Att.: A tutti gli Odc accreditati

Ns. rif.: DC2017SPM080 *Milano,* 27/02/2017

Oggetto: **Dipartimento Certificazione e Ispezione ACCREDIA - Circolare n° 5/2017**
Schema di accreditamento degli Organismi di Certificazione, per il processo di certificazione dei Conservatori a Norma, secondo le disposizioni dell'Agenzia per l'Italia Digitale.

1. Introduzione

Le esigenze da parte delle pubbliche amministrazioni di conservazione a norma dei documenti informatici, già esistenti nel mercato domestico a fronte del processo di fatturazione elettronica e di protocollazione digitale, riguarderanno nell'immediato futuro nuovi ambiti di applicazione, in quanto la normativa vigente in materia prevede che entro tempi brevissimi la Pubblica Amministrazione formi i propri documenti solo in modalità digitale. Le eventuali date di slittamento di possibili aree della PA che necessitino di tempi maggiori, non potranno essere che minime. Per la conservazione dei documenti prodotti nativamente su carta e trasformati in digitale, nonché per quelli nativi digitali, sarà necessario un adeguato dimensionamento dei relativi servizi di conservazione. Tali servizi di tipo informatico, che le PA possono attivare anche internamente, già da oggi sono offerti anche da soggetti privati e pubblici, i cosiddetti Conservatori accreditati da AgID.

2. Contesto Normativo

I soggetti che intendono accreditarsi presso AgID nel ruolo di Conservatori devono dimostrare il possesso dei requisiti stabiliti dalle norme specifiche attraverso la presentazione di documenti e certificazioni tra i quali, dopo l'entrata in vigore della d.lgs n. 179 del 2016, è compreso anche un certificato di conformità ai requisiti tecnici organizzativi stabiliti dall'AgID, rilasciato da un ente di certificazione accreditato da ACCREDIA, o da altro ente di Accreditamento rientrante nell'ambito del Reg. UE 2008/765, firmatario degli accordi di Mutuo riconoscimento nello schema specifico. Stante il dettato normativo sul ruolo dei Conservatori e delle prescrizioni della Norma ISO/IEC 17065:2012, sulla quale sarà basato lo schema, sarà prevista una sorveglianza annuale e un rinnovo biennale, in occasione del quale i Conservatori dovranno trasmettere il rapporto ad AgID.

2.a. Si applicano in particolare i seguenti provvedimenti legislativi:

- D. Lgs. 82 del 2005 – Codice Amministrazione Digitale (Art. 29, 32, 44 bis, 71, 61,50 bis, 51) e s.m.i;
- D.lgs 30 giugno 2003 n. 196 – codice in materia di protezione dei dati personali;
- DPCM del 3 Dicembre 2013 [Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'am- ministrazione digitale di cui al decreto legislativo n. 82 del 2005] e relativi allegati tecnici;
- DPCM del 13 novembre 2014 (Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici;
- DPCM del 3 dicembre 2013 sul protocollo informatico;
- Circolare 65 del 10 Aprile 2014 di AgID e relativi allegati tecnici.

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

2.b. Modalità di esecuzione delle verifiche

Lo schema di accreditamento definito da AgID, in qualità di Proprietario dello stesso schema, effettuerà la verifica di conformità alle Norme Tecniche che seguono:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- UNI CEI EN ISO/IEC 27001:2014, Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.1.1 (2011-05) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.1.1 (2011-05) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Vista l'esigenza di integrazione di più Norme e Leggi dello Stato, la Norma di riferimento per l'accreditamento è, naturalmente, la ISO/IEC 17065:2012.

3. Processo di Accreditamento degli Organismi di Certificazione

Di seguito si indicano le modalità previste per l'accreditamento degli Organismi di Certificazione e si forniscono alcune indicazioni mandatorie in ordine al processo di certificazione dei conservatori che intendono ottenere l'accreditamento pubblico di AgID.

1) Norma e regole di Certificazione AGID

Norma di Certificazione	UNI CEI EN ISO/IEC 27001:2014 con scopo di certificazione comprendente i servizi di Conservazione a Norma, con copertura di tutti i siti interessati e di tutti i fornitori di servizi "underpinning" a questo riconducibili. Ove l'Organismo di Certificazione che ha rilasciato la certificazione a fronte della Norma UNI CEI ISO/IEC 27001:2014 sia diverso da quello che svolge le attività riferite alla verifica di conformità di cui al presente schema, dovrà essere, comunque, un organismo accreditato da un Ente di Accreditamento nazionale ai sensi del Reg. (UE) 765/2008. Norme di legge e tecniche di cui al precedente paragrafo 2.a e 2.b. valutate dall'Organismo di Certificazione a fronte della Check List appositamente predisposta da AgID.
Criteri di competenza del Gruppo di Verifica dell'OdC	All'interno del gruppo di verifica devono essere disponibili queste competenze, facenti capo ad una persona singola, o al Team nel suo complesso: • Qualifica come Team Leader UNI CEI ISO/IEC 27001:2014, rilasciata dall'Organismo in conformità alla ISO 27006 in vigore • Qualifica come Auditor UNI CEI EN ISO 20000-1:2012 ovvero qualifi-

	ca come Auditor SGQ EA 33 e conoscenza architettura ITIL, rilasciata dallo stesso Organismo di Certificazione • Conoscenza della CIRCOLARE N. 65 del 10 aprile 2014 emessa dall'Agenzia per l'Italia Digitale e dell'Allegato relativo ai Profili Professionali. • Superamento dello specifico corso di formazione erogato da AgID e ACCREDIA per la comprensione e l'addestramento all'uso della Lista di Riscontro AgID per i Conservatori a Norma.
Valutazioni di robustezza del sistema IT	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. L'Organismo di Certificazione che svolge la verifica di conformità ai requisiti della Check List di Agid, verificherà anche l'esistenza e l'accettabilità dei controlli operativi, riferiti alla Norma UNI CEI EN ISO/IEC 27001, relativi ai processi di VA (Vulnerability Assessment) e PT (Penetration Test). Gli stessi dovranno essere svolti da strutture interne o esterne al Conservatore, ovvero da strutture interne o esterne agli stessi Organismi di Certificazione, la cui qualificazione deve essere 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 (quali qualifiche, da chi rilasciate, quale esperienza nel settore) delle Risorse Umane addette a tali test; e - 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 valutazione di cui sopra, 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 da parte dell'Organismo di Certificazione. Diversamente, se il Laboratorio sarà stato scelto dall'Organismo di Certificazione, si applicheranno le regole di qualifica previste dalla Norma di accreditamento 17065. Dal 01 Giugno 2018, gli Operatori che effettueranno tali attività di PT e VA dovranno essere accreditati secondo la ISO/IEC 17025:2005.
Indicazioni specifiche sulla registrazione di NC	La certificazione a fronte della Norma UNI CEI EN ISO/IEC 27001 può essere condotta da un qualsivoglia Organismo di Certificazione, purché accreditato a fronte del Regolamneto (UE) 765/2008. Sarà compito dell'Organismo di Certificazione che effettua la verifica a fronte della Check List di AgID di verificare che lo scopo di certificazione comprenda i servizi di conservazione a norma. Ove tale requisito non dovesse essere riscontrato, l'Organismo di Cer-

	tificazione che esegue la verifica a fronte della Check List di AgID registrerà tale situazione nel proprio rapporto, specificando che questa condizione preclude il rilascio del certificato di conformità. Qualunque altra risultanza di verifica, riferita a scostamenti dall'efficace adempimento ai requisiti previsti dalla Check List di AgID dovrà essere registrata come Non Conformità. Ove tali Non Conformità risultino potenzialmente in grado di inficiare il processo di conservazione o l'integrità, disponibilità e riservatezza delle informazioni soggette a conservazione, la stessa risultanza dovrà essere classificata come Non Conformità maggiore. 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 stssa Agenzia. La gestione delle Non Conformità da parte dell'operatore della conservazione, deve essere improntata ai requisiti della Norma UNI CEI EN ISO/IEC 27001. L'Organismo di Certificazione preposto alla verifica di conformità alla Check List di AgID dovrà prevedere nel proprio Regolamento Specifico di Certificazione per questo schema, che gli sia comunicato dall'operatore della conservazione il trattamento immediato adottato per interrompere gli effetti della Non Conformità entro e non oltre cinque giorni lavorativi. Entro quindici giorni lavorativi dovrà essere comunicata l'analisi delle cause radice, che l'Organismo di Certificazione dovrà analizzare e approvare, nonché la definizione dell'azione correttiva e la pianificazione della sua attuazione. 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. Ove a fronte della verifica di attuazione ed efficacia del trattamento immediato e dell'azione correttiva, l'Organismo di Certificazione dovesse registrare una nuova NC, si innescherà nuovamente il processo di risposta precedentemente descritto. Per le NC maggiori registrate in vigenza dell'Accreditamento rilasciato da AgID, l'Organismo di Certificazione dovrà segnalare tale evento 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.
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli Odc la dimostrazione della: • Qualifica interna come ispettore UNI CEI ISO/IEC 27001:2014, rilasciata in conformità alla ISO 27006 in vigore. • Conoscenza della CIRCOLARE N. 65 del 10 aprile 2014 emessa dall'Agenzia per l'Italia Digitale e allegato relativo ai Profili Professionali.
Tempi di verifica	La valutazione di un conservatore si svolge in due specifici momenti: • prima valutazione e/o rinnovo; • sorveglianza periodica, secondo un ciclo biennale.

	La valutazione di sorveglianza necessita un terzo del tempo della valutazione iniziale e/o di rinnovo (che richiedono lo stesso tempo). Gli Organismi di Certificazione effettueranno le verifiche di certificazione secondo il seguente criterio: La verifica sarà limitata all'accertamento dell'applicazione dei requisiti individuati della Lista di Riscontro predisposta da AgID. Inoltre, l'Organismo di Certificazione prenderà atto in tutte le verifiche, dell'esito delle valutazioni a fronte della Norma UNI CEI ISO/IEC 27001:2014. Per gli operatori non già certificati eIDAS, la verifica richiederà due giorni uomo aggiuntivi per la verifica della conformità all'Art. 24 del Regolamento eIDAS. Per gli operatori già certificati eIDAS, tale verifica richiederà un giorno uomo. Per la valutazione dei requisiti individuati dalla Lista di riscontro predisposta da AgID sulla applicazione delle Norme di cui ai precedenti §§ 2.a e 2.b, se in sede di valutazione iniziale o di rinnovo saranno necessari 6 gg-uomo, mentre in sede di sorveglianza, saranno necessari 2 gg-uomo. Non sono previste riduzioni di alcun tipo su tali livelli minimi di tempo. Nel caso di Conservatori che operino su più siti, per ogni sito aggiuntivo a quello centrale, l'Organismo di Certificazione dovrà prevedere una verifica di un giorno uomo. Si applica il documento IAF MD01 per certificazione multi-site.
Certificato e rapporto	Il Certificato (PRD) avrà validità biennale, con obbligo di sorveglianza annuale. Lo scopo di certificazione dovrà riportare il riferimento al servizio di Conservazione a Norma in conformità all'Art. 29 del D. Lgs. 82 del 2005 e smi, nonché al presente schema di certificazione. Il rapporto di Audit verrà sottoscritto con dal Gruppo di Audit dell'Organismo di Certificazione al termine della riunione finale e ne verrà lasciata copia al conservatore. In un periodo massimo di quindici giorni, l'Organismo di Certificazione si esprimerà sulla conferma o necessità di correzione / integrazione di tale rapporto e/o sui tempi e modalità per l'esecuzione delle verifiche di "follow-up" relative alle eventuali Non Conformità registrate dal Gruppo di Verifica. Nelle verifiche iniziale e di rinnovo, una volta approvato definitivamente il rapporto, l'Organismo di Certificazione potrà emettere il proprio certificato di conformità o negare la certificazione, comunicando al Conservatore le ragioni di tale decisione. Il rapporto di valutazione iniziale e di rinnovo dovranno riportare la dicitura "Conforme all'Art. 24 del Regolamento UE 2014/910 "eIDAS". Dopo l'approvazione del Rapporto del Gruppo di Audit, per come eventualmente integrato a fronte delle decisioni dell'Organismo di Certificazione, lo stesso Organismo provvede alla firma digitale con marca temporale dello

	stesso rapporto e ad inviarlo via PEC al Conservatore, affinché quest'ultimo possa inviarlo ad AgID per il prosieguo dell'iter di accreditamento pubblico come Conservatore a Norma. Per i certificati 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. Il Certificato di Conformità (PRD) rilasciato dall'Organismo di Certificazione dovrà essere riferito alla conformità alla Check List di AgID, nella versione applicabile. Inoltre, il Certificato dovrà fare riferimento al presente schema di accreditamento ed alla Norma UNI CEI EN ISO/IEC 17065:2012, con riferimento alla conformità dei Conservatori ai requisiti individuati dalla Lista di Riscontro AgID, nella versione applicabile.

2) Processo di Accreditamento ACCREDIA

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.
Non occorre aver già rilasciato certificati nel settore, ma aver condotto almeno una verifica ispettiva ai fini di certificazione.

OdC già accreditato prodotto e contemporaneamente già accreditato ISO 17021:2011 per lo schema SSI (ISO/IEC 27001) ovvero OdC già accreditato eIDAS	Esame documentale ISO 17065 specifico per lo schema di 0,5 giornate Verifica in accompagnamento
OdC già accreditato PRD e contemporaneamente già accreditato ISO 17021:2011 ma non per la Norma ISO/IEC 27001. oppure OdC già accreditato PRD ma non accreditato ISO/IEC 17021-1	Il processo di accreditamento secondo le regole sopra menzionate potrà iniziare solo dopo l'ottenimento dell'accreditamento 17021-1 nello schema ISO 27001.
OdC non accreditato per lo schema Prodotto ma accreditato ISO/IEC 17021.	Esame documentale ISO 17065 di 1 giornata Verifica ispettiva presso la sede dell'OdC di 2 giornate sullo schema PRD, con particolare riferimento al presente schema di accreditamento. Verifica in accompagnamento.
OdC non ancora accreditato prodotto, e neanche ISO/IEC 17021.	Acquisizione degli accreditamenti ISO/IEC 17021-1 per lo schema 27001 e Successivamente accreditamento secondo lo schema ISO/IEC 17065 per lo specifico schema dei conservatori.

Documentazione da presentare ad ACCREDIA per l'esame documentale

a) Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
b) Curricula degli ispettori e dei Decision Maker, da cui si deve si deve evincere rispettivamente: la frequenza e superamento del corso di formazione per Auditor organizzato da AgID e ACCREDIA e il rispetto dei requisiti di qualifica indicati nella sezione Decision Maker;
c) Modulo del Rapporto di Audit;
d) Attestato/Certificato rilasciato dall'OdC;
e) Lista delle prossime attività di verifica;
f) Procedure / regolamenti contrattuali applicabili al processo di valutazione, nonché le procedure interne per la gestione della pratica di certificazione;
g) Per gli OdC NON accreditati ISO/IEC 17021, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

3) Mantenimento dell'Accreditamento

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo…), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso meno di 10 certificati nello schema di certificazione, devono essere effettuate una verifica in accompagnamento e una verifica in sede;
- se l'OdC ha emesso tra 11 e 50 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso più di 51 certificati nello schema, devono essere effettuate 3 verifiche in accompagnamento.

Riferimenti Normativi per l'accreditamento

Vista l'esigenza di integrazione di più Norme e Leggi dello Stato, la Norma di riferimento per l'accreditamento è, naturalmente, la Norma UNI CEI EN ISO/IEC 17065:2012 Valutazione della conformità. Requisiti per organismi che certificano prodotti, processi e servizi.
Ovunque, nel presente documento, sia riportato il riferimento ad una Norma referenziata con la revisione o l'anno di emissione, vale esattamente quella Norma. Ove, invece, le Norme non siano referenziate con lo stato di revisione e/o l'anno di emissione, dovrà essere considerata applicabile la Norma vigente al momento dello svolgimento delle attività operative: sia di accreditamento, sia di sorveglianza, sia di rinnovo.

Prescrizioni relative al processo di accreditamento

Condizione perché un OdC possa essere accreditato è il possesso dei requisiti di cui al Regolamento ACCREDIA RG-01 per l'accreditamento degli Organismi di Certificazione e di Ispezione e al Regolamento ACCREDIA RG-01-03 per l'accreditamento degli Organismi di Certificazione del Prodotto.

Accertato il possesso dei requisiti minimi, si darà avvio all'iter di accreditamento con la conduzione delle attività di verifica come previste nei Regolamenti di cui sopra e in conformità alle norme/documenti applicabili all'accreditamento.

Siamo a disposizione per chiarimenti.

Con cordialità.

Il Direttore di Dipartimento
Dr. Emanuele Riva