Organismo di Certificazione
della Sicurezza Informatica

Nota Informativa dello Schema N. 2/13

Modifiche alla LGP2

Novembre 2013
Versione 1.0

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

L'elenco delle aggiunte e varianti al documento verrà mantenuto aggiornato in modo tale da riportare tutti gli emendamenti effettuati sul presente documento.

Paragrafi della LGP2 modificati	**Data**
2.2, 2.3.2, 2.4, 2.6, 3.1, 3.2.1, 3.2.2, 3.3, 4.2, 4.3, 4.4, 4.6, 4.7, 5, 5.1 e 5.3	Marzo 2007
Tutti	Novembre 2013

INDICE

Scopo del documento

Il presente documento ha lo scopo di modificare e integrare le procedure descritte nella Linea Guida Provvisoria LGP2 avente per titolo “Accreditamento degli LVS e abilitazione degli Assistenti”.

Tali modifiche includono e ampliano anche le disposizioni contenute nella NIS 2/07 (marzo 2007), che pertanto si intende superata.

Per facilità di lettura, nel seguito viene riportata l’intera Linea Guida Provvisoria LGP2, così come appare per effetto delle modifiche intervenute.

Le disposizioni contenute nella NIS 2/13 sono immediatamente operative e quindi sostituiscono a tutti gli effetti le parti corrispondenti contenute nella LGP2.

1 Introduzione

La Linea Guida Provvisoria 2 (LGP2) definisce le procedure per ottenere e mantenere nel corso del tempo l'accreditamento di un Laboratorio per la Valutazione della Sicurezza informatica (LVS) secondo lo Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione. Inoltre, vengono specificati gli ambiti di attività di un LVS e descritti i requisiti generali gestionali e di competenza tecnica per i laboratori. Infine, vengono descritti i requisiti e le procedure per ottenere e mantenere nel corso del tempo l'abilitazione al ruolo di Assistente.

2 I Laboratori per la Valutazione della Sicurezza (LVS)

Lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione prevede che le attività di valutazione siano necessariamente condotte da laboratori, denominati Laboratori per la Valutazione della Sicurezza (LVS), che abbiano ricevuto preventivamente un accreditamento da parte dell'Organismo di Certificazione (OC).

Ai fini dell'accreditamento, l'LVS deve possedere i seguenti requisiti:

1. la capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;
2. la disponibilità di locali e mezzi adeguati ad effettuare valutazioni della sicurezza nel settore della tecnologia dell'informazione;
3. un'organizzazione in grado di controllare il rispetto delle misure di sicurezza e di gestione della qualità previste per il processo di valutazione;
4. la disponibilità di personale sufficiente dotato delle necessarie competenze tecniche;
5. la conformità ai requisiti specificati nelle norme UNI CEI EN ISO/IEC 17025 [UNI1] e UNI CEI EN ISO/IEC 17065 [UNI2], per quanto applicabili;
6. la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

Le procedure e i requisiti necessari per ottenere e mantenere l'accreditamento sono riportati nel seguito di questo documento.

Si precisa che l'accreditamento del laboratorio non implica una garanzia sulla qualità della valutazione di uno specifico prodotto o sistema, bensì rappresenta una dichiarazione riguardo alle competenze tecniche generiche possedute da un LVS.

Il laboratorio richiedente l'accreditamento può essere un organismo pubblico o una impresa regolarmente registrata secondo le norme vigenti.

2.1 Tipologie di accreditamento

Lo Schema prevede la possibilità di valutare e certificare prodotti e sistemi IT in conformità allo standard internazionale Common Criteria [CC1,2,3] e alla relativa metodologia [CEM].

I Common Criteria prevedono vari livelli di valutazione che richiedono, da parte dell'LVS che effettua la valutazione, una diversa e crescente competenza tecnica.

Per tali motivi, lo Schema prevede diverse tipologie di accreditamento, in dipendenza della competenza dell'LVS. La tipologia di accreditamento standard prevista è quella relativa al livello di valutazione EAL4 secondo i Common Criteria. L'insieme delle prove che l'LVS è autorizzato a svolgere, comprende le azioni associate alla valutazione delle componenti di garanzia al livello EAL4, secondo quanto descritto per questo livello di valutazione in [CEM].

L'OC si riserva la facoltà di rilasciare l'accreditamento di un LVS sulla base di tipologie di accreditamento *ad hoc* nei casi in cui ne riconosca la necessità.

2.2 Validità e durata dell'accreditamento

Agli LVS che ottengono l'accreditamento ad operare nell'ambito dello Schema viene rilasciato un Certificato di Accreditamento in cui viene riportata la tipologia dell'accreditamento stesso.

L'accreditamento ha una validità di tre anni. Durante tale periodo, l'OC si riserva di effettuare verifiche in concomitanza di particolari eventi che coinvolgono l'LVS (quali ad esempio cambiamento di sede, variazione dell'organico, inizio di una valutazione) finalizzate a verificare il perdurare delle condizioni necessarie ad operare nell'ambito dello Schema.

Al termine dei tre anni, la validità dell'accreditamento deve essere confermata dall'OC, attraverso visita ispettiva o altri controlli che l'OC dovesse ritenere opportuni. Le modalità specifiche vengono comunicate all'LVS con congruo anticipo.

La variazione della tipologia dell'accreditamento può essere richiesta in qualsiasi momento da un LVS. Le procedure di variazione sono simili a quelle previste per l'accreditamento iniziale e vengono attivate mediante una richiesta formale. L'OC si riserva la facoltà di estendere temporaneamente la tipologia dell'accreditamento di un LVS, su richiesta esplicita di quest'ultimo, per lo svolgimento di una specifica valutazione che richieda un livello di valutazione 'con aggiunta' (*augmented* nella terminologia dei Common Criteria).

2.3 Elenco degli LVS accreditati

L'elenco degli LVS accreditati nell'ambito dello Schema nazionale è pubblicato sul sito web dell'OC [OCSI].

2.4 Sospensione e revoca dell'accreditamento

L'OC può sospendere o revocare l'accreditamento di un LVS, motivando dettagliatamente le ragioni della sospensione o della revoca.

Potenziali motivazioni per una revoca od una sospensione dell'accreditamento possono essere ad esempio: perdita delle competenze necessarie a causa di riduzione del personale, temporanea mancanza di adeguata infrastruttura e/o strumentazione a causa di un cambio di sede, perdita di uno o più dei requisiti necessari elencati in precedenza.

2.5 Gestione del contenzioso

Ogni controversia inerente le attività di accreditamento dei laboratori deve essere riferita alla Direzione dell'OC.

3 Competenze di un LVS

3.1 Attività dell'LVS

Oltre alle attività di valutazione, un LVS può svolgere anche le seguenti attività:

a) Assistenza al Committente per:
   1) la stesura della documentazione di sicurezza durante le fasi di preparazione e/o di conduzione della valutazione;
   2) la determinazione della valutabilità del TDS, ODV o Profilo di Protezione;
   3) le attività connesse con la gestione e il mantenimento dei Certificati.
b) Formazione sulle tematiche della sicurezza nel settore della tecnologia dell'informazione in generale e, in particolare, sulle tecniche di valutazione.

L'LVS è tenuto a dare comunicazione preventiva all'OC ogni volta che effettua una delle suddette attività.

3.2 I Valutatori

Tutto il personale tecnico di un LVS deve possedere una adeguata preparazione nel campo della sicurezza IT, deve conoscere lo Schema, lo standard Common Criteria [CC1,2,3] e la relativa metodologia [CEM]. Inoltre, dovrà essere in grado di svolgere attività di redazione ed analisi della documentazione di valutazione nonché di verificare la corretta operatività di un ODV.
Al personale tecnico di un LVS viene riconosciuta la qualifica di "Valutatore", secondo due profili distinti:

- Valutatore Documentale, svolge l'attività di analisi e scrittura della documentazione di valutazione;
- Valutatore Operativo, svolge il ruolo di verifica e predisposizione dei test funzionali, delle prove di intrusione e dell'analisi di vulnerabilità dell'ODV.

Un Valutatore può ottenere l'accreditamento per entrambi i profili. La qualifica di Valutatore è valida solo ed esclusivamente all'interno di un LVS.
In un LVS è richiesto un numero minimo di tre persone operanti nel laboratorio, con almeno due valutatori (uno per ciascun profilo) in aggiunta al Responsabile dell'LVS.
L'OC si riserva la possibilità di verificare la competenza tecnica del personale di un LVS anche in tempi diversi dalle visite ispettive periodiche, ad esempio quando si verifichi una qualsiasi variazione nella composizione dell'organico dell'LVS rispetto a quanto dichiarato nel Manuale di Qualità: immissione di nuovo personale, variazione di compiti e responsabilità anche di personale già in forze all'LVS stesso, ecc.

3.3 Il Responsabile del Laboratorio

Il Responsabile del Laboratorio è chiamato a rispondere delle attività svolte complessivamente dall'LVS, a mantenere i rapporti con l'OC, a nominare i Valutatori del gruppo di valutazione e il Responsabile per l'LVS in ogni singola valutazione.

Inoltre, il Responsabile del Laboratorio deve comunicare tempestivamente all'OC ogni variazione della sua identità giuridica, nonché ogni variazione riguardante l'organico, la sede, la strumentazione, ecc., rispetto alla situazione verificata dall'OC nella fase di accreditamento o nell'ultima visita ispettiva di controllo effettuata.

Qualora il Responsabile del Laboratorio non fosse disponibile (ad esempio perché non ancora designato o perché non più in carica) i rapporti con l'OC verranno mantenuti da un responsabile designato dalla direzione dell'impresa a cui fa capo il laboratorio, in base a quanto indicato nel relativo manuale di qualità.

3.4 Impiego di esperti esterni all'LVS

Nello svolgimento delle sue attività di valutazione o di assistenza, l'LVS potrebbe avere la necessità di avvalersi delle prestazioni di esperti su particolari tematiche di sicurezza. In tal caso dovrà darne tempestiva comunicazione all'OC, indicando il nome degli esperti esterni coinvolti, le modalità del loro contributo, le attività in cui saranno impegnati (assistenza o parti del processo di valutazione), ecc. In ogni caso, l'impiego di esperti esterni dovrà essere esplicitamente approvato dall'OC.

4 La procedura di accreditamento di un LVS

L' accreditamento di un LVS si svolge in quattro fasi:

1. richiesta;
2. istruttoria;
3. verifica;
4. rilascio.

Nella Figura 1 viene fornito uno schema riassuntivo di tutte le azioni che caratterizzano la procedura di accreditamento di un LVS.

4.1 Richiesta

L'LVS interessato all'accreditamento deve presentare formale richiesta all'OC, utilizzando il modulo predisposto disponibile sul sito web dell'OC [OCSI].

Nel modulo, compilato nella sua interezza, devono essere obbligatoriamente contenute le seguenti informazioni:

1. nome e ragione sociale del laboratorio candidato;
2. indirizzo della sede del laboratorio candidato;
3. tipologia dell'accreditamento richiesto;
4. nominativo delle persone coinvolte operativamente nell'attività di laboratorio e, per i Valutatori, il profilo di orientamento di ciascuno (Documentale o Operativo)
5. dichiarazione di impegno a sostenere le spese relative all'accreditamento del laboratorio;
6. firma del Legale Rappresentante per il laboratorio.

4.2 Istruttoria

Sulla base delle informazioni presenti nella richiesta di accreditamento, l'OC emette un preventivo di spesa per l'accreditamento dell'LVS, calcolato in base al Decreto Ministeriale del 15/02/2006, ai sensi dell'articolo 6 del decreto legislativo del 30 dicembre 2003, n. 366 [DM].

Il richiedente, ricevuto il preventivo, per avviare la fase delle verifiche di competenza e dell'organizzazione del Laboratorio deve presentare la seguente documentazione:

1. Attestazione di pagamento dell'acconto specificato nel preventivo;
2. Manuale della qualità del laboratorio redatto secondo le norme [UNI1] e [UNI2];
3. Curriculum Vitae dei valutatori;
4. Certificato di iscrizione alla Camera di commercio, industria, artigianato e agricoltura qualora si configuri come impresa nazionale o documentazione equivalente per imprese non nazionali;

5. Attestazione comprovante l'appartenenza, solo quando di pertinenza, ad una Amministrazione dello Stato o Ente Pubblico.

4.3 Verifica

Per le attività di verifica dell'accreditamento l'OC nomina un gruppo di valutazione, composto da Ispettori dell'OC.

L'attività svolta dal gruppo di valutazione si suddivide essenzialmente in tre fasi:

1) verifica della documentazione di qualità fornita dal laboratorio;
2) verifica della competenza tecnica del laboratorio nel suo insieme e dei singoli componenti lo staff tecnico;
3) esecuzione di visite ispettive presso la sede del laboratorio.

Gli Ispettori durante la loro attività possono interagire con il Responsabile del laboratorio al fine di richiedere modifiche e integrazioni alla documentazione e alle procedure.

Gli Ispettori devono fornire il Rapporto Finale di Visita Ispettiva firmato per accettazione dal responsabile dell'LVS, riguardante l'esito della visita ispettiva e di tutte le attività di verifica di competenza effettuate.

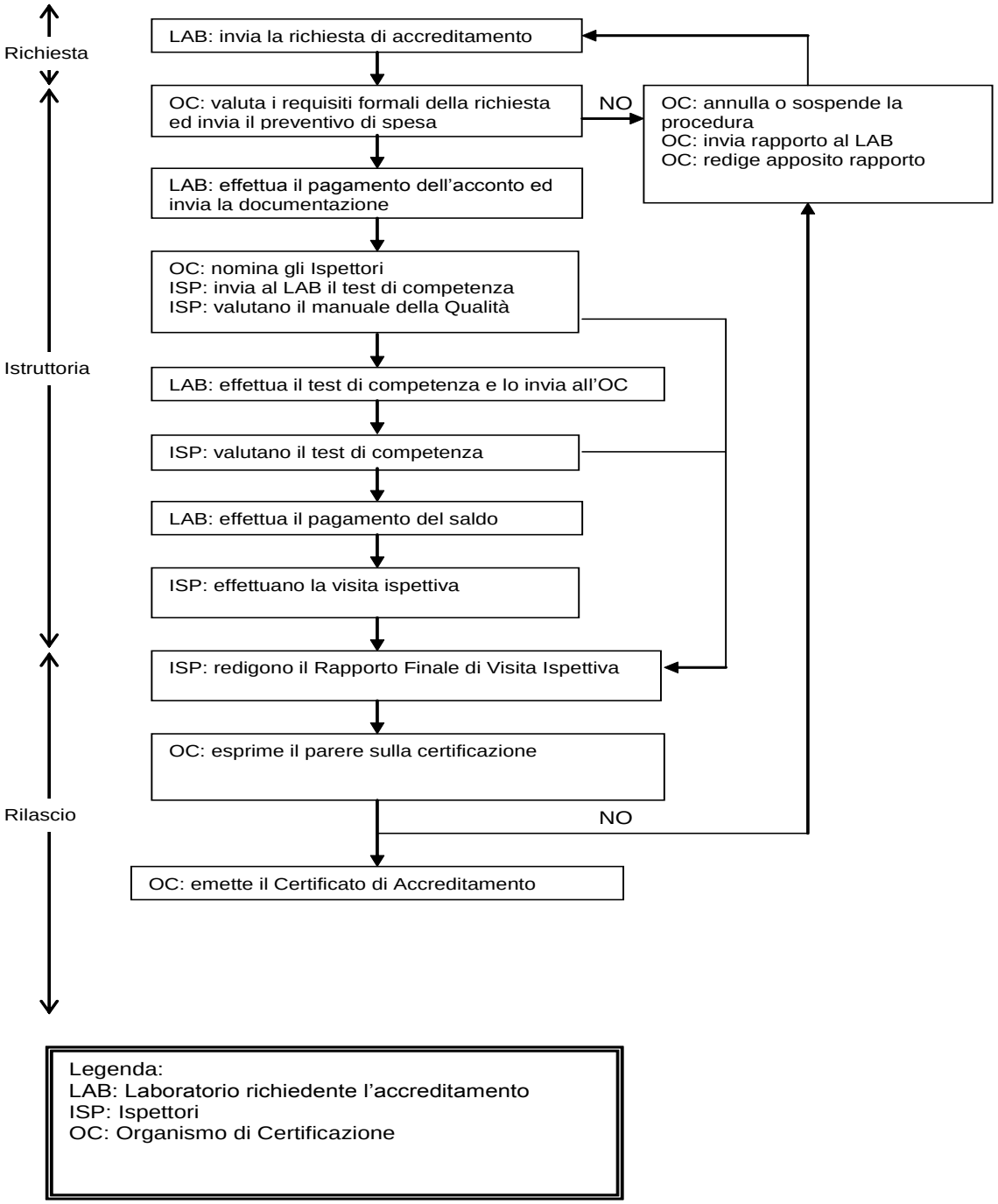
4.4 Rilascio

L'OC emette il Certificato di Accreditamento sulla base del Rapporto Finale di Visita Ispettiva del gruppo di valutazione.

4.5 Durata della procedura di accreditamento

La procedura di accreditamento deve concludersi entro sessanta giorni, a partire dalla ricezione della richiesta e fino all'emissione del Certificato di Accreditamento.

L'LVS può richiedere all'OC, motivandola, una o più sospensioni delle attività di accreditamento. In ogni caso, e in riferimento alla legge sui procedimenti amministrativi erogati dalla pubblica amministrazione, la procedura può durare fino ad un massimo di 180 giorni comprensivi di sospensioni e deroghe, dopodiché la procedura deve essere riavviata e l'LVS è tenuto a versare all'OC il saldo per le attività di accreditamento effettuate, anche in caso di esito negativo.



245

Figura 1– Schema riassuntivo della procedura di accreditamento LVS

5 Gli Assistenti

Lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione prevede il ruolo di Assistente.

L'Assistente è una persona abilitata a fornire assistenza al Committente, al Fornitore o a un LVS nelle diverse fasi della valutazione di un ODV.

5.1 Competenza tecnica

Il candidato al ruolo di Assistente deve possedere una adeguata preparazione nel campo della sicurezza IT, deve conoscere lo Schema, lo standard Common Criteria [CC1,2,3] e la relativa metodologia [CEM]. Inoltre, dovrà essere in grado di svolgere attività di redazione ed analisi della documentazione di valutazione nonché di verificare la corretta operatività di un ODV.

5.2 Tipologia dell'abilitazione

L'abilitazione ad Assistente può essere rilasciata secondo due profili distinti:

- Assistente Documentale, svolge l'attività di analisi e scrittura della documentazione di valutazione;
- Assistente Operativo, svolge il ruolo di progettazione e produzione di test funzionali, delle prove di intrusione e dell'analisi di vulnerabilità dell'ODV.

L'Assistente deve garantire:

1. l'imparzialità, l'indipendenza, la riservatezza e l'obiettività nello svolgimento del proprio ruolo;
2. la capacità di mantenere nel tempo i requisiti in virtù dei quali è stato abilitato.

La tipologia di abilitazione standard prevista è quella relativa al livello di valutazione EAL4 secondo i Common Criteria. L'insieme delle attività che l'Assistente è autorizzato a svolgere, per entrambi i profili, comprende le azioni associate alla valutazione delle componenti di garanzia al livello EAL4, secondo quanto descritto per questo livello di valutazione in [CEM].

5.3 Validità e durata dell'abilitazione

Il rilascio dell'abilitazione è subordinato al superamento di un test di valutazione, proposto dall'OC, sulla competenza tecnica del richiedente.

L'abilitazione ha una validità di tre anni. Durante tale periodo, l'OC si riserva di verificare il perdurare delle condizioni necessarie ad operare nell'ambito dello Schema. Al termine dei tre anni, la validità dell'abilitazione deve essere confermata dall'OC, attraverso test di valutazione o altri controlli che l'OC dovesse ritenere opportuni. Le modalità specifiche vengono comunicate all'Assistente con congruo anticipo.

5.4 Elenco degli Assistenti abilitati

L'elenco degli Assistenti abilitati a operare nello Schema nazionale è pubblicato sul sito web dell'OC [OCSI].

5.5 Sospensione e revoca dell'abilitazione

L'OC può sospendere o revocare l'abilitazione di un Assistente, motivando dettagliatamente le ragioni della sospensione o della revoca.

Potenziale motivazione per una revoca od una sospensione dell'abilitazione può essere, ad esempio, la perdita dei requisiti di imparzialità e indipendenza, a seguito dell'assunzione nella Pubblica Amministrazione o nell'organico di un LVS o di una società committente o fornitrice di prodotti da sottoporre a valutazione CC.

5.6 Gestione del contenzioso

Ogni controversia inerente le attività di abilitazione di un Assistente deve essere riferita alla Direzione dell'OC.

6 La procedura di abilitazione al ruolo di Assistente

L' abilitazione di un Assistente si svolge in quattro fasi:

1. richiesta;
2. istruttoria;
3. verifica;
4. rilascio.

Nella Figura 2 viene fornito uno schema riassuntivo di tutte le azioni che caratterizzano la procedura di abilitazione di un Assistente.

6.1 Richiesta

La persona interessata all'abilitazione al ruolo di Assistente deve presentare formale richiesta all'OC, utilizzando il modulo predisposto disponibile sul sito web dell'OC [OCSI] e specificando il profilo o i profili richiesti. Al modulo, compilato nella sua interezza, deve essere obbligatoriamente allegato il Curriculum Vitae, specificando, in particolare, la propria esperienza nel campo della sicurezza IT.

6.2 Istruttoria

Una volta ricevuta la richiesta, l'OC comunica alla persona interessata data e luogo dello svolgimento del test di valutazione per la verifica delle competenze.
L'attestazione di pagamento dei relativi costi, calcolati in base al Decreto Ministeriale del 15/02/2006, ai sensi dell'articolo 6 del decreto legislativo del 30 dicembre 2003, n. 366 [DM], descritti nel modulo di richiesta di abilitazione, dovrà essere inviata almeno cinque giorni prima dell'effettuazione dei test di valutazione.

6.3 Verifica

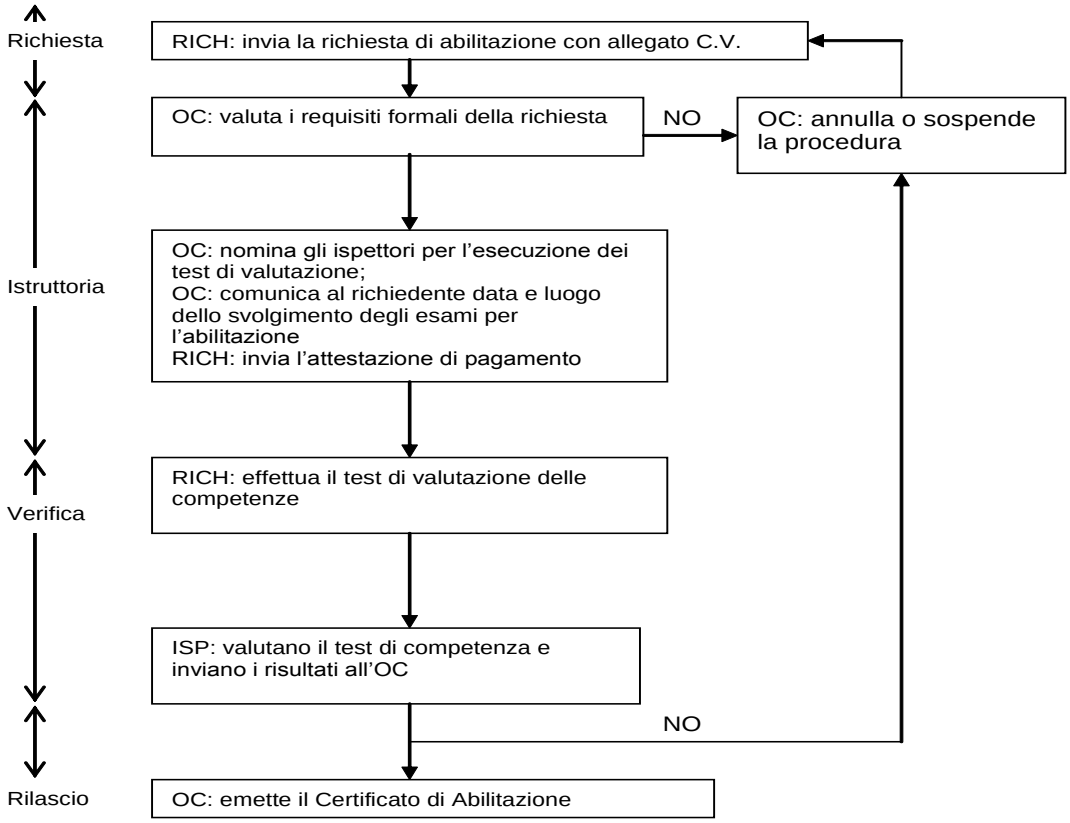
Per le attività di verifica delle competenze, l'OC nomina un gruppo di valutazione, composto da Ispettori dell'OC, che sottopone il candidato a un test di valutazione, volto ad accertarne la competenza in materia di sicurezza IT, la conoscenza dei criteri di valutazione di sicurezza, la padronanza nell'uso delle metodologie per la redazione e l'analisi della documentazione di valutazione e per la verifica della corretta operatività di un ODV.
Il gruppo di valutazione riassume i risultati del test di valutazione nel Rapporto Finale di Esame.

6.4 Rilascio

L'OC emette il Certificato di Abilitazione sulla base del Rapporto Finale di Esame emesso dal gruppo di valutazione.

6.5 Durata della procedura di abilitazione

La procedura di abilitazione deve concludersi entro sessanta giorni, a partire dalla ricezione della richiesta e fino all'emissione del Certificato di Abilitazione Assistente, in
330 riferimento alla legge sui procedimenti amministrativi erogati dalla pubblica amministrazione.



Legenda:
RICH: Persona richiedente l'abilitazione al ruolo di assistente
ISP: Ispettori
OC: Organismo di Certificazione

Figura 2– Schema riassuntivo della procedura di abilitazione Assistente

Riferimenti bibliografici

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[ISO1] ISO/IEC 2382-8 “Information technology – Vocabulary” – Part 8: Security, 1998

[DM] "Individuazioni delle prestazioni, eseguite dal Ministero delle comunicazioni per conto terzi, ai sensi dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366", Decreto Ministero Comunicazioni del 15 febbraio 2006, GU n. 82 del 7 Aprile 2006

[OCSI] Sito web dell'OCSI: <www.ocsi.isticom.it>

[UNI1] UNI/CEI EN ISO/IEC 17025, “Requisiti generali per la competenza dei laboratori di prova e di taratura”, 2005

[UNI2] UNI/CEI EN ISO/IEC 17065, “Valutazione della conformità: requisiti per organismi che certificano prodotti, processi e servizi”, 2012

Lista degli acronimi

CC	=	Common Criteria
CEI	=	Comitato Elettrotecnico Italiano
EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
EN	=	European Norm
IEC	=	International Electrotechnical Commission
ISO	=	International Organization for Standardization
IT	=	Information Technology
LGP	=	Linea Guida Provvisoria
LVS	=	Laboratorio per la Valutazione della Sicurezza
NIS	=	Nota Informativa dello Schema
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
PDV	=	Piano Di Valutazione
PP	=	Profilo di Protezione (Protection Profile)
TDS	=	Traguardo di Sicurezza (ST - Security Target)
UNI	=	Ente Nazionale Italiano di Unificazione