Organismo di Certificazione
della Sicurezza Informatica

Nota Informativa dello Schema N. 3/07

Modifiche alla LGP3

Marzo 2007
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

INDICE

Scopo del documento

La Nota Informativa dello Schema N. 3/07, nel seguito brevemente indicata NIS 3/07, viene emessa dall'OCSI in base a quanto previsto dalle vigenti pubblicazioni dello Schema, ed in particolare dalla Linea Guida Provvisoria LGP3.

Il presente documento ha lo scopo di modificare e integrare le procedure descritte nella Linea Guida Provvisoria LGP3 avente per titolo "Procedure di Valutazione".

In particolare, sono stati modificati i seguenti paragrafi della LGP3: 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, che sostituiscono integralmente gli analoghi paragrafi attualmente contenuti nella LGP3 stessa.

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 3/07 sono immediatamente operative e quindi sostituiscono a tutti gli effetti le parti corrispondenti contenute nella LGP3; tali disposizioni verranno successivamente integrate nelle Linee Guida Definitive.

1 Introduzione

L'istituzione dell'Organismo di Certificazione italiano per la sicurezza dei sistemi e dei prodotti nel settore della tecnologia dell'informazione, avvenuta attraverso un decreto del Ministro per l'Innovazione e le Tecnologie di concerto con i Ministri delle Comunicazioni, delle Attività Produttive e dell'Economia e delle Finanze, si pone come naturale termine di un percorso che è stato individuato e seguito in questi ultimi anni anche da numerosi altri stati nazionali, sia in Europa sia nel resto del mondo.

Il decreto riconosce che l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI) del Ministero delle Comunicazioni possiede i requisiti di indipendenza, affidabilità e competenza tecnica richiesti dalla decisione della Commissione europea del 6 novembre 2000 (2000/709/CE) e stabilisce che:
"l'ISCTI è l'Organismo di Certificazione della sicurezza informatica nel settore della tecnologia dell'informazione, anche ai sensi dell'articolo 10 del decreto legislativo 23 gennaio 2002, n. 10 e dell'articolo 3, paragrafo 4 della direttiva 1999/93/CE".

Per consentire l'applicazione dello Schema Nazionale previsto dal decreto l'Organismo di Certificazione ha predisposto le "Linee Guida Provvisorie" (LGP). Tali LGP sono organizzate in documenti distinti: una breve sintesi del loro contenuto è presentata nella LGP1.

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 LVS, un Committente, un Fornitore e l'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, vale a dire:

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 sistema per l'elaborazione elettronica delle informazioni, cioè l'Oggetto Della Valutazione (ODV), così come definito in ITSEC o nei Common Criteria;

- 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.

E' importante osservare che la differenza più grande tra 'prodotto' e 'sistema' risiede nell'ambiente operativo in cui la soluzione viene impiegata. Infatti, l'ambiente in cui il 'sistema' andrà ad operare è perfettamente conosciuto dal Committente e Fornitore e da essi ben documentato, mentre per il 'prodotto' il Fornitore può definire solo un generico ambiente applicativo della soluzione sicura e non potrà mai precisare il reale ambito operativo di utilizzo, anche se fornisce un metodo di uso del prodotto e una lista delle minacce considerate nell'ambiente ipotizzato. Il processo di valutazione tra un sistema ed un prodotto non cambia se non per il tempo impiegato; infatti, il PDV di un prodotto richiede meno tempo rispetto ad un sistema, sebbene le attività di verifica siano le stesse.

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 ri-valutazione di un ODV o di un PP;
- una riutilizzazione dei risultati di una precedente valutazione di un ODV o di un PP.

Il documento è strutturato come segue.

Il capitolo 2 definisce il ruolo e le responsabilità dei Valutatori.

Il capitolo 3 descrive l'organizzazione di un processo di valutazione distinguendo le tre fasi di preparazione, conduzione e conclusione.

Il capitolo 4 illustra le procedure da seguire nella fase di preparazione; in particolare fornisce indicazioni sulla produzione di un PDV e sull'elenco dei materiali per la valutazione.

Il capitolo 5 definisce le procedure da seguire durante la fase di conduzione, ed in particolare la finalità e il contenuto delle diverse tipologie di rapporti prodotti nel corso della valutazione.

Il capitolo 6 descrive la fase di conclusione, con il rilascio da parte dell'LVS del Rapporto Finale di Valutazione.

Il capitolo 7 descrive il processo di certificazione, con il rilascio da parte dell'Organismo di Certificazione del Rapporto di Certificazione e del Certificato.

2 Ruolo e responsabilità dell'LVS

In questo capitolo saranno 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 sarà ampiamente descritto nei capitoli 3, 4, 5.

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;
- all'OC.

L'assistenza può coprire ogni aspetto della valutazione: tipicamente consisterà 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.

L'LVS deve informare l'OC qualora si verifichi un potenziale conflitto di interessi. In tal caso, l'OC verificherà che tutte le condizioni poste agli LVS siano rispettate e determinerà se i potenziali conflitti di interessi possono effettivamente minacciare l'integrità delle valutazioni condotte all'interno dello Schema.

2.3 Trasmissione dei materiali della valutazione e della documentazione

L'LVS, tenendo in considerazione le richieste e le esigenze del Committente, concorda con quest'ultimo le modalità di trasmissione della documentazione e dei materiali attinenti alla valutazione. Tale accordo viene formalizzato nel contratto tra il Committente e l'LVS e riguarda sia la trasmissione dei materiali tra Committente e LVS sia le modalità di trasmissione della documentazione dall'LVS all'OC.

Per quello che concerne la trasmissione di documenti tra l'LVS e l'OC, è comunque richiesta la trasmissione dei documenti ufficiali in forma cartacea. L'OC si riserva la possibilità di consentire l'utilizzo di metodi elettronici di trasmissione protetta dei documenti di lavoro, con modalità che verranno concordate durante la Riunione di Avvio dei Lavori.

3 Organizzazione della valutazione

L'OC deve poter controllare una valutazione durante il suo intero svolgimento per esprimere un verdetto sui risultati di tale attività. Questo processo è reso considerevolmente più semplice se tutte le valutazioni sono organizzate secondo uno standard comune.

3.1 Processo di valutazione

Ai fini della pianificazione e del resoconto delle attività, un processo di valutazione corrisponde alle attività di valutazione svolte da un LVS su un singolo ODV o PP. Ciascun processo di valutazione 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 produrranno 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 potranno 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 Committente e LVS, quest'ultimo deve sottoporre una richiesta perché la valutazione sia formalmente accettata nello Schema. A tal fine, l'LVS sottopone all'OC:

1) un TDS o un PP completo;
2) un PDV completo;
3) una descrizione dell'estensione e della natura dell'attività di preparazione svolta con il Committente, compresi i nomi delle persone coinvolte;
4) i nomi dei Valutatori incaricati di condurre la valutazione;
5) i nomi dei responsabili per la valutazione designati dall'LVS e dal Committente.

L'LVS deve consegnare al Committente il facsimile del contratto, fornendogli le informazioni necessarie per la stima dei compensi dovuti all'OC. Il Committente rilascia una ricevuta firmata che l'LVS a sua volta trasmette all'OC insieme alla richiesta di accettazione della valutazione. Quando l'OC riceve il PDV, calcola il costo per il Committente e gli invia il contratto completo nella parte economica, che dovrà essere restituito firmato all'OC in sede di Riunione di Avvio dei Lavori.

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

L'LVS ed il Committente devono designare un proprio responsabile per ogni valutazione, mentre l'OC nomina uno o più certificatori, individuando tra questi un referente che fungerà da interfaccia verso l'LVS e il Committente.

Nel corso della fase di conduzione possono essere prodotti rapporti di vario tipo:

- Rapporti di Attività (RA)
- Rapporti di Osservazione (RO)
- Rapporti di Osservazione sullo Schema (ROS)
- Rapporto delle Metodologie (RM)

Tali rapporti saranno descritti in dettaglio nel cap. 5.

Nella fase di conclusione, l'LVS produce un Rapporto Finale di Valutazione (RFV) che riassume tutti i risultati ottenuti durante la valutazione e che verrà utilizzato dall'OC come base per la stesura del Rapporto di Certificazione.

3.2 Attività di valutazione

Per scopi gestionali e per facilitare il resoconto delle attività, la valutazione è suddivisa in Attività di valutazione. Le singole azioni da effettuare per ciascuna Attività di valutazione dovranno essere specificate nel PDV.

I risultati raggiunti durante le Attività di valutazione saranno contenuti in uno o più Rapporti di Attività (RA). Tali rapporti saranno comunque compresi nell'RFV. Qualora i Valutatori ne ravvisino la necessità, gli RA potranno essere inviati all'OC nel corso della valutazione. Dettagli sul formato e sul contenuto di tali rapporti saranno dati nel seguito (par. 5.5).

3.3 Archivio dei processi di valutazione

Per ciascun processo di valutazione, l'LVS deve mantenere un archivio di tutte le informazioni (ad esempio materiali per la valutazione, attività svolte, risultati della valutazione, rapporti di osservazione, contatti col Committente).

L'archivio per ciascun processo di valutazione dovrebbe essere mantenuto in accordo a quanto previsto nel manuale di qualità dell'LVS relativamente alle procedure di archiviazione (cfr. LGP2).

3.4 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 a 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 o 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 potranno essere apportate durante le Riunioni di Controllo della Valutazione.

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

3.5 Diritti di proprietà

Prima dell'inizio di una valutazione, l'LVS e il Committente determineranno chi tra loro dovrà detenere i diritti di proprietà dell'RFV e di altri 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 ri-valutare 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.

4 Preparazione

Questo capitolo descrive le procedure che devono essere seguite da un LVS nella fase di preparazione della valutazione.

Il primo passo in questa fase è compiuto dal Committente, che sceglie un LVS per realizzare il lavoro di preparazione della valutazione. L'LVS prescelto esegue le seguenti azioni:

1) revisiona il TDS o il PP per determinare se fornisce una base adeguata per la valutazione;
2) prepara un Piano di Valutazione (PDV);
3) prepara un elenco dettagliato di materiali per la valutazione.

Prima che possa iniziare la fase di conduzione, la valutazione deve essere approvata dall'OC. Infatti, l'OC potrebbe opporsi allo svolgimento di una valutazione basandosi sul fatto che l'indipendenza o l'imparzialità dell'LVS possono essere compromesse, o che il tipo di ODV o PP è inaccettabile per lo Schema. Durante la fase di preparazione deve quindi essere posta molta attenzione per assicurare l'indipendenza o l'imparzialità.

4.1 Obiettivi

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.

L'ambito di questa fase è oggetto di accordo tra il Committente e l'LVS. Ad esempio, il Committente può richiedere all'LVS attività di assistenza. In tal caso valgono le considerazioni fatte nel par. 2.1.

Prima che sia formalizzato un contratto per lo svolgimento della valutazione, l'LVS deve fornire al Committente un preventivo in cui siano specificati:

1) gli oneri dovuti all'LVS stesso per la valutazione e l'eventuale assistenza;
2) i criteri con cui verranno calcolati tutti gli oneri dovuti all'OC.

4.2 Adeguatezza per la valutazione

L'LVS selezionato per svolgere la fase di preparazione effettua una revisione del TDS o del PP. Nel caso fosse necessario modificare il TDS o il PP, l'LVS richiederà al Committente di apportare le necessarie variazioni.

Assicurarsi che il TDS o il PP costituisca una base adeguata per la valutazione è un adempimento separato dallo stabilire la conformità di un TDS o di un PP rispetto ai criteri di valutazione, operazione che verrà invece effettuata nella fase di conduzione.

4.3 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 o ritardi. Tipicamente, questi aspetti saranno discussi tra il Fornitore, il Committente e l'LVS prima che questi ultimi due formalizzino un contratto per lo svolgimento della valutazione.

4.4 Piano di Valutazione (PDV)

Generalità

Una volta stabiliti i requisiti per la valutazione, è necessario pianificare le Attività di valutazione. Tale pianificazione è documentata, dettagliando le singole azioni, in un Piano di Valutazione (PDV).

Un PDV così dettagliato consentirà, tra l'altro, di verificare che le Attività di valutazione previste siano conformi ai criteri di valutazione e allo Schema e adeguate a conseguire la certificazione al livello di garanzia richiesto.

Parti interessate

Le parti interessate a un PDV sono:

- l'LVS che effettua il lavoro di valutazione;
- l'OC;
- il Committente.

Contenuti

Il PDV dovrebbe 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.

Approvazione

Il contenuto di un PDV deve essere approvato dall'OC per confermare che:

- sono stati correttamente applicati i requisiti dei criteri di valutazione e dello Schema e/o ogni previsto scostamento da questi è stato accettato;
- la pianificazione delle attività è commisurata ai requisiti della valutazione;
- l'attività di valutazione che deve essere effettuata è in accordo al livello di garanzia richiesto;
- il lavoro, se completato con successo, è adeguato per la certificazione del PP oppure dell'ODV al livello di garanzia richiesto;
- gli strumenti da utilizzare sono giudicati dall'OC idonei per la valutazione.

Aggiornamenti

Nel corso di una valutazione, potrebbe essere necessario emendare alcune parti di un PDV per poter valutare l'ODV al livello di garanzia richiesto. Per assicurarsi che qualsiasi modifica al PDV non abbia un impatto sulla sua accettabilità per quello specifico livello di garanzia, tutte le variazioni apportate a un PDV devono essere approvate dall'OC. Un aggiornamento del PDV può essere necessario, 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.

Per una valutazione di breve durata, quale ad esempio nel caso di un PP, è improbabile che il PDV debba essere aggiornato.

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 ri-valutazioni 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. Per individuare scostamenti accettabili da una rigida interpretazione dello Schema o dei criteri di valutazione si possono utilizzare Rapporti di Osservazione sullo Schema (ROS), come descritto nel seguito (par. 5.5).

È importante osservare che una modifica nel PDV può, in alcuni casi, richiedere emendamenti al contratto tra il Committente e l'LVS.

4.5 Elenco dei materiali per la valutazione

Generalità

Perché 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 sarà dettagliato dai Valutatori per ogni specifica valutazione, e potrà costituire un documento separato rispetto al PDV oppure far parte integrante del PDV stesso.

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 (nel caso di un sistema);
- l'accesso al sito dello sviluppo dell'ODV.

Per la produzione di tutti i tipi di documentazione relativi alla valutazione e certificazione è obbligatorio l'uso della lingua italiana, tranne nei seguenti casi, nei quali si raccomanda invece l'uso della lingua inglese:

- parti riportate integralmente dai criteri internazionali, quali ad esempio requisiti funzionali e di garanzia definiti secondo i Common Criteria, brani estratti da Profili di Protezione, ecc.
- eventuali terminologie in lingua inglese, non tradotte nel glossario di riferimento dello Schema, utilizzate nei documenti originali che descrivono i criteri e le metodologie;
- documenti di valutazione e certificazione già esistenti in lingua inglese.

Parti interessate

L'elenco dei materiali per la valutazione è prodotto per essere usato da:

- i Valutatori;
- l'OC;
- il Committente;
- il Fornitore.

Contenuti

L'elenco dei materiali per la valutazione comprenderà tipicamente i seguenti dettagli, per ciascun elemento presente:

1) numero progressivo;
2) titolo o nome;
3) riferimenti incrociati ai criteri di valutazione e a generici materiali identificati nel PDV;
4) stato della consegna, ad esempio:
   - data prevista;

   - versione;
5) revisioni future pianificate, ad esempio:
   - data prevista;
   - versione;
6) metodo di archiviazione.

I materiali richiesti per la valutazione e le date previste per la loro consegna devono essere conformi al PDV.

4.6 Richiesta di iscrizione della valutazione nello Schema

A conclusione della fase di preparazione, l'LVS deve sottoporre una richiesta affinché la valutazione sia formalmente accettata nello Schema. A tal fine, l'LVS invia all'OC:

1) il TDS o il PP;
2) il PDV;
3) una descrizione dell'estensione e della natura dell'attività di preparazione svolta con il Committente, compresi i nomi delle persone coinvolte;
4) i nomi dei Valutatori incaricati di condurre la valutazione;
5) i nomi dei responsabili per la valutazione designati dall'LVS e dal Committente.

4.7 Riepilogo della fase di preparazione

Elementi di ingresso

Gli elementi di ingresso a questa fase sono:

1) un TDS o un PP;
2) l'accesso ai materiali per la valutazione disponibili;
3) la pianificazione predisposta per lo sviluppo dell'ODV (per valutazioni concomitanti).

Elementi di uscita

Gli elementi di uscita da questa fase sono:

1) un PDV;
2) un elenco dei materiali per la valutazione;
3) un rapporto sull'adeguatezza per la valutazione (opzionale);
4) una richiesta di iscrizione della valutazione nello Schema.

5 Conduzione

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

Durante la fase di conduzione, i Valutatori effettuano l'attività di valutazione tecnica come definita dal PDV. I risultati delle attività di valutazione saranno riportati in uno o più Rapporti di Attività (RA).

Se durante la valutazione sono individuate anomalie o errori, questi devono essere tempestivamente notificati: per il caso di anomalie si utilizzano i Rapporti di Osservazione per Anomalia (ROA), mentre per il caso di errori e vulnerabilità sfruttabili si utilizzano i Rapporti di Osservazione per Errore (ROE).

Problemi minori o esigenze di chiarimenti che potrebbero verificarsi durante la valutazione saranno risolti mediante comunicazioni informali tra le parti interessate.

Questo capitolo descrive le procedure che dovrebbero essere seguite nell'effettuare i seguenti aspetti dell'attività di valutazione:

1) avvio della valutazione;
2) realizzazione delle singole azioni di valutazione;
3) produzione dei Rapporti di Osservazione (ROA e ROE);
4) produzione dei Rapporti di Attività (RA);
5) produzione dei Rapporti di Osservazione sullo Schema (ROS) e delle Note dell'OC (NIS, NOC);
6) produzione del Rapporto delle Metodologie (RM);
7) controllo dell'attività di valutazione.

In Figura 1 sono illustrati gli scambi di materiali e rapporti tra le varie entità coinvolte nella fase di conduzione della valutazione.

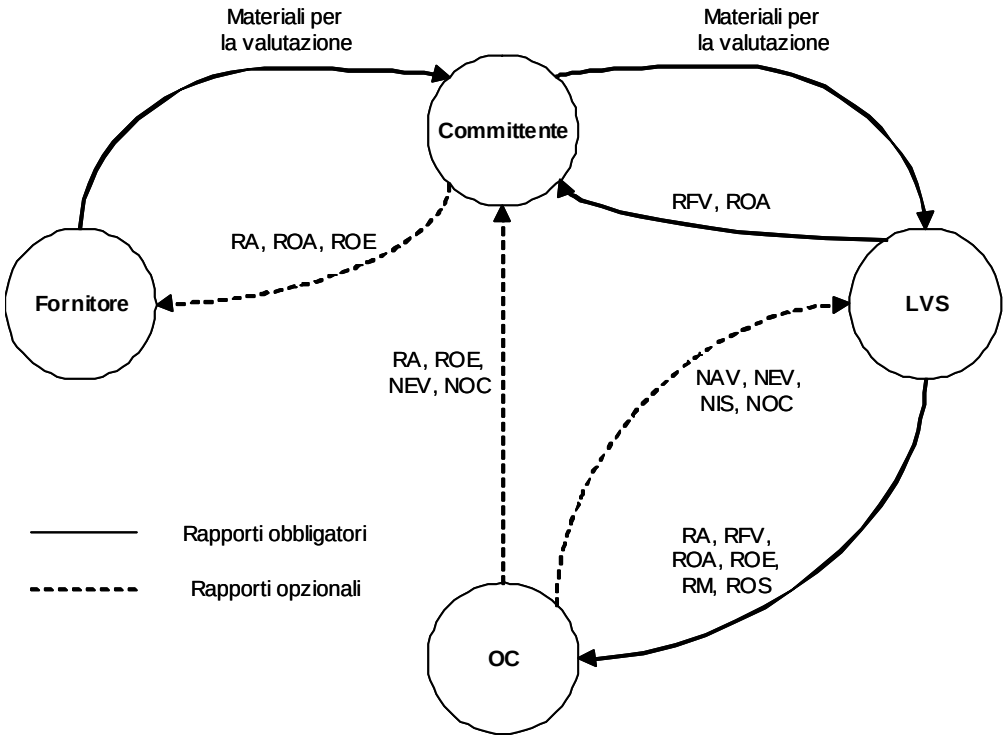

Figura 1 – Flussi informativi tra le entità coinvolte nella valutazione.

5.1 Obiettivi

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 in modo adeguato;
- 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.

5.2 Avvio del processo di valutazione

Generalità

All'avvio del processo di valutazione sono previste le seguenti azioni da parte dell'LVS:

- tenere una riunione iniziale interna ed avviare le procedure appropriate per il processo di valutazione;
- ottenere accettazione formale della valutazione nello Schema da parte dell'OC;
- consegnare all'OC una Notifica di Inizio Lavori (NIL);
- chiedere l'inserimento di una annotazione nell'elenco dei prodotti, sistemi e PP in valutazione.

Accettazione formale del processo di valutazione

Prima che possa iniziare la valutazione di un ODV o di un PP, l'LVS deve assicurarsi che l'OC approvi il processo di valutazione e lo accetti nello Schema.

Infatti, è possibile che l'OC si opponga a una valutazione sulla base dei seguenti motivi:

- un LVS non soddisfa i requisiti di indipendenza e imparzialità;
- il grado di robustezza dei meccanismi di sicurezza è inadeguato al livello di garanzia richiesto.

Se l'OC non ha obiezioni, entro 15 giorni lavorativi dalla ricezione della richiesta nomina uno o più certificatori, individuando tra questi un referente che fungerà da interfaccia verso l'LVS, ed invia all'LVS l'autorizzazione ad iniziare la valutazione.

Notifica di Inizio Lavori (NIL)

Successivamente alla comunicazione dell'esito favorevole della richiesta di iscrizione allo Schema, l'LVS notifica formalmente all'OC l'effettivo inizio della valutazione, attraverso una Notifica di Inizio Lavori (NIL).

Il Committente, per sue esigenze specifiche (per esempio per stringenti requisiti temporali), può richiedere all'LVS di presentare la Notifica di Inizio Lavori contestualmente alla presentazione del PDV. In questo caso il Committente deve essere consapevole che sono a suo carico tutti gli oneri e i rischi relativi alla mancata attesa della comunicazione ufficiale dell'OC.

Riunione di Avvio dei Lavori

Dopo l'accettazione formale del processo di valutazione, l'OC convocherà una Riunione di Avvio dei Lavori (RAL), durante la quale saranno affrontati diversi argomenti, quali ad esempio:

- comunicazione dei nominativi dei certificatori 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 (archivio di base);
- 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);
- riutilizzazione di risultati di precedenti valutazioni;
- requisiti e frequenza delle Riunioni di Controllo della 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 della stesura del verbale.

Alla Riunione di Avvio dei Lavori parteciperanno, oltre all'OC stesso, l'LVS e il Committente (di solito i rispettivi responsabili designati per la valutazione). Vista

l'importanza di tale riunione, potrà rendersi necessario invitare altri partecipanti, quali ad esempio il Fornitore.

Nella Riunione di Avvio dei Lavori sono assegnati i seguenti ruoli:

1) Presidente: un rappresentante dell'OC o dell'LVS;
2) Segretario: un rappresentante dell'LVS.

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

Un ODV o un PP in valutazione deve essere incluso nell'elenco dei prodotti, sistemi e PP in valutazione, gestito dall'OC. Una richiesta in tal senso viene inoltrata dall'LVS all'OC tramite la NIL. L'avvenuto inserimento nell'elenco sarà notificato dall'OC al Committente e all'LVS.

Se un ODV o un PP in valutazione è inserito nell'elenco, ma la valutazione viene sospesa, l'OC informerà sia l'LVS sia il Committente che quell'ODV o PP verrà rimosso dalla successiva versione di tale elenco. Il Committente può sottoporre all'OC argomenti a favore del mantenimento nell'elenco. E' comunque prerogativa dell'OC la decisione riguardo al mantenimento della valutazione nell'elenco. Un ODV o un PP potrà essere reintegrato nell'elenco quando i problemi che hanno condotto alla sua esclusione saranno stati risolti.

5.3 Realizzazione di un'attività di valutazione

Generalità

La valutazione è effettuata svolgendo le Attività di valutazione definite nel PDV. Ciascuna Attività di valutazione è specificata nel PDV come l'insieme delle singole azioni che devono essere eseguite.

A conclusione delle Attività di valutazione devono essere prodotti uno o più Rapporti di Attività (RA), come sarà descritto nel par. 5.5.

Se nel corso della valutazione sono riscontrate anomalie o errori, devono essere generati Rapporti di Osservazione.

Materiali per la valutazione

Per poter effettuare le Attività di valutazione, i Valutatori devono avere a disposizione i materiali per la valutazione richiesti. Normalmente, una copia di tali materiali dovrà essere inviata anche all'OC, con modalità che verranno concordate durante la Riunione di Avvio dei Lavori.

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 avrà inevitabilmente un impatto sui tempi di esecuzione della valutazione. Perché 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 e non saranno ulteriormente considerati in questo documento. Tuttavia, tali cambiamenti possono avere un impatto sulle risorse di certificazione disponibili, e quindi l'LVS deve avvisare l'OC sui ritardi e sulle modifiche proposte nelle tappe fondamentali della valutazione e certificazione. La non disponibilità o i ritardi nel rilascio dei materiali per la valutazione può condurre alla produzione di un Rapporto di Osservazione.

Tutti i materiali ricevuti per un processo di valutazione devono essere registrati nell'elenco dei materiali per quel processo di valutazione. Il contenuto degli elenchi dei materiali per la valutazione deve essere mantenuto aggiornato dall'LVS e deve essere consultabile nel corso della valutazione. L'elenco completo dei materiali per la valutazione deve essere contenuto nell'RFV.

Supporto da parte del Fornitore

In alcuni casi, l'attività di valutazione può richiedere il supporto tecnico da parte del Fornitore. Qualora la natura delle informazioni da scambiare sia di entità minore, il contatto tra il Fornitore e il Committente o l'LVS può assumere la forma di riunioni o scambio di corrispondenza senza coinvolgimento da parte dell'OC.

Si raccomanda di regolamentare contrattualmente tra Committente e Fornitore l'attività di supporto alla valutazione da parte del Fornitore.

L'LVS deve annotare in un apposito registro tutti i contatti significativi con il Fornitore che influenzino la valutazione.

Prima di iniziare le prove di intrusione, i Valutatori dovrebbero assicurarsi che il Fornitore o il Committente firmi un'opportuna dichiarazione di esonero di responsabilità affinché i Valutatori non siano ritenuti responsabili di eventuali danni durante le prove stesse.

Registrazione dei risultati e osservazioni

Quando ciascuna Attività di valutazione è completata, il lavoro svolto, le osservazioni fatte ed i risultati ottenuti devono essere registrati chiaramente e permanentemente.

In particolare, l'LVS deve annotare le informazioni riguardanti l'uso di strumenti in una valutazione, in quanto:

- l'OC deve assicurare che la valutazione sia stata condotta in una maniera conforme al livello di garanzia richiesto; è quindi necessario conoscere come e perché ciascuno strumento è stato usato per una data attività, o perché non è stato utilizzato nessuno strumento;
- può essere necessario condurre prove che possano essere ripetute o riprodotte, in particolare se alcuni risultati sono oggetto di disputa tra alcune parti (ad esempio il Fornitore, il Committente o gli utenti);
- nel caso di una ri-valutazione di un ODV o di un PP, i Valutatori che conducono la ri-valutazione possono ritenere opportuno usare uno strumento in modo conforme alla valutazione originale;
- la comunità di valutazione può aver beneficio dalla conoscenza dei risultati ottenuti utilizzando specifici strumenti in una valutazione.

5.4 Rapporti di Osservazione (RO)

Obiettivo

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.

Non è di solito soddisfacente che i problemi siano notificati soltanto alla fine della valutazione, perché ciò non consentirebbe al Committente di prendere le appropriate contromisure, come ad esempio:

- abbandonare la valutazione per effetto del problema;
- sospendere la valutazione finché il problema non sia stato risolto.

Eventuali vulnerabilità sfruttabili o altre anomalie rilevate nel corso del processo di valutazione, devono essere riportate dai Valutatori sotto forma di Rapporti di Osservazione.

L'OC esaminerà tutti i Rapporti di Osservazione per approvare le conclusioni e stabilire l'impatto sulla certificazione.

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.

Un'indicazione sulla struttura tipica e sui contenuti minimi di un ROE è la seguente:

1) Generalità
   - identificazione dell'LVS;
   - identificazione della valutazione;
   - identificazione della parte del lavoro di valutazione;
   - numero del ROE;
   - data;
   - oggetto del ROE;
   - firma del Valutatore che ha identificato il problema;
   - firma del responsabile della Valutazione che ha autorizzato l'emissione del ROE.
2) Osservazioni, implicazioni e raccomandazioni

   In tale capitolo dovranno essere riportate le singole osservazioni relative agli errori riscontrati. In particolare, per ogni osservazione (numerata progressivamente) dovrà essere presente:
   - un paragrafo recante la *descrizione* dettagliata dell'errore riscontrato durante la valutazione dell'ODV, corredata dalle prove o dalle azioni che hanno evidenziato l'errore, riportando i documenti di riferimento;
   - un paragrafo recante le *implicazioni* per la sicurezza che il problema identificato nell'osservazione può comportare e le minacce, i rischi e le vulnerabilità correlate. Deve essere indicata l'unità di lavoro nello svolgimento della quale è stato evidenziato l'errore. Devono essere inserite le implicazioni sulla valutazione, compresa l'eventuale revisione della pianificazione temporale prevista nel PDV;
   - un paragrafo di *raccomandazioni*, recante le opzioni attraverso le quali l'errore evidenziato nelle osservazioni può essere risolto (nel caso sia possibile); tali indicazioni possono essere rivolte all'OC per la eventuale sospensione della valutazione.

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, come appropriato, evidenziando la necessità di una risposta tempestiva. In caso di dubbio sull'opportunità di emettere un ROA, dovrebbe essere consultato l'OC.

La struttura tipica e i contenuti minimi di un ROA sono i seguenti:

1) Generalità
   - identificazione dell'LVS;
   - identificazione della valutazione;
   - identificazione della parte del lavoro di valutazione;
   - numero del ROA;
   - data;
   - oggetto del ROA;
   - firma del Valutatore che ha identificato il problema;
   - firma del responsabile della valutazione che ha autorizzato l'emissione del ROA.
2) Osservazioni, implicazioni e raccomandazioni

   In tale capitolo dovranno essere riportate le singole osservazioni relative alle anomalie riscontrate. In particolare, per ogni osservazione (numerata progressivamente) dovrà essere presente:
   - un paragrafo recante la *descrizione* dettagliata dell'anomalia riscontrata durante la valutazione dell'ODV, riportando i documenti di riferimento e le osservazioni dell'LVS se il problema è di carattere procedurale;
   - un paragrafo recante le *implicazioni* per la sicurezza o per la prosecuzione della valutazione che il problema identificato nell'osservazione può comportare e le minacce, i rischi e le vulnerabilità correlate. Deve essere indicata l'unità di lavoro nello svolgimento della quale è stata evidenziata l'anomalia. Devono essere inserite le implicazioni sulla valutazione, compresa l'eventuale revisione della pianificazione temporale prevista nel PDV;
   - un paragrafo di *raccomandazioni*, recante le opzioni attraverso le quali l'anomalia evidenziata nelle osservazioni può essere risolta (nel caso sia possibile). Tali indicazioni possono essere rivolte:
     - al Committente, per eventuali modifiche al TDS o al PP;

– al Fornitore, indicando le modifiche sull'implementazione dell'ODV.

Le indicazioni suddette devono essere espresse in termini generali, poiché i Valutatori non possono contribuire allo sviluppo dell'ODV o alla preparazione del PP.

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 coprire:

- un singolo problema;
- più problemi tra loro collegati.

Ciascun Rapporto di Osservazione è individuato univocamente da un numero di riferimento, che comprende un identificativo del processo di valutazione cui si riferisce e un numero seriale progressivo. Nel caso in cui in un Rapporto di Osservazione siano documentati più problemi collegati, ciascuno di essi dovrebbe essere numerato separatamente. Ciascun problema dovrebbe essere indicato separatamente anche nell'elenco dello stato dei Rapporti di Osservazione; gli avanzamenti relativi a ciascun problema dovranno essere seguiti singolarmente.

I Rapporti di Osservazione, prima di essere emessi, 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. Se necessario, sarà tenuta una riunione tecnica tra l'LVS e il Committente; possono essere invitati a partecipare anche rappresentanti del Fornitore, purché il Committente non abbia obiezioni. Lo scopo di tale riunione è discutere i dettagli tecnici del ROA e determinare le azioni future.

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 in cui non sia raggiunto un accordo, possono essere convocate ulteriori riunioni con la partecipazione dell'OC.

Qualora lo ritenga necessario, l'OC potrà esprimere il proprio parere sui problemi esposti nel ROA emettendo una Nota per Anomalia nella Valutazione (NAV), che sarà inviata all'LVS che ha generato il ROA.

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. Inoltre, l'OC potrà emettere una Nota per Errore nella Valutazione (NEV), che sarà inviata all'LVS che ha generato il ROE ed eventualmente al Committente, se lo ritenesse opportuno. Qualora, invece, la soluzione del problema implichi azioni più rilevanti (quali ad esempio modifiche del PDV), l'OC convocherà un'apposita riunione a cui parteciperanno l'LVS e il Committente (ed eventualmente il Fornitore) per verificare la fattibilità e l'opportunità delle azioni richieste.

Si ricorda infine che, qualora ne ravvisasse la necessità, l'OC potrà emettere autonomamente una Nota dell'Organismo di Certificazione (NOC) e/o una Nota Informativa dello Schema (NIS) (vedi par. 5.6).

Elenco dello stato dei Rapporti di Osservazione

L'elenco dello stato dei Rapporti di Osservazione è mantenuto durante il processo di valutazione dall'LVS ed è analizzato nelle Riunioni di Controllo della Valutazione. Tale elenco è diviso in due sezioni: una per i ROA e una per i ROE. Ciò consente alle parti coinvolte nella valutazione di conoscere lo stato di tutti i Rapporti di Osservazione di un processo di valutazione, e cioè se il problema è ancora aperto o se è stato risolto con le azioni e le contromisure indicate nella Risposta al Rapporto di Osservazione.

All'interno dell'elenco, ciascun Rapporto di Osservazione è individuato univocamente da un numero di riferimento, che comprende un identificativo del processo di valutazione cui si riferisce e un numero seriale progressivo. Nel caso in cui in un ROA siano documentati più problemi collegati, ciascun problema dovrebbe essere numerato separatamente. Infine, dovrà essere indicata anche l'eventuale Risposta al ROA emessa dal Committente.

5.5 Rapporto di Attività (RA)

I risultati raggiunti durante le Attività di valutazione saranno contenuti in uno o più Rapporti di Attività (RA). In ogni caso tali Rapporti saranno compresi nell'RFV. Qualora i Valutatori ne ravvisino la necessità oppure su richiesta dell'OC, gli RA potranno essere inviati all'OC nel corso della valutazione. In relazione al contenuto degli RA l'OC decide sull'opportunità di trasmetterli al Committente.

Un RA fornisce all'OC e al Committente un resoconto dell'attività di valutazione. L'emissione degli RA dovrebbe essere concordata durante la fase di avvio del processo di valutazione (di norma nella Riunione di Avvio dei Lavori).

Per le valutazioni che non presentino particolare complessità comunque, gli RA saranno prodotti alla fine della valutazione.

Contenuti

Un RA fornisce un riassunto dei risultati della valutazione in termini di Attività di valutazione, così come riportate nei corrispondenti capitoli del PDV. Dovrà essere emesso un verdetto (*positivo, negativo, sospeso*) *per ciascuna unità di lavoro*.

Un'azione di valutazione conseguirà un verdetto positivo solo se tutte le relative singole unità di lavoro avranno ottenuto lo stesso verdetto. In modo analogo, un'attività di valutazione conseguirà un verdetto positivo solo se tutte le relative singole azioni avranno ottenuto lo stesso verdetto. Si osservi che un verdetto può risultare *sospeso* nel caso in cui, al momento dell'emissione dell'RA, il Valutatore non disponga degli elementi necessari per svolgere l'unità di lavoro.

Qualora nel corso della valutazione si verificasse la necessità di usare o sviluppare uno strumento non documentato nel PDV, questo deve essere descritto e motivato in un RA. Ad esempio, per uno strumento *software*, l'RA deve contenere:

1) il numero di versione del *software*;
2) l'ambiente in cui il *software* ha funzionato (ad esempio la piattaforma *hardware*, il sistema operativo, altri *software* dipendenti, l'insieme delle variabili ambientali);
3) la funzionalità dello strumento (ad esempio le opzioni di un menù);
4) il modo in cui lo strumento è stato applicato agli elementi della prova;
5) i dettagli di ogni prova in cui lo strumento è stato usato.

Analogamente, se nel PDV è stato pianificato di usare uno strumento, ma in seguito questo è risultato non appropriato, i motivi devono essere riportati in un RA.

Gli RA prodotti nel corso della valutazione saranno inseriti nell'RFV nella sezione che riassume i risultati della valutazione.

Le strutture di riferimento di un RA, differenziate in base alla metodologia di valutazione adottata (CEM/ITSEM), sono riportate in Appendice A.

5.6 Rapporti di Osservazione sullo Schema (ROS) e Note dell'OC (NIS, NOC, Note tecniche)

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 Informativa dello Schema (NIS). Questa verrà inviata all'LVS che ha prodotto il ROS; nei casi in cui il problema fosse di interesse generale, l'OC distribuirà la NIS a tutti gli LVS accreditati.

Una NIS può anche essere emessa autonomamente dall'OC. La NIS costituisce, infatti, uno strumento agile per interpretare ed integrare le pubblicazioni dello Schema

e/o dei criteri di valutazione in modo più immediato rispetto all'aggiornamento periodico delle Linee Guida prodotte dall'OC.

L'OC gestisce un elenco aggiornato delle NIS, che è distribuito a tutti gli LVS.

Le NIS saranno regolarmente revisionate e potranno essere incorporate nelle Linee Guida. Una volta che una NIS è stata incorporata nelle Linee Guida verrà eliminata dall'elenco.

Qualora lo ritenga necessario, l'OC può emettere autonomamente anche una Nota dell'Organismo di Certificazione (NOC), rivolta all'LVS e/o al Committente, su tutti gli aspetti inerenti una singola valutazione. Una NOC potrà essere emessa in qualsiasi fase della valutazione stessa e conterrà delle indicazioni dell'OC relativamente alle attività svolte nel corso di quella specifica valutazione, quali ad esempio l'adeguatezza della risposta ad un ROA, il corretto svolgimento di un'attività, la corretta interpretazione delle norme, ecc.

Si ricorda, inoltre, che l'OC può emettere autonomamente dei documenti interpretativi su particolari aspetti normativi, metodologici o applicativi. Tali documenti assumeranno la forma di Note Tecniche (NT) (cfr. LGP1, par. 5.4).

5.7 Rapporto delle Metodologie (RM)

Obiettivo

Un Rapporto delle Metodologie (RM) viene prodotto se nel corso della valutazione vengono impiegati metodi di valutazione e/o di sviluppo che presentano carattere innovativo.

Procedure di emissione

L'RM è inviato dall'LVS all'OC al termine di una valutazione; è compito dell'OC stabilirne l'eventuale diffusione agli altri LVS.

Contenuto

L'RM contiene un'introduzione che descrive l'ambito della valutazione effettuata al fine di definire il contesto in cui sono stati applicati i metodi di valutazione e di sviluppo oggetto del rapporto. Seguono due distinte sezioni che descrivono rispettivamente i metodi di valutazione e di sviluppo impiegati.

5.8 Metodi di valutazione

In questa sezione non sono descritte tutte le tecniche e/o gli strumenti utilizzati nel corso della valutazione, già riportati nell'RA, ma soltanto quelli che presentano un carattere innovativo per il processo di valutazione.

Tale carattere innovativo può riguardare, ad esempio:

- un criterio di valutazione ITSEC/CC;

- un riferimento a una norma dello Schema;
- un riferimento al manuale ITSEM/CEM;
- una fase del PDV.

Questo capitolo precisa:

- le caratteristiche dei metodi utilizzati;
- le condizioni di utilizzo;
- i loro vantaggi e svantaggi.

5.9 Metodi di sviluppo

Questo capitolo può essere presente soltanto in caso di valutazioni concomitanti. Se presente, contiene i commenti dei Valutatori su metodi, tecniche e strumenti utilizzati per lo sviluppo dell'ODV che presentano un carattere innovativo per il processo di valutazione.

5.8 Riunioni di Controllo della Valutazione

Obiettivo

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).

Le Riunioni di Controllo della Valutazione possono essere convocate dall'OC o dall'LVS. Nelle valutazioni più estese può essere utile programmare nel PDV Riunioni di Controllo della Valutazione, ad esempio per la verifica dello stato di avanzamento della valutazione.

Nel seguito sono presentate delle indicazioni di massima che dovrebbero essere considerate nello svolgimento di eventuali Riunioni di Controllo della Valutazione.

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.

Sono usualmente assegnati i seguenti ruoli:

- Presidente: un rappresentante dell'OC;
- Segretario: un rappresentante dell'LVS.

L'ordine del giorno è a discrezione della parte che ha convocato la riunione (cioè l'LVS o l'OC) e verrà approvato all'inizio della riunione. L'LVS è responsabile per la stesura e la distribuzione del verbale.

Pianificazione temporale

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

5.9 Riepilogo della fase di conduzione

Elementi di ingresso

Gli elementi di ingresso a questa fase sono:

1) un TDS o un PP;
2) un PDV;
3) i materiali per la valutazione.

Elementi di uscita

Gli elementi di uscita da questa fase possono comprendere:

1) Rapporti di Osservazione;
2) uno o più RA;
3) eventuali ROS e NIS;
4) eventuale RM;
5) verbali delle Riunioni di Avvio dei Lavori e delle Riunioni di Controllo della Valutazione.

6 Conclusione

Nella fase di conclusione l'LVS produce il Rapporto Finale di Valutazione (RFV). In questo rapporto vengono riportati i verdetti e le considerazioni svolte dai Valutatori. Nel seguito viene dettagliata la struttura tipica di un RFV.

6.1 Rapporto Finale di Valutazione (RFV)

Obiettivo

L'obiettivo del Rapporto Finale di Valutazione è riassumere i risultati della valutazione. L'RFV sarà usato dall'OC come elemento d'ingresso per la produzione del Rapporto di Certificazione.

Contenuti

Questo paragrafo fornisce un'indicazione sulla struttura tipica e sui contenuti minimi di un RFV per la valutazione di un ODV o di un PP; comunque, i Valutatori possono aggiungere voci o variare la struttura a seconda della necessità, concordando le variazioni con l'OC. L'indice di un RFV è riassunto in Tabella 1.

RAPPORTO FINALE DI VALUTAZIONE (RFV)
Capitolo 1 – Introduzione Capitolo 2 – Sommario Capitolo 3 – Descrizione dell'ODV Capitolo 4 – Caratteristiche di Sicurezza dell'ODV o del PP Capitolo 5 – Valutazione Capitolo 6 – Riassunto dei Risultati della Valutazione Capitolo 7 – Guida per la Ri-valutazione Capitolo 8 – Conclusioni e Raccomandazioni Allegato A – Elenco dei Materiali per la Valutazione Allegato B – Elenco degli Acronimi/Glossario dei termini Allegato C – Configurazione valutata Allegato D – Elenco dei Rapporti di Osservazione

Tabella 1 – Contenuto di un Rapporto Finale di Valutazione (RFV)

Capitolo 1 – Introduzione

Presenta sinteticamente la valutazione e riporta l'indice della struttura dell'RFV.

Capitolo 2 – Sommario

Fornisce le informazioni di base sui risultati della valutazione, a beneficio dell'OC (il nome dell'LVS e del Committente, una breve descrizione dell'ODV o del PP e delle sue caratteristiche di sicurezza, un riassunto delle principali conclusioni della valutazione).

In questa sezione devono essere indicati:

- lo Schema di valutazione, i criteri e le metodologie adottate;
- un identificativo dell'RFV (nome, data e numero di versione);
- un identificativo dell'ODV o del PP;
- il/i PP con cui viene eventualmente dichiarata conformità (mancante nel caso di valutazione di un PP);
- l'identità del Committente;
- l'identità dell'LVS;
- l'identità del Fornitore.

Capitolo 3 – Descrizione dell'ODV

Questa sezione è presente solo se l'RFV è relativo alla valutazione di un ODV. Deve essere riportata una descrizione ad alto livello dell'ODV (la sua architettura e le componenti hardware, software e firmware).

Capitolo 4 – Caratteristiche di Sicurezza dell'ODV o del PP

Questo capitolo può fare riferimento al TDS o al PP o riportare per esteso la descrizione delle caratteristiche di sicurezza dell'ODV o PP.

Capitolo 5 – Valutazione

Descrive le procedure di valutazione adottate, con riferimento al PDV, motivandone gli eventuali scostamenti. In particolare, il Valutatore deve riportare:

- i metodi, le tecniche, gli strumenti e gli standard di valutazione utilizzati;
- eventuali vincoli sulla valutazione e sulle ipotesi fatte durante la valutazione che possono avere impatto sul risultato della valutazione stessa;
- l'identificativo dell'RFV.

Capitolo 6 – Riassunto dei Risultati della Valutazione

Fornisce un riassunto dei risultati della valutazione in termini di Attività di valutazione, così come riportate nei corrispondenti capitoli del PDV. Per ciascuna di queste attività deve essere riportato un verdetto, corredato di una motivazione, che deve:

- avvalorare il verdetto finale sulla base dei criteri di valutazione adottati e della documentazione utilizzata;
- mostrare se i risultati della valutazione soddisfano o meno ogni aspetto dei criteri.

Questo capitolo contiene gli RA prodotti nel corso della valutazione.

Capitolo 7 – Guida per la Ri-valutazione

In questo capitolo vengono fornite indicazioni su eventuali future rivalutazioni dell'ODV o del PP o sull'eventuale adesione allo Schema di Gestione dei Certificati. Questo capitolo può essere omesso se il Committente non ha espresso queste esigenze.

Capitolo 8 – Conclusioni e Raccomandazioni

Devono essere riportate le conclusioni del Valutatore sulla valutazione, che indicheranno in particolare se l'ODV ha soddisfatto il suo TDS ed è esente da vulnerabilità sfruttabili. Sarà indicato il verdetto complessivo, derivato dall'analisi dei verdetti sulle varie attività. Può inoltre essere riportato qualunque commento/raccomandazione/suggerimento del Valutatore che possa essere di utilità per l'OC.

Allegato A – Elenco dei Materiali per la Valutazione

Viene riportato l'elenco completo ed aggiornato dei materiali per la valutazione; per ogni elemento dell'elenco devono essere indicati almeno: l'entità che lo ha emesso, il titolo ed un riferimento univoco.

Allegato B – Elenco degli Acronimi/Glossario dei termini

Devono essere riportati gli acronimi e le abbreviazioni utilizzati nell'RFV, soprattutto quelli non definiti nello Schema.

Allegato C – Configurazione Valutata

Va indicata chiaramente la specifica configurazione dell'ODV valutata (versione, modalità di funzionamento, ambiente operativo, ecc.)

Allegato D – Elenco dei Rapporti di Osservazione

Deve essere riportata una lista che identifichi univocamente i ROA e i ROE emessi nel corso della valutazione. Per ogni rapporto devono essere indicati: l'identificativo, il titolo, un eventuale breve riassunto del contenuto e le contromisure adottate per la soluzione del problema.

Procedure di emissione

L'RFV viene emesso dall'LVS al termine della valutazione e deve essere scritto in modo tale da proteggere eventuali informazioni riservate. A tale proposito valgono le stesse considerazioni svolte per gli RA nel par. 5.5.

La versione integrale dell'RFV viene inviata dall'LVS all'OC, che la revisiona per accertare che fornisca un adeguato riassunto dei risultati della valutazione.

Al Committente verrà invece consegnata dall'LVS la versione divulgabile.

6.2 Riepilogo della fase di conclusione

Elementi di ingresso

Gli elementi di ingresso a questa fase possono comprendere:

1) Rapporti di Osservazione;
2) uno o più RA;

3) eventuali ROS e NIS;
4) eventuale RM;
5) verbali delle Riunioni di Avvio dei Lavori e delle Riunioni di Controllo della Valutazione.

Elementi di uscita

L'elemento di uscita da questa fase è l'RFV.

7 Fase di 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 sessanta giorni dalla sua ricezione.

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

Decorso inutilmente il termine di sessanta giorni dalla sua ricezione, l'RFV si intende approvato.

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 e della volontà dello stesso di ottenere il rilascio del Rapporto di Certificazione e del relativo Certificato, nonché dell'assenza di elementi che contengano informazioni riservate. L'LVS e il Committente si pronunciano sulla richiesta entro i successivi cinque giorni.

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, può essere utilizzato esclusivamente dall'OC e dal Committente e 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 sfruttabili ed eventualmente raccomandare delle contromisure;
f) motivare l'eventuale emissione di verdetti in contrasto con quelli dell'LVS. In relazione alla valutazione di sistemi, i termini di cui sopra possono essere differiti, d'intesa con le parti, in ragione della complessità del sistema stesso. 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 (CC/ITSEC) 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

Quando l'LVS riceve il Rapporto di Certificazione, richiede formalmente all'OC la chiusura del processo di valutazione.

A tale proposito potrà tenersi una Riunione formale di Chiusura del Processo di valutazione. La necessità di tale riunione, convocata dall'OC di sua iniziativa o su richiesta dell'LVS o del Committente, dipenderà dalle circostanze della valutazione.

Una Riunione di Chiusura del Processo di valutazione sarà probabilmente convocata se sono stati riscontrati problemi significativi nella conduzione della valutazione, ad esempio nei casi in cui:

- un Committente contesta i risultati di una valutazione;
- sono stati riscontrati problemi relativi ai criteri di valutazione o allo Schema;
- è necessario accordarsi sull'assegnazione dei materiali del processo di valutazione.

8.1 Riunione di Chiusura della Valutazione

Obiettivo

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.

Normalmente, una Riunione di Chiusura della Valutazione dovrebbe essere convocata e organizzata dall'OC, che sarà anche responsabile della produzione e della distribuzione dell'ordine del giorno. Sarà responsabilità dell'LVS redigere il verbale.

Partecipanti

Si raccomanda che partecipino alla Riunione di Chiusura della Valutazione 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.

Sono normalmente assegnati i seguenti ruoli:

1) Presidente: un rappresentante dell'OC;
2) Segretario: un rappresentante dell'LVS.

Pianificazione temporale

Se è richiesta una Riunione di Chiusura della Valutazione, dovrebbe tenersi dopo che tutti i rapporti di valutazione richiesti ed il Rapporto di Certificazione siano stati emessi ed approvati.

8.2 Assegnazione dei materiali di un processo di valutazione

Generalità

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.

Archivio di base

Per la chiusura di un processo di valutazione, l'LVS deve produrre un archivio di base, che deve elencare tutti i materiali del processo di valutazione e dettagliare come i materiali stessi sono stati assegnati (cioè se sono stati archiviati, restituiti o distrutti).

L'archivio di base deve dare sufficienti dettagli per ciascun elemento (inclusi titolo, identificativo unico, data di emissione, numero della versione, assegnazione) per consentire che l'elemento stesso possa essere individuato in futuro, se necessario.

Una copia dell'archivio di base dovrebbe essere tenuta dall'LVS e una copia deve essere comunque inoltrata all'OC.

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:

- l'archivio di base;
- 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 archivierà l'RC e le proprie copie della documentazione del processo di valutazione in modo da soddisfare i propri specifici requisiti per l'archiviazione. Inoltre conserverà una copia dell'archivio di base del processo di valutazione, ricevuta dall'LVS.

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 ri-valutazione;
- fosse richiesta una ri-utilizzazione dei risultati della valutazione.

Materiali distrutti

In generale, i materiali 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 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 NIL, verbali di Riunioni di Controllo della Valutazione).

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

L'elenco dei prodotti, sistemi e PP certificati contiene dettagli di tutti i prodotti, sistemi e PP che sono stati certificati nello Schema.

L'OC, contestualmente all'emissione della certificazione, inserirà nell'elenco un'annotazione per quel prodotto, sistema o PP.

9 Appendice A - Contenuto di un Rapporto di Attività

Un Rapporto di Attività (RA) fornisce un riassunto dei risultati della valutazione in termini di Attività di valutazione, così come riportate nei corrispondenti capitoli del PDV. In questa appendice è indicata la struttura di riferimento di un RA, differenziata in base alla metodologia di valutazione adottata.

9.1 Rapporto di Attività: valutazione ITSEM

La struttura di riferimento di un RA quando venga applicata la metodologia descritta in [ITS2] è la seguente.

1) Introduzione
2) Elenco delle azioni svolte dai Valutatori
3) Osservazioni relative alle singole azioni
4) Verdetto sull'attività svolta
5) Conclusioni

Nel seguito è riportato l'elenco delle attività tipicamente previste per una valutazione secondo ITSEM, ognuna delle quali è normalmente oggetto di un RA.

1) Inizio del processo di valutazione
2) Verifica dei requisiti
3) Verifica del progetto architetturale
4) Verifica del progetto di dettaglio
5) Verifica dell'implementazione
6) Verifica dell'ambiente di sviluppo
7) Verifica della documentazione operativa
8) Verifica dell'ambiente operativo
9) Verifica dell'analisi dell'idoneità
10) Verifica dell'analisi di integrazione
11) Verifica dell'esame di robustezza dei meccanismi
12) Valutazione delle vulnerabilità nella costruzione
13) Valutazione delle vulnerabilità di esercizio
14) Valutazione della facilità d'uso
15) Prove di intrusione
16) Gestione del processo di valutazione
17) Fase di chiusura

9.2 Rapporto di Attività: valutazione CEM

La struttura di riferimento di un RA quando venga applicata la metodologia descritta in [CEM] è la seguente.

1) Introduzione

2) Elenco delle unità di lavoro svolte dai Valutatori
3) Osservazioni relative alle unità di lavoro
4) Verdetto sul risultato di valutazione ottenuto, espresso a partire dalle unità di lavoro arrivando fino all'attività complessiva
5) Conclusioni

Nel seguito è riportato l'elenco delle attività tipicamente previste per la valutazione di un ODV secondo CEM, ognuna delle quali è normalmente oggetto di un RA.

1) Inizio del processo di valutazione
2) Valutazione del Traguardo di Sicurezza
3) Valutazione della gestione della configurazione
4) Valutazione della consegna e della messa in opera dell'ODV
5) Valutazione del processo di sviluppo dell'ODV
6) Valutazione della documentazione dell'ODV
7) Valutazione delle misure di sicurezza connesse al ciclo di vita dell'ODV (dal livello EAL3 in poi)
8) Test funzionali sull'ODV
9) Stima di vulnerabilità (dal livello EAL2 in poi)
10) Fase di chiusura della valutazione

Si osservi che nel caso della valutazione di un PP è prevista un'unica attività denominata 'Valutazione del PP'.

10 Riferimenti bibliografici

[CC1] CCMB-2005-08-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, version 2.3, agosto 2005

[CC2] CCMB-2005-08-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, version 2.3, agosto 2005

[CC3] CCMB-2005-08-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, version 2.3, agosto 2005

[CEM] CCMB-2005-08-004, “Common Evaluation Methodology for Information Technology Security Evaluation – Evaluation Methodology”, version 2.3, agosto 2005

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

[ISO2] ISO/IEC TR 15446 “Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets”, dicembre 2003

[ITS1] Information Technology Security Evaluation Criteria, version 1.2, giugno 1991

[ITS2] Information Technology Security Evaluation Manual, version 1.0, settembre 1993

[SGC] OCSI, Procedure dello Schema di Gestione dei Certificati

[UNI1] UNI/CEI EN ISO/IEC 17025 Requisiti generali per la competenza dei laboratori di prova e di taratura, 2000.

11 Lista degli acronimi

EAL	=	(Evaluation Assurance Level) Livello di garanzia della valutazione
IT	=	Information Technology
LVS	=	Laboratorio di Valutazione della Sicurezza
NAV	=	Nota per Anomalia nella Valutazione
NEV	=	Nota per Errore nella Valutazione
NIL	=	Notifica di Inizio Lavori
NIS	=	Nota Informativa dello Schema
NOC	=	Nota dell'Organismo di Certificazione
NT	=	Nota Tecnica
OC	=	Organismo di Certificazione
ODV	=	Oggetto Della Valutazione (TOE - Target of Evaluation)
OSP	=	(Organisational Security Policy) Politica di Sicurezza di un'Organizzazione
PGC	=	Piano per la Gestione del Certificato
PDV	=	Piano Di Valutazione
PP	=	Profilo di Protezione
RA	=	Rapporto di Attività
RAL	=	Riunione di Avvio dei Lavori
RC	=	Rapporto di Certificazione
RCC	=	Rapporto di Classificazione delle Componenti dell'ODV
RFV	=	Rapporto Finale di Valutazione
RGC	=	Responsabile per la Gestione del Certificato
RM	=	Rapporto delle Metodologie
RO	=	Rapporto di Osservazione
ROA	=	Rapporto di Osservazione: Anomalia
ROE	=	Rapporto di Osservazione: Errore
ROS	=	Rapporto di Osservazione sullo Schema
SAR	=	(Security Assurance Requirement) Requisito di Garanzia
SGC	=	Schema di Gestione dei Certificati
SFP	=	(Security Function Policy) Politica della Funzione di Sicurezza
SFR	=	(Security Functional Requirement) Requisito Funzionale di Sicurezza
SOF	=	(Strength of Function) Robustezza di una Funzione di Sicurezza
TDS	=	Traguardo di Sicurezza (ST - Security Target)
TSF	=	(TOE Security Function) Funzione di Sicurezza dell'ODV
TSP	=	(TOE Security Policy) Politica di Sicurezza dell'ODV
UL	=	Unità di Lavoro