CIRCOLARE TECNICA Prot. DC2024SPM086 **DATA** Milano, 16-05-2024

A tutti i CAB accreditati per gli schemi PRD

Alle Associazioni degli Organismi di valutazione della conformità

A tutti gli Ispettori/Esperti di Accredia

Loro sedi

OGGETTO **Dipartimento Certificazione e Ispezione**

Circolare tecnica DC N° 17/2024 - Disposizione in merito all'accreditamento per lo schema DSEEDC a fronte della Serie ISO/IEC 22237 – Disponibilità, Sicurezza, Efficienza Energetica dei Data Center.

Il presente documento annulla e sostituisce la circolare tecnica DC N° 42/2022 del 15/11/2022

INTRODUZIONE

L'attuale scenario del mercato dell'UE rende sempre più centrale il tema della gestione dei dati. In questo ambito ha assunto un'importanza strategica anche la gestione delle strutture deputate a svolgere attività di "Data Center".

A questa esigenza dà una risposta efficace la serie di Norme ISO/IEC 22237, che comprende sette diverse Norme specializzate.

Le aree disciplinate sono rispettivamente:

- ISO/IEC 22237-1:2021 - Part 1: General concepts;
- ISO/IEC 22237-2:2024 - Part 2: Building construction;
- ISO/IEC 22237-3:2021 - Part 3: Power distribution;
- ISO/IEC 22237-4:2021 - Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 - Part 5: Telecommunications cabling infrastructure;
- ISO/IEC 22237-6:2024 - Part 6: Security systems;
- ISO/IEC TS 22237-7:2018 - Part 7: Management and operational information.

SEDE LEGALE
Via Guglielmo Saliceto, 7/9
00161 Roma
T +39 06 8440991
F +39 06 8841199
accredia.it / info@accredia.it
C.F. / P. IVA 10566361001

SEDE OPERATIVA E AMMINISTRATIVA
Via Tonale, 26
20125 Milano
T +39 02 2100961
F +39 02 21009637
milano@accredia.it

CONTESTO NORMATIVO

La Serie ISO/IEC 22237, nelle sue diverse specializzazioni, si inserisce in un contesto che era già oggetto di presidio della Normazione Europea, attraverso la Norma precorritrice EN 50600, anch'essa strutturata in più documenti, pubblicata nel 2010 e, successivamente, aggiornata nel 2014.

Questa serie di norme, a tutt'oggi valida, offre ora una copertura completa per le migliori pratiche per i data center, dagli standard di progettazione, inclusi alimentazione, raffreddamento, telecomunicazioni e sicurezza (compresa la sicurezza contro gli incendi), agli standard operativi con attenzione agli aspetti di efficientamento energetico.

Si tratta di una Serie omnicomprensiva, che tratta di tutti gli aspetti tecnici inerenti il governo di un Data Center; essa riceve in eredità - dalla precedente EN 50600 - la struttura modulare e anche la specializzazione dei contenuti, ma assume maggiore rilevanza trattandosi di normazione internazionale.

La Serie non è riferibile alla famiglia HLS, tipicamente certificabile con un approccio da sistema di gestione, bensì risulta idonea per una certificazione di prodotto, secondo la Norma di Accreditamento UNI CEI EN ISO/IEC 17065:2012.

Processo di Certificazione

REGOLE DI CERTIFICAZIONE	
Norma di Certificazione	Serie ISO/IEC 22237 nella sua completezza così come sopra delineata.
Soggetti che possono richiedere la certificazione	La valutazione di conformità può essere richiesta da qualunque Organizzazione, di qualsiasi dimensione e/o forma giuridica, il cui oggetto sociale o ambito di applicazione sia afferente alla progettazione, realizzazione e gestione di Data Centers così come delineato dalla serie IEC 22237. Non è fatto obbligo la sussistenza di ulteriori certificazioni come prerequisito di accesso, tuttavia qualora l'Organizzazione sia già in possesso di una certificazione accreditata in ambito EA/IAF MLA del sistema di gestione in accordo alla ISO 9001, ISO/IEC 27001 e ISO 22301, nelle revisioni vigenti, è possibile applicare delle riduzioni sui tempi di audit.
Requisiti dello schema di certificazione	Nel predisporre e mantenere lo schema di certificazione, l'Organismo deve considerare i seguenti elementi: a. Per la fase progettuale, devono essere considerate le modalità previste (adeguatezza delle scelte progettuali) per rendere operativi tutti i requisiti Normativi, in conformità ai seguenti punti: i. Valutazione delle scelte progettuali a fronte dei requisiti Normativi e del tipo di servizio offerto;

	ii. Valutazione sulle modalità adottate per provvedere alla valutazione dei rischi ipotizzabili in sede progettuale (analisi dei rischi del processo di progettazione e dei processi di supporto); iii. Valutazione delle modalità previste per la formazione, coinvolgimento e consapevolezza delle Risorse Umane, in funzione dei rischi inerenti i processi nei quali saranno coinvolte; iv. Valutazione delle modalità previste per la selezione dei fornitori che provvederanno alle diverse fasi di realizzazione del Data Center, dal punto di vista della sicurezza (humint) e modalità previste per il loro monitoraggio; v. Valutazione delle modalità adottate per individuare e mantenere sotto controllo (mantenimento delle registrazioni) delle forniture di beni che richiedono certificazioni di prodotto (es.: marcature CE; livelli di attenuazione del segnale; livelli di efficienza ambientale/energetica; certificazioni di sicurezza IoT, per quanto applicabile); vi. Procedure di collaudo presidiato, reportistica richiesta (es.: test memoranda su materiali installati e su funzionamento e prestazioni); vii. Modalità adottate per garantire l'ispezionabilità, manutenibilità e sicurezza antintrusione delle infrastrutture, ivi compresi i cavedi; viii. Sviluppo di adeguate "Policies" per la realizzazione e l'esercizio di SOC e NOC dedicati al Data Center. b. Per la fase operativa, sono previsti 4 livelli di maturità nell'applicazione così come definiti dalla ISO/IEC TS 22237-7, di cui i soli livelli 3 e 4 sono certificabili. 2. Dovranno essere oggetto di valutazione, nell'ambito indicato, tutte le Norme della serie 22237 (da 1 a 7), senza esclusioni. L'estensione della Certificazione e relativo Accreditamento a tutte le Norme indicate è supportata, dal fatto che i relativi requisiti siano richiamati e ritenuti funzionali all'applicazione di tutte le Norme citate sia integralmente, sia in modo incrociato come segue: a. ISO/IEC 22237-1 richiama la ISO/IEC 22237-6; b. ISO/IEC 22237-2 richiama le ISO/IEC 22237-3, 4 e 6; c. ISO/IEC 22237-3 richiama le ISO/IEC 22237-1,4 e 6; d. ISO/IEC 22237-4 richiama le ISO/IEC 22237-1,3 e 6; e. ISO/IEC TS 22237-5 richiama le ISO/IEC 22237-1, 2, 4 e 7; f. ISO/IEC 22237-6 richiama le ISO/IEC-1, 2, 3, 4, 5; g. ISO/IEC TS 22237-7 richiama tutte le precedenti;

3. Tutte le Norme richiamano la filosofia applicativa che vede nella ISO/IEC 22237-7 il riferimento per la chiusura del ciclo di controllo operativo (anello cibernetico a ciclo chiuso, approccio di DEMING);
4. Nel caso di Data Center strutturati su più unità operative, tutte le unità dovranno essere oggetto di valutazione. La valutazione dell'aderenza ai diversi requisiti normativi deve prevedere una logica di campionamento robusta, atta a garantire la verifica dell'operatività di tali unità satellite, prevedendo il test dei controlli operativi che mitigano i rischi maggiori in ottica di efficacia del Data Center;
5. Il processo di Audit deve prevedere la verifica di tutti i requisiti Normativi, con focus primario sulle logiche di "risk management", che debbono essere basate sulla Norma (Guida) ISO 31000 e prevedere una valutazione di accettazione del rischio residuo funzionale al livello di operatività atteso e dichiarato del Data Center. Sulla base di tale valutazione dovranno essere progettati e sviluppati i controlli operativi. Tale campionamento robusto deve consentire di valutare in modo inequivocabile le strutture e le loro prestazioni. Il campionamento dei requisiti deve garantire la rappresentatività nei confronti di tutto il Data Center, la presa in carico di parametri prestazionali (KPI e KRI), che evidenzino la validità delle scelte di governo dei processi. Il campionamento deve tener conto dei diversi aspetti governati (ambientali e di security in primo luogo), i processi che li gestiscono e i siti ove vengono realizzati tali risultati. Tali valutazioni dovranno essere riferite a tutti i requisiti delle sette Norme di riferimento, dando evidenza dei criteri utilizzati per l'individuazione degli obiettivi, dei risultati chiave che li sostengono, dei relativi KPI e KRI e, infine, dell'effettivo livello di raggiungimento degli obiettivi medesimi. Tutto ciò deve essere rendicontato dai CAB in ottica di conformità e di adeguatezza alle politiche dichiarate e rese pubbliche dalla Direzione;
6. Ove vi siano dei processi gestiti in outsourcing (es. manutenzioni) la direzione del Data Center deve dare evidenza dei criteri e strumenti adottati per garantire il controllo di tali processi, sui quali mantiene la completa responsabilità;
7. Svolgimento di una validazione delle metodiche di valutazione dei rischi delle quali la direzione del Data Center si sarà dotata. Le indicazioni di buona tecnica per lo sviluppo della valutazione dei rischi dovranno essere individuate, in modo pertinente, tra quelle riportate dalla Norma (Guida Tecnica) ISO 31010;
8. Le tecniche di valutazione adottate dai CAB dovranno prevedere sia valutazioni documentali, sia de visu, sia interviste alle Risorse Umane che operano presso il Data Center, ivi comprese quelle dei processi dati in outsourcing (vedi il precedente § 4);

	9. Il business del Data Center può prevedere in alternativa: a. Servizio di base, quale la semplice messa a disposizione di spazi, security antintrusione, alimentazione e raffrescamento e cablaggio interno al Data Center sino all'attestazione all'interfaccia con i "carrier" o con gli ISP individuati dal Cliente. Questo tipo di servizio prevede sotto la responsabilità del Data Center la realizzazione del cablaggio di connessione sino allo switch, a cui il Cliente connette le proprie macchine; b. L'erogazione di servizi avanzati, che comprendono il servizio base e la connettività (servizi di comunicazione "carrier telefonici o ISP") o l'erogazione di Servizi Cloud "aaS". Tali casistiche ricomprendono anche il ricorso a Vulnerability Assessment condotti, a frequenze stabilite e motivate, da laboratori accreditati o qualificati dall'OdC (si veda RG-01-03) e, sulla base delle indicazioni desumibili dalla valutazione dei rischi, anche degli specifici Penetration Test. In particolare, per l'erogazione dei servizi Cloud è raccomandabile la conduzione della valutazione dei rischi - già menzionate - ai fini della selezione e applicazione dei controlli operativi così come richiamati dalle Norme (Guide) ISO/IEC 27017 e ISO/IEC 27108. 10. Prevedere un processo di valutazione dinamico dei fornitori di servizi critici per il Data Center a fronte delle Norme individuate in questa Circolare.
Possibili esclusioni	Lo schema non prevede esclusioni.
Criteri di competenza del personale coinvolto nel processo di certificazione	Gli Auditor devono essere qualificati a livello tecnico dagli stessi CAB sulla base dei seguenti elementi minimi: • Conoscenza della norma UNI EN CEI ISO/IEC 17065 e delle procedure di certificazione dell'Organismo; • Superamento di corsi di formazione specialistici sulla serie IEC 22237; • Esperienza in ambito informatico e della sicurezza delle informazioni di almeno 5 anni documentata attraverso progettazione/validazione o consulenza o auditing su data center e relativi domini previsti dalla serie IEC 22237 o standard similari (a mero titolo di esempio: ANSI TIA 942, EN 50600, BICSI 002). Il personale incaricato per la gestione contrattuale o la decisione deve avere le medesime conoscenze degli Auditor, ma non necessariamente il medesimo livello di esperienza.

Tempi di audit	È responsabilità dell'Organismo disporre di procedure armonizzate per: a. il calcolo delle durate di audit, tenendo in considerazione anche l'assistenza ai test sui controlli operativi e le fasi documentali condotte eventualmente in modalità off-site; b. distribuzione delle giornate di audit su più siti di certificazione e relativo campionamento nel ciclo di certificazione; Alla luce delle esperienze fatte si ritiene utile raccomandare un audit time minimo di 8 gg/u per singolo sito finalizzato alla valutazione iniziale dei requisiti di cui alle norme di certificazione. Sulla scorta di un'opportuna valutazione del rischio, l'Organismo può applicare riduzioni qualora sussistano pertinenti certificazioni accreditate per il sistema di gestione in accordo alle norme ISO 9001, ISO/IEC 27001 e ISO 22301.
Modalità di svolgimento dell'audit	La documentazione di audit dovrebbe tener conto, fra le altre registrazioni, anche di quanto segue: ▪ il perimetro e l'applicabilità ISO/IEC 22237; ▪ la mappatura dei processi (interni ed esterni) e l'elenco delle relative leggi, Norme e regolamenti applicabili; ▪ la valutazione dei rischi per il campo di applicazione specifico del Data Center, con riferimento a tutti i processi ivi compresi quelli affidati in outsourcing; ▪ l'analisi degli "incidents" e "problems" già occorsi, completata dalla valutazione sulle modalità di gestione previste e adottate, alla luce delle indicazioni delle Autorità (EDPB – Garante per la protezione dei Dati Personali) e delle Norme (Guide) esistenti applicabili, ad esempio, ISO/IEC 27035 e ISO/IEC 27043; ▪ La definizione ragionata degli obiettivi, dei risultati chiave che li sostengono, dei relativi KPI e KRI e le relative attività di pianificazione.
Scopo del certificato	Oltre a quanto stabilito dalla UNI CEI EN ISO/IEC 17065, nel riportare le norme di certificazione complete di anno di revisione, l'Organismo deve formulare il seguente scopo di certificazione: *Disponibilità, sicurezza fisica, logica e organizzativa, efficienza energetica delle infrastrutture e processi di supporto dei Data Center [XXX] costituito da: [Sito principale; sito secondario; sito secondario…].*
Documenti IAF applicabili	IAF MD 01, 02, 04 in revisione vigente.

PROCESSO DI ACCREDITAMENTO

Le verifiche necessarie per il rilascio di certificazioni ISO/IEC 22237 devono essere condotte da Organismi di certificazione accreditati secondo la Norma UNI CEI EN ISO/IEC 17065:2012.

Il certificato di accreditamento è rilasciato senza alcuna limitazione settoriale.
Nel caso in cui il CAB possegga già accreditamenti rilasciati da altri Enti di Accreditamento, deve essere effettuata una valutazione caso per caso, in base agli accordi EA/IAF MLA applicabili.
Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-03 per la concessione dell'accreditamento ed estensione, integrati dalle seguenti regole.
Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione, come segue:

ITER DI ACCREDITAMENTO/ESTENSIONE		
A	CAB già accreditato in conformità alle Norme UNI CEI EN ISO/IEC 17065:2012 e ISO/IEC 17021-1:2015 per gli schemi SSI e BCMS	• Esame documentale di 1 gg/uomo (da effettuarsi, almeno in parte, in remoto). • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
B	CAB già accreditato in conformità alla Norma UNI CEI EN ISO/IEC 17065:2012 ma non per la ISO/IEC 17021-1:2015 per gli schemi SSI e BCMS	• Esame documentale di 1 gg/uomo (da effettuarsi, almeno in parte, in remoto). • Verifica presso la sede del CAB di 2 gg/uomo, da effettuarsi o in presenza o da remoto. • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
C	CAB non accreditato	• Esame documentale di 1 gg/uomo (da effettuarsi, almeno in parte, in remoto). • Verifica presso la sede del CAB di 4 gg/uomo, da effettuarsi o in presenza o da remoto. • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.

DOCUMENTAZIONE DA PRESENTARE AD ACCREDIA PER L'ESAME DOCUMENTALE

Oltre a quanto richiesto nelle Domande DA-00 e DA-01 per la conduzione dell'esame documentale devono essere presentati:

a) Lista di riscontro e linea guida o istruzioni predisposte dall'OdC per il GVI;
b) Criteri di qualifica di chi effettua il riesame del contratto, degli auditor e dei decision maker;
c) Curricula degli auditor e dei decision maker completi delle evidenze a supporto per la loro singola qualifica.

MANTENIMENTO DELL'ACCREDITAMENTO

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (es.: trend di certificati rilasciati, gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo o altre situazioni similari), essendo uno schema ad alta complessità, ACCREDIA-DC effettuerà almeno 2 verifiche in sede ed 1 Verifica in accompagnamento.

L'occasione è gradita per porgere cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da:
EMANUELE RIVA
Data: 16/05/2024 12:07:50