



L'interpretazione dello standard BS7799 relativamente alle aree di confine con i Common Criteria

Gabriella Actis Dato
UNINFO



Sommario

- ISO/IEC 15408 e ISO/IEC 17799
- ... e gli altri
- La normazione e la certificazione
- Cosa possiamo fare per voi

ISO/IEC 15408 e ISO/IEC 17799

Orientamento dei metodi

	Technical	Non Technical
System specific	IT Baseline	ISO 9000 ISO 133335 CobiT ISO 17799
Product Specific	FIPS 140	ISO 15408

Da ISO/IEC 15443



Approccio e ciclo di vita

	Design	Integration	Deployment	Operation
Product	15408	15408	15408	15408
Process				17799
Environment				

Da ISO/IEC 15443



Lavoro in Italia (FUB)

- Interpretazione dello standard BS 7799 in relazione ai controlli applicabili a sistemi o prodotti ICT (Cimitan, Orazi, Romeo)



Sovrapposizione - Aree

- 8. Communications and operations management
- 9. Access control
- 10. System development and maintenance
- 12. Compliance (review of security policy and technical compliance)



Sovrapposizione - aspetti

- A. Organizzativo – procedurale
- B. Tecnologico (documenti ed interviste)
- C. Tecnologico (puntuale)
- D. Tecnologico (sottoattività)



Aree da approfondire

	8 Comm.	9 Access	10 Systems	12 Compl.
A - Org	2		1	
B - Tec1	2	4	4	
C - Tec2		1	4	
D - Tec3				1



Strategia congiunta

- Gestione rischi
 - Alto rischio. Trasferimento del rischio a organizzazione esterna
 - Rischio basso. Verifica prodotto o sistema
- Misure non tecniche in TS e PP



... e gli altri

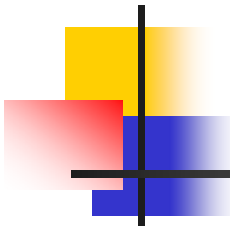
Almeno altre 33 specifiche de jure in questa area. Cosa scegliere? La risposta in :

ISO/IEC 15443 - IT Security Techniques

Part 1 - Overview and framework (TR)

Part 2 - Assurance methods (DTR)

Part 3 - Analysis of assurance methods (WD)



ISO/IEC 15443 - IT Security Techniques

Part 1 - Overview and framework

- Definizioni: assurance, confidence, deliverables, schemes, approaches....
- Modello di riferimento

ISO/IEC 15443 -

Part 2 - Assurance methods

- 35 metodi valutati individualmente dal punto di vista dell'approach e dello stadio del ciclo di vita del prodotto
- ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 21827, TCMM, FIPS 140, X/OPEN, CobiT, IT baseline, TDEP ...

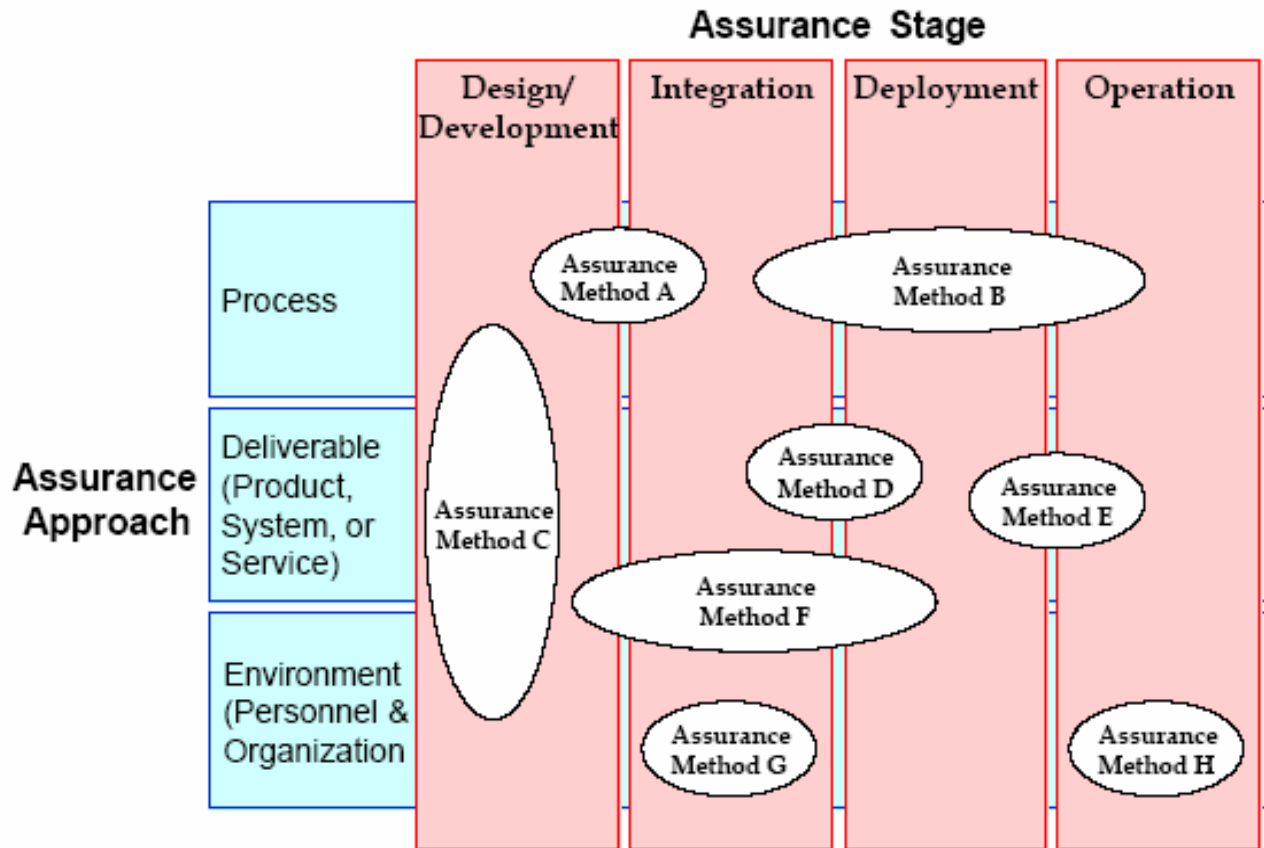


Figure 2: Categorisation of existing assurance methods

ISO/IEC 15443 -

Part 3 - Analysis of assurance methods

- Properties
- Composition
- Benchmarking
- One-to-one comparaison



Da ISO/IEC 15443-3

Table 7 - IT service management properties

DOMAIN	COBIT	PROCESS
Planning & Organisation	PO1	Define a strategic IT plan
	PO2	Ensure compliance with external requirements
	PO3	Manage human resources
	PO4	Communicate management aims and direction
	PO5	Manage the IT investment
	PO6	Determine technological direction



ISO/IEC 15443 -

Part 3 - Composition

- IT baseline and ISO/IEC15408
- ISO 17799 and IT Baseline
- ISO 9000 and ISO 17799
- FIPS140 and ISO/IEC15408 and ISO/IEC 21827
- IT Baseline and CobiT



ISO/IEC 15443 -

Part 3 - Benchmarking

- IT Baseline
- ISO/IEC 17799 and BS7799
- ISO TR 13335
- ITSECC/ISO/IEC 15408
- FIPS 140-1/2
- CobiT
- ISO 9000



ISO/IEC 15443 -

Part 3 - One to one comparaision

- ISO/IEC 21827 con ISO/IEC 15408
- TCMM con ISO/IEC 15408
- ISO 9000 con ISO/IEC 15408
- X/OPEN con ISO/IEC 15408
- FIPS 140-2 con ISO/IEC 15408
- ISO/IEC 21827 con ISO 13335
- ISO/IEC 21827 con ISO 17799



Normazione e certificazione

- Due diverse facce di stessa medaglia
- Non vi può essere buona certificazione senza buona normazione.
- Difficile buona normazione per gestione sicurezza: fattori intangibili, dipendenza da ambiente
- Frammentazione e volatilità di iniziative



Cosa vogliono gli utenti

- Ascoltare, non parlare, risposte puntuali a esigenze precise
- Sportello unico
- Loro linguaggio
- Impegno limitato di risorse (quantità e durata)



Cosa trovano gli utenti

- Frammentazione (es. traffico: CEN, ETSI, ISO; Smart Cards: CEN, JTC1, ISO, ETSI; Design for All: ETSI, CEN, CENELEC, ISO, IETF, ITU, W3C)
- 21 enti nella lista precedente, e 35 norme su argomenti simili
- Poche norme formali (TRs, ETSI stds, CWs, fast track)



Scioglilingua

Analysis of Assurance Methods analyses the various assurance methods with respect to their assurance properties. The analysis will aid the Assurance Authority in deciding the relative value of each Assurance Approach and determining the assurance approach(s) that will provide the assurance results most appropriate to their needs within the specific context of their operating environment. Furthermore, the analysis will also aid the Assurance Authority to use the assurance results to achieve the desired confidence of the deliverable

(Da: ISO/IEC 15443-1)



Cosa gli NSO possono fare

- Servizi
- Ricerche
- Disseminazione
- Accreditamento
- Legittimazione



Gruppo di lavoro UNINFO

- Prima riunione del gruppo di lavoro “Sicurezza delle informazioni” nell’ambito della Commissione Tecnica “Tecnologia della informazione – tecniche di sicurezza”
- L'attività del gruppo di lavoro sarà orientata alla proposta di norme nazionali sul tema della sicurezza delle informazioni, sulla base di quanto già esistente al livello internazionale o in altri paesi.
- Prima attività sarà orientata alla valutazione e traduzione della norma BS 7799-2 per eventuale adozione a livello nazionale.
- Partecipazione allo sviluppo di norme europee o internazionali.



Logistica

- Data: 24 febbraio 2005
- Dove: Sede UNI di Roma
- Per partecipare: segretaria UNINFO



Domande?

- uninfo@uninfo.polito.it
- Tel 011 501027
- www.uninfo.polito.it
- http://www.uninfo.polito.it/INDEX_SICUREZZA.htm

Assurance methods in the framework

Assurance Phase → Approach V	Design Implem.	Integration Verification	Deploym. Transition	Operation
Product (system / Service)	=>D=>	=>I=>	=>T=>	=>O=>
Process	D	I	T	O
Environm. (Organiz / Personn.)	D	I	T	O

Da ISO/IEC 15443

Da ISO/IEC 15443-2

Assurance ISO e non	Design/ Implem.	Integr./ Verif.	Deploy./ Transit.	Operat.
15408	=>D=>	=>I=>	=>T=>	=>O=>
12207	=>D=>	=>I=>	=>T=>	=>O=>
15288	=>D=>	=>I=>	=>T=>	=>O=>
17799				0
13335		I	T	0
17025	D	I		
-----	-----	-----	-----	-----
Altri 35	-----	-----	-----	-----



6.20 ISO/IEC 17799 – Code of practice for information security management

6.20.1 Aim

A framework to enable companies to develop, implement and measure effective security management practice, typically on the organization level.

6.20.2 Description

ISO/IEC 17799 is an International Standard for best practice in information security management. It was first published as a British Standard, BS 7799, prior to adoption by ISO and IEC through the Publicly Available Specification fast-track process. [...] ISO/IEC 17799 is a code of practice for good information security management. Related standard BS 7799-2:1999 is a specification for information security management systems. [...] The controls listed below are defined in ISO/IEC 17799 as those generally accepted as defining the industry baseline of good security practice:

- _ Information security policy
- _ Security organization
- _ [...]

6.20.3 Sources

ISO/IEC JTC 1/SC 27/WG 1 - Information technology - Security techniques - Requirements, security services and guidelines

ISO/IEC 17799 Information technology -- Code of practice for information security management

Table 13 - Target User Group

		IT Baseline Protection Manual	ISO 17799 / BS7799	ISO 13335	ITSEC / Common Criteria	FIPS 140	CobiT	ISO 9000
Key:								
P: primary target group								
S: secondary target group								
X: any organisation								
Type of enterprise	Hardware vendor	S			S	P		X
	Software vendor	S	S		P	P		X
	Network provider		S			S	S	X
	Server operator	P	P			S	S	X
	Content provider	P	P					X
	Enterprise as user	P	P	P		S	P	X
Role within the enterprise	Management	S	P	P			P	P
	Project management	P	P	P	P	P	P	P
	IT security officer	P	P	P	P	P	S	S
	IT management	P	P	P	S	S	P	S
	Administrators	P	S			S	S	S
	Auditors	S	S				P	S