A tutti gli Organismi di Certificazione accreditati

Loro Sedi

Ns. rif.: DC2016SSV440 *Milano,* 16/12/2016

Oggetto: **Dipartimento Certificazione e Ispezione Accredia - Circolare N° 36/2016**
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.
- ETSI EN 319 401 V2.1.1.

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 ISO/IEC 27001:2014 e Norma ETSI EN 319 401 V2.1.1, con scopo di certificazione comprendente i servizi SPID, con copertura di tutti i siti interessati e di tutti i fornitori di servizi "underpinning" a questo riconducibili. Norma ISO/IEC 29115:2013 – "Entity authentication assurance program". Requisiti tecnici definiti con il Regolamento di attuazione UE 2015/1502 della Commissione. 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.
Criteri di competenza del Gruppo di Verifica dell'OdC	All'interno del gruppo di verifica devono essere disponibili queste competenza, 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 qualifica 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 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. I controlli operativi, riferiti alle Norme UNI CEI ISO/IEC 27001 ed ETSI EN 319 401 riferiti ai processi di VA (Vulnerability Assessment) e PT (Penetration Test), 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.
Indicazioni specifiche sulla registrazione di NC	La registrazione di non conformità maggiori sistemiche o sui controlli operativi (UNI CEI ISO/IEC 27001:2014 e/o ETSI EN 319 401V2.0.0) o sui requisiti normativi richiamati dalla Lista di Riscontro di AgID, che pregiudicano il corretto svolgimento dei servizi di conservazione a norma, deve condurre, a seconda della situazione rilevata, anche alla revoca della certificazione, non solo alla sospensione. Inoltre, nel caso di sospensione (e ovviamente di revoca) deve essere indicato al Conservatore che egli stesso è responsabile della comunicazione di tale evento ad AgID, ma che analoga comunicazione

	viene trasmessa immediatamente anche ad ACCREDIA per le necessarie attività di coordinamento con la stessa AgID. Le eventuali NC maggiori, per gli operatori già in possesso di accreditamento pubblico di AgID, dovranno prevedere una risposta immediata, entro 5 gg lavorativi, con l'indicazione dei provvedimenti adottati per tamponare le criticità individuate. Entro i successivi 5gg lavorativi dovrà essere definita l'analisi delle cause e la pianificazione delle azioni necessarie per eliminarle e/o mitigarle in modo da avere come risultato un rischio di disservizio / non conformità valutato accettabile. La mancata comunicazione di modifiche dell'organizzazione o dell'infrastruttura IT del Conservatore, che abbiano un impatto diretto sulla sicurezza delle informazioni dell'infrastruttura oggetto di valutazione, è da considerare come NC Maggiore e come tale va trattata, valutando in modo formale, quindi con adeguata registrazione sul rapporto di verifica, se tali modifiche possano aver creato delle brecce di sicurezza o nella qualità attesa del servizio (capacità di fornire servizi di conservazione secondo le disposizioni riportate nel presente documentate e descritte nel Manuale di Conservazione) nel periodo intercorrente dalla applicazione di tali modifiche sino alla data dell'audit in corso. Il conservatore dovrà collaborare attivamente a tale analisi. In casi gravi, vista la responsabilità oggettiva dell'Organismo di Certificazione nei confronti di ACCREDIA e di AgID, lo stesso Organismo di Certificazione dovrà fare una specifica segnalazione ad ACCREDIA per ricevere specifiche istruzioni di vigilanza. Carenze inerenti la sicurezza delle informazioni, che possano compromettere o che possano aver compromesso i servizi debbono essere sempre classificate come NC Maggiori. Il campionamento dei processi di conservazione e di quelli di supporto, nonché dei requisiti organizzativi del conservatore, in sede di certificazione e rinnovo, dovrà essere completo. Il campionamento sugli oggetti di conservazione dovrà essere fatto a fronte dell'applicazione della Norma ISO 2859-1, con LQA=0. Le eventuali NC di servizio (PRD) riscontrate a fronte di tale campionamento costituiscono NC Maggiore e dovranno essere gestite prevedendo un follow-up con un campionamento allargato tale da offrire una significativa fiducia sul ripristino della conformità del processo che conduce alla produzione dei pacchetti di versamento→conservazione→distribuzione.
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. • Qualifica interna come Auditor UNI CEI EN ISO 20000-1:2012 ovvero qualifica come Auditor SGQ EA 33 e conoscenza architettura ITIL. • 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: Se il TSP che intende essere certificato come operatore conservatore è già certificato per lo schema eIDAS, la verifica sarà limitata all'accertamento dell'applicazione dei requisiti sistemici e dei controlli operativi della ETSI EN 319 401 e 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 registrando eventuali NC maggiori da dover investigare con un tempo aggiuntivo uguale alt tempo per una sorveglianza su tale Norma. Per tali operatori, già accreditati eIDAS, la verifica a fronte della Norma ETSI EN 319 401 richiederà 5 gg in sede iniziale e di rinnovo e 3 gg in sede di sorveglianza. Non sono previste riduzioni di alcun tipo su tali livelli minimi di tempo. Per gli operatori non già certificati eIDAS, la verifica richiederà due giorni aggiuntivi per la verifica della conformità al regolamento citato. 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 almeno 6 gg-uomo, mentre in sede di sorveglianza, saranno necessari almeno 3 gg-uomo. Non sono previste riduzioni di alcun tipo su tali livelli minimi di tempo. Gli Organismi di Certificazione potranno valutare, caso per caso, l'esigenza di tempo aggiuntivo, sulla base della complessità del processo di conservazione: - numero dei siti coinvolti; - coesistenza di altri servizi IT erogati dalla società che svolge la funzione di conservatore, architettura di controllo della complessità sistemica e tecnica di tali servizi (sulla base dei criteri ITIL); - maturità e architettura del sistema di Business Continuity e Disaster Recovery; - presenza di fornitori "underpinning critici" per processi in outsourcing; - modalità e maturità nella gestione dell'outsourcing; - precedenti criticità severe registrate etc. Si applica il documento IAF MD01 per certificazione multi-site. Si applica il documento IAF MD 04 per la CAAT
Certificato e rapporto	Il certificato 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. 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 ai requisiti applicabili 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 dietro esplicita richiesta di quest'ultima, in quanto Autorità di Vigilanza. Il Certificato di Conformità eventualmente rilasciato dall'Organismo di Certificazione al conservatore dovrà riportare la versione della SOA e del Trust Service Practice Statement (ETSI EN 319 401 V.2.1.1). Nel certificato dovrà essere fatto riferimento alla conformità allo schema di accreditamento di ACCREDIA, alla conformità alla Norma ETSI EN 319 401 V2.1.1, alla conformità ai requisiti individuati dalla Lista di Riscontro AgID per la certificazione dei conservatori in Rev. 00 del 24 Novembre 2016.

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	Il processo di accreditamento secondo le regole sopra menzionate potrà iniziare solo dopo l'ottenimento dell'accreditamento 17021-1 nello schema ISO 27001.

17021:2011 ma non per la Norma ISO/IEC 27001. oppure OdC già accreditato PRD ma non accreditato ISO/IEC 17021-1	
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 e porgiamo cordiali saluti.

Il Direttore di Dipartimento
Dr. Emanuele Riva