La valutazione della sicurezza

Bernardo Palazzi

UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Valutazione della sicurezza

- La valutazione è un processo nel quale la sicurezza è raccolta e analizzata tramite il confronto con criteri generali.
- Il risultato consta di una misura del livello di fiducia che indica il grado con cui il sistema sia conforme a particolari criteri.
- I criteri utilizzati dipendono dall'obiettivo di valutazione e dalla metodologia di valutazione desiderata.

UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

L'importanza della valutazione della sicurezza informatica

- Decidere le azioni e gli investimenti economici per ridurre l'esposizione ai rischi
- Valutare l'opportunità di acquisire prodotti e servizi
- Sapere fino a che punto è possibile fidarsi di prodotti, sistemi e servizi
- Pubblicizzare le caratteristiche di sicurezza di un prodotto o di un servizio

Problemi della valutazione

- Per misurare qualcosa bisogna prima definirla con precisione
- Qual è l'oggetto della valutazione?
  - Per valutare il livello di sicurezza occorre definire una metrica
  - Qual è la scala in base cui si può asserire che un oggetto è più sicuro di un altro
    - più contromisure?
    - meno rischi?
    - più attenzione alla sicurezza?

Caratteristiche generali per la valutazione

- **Imparzialità**: il Laboratorio per la Valutazione del Software (LVS) non deve avere interessi economici connessi con il risultato della valutazione
- **Ripetibilità**: un LVS deve ottenere lo stesso risultato ripetendo la valutazione
- **Riproducibilità**: un altro LVS deve ottenere lo stesso risultato ripetendo la valutazione
- **Obiettività**: il risultato della valutazione non deve essere determinato da giudizi soggettivi

La certificazione della sicurezza

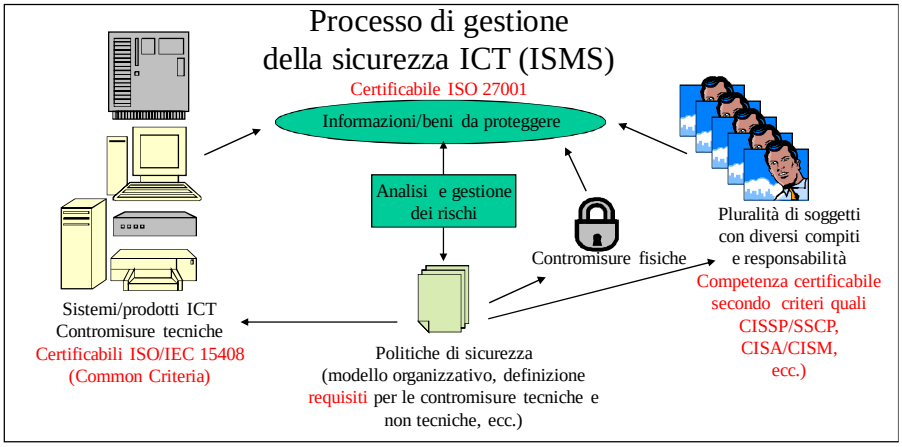
La certificazione deve essere eseguita in modo da garantire l'imparzialità, l'oggettività, la ripetibilità e la riproducibilità dell'intero processo di certificazione. A tal fine:

- l'accreditatore, il certificatore ed il valutatore (qualora sia presente) devono essere terza parte indipendente rispetto al:
  - Fornitore/titolare dell'oggetto da certificare
  - Fruitore della certificazione
- la certificazione deve basarsi su criteri o standard di riferimento comunemente accettati
- deve essere verificata la competenza di chi applica la norma di riferimento (valutatore/certificatore)

Metodi di certificazione

- **DEI PRODOTTI / DEI SISTEMI**
  - TCSEC
  - ITSEC
  - COMMON CRITERIA (ISO 15408)
  - FIPS
- **DEI SISTEMI / PROCESSI**
  - ISO 27001
- **DELLE PERSONE (suddivise per ambiti...)**
  - CISSP/SCCP/CAP/CSSLP
    (differenti livelli di esperienza professionale)
  - CISA/CISM (audit e management)
  - OPSA (security tester, VA, ecc…)
  - OSCP (offensive security) (pen tester, ecc.…)

La valutazione della sicurezza ICT in un'organizzazione



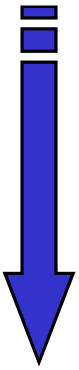
Fonte: FUB-ISCOM

TCSEC (1983-1999)

- Trusted Computer System Evaluation Criteria elaborato dal governo U. S. (Orange Book)
- Prima metodologia completa per la valutazione della sicurezza
- Non sicurezza ma livelli di fiducia
- Un prodotto/sistema è fidato se è dotato di determinate protezioni
- La scala è determinata dal numero di protezioni presenti (orientato tendenzialmente ai sistemi operativi e successivamente esteso ad altri ambiti tramite le “rainbow series”)

Scala TCSEC

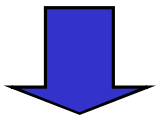
- **Criteri di valutazione della garanzia:** sono i metodi con cui viene valutata la fiducia che può essere accordata ai sistemi e ai prodotti informatici di sicurezza



  - **C1** protezione di sicurezza discrezionale
    - Modello DAC
  - **C2** protezione ad accessi controllati
    - C1 + riuso degli oggetti e auditing
  - **B1** protezione obbligatoria (labeled security)
    - MAC su un insieme ridotto di oggetti
  - **B2** protezione strutturata
    - MAC per tutti gli oggetti
  - **B3** domini di sicurezza
    - Implementa un reference monitor
  - **A1** progetto controllato (verified protection)
    - B3 + analisi covert channel, verifica “formale” del progetto

Limiti del TCSEC

- Le protezioni menzionate nello standard sono tipiche di elaboratori non connessi in rete
- Lo standard non consente flessibilità nella modalità di valutazione: la complessità è proporzionale al livello di sicurezza
- Ci sono pochi livelli per cui quasi tutti i prodotti sono stati valutati con livello medio-alto (C2)



Il processo di valutazione è costoso

I miglioramenti dello standard europeo ITSEC

- Elaborato dalla Gran Bretagna, Francia, Germania e Olanda
- Deve essere definito l'oggetto della valutazione (Target Of Evaluation)
- Deve essere definito l'obiettivo della valutazione (Security Target)
- E' possibile effettuare la valutazione con diversi livelli di severità (Evaluation Assurance Level)

Dall'ITSEC ai Common Criteria (CC)

- ITSEC è uno standard europeo mentre i Common Criteria sono uno standard internazionale
- In ITSEC gli elementi che qualificano la valutazione sono scelti dal committente se non si leggono i documenti della valutazione non si hanno informazioni sulle caratteristiche di sicurezza
- Nei Common Criteria è possibile fare riferimento a profili di protezione predefiniti e certificati (Protection profile) relativi a tipologie omogenee di prodotti

Caratteristiche dei CC (ISO 15408)

- Forniscono un'istantanea della sicurezza di un prodotto o di un sistema
- Il risultato è significativo quando il prodotto è utilizzato nelle condizioni in cui è stato valutato
- Il processo di valutazione ha una durata commisurata al livello di severità
- E' suddiviso in 3 parti
  - Parte 1: Introduzione e modello generale
  - Parte 2: Requisiti funzionali di sicurezza
  - Parte 3: Requisiti di *assurance*
- http://www.commoncriteriaportal.org/

Target Of Evaluation (TOE)

- Costituisce l'Oggetto Della Valutazione (ODV), può essere:
  - un prodotto, cioè un pacchetto IT che può essere acquistato e impiegato in svariati ambienti operativi
  - un sistema, cioè una specifica installazione IT per cui sono definiti a priori lo scopo e l'ambiente operativo

Security Target (ST)

- E' un documento che definisce il Traguardo Di Sicurezza (TDS), come:
  - Beni
  - Minacce
  - Ipotesi
  - Ambiente operativo
- E' suddiviso generalmente in:
  - Obiettivi di sicurezza
  - Requisiti funzionali relativi alla sicurezza
  - Requisiti di sicurezza informatica
  - Assunzioni
  - Rationale

Protection Profile (PP)

- Normalmente è creato da una società o da un gruppo di utenti
- E' una specifica indipendente di requisiti di sicurezza
- Costituisce un modello per il Security Target

Significato CC

- Ha senso certificare che un apparato ICT è sicuro solo se si specifica:
  - sicuro per fare cosa (obiettivi di sicurezza)
  - sicuro in quale contesto (ambiente di sicurezza)
  - sicuro a fronte di quali verifiche eseguite (soddisfacimento requisiti di *assurance*)
- In altri termini:
  - la valutazione della sicurezza secondo i CC ha lo scopo di offrire garanzie (*assurances*), che è possibile graduare, sulla capacità del TOE di soddisfare i propri *obiettivi di sicurezza* nell'*ambiente di sicurezza* per esso ipotizzato

Evaluation Assurance Level (EAL)

- Rappresenta una misura della garanzia che il TOE raggiunga i suoi obiettivi di sicurezza rispetto al proprio ST
  - **EAL1** testato funzionalmente
  - **EAL2** testato strutturalmente
  - **EAL3** testato e verificato metodicamente
  - **EAL4** progettato, testato e riveduto metodicamente
  - **EAL5** progettato e testato in modo semi-formale
  - **EAL6** verifica del progetto e testing semi-formali
  - **EAL7** verifica del progetto e testing formali

Livelli di sicurezza

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

Livello di *assurance* crescente

- Sicurezza maggiore

- Componenti di livello gerarchico più elevato (numeri identificativi più grandi)

Un prodotto certificato CC è sicuro?

- Microsoft Windows 2000 è un prodotto certificato EAL4+, ma sono state pubblicate regolarmente da Microsoft patch di sicurezza per vulnerabilità
- Ciò è possibile perché il processo di certificazione Common Criteria permette a un produttore di effettuare assunzioni riguardo all'ambiente operativo e alle relative tipologie delle minacce
- Basandosi su queste assunzioni vengono valutate le funzioni di sicurezza rivendicate dal prodotto

Un prodotto certificato CC è sicuro? (2)

- Quindi la certificazione EAL4+ di Microsoft Windows 2000, deve essere considerata sicura solo nella configurazione di valutazione specificata da Microsoft
- Ogni vulnerabilità che possa compromettere il prodotto nella configurazione di valutazione, dovrebbe comportare:
  - La cancellazione volontaria da parte del produttore della propria certificazione
  - Il produttore dovrebbe rivalutare il prodotto per includere l'applicazione delle patch per fissare le vulnerabilità nella configurazione di valutazione
  - Teoricamente la certificazione dovrebbe essere sospesa o cancellata dall'ente che l'ha emessa
- Microsoft Windows 2000 resta certificato EAL4+ solo se non si applica di nessuna patch
- Ciò mostra sia i limiti che la forza di una configurazione valutata

FIPS 140: 1994 - oggi

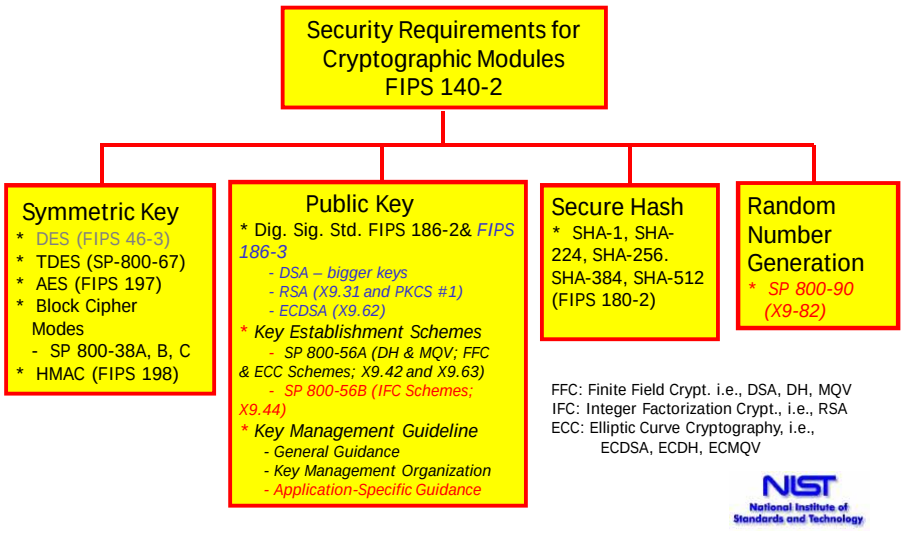
- Federal Information Processing Standards sviluppati dal CSE Canadese e NIST Americano
- Standard mirato alla certificazione della crittografia
- Gli utenti (agenzie governative, banche, ecc.)che desiderano implementare moduli crittografici devono certificare la validità rispetto ai certificati FIPS 140
- FIPS 140-1 e FIPS 140-2 specificano esattamente moduli e versioni di: hardware, software, firmware.
- I requisiti coprono non solo il funzionamento ma anche la documentazione e ad alto livello alcuni commenti nel codice sorgente.

FIPS 140-2

- FIPS 140-2 definisce 4 livelli di sicurezza.

1. Tutti i componenti devono essere "production-grade" e le vulnerabilità più note devono essere verificate
2. Aggiunge “tamper-evidence” fisica e autenticazione role-based RBAC
3. Aggiunge “tamper-resistance” fisica, autenticazione identity-based
4. Aggiunge requisiti di sicurezza fisica più stringenti, ad es. robustezza contro attacchi ambientali.

Standard Crittografici



FFC: Finite Field Crypt. i.e., DSA, DH, MQV
IFC: Integer Factorization Crypt., i.e., RSA
ECC: Elliptic Curve Cryptography, i.e., ECDSA, ECDH, ECMQV

NIST National Institute of Standards and Technology

Dalla sicurezza dei prodotti a quella dei processi

- Finora l'attenzione si è rivolta soprattutto alla sicurezza dei prodotti che realizzano le protezioni, con metodi e standard che forniscono una "fotografia" della sicurezza
- L'attuale modello di erogazione dei servizi informatici sposta l'attenzione verso i processi organizzativi: occorre verificare se vi siano o meno i presupposti per la corretta gestione della sicurezza nel tempo

ISO 27001

- Punto di partenza per impostare un sistema organizzativo che abbracci tutti gli aspetti della sicurezza delle informazioni.
- Contiene i requisiti per la implementazione, gestione e certificazione di un ISMS (Information Security Management System) oppure SGSI (Sistema Gestione Sicurezza Informazioni).
- (opzionale) È applicabile a qualsiasi contesto produttivo e a qualsiasi tipo di organizzazione. (come tutte le iso)
- Si ispira ai principi guida dell'OECD (OCSE). (doc. cultura sicurezza)
- Ha come modello di riferimento per la descrizione dei processi e dei requisisti dello standard il modello PDCA (Plan-Do-Check-Act). Ciclo di deming

ISO 27001 (2)

- Nasce dal Bristish Standard, poi diventato ISO
  - BS7799-1 (ISO 17799 –> ISO 27002)
    - Propone una serie di best practice per i controllo di sicurezza fisica, logica, organizzativa. Non sempre sono tutte applicabili. Viene spiegato cosa fare non come farlo.
  - BS7799-2 (ISO 27001)
    - Descrive come strutturare il sistema di gestione della sicurezza delle informzioni (SGSI oppure ISMS).
- L'Allegato A della ISO 27001 è allineato con la ISO 27002. è il primo allegato obbligatorio di una norma iso.

ISO 27001: obiettivi

- **Dimostrare** la conformità e efficacia delle scelte organizzative e delle attività operative poste in atto per garantire il RID delle informazioni incluse nel perimetro coperto dal ISMS.
- **Assicurare** la continuità del business, minimizzare danni in caso di incidenti, massimizzare investimenti per la gestione della sicurezza, miglioramento continuo.

ISO 27001: argomenti

- Caratteristiche del sistema di gestione della sicurezza - Information Security Management Systems (ISMS)
  - Strategie di sicurezza
  - Definizione del contesto
  - Identificazione dei beni
  - Valutazione dei rischi
  - Identificazione delle aree critiche
  - Gestione dei rischi
  - Identificazione ed attuazione dei controlli appropriati
  - Formalizzazione delle scelte

ISO 27001 – Allegato A

- Politiche di sicurezza
- Organizzazione
- Classificazione e controllo dei beni
- Personale
- Sicurezza fisica
- Gestione dei sistemi e delle infrastrutture
- Controllo accessi
- Sviluppo e gestione dei sistemi
- Continuità del servizio
- Aderenza a norme e direttive

La norma ISO 27001 (2)

- Attività di verifica
  - Verifica della conformità alla norma
  - Verifica dell'efficacia e correttezza
- Strategie di sicurezza
- Obiettivi di sicurezza
  - Identificazione di eventuali lacune di sicurezza
- Miglioramento della gestione della sicurezza
  - Verifica del rispetto degli obblighi contrattuali
  - Verifica del rispetto delle norme

Le motivazioni alla base del successo della norma ISO 27001

- Attenzione agli aspetti organizzativi
- Semplicità del processo di certificazione
- Analogia con gli standard di certificazione della qualità (serie ISO 9000)
- Possibilità di verifica dei presupposti per la corretta gestione della sicurezza nel tempo, con l'obiettivo di un improvement continuo, nell'ottica PDCA

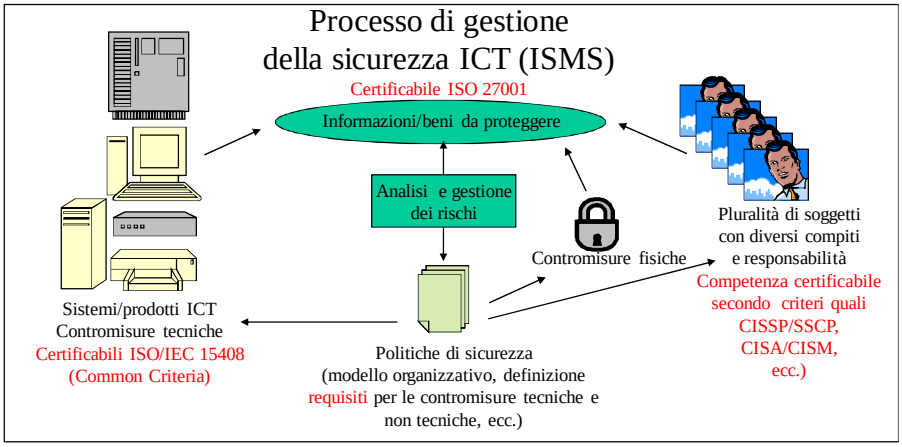
Limiti della ISO 27001

- Chi è sottoposto a verifica decide lo "scope" dei controlli, cioè può escludere alcune aree dal controllo
- La certificazione non attesta il livello di sicurezza, ma la presenza di un processo idoneo a gestire la sicurezza
- I margini di discrezionalità di chi esegue la certificazione in "pratica" sono ampi, anche se esiste una ISO 19011 che descrive le tecniche di auditing

CISSP – SSCP e CISA – CISM

- Gestiti dall'$(ISC)^2$
  - Certified Information Systems Security Professional
  - System Security Certified Practitioner
- Esami di certificazione della competenza professionale nella sicurezza informatica, richiedono:
  - un'esperienza professionale di almeno 4 anni maturata nel settore della sicurezza ICT
  - Il superamento di una prova scritta composta da 250 domande a risposta multipla in lingua inglese in 6 ore su differenti argomenti della sicurezza ICT
- Gestiti dall'ISACA
  - Certified Information Systems Auditor (dal 1978 – 44000 certificati)
  - Certified Information Security Manager (dal 2003 – 5400 certificati)

La valutazione della sicurezza ICT in un'organizzazione



Fonte: FUB-ISCOM

Organismi che si occupano di sicurezza informatica

Organismi internazionali

OCSE (WPISP)	www.oecd.org	OECD
IETF	sec.ietf.org	IETF
ITU	www.itu.int	ITU

Organismi americani

NIST	csrc.nist.gov	
NSA	www.nsa.gov	
DHS	www.dhs.gov	

Organismi Europei
ENISA

- www.enisa.eu.int
- Agenzia dell'Unione Europea istituita nel 2004, ha la missione di assicurare un livello di sicurezza alto ed efficace per le reti e le informazioni nell'ambito dell'Unione Europea (istituita con regolamento (CE) n. 460/2004)
- Composizione:
  - Direttore generale (Andrea Pirotti)
  - Management Board composto da:
    - rappresentanti degli stati membri
    - rappresentanti della commissione europea
    - Permanent Stakeholder Group
    - Ad hoc working group su
      - Awareness Raising
      - Cert Cooperation and Support
      - Technical and Policy aspects on risk assessment and management

Organismi italiani

Organismi di controllo

- Ogni corpo dello stato può intervenire nel controllo e nella repressione di ogni tipo di crimine informatico:
  - La polizia postale, in particolare, si occupa di reati di pedofilia online
  - Il nucleo operativo della guardia di finanza si occupa di repressioni frodi telematiche e violazione del diritto d'autore

Organismi di normazione e formazione

CNIPA	www.cnipa.gov.it	CNIPA Centro Nazionale per l'Informatica nella Pubblica Amministrazione
GOVCERT	www.govcert.it	GOV CERT IT Computer Emergency Readiness Team
CTNSI	www.cnipa.gov.it	**Comitato Tecnico Nazionale Sicurezza Informatica**

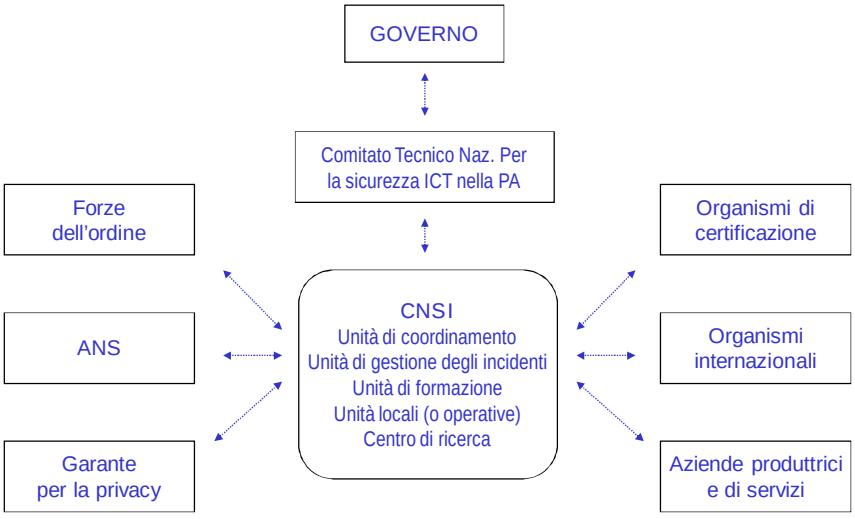
Organismi di certificazione Italiani

COMMON CRITERIA	OCSI	www.ocsi.gov.it	OCSI Organismo di Certificazione della Sicurezza Informatica
COMMON CRITERIA	ANS	www.serviziinformazionesicurezza.gov.it	cesis
ISO 27001	Accredia	www.sincert.it www.accredia.it	SINCERT ACCREDIA SISTEMA ITALIANO DI ACCREDITAMENTO

La verifica della sicurezza nella PA

- La legge sulla privacy prescrive, con cadenza almeno annuale, la revisione del documento programmatico sulla sicurezza ed attività di verifica della "sussistenza delle condizioni per la conservazione dei profili di autorizzazione"(DL 196/03 allegato B)
- Possibilità di auto-valutazione (ad es. con questionario allegato alla Direttiva del Ministro per l'Innovazione e le Tecnologie)
- Possibilità di utilizzo di checklist costruite a partire dai controlli della norma ISO/IEC 17799 (BS7799 parte 1)
- Esistono linee guida provvisorie disponibili sul sito dell'ISCOM - OCSI:
  - http://www.ocsi.gov.it/Default.aspx?tabid=187

Il Centro Nazionale per la Sicurezza Informatica



Enti privati

- clusit
- ipsa
- issa
- sikurezza.org
- interlex.it
- www.infosecworld.com
- ...
- ...