# Standard di valutazione e certificazione della sicurezza IT

10 ottobre 2003

*Ing. Pierluigi Bagni, CISA* *pbagni@deloitte.it*



## Agenda

- Premessa
- Panoramica storica
- Cenni sui principali standards
- L'organizzazione della certificazione nei vari Paesi: ruoli, responsabilità, criteri seguiti.
- La certificazione in Italia. Sviluppi futuri.

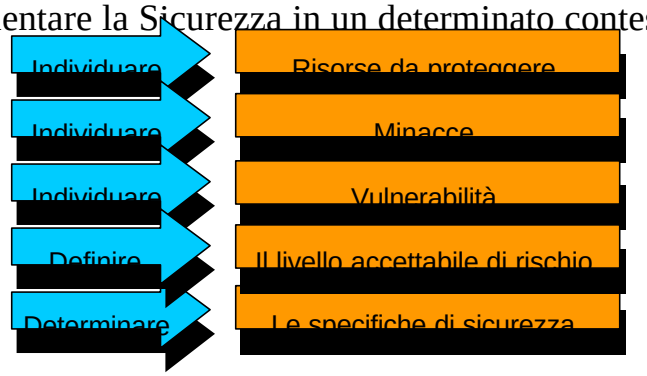
# Premessa – Sicurezza IT

- La Sicurezza IT sta ad indicare la capacità di garantire:
  - Riservatezza (accesso non autorizzato)
  - Integrità (modifiche non autorizzate, deterioramento dei dati e/o dei canali di comunicazione)
  - Disponibilità (continuità dei sistemi)



# Premessa – Sicurezza IT (cont.)

- Implementare la Sicurezza in un determinato contesto vuol dire:




- Un sistema sicuro è dunque un sistema che rispetta una serie di specifiche di sicurezza

## Premessa – Valutazione (cont.)

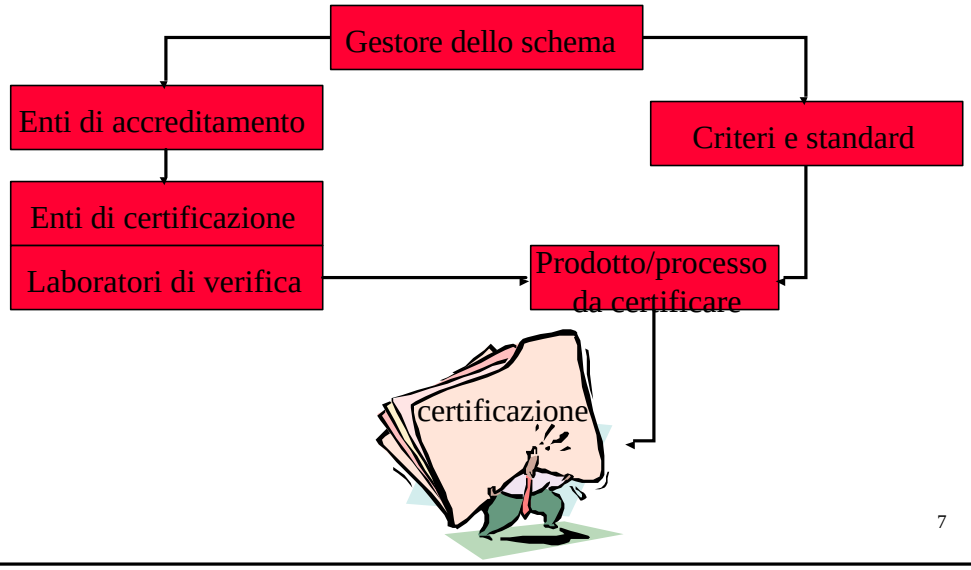
- In linea generale la valutazione consente di rispondere, in maniera probabilistica circa la capacità di un sistema (assurance) di rispettare determinate specifiche di sicurezza
- Emerge dunque la necessità, tra utilizzatore e fornitore di sistemi IT di definire criteri e metodologie per la valutazione delle specifiche di sicurezza richieste da un sistema



## Premessa – Certificazione (cont.)

- La valutazione eseguita da una terza parte indipendente (*Organismo di Certificazione*), sulla base di standards e metodologie riconosciute per le quali l'organismo è stato accreditato da un *Ente di Accreditamento*, consente di ottenere la CERTIFICAZIONE

# Premessa – Certificazione (cont.)






# Panoramica storica

Standard attuali

- TCSEC (Trusted Computer Security Evaluation Criteria o Orange Book, del 1985).
- ITSEC (Information Techonology Security Evaluation Criteria, del 1991) Francia, Germania, Olanda e Regno Unito.
- CTCPEC (Canadian Trusted Computer Product Evaluation Criteria, del 1993) finalizzato a conciliare i concetti del TCSEC e del ITSEC.
- FC (Federal Criteria for Information Technology Security, draft del 1993) volto a unificare il modello Nord Americano con quello Europeo.
- Common Criteria: Stati Uniti, Canada, Francia, Germania, Olanda e Regno Unito, in collaborazione con l'ISO (**I**nternational **O**rganization for **S**tandardization),

# Panoramica storica

- 1980 Inizio attività del Department of Defence Computer Security Center (ora National Computer Security Center, NCSC)
- 1983 Versione preliminare del Trusted Computer Systems Evaluation Criteria, TCSEC
- 1985 Versione definitiva del TCSEC, chiamata Orange Book e degli altri volumi della serie
  - Valutazione effettuata da un organismo governativo in base a principi definiti
  - Il risultato non è un valore assoluto, ma deve intendersi in modo probabilistico
  - L'attività di valutazione stima la fiducia (assurance) che può essere riposta nella capacità del prodotto di soddisfare le specifiche di sicurezza



# Panoramica storica

1989 Germania: *Criteria for the Evaluation of Trustworthness of Information Technology*

1989 Regno Unito: *UK System Security Confidence Levels*

1989 Francia: *Catalogue de Critères Destiné à évaluer le Degré de Confiance des Systèmes d'Information*

1989 Prima versione del *Canadian Trusted Computer Product Evaluation Criteria, CTCPEC*

1990 Versione preliminare di *Information Technology Security Evaluation Criteria, ITSEC* (Francia, Germania, Olanda, Regno Unito)

# Panoramica storica (cont.)

1991 Versione ITSEC 1.2 - Giugno 1991

1991 USA: inizio delle attività del *NIST (National Institute for Standard and Technology)* e dell'*NSA (National Security Agency)* per il *Federal Criteria Project*

1992 Versione preliminare dei Federal Criteria

1993 *Information Technology Security Evaluation Manual, ITSEM* (Commissione delle Comunità Europee) - Versione : 1.0 - Settembre 1993

1993 *CCEB (Common Criteria Editorial Board)* di iniziativa europea con la partecipazione di esperti europei, USA e canadesi per definire i nuovi Common Criteria che armonizzi i criteri europei, USA e canadesi



# Panoramica storica (cont.)

1995 Standard BS 7799 (Gran Bretagna)

1996 Versione iniziale (1.0) dei nuovi Common Criteria

1996 CCEB termina i lavori. I Paesi che hanno sostenuto l'iniziativa decidono di costituire un nuovo gruppo di lavoro (CCIB, Common Criteria Implementation Board) con l'obiettivo di effettuare valutazioni di prova dei CC, sviluppare metodologie comuni di applicazione, ricercare approcci alternativi alla valutazione della sicurezza, negoziare tra i vari Paesi accordi di mutuo riconoscimento dei risultati delle valutazioni condotte

# Panoramica storica (cont.)

1999 Il DPCM 8 febbraio '99 introduce per la prima volta in un atto amministrativo pubblicato sulla G.U. un *requisito di valutazione ITSEC*

2000 ISO 17799 pubblicata nel mese di dicembre del 2000 sulla base della prima parte dello standard BS 7799

2002 Con il dpcm 11 aprile 2002 è stato emanato lo schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato; secondo gli standard ITSEC ITSEM o CC



# Panoramica storica (cont.)

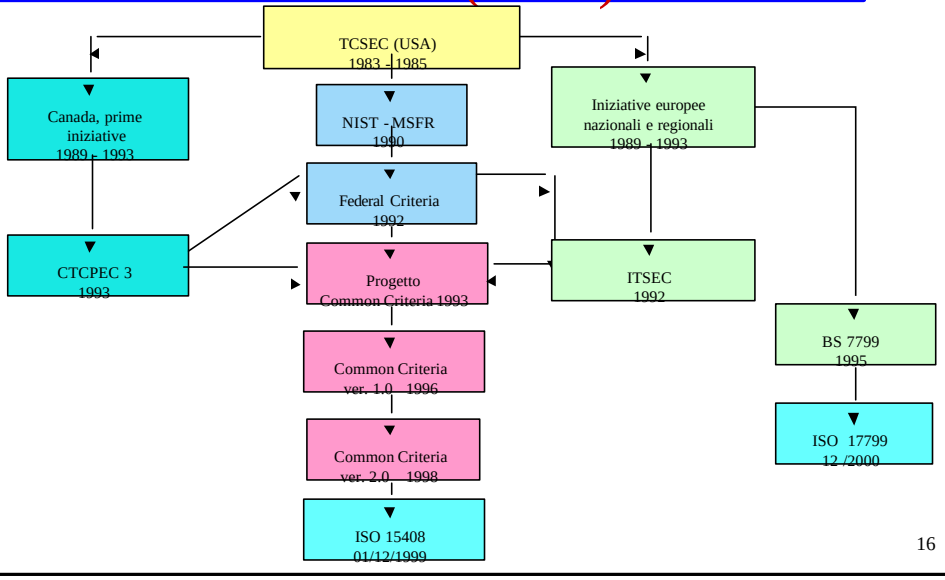
- La caratteristica comune è che il livello di assurance deve essere stimato da un valutatore imparziale e, come precisato dai diversi criteri, dipende:
  - dalle caratteristiche dell'oggetto da valutare
  - dal rigore con cui il valutatore analizza l'oggetto della valutazione e la sua documentazione
  - dalla severità dei requisiti che vengono imposti dai criteri sia sulla stesura della documentazione necessaria alla valutazione sia sull'ambiente e sul processo di sviluppo dell'oggetto stesso

# Panoramica storica (cont.)

- Approccio simile a quello seguito nell'area del controllo di qualità ed implica:
  - la valutazione può essere condotta solo se si conosce a priori a quale livello di assurance si ambisce
  - le azioni che il valutatore deve compiere dipendono da tale livello
- I criteri definiscono una metrica per l'assurance:
  - aspetti e documentazione da considerare
  - azioni che il valutatore deve compiere
  - requisiti sull'ambiente e sul processo di sviluppo
  - modalità di descrizione dell'oggetto da valutare
  - funzioni di sicurezza che deve offrire
  - mirano a soddisfare tutte le esigenze (utilizzatori, produttori, valutatori)
  - precisano ruoli, compiti ed aspettative



# Panoramica storica (cont.)



# Cenni sui principali standards
# Criteri TCSEC

- Orientati alla riservatezza (approccio militare)
- 7 classi: D, C1, C2, B1, B2, B3, A1
- Appartenenza ad una classe sulla base di:
  - politica di sicurezza
  - audit (accountability)
  - fiducia (assurance)
  - documentazione



# Cenni sui principali standards
# Criteri TCSEC (cont.)

- **Classe (D)** Protezione minima
- **Classe (C)** Protezione discrezionale
  - C1 - restrizione d'accesso
  - C2 - controllo accessi
- **Classe (B)** Protezione mandatoria
  - B1 - protezione con etichette
  - B2 - protezione strutturata
  - B3 - domini di sicurezza
- **Classe (A)** Protezione certificata
  - A1 - Progetto certificato

## Criteri ITSEC (cont.)

- ITSEC (Information Technology Security Evaluation Criteria) Gruppo di lavoro misto F, UK, D, NL
- Finalizzato alla "**valutazione**" di sistemi o di prodotti specifici
- Non sono norme ma criteri: identificano le verifiche da eseguire nel corso della valutazione.



## Criteri ITSEC (cont.)

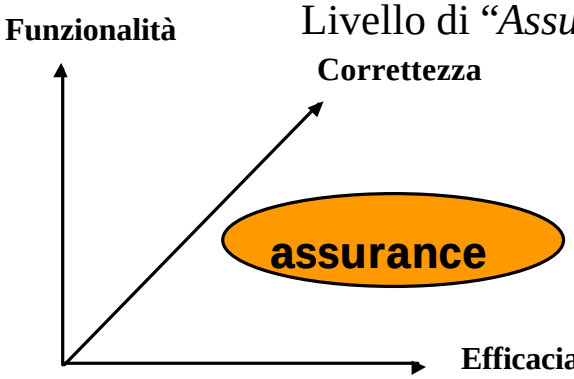
- Formale: cioè basata su azioni note, imparziali, ripetibili, riproducibili (metodologie).
- Hanno come oggetto le contromisure IT, anche se il contesto dell'ambiente di esercizio deve essere descritto con tutte le contromisure anche di altro genere.
- Introduce il concetto di "T.O.E." (**Target of Evaluation**)

# Criteri ITSEC

- IL "Target of Evaluation" viene analizzato separatamente nelle sue due componenti:

  *Funzionalità* di sicurezza previste

  Livello di "*Assurance*" per le funzionalità






# Criteri ITSEC

**Funzionalità**:

- Necessità di specificare gli obiettivi di sicurezza previsti (Security Target)
- 10 classi di funzionalità predefinite, derivate dai criteri tedeschi e dall'Orange Book (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX)

1) Identification and authentication
2) Access control
3) Accountability
4) ……

# Criteri ITSEC

**Aassurance**, due obiettivi:

- efficacia delle funzioni di sicurezza per contrastare le minacce
- correttezza nella realizzazione delle funzioni e dei meccanismi di sicurezza (assurance)

- 7 livelli (E0, E1, ..., E6) di valutazione dell'assurance



# Criteri CTCPEC

- Suddivisione in Criteri Funzionali (Functional Criteria) e criteri per la valutazione dell'assurance (Trust Criteria)
- I criteri funzionali si riferisco a:
  - confidentiality
  - integrity
  - availability
  - accountability
- Ognuno è diviso in aspetti base (Services) con descrizioni di funzionalità precise e ordinate gerarchicamente
- I criteri di assurance fanno riferimento ad un unico aspetto (Trust) con otto livelli di valutazione (T-0 ... T-7)

# Criteri CTCPEC (cont.)

- Il livello di valutazione conseguito da un prodotto esprime la fiducia complessiva che può essere riposta nel prodotto stesso
- E' riferito complessivamente all'insieme di tutte le funzionalità di sicurezza offerte e descritte per mezzo dei criteri funzionali
- Il risultato della valutazione è una lista i cui elementi sono coppe service-level (es.: CD-2, CR-1, ID-1, IS-1, IT-1, WA-1, WI-1, T-2 è la valutazione equivalente di un sistema TCSEC C2)
- Approccio molto sistematico
- Rigido perché considera un ben preciso insieme di funzionalità



# Criteri CC

- Fanno propri alcuni concetti alla base dei criteri preesistenti
- Gli aspetti di assurance vengono separati da quelli funzionali come in ITSEC
- I Common Criteria contengono essenzialmente i principi tecnici fondamentali — di validità generale, chiari e flessibili - per descrivere e valutare**:**
  - **Requisiti funzionali**
  - **Requisiti di affidabilità**

# Criteri CC

**Requisiti funzionali**

- Tali requisiti sono descritti in modo organico e strutturato per due tipologie di situazioni:
  - Protection Profile (PP) — Si riferiscono a famiglie o categorie di prodotti e ambienti generici senza riferimenti a specifici prodotti o sistemi.
  - Security Target (ST) — Si riferisce ad uno specifico prodotto o sistema di cui si conoscono le specifiche di sicurezza.
- Tutti i requisiti di sicurezza (specifiche, descrizione, collegamenti, interdipendenze, ecc.) che si possono comporre nei PP e ST sono contenuti in un
  - Catalogo dei requisiti funzionali della sicurezza



# Criteri CC

**Struttura Protection Profile/Security Target**

Introduction
TOE description
Security environment
Assumptions
Threats
Organizational security
Policies
Security objectives
Security requirements
Functional req’ts
Assurance req’ts
TOE summary specification
Rationale

# Criteri CC

**Classi funzionali per i requisiti di sicurezza**

| Classi funzionali dei CC | Classi funzionali di ITSEC |
|---|---|
| Audit | Audit |
| Communications | Accountability |
| | |
| | Data Exchange |
| User Data Protection | Access Control |
| | |
| | Accuracy |
| | |
| | Object Reuse |
| Privacy | |
| Identification and Authentication | Identification and Authentication |
| Protection of Trusted Security Functions | |
| Resource Utilisation | Reliability of Service |
| TOE Access | Access Control |
| Trustedd path/Channels | Access control |
| | |
| | Data Exchange |



# Criteri CC (cont.)

L'assurance viene trattata definendo 10 classi dei requisiti che concorrono a determinare l'affidabilità della sicurezza

| Classe | Nome |
|---|---|
| ACM | Configuration Management |
| ADO | Delivery & Operation |
| ADV | Development |
| AGD | Guidance Documents |
| ALC | Life Circle Support |
| ATE | Tests |
| AVA | Vulnerability Assessment |
| APE | Protection Profile Evaluation |
| ASE | Security Target Evaluation |
| AMA | Maintenance of Assurance |

# Criteri CC (cont.)

- **I livelli di valutazione dei CC sono 7** e vengono definiti con la sigla **EAL** (Evaluation Assurance Levels) (AL-0, ..., AL-7)

| Livello | |
|---|---|
| EAL1 | functionally tested |
| EAL2 | structurally tested |
| EAL3 | methodically tested |
| EAL4 | methodically tested and checked |
| EAL5 | semiformally designed and tested |
| EAL6 | semiformally verified designed and tested |
| EAL7 | formally verified designed and tested |



# BS 7799

- Gli standard organizzativi (ISO/IEC 17799, ISO/IEC TR 13335) sono rivolti principalmente all'infrastruttura organizzativa ed individuano gli aspetti di sicurezza legati alla politica aziendale, personale, fisica e di gestione del sistema informativo IT. Questi standard si applicano quindi all'intera struttura di sicurezza di un'organizzazione mentre ITSEC e i Common Criteria si applicano ai singoli prodotti IT che costituiscono il sistema informativo IT (es. firewall, data base, dispositivi di firma digitale).
- Lo standard ruota intorno ai due concetti ***politica di sicurezza dell'informazione*** e di **sistema di governo della sicurezza dell'informazione** o ISMS (*Information Security Management System*)

# BS 7799 (cont.)

- La Parte 1 dello standard è un elenco di funzioni di sicurezza (controlli) di tipo organizzativo, logico, fisico, che costituiscono la prassi corrente per garantire la sicurezza dell'informazione in ambito industriale. Lo standard propone un insieme di 127 *controlli* raggruppati in 10 categorie:
  - Security policy
  - Security organization
  - Asset classification and control
  - Personnel security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - System development and maintenance
  - Business continuity management
  - Compliance



# BS 7799 (cont.)

- La Parte 2 dello standard BS7799 propone un modello ISMS dinamico nel quale vengono individuate 6 fasi di analisi e gestione del problema.

# Valutazione e certificazione nei paesi

- Complessa operazione di carattere tecnico
- Svolta da:
  - laboratori specializzati
  - persone accreditate a livello internazionale
- I criteri seguiti devono godere di forme di mutuo riconoscimento in ambito nazionale ed internazionale
- Necessaria quindi una metodologia che segua uno degli standard esistenti
- Alcuni Paesi hanno definito i piani nazionali per la valutazione dei sistemi e dei prodotti IT



# Valutazione e certificazione in USA

- Criteri TCSEC
- Svolta dall'US National Computer Security Center (NCSC), parte della National Security Agency (NSA)
- Modalità di esecuzione specificate dall'NCSC nel Trusted Product Evaluation Program (TPEP), ora divenuto Trusted Product Assessment Program (TPAP)

# Valutazione e certificazione in USA (cont.)

- TPAP:
  - ogni richiesta di valutazione è sottoposta ad un'analisi tecnica preliminare
  - I risultati vengono raccolti nell'Independent Assessment Report (IPAR) che precisa se a parere del gruppo il prodotto potrà superare la valutazione
  - In caso di parere favorevole si procede alle fasi DAP e FEP
  - In caso di parere sfavorevole si avvia la Advice Phase in cui lo sviluppatore può ricevere consigli dai valutatori NCSC o loro consulenti
- L'NCSC ha definito anche il Ratings Maintenance Program (RAMP) per le rivalutazioni



# Valutazione e certificazione in Europa

- Basata su ITSEC/ITSEM
- Il sistema o il prodotto deve essere valutato da un laboratorio accreditato (IT Security Facility, ITSEF)
- Lo sponsor richiede la valutazione
- Certificazione attribuita da un Certification Body che garantisce:
  - imparzialità
  - obiettività
  - ripetibilità
  - riproducibilità
- Necessari i piani nazionali (National Scheme) che specifichino:
  - organizzazione
  - ruoli
  - procedure
  - responsabilità

# Valutazione e certificazione in Europa (cont.)

- I Paesi con maggiore esperienza sono la Germania ed il Regno Unito
- In Germania:
  - esiste il piano nazionale
  - il certificatore e accreditatore è unico: il Bundesant für Sicherheit in der Informationstechnik (BSI)
  - oltre 10 laboratori accreditati dal BSI
- In UK:
  - L'UK IT Security Evaluation and Certification Scheme prevede:
    - » laboratori accreditati (Commercial Licensed Evaluation Facilities, CLEF)
    - » accreditatore il National Measurement Accreditation Service (NAMAS)
    - » ruolo del certificatore congiuntamente affidato al Communication-Electronics Security Group (CESG) e al Department of Trade and Industry (DTI)
  - Le CLEF operano in accordo ad un Quality Manual e ad un Security Manual
  - I prodotti certificati sono sottoposti a verifica annuale
  - Attualmente sono attive cinque CLEF



# Valutazione e certificazione in Europa (cont.)

- Anche la Francia, dopo un periodo di studio di tre anni, ha sviluppato un piano nazionale (1995):
  - Gestione del piano e certificatore è il Service Central de la Securité des Systemes d'Information (SCSSI)
  - Valutazioni in accordo a ITSEC/ITSEM da laboratori accreditati ITSEF (IT Security Evaluation Facility)
  - SCSSI accredita i laboratori

# La valutazione e certificazione in Italia

- 30 Agosto 1995: emanazione di due direttive governative che riguardano:
  - come devono essere condotte le operazioni di omologazione (accreditamento secondo ITSEC) dei laboratori di valutazione
  - come devono essere condotte le valutazioni per i prodotti o sistemi che trattano dati coperti da segreto di stato e vietata divulgazione
  - il ruolo di omologatore dei laboratori, detti Centri di Valutazione (CE.VA.) che è affidato all'Autorità Nazionale per la Sicurezza (ANS) che svolgerà tale compito tramite l'Ufficio Centrale per la Sicurezza (UCSi)
  - attualmente i centri di valutazione sono : IMQ, inforsud , ISCTI e RES
- 2002 Il SINCERT (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione) ha accreditato il Rina quale ente certificatore iso 17799



# Il ruolo del valutatore

- Persona accreditata a livello nazionale (meglio se internazionale)
- Rispetto di un codice di comportamento ed etica professionale
- Creazione di un Albo
- Attualmente esistono delle certificazioni aggiuntive (USA):
  - CISA (Certified Information Systems Auditor)
  - CISM (Certified Information Security Manager)
  - CISSP (Certified Information Systems Security Professional)

# Sviluppi futuri della certificazione

- Possibili fattori di incremento delle richieste di certificazione della sicurezza dei sistemi e dei prodotti:
  - specifici requisiti di un particolare progetto
  - esigenza di creare un'immagine prestigiosa dell'azienda dimostrando la capacità di riservatezza, integrità e disponibilità delle informazioni trattate
  - migliori condizioni assicurative
  - ridurre il rischio di costi connessi ad una gestione non adeguata della sicurezza



www.isacaroma.it

*Ing. Pierluigi Bagni, CISA*
*pbagni@deloitte.it*