Prot. DC2018SSV022 Milano, 12-02-2018

A tutti gli Organismi di Certificazione accreditati ISO/IEC 17021

Alle Associazioni degli Organismi di valutazione della conformità

Vostra mail

Oggetto: **<u>Dipartimento DC - Circolare Tecnica N° 02/2018</u>**
Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 270XX:20YY "Information Technology, Security techniques, Code of practice"

Introduzione

Con la diffusione del **Cyber Crime** sono aumentate le preoccupazioni dei clienti per la trasparenza, la riservatezza e la disponibilità sui servizi erogati; i clienti spesso non sono a conoscenza di come sono protette le informazioni archiviate e dove sono localizzate.

Sulla spinta della Commissione Europea, delle Autorità Nazionali e delle Commissioni per la protezione dei dati, ISO e IEC hanno quindi sviluppato delle nuove linee guida per la protezione delle informazioni, alcuni esempi:

1. ISO/IEC 27108:2014 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors);
2. ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services";
3. ISO/IEC 27011:2016 Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations;
4. ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity;
5. ISO 27799:2016 Health informatics -- Information security management in health using ISO/IEC 27002;
6. ISO/IEC TR 27019:2013 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

Contesto Normativo

Le linee guida a livello internazionale sono state sviluppate per contribuire a garantire il rispetto dei principi e delle sicurezza delle informazioni, da parte dei fornitori di servizi che se ne dotano.

Definiscono delle linee guida basate sulla ISO/IEC 27002, prendendo in considerazione i requisiti normativi per la protezione delle informazioni che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi.

Trattandosi di Linee guida, le norme ISO/IEC 270XX NON sono quindi certificabili. Ciò nonostante, è possibile ottenere una integrazione di un certificato ISO/IEC 27001 esistente e rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati, basato sulla integrazione delle Linea Guida citata con la Norma ISO/IEC 27001. Le linee guida si basano e rinforzano i precedenti standard ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni, e stabiliscono obiettivi di controllo, regole e

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

procedure per implementare misure di protezione dei fornitori di servizi.

1) Norma e regole di Certificazione

Norma di Accreditamento	ISO 17021-1:2015, ISO/IEC 27006:2015
Norma di Certificazione	ISO/IEC 270XX:20YY come addendum alla Norma ISO/IEC 27001:2013
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: • auditor ISO/IEC 27001:2013, con esperienza specifica di audit nella ISO/IEC 27001 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. • auditor ISO 20000-1:2012, con esperienza specifica di audit nella ISO/IEC 20000 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. Deve inoltre essere data dimostrazione della conoscenza della linea guida ISO/IEC 270XX:20YY applicabile.
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli Odc la dimostrazione della: • Qualifica come ispettore ISO/IEC 27001, rilasciata in conformità alla ISO/IEC 27006 • Conoscenza della linea guida ISO/IEC 270XX:20YY applicabile
Tempi di verifica	Possono essere estese alla linea guida ISO/IEC 270XX solo organizzazioni già certificate ISO/IEC 27001. Per certificare una organizzazione a fronte di ognuna delle Norme della famiglia ISO/IEC 270XX occorre incrementare del 30% (**del tempo di Stage 1+Stage 2**) la durata dell'audit condotto per la ISO 27001. È possibile comunque condurre la verifica ISO/IEC 27001 in momenti distinti dalla verifica ISO/IEC 270XX. Prima del rilascio della certificazione devono essere verificati tutti i datacenter presso cui sono dislocati i server che gestiscono il servizio e tutti i siti ove sono ubicati asset critici ai fini dello scopo di certificazione e dei processi gestiti sotto questo. Nel caso in cui il certificato accreditato ISO/IEC 27001 sia stato rilasciato da un organismo differente, la durata dell'audit ISO/IEC 270XX deve essere pari al 50% (**del tempo di Stage 1 + Stage 2**) dell'audit ISO/IEC 27001, e l'OdC deve avere accesso ai rapporti della verifica ISO/IEC 27001.
Certificato	Deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della/e linea/e guida ISO/IEC 270XX nella sua applicazione. Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.
Documenti IAF e EA	Si applicano tutti i documenti IAF ed EA in vigore per lo schema ISO/IEC 27001.

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.

Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-01 per la concessione dell'accreditamento ed estensione.
Per organismi già accreditati ISO/IEC 27001 con ACCREDIA, non occorre che questi abbiano già rilasciato dei certificati in questo schema per fare domanda di estensione dell'accreditamento.

Il certificato di accreditamento non riporta settori di accreditamento.

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.

A	OdC già accreditato per lo schema ISO/IEC 27001	Esame documentale di 1 giornata (da svolgersi possibilmente presso la sede dell'OdC) per valutare la capacità dell'OdC di certificare a fronte delle linee guida ISO/IEC 270XX:20YY (non occorre quindi fare 1 esame documentale per ogni linea guida). 1 Verifica in accompagnamento su ogni linea guida ISO/IEC 270XX:20YY di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni scelte per l'accompagnamento ai fini del processo di accreditamento e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
B	OdC non accreditato ISO/IEC 27001	Occorre accreditarsi ISO/IEC 27001

Documentazione da presentare ad ACCREDIA per l'esame documentale

- Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
- Curricula degli ispettori e dei Decision Maker
- Modulo del Rapporto di Audit;
- Attestato/Certificato rilasciato dall'OdC;
- Lista dei certificati già emessi, e delle prossime attività di verifica (nel caso sia necessario condurre una verifica in accompagnamento)
- Procedure / regolamenti contrattuali applicabili al processo di valutazione, nonché le procedure interne per la gestione della pratica di certificazione;
- 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:

- Verifica in sede:
  - 0,5 giornate ogni anno per organismi accreditati ISO/IEC 27001 con ACCREDIA
  - 1 giornate ogni anno per organismi non accreditati ISO/IEC 27001 con ACCREDIA

- Verifica in accompagnamento, da svolgersi nel ciclo di accreditamento, in una qualsiasi delle linee guida ISO/IEC 270XX:20YY:
  - se l'OdC ha emesso fino a 50 certificati nello schema di certificazione, deve essere effettuata una verifica in accompagnamento ogni 4 anni

- se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento
- se l'OdC ha emesso più di 201 certificati nello schema, devono essere effettuate 3 verifiche in accompagnamento

Siamo a disposizione per chiarimenti.

Con cordialità.

Dott. Emanuele Riva
Direttore Dipartimento Certificazione e Ispezione