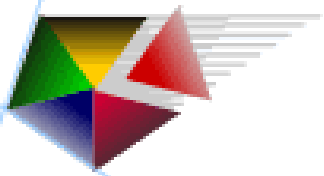
TECHNISBLU

LVS ACCREDITATO OCSI



LABORATORIO di VALUTAZIONE della SICUREZZA

Accreditato dal 13 marzo 2007

OCSI
(Organismo di Certificazione della Sicurezza Informatica)
Ministero dello Sviluppo Economico

TECHNIS BLU SRL
Sede Legale ed Operativa: Via Riccardo Gigante, 4 – 00143 Roma – Sede Operativa LVS : Viale Luigi Schiavonetti, 290/B 00173 Roma
Capitale Sociale € 400.000,00 i.v. REA 1217316 – P.IVA/Cod.Fisc. 10207141002
tel. +39 06 8928 5229 – fax +39 06 9294 1268
e-mail: lvs.technisblu@technisblu.it - www.technisblu.it

LVS (Laboratorio di Valutazione della Sicurezza) TECHNIS BLU

Presentazione del Laboratorio

Il Laboratorio è un soggetto indipendente e neutrale, organizzato come unità di business all'interno di Technis Blu s.r.l. e svolge attività di Valutazione di Prodotti e Sistemi Informatici secondo lo standard ISO 15408 (Common Criteria), in linea con quanto previsto dallo Schema Nazionale di Valutazione e Certificazione. Unitamente alle attività di Valutazione, il Laboratorio svolge attività di Formazione e Consulenza per lo studio, progettazione e diffusione nelle aziende/amministrazioni di efficaci soluzioni di Sicurezza organizzativa ed informatica.

Per le attività di Valutazione, indipendente e neutrale significa che il Laboratorio:

- ☑ *ha una propria struttura di governo indipendente costituita da apposito verbale del CDA Technis*
- ☑ *ha una sua struttura commerciale indipendente da quella Technis*
- ☑ *non impiega Valutatori che abbiano svolto attività di consulenza su ODV in valutazione*
- ☑ *non effettua Valutazioni per Committenti legati da eventuali rapporti di partnership (ad es. di proprietà/controllo, RTI/ATI, ecc.)*

Obiettivi del Laboratorio

La missione del Laboratorio è di condurre il business della consulenza, della ricerca e dell'addestramento nelle pratiche aziendali collegate alla Tecnologia della Sicurezza dell'Informazione, del disegno dei processi, delle operations e dell'organizzazione, quali ad esempio:

- ☑ *Scrittura di Protection profile e Security Target*
- ☑ *Valutazioni ai fini della certificazione OCSI*
- ☑ *Assessment e pianificazione della sicurezza organizzativa (ISO/IEC 27001)*
- ☑ *Analisi di vulnerabilità e penetration test su prodotti e sistemi*
- ☑ *Formazione specifica*

Struttura del laboratorio

Il LVS Technis Blu consta:

- di un responsabile del Laboratorio
- di 5 valutatori senior accreditati, di cui 2 "Documentali" e 3 "Operativi"
- di personale tecnico con specifiche competenze ICT
- di un'area riservata di seconda classe per la custodia in armadio blindato a norma del materiale del cliente soggetto a valutazione
- di apposita area dedicata per lo svolgimento delle prove di laboratorio

Competenze del laboratorio

Il Laboratorio ritiene che la sicurezza di prodotti e sistemi ICT non possa prescindere da aspetti di sicurezza legati alla organizzazione ed ai processi aziendali, e ritiene questi aspetti imprescindibili e sinergici.

Per questa ragione, le competenze raccolte nel laboratorio, oltre ai valutatori accreditati OCSI, comprendono due Lead Auditor ISO 27001, e consulenti esperti nelle analisi di vulnerabilità (Assessment e Penetration Test).

Altro aspetto rilevante è la competenza nella formazione, che viene erogata con corsi personalizzati sugli standard ISO/IEC 15408 e ISO/IEC 27001.

Referenze del Laboratorio

Il Laboratorio ha già acquisito notevoli esperienze nell'erogazione di servizi riguardanti i Criteri Comuni dello standard ISO/IEC 15408. In particolare si citano:

- ✓ *Approntamento Security Target per tutte le valutazioni sotto indicate*
- ✓ *Valutazioni per l'ottenimento dei relativi certificati* ***nell'ambito slot machine***
  - *Valutazione per Electro System S.p.a. del prodotto "Backoffice v.5.0" Incluso nella scheda di gioco ELSY JOE001 Black Killer" per l'ottenimento del relativo certificato.*
  - *Valutazione per Electro System S.p.a. del prodotto "Backoffice v.4.0" Incluso nella scheda di gioco ELSY JOH001 Isola del Tesoro" per l'ottenimento del relativo certificato.*
  - *Valutazione per Electro System S.p.a. del prodotto "Backoffice v.3.0" Incluso nella scheda di gioco ELSY JOD001 Vampire" per l'ottenimento del relativo certificato.*
  - *Valutazione per Electro System S.p.a. del prodotto "Backoffice v.2.0" Incluso nella scheda di gioco ELSY JOP001 Myan Temple" per l'ottenimento del relativo certificato.*
  - *Valutazione per Electro System S.p.a. del prodotto "Backoffice v.1.0" Incluso nella scheda di gioco ELSY JOA001 Diamond" per l'ottenimento del relativo certificato.*
- ✓ *Valutazioni per l'ottenimento dei relativi certificati relativi a* ***dispositivi di firma elettronica avanzata (FEA)***
  - *Valutazione per Euronovate SA del prodotto "E-Signature ENsoft v1.1".*
- ✓ *Valutazioni in corso per l'ottenimento dei relativi certificati* ***nell'ambito:***
  - *dei sistemi di videosorveglianza e lettura targhe*
  - *di piattaforme di comunicazione (LAN/WAN)*
  - *di sistemi bancari di Firma Elettronica Avanzata (FEA)*

Riconoscimento internazionale dei certificati

Lo standard dei Common Criteria, unitamente alla metodologia definita nel documento complementare Common Methodology for Information Technology Security Evaluation (CEM), costituisce il fondamento tecnico di un gruppo internazionale denominato CCRA (Common Criteria Recognition Arrangement), frutto di un accordo di mutuo riconoscimento sottoscritto nel 2000 da dodici Paesi, tra cui l'Italia, che si occupa per l'appunto dell'applicazione, dell'armonizzazione e dell'evoluzione dello standard Common Criteria. Negli anni seguenti, altri Paesi hanno aderito all'accordo, che attualmente comprende 26 partecipanti e 57 LVS.

All'interno di questo contesto i certificati emessi dall'OCSI, tramite le attività di valutazione svolte dai suoi quattro LVS, vengono riconosciuti da tutti i paesi aderenti fino al livello EAL4.

I processi di certificazione sui CC sono supportati da direttive legislative in vigore, emesse dalla Unione Europea e dalla Repubblica Italiana.

Il valore di una certificazione Common Criteria (ISO/IEC 15408)

I Common Criteria consentono di determinare il livello di garanzia a cui si vuole che un prodotto/sistema risponda, in base alle sue esigenze specifiche di applicazione. Questa determinazione avviene mediante la scelta del livello di garanzia. Come abbiamo visto il mutuo riconoscimento è fino al livello EAL4. Direttamente a stralcio della "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components - Version 3.1 Revision 2", vengono nel seguito riportate le caratteristiche di garanzia sempre crescenti derivanti dai primi quattro livelli, caratteristiche di garanzia che esprimono il valore della relativa certificazione.

EAL1 - functionally tested

provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour. The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF. EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents. This EAL provides a meaningful increase in assurance over unevaluated IT.

EAL2 - structurally tested

provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour. This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

EAL3 - methodically tested and checked

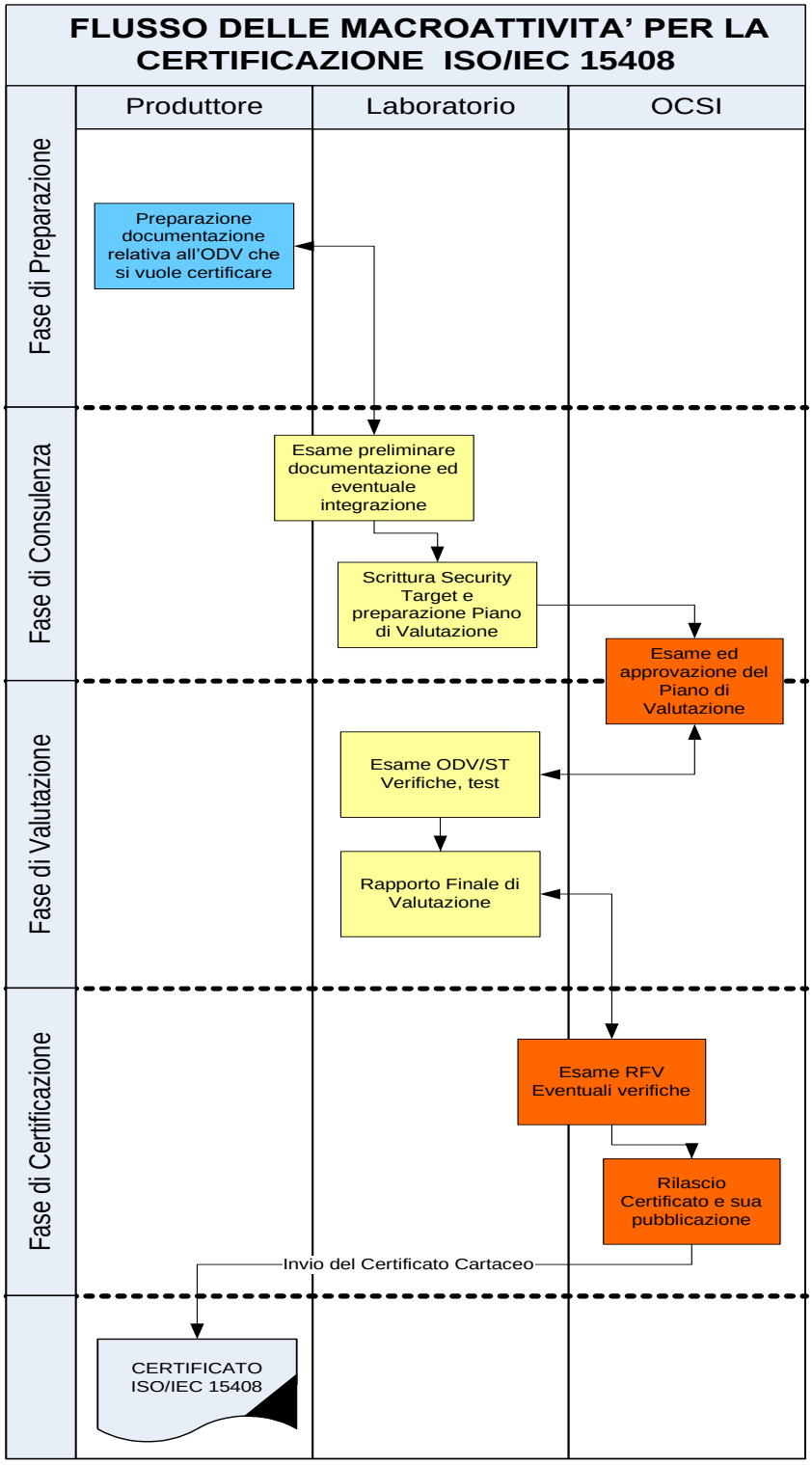
provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behaviour. This EAL represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functionality and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.

EAL4 - methodically designed, tested, and reviewed

provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour. This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

Flusso standard di una certificazione (fasi, ruoli e macroattività)

Si ritiene utile riepilogare nello schema seguente il processo che porta alla certificazione di un prodotto/sistema, così da consentire una più immediata comprensione della sequenza delle fasi, dei ruoli che i tre attori del processo rivestono e delle macroattività previste. Lo schema per esigenze di semplicità esplicativa non riporta il dettaglio delle attività, che la norma condiziona in base al livello di assicurazione richiesto (EAL1-EAL7), così come il dettaglio delle interazioni che sono semplicemente rappresentate dalle frecce.



Come si può vedere nel complesso il processo può essere semplificato in 4 fasi:

- la prima "Preparazione" che può essere svolta anche in autonomia da parte del produttore (con l'eventuale ausilio del LVS),
- la seconda "Consulenza" dove è necessario avere delle competenze specifiche sui Common Criteria (CC),
- la terza "Valutazione" che è quella istituzionale svolta dal LVS,
- la quarta "Certificazione" che è quella istituzionale dell'OCSI al termine del processo per il rilascio della certificazione.