Document No.:	Revision:	Date:	Replace:	Page:
ZSEIT-5-OP-678 (I)	4	2021-03-17	3	1 of 6
Prepared by:	Reviewed by:		Approved by:	Valid for:
FVF, LUCTOM	CLB		SCL	All in DNV GL Business Assurance Italia S.r.l.

Elenco di dettaglio delle attività gestite con scopo di accreditamento flessibile (ACCREDIA)

Revisions in this document

0	*2018-06-18*	*Prima emissione*
1	*2018-09-27*	*Aggiornamento §4*
2	*2019-02-11*	- *Circolare Informativa ACCREDIA N° 01/2019* - *Pubblicazione nuova ISO/IEC 27018:2019*
3	*2019-12-16*	- *Circolare Informativa ACCREDIA N° 10/2019* - *Pubblicazione nuova ISO/IEC 27701:2019*
4	*2021-03-17*	- *Aggiornamento per cambio Organizzazione*

1. SCOPO E CAMPO DI APPLICAZIONE

La presente procedura disciplina le modalità con cui devono essere gestiti i processi interni legati alla certificazione ISO/IEC 27001:2013 e all'accreditamento flessibile (RT-37 "*Prescrizioni per l'accreditamento con scopo di accreditamento flessibile, Dipartimento Organismi di Certificazione e Ispezione*") per l'estensione della certificazione dei Sistemi di Gestione della Sicurezza delle Informazioni (SGSI) all'utilizzo delle linee guida e delle norme di settore sotto accreditamento ACCREDIA.

2. NORME E GUIDE INTERNAZIONALI DI RIFERIMENTO

1. Norma ISO: ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems;

2. Norma ISO: ISO/IEC 27006:2015 – Information Technology – Security Tecniques - Requirements for bodies providing audit and certification of Information Security Management Systems;

3. Documento IAF: IAF MD11:2013 – Mandatory Document for the application of ISO/IEC 17021 for audits of Integrated Management Systems (IMS);

4. Documento: IAF: IAF MD2:2017 - IAF Mandatory Document for the Transfer of Accredited Certification of Management Systems;

5. Documento IAF MD 1:2018 IAF Mandatory Document for the Audit and Certification of a Management system Operated by a Multi-Site Organization;

6. Circolare Tecnica N° 02/2018 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";

7. Circolare informativa N° 27/2017 Comunicazione in merito all'adeguamento delle certificazioni per lo schema SSI (UNI CEI EN ISO/IEC 27001:2017);

8. RT-37 Rev. 00 "Prescrizioni per l'accreditamento con scopo di accreditamento flessibile, Dipartimento Organismi di Certificazione e Ispezione";

9. RG-01 Regolamento per l'accreditamento degli Organismi di Certificazione, Ispezione, Verifica e Convalida- Parte Generale, nella versione vigente;

10. RG-01-01 Regolamento per l'accreditamento degli Organismi di Certificazione del Sistema di Gestione, nella versione vigente;

11. Circolare Informativa N° 01/2019 Accreditamento schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Questa Informativa annulla e sostituisce la precedente Circolare DC N° 13/2017 rif. DC2017SSV206 del 21-07-2017;

12. Circolare Informativa N° 10/2019 Disposizioni in merito all'accreditamento norma ISO/IEC 27701

3. PERSONA DI RIFERIMENTO

3.1 Riferimenti

N.	Persona	Ruolo	e-mail	Cellulare
1	*Claudia Baroncini*	*Accreditation Manager Italy*	*claudia.baroncini@dnv.com*	*+393487116826*
2	*Alessandra Scamarcio*	*Technical Manager Italy*	*Alessandra.scamarcio@dnv.com*	*+393401878942*
3	*Franco Vincenzo Ferrari*	*Scheme Manager ICT*	*franco.ferrari@dnv.com*	*+393481529229*
4	*Luca Tommasella*	*Scheme Specialist ICT*	*Luca.tommasella@dnv.com*	*+393427489538*

3.2 Responsabilità

N.	Persona	Ruolo	Responsabilità
1	*Claudia Baroncini*	*Accreditation Manager Italy*	*Responsabile della gestione degli accreditamenti con Accredia e altri Accreditation Body.*
2	*Alessandra Scamarcio*	*Technical Manager Italy*	*Responsabile Tecnico per il Country Italy*
3	*Franco Vincenzo Ferrari*	*Scheme Manager ICT*	*Responsabile Tecnico per gli schemi ISO 9001 (IAF 31b, 33), ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, WLA, eIDAS, SPID, CONSERVATORI, RT-37 (Scopo flessibile). Nel processo di gestione dello scopo flessibile definisce la famiglia delle Linee Guida per le quali il CAB intende applicare lo scopo flessibile ed è il responsabile per la gestione dell'Elenco controllato di tutti gli elementi ricompresi nello scopo flessibile.*

4	*Luca Tommasella*	*Scheme Specialist ICT*	*Supporto Tecnico Specialistico per gli schemi ISO 9001 (IAF 31b, 33), ISO/IEC 27001, eIDAS, RT-37 (Scopo flessibile).* *Nel processo di gestione dello scopo flessibile supporta la gestione della famiglia delle Linee Guida per le quali il CAB intende applicare lo scopo flessibile ed è il responsabile per la gestione dell'Elenco controllato di tutti gli elementi ricompresi nello scopo flessibile.*

3.3 Competenze

N.	Persona	Ruolo	Competenze
1	*Franco Vincenzo Ferrari*	*Scheme Manager ICT*	*Qualifica come Lead Auditor per i seguenti schemi:* *a) ISO 9001, Settori IAF 31b, 33, 19, 39 (registro IRCA);* *b) ISO/IEC 27001 (Certificato n. 29 AICQ-SICEV);* *c) World Lottery Association, WLA-SCS:2016;* *d) ISO/IEC 22301;* *e) ISO/IEC 20000-1;* *f) eIDAS, SPID, CONSERVATORI;* *g) Corso 24 h GDPR Privacy Specialist AICQ-SICEV;*
2	*Luca Tommasella*	*Scheme Specialist ICT*	*Qualifica come Lead Auditor per i seguenti schemi:* *a) ISO 9001, Settori IAF 33;* *b) ISO/IEC 27001;* *c) eIDAS;*

4. ELENCO LINEE GUIDA E NORME OGGETTO DELL'ACCREDITAMENTO

L'elenco delle Linee Guida e delle Norme che sono sotto l'accreditamento, come estensione del campo applicativo della ISO/IEC 27001:2013 sono:

N.	*LINEA GUIDA*	*DATA emissione*	*DESCRIZIONE*	*NOTE*
1	*ISO/IEC 27018:2019*	*2019/01*	*"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*	*2015/12/15*	*"Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services"*	-
3	*ISO/IEC 27035-1:2016*	*2016/11/01*	*"Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management"*	-
4	*ISO/IEC 27035-2:2016*	*2016/11/01*	*"Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response"*	-
5	*ISO/IEC 27701:2019*	*2019/08*	*"Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines"*	-

In relazione alla circolare ACCREDIA n. 01/2019:

La Norma 27017:2015 può essere oggetto di estensione della certificazione anche da sola.
Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018.

Dalla data di entrata in vigore della presente circolare, non è ammessa l'estensione alla sola Norma ISO/IEC 27018.

In relazione alla circolare ACCREDIA n. 10/2019:

Il certificato deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della norma ISO/IEC 27701 nella sua applicazione.
Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.

5. SVILUPPO DELLO SCHEMA DI ACCREDITAMENTO

Lo sviluppo dello schema di accreditamento è il seguente:

N.	DESCRIZIONE	OWNER	NOTE
1	*Raccolta esigenze di sviluppo di inserimento di nuove Linee Guida o norme.*	*Scheme Manager ICT, Scheme Specialist ICT, Key Customer Manager, Commercial Customer Manager, Enterprise Customer Manager, Enterprise Customer Sales Manager*	*Le esigenze si sviluppano dal mercato maturate per richieste di gare o da parte di AgID.*
2	*Aggiornamento documento ZSEIT-5-OP-678 (I) per inserimento nuova Linea Guida o norme al §4.*	*Scheme Manager ICT, Scheme Specialist ICT*	-
3	*Predisposizione Checklist per nuova Linea Guida o norme*	*Scheme Manager ICT, Scheme Specialist ICT*	-
4	*Predisposizione test dopo self-training*	*Scheme Manager ICT, Scheme Specialist ICT*	-
5	*Predisposizione tool ProProf (test)*	*Competence Manager Italy*	-
6	*Lancio self-training e test per tutti gli Auditor / Lead Auditor qualificati*	*Scheme Manager ICT, Scheme Specialist ICT & Competence Manager Italy*	-
7	*Gestione casi di non superamento test, con intervista.*	*Scheme Manager ICT, Scheme Specialist ICT*	-
8	*Discussione problematiche, modalità di approccio, approfondimenti durante i Calibration ICT annuali.*	*Scheme Manager ICT, Scheme Specialist ICT*	-

6. QUALIFICA DELLE PERSONE CHE EROGANO LE ATTIVITA'

Il personale che eroga queste attività deve avere le seguenti competenze:

N.	DESCRIZIONE	NOTE
1	*Essere qualificato come Auditor / Lead Auditor ISO/IEC 27001:2013*	*Auditor ISO/IEC 27001:2013, con esperienza specifica di audit nella ISO/IEC*

		*27001 di almeno **5 anni**, preferibilmente in possesso di certificazione professionale.*
2	*Ha svolto una attività di autoformazione sulla linea guida o norma specifica, con sottoscrizione di una self-declaration*	*-*
3	*Ha superato il test relativo alla linea guida o norma specifico*	*Utilizzo piattaforma ProProf*

6.1. COMPETENZE DELLE PERSONE CHE EROGANO LE ATTIVITA' PER LA ISO/IEC 27701

N.	***DESCRIZIONE***	***NOTE***
1	*Per le organizzazioni che operano con servizi "cloud" deve inoltre essere data dimostrazione della conoscenza delle norme ISO/IEC 27017 e ISO/IEC 27018 e della normativa in tema di GDPR. Si ritiene soddisfatto questo requisito per il personale certificato sotto accreditamento a fronte della UNI 11697.*	-
2	*Conoscenza del GDPR (es: almeno 24 ore di formazione documentata in materia di protezione dei dati personali), o altra legislazione applicabile al Paese oggetto di audit. Per attività svolte in Italia, si ritiene soddisfatta questa condizione per figure professionali certificate sotto accreditamento in base alla UNI 11697, o altra normativa equivalente.*	-
3	*Conoscenza degli elementi caratterizzanti la gestione della qualità o dei servizi IT (es. ISO 9001, ITIL, ISO/IEC 20000-1.*	-

7. ASPETTI COMMERCIALI

Gli aspetti di carattere commerciale e di durata delle attività sono descritti nella "*Nota Tecnica: GESTIONE PROCESSI SALES ISO/IEC 27001 (Sotto accreditamento ACCREDIA)*" ***ZSEIT-4-TN-43 (E)_KIT_SALES_ISO-IEC 27001***, in ultima revisione.

8. REGOLAMENTO PARTICOLARE

Il regolamento particolare ISO/IEC 27001:2013 applicabile è il ***ZSEIT-10-RG-017 (I)_Regolamento Particolare ISO_IEC 27001***, in ultima revisione.

9. CHECKLIST ASSOCIATE ALLE LINEE GUIDA

Sono state predisposte le seguenti checklist:

1. **ZSEIT-5-f-035 (I)_CKL _27018**
2. **ZSEIT-5-f-040 (I)_CKL _27017**
3. **ZSEIT-5-f-679 (I)_CKL _27035**

4. ZSEIT-5-f-718 (E)_CKL _27701

10. ATTIVITA' DI DELIBERA (TECHNICAL REVIEW)

Le attività di delibera della certificazione (Technical Review) sono svolte come per tutte le pratiche MSC (Management System Certification) seguendo la procedura **ZSEIT-5-OP-568 (E)** in ultima revisione e **ZSEIT-5-OP-168 (I)** in ultima revisione.