasciata a seguito del parere positivo del Comitato di Delibera (Decision Committee) che valuta i documenti relativi all’Audit e prendendo anche in considerazione eventuali informazioni inerenti l’Organizzazione raccolte dal mercato o comunque di pubblico dominio.

In questa fase il Comitato di Delibera:

- può richiedere all’Organizzazione di fornire eventuali informazioni mancanti;
- può disporre un Follow-Up Audit o documentale per integrare eventuali mancanze della verifica.

Il parere positivo del Comitato di Delibera consente:

- l’emissione del Certificato la cui validità è biennale e decorre dalla data della Delibera;
- l’iscrizione e la pubblicazione dei dati dell’Organizzazione nel Registro Certificazioni.

Il Comitato di Delibera può anche disporre Audit di Sorveglianza ad intervalli più frequenti (ad esempio semestrali) a seguito di:

- proposta dell’Audit Team o esito dell’Audit tale per cui sia necessario monitorare il processo di conservazione con frequenza maggiore rispetto all’anno;

Dasa - Rägister

– specifica richiesta del Organizzazione.

In caso di concessione della Certificazione, Dasa-Rägister provvede alla trasmissione formale del Rapporto di Audit, come eventualmente integrato a seguito della Delibera, al Conservatore che avrà cura di inviarlo ad AgID per la qualifica come Conservatore a Norma.

In caso di non concessione della Certificazione, le ragioni di tale decisione vengono comunicate formalmente all'Organizzazione, precisando gli scostamenti rispetto ai requisiti richiesti che la stessa si deve impegnare a correggere entro un termine di tempo proposto e accettato da Dasa-Rägister. Tale termine non deve in ogni caso essere superiore a sei mesi, superati i quali deve essere ripetuto l'intero Initial Audit.

4. AUDIT DI SORVEGLIANZA (SURVEILLANCE AUDIT)

Al fine di accertare il continuo rispetto di quanto stabilito dalla norma di riferimento, con la periodicità prevista dal Programma di Certificazione viene effettuato un Audit di Sorveglianza, durante il quale vengono valutati solo alcuni aspetti del Sistema di Gestione.

L'Audit di Sorveglianza è eseguito con le stesse modalità dell'Initial Audit, valutando i requisiti/processi indicati nel Piano delle Sorveglianze. L'Audit può comunque essere condotto anche su altri punti a discrezione del Lead Auditor.

Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima.

L'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del successivo Audit di Sorveglianza salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria:

– una verifica documentale supplementare (Follow-Up documentale) con l'invio di documenti da parte dell'Organizzazione a Dasa-Rägister;
– un audit supplementare presso l'Organizzazione (Follow-Up Audit – par. 5.).

Per le Non Conformità Maggiori, Dasa-Rägister definisce un tempo massimo entro il quale effettuare il Follow Up Audit al fine di verificare l'efficacia del trattamento e delle eventuali Azioni Correttive. Qualora questo non abbia luogo nei tempi previsti, la Certificazione verrà sospesa per un periodo massimo di sei mesi trascorsi i quali la Sospensione si trasformerà in Revoca.

In fase di sorveglianza, pur valendo la stessa regola della conferma e dell'invio al Conservatore via PEC, a fronte di firma digitale e marcatura temporale, non è richiesto che lo stesso Conservatore ne invii copia ad AgID, se non in caso di registrazione di Non Conformità Maggiori e/o dietro esplicita richiesta di quest'ultima, in quanto Autorità di Vigilanza.

La documentazione prodotta durante gli Audit di Sorveglianza viene sottoposta al Comitato di Delibera nei seguenti casi:

– siano state rilevate Non Conformità Maggiori;
– sia stato modificato il Programma di Certificazione (per esempio, riduzioni, estensioni…);
– su esplicita richiesta dell'Audit Team, che può segnalare quelle situazioni che possono avere influenza sulla validità del Certificato.

L'Audit di Sorveglianza ha cadenza annuale e deve essere effettuata entro i dodici mesi dalla data della delibera del certificato.

5. AUDIT SUPPLEMENTARI (FOLLOW-UP AUDIT)

Il Follow-Up Audit è eseguito con le stesse modalità dell'Initial Audit ed ha normalmente come oggetto di verifica le sole parti interessate (per es. correzione Non conformità Maggiori, estensione, scopo,...). La valutazione può comunque essere condotta anche su altri punti a discrezione del Lead Auditor.

Qualora il Follow-Up Audit per la verifica dell'efficacia del trattamento delle Non Conformità Maggiori abbia esito negativo, la Certificazione verrà sospesa fino a che non sia stata valutata l'efficacia del nuovo trattamento e delle eventuali Azioni Correttive, e comunque per un periodo massimo di sei mesi, trascorsi i quali la Sospensione si trasformerà in Revoca.

6. AUDIT DI RINNOVO (RE-AUDIT)

La validità del Certificato è confermata a seguito dell'esito positivo di una verifica completa

Dasa - Rägister

(Re-Audit) condotta con gli stessi criteri dell'Initial Audit.
Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima; per le Non Conformità Minori l'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del Audit di Sorveglianza salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria:

- una verifica documentale supplementare (Follow-Up documentale) con l'invio di documenti da parte dell'Organizzazione a Dasa-Rägister;
- un audit supplementare presso l'Organizzazione (Follow-Up Audit).

In caso di Non Conformità Maggiori è necessario verificare l'efficacia del trattamento e delle eventuali Azioni Correttive entro la data di scadenza in vigore del Certificato.
Entro la medesima data la Certificazione può essere rinnovata a seguito del parere positivo del Comitato di Delibera (Decision Committee) con le stesse modalità del rilascio iniziale (par. 3.3).
Ciò implica che il Re-Audit deve essere effettuato con sufficiente anticipo al fine di permettere la gestione di eventuali Non Conformità.
Qualora non si riesca a completare l'iter entro la data di scadenza del certificato (ad esempio Follow Up), il Comitato di Delibera non potrà procedere con il rinnovo. Se le attività pendenti si riescono a completare entro sei mesi dalla scadenza, il Comitato di Delibera potrà ripristinare il certificato sul quale comparirà il periodo di interruzione della sua validità. Altrimenti, trascorsi sei mesi e non più di un anno dalla scadenza, dovrà essere condotto almeno uno Stage 2 perché il Comitato di Delibera possa ripristinare il certificato. Trascorso un anno si dovrà procedere con un Audit Iniziale (Stage 1+Stage 2) ed il rilascio di un nuovo certificato senza mantenere la storicità della certificazione precedente.

7. CLASSIFICAZIONE DEI RILIEVI

I rilievi riscontrati durante l'Audit sono classificati in Non Conformità Maggiori e Non Conformità Minori.
Una Non Conformità si definisce "Maggiore" quando si ha:

- lo scostamento dall'efficace adempimento ai requisiti della Check List di AgID risulti potenzialmente in grado di inficiare il processo di conservazione o l'integrità, disponibilità e riservatezza delle informazioni soggette a conservazione;
- l'Organizzazione non dimostri di essere in possesso della certificazione a fronte della Norma UNI CEI EN ISO/IEC 27001, rilasciata da un organismo accreditato a fronte del Regolamento UE 765/2008, per i servizi di conservazione a norma (tutti i servizi di conservazione, compresi i servizi "underpinning" affidati all'esterno e tutti i siti interessati), in quanto ciò è un requisito propedeutico al rilascio del certificato di conformità al presente schema.

La presenza di una o più Non Conformità Maggiori preclude l'emissione del certificato di conformità e non consente la trasmissione ad AgID del rapporto ai fini dell'Accreditamento rilasciato dalla stessa Agenzia. Le Non Conformità Maggiori registrate in vigenza dell'Accreditamento rilasciato da AgID, saranno segnalate alla stessa Agenzia, inviando direttamente una copia del Rapporto di Verifica, con le modalità di firma e invio utilizzate per l'invio dello stesso rapporto all'operatore della conservazione.

Una Non Conformità si definisce "Minore" quando:

- lo scostamento dall'efficace adempimento ai requisiti della Check List di AgID non risulti potenzialmente in grado di inficiare il processo di conservazione o l'integrità, disponibilità e riservatezza delle informazioni soggette a conservazione.

In caso di Non Conformità, sia minori che maggiori, è necessario che il Conservatore comunichi il trattamento immediato adottato per interrompere gli effetti della Non Conformità entro e non oltre cinque giorni lavorativi. Entro quindici giorni lavorativi dovranno essere comunicate l'analisi delle cause, l'azione correttiva e la pianificazione della sua attuazione, che dovranno essere analizzate ed approvate da Dasa-Rägister. La verifica dell'attuazione e dell'efficacia del trattamento immediato adottato dall'operatore della conservazione e dell'azione correttiva dovrà essere condotta entro e non oltre tre mesi dalla comunicazione della stessa azione correttiva.
I rilevi che dovessero emergere durante il Pre-Audit non vengono classificati.