

IMQ per le aziende con esigenze di valutazione/certificazione formale delle caratteristiche di sicurezza dei propri sistemi o prodotti IT

I criteri di valutazione ITSEC/Common Criteria

Fu alla fine degli anni ottanta che in Europa si cominciò a sentire l'esigenza di sviluppare criteri di valutazione della sicurezza che, partendo dai vecchi criteri nazionali esistenti, mirassero alla loro armonizzazione. Il risultato di questa iniziativa fu la nascita dei Criteri ITSEC, pubblicati per la prima volta nel maggio del 1990, a cui fece seguito nel 1999 la pubblicazione dei Common Criteria (ISO/IEC 15408).

I criteri ITSEC/Common Criteria trattano il tema della sicurezza, per sistemi e prodotti informatici, nelle loro tre componenti fondamentali:

- **Funzionalità** (ciò che il sistema deve fare per la sicurezza)
- **Efficacia** (in che misura le contromisure contrastano le minacce)
- **Correttezza** (come le contromisure sono state implementate)

Ogni valutazione offre così la garanzia che le funzioni di sicurezza dell'oggetto valutato sono progettate ed implementate correttamente ed efficacemente, in modo tale da soddisfare gli obiettivi di sicurezza e non presentare vulnerabilità sfruttabili.

Tale garanzia è definita su diversi livelli che rappresentano una fiducia crescente nelle capacità del sistema o del prodotto di soddisfare i suoi obiettivi di sicurezza. La funzionalità suddetta è definita, da chi richiede la valutazione, in un documento formale definito "Target di Sicurezza", che nel caso di valutazioni secondo i Common Criteria può essere derivato da un Profilo di Protezione di riferimento. Tale documento fornisce il legame tra

tutti gli aspetti di sicurezza (organizzativi, fisici, tecnico-informatici, procedurali, etc.), comprendendo l'esplicitazione non ambigua degli obiettivi da raggiungere, delle minacce, della politica di sicurezza, delle funzioni che implementano la sicurezza e del livello di garanzia richiesto.

Sulla base del Target di Sicurezza e della documentazione di progetto necessaria (che dipende dal livello di garanzia richiesto), l'attività di valutazione comprende analisi di correttezza e di efficacia che considerano aspetti relativi allo sviluppo e all'esercizio dell'ODV.

La valutazione dell'efficacia è completata con prove di intrusione volte a dimostrare la non sfruttabilità delle vulnerabilità residue del sistema/prodotto.

I vantaggi di una valutazione/certificazione formale di sicurezza

L'uso di criteri ben definiti ed internazionalmente riconosciuti fornisce un'unità di misura per la sicurezza informatica presentando una serie di vantaggi, tra i quali:

- assicurare un significato noto e non ambiguo al risultato della valutazione stessa;
- aiutare nella scelta di prodotti e sistemi evidenziandone le loro caratteristiche di sicurezza;
- agevolare il confronto sulla sicurezza tra sistemi e prodotti diversi;
- facilitare la valutazione di sistemi realizzati integrando altri sistemi o prodotti già valutati e certificati riutilizzandone il certificato;
- salvaguardare l'investimento sostenuto con la valutazione, in caso di

rivalutazioni successive o in caso di emanazione di nuovi criteri armonizzati;

- favorire il riconoscimento del risultato della valutazione/certificazione tra i diversi Paesi che hanno sottoscritto l'accordo di mutuo riconoscimento dei certificati;
- utilizzare i risultati della valutazione in contesti contrattuali o legislativi.

I servizi offerti

Valutazioni Formali di sicurezza secondo ITSEC e Common Criteria (ISO/IEC 15408) in ambito commerciale

Servizio dedicato alle organizzazioni che forniscono prodotti e sistemi destinati al settore commerciale.

Gli scopi di una valutazione di un prodotto/sistema sono molteplici. Per l'utenza finale, la valutazione consente di avere una base per confrontare le prestazioni, in materia di sicurezza, dei vari prodotti IT. Per il fornitore/sviluppatore, la valutazione stabilisce la volontà di dimostrare che le prestazioni di sicurezza dichiarate sono effettive, in quanto verificate in modo obiettivo e riproducibile, da una terza parte.

Per le organizzazioni che non fossero in grado autonomamente di sintetizzare i requisiti di sicurezza di un proprio sistema/prodotto da sottoporre a valutazione

formale è inoltre disponibile un servizio di assistenza iniziale (in fase di preparazione della valutazione) per la stesura e la verifica indipendente della congruenza (copertura e consistenza) formale e sostanziale dei requisiti di sicurezza e per la stima della "valutabilità di un sistema o prodotto oggetto di valutazione".

Programma di assistenza alle valutazioni secondo ITSEC e Common Criteria

La parte operativa della valutazione/certificazione comprende la produzione, da parte del Fornitore, di documenti di correttezza (come il sistema è stato implementato) e di efficacia (in che misura le contromisure contrastano le minacce).

IMQ/LPS fornisce un servizio di supporto alle organizzazioni per la redazione della documentazione necessaria alla valutazione e può fornire assistenza nella specifica dei requisiti di sicurezza inseriti in un Protection Profile (Profilo di Protezione).

Un Profilo di Protezione è un documento che descrive in modo indipendente dalla tecnologia (technology neutral) i requisiti di sicurezza di una categoria di prodotti informatici che soddisfano particolari esigenze dei potenziali consumatori (ad esempio: firewall, database, dispositivi sicuri per la firma digitale ai sensi della direttiva europea...).

Qualsiasi associazione di utilizzatori o di sviluppatori di prodotti informatici, ente di standardizzazione o governativo può

redigere un Profilo di Protezione per una tipologia di prodotti di loro interesse e ottenerne la certificazione in accordo ai Common Criteria. I Protection Profile certificati, inseriti in cataloghi pubblici, possono essere usati dai fornitori/sviluppatori come riferimenti per decidere di quali funzionalità di sicurezza dotare i loro prodotti, dagli Enti di normazione come mezzo per formulare standard di sicurezza di riferimento, dagli utilizzatori di prodotti informatici come base per la stesura di capitolati.

Conduzione di Risk Assessment

Servizio dedicato alle Aziende che vogliono fare valutare e certificare le caratteristiche di sicurezza del proprio sistema IT e necessitano di assistenza nella definizione dei confini dell'oggetto di valutazione (ODV), ovvero della definizione di obiettivi, requisiti e funzioni di sicurezza preposte a contrastare le minacce che possono compromettere la sicurezza dell'ODV nel suo ambiente di esercizio, eventualmente sfruttando vulnerabilità note di progettazione o in esercizio.

L'attività, in genere condotta con metodologia CRAMM o metodologia sviluppata ad hoc per il cliente, è finalizzata ad identificare l'oggetto di valutazione e a consolidare il suo Target di Sicurezza (o Traguuardo di sicurezza), documento capostipite di una valutazione formale di sicurezza.

IMQ per le aziende con esigenze di certificazione secondo la ISO/IEC 27001 del proprio sistema di gestione della sicurezza delle informazioni

La norma ISO/IEC 27001

La sicurezza delle informazioni è un concetto che supera il puro fatto tecnologico, la sicurezza è un processo che si rivolge alle persone componenti l'organizzazione ed alle modalità in cui le persone utilizzano la tecnologia a loro disposizione.

La norma ISO/IEC 27001, derivata dalla BS7799 del BSI (British Standard Institution) è uno standard di gestione della sicurezza delle informazioni che mira a preservare l'informazione, in qualsiasi forma essa sia presente nell'organizzazione, in termini di **confidenzialità, integrità e disponibilità**.

Queste, che sono le tre componenti fondamentali della sicurezza dell'informazione, sono anche le componenti fondamentali da cui dipendono la competitività dell'azienda, i suoi profitti, il suo rispetto di obblighi legislativi e in definitiva la sua immagine commerciale.

Allo standard ISO/IEC 27001 è associata la "linea guida" ISO/IEC 27002 (precedentemente denominata 17799) che individua un insieme di punti d'intervento e le relative possibili misure organizzati in 11 aree distinte: **Politiche di sicurezza, Organizzazione della sicurezza, Gestione dei beni, Sicurezza delle risorse umane, Sicurezza fisica ed ambientale, Gestione delle comunicazioni e delle attività, Controllo degli accessi, Acquisizione di sistemi informatici, sviluppo e manutenzione, Gestione degli incidenti della sicurezza delle informazioni, gestione della continuità dei processi aziendali, Conformità**.

Per ciascuna delle aree precedentemente identificate sono individuati uno o più obiettivi di sicurezza e, per ognuno di questi obiettivi, si individuano i punti d'intervento e le misure che dovrebbero essere utilizzate per perseguirli.

Lo standard ISO/IEC 27002 si propone di fatto come un catalogo organizzato di buone pratiche di sicurezza che potrebbero essere utilizzate per raggiungere gli obiettivi di sicurezza individuati, ma che non è obbligatorio applicare e che potrebbero essere sostituiti da nuove contromisure, più adeguate, scelte dall'azienda.

La norma ISO/IEC 27001, invece, è nata come base per eseguire le verifiche di conformità del Sistema di Gestione della Sicurezza dell' Informazione (SGSI o ISMS, come indicato nella norma, acronimo dell'inglese Information Security Management System).

E' quindi importante sottolineare che la certificazione di conformità del sistema di gestione della sicurezza delle informazioni di un'azienda è quindi emessa nel rispetto della ISO/IEC 27001 e non della ISO/IEC 27002. E' infatti nella ISO/IEC 27001 che, rispetto alla ISO/IEC 27002, la terminologia cambia da 'should' (dovrebbe) a 'shall' (deve) assumendo così il rigore del documento normativo. La creazione e manutenzione di un ISMS prevede l'esecuzione di diversi passi: **Impostazione della struttura di gestione dell'ISMS (Management Framework), Realizzazione delle misure, Realizzazione della Documentazione, Monitoraggio e revisione dell'ISMS, Mantenimento e miglioramento dell'ISMS, Gestione**



controllata della documentazione e **Raccolta delle RegISTRAZIONI.**

È previsto che l'organizzazione definisca la politica di sicurezza, l'ambito (i confini) del sistema informativo, esegua l'attività di valutazione del rischio e rediga la dichiarazione di applicabilità (**statement of applicability**), documento in cui sono giustificate le scelte fatte.

Due i fatti da sottolineare: la ISO/IEC 27001 permette non solo la certificazione dell'intera organizzazione, come verrebbe spontaneo pensare, ma anche la selezione di un ben determinato 'dominio' interno all'azienda; in secondo luogo la norma non richiede necessariamente che tutti i punti d'intervento in elenco siano soddisfatti, ma permette che l'azienda scelga, dando dei razionali a giustificazione di eventuali omissioni sulla base dei risultati di un'analisi di rischio, solo alcuni tra tali punti o misure o ancora che ne inserisca altre non descritte nella ISO/IEC 27002. La ISO/IEC 27001 è una norma flessibile, che permette di ottenere diversi vantaggi tra i quali la facilitazione del rispetto dei requisiti contrattuali e legislativi, il rafforzamento della credibilità aziendale ed una razionalizzazione degli investimenti impiegati per la sicurezza.

I servizi offerti

Supporto alla certificazione CSQ-Data

Il personale dell'Area Security ICT collabora con i team di valutazione per lo Schema CSQ-Data (Sistema di Gestione della Sicurezza delle Informazioni) per la verifica di conformità in accordo alla ISO/IEC 27001.

Gap analysis

Servizio dedicato alle organizzazioni sensibili al tema della sicurezza e che vogliono confrontare i loro standard interni all'unico standard di riferimento per un sistema di gestione per la sicurezza delle informazioni.

Tale servizio è mirato alla produzione di un report che identifichi in modo sintetico e mirato quanto i processi aziendali, afferenti la sicurezza dell'informazione, sono distanti da quanto previsto dalla Norma.

Audit di sicurezza

Servizio dedicato alle organizzazioni che vogliono focalizzare l'attenzione sulla sicurezza delle informazioni legate ad un aspetto preciso della propria realtà andando, ad esempio, a selezionare dai 'controls' della ISO/IEC 27002 un subset

degli stessi e verificarne l'applicazione nella propria realtà. Siamo in grado di mettere al vostro servizio le nostre competenze acquisite nella conduzione delle valutazioni formali di sicurezza per consentirvi una valutazione dell'efficacia delle contromisure (o 'controls') selezionati per soddisfare i requisiti dei vostri Sistemi di Gestione della Sicurezza delle Informazioni (SGSI).

Assistenza tecnico normativa

Laddove esistano dubbi sull'applicazione delle normative e sui criteri sopra citati, è disponibile un servizio di assistenza tecnico normativa condotto da auditor ISO/IEC 27001.

Tale servizio, di durata variabile in funzione delle esigenze del Cliente, consiste in meeting allargati e/o incontri specifici con personale dell'azienda, durante i quali saranno affrontati i temi salienti della Norma in modo da avere una visione chiara delle diverse implicazioni dell'applicazione della stessa nella propria organizzazione.

IMQ per le aziende del settore "Finance"

Assessment dei sistemi di Business Continuity/Disaster Recovery

Dal 2004 la Banca d'Italia sta svolgendo attività di sensibilizzazione degli operatori del settore finance sui temi della sicurezza ICT, con particolare riguardo al tema della **Business Continuity e Disaster Recovery**.

Il provvedimento del Governatore della Banca d'Italia del 24/02/2004 e le successive Linee Guida del 24/11/2004, pur riguardando tutti i soggetti coinvolti nella emissione e/o gestione di strumenti di pagamento, hanno concentrato il focus sui gestori delle cosiddette "infrastrutture qualificate", ovvero giudicate rilevanti per numerosità e caratteristiche delle informazioni trattate, richiedendo l'attuazione di "Piani di Continuità (o Business Continuity Plan)" che permettano di far fronte ai vari scenari di disastro ipotizzati.

Le Linee Guida sopra citate pongono l'accento sull'importanza di verifiche dell'affidabilità del piano di continuità effettuate da terze parti indipendenti, eventualmente orientate al conseguimento di certificazioni di sicurezza sulla base di standard nazionali e/o internazionali da parte di laboratori accreditati dagli enti preposti.

IMQ può rispondere a tali esigenze supportando le aziende clienti nei processi di:

- **Valutazione formale della sicurezza dei sistemi IT** coinvolti nel piano di Business Continuity secondo i criteri internazionali ITSEC e Common Criteria (ISO/IEC 15408) all'interno dello Schema Nazionale gestito dall'OCSI/ISCOM (www.ocsi.gov.it) in cui IMQ è accreditato ad operare come Laboratorio di Valutazione della sicurezza (LVS);
- **Certificazione ISO/IEC 27001** del Sistema di Gestione della Sicurezza delle Informazioni dell'azienda, comprendente al suo interno anche la gestione del Piano di Continuità Operativa (Business Continuity e Disaster Recovery). In questo contesto IMQ opera come organismo di certificazione accreditato dal SINCERT;
- **Audit di Sicurezza** volto ad attestare che l'implementazione del piano di Business Continuity e Disaster Recovery è conforme ai requisiti che l'azienda si propone di soddisfare, derivati da una Business Impact Analysis. Le verifiche riguardano sia gli aspetti organizzativi/procedurali che quelli tecnici attraverso un insieme di test, specificati con il supporto di IMQ ed eseguiti in presenza di auditor di IMQ.

Attraverso le certificazioni o le attestazioni rilasciate da IMQ l'azienda ottiene, oltre al riconoscimento ufficiale che una terza parte esterna ha valutato positivamente il suo piano di Business Continuity e Disaster Recovery, anche



dei benefici derivanti dalla riduzione dei cosiddetti "costi della non sicurezza" dovuti a:

- danni economici diretti derivanti dalla indisponibilità dei servizi ICT;
- danni economici indiretti a causa della perdita di immagine verso i propri clienti;
- danni economici indiretti a seguito di eventuali problemi legali/contrattuali legati a particolari servizi forniti (SLA stringenti, D.Lgs. 196/2003, ...).

Valutazione della conformità alle norme CEI 79-5 e 79-6 dei protocolli di comunicazione per il trasferimento di informazioni di sicurezza (allarmi) tra una Centrale d'Allarme (CA) e un Centro di Supervisione e Controllo (CSC)

Le norme CEI 79-5 e 79-6 definiscono, rispettivamente, il livello di trasporto e il livello applicativo del protocollo di comunicazione per il trasferimento di informazioni di sicurezza (allarmi) implementato dagli elementi (CA e CSC) di un sistema di

centralizzazione degli allarmi.

Il personale dell'Area Security ICT ha maturato una significativa esperienza nella verifica della conformità dei due suddetti livelli di protocollo alle norme CEI 79-5 e 79-6 basandosi sull'applicazione di una metodologia proprietaria finalizzata al rilascio di una **attestazione di conformità** alle norme sopra citate.

Metodologia utilizzata da IMQ per la verifica di conformità alle norme CEI 79-5 e 79-6

L'attività di valutazione della conformità di un protocollo di trasmissione di segnalazioni di sicurezza è tipicamente strutturata in tre fasi:

Fase 1:

Valutazione della documentazione inerente l'ambiente di test del sistema integrato di sicurezza o del CSC o della CA sottoposta a verifica di conformità

Si tratta della prima attività da effettuare, in quanto presupposto per instaurare un dialogo tra il personale IMQ/LPS ed il personale che sarà coinvolto nelle fasi successive dell'attività. L'attività prevede l'esame approfondito della documentazione consegnata, compresa la documentazione di test, e la redazione di un Rapporto che riassume i commenti e le osservazioni ine-

renti ad eventuali lacune, inconsistenze interne ai documenti consegnati, esplicitando i chiarimenti o le integrazioni necessarie per poter condurre le successive fasi di attività. In questa fase è previsto in genere un sopralluogo sull'ambiente che sarà utilizzato in fase di test.

Fase 2:

Valutazione della conformità alle norme CEI 79-5 e 79-6

Questa fase consiste nella definizione ed esecuzione da parte del personale di IMQ/LPS dei test che saranno condotti nell'ambiente messo a disposizione dal cliente e con il supporto di personale tecnico del cliente. Al termine di ogni sessione di test è previsto il rilascio di un rapporto di attività che sintetizzi i principali risultati emersi nel corso delle prove.

Fase 3:

Chiusura della Valutazione

Tale attività consiste nella redazione ed emissione del Rapporto Finale di Valutazione che attesti il grado di rispondenza dei protocolli implementati, a valle dell'analisi puntuale dei tracciati raccolti nella fase precedente, e che documenti nel dettaglio le Estensioni Proprietarie Transitorie (EPT) definite.

IMQ per le aziende con particolari esigenze di disponibilità dei servizi ICT offerti

IMQ è l'unico Ente italiano ad essere accreditato:

- dall'ANS e dall'OCSI/SCOM per poter effettuare, negli schemi nazionali, valutazioni formali della sicurezza di sistemi IT secondo i criteri ITSEC e ISO/IEC 15408;
- dal SINCERT per certificare i Sistemi di Gestione della Sicurezza delle Informazioni delle aziende in base alla ISO/IEC 27001;

IMQ può quindi aiutare le aziende interessate ad avere una ragionevole fiducia che i propri Servizi ICT siano disponibili quando necessario attraverso verifiche puntuali delle misure messe in atto sia dal punto di vista organizzativo/gestionale, sia dal punto di vista tecnico (come ridondanza dei server, delle linee di comunicazione, dei sistemi di storage, etc.).

Metodologia utilizzata da IMQ per la conduzione di audit dei sistemi di Business Continuity/Disaster Recovery

Per quanto riguarda le attività di verifica degli aspetti gestionali/organizzativi, l'approccio di IMQ si basa sull'analisi e la verifica dell'applicazione di un insieme di "con-

trols" selezionati dallo standard ISO/IEC 27002 e che risultino applicabili al servizio che si intende verificare.

La verifica degli aspetti più tecnici invece è effettuata attraverso il supporto alla definizione di un piano di test tecnici, che copra gli aspetti più critici dei servizi erogati, e la supervisione della conduzione di tali test finalizzata all'attestazione della loro positiva esecuzione.

Benefici ottenibili da un audit di sicurezza di un sistema ICT con elevate esigenze di disponibilità dei dati/servizi offerti

Il primo ritorno per un'organizzazione che si affida ad un Ente terzo, quale IMQ, per la conduzione di un audit di sicurezza sul proprio sistema di Business Continuity / Disaster Recovery è quello di ridurre i cosiddetti "costi della non sicurezza" dovuti a:

- danni economici diretti derivanti dalla indisponibilità dei servizi ICT;
- danni economici indiretti a causa della perdita di immagine verso i propri clienti;



IMQ PER LE AZIENDE CON PARTICOLARI ESIGENZE DI DISPONIBILITÀ DEI SERVIZI ICT OFFERTI

- danni economici indiretti a seguito di eventuali problemi legali/contrattuali legati a particolari servizi forniti (SLA stringenti, D.Lgs 196/2003, ...).

L'organizzazione richiedente l'audit può inoltre ottenere un'attestazione di conformità del sistema IT verificato (o di un suo sottosistema, come ad esempio quello preposto al Disaster Recovery) ad un documento che specifichi i requisiti che esso si propone di soddisfare, in base alla documentazione dei test effettuati in presenza degli auditor IMQ. Tale attestazione può essere utilizzata da un'organizzazione come strumento per dare evidenza, pubblicizzare e documentare alla propria clientela che una parte esterna ed indipendente all'organizzazione ha verificato il soddisfacimento dei requisiti di sicurezza del sistema IT considerato.