Prot. DC2018SSV023 Milano, 12-02-2018

A tutti gli Organismi di Certificazione accreditati nello schema PRS e operanti la certificazione di sistemi di gestione Servizi Informatici
Att.: Responsabili di schema

Alle Associazioni degli Organismi di valutazione della conformità

Vostra mail

Oggetto: **Dipartimento DC - Circolare Tecnica N° 03/2018**
Disposizioni in materia di certificazione e accreditamento per la conformità alla norma UNI 11697:2017 – Profili professionali relativi al trattamento e alla protezione dei dati personali.

Introduzione

Questa circolare fornisce indicazioni per l'accreditamento degli Organismi di certificazione ai fini del rilascio di certificazioni di profili professionali relativi al trattamento e alla protezione dei dati personali di cui alla UNI 11697:2017. La presente circolare è stata predisposta da un gruppo di lavoro, coordinato da ACCREDIA, a cui hanno preso parte tutte le principali parti interessate.

L'obiettivo è quello di definire regole e i criteri comuni per tutti gli enti di certificazione.

Contesto Normativo

Si rimanda a quanto riportato nella Bibliografia della norma UNI 11697:2017.

1) Regole di certificazione

Norma di accreditamento	UNI CEI EN ISO/IEC 17024
Norma di certificazione	UNI 11697:2017
Criteri di competenza dei commissari d'esame	La Commissione d'esame dovrà possedere, nel suo insieme, queste professionalità: 1. la conoscenza delle regole e criteri definiti dall'ente di Certificazione per l'esame di certificazione, che devono essere coerenti con quanto richiamato dalla ISO/IEC 17024; 2. Il possesso della certificazione sotto accreditamento ACCREDIA del profilo della norma UNI oggetto dell'esame[1] 3. Competenza, maturata a seguito di esperienze lavorative di almeno 8 anni, in materie attinenti la sicurezza delle informazioni e la protezione dei dati personali 4. Competenza, maturata a seguito di esperienze lavorative di almeno 8 anni, in ambito giuridico (Es: avvocato, magistrato, giurista) con comprovata esperienza nella data protection.

[1] Il possesso di una certificazione sotto accreditamento deve essere adeguata al profilo da esaminare:
- Un commissario certificato come DPO può esaminare DPO, Manager, Valutatore, Specialist.
- Un commissario certificato come Manager può esaminare Manager, Valutatore, Specialist
- Un commissario certificato come Verificatore può esaminare Valutatore, Specialist
- Un commissario certificato come Specialist può esaminare uno Specialist

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

	La Commissione d'esame deve essere composta da almeno 2 membri. <u>Grandparent</u> Per i primi tre anni di operatività, in sostituzione del membro della Commissione d'esame in possesso di una certificazione sotto accreditamento nello stesso profilo oggetto di valutazione (punto 2 di cui sopra), l'OdC può servirsi di un Grandparent che possieda almeno uno dei requisiti indicati nei punti seguenti: 1. aver operato con funzioni di Responsabile (in ambiti quali il "trattamento di dati personali" o "della sicurezza delle informazioni" o "della protezione dei dati personali") per un periodo non inferiore a 8 anni; 2. aver operato con funzioni di Responsabile (in ambiti quali il "trattamento di dati personali" o "della sicurezza delle informazioni" o "della protezione dei dati personali") per un periodo non inferiore ad anni 3 ed aver acquisito altre esperienze professionali nel campo (anche in qualità di docente universitario per un periodo di almeno 2 anni, o come auditor tecnico/esperto nei sistemi di gestione per la protezione dei dati personali). Gli anni di esperienza complessiva devono comunque essere almeno 8; 3. aver operato quale responsabile di Sistemi di Gestione per la sicurezza delle informazioni e/o gestione dei servizi informatici (es: persona certificata sotto accreditamento come Team Leader per la norma UNI ISO/IEC 27001 o UNI ISO/IEC 20000-1, oppure auditor CISA) per un periodo non inferiore ad anni 8; 4. aver ricoperto ruoli e funzioni significative in istituzioni pubbliche o di tipo privato operanti in ambito privacy e/o sicurezza delle informazioni per un periodo non inferiore a 6 anni, o aver partecipato con funzioni rilevanti a importanti programmi e progetti in campo privacy, ad attività scientifica, normativa, pubblicistica tecnica e simili, per un periodo non inferiore a 8 anni; 5. Essere in possesso di una certificazione professionale ai sensi della UNI 11506 e norme multi parte correlate per i profili di ICT security Manager o ICT Security Specialist o web security expert e 2 anni di esperienza come consulente in ambito privacy, ovvero di una certificazione come ISMS Professional sulla base del-la Norma ISO 27021.
Criteri di competenza del *decision maker*	L'OdC deve dotarsi di criteri di qualifica del Decision Maker, che può essere membro della struttura interna dell'OdC, per assicurarsi che possieda adeguate competenze. I criteri dovranno considerare i seguenti elementi minimi: • conoscenza dei processi di delibera dell'OdC; • conoscenza generale della Norma UNI 11697:2017
Durata della certificazione	4 anni con sorveglianze annuali
Modalità d'esame per la certificazione (esame scritto e orale)	<u>Requisiti di accesso agli esami di certificazione</u> Per essere ammessi all'esame i candidati devono soddisfare tutti i requisiti indicati nell'appendice B della UNI 11697:2017, con i chiarimenti forniti dalla Nota riportata al punto 4.1 della stessa norma, attraverso: • la presentazione di idonea documentazione, anche attraverso una "autodichiarazione" redatta in conformità agli artt. 46 e 76

	del D.P.R. 445/2000 e comunque soggetta a verifica su richiesta da parte dell'OdC. Uniformità, valutazione e contenuti delle domande - Per lo scritto, devono essere previste griglie di correzione - Per l'orale, deve essere previsto un elenco di domande di cui un campione rappresentativo verrà sottoposto al candidato - Per la prima prova scritta la commissione di esame deve preparare un numero di domande almeno doppio rispetto a quelle presentate all'esame. Successivamente al primo esame di certificazione, il numero delle domande deve essere ulteriormente incrementato al fine di ottenere una adeguata rotazione, tale da non rischiare di riproporre gli stessi gruppi di domande negli esami successivi. Analoga impostazione dovrà essere attuata per il caso di studio da sottoporre al candidato nelle due prove (scritta e orale). Le prove che costituiscono l'intero esame, nel loro insieme, devono ricoprire, per tutti i candidati, le abilità e conoscenze fondamentali richieste dalla norma UNI 11697. Deve essere garantito l'aggiornamento continuo delle domande in base all'evoluzione del contesto normativo e tecnologico. Per quanto riguarda la formazione specifica (corso e durata), si conferma che ci si deve attenere a quanto scritto nell'Appendice B della norma, alla luce del punto 4.1[2]. Il numero di ore complessivo può quindi essere raggiunto anche con più corsi di formazione e/o con la partecipazione a seminari o con l'effettuazione di docenza specifica. Criteri per il superamento dell'esame Per superare l'esame il candidato deve ottenere almeno un punteggio del 65% nelle singole prove, rispetto al punteggio massimo previsto per ogni prova. Qualora il candidato non abbia concluso con esito positivo l'esame le eventuali singole prove superate rimangono valide per 12 mesi.
Certificazione per più profili	Il candidato che - in possesso dei necessari prerequisiti - richieda la certificazione per più profili nella medesima sessione deve sostenere l'esame completo per il più alto dei profili per cui fa richiesta, secondo la seguente classificazione (dal più alto al più basso): • Responsabile della protezione dei dati • Manager Privacy • Valutatore Privacy • Specialist Privacy *Nota: la classificazione riportata non vuole suggerire una gerarchia nella importanza dei profili o nella complessità dei compiti, ma è tesa a dare una indicazione operativa all'OdC.* All'esame completo vanno aggiunte: • 10 domande a risposta multipla per ogni profilo oltre al primo; • Un esame scritto su 1 "caso di studio" per ogni profilo oltre al primo;

[2] Punto 4.1: *"Ove dei professionisti abbiano già eseguito precedenti percorsi di formazione, non coincidenti con le indicazioni di questa norma sarà cura dell'OdC effettuare una analitica comparazione tra il percorso già seguito dal candidato alla certificazione ed il percorso illustrato in questa norma, assumendosi le responsabilità relative*".

	• Minimo 15 minuti di esame orale per ogni profilo oltre al primo. Il candidato che, già certificato per almeno un profilo, richieda la certificazione per altri profili (escluso il Responsabile della protezione dei dati), in una sessione successiva, dovrà sostenere: • 20 domande a risposta multipla per ogni profilo oltre al primo; • Un esame scritto su 1 "caso di studio" per ogni profilo oltre al primo; • Esame orale della durata minima di 20 minuti per ogni ulteriore profilo. Il candidato che, già certificato per almeno un profilo, richieda la certificazione per il Responsabile della protezione dei dati, in una sessione successiva, dovrà sostenere: • 30 domande a risposta multipla per ogni profilo oltre al primo; • Un esame scritto su 2 "casi di studio"; • Esame orale della durata minima di 30 minuti. L'OdC deve dotarsi di istruzioni, griglie o procedure per garantire che gli esami integrativi coprano le conoscenze e le abilità specifiche di ogni profilo e per assicurare l'uniformità nella valutazione.
Sorveglianza annuale (esame documentale)	L'Organismo di Certificazione deve effettuare durante il ciclo di certificazione delle verifiche per mantenere e confermare la validità delle certificazioni emesse. La verifica documentale può essere effettuata in assenza del candidato e riguarderà i seguenti documenti: 1) almeno un incarico/attività/contratto attraverso il quale si dimostri di aver operato nell'ambito dei compiti richiamati dalla Norma UNI; 2) la dimostrazione tramite titoli (attestati/contratti/registri partecipazione e similari) di partecipazione ad attività di formazione / convegni / docenze / relazioni / gruppo di lavoro normativo o tecnico, durante l'anno, finalizzate al mantenimento delle competenze specifiche per la certificazione posseduta, per almeno 16 ore/anno per il DPO, e 8 ore per gli altri 3 profili. 3) un'"autodichiarazione" ai sensi degli artt. 46 e 76 del D.P.R. 445/2000 contenente: a) le attività svolte, di cui al punto 1 rispetto ai punti 4 e 5 della norma UNI 11697:2017, specifiche nel campo della protezione dati, durante l'anno; b) l'elenco completo, di cui al punto 2, dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze, inerenti gli argomenti relativi nel settore della privacy come declinato nelle tabelle riepilogative per profilo c) la presenza di reclami relativi all'attività certificata; d) la presenza di contenziosi legali in corso relativi all'attività certificata. e) pagamento regolare delle quote annuali dovute all'Organismo di certificazione, se previste Nel caso in cui siano presenti reclami o contenzioni legali spetta all'OdC valutarne la relativa gestione. L'attività di sorveglianza può avere come esito il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione

	dell'OdC in merito alla completezza, congruità della documentazione presentata nonché gestione di eventuali reclami e/o contenziosi legali.
Rinnovo (esame documentale, esame scritto ed eventuale orale)	L'Organismo di Certificazione, al termine del ciclo di certificazione, deve condurre delle verifiche per rinnovare la validità delle certificazioni emesse. Oltre a raccogliere le evidenze già previste per l'attività di sorveglianza, l'organismo deve assicurarsi che siano mantenute le competenze previste dal punto 5 della norma UNI 11697:2017. In sede di rinnovo deve essere prevista una prova scritta composta da domande a risposta multipla, strutturato come l'esame di certificazione (rimangono invariati anche i criteri per il superamento dell'esame). Nel caso in cui il candidato non superasse questa prima prova, può ripeterla in una sessione d'esami successiva (se la certificazione non è già scaduta), ripetendo la prova scritta composta da domande a risposta multipla ma con l'aggiunta dell'esame scritto sui casi di studio, strutturato come l'esame di certificazione (rimangono invariati anche in questo caso i criteri per il superamento dell'esame). In caso di esito negativo anche di questa seconda prova, è necessario effettuare un esame completo di prima certificazione (domande a risposta multipla, casi di studio e orale).
Trasferimento del certificato	Il trasferimento di un certificato rilasciato ad una persona fisica, può essere perfezionato in qualsiasi momento, presentando all'OdC subentrante una richiesta, allegando il certificato in corso di validità, e sostenendo l'esame orale con la metodologia richiamata nel presente schema di certificazione. Devono essere presentate dal candidato al nuovo Organismo anche i documenti applicabili per la sorveglianza. Il candidato deve anche fornire l'evidenza di chiusura di eventuali pendenze (economiche e tecniche) aperte dall'Organismo precedente nei suoi confronti. Il certificato emesso manterrà la scadenza di quello precedente.
Centro d'Esame	Affidarsi ad un centro d'esame esterno al proprio Organismo, eventualmente situato presso i locali di un'associazione o di un ordine professionale, costituisce una possibile minaccia al principio dell'imparzialità (si vada anche quanto previsto dal RG-01-02), che l'Organismo deve gestire adeguatamente (analisi dei rischi). In particolare, si richiede che le date d'esame vengano comunicate con adeguato anticipo all'Organismo, perché questo possa pianificare delle verifiche anche non annunciate o verifiche in incognito (mistery). Gli audit (compresi quelli non annunciati e in incognito) presso il Centro d'esame devono essere previsti contrattualmente negli accordi tra il centro d'Esame e l'Organismo. Spetta all'Organismo determinarne, in base al rischio identificato, la frequenza e la modalità. L'Organismo deve avere inoltre a disposizione (e rese disponibili all'Ente di Accreditamento su richiesta) le statistiche degli esiti degli esami erogati nei vari centri d'esame, perché possano essere valutati eventuali scostamenti.

	La qualifica dei Commissari d'Esame deve essere gestita dall'organismo. Per gli esami in remoto / on line si rimanda a quanto previsto dal RG-01-02.
Migrazione	Gli OdC che abbiano rilasciato certificazioni (fuori accreditamento ACCREDIA prima o dopo la pubblicazione della norma UNI 11697), secondo schemi proprietari, di profili professionali in ambito protezione dati, devono effettuare un'analisi comparativa per ciascun profilo certificato rispetto a quello corrispondente UNI che evidenzi l'eventuale scostamento fra i requisiti di accesso, le conoscenze, competenze e abilità richieste, le modalità di svolgimento e i contenuti degli esami. Tale analisi deve essere sottoposta alla valutazione di ACCREDIA, assieme alla documentazione prevista per l'accreditamento, per definire eventuali percorsi differenziati e semplificati per la certificazione secondo la norma UNI delle persone in possesso di certificazioni pregresse.
Valutazione dei risultati dell'apprendimento	Il punto 6 della UNI 11697 richiama una combinazione di più metodi di valutazione, riportati di seguito con alcune note di chiarimento. Si rimanda ai singoli profili professionali riportati nel paragrafo a seguire per comprendere quali di questi metodi siano applicabili e obbligatori.

N°	Metodo di valutazione	Note di chiarimento
1	Analisi e valutazione del "curriculum vitae	Deve essere integrato da documentazioni comprovanti le attività lavorative e formative dichiarate dal candidato
2	Esame scritto per la valutazione delle conoscenze	L'esame scritto consiste in una serie di domande a risposta chiusa ciascuna delle quali ha almeno 4 possibili risposte, di cui una sola corretta (domande a risposta multipla). Le domande devono coprire gli elementi fondamentali di abilità e conoscenza previsti dalla norma UNI 11697 per lo specifico profilo. Per la risposta possono essere concessi al massimo 2 minuti a domanda. Durante l'esame il candidato può consultare la norma UNI 11697 e il Regolamento (UE) 2016/679 (ed eventuali successive modifiche).
3	Esame scritto su "casi di studio"	Al candidato verrà sottoposto un caso di studio volto a verificare l'attitudine, le abilità, le competenze e le conoscenze del medesimo su questioni pratiche connesse al profilo professionale oggetto di certificazione. Il caso di studio deve prevedere 4 possibili risposte, di cui una sola corretta (domande a risposta multipla). Per la risposta per l'esame scritto su "casi di studio" possono essere concessi al massimo 10 minuti per ogni caso di studio.
4	Esame orale	È necessario per approfondire eventuali incertezze riscontrate nelle prove scritte e/o per approfondire il livello delle conoscenze acquisite dal candidato in tutte le aree previste dalla Norma UNI 11697, per le diverse figure professionali. Durante l'esame orale si devono anche prevedere: • Simulazioni di situazioni reali operative (Es: casi di studio, esercitazioni, role-play, simulazioni…), per valutare oltre alle abilità e alle competenze, anche le capacità personali (per esempio, capacità relazionali, comportamenti personali

		attesi). • Analisi e valutazione di lavori effettuati. Questo metodo comprende anche un confronto, in presenza del candidato, per approfondire la valutazione delle abilità, delle conoscenze e delle capacità relazionali.

Modalità di svolgimento dell'esame

Si riportano di seguito ulteriori informazioni sui metodi di valutazione, con l'indicazione di quali di questi metodi siano applicabili e obbligatori ai vari profili.

N°	Profili professionali	Metodo di valutazione
1	Responsabile della protezione dei dati personali	• Esame del curriculum vitae e dei prerequisiti previsti dalla norma • Una prova scritta composta da almeno 40 domande a risposta multipla • Esame scritto su almeno 3 casi di studio. • Esame orale dalla durata minima di 40 minuti (compreso la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
2	Manager Privacy	• Esame del curriculum vitae e dei prerequisiti previsti dalla norma • Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 3 casi di studio. • Esame orale dalla durata minima di 40 minuti (compreso la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
3	Specialista privacy	• Esame del curriculum vitae e dei prerequisiti previsti dalla norma • Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 2 casi di studio. • Esame orale dalla durata minima di 30 minuti (compreso la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)
4	Valutatore Privacy	• Esame del curriculum vitae e dei prerequisiti previsti dalla norma • Una prova scritta composta da almeno 35 domande a risposta multipla • Esame scritto su almeno 2 casi di studio. • Esame orale dalla durata minima di 30 minuti (compreso la simulazione di situazioni reali operative, della durata di circa 10 minuti, e l'analisi e la valutazione di lavori effettuati)

2) Processo di Accreditamento

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.

Rimangono invariati i prerequisiti previsti dal RG-01 e RG-01-02 per la concessione dell'accreditamento ed estensione.

Nel caso in cui l'OdC possegga già accreditamenti rilasciati da altri enti di accreditamento, dovrà essere fatta una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili ed a quanto eventualmente disposto dalle Autorità competenti in materia.

A	OdC già accreditato per lo schema ISO/IEC 17024	Esame documentale di 1 giornata (da svolgersi possibilmente presso l'OdC). Osservazione di 1 sessione d'esame (la sessione d'esame può essere relativa anche a più profili previsti dalla norma UNI). L'accreditamento per ogni singola figura prevista dalla norma UNI viene concesso solo a seguito di osservazione diretta di quella singola figura (non è quindi ammesso ottenere l'accreditamento in una figura professionale di cui non è stato osservato almeno un esame. Non si applica cioè l'accreditamento flessibile).
B	OdC non ancora accreditato ISO/IEC 17024, ma accreditato per altri schemi di accreditamento	Oltre a quanto riportato al punto A, occorre svolgere una verifica ispettiva presso la sede dell'OdC di 2 giornate.
C	OdC non ancora accreditato in nessuno schema	Oltre a quanto riportato al punto A, occorre svolgere una verifica ispettiva presso la sede dell'OdC di 4 giornate.

Documentazione da presentare ad ACCREDIA per l'esame documentale (nel caso di OdC che richieda l'estensione)

a) Procedure o istruzioni interne predisposte dall'Odc per la gestione dello schema oggetto della presente circolare
b) Procedure / regolamenti contrattuali applicabili per questo schema;
c) Criteri di qualifica dei commissari d'esame e dei *decision maker*;
d) *Curricula* dei commissari d'esame e dei *decision maker* e le motivazioni in base alle quali l'Organismo ha assegnato tale ruolo/incarico;
e) Fac-simile di Certificato rilasciato dall'OdC;
f) Lista dei certificati già emessi per i vari profili, e elenco dei prossimi esami (dato necessario per poi pianificare l'osservazione dell'esame);
g) Per gli OdC NON accreditati ISO/IEC 17024, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

Ove l'Organismo di Certificazione richieda il primo accreditamento, valgono i documenti elencati nelle specifiche domande DA-00 e DA-01.

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, implicazioni in cause giudiziarie…), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso fino a 20 certificati in questo schema di certificazione considerando tutti i profili per cui è accreditato, devono essere osservato 1 esame su almeno 1 profilo e condotta una verifica in sede specifica per questo schema;
- se l'OdC ha emesso tra 21 e 200 certificati in questo schema di certificazione considerando tutti i profili per cui è accreditato, devono essere osservati 2 esami su

almeno 2 profili differenti e condotta una verifica in sede specifica per questo schema;

- se l'OdC ha emesso più di 200 certificati in questo schema di certificazione considerando tutti i profili per cui è accreditato, devono essere osservati 2 esami su almeno 2 profili differenti e condotte 2 verifiche in sede specifiche per questo schema;

Si conferma che comunque ACCREDIA ogni anno deve condurre una verifica presso la sede Organismi di certificazione per valutare la conformità alla ISO/IEC 17024.

Siamo a disposizione per chiarimenti e con l'occasione Vi porgiamo cordiali saluti.

Dott. Emanuele Riva
Direttore Dipartimento Certificazione e Ispezione