

La certificazione della sicurezza di sistemi e prodotti ICT

Franco Guida

Fondazione Ugo Bordonì

INFOSECURITY Roma 2006: *«I servizi di supporto alla security governance»*

Roma, 21 giugno 2006

La sicurezza ICT in un'Organizzazione

Processo di gestione della sicurezza ICT (ISMS)

Certificabile ISO/IEC 27001

Informazioni/beni da proteggere

Analisi e gestione dei rischi

Contromisure fisiche

Politiche di sicurezza

(modello organizzativo, definizione requisiti per le contromisure tecniche e non tecniche, ecc.)

Pluralità di soggetti con diversi compiti e responsabilità

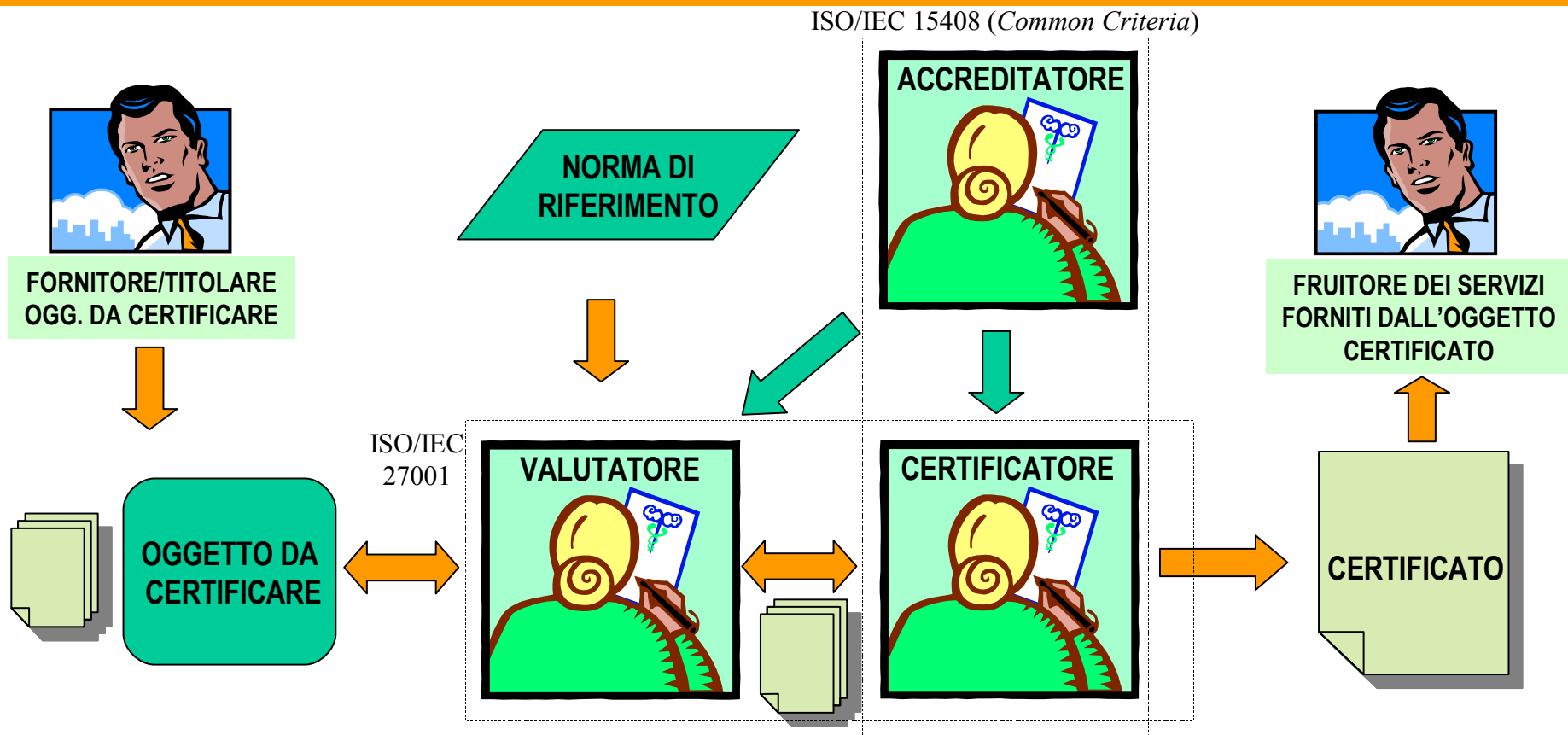
Competenza certificabile secondo criteri quali CISSP/SSCP, CISA/CISM, ecc.)

Sistemi/prodotti ICT
Contromisure tecniche
Certificabili ISO/IEC 15408
(Common Criteria)

Tipi di certificazione

Oggetto certificato	Norme di riferimento
Processo di gestione della sicurezza ICT (ISMS)	ISO/IEC 27001
Sistema/prodotto ICT	ISO/IEC 15408 (<i>Common Criteria</i>) ITSEC
Competenza del personale	CISSP/SSCP, CISA/CISM, ecc.

Le entità in gioco



Le certificazioni in Italia regolate da DPCM

- Certificazione di prodotto/sistema ICT
 - Schema Nazionale del 1995 aggiornato nel 2002 (DPCM 11 aprile 2002 – GU n. 131 del 6 giugno 2002) applicabile nel contesto della sicurezza interna e esterna dello Stato
 - Ente di Certificazione/Accreditamento (EC): ANS/UCSi
 - Centri di Valutazione (Ce.Va.): 3 privati, 2 pubblici (tra cui ISCOM)
 - Schema Nazionale del 2003 (DPCM 30 ottobre 2003 – GU n. 98 del 27 aprile 2004) applicabile in tutti i contesti non coperti dal primo Schema
 - Organismo di Certificazione/Accreditamento (OCSI): ISCOM (Ministero Comunicazioni) coadiuvato dalla Fondazione Ugo Bordoni (FUB)
 - Laboratori di Valutazione (LVS): 4 privati
 - Assistenti: 5

I principali compiti dell'OCSI

- Accreditare i Laboratori di valutazione (LVS) e abilitare gli Assistenti (ad oggi 4 LVS accreditati e 5 Assistenti abilitati)
- Revisionare e approvare i rapporti di valutazione sviluppati dagli LVS
- Emettere i certificati
- Gestire lo schema di mantenimento dei certificati
- Produrre e aggiornare la normativa di riferimento nell'ambito dello Schema Nazionale di certificazione
- Mantenere i rapporti con gli Organismo di certificazione esteri anche ai fini del mutuo riconoscimento internazionale

La certificazione dei sistemi e prodotti ICT

Oggetto della valutazione (ODV)

- **Sistema** — Una specifica installazione ICT, caratterizzata da una completa definizione dei servizi svolti e dell'ambiente operativo
- **Prodotto** — Una componente *software, firmware e/o hardware*, che fornisce funzionalità di sicurezza utilizzabili in una molteplicità di sistemi

Approccio generale

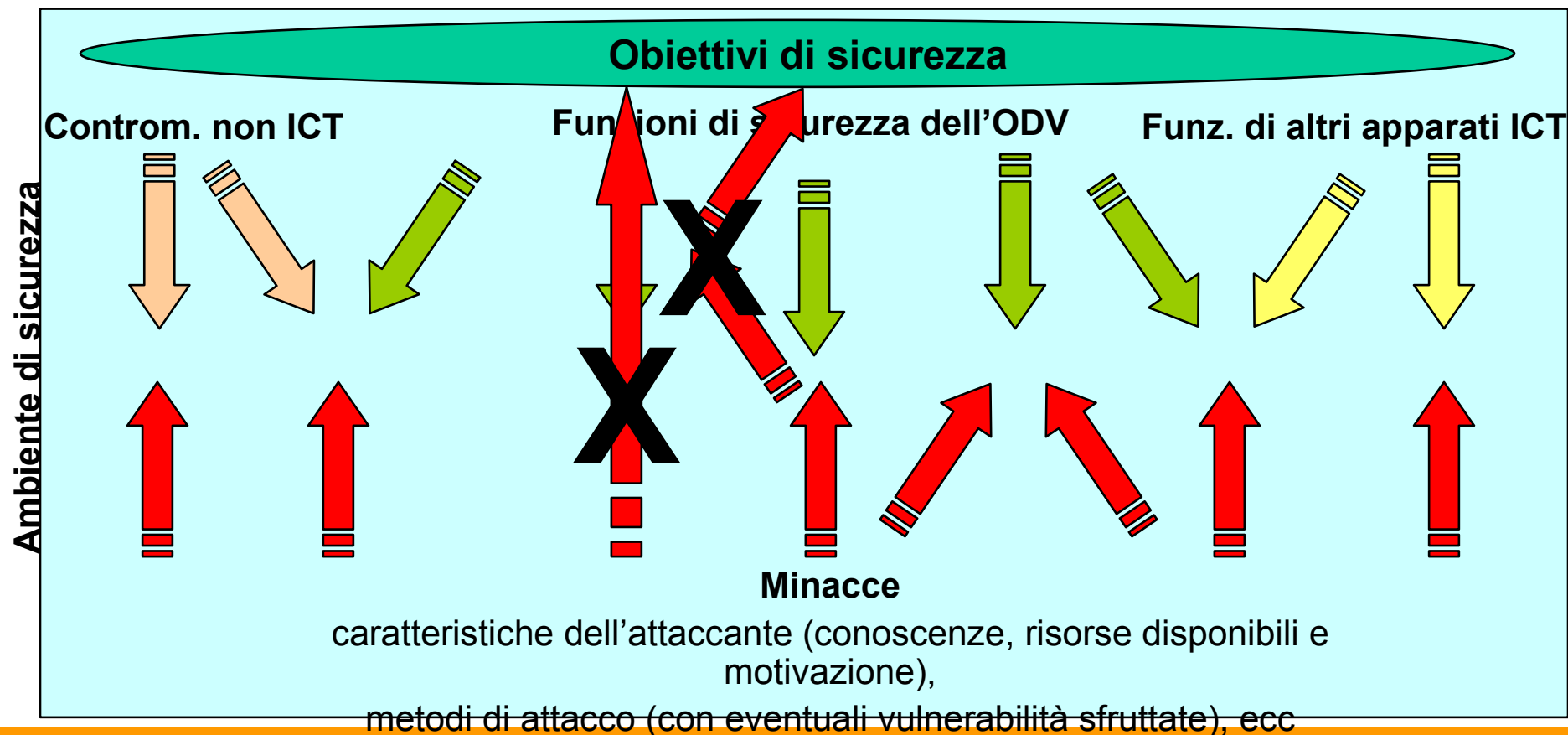
- Verifiche di tipo 1 (ad alto livello)
 - controllano che vi siano tutte le funzioni di sicurezza necessarie, che siano in grado di cooperare efficacemente e che la robustezza dichiarata sia confermabile teoricamente
- Verifiche di tipo 2
 - controllano, con una severità dipendente dal livello di garanzia, che il sw/hw con cui le funzioni sono realizzate esibisca **nelle condizioni di utilizzo dichiarate** il comportamento teorico previsto a fronte di eventi accidentali o di attacchi

Adeguatezza teorica funzioni di sicurezza



caratteristiche dell'attaccante (conoscenze, risorse disponibili e motivazione),
metodi di attacco (con eventuali vulnerabilità sfruttate), ecc

Violazione diretta o indiretta delle funzioni



Modalità di verifica inviolabilità funzioni (1)

Analisi basate su descrizioni delle funzioni

Livello di garanzia →	EAL7	F	F	SF	ST
	EAL6	SF	SF	SF	ST
	EAL5	SF	SF	I	C
	EAL4	I	I	I	P
	EAL3	I	I		
	EAL2	I	I		
	EAL1	I			
		L1	L2	L3	L4

Prove funzionali

V	S
V	S
V	S
V	S
V	S
V	S
V	

Prove d'intrusione

V
V
V
V
V

Document. Ut. e Ammin. Completa. Stati insicuri

X	X
X	X
X	X
X	X
X	X
X	

Dettaglio descrizioni →

L1: Specif. funzionali – L2: Progetto architetture – L3: Prog. dettagliato – L4: Implementaz.
Mod. descritt. I: inform. – SF: semiform. – F: formale – P: parziale – C: completa – ST: struttur.
Prove funzionali e d'intrusione eseguite da V: valutatore – S: sviluppatore

Modalità di verifica inviolabilità funzioni (2)

	Gestione versioni dell'ODV	Consegna e installaz. dell'ODV	Sicurezza amb. svilup. dell'ODV	Strumenti di sviluppo dell'ODV	Correzione difetti dopo la certifi.az.	Mantenimen. certificazione
EAL7	X	X	X	X		
EAL6	X	X	X	X		
EAL5	X	X	X	X		
EAL4	X	X	X	X		
EAL3	X	X	X			
EAL2	X	X				
EAL1	X	X				

Le ultime due modalità di verifica non sono obbligatorie per nessun livello di garanzia ma ne viene raccomandato l'utilizzo

Table 6.1 - Evaluation assurance level summary

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Analisi delle vulnerabilità e robustezza delle funzioni

Caratteristica comune

Entrambe fanno riferimento al potenziale dell'attacco necessario in un caso per individuare e sfruttare la vulnerabilità, nell'altro per forzare la funzione

Differenze

- Nell'analisi delle vulnerabilità vengono considerate tutte le funzioni, in quella relativa alla robustezza solo quelle basate su analisi di tipo statistico
- Nell'analisi di robustezza l'attacco viene portato verso i principi di progetto della funzione e non verso eventuali suoi difetti realizzativi

Alcuni parametri del potenziale d'attacco

- Qualifica dell'attaccante dal punto di vista delle sue **conoscenze tecniche**
 - *layman* (profano, privo di conoscenze specifiche), *proficient* (competente, in possesso di conoscenze relative al comportamento di sicurezza del tipo di sistema/prodotto), *expert* (esperto, conosce approfonditamente il tipo di sistema/prodotto)
- **Tipo di apparato** necessario per condurre un attacco con successo
 - *standard* (facilmente reperibile), *specialised* (reperibile ma con difficoltà), *bespoke* (realizzato specificamente per l'attacco)

Table B.3 Calculation of attack potential

Factor	Range	Identifying value	Exploiting value
Elapsed Time	< 0.5 hour	0	0
	< 1 day	2	3
	< 1 month	3	5
	> 1 month	5	8
	Not practical	*	*
Expertise	Layman	0	0
	Proficient	2	2
	Expert	5	4
Knowledge of TOE	None	0	0
	Public	2	2
	Sensitive	5	4
Access to TOE	< 0.5 hour, or access undetectable	0	0
	< 1 day	2	4
	< 1 month	3	6
	> 1 month	4	9
	Not practical	*	*
Equipment	None	0	0
	Standard	1	2
	Specialised	3	4
	Bespoke	5	6

* Indicates that the attack path is not exploitable within a timescale that would be useful to an attacker. Any value of * indicates a High rating.

Table B.4 Rating of vulnerabilities

Range of values	Resistant to attacker with attack potential of:	SOF rating
<10	No rating	
10-17	Low	Basic
18-24	Moderate	Medium
>25	High	High



Organismo

Le linee d'azione strategiche dell'OCSI

Gli obiettivi prioritari

- Fare tesoro delle esperienze non del tutto positive delle certificazioni eseguite negli schemi esteri
- Tenere in grande considerazione gli interessi dell'**utilizzatore finale** dei sistemi ICT e non solo quelli dei fornitori di prodotti
- Individuare soluzioni utilizzabili anche dai numerosi **integratori di sistema** esistenti in Italia

Le certificazioni eseguite all'estero

Sono quasi tutte certificazioni **di prodotto** finanziate dai fornitori che le eseguono per migliorare l'immagine del proprio prodotto

- sono eseguite a livelli di *assurance* medi o alti (altrimenti l'immagine del prodotto non risulterebbe migliorata)
- richiedono tempi e costi elevati (quindi poche certificazioni eseguite)
- spesso vengono eseguite in condizioni piuttosto distanti da quelle tipiche di utilizzo del prodotto
- non vengono generalmente mantenute valide nel tempo, sia per motivi di costo, sia perché viene di fatto consentito che si continui a pubblicizzarle

Come eseguire le certificazioni: considerazioni iniziali (1/2)

- Il maggior numero di incidenti informatici deriva da vulnerabilità note per le quali spesso esistono le *patch*
- Non ha molto senso utilizzare prodotti “molto sicuri” in sistemi complessivamente molto vulnerabili
 - Il livello di sicurezza del sistema dipende dalla robustezza dell'anello più debole della catena

Come eseguire le certificazioni: considerazioni iniziali (2/2)

- Spesso si incrementa maggiormente il livello di sicurezza effettivo
 - verificando le modalità di utilizzo delle funzioni di sicurezza nel sistema IT (es.: configurazione firewall, non specificata nella certificazione di prodotto)
- piuttosto che
 - analizzando la struttura interna di una parte delle funzioni (livelli medi e alti di certificazione su prodotti inclusi nel sistema) sperando di trovare nuove vulnerabilità

Come eseguire le certificazioni: le indicazioni principali

- Promuovere la certificazione a **bassi livelli** di assurance dell'intero **sistema** (vulnerabilità note sfruttabili assenti anche al primo livello di certificazione EAL1 – cfr anche versione 3.0 dei Common Criteria)
- Promuovere ai bassi livelli di *assurance* il **mantenimento** sistematico dei certificati

Vantaggi della certificazione a bassi livelli di assurance (EAL1-2)

- 1) Si può condurre in modo relativamente semplice sull'intero sistema ICT, consentendo così
 - di incrementare notevolmente il livello di sicurezza effettivo
 - di verificare la validità delle integrazioni di sistema
- 2) Risulta sensibilmente più economica e rapida rispetto ai livelli medi e alti di assurance
- 3) Risulta sufficientemente agevole mantenere il certificato nel tempo
- 4) E' possibile individuare una ampia fascia di potenziali Assistenti di sicurezza con le competenze necessarie per svolgere compiti di supporto alla valutazione e di mantenimento del certificato

Gli ulteriori obiettivi

- Collaborare con i soggetti che gestiscono **certificazioni di sicurezza complementari** (es: collaborazione con Sincert)
- Favorire la diffusione delle certificazioni sia in ambito pubblico (es: collaborazione con CNIPA) sia in ambito privato (es: partecipazione a convegni anche in affiancamento agli LVS)
- Evidenziare e valorizzare il più possibile i pregi principali della certificazione
 - garanzia fornita da una **terza parte**
 - applicazione di uno **standard internazionale**

Grazie dell'attenzione

Per ulteriori informazioni:
www.ocsi.gov.it