Organismo di Certificazione
della Sicurezza Informatica

Nota Informativa dello Schema N. 3/13

Modifiche alla LGP3

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 LGP3 modificati	**Data**
3.1, 3.5, 4.5.1, 4.6, 5, 5.2.2, 5.2.4, 5.3.2, 5.4.2, 5.4.3, 5.4.5, 5.4.6, 5.5.1, 5.6, 6.1.2	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 LGP3, “Procedure di Valutazione”.

Tali modifiche includono e ampliano anche le disposizioni contenute nella NIS 3/07 (marzo 2007), che pertanto si intende superata.

Per facilità di lettura, nel seguito viene riportata l’intera Linea Guida Provvisoria LGP3, così come appare per effetto delle modifiche intervenute.

Le disposizioni contenute nella NIS 3/13 sono immediatamente operative e quindi sostituiscono a tutti gli effetti le parti corrispondenti contenute nella LGP3.

1 Introduzione

La Linea Guida Provvisoria 3 (LGP3) definisce le procedure che devono essere seguite nel corso di un processo di valutazione condotto all'interno dello Schema. Tali procedure descrivono le modalità secondo cui effettuare:

- le comunicazioni tra un Laboratorio per la Valutazione della Sicurezza (LVS), un Committente, un Fornitore e l'Organismo di Certificazione (OC);
- l'organizzazione e la pianificazione delle attività di una valutazione;
- il controllo di una valutazione;
- la pubblicazione dei risultati di una valutazione;
- la segnalazione di anomalie.

Un processo di valutazione è suddiviso in tre fasi distinte:

1) Preparazione
2) Conduzione
3) Conclusione

Le procedure di valutazione definite in questo documento sono applicabili alla valutazione della sicurezza di:

- un prodotto o un insieme di prodotti software, firmware e/o hardware per l'elaborazione elettronica delle informazioni, cioè l'Oggetto Della Valutazione (ODV), così come definito nei Common Criteria [CC1,2,3];
- un Profilo di Protezione (PP), cioè il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di garanzia, definito nei Common Criteria.

Le procedure di valutazione sono altresì applicabili a:

- una valutazione *concomitante* (cioè effettuata durante lo sviluppo di un ODV);
- una valutazione *consecutiva* (cioè effettuata dopo lo sviluppo di un ODV);
- una rivalutazione di un ODV o di un PP;
- una riutilizzazione dei risultati di una precedente valutazione di un ODV o di un PP.

2 Ruolo e responsabilità dell'LVS

In questo capitolo sono descritti in dettaglio il ruolo e le responsabilità dell'LVS nel processo di valutazione e certificazione. Per quanto riguarda le altre parti coinvolte, si rimanda a quanto esposto nella LGP1.

Il ruolo dei Valutatori, durante il corso di una valutazione, è quello di svolgere le azioni definite nei criteri di valutazione e di riportare all'OC i risultati dell'attività svolta, come viene ampiamente descritto nel seguito.

Un LVS può svolgere altre mansioni, non necessariamente classificate come attività di valutazione. Esempi di tali attività non di valutazione svolte dall'LVS includono:

- supporto all'OC (ad esempio relativamente alla definizione delle metodologie di valutazione);
- addestramento;
- produzione di Traguardi di Sicurezza e/o Profili di Protezione;
- assistenza per la valutazione.

Tra queste, particolare importanza assume quella di assistenza per la valutazione.

2.1 Assistenza per la valutazione

A causa dell'elevata complessità del processo di valutazione, le organizzazioni coinvolte avranno spesso la necessità di richiedere l'assistenza di esperti, che potranno appartenere o meno a un LVS. L'assistenza può essere fornita prima che una valutazione inizi o in parallelo alla valutazione stessa e può essere data:

- al Committente di una valutazione;
- al Fornitore di un ODV.

L'assistenza può coprire ogni aspetto della valutazione: tipicamente consiste in assistenza al Committente per la stesura o la revisione di un TDS o di un PP e/o di ogni altra documentazione necessaria per la valutazione, oppure per stimare la probabilità di riuscita del processo di certificazione.

L'ambito dell'assistenza durante la valutazione viene direttamente negoziato tra il Committente e l'Assistente. L'OC lascia i dettagli contrattuali alle due parti in gioco, senza alcun coinvolgimento.

Comunque, quando un LVS fornisce sia l'assistenza sia il servizio di valutazione per un particolare ODV o PP, è obbligato sia a definire chiaramente l'ambito dell'assistenza, sia a dimostrare all'OC che l'assistenza fornita non influenza l'indipendenza dei Valutatori o l'imparzialità della valutazione, assicurando che sia sempre rispettata la separazione e la distinzione tra le strutture e le persone che forniscono l'assistenza e quelle che effettuano la valutazione.

L'LVS deve informare l'OC di tutte le assistenze fornite e ricevute nel corso della valutazione.

2.2 Limiti all'attività dei Valutatori

Un Valutatore non può in nessun caso:

- partecipare contemporaneamente allo sviluppo ed alla valutazione di un ODV o di un PP;
- fornire al Committente di una valutazione o al Fornitore di un ODV o PP servizi di assistenza che potrebbero compromettere l'indipendenza della valutazione.

L'LVS deve conformarsi alle condizioni fissate nell'accreditamento per garantire che l'assistenza fornita non influenzi la sua indipendenza o imparzialità in ogni valutazione.

2.3 Trasmissione della documentazione

La trasmissione di documenti ufficiali tra l'OC, l'LVS e il Committente, avviene in base alle norme vigenti in materia di comunicazioni tra imprese e amministrazioni pubbliche. In particolare, le modalità di trasmissione della documentazione e dei materiali attinenti una valutazione vengono concordate durante la Riunione di Avvio dei Lavori.

3 Processo di valutazione

Un processo di valutazione corrisponde alle attività di valutazione svolte da un LVS su un singolo ODV o PP e comprende le seguenti fasi:

1) Preparazione
2) Conduzione
3) Conclusione

La fase di preparazione vede coinvolti il Committente e l'LVS, che esamina il TDS o il PP del Committente e produce un Piano di Valutazione (PDV), dettagliando come deve essere effettuata la valutazione.
I Valutatori producono anche un elenco di materiali per la valutazione, individuando la documentazione necessaria e l'eventuale supporto richiesto al Fornitore dell'ODV.
Prima di definire un rapporto contrattuale, il Committente e l'LVS possono contattare, sia pure in modo informale, l'OC per accertare la possibilità di condurre la valutazione nell'ambito dello Schema.
Una volta definito l'accordo tra LVS e Committente, quest'ultimo deve sottoporre all'OC la richiesta di iscrizione formale della valutazione nello Schema, allegando il TDS e il Piano di Valutazione (PDV) predisposto dall'LVS designato.

La fase di conduzione inizia quando l'OC, esaminato il materiale ricevuto, approva il PDV e accetta formalmente la valutazione nello Schema.

Nella fase di conclusione, l'LVS produce un Rapporto Finale di Valutazione (RFV) che riassume tutti i risultati ottenuti durante la valutazione e che viene utilizzato dall'OC come base per la stesura del Rapporto di Certificazione.
Maggiori dettagli sulle singole fasi vengono forniti nei paragrafi successivi.

3.1 Riservatezza del processo di valutazione

Oltre agli impegni contrattuali assunti dall'LVS relativamente alla riservatezza, i Valutatori che hanno accesso a informazioni proprietarie relative a un ODV o ad un PP possono essere tenuti a firmare un accordo di riservatezza con il Committente e/o il Fornitore. L'obiettivo di tale accordo è assicurare che i Valutatori non comunichino informazioni concernenti la loro attività ad alcuna terza parte non autorizzata a ricevere tali informazioni, all'interno o all'esterno dell'LVS.
Nel firmare un accordo di riservatezza, un Valutatore si impegna a:

- usare le informazioni ottenute nel corso della valutazione soltanto ai fini della valutazione stessa;
- non divulgare tali informazioni ad alcuna terza parte se non espressamente autorizzato dal Committente o dal Fornitore.

Oltre all'accordo di riservatezza tra i Valutatori e il Committente/Fornitore, le informazioni su ciascun processo di valutazione devono essere controllate all'interno di un LVS sulla base della "necessità di conoscere".

Si noti che alcuni ambiti della valutazione potrebbero implicare la presenza di informazioni proprietarie del Fornitore che questi non desidera siano divulgate al Committente o a qualsiasi altra parte tranne all'LVS e all'OC, o di informazioni riservate che un LVS non vuole siano rivelate ad altri LVS: in questi casi è raccomandata la discussione della disciplina di tali informazioni riservate nella Riunione di Avvio dei Lavori. Eventuali modifiche a queste decisioni possono essere apportate durante le Riunioni di Controllo della Valutazione.

I materiali per la valutazione sono gestiti, come materiale riservato, in accordo al manuale di qualità dell'LVS.

3.2 Diritti di proprietà

Prima dell'inizio di una valutazione, l'LVS e il Committente determinano chi tra loro dovrà detenere i diritti di proprietà dei documenti prodotti durante la valutazione. Entrambe le parti devono considerare, quando prendono questa decisione, che l'OC può richiedere il riuso della documentazione prodotta dall'LVS nel corso di una valutazione allo scopo di rivalutare un ODV o un PP, o di riutilizzarla nella valutazione di un diverso ODV o PP.

Sarà responsabilità del Committente della nuova valutazione fare in modo che i relativi rapporti siano forniti all'LVS che conduce la valutazione. Questo richiederà il rilascio di autorizzazioni da parte del detentore del diritto di proprietà, e di ogni altra parte con interessi commerciali.

L'OC gestisce e tratta tutte le informazioni ottenute nel corso delle attività di certificazione, in maniera strettamente riservata e protetta e in accordo alla legislazione vigente.

Nelle attività di accreditamento e mantenimento degli LVS, l'OC assicura che i Laboratori per la Valutazione della Sicurezza applichino analoghi criteri di riservatezza e protezione alle informazioni da loro acquisite durante le attività di valutazione.

3.3 Lingua utilizzata

Per la produzione dei Rapporti di Attività e del Rapporto Finale di Valutazione è obbligatorio l'uso della lingua italiana.

Per tutti gli altri documenti prodotti nel corso del processo di valutazione è consentito anche l'uso della lingua inglese.

In ogni caso, l'uso della lingua inglese è obbligatorio per le parti riportate integralmente dai criteri internazionali, quali ad esempio la formulazione dei requisiti funzionali e di garanzia definiti secondo i Common Criteria.

4 Preparazione

Gli obiettivi di questa fase sono:

1) assicurare che tutte le parti coinvolte nella valutazione abbiano un'interpretazione comune dello scopo e dell'ambito della valutazione, e siano consapevoli delle loro responsabilità;
2) determinare l'adeguatezza per la valutazione del TDS o del PP;
3) determinare l'adeguatezza dei materiali per la valutazione disponibili;
4) produrre un PDV e un elenco dei materiali per la valutazione.

Il primo passo in questa fase è compiuto dal Committente, che individua un LVS per lo svolgimento delle attività di valutazione, al quale consegna un TDS o un PP. Il Committente può richiedere all'LVS anche attività di assistenza, ad esempio per la stesura di un TDS o di un PP o di altra documentazione necessaria per la valutazione; in tal caso valgono le considerazioni fatte nel par. 2.1.

L'ambito di questa fase è oggetto di accordo tra il Committente e l'LVS. Tuttavia, se necessario, prima di definire un rapporto contrattuale, il Committente e l'LVS possono contattare, sia pure in modo informale, l'OC per accertare la possibilità di condurre la valutazione nell'ambito dello Schema.

4.1 Relazioni tra Committente e Fornitore

Secondo lo Schema, è responsabilità del Committente assicurarsi che il Fornitore sia in grado di fornire i materiali per la valutazione richiesti.

L'LVS deve controllare che il Committente e il Fornitore siano pienamente a conoscenza:

- del processo di valutazione;
- del ruolo dell'LVS;
- delle loro responsabilità durante tutta la valutazione.

I Valutatori devono assicurarsi che il Committente e il Fornitore abbiano concordato contrattualmente la fornitura dei materiali per la valutazione e che siano state considerate le conseguenze sull'andamento della valutazione di eventuali condizioni particolari che potrebbero causare ritardi nello svolgimento delle attività previste.

4.2 Richiesta di iscrizione della valutazione nello Schema

Affinché una valutazione sia formalmente accettata nello Schema, il Committente deve sottoporre una richiesta all'OC, utilizzando il modulo predisposto disponibile sul sito web dell'OC [OCSI].

Al modulo, compilato nella sua interezza, devono essere obbligatoriamente allegati il TDS o il PP e il PDV predisposto dall'LVS designato dal Committente.

Una volta ricevuta la richiesta, l'OC esamina la documentazione allegata per verificare l'assenza di elementi che possano pregiudicare il buon esito della valutazione.

In particolare, l'OC verifica che il PDV contiene la descrizione di tutte le attività che i Valutatori eseguiranno durante la valutazione e le modalità secondo le quali queste attività risultano organizzate, pianificate, correlate e suddivise nell'ambito del periodo di valutazione.

L'OC inoltre verifica la congruità delle risorse e delle tempistiche previste dall'LVS per la conduzione della valutazione con il livello di garanzia richiesto e con la natura e la complessità del prodotto da valutare, descritto nel relativo TDS, o del PP.

Se l'OC non ha obiezioni, entro trenta giorni dalla ricezione della richiesta approva il PDV e iscrive la valutazione nello Schema, designando il responsabile del procedimento, che fungerà da referente della certificazione verso il Committente e l'LVS. L'OC comunica tale decisione simultaneamente al Committente e all'LVS, che può quindi avviare le attività di valutazione. Nella comunicazione rivolta al Committente, sarà compreso anche il preventivo dei costi dovuti all'OC per le attività di certificazione, 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]. Di norma, tali costi sono stabiliti nella misura del 10% delle ore/persona previste nel PDV predisposto dall'LVS, tariffate in base al citato Decreto Ministeriale, oltre a eventuali spese di missione e alle spese generali, pari al 20% del costo complessivo.

Nel caso in cui l'OC rilevi la presenza di potenziali problemi nella documentazione esaminata, richiede al Committente e/o all'LVS le necessarie integrazioni e correzioni. Tale richiesta sospende, fino al relativo esito, il decorso del suddetto termine di trenta giorni.

4.3 Piano di Valutazione (PDV)

Il PDV deve descrivere le attività previste per il processo di valutazione, fornendo sufficienti dettagli per poter stimare lo stato di avanzamento del processo di valutazione per ciascuna Attività prevista.

Il PDV deve essere redatto tenendo conto di tutte le informazioni presenti nel TDS o nel PP, nella consapevolezza che alcune informazioni relative ad aspetti della valutazione risulteranno disponibili solo durante la fase di conduzione.

Nel corso di una valutazione, potrebbe essere necessario emendare alcune parti di un PDV, ad esempio, nei seguenti casi:

- l'ODV viene modificato durante la valutazione (per il rilascio di una nuova versione di un prodotto o perché alcuni problemi sono stati eliminati);
- il Committente non fornisce i materiali per la valutazione nel formato e nel modo concordati, o non rispetta i tempi di esecuzione stabiliti.

Tutte le variazioni apportate a un PDV devono essere approvate dall'OC.

Durante una valutazione, i Valutatori potrebbero voler effettuare attività che non fanno parte della valutazione "standard". Ad esempio, i Valutatori possono:

- ritenere necessario scostarsi da una rigida interpretazione dei requisiti dello Schema o dei criteri di valutazione;
- voler effettuare attività opzionali per facilitare future rivalutazioni dell'ODV o del PP.

È importante che qualsiasi attività aggiuntiva, come quelle sopra indicate, sia chiaramente identificata come tale e approvata in anticipo dall'OC.

4.4 Elenco dei materiali per la valutazione

Affinché i Valutatori possano effettuare le singole azioni specificate nel PDV, devono avere a disposizione i materiali per la valutazione richiesti. I criteri di valutazione forniscono un elenco dei materiali per la valutazione per ciascun livello di garanzia. Questo elenco deve essere dettagliato dai Valutatori per ogni specifica valutazione, e di norma fa parte integrante del PDV.

I materiali per la valutazione possono comprendere:

- gli elementi hardware, firmware o software che costituiscono l'ODV;
- la documentazione per l'utente dell'ODV;
- la documentazione tecnica di supporto, generata durante lo sviluppo dell'ODV o per sostenere il processo di valutazione;
- il supporto tecnico del Fornitore.

Possono essere considerati materiali per la valutazione anche:

- l'accesso al sito operativo;
- l'accesso al sito dello sviluppo dell'ODV.

5 Conduzione

Gli obiettivi di questa fase sono avviare la valutazione, assicurare che siano effettuati gli appropriati controlli e svolgere l'attività di valutazione tecnica, registrando il lavoro eseguito, le osservazioni fatte ed i risultati ottenuti in modo tale che:

- sia dimostrato che l'attività è stata effettuata nel rispetto dello standard Common Criteria, delle Linee Guida dell'OC e del PDV;
- sia dimostrato che l'attività è stata effettuata obiettivamente ed imparzialmente;
- i risultati siano ripetibili e riproducibili;
- sia fornita sufficiente evidenza per giustificare le conclusioni dei Valutatori.

5.1 Avvio del processo di valutazione

Riunione di Avvio dei Lavori

Dopo l'approvazione formale del PDV, l'OC convoca una Riunione di Avvio dei Lavori (RAL), durante la quale vengono affrontati diversi argomenti, quali ad esempio:

- identificazione dei responsabili della valutazione del Committente e dell'LVS;
- identificazione dei componenti del gruppo di certificazione designati dall'OC;
- precisazioni sui contenuti del TDS o del PP;
- precisazioni sui contenuti del PDV;
- gestione di documenti riservati;
- organizzazione dei materiali per la valutazione;
- aspetti riguardanti il personale designato dall'LVS per la valutazione;
- vincoli sulla valutazione (ad esempio limitazioni sull'accesso a determinate aree o sui contatti con il Fornitore e/o il Committente);
- comunicazione da parte dell'LVS della data di inizio effettivo della valutazione;
- riutilizzazione di risultati di precedenti valutazioni;
- frequenza delle Riunioni di Controllo della Valutazione;
- modalità di trasmissione della documentazione e dei materiali prodotti durante la valutazione.

L'organizzazione della Riunione di Avvio dei Lavori è responsabilità dell'OC, che è anche responsabile per la produzione e la distribuzione dell'ordine del giorno e del successivo verbale.

Alla Riunione di Avvio dei Lavori partecipano, oltre all'OC stesso, l'LVS e il Committente (di solito i rispettivi responsabili designati per la valutazione). Vista l'importanza di tale riunione, potrebbe rendersi necessario invitare altri partecipanti, quali ad esempio il Fornitore.

Inserimento nell'elenco dei prodotti, sistemi e PP in valutazione

Un ODV o un PP in valutazione può essere incluso nell'elenco dei prodotti, sistemi e PP in valutazione, pubblicato sul sito web dell'OC [OCSI], previo consenso del Committente. Se un ODV o un PP in valutazione è inserito nell'elenco, ma la valutazione viene sospesa o annullata, l'OC informa sia l'LVS sia il Committente che quell'ODV o PP verrà rimosso dall'elenco.

5.2 Realizzazione di un'attività di valutazione

Materiali per la valutazione

Per poter effettuare le Attività di valutazione, i Valutatori devono avere a disposizione i materiali per la valutazione richiesti.

Per una valutazione consecutiva, tutti i materiali sono normalmente disponibili all'inizio della valutazione.

Per una valutazione concomitante, la tempistica delle Attività di valutazione dipende dai tempi di esecuzione dello sviluppo dell'ODV. Lo slittamento delle tappe fondamentali di tale sviluppo ha inevitabilmente un impatto sui tempi di esecuzione della valutazione. Affinché il Valutatore possa modificare di conseguenza la pianificazione delle Attività di valutazione, è necessario uno stretto contatto con il Fornitore.

Un ritardo nella data di rilascio di un materiale per la valutazione può avere diverse conseguenze sui tempi di esecuzione della valutazione stessa. L'LVS può, ad esempio:

1) sospendere soltanto la singola azione interessata e (se attuabile) procedere con un'altra azione;
2) sospendere la valutazione finché il materiale richiesto non sia disponibile.

I cambiamenti nei tempi di esecuzione della valutazione sono materia contrattuale tra l'LVS e il Committente. Tuttavia, poiché tali cambiamenti potrebbero avere un impatto sulle risorse di certificazione disponibili, l'LVS deve avvisare l'OC sui ritardi e sulle modifiche proposte nelle tappe fondamentali del processo di valutazione. La non disponibilità o i ritardi nel rilascio dei materiali per la valutazione può condurre alla produzione di un Rapporto di Osservazione.

5.3 Rapporti di Osservazione (RO)

Durante una valutazione, i Valutatori possono rilevare vari problemi relativi all'ODV o al PP. Alcuni di questi problemi possono consistere specificamente in vulnerabilità sfruttabili, mentre altri possono riferirsi ad anomalie più generali (riguardanti ad esempio l'ambiente di sviluppo o la documentazione operativa). Qualunque sia il problema, è essenziale che riceva un'appropriata e pronta attenzione dalle parti interessate.

Tutti i problemi riscontrati nel corso del processo di valutazione, devono essere riportati dai Valutatori sotto forma di Rapporti di Osservazione.

Per facilitare la gestione da parte dell'OC, sono usati due tipi di Rapporti di Osservazione:

1) Rapporto di Osservazione per Errore (ROE);
2) Rapporto di Osservazione per Anomalia (ROA).

Rapporto di Osservazione per Errore (ROE)

Un ROE viene prodotto quando si identifica, in qualsiasi momento della valutazione, una vulnerabilità sfruttabile, anche se solo potenziale. Tale rapporto è da considerarsi estremamente importante, poiché in caso di vulnerabilità sfruttabile non risultano più soddisfatti gli obiettivi di sicurezza previsti nel TDS.

Nel caso di individuazione di una potenziale vulnerabilità sfruttabile il ROE prodotto dovrebbe essere in seguito aggiornato in base al risultato della prova di intrusione. Non è necessario invece dimostrare che la vulnerabilità sia sfruttabile nel caso di vulnerabilità già note.

I ROE non devono essere usati per riportare altri problemi relativi alla sicurezza dell'ODV diversi dalle vulnerabilità.

Rapporto di Osservazione per Anomalia (ROA)

Il ROA deve essere usato per riportare tutti i problemi relativi all'ODV o al PP diversi dalle vulnerabilità sfruttabili. Questo copre un'ampia tipologia di problemi, quali ad esempio:

- problemi riguardanti lo sviluppo o la gestione dell'ODV;
- problemi riguardanti il contenuto, la presentazione e l'evidenza di materiali per la valutazione;
- problemi che possono avere un impatto sulla sicurezza.

Ci sono casi in cui i Valutatori necessitano di chiedere chiarimenti di minore entità su documenti del Committente e/o del Fornitore. In tali casi, può non essere appropriato usare i ROA, ma utilizzare invece comunicazioni informali con il Committente e/o con il Fornitore, a seconda dei casi, evidenziando la necessità di una risposta tempestiva. In caso di dubbio sull'opportunità di emettere un ROA, dovrebbe essere consultato l'OC.

Procedure di emissione

I Valutatori possono produrre un Rapporto di Osservazione in ogni momento durante la valutazione. Un Rapporto di Osservazione può essere usato per descrivere un singolo problema o più problemi tra loro collegati.

I Rapporti di Osservazione devono essere firmati dal Valutatore che ha riscontrato il problema e dal responsabile per la valutazione dell'LVS.

I ROA devono essere distribuiti al Committente e all'OC simultaneamente, mentre i ROE devono essere inviati per la revisione all'OC prima di essere consegnati al Committente.

Azioni susseguenti ai Rapporti di Osservazione

Nel caso venga emesso un ROA, il Committente intraprende le azioni necessarie a risolvere il problema sollevato.

Una volta individuate le azioni e le contromisure proposte per la risoluzione del problema sollevato, il Committente dovrà emettere la risposta al ROA, che verrà inviata contemporaneamente all'LVS e all'OC.

Nel caso, invece, venga emesso un ROE, l'OC lo esaminerà per valutare la gravità del problema sollevato. Nei casi più semplici, trasmetterà il ROE al Committente, affinché lo gestisca al pari di un ROA, come descritto in precedenza.

Qualora, invece, la soluzione del problema implichi azioni più rilevanti (quali ad esempio modifiche dell'ODV), l'OC convocherà un'apposita Riunione di Controllo della valutazione, cui parteciperanno l'LVS e il Committente (ed eventualmente il Fornitore) per verificare la fattibilità e l'opportunità delle azioni richieste.

Qualora lo ritenga necessario, l'OC può emettere autonomamente, in qualsiasi fase della valutazione, una Nota dell'Organismo di Certificazione (NOC), rivolta all'LVS e/o al Committente. Una NOC contiene indicazioni dell'OC relativamente alle attività svolte nel corso di quella specifica valutazione, quali ad esempio i problemi esposti in un ROA/ROE, il corretto svolgimento di un'attività, la corretta interpretazione delle norme, ecc.

Nei casi in cui il problema fosse di interesse generale, l'OC adotterà una soluzione che sarà oggetto di una Nota Informativa dello Schema (NIS), che sarà distribuita a tutti gli LVS accreditati.

5.4 Rapporto di Attività (RA)

Al termine di ogni attività, l'LVS predispone dei Rapporti di Attività (RA) che riassumono i risultati delle analisi condotte per quella specifica attività, indicando anche se sono stati impiegati metodi di valutazione e/o di sviluppo che presentano carattere innovativo. Tali Rapporti vengono di norma inviati all'OC al termine di ciascuna attività. In relazione al contenuto degli RA, l'OC decide sull'opportunità di trasmetterli al Committente.

Per le valutazioni che non presentino particolare complessità, gli RA possono essere prodotti alla fine della valutazione. Le modalità di emissione degli RA vengono concordate nella Riunione di Avvio dei Lavori.

In ogni caso tali Rapporti debbono essere compresi nell'RFV.

5.5 Rapporti di Osservazione sullo Schema (ROS)

Tutti gli LVS accreditati possono fare osservazioni sul funzionamento dello Schema, anche se non coinvolti in processi di valutazione. Ad esempio, possono essere segnalati:

- difficoltà di applicazione delle regole dello Schema;
- problemi di interpretazione dei criteri di valutazione o dello Schema;
- problemi circa l'applicabilità di un particolare metodo di valutazione;
- tecniche di valutazione, strumenti o procedure interessanti o innovative.

Le segnalazioni sono inviate all'OC sotto forma di Rapporto di Osservazione sullo Schema (ROS). In tale rapporto dovrebbe anche essere proposta una soluzione per il problema rilevato.

L'OC, esaminato il ROS, adotterà una soluzione che sarà oggetto di una Nota dell'Organismo di Certificazione (NOC), rivolta all'LVS che ha prodotto il ROS.

Nei casi in cui il problema fosse di interesse generale, la soluzione adottata dall'OC sarà oggetto di una Nota Informativa dello Schema (NIS), che sarà distribuita a tutti gli LVS accreditati.

5.6 Riunioni di Controllo della Valutazione

Le Riunioni di Controllo della Valutazione sono un'occasione per l'LVS e l'OC (ed eventualmente il Committente e/o il Fornitore) per discutere l'attività tecnica dettagliata relativa ad una particolare valutazione, revisionare lo stato di avanzamento ed i tempi di esecuzione del processo di valutazione, individuare e discutere i problemi e attivare le azioni appropriate. Tali riunioni possono essere tenute periodicamente durante il corso della valutazione o possono essere convocate 'ad hoc' per discutere un particolare problema (individuato, ad esempio, in un ROA).

La pianificazione delle Riunioni di Controllo della Valutazione dovrebbe essere concordata all'inizio della valutazione nella Riunione di Avvio dei Lavori. Tuttavia, tale programmazione può essere modificata nel corso della valutazione.

Le Riunioni di Controllo della Valutazione possono essere convocate dall'OC, autonomamente o su richiesta dell'LVS.

Partecipanti

Alla Riunione di Controllo della Valutazione partecipano uno o più rappresentanti dell'OC e dell'LVS (almeno i rispettivi responsabili designati per la valutazione). Altri partecipanti, quali il Committente e/o il Fornitore, possono essere invitati se necessario. Il Committente può infatti desiderare che anche il Fornitore sia invitato a partecipare ad alcune o a tutte le riunioni.

L'organizzazione della Riunione di Controllo della Valutazione è responsabilità dell'OC, che è anche responsabile per la produzione e la distribuzione dell'ordine del giorno e del successivo verbale.

6 Conclusione

Nella fase di conclusione l'LVS produce il Rapporto Finale di Valutazione (RFV), in cui vengono riportati i verdetti e le considerazioni svolte dai Valutatori.

In linea di massima, i contenuti minimi di un RFV dovrebbero essere i seguenti:

- una chiara indicazione della specifica configurazione dell'ODV valutata;
- le informazioni di base sui risultati della valutazione, a beneficio dell'OC;
- le procedure di valutazione adottate, con riferimento al PDV, motivandone gli eventuali scostamenti;
- un riassunto dei risultati della valutazione in termini di Attività di valutazione, così come riportate nei corrispondenti capitoli del PDV;
- una lista dei ROA/ROE emessi nel corso della valutazione.

L'RFV viene emesso dall'LVS al termine della valutazione e inviato esclusivamente all'OC, che lo revisiona per accertare che fornisca un adeguato riassunto dei risultati della valutazione.

L'RFV viene usato dall'OC come base per la produzione del Rapporto di Certificazione.

7 Certificazione

La fase di certificazione prevede, nella sua parte iniziale, la revisione dell'RFV da parte dell'OC. Terminata questa parte, l'OC è nella condizione di produrre il Rapporto di Certificazione e il Certificato. Nel seguito vengono descritti gli adempimenti e le attività che l'OC, interagendo con l'LVS e il Committente, deve svolgere in questa fase.

7.1 Approvazione del Rapporto Finale di Valutazione

Quando l'OC riceve l'RFV dall'LVS, lo revisiona per determinare se soddisfa i requisiti dello Schema e dei criteri di valutazione. Se tale revisione dà esito positivo l'RFV viene approvato entro trenta giorni dalla sua ricezione.

Qualora nell'RFV vengano individuate delle anomalie risolvibili, l'OC ne richiede all'LVS la correzione. In tal caso, l'LVS è tenuto a modificare il rapporto entro i successivi quindici giorni. Tale richiesta sospende, fino al relativo esito, il decorso del suddetto termine di trenta giorni.

7.2 Ruolo dell'LVS nella fase di certificazione

Il ruolo dell'LVS durante la fase di certificazione è quello di fornire supporto tecnico all'OC nella revisione dell'RFV e nella produzione del Rapporto di Certificazione. Ad esempio, questo supporto potrebbe coinvolgere i Valutatori nel:

- fornire accesso a specifiche dimostrazioni tecniche (ad esempio materiali per la valutazione, risultati ottenuti dall'utilizzazione di specifici strumenti) per supportare le conclusioni dei Valutatori;
- fornire chiarimenti sui contenuti degli RA e dell'RFV;
- partecipare a un comitato/commissione di revisione tecnica, convocato se considerato necessario dall'OC (ad esempio se i risultati degli RA non sono chiari);
- revisionare il Rapporto di Certificazione per assicurare che sia tecnicamente accurato e sia un'equa valutazione dell'ODV o del PP e dell'RFV.

7.3 Rapporto di Certificazione

Entro trenta giorni dall'approvazione dell'RFV, l'OC redige una bozza di Rapporto di Certificazione (RC) che invia all'LVS e al Committente per avere conferma dell'assenza di errori materiali, nonché dell'assenza di elementi che contengano informazioni riservate. L'LVS e il Committente si pronunciano sulla richiesta entro i successivi cinque giorni lavorativi.

Acquisita la conferma da parte dell'LVS e del Committente, o decorso inutilmente il termine per la loro pronuncia, l'OC emette entro i successivi trenta giorni il Rapporto di Certificazione. Tale rapporto riassume i risultati della valutazione e contiene commenti e raccomandazioni da parte dell'OC. L'RC non deve contenere informazioni riservate, e può essere reso pubblico solo integralmente. In particolare, nel rapporto l'OC deve:

a) dichiarare se la valutazione è stata condotta secondo i criteri e la metodologia prevista dallo Schema nazionale;
b) dichiarare se il Profilo di Protezione è completo, congruente e tecnicamente corretto;
c) dichiarare se il Traguardo di Sicurezza è completo, congruente e tecnicamente corretto;
d) dichiarare se l'Oggetto della Valutazione soddisfa il Traguardo di Sicurezza al livello di garanzia richiesto;
e) identificare le eventuali vulnerabilità residue ed eventualmente raccomandare delle contromisure.

Nei casi di valutazioni di ODV particolarmente complessi, i termini di cui sopra possono essere differiti, d'intesa con le parti. Ai fini del decorso dei predetti termini non è computato il tempo richiesto per il riscontro ad eventuali osservazioni e chiarimenti.

7.4 Emissione del Certificato

In caso di valutazione positiva, l'OC allega all'RC il relativo Certificato, cioè l'attestazione che l'ODV o il PP è stato valutato da un LVS accreditato in conformità con i criteri di valutazione e con le procedure dello Schema. Il Certificato si applica soltanto alla specifica versione dell'ODV o del PP nella configurazione valutata ed attesta che il livello di garanzia richiesto è stato raggiunto. Per i dettagli si fa esplicito riferimento al TDS o al PP e all'RC.

8 Chiusura di un processo di valutazione

La chiusura formale del processo di valutazione avviene con l'emissione del Rapporto di Certificazione e del Certificato.

Successivamente si tiene di norma una Riunione di Chiusura del Processo di valutazione, convocata e organizzata dall'OC di sua iniziativa o su richiesta dell'LVS o del Committente.

8.1 Riunione di Chiusura della Valutazione

Gli obiettivi di una Riunione di Chiusura della Valutazione sono:

- consentire alle organizzazioni coinvolte in una valutazione di esprimere un verdetto sulla conduzione complessiva della valutazione;
- fornire all'LVS commenti sulla sua esecuzione della valutazione;
- registrare ogni esperienza maturata nella valutazione;
- accordarsi sull'assegnazione dei materiali del processo di valutazione;
- stabilire il periodo di tempo in cui i materiali archiviati dovranno essere conservati.

Partecipanti

Alla Riunione di Chiusura della Valutazione partecipano di norma i responsabili per la valutazione designati da ciascuna organizzazione coinvolta nella valutazione.

A discrezione dell'OC e in consultazione con l'LVS, possono essere invitati altri partecipanti, quali ad esempio il Fornitore ed altri Valutatori dell'LVS.

L'OC sarà responsabile della produzione e della distribuzione dell'ordine del giorno e del successivo verbale.

8.2 Assegnazione dei materiali di un processo di valutazione

La chiusura di un processo di valutazione include l'assegnazione di tutti i materiali associati al processo stesso. Tale assegnazione dovrebbe comprendere le seguenti attività:

- archiviazione di materiali da parte dell'LVS;
- archiviazione di materiali da parte dell'OC;
- restituzione di materiali agli originatori;
- distruzione di materiali.

Durante una valutazione, i materiali dovrebbero essere organizzati in modo da rendere l'effettiva chiusura del processo di valutazione più semplice possibile. La chiusura di un processo di valutazione può anche essere semplificata restituendo e/o distruggendo i documenti sostituiti durante la valutazione.

Materiali archiviati dall'LVS

Il manuale di qualità dell'LVS dovrebbe indicare i requisiti per l'archiviazione. Come minimo, dovrebbero essere archiviati dall'LVS i seguenti materiali del processo di valutazione:

- il TDS o il PP, l'elenco dei materiali per la valutazione, il PDV;
- la corrispondenza scambiata nel corso della valutazione che ha una relazione diretta con il risultato della valutazione;
- l'RFV e l'RC.

Materiali archiviati dall'OC

Normalmente l'OC archivia l'RC e le proprie copie della documentazione del processo di valutazione in modo da soddisfare i propri specifici requisiti per l'archiviazione.

Materiali restituiti al Committente/Fornitore

Il Committente e/o il Fornitore dovrebbero conservare i materiali loro assegnati per il periodo stabilito nella Riunione di Chiusura della Valutazione. La disponibilità di tali materiali agevolerà il processo di gestione e mantenimento dei Certificati per l'ODV o PP se, ad esempio, in futuro:

- sorgesse una disputa;
- fosse richiesta una rivalutazione;
- fosse richiesta una riutilizzazione dei risultati della valutazione.

Materiali distrutti

In generale, i materiali cartacei ricevuti dall'LVS da parte del Committente o del Fornitore non dovrebbero essere archiviati, ma dovrebbero essere restituiti o distrutti, come concordato nella RAL.

Normalmente dovrebbero essere distrutti i seguenti materiali cartacei del processo di valutazione:

1) documentazione minore, che non contiene informazioni tecniche, generata durante la valutazione (ad esempio lettere, agende);
2) documentazione di gestione/controllo del processo di valutazione (ad esempio, i verbali di Riunioni di Controllo della Valutazione).

8.3 Inserimento di annotazioni nell'elenco dei prodotti, sistemi e PP certificati

Contestualmente all'emissione del Rapporto di Certificazione e del Certificato, l'OC inserisce nell'elenco dei prodotti, sistemi e PP certificati, pubblicato sul proprio sito web [OCSI], un'annotazione per quel prodotto, sistema o PP, con la versione elettronica del TDS e dell'RC.

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

[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>

Lista degli acronimi

CC	=	Common Criteria
EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
IT	=	Information Technology
LGP	=	Linea Guida Provvisoria
LVS	=	Laboratorio per la Valutazione della Sicurezza
NIS	=	Nota Informativa dello Schema
NOC	=	Nota dell'Organismo di Certificazione
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
PDV	=	Piano Di Valutazione
PP	=	Profilo di Protezione (Protection Profile)
RA	=	Rapporto di Attività
RAL	=	Riunione di Avvio dei Lavori
RC	=	Rapporto di Certificazione
RFV	=	Rapporto Finale di Valutazione
RO	=	Rapporto di Osservazione
ROA	=	Rapporto di Osservazione per Anomalia
ROE	=	Rapporto di Osservazione per Errore
ROS	=	Rapporto di Osservazione sullo Schema
TDS	=	Traguardo di Sicurezza (ST - Security Target)