Organismo di Certificazione della Sicurezza Informatica

Lo standard ISO/IEC 15408: le modalità applicative a tutela degli utilizzatori dei sistemi ICT e la complementarità con lo standard ISO/IEC 27001

Massimiliano Orazi
Fondazione Ugo Bordoni

Sessione di studio comune AIEA-ISCOM
Roma, Ministero delle Comunicazioni, 31 Gennaio 2007

Organismo di Certificazione della Sicurezza Informatica

Sommario (1/2)

- I Concetti di base della certificazione Common Criteria
- Definizione della strategia dell'OCSI
  - Da dove partire
  - Strategie per la tutela dell'utente finale
  - La situazione italiana
  - La strategia dell'OCSI

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Sommario (2/2)

- Aspetti di complementarietà delle certificazioni ISO/IEC 15408 e 27001
  - La sicurezza ICT in una organizzazione
  - Ambiti di applicazione delle certificazioni della sicurezza ICT
  - Benefici delle certificazioni ISO/IEC 27001 e 15408
  - Confronto e interpretazioni delle due norme
  - Analisi dei rischi e ISO/IEC 15408
  - Analisi dei controlli della norma ISO/IEC 27001

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

La certificazione CC

Ha senso certificare che un apparato ICT è sicuro solo se si specifica:

- sicuro per fare cosa (obiettivi e politiche di sicurezza)
- sicuro in quale contesto (ambiente di sicurezza)
- sicuro a fronte di quali verifiche eseguite (soddisfacimento requisiti di *assurance*)

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Cosa vuol dire *garanzia (assurance)*? (1/2)

E’ una misura della fiducia che l’ODV raggiunga i suoi obiettivi di sicurezza

Il rischio che i beni siano compromessi è ridotto ad un livello accettabile

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Cosa vuol dire *garanzia (assurance)*? (2/2)

- La garanzia dipende da
  - Il livello di dettaglio dell'analisi del Valutatore
  - Il livello dell'attività di test svolta dal Fornitore e dal Valutatore
  - Il rigore della documentazione prodotta dal Fornitore

- Ne deriva il concetto di Livello di garanzia

  (nei Common Criteria da EAL1 a EAL7)

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

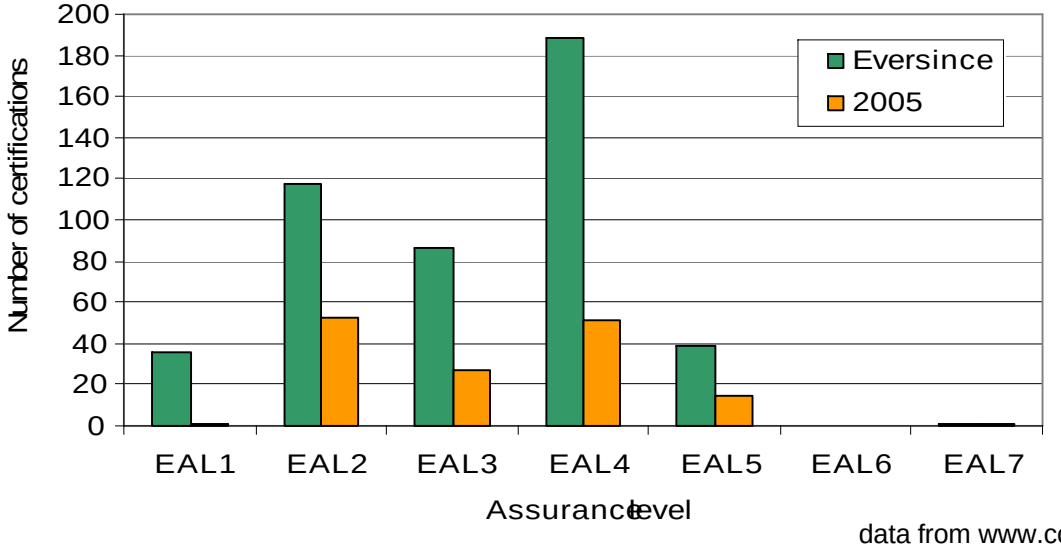
Da dove partire per una strategia efficace?

1) Fare tesoro delle esperienze non del tutto positive delle certificazioni eseguite negli schemi esteri
2) Tenere in grande considerazione gli interessi dell'utilizzatore finale dei sistemi ICT e non solo quelli dei fornitori di prodotti
3) Prevenire le critiche che i detrattori delle certificazioni possono fondatamente muovere osservando i limiti, spesso macroscopici, delle certificazioni già eseguite

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Come vanno le cose all'estero?



data from www.commoncriteriaportal.org

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

iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

L'utilità delle certificazioni di prodotto

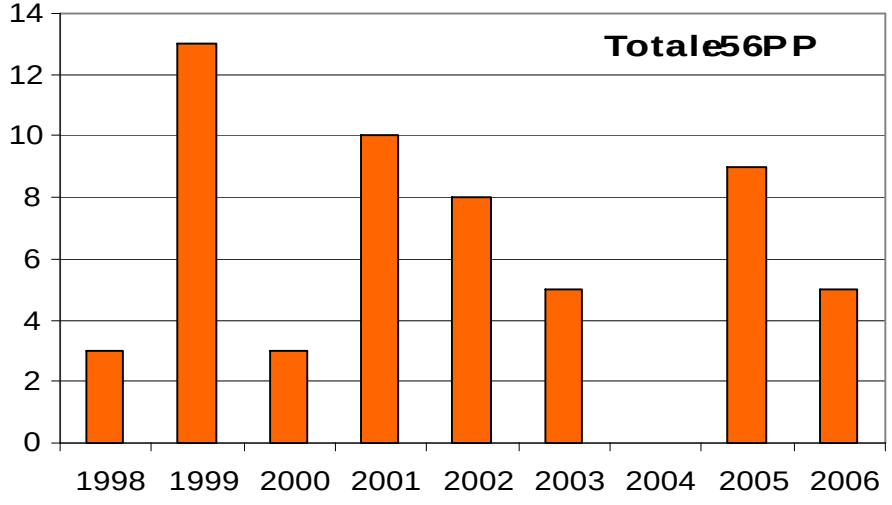
- Sono i grandi produttori di *sw*, per lo più, a far certificare i propri **prodotti** a livelli **medi o alti** i quali, pur essendo già molto onerosi, sono però i livelli minimi che consentono lo sfruttamento a fini pubblicitari della certificazione
- Le certificazioni a livelli medi o alti implicano **tempi e costi elevati**, il che costituisce un freno al diffondersi della certificazione
- Spesso le certificazioni vengono eseguite in condizioni piuttosto distanti da quelle tipiche di utilizzo del prodotto

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

La certificazione, i PP e i sistemi

- La certificazione dei **Protection Profile** è stata particolarmente incentivata dalla PA USA. Tali certificazioni vengono utilizzate soprattutto come “capitolati” per la fornitura



Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Esempi di Protection Profile

- CAPP (Controlled Access PP), NSA, USA, 1999:

  Specifica un insieme di requisiti funzionali per implementare delle limitazioni sui diritti di accesso degli utenti sulle risorse del sistema e per fornire potenzialità di auditing.

- SSCD (Secure Signature Creating Devices), CEN, Germania, 2002:

  Specifica un insieme di requisiti crittografici e gestionali per i dispositivi di generazione di firma elettronica; è utilizzato come standard di riferimento nella normativa europea.

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

La certificazione, i PP e i sistemi

- Sono poco diffuse le certificazioni di **sistema**, ad eccezione del contesto relativo alla sicurezza nazionale

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

La tutela dell'utilizzatore (1)

- Spesso i prodotti vengono certificati in condizioni molto diverse dalle normali condizioni di utilizzo (es: sistema operativo con funzionalità di rete disattivate)
- A volte dai livelli di certificazione si può essere ingannati. Spesso è più importante verificare le modalità di utilizzo delle funzioni di sicurezza (configurazioni) nel sistema IT dell'utilizzatore, piuttosto che studiare a fondo la struttura di un singolo componente
- L'utilizzatore finale del prodotto è spesso vittima di una pubblicità ingannevole, anche a causa dell'atteggiamento non sempre chiaro degli Organismi di certificazione

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

La tutela dell'utilizzatore (2)

Il **mantenimento nel tempo** delle certificazioni, pur essendo essenziale per l'utilizzatore, non viene eseguito perché:

– le certificazioni risulterebbero più costose

– molti Organismi di certificazione esteri non revocano né impediscono l'uso pubblicitario di certificazioni che non sono più efficaci, limitandosi a precisare che le certificazioni valgono solo nel momento in cui vengono emesse

– non vengono forniti o pubblicizzati strumenti per il mantenimento della certificazione

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Scenario italiano

- Non vi sono i grandi produttori di *sw* come all'estero
- Vi sono invece molti integratori di sistemi
- Seguire lo stesso approccio estero comporterebbe:
  - una diffusione ancor più limitata delle certificazioni (di prodotto)
  - una scarsa tutela dell'utilizzatore finale

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Alcune considerazioni a corredo

- 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

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Quindi cosa fare???

- Promuovere la certificazione ai **livelli di garanzia iniziali**, soprattutto nel caso di **sistemi**
- Promuovere, per certificazioni a livelli di garanzia iniziali il **mantenimento** sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**
- Diffondere la certificazione di **sistema** a **livelli di garanzia iniziali** nella PA, eventualmente utilizzando i Protection Profile, per innescare un effetto “volano”

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Vantaggi della certificazione a livelli di garanzia iniziali (EAL1-2)

1) E’ comunque garantita l’assenza nell’ODV delle vulnerabilità più comuni
2) E’ abbastanza agevole **mantenere il certificato nel tempo**
3) La certificazione è **più economica e più rapida** rispetto ai livelli medio-alti di assurance
4) Si può condurre in modo semplice **sull'intero sistema ICT**
5) I compiti di valutazione e mantenimento del certificato possono essere svolti da una ampia fascia di Assistenti di sicurezza

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Quindi cosa fare???

- Promuovere la certificazione a **livelli di garanzia iniziali**, soprattutto per i **sistemi**
- Promuovere, per certificazioni a livelli di garanzia iniziali, il **mantenimento** sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**
- Diffondere la certificazione di **sistema** a **livelli di garanzia iniziali** nella PA, eventualmente utilizzando i Protection Profile, per innescare un effetto “volano”

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Quindi cosa fare???

- Promuovere la certificazione a **livelli di garanzia iniziali**, soprattutto per i **sistemi**
- Promuovere, per certificazioni a livelli di garanzia iniziali il **mantenimento** sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**
- Diffondere la certificazione di **sistema** a **livelli di garanzia iniziali** nella PA, eventualmente utilizzando i Protection Profile, per innescare un effetto “volano”

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Quindi cosa fare???

- Promuovere la certificazione a **livelli di garanzia iniziali**, soprattutto per i **sistemi**
- Promuovere, per certificazioni a livelli di garanzia iniziali il **mantenimento** sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**
- Diffondere la certificazione di **sistema** a **livelli di garanzia iniziali** nella PA, eventualmente utilizzando i Protection Profile, per innescare un effetto “volano”

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

E inoltre…

- Cercare un dialogo, piuttosto che uno scontro, con i soggetti che gestiscono **certificazioni di sicurezza complementari** (ad es. ISO/IEC 27001)
- Valorizzare il più possibile i pregi principali della certificazione: garanzia fornita da una **terza parte** e applicazione di uno **standard internazionale**

Massimiliano Orazi

Fondazione Ugo Bordoni

31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Sommario

Aspetti di complementarietà delle certificazioni ISO/IEC 15408 e 27001

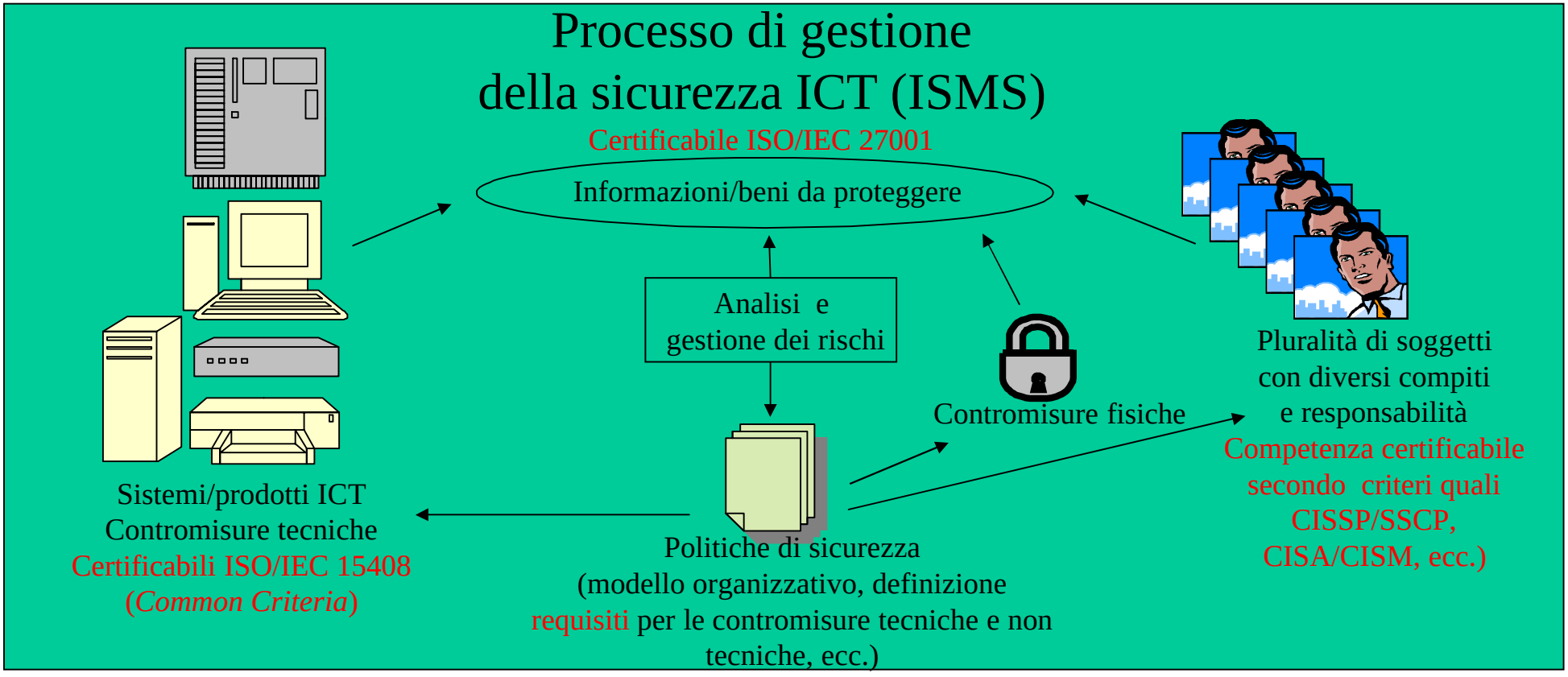
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

La sicurezza ICT in un'Organizzazione



iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Tipi di certificazione

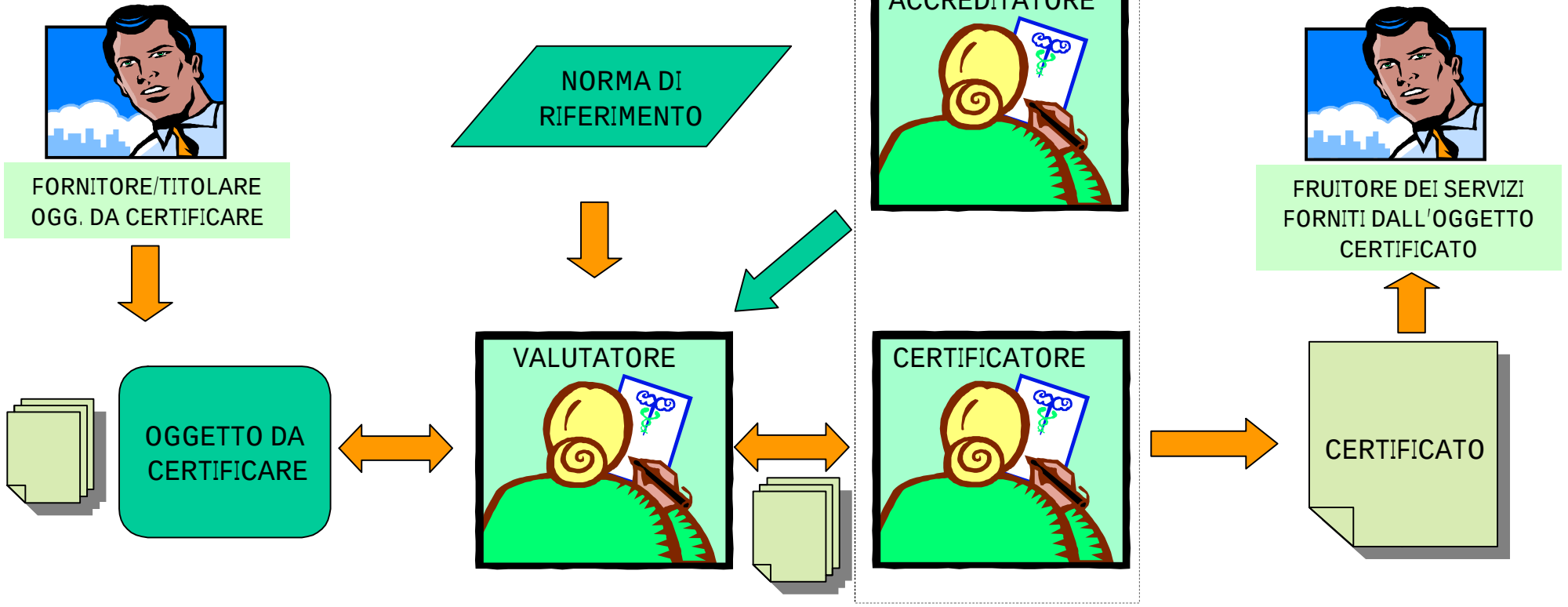
Oggetto certificato	**Norme di riferimento**
Processo di gestione della sicurezza ICT (ISMS)	ISO/IEC 27001
Sistema/prodotto ICT	ISO/IEC 15408 (*Common Criteria*) ITSEC
Competenza del personale	CISSP/SSCP, CISA/CISM, ecc.

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Le entità in gioco

ISO/IEC 15408 (*Common Criteria*)



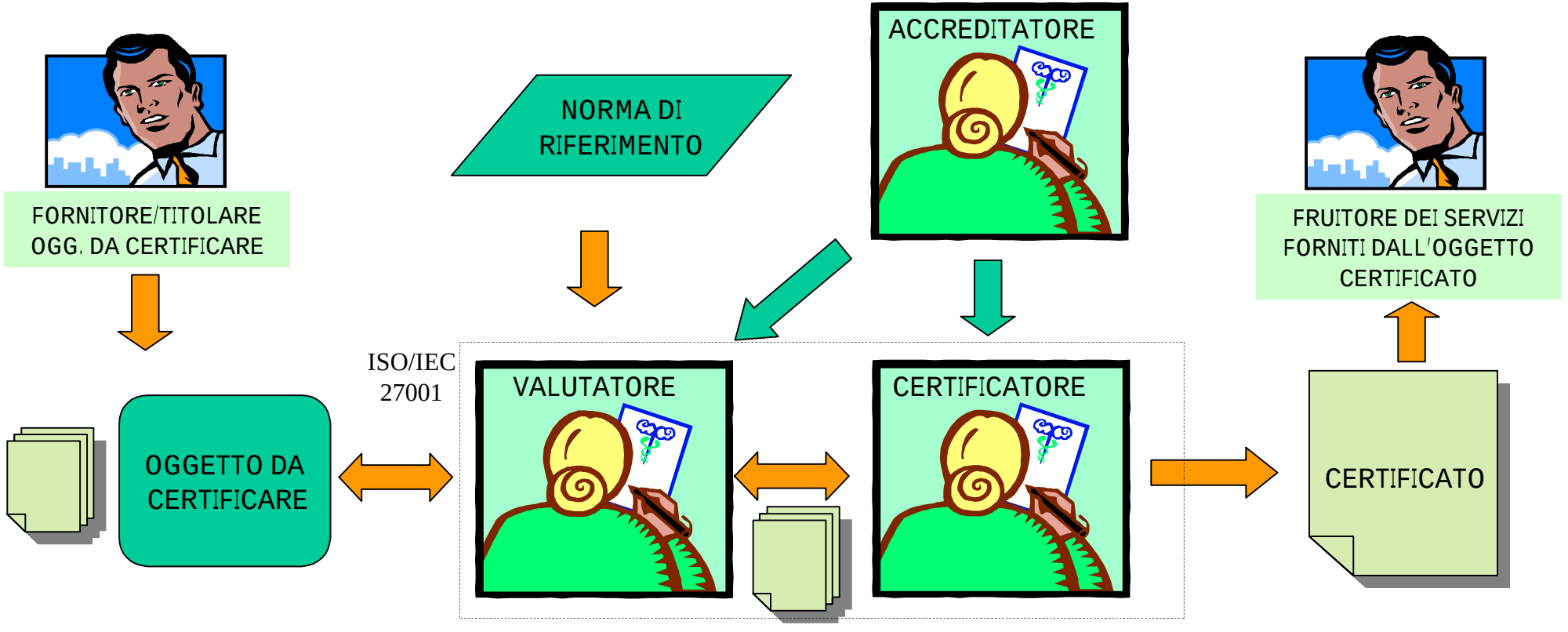
iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Le entità in gioco



Massimiliano Orazi

Fondazione Ugo Bordoni

31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

I benefici delle certificazioni ISO/IEC 27001 e 15408

- Verifica continua delle competenze dei laboratori di valutazione
- Lo standard ISO/IEC 15408 è l'unico che fornisce gli strumenti per effettuare una valutazione della sicurezza di prodotti e sistemi ICT
- L'OCSI dispone di una struttura che opera un monitoraggio costante delle vulnerabilità dei prodotti certificati
- I benefici della certificazione ISO 27001

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Complementarietà delle norme ISO/IEC 27001 e 15408 (1/3)

- Le norme hanno finalità diverse:
  - lo standard ISO/IEC 27001 è stato sviluppato per certificare il sistema di gestione della sicurezza delle informazioni (ISMS);
  - lo standard ISO/IEC 15408 (ed i criteri ITSEC) è stato sviluppato per certificare la sicurezza di sistemi o prodotti ICT.
- Tuttavia prevedono in alcuni casi requisiti e verifiche che presentano aspetti similari

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Complementarietà delle norme ISO/IEC 27001 e 15408 (2/3)

Obiettivi

1. Sfruttare al meglio le potenzialità di ciascuna norma nell'ambito delle finalità per cui è stata sviluppata
2. Evitare sconfinamenti reciproci che porterebbero a coprire con una norma inadeguata attività di verifica per le quali l'altra norma è specializzata
3. Individuare possibili economie in caso di uso congiunto delle due norme (eliminazione di possibili duplicazioni di attività)

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Complementarietà delle norme ISO/IEC 27001 e 15408 (3/3)

- Le certificazioni secondo le due norme vengono rese **complementari** e **sinergiche**
- Qualora venissero eseguite entrambe le certificazioni si otterrebbe un'ottimizzazione in termini di efficacia ed efficienza:
  - un livello di sicurezza globale più elevato
  - un costo globale minore

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Le norme ISO/IEC 27001 e 15408 confronto e interpretazioni (1/3)

• In presenza di certificazioni della sicurezza di sistemi o prodotti ICT, nell'organizzazione che sta certificando il proprio ISMS, l'Auditor ISO 27001 verificherà se **le ipotesi e le politiche dichiarate nel Traguardo di Sicurezza** (ST, Security Target) del sistema o prodotto ICT in esame **trovano riscontro nell'ISMS dell'organizzazione**

(interpretazione riferibile all'Obiettivo 1)

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Le norme ISO/IEC 27001 e 15408 confronto e interpretazioni (2/3)

- La norma ISO/IEC 27001 definisce anche controlli che riguardano misure di tipo tecnico
- L'Auditor ISO 27001 non dovrà eseguire alcuna verifica finalizzata alla valutazione dell'affidabilità della funzionalità di sicurezza. Qualora, discostandosi dallo spirito della norma, tentasse ugualmente di farlo, non troverebbe nella norma alcun riferimento alla metodologia con la quale operare

(interpretazione riferibile all'Obiettivo 2)

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Le norme ISO/IEC 27001 e 15408 confronto e interpretazioni (3/3)

• In presenza di sistemi o prodotti ICT certificati ISO/IEC 15408 l'Auditor ISO 27001 non dovrà necessariamente eseguire su essi test miranti ad ottenere garanzie che siano già fornite dalla certificazione ISO/IEC 15408.

(interpretazione riferibile all'Obiettivo 3)

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Analisi dei rischi e ISO/IEC 15408

- La certificazione dell'ISMS prevede la possibilità di **ridurre i rischi mediante l'utilizzo di prodotti e sistemi ICT certificati ISO/IEC 15408**
- La certificazione ISO/IEC 15408 infatti:
  - può ridurre la probabilità di incidenti informatici
  - può diminuire i danni per l'Organizzazione, una volta che gli incidenti informatici si siano comunque verificati

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Analisi dei rischi e ISO/IEC 15408

L'eventuale scelta di non avvalersi delle certificazioni ISO/IEC 15408/ITSEC dovrebbe essere adeguatamente giustificata nell'analisi dei rischi, sopratutto nei casi di particolare criticità per l'Organizzazione

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Analisi dei controlli della norma ISO/IEC 27001

- Analisi effettuata sugli standard:
  - ISO/IEC 17799:2005 "*Information technology – Security techniques - Code of practice for information security management*"
  - ISO/IEC 27001 "*Information technology – Security techniques - Information security management system - Requirements*"

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Fondazione Ugo Bordoni

Massimiliano Orazi

Fondazione Ugo Bordoni

31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Classifica Controlli ISO 27001

- Individuazione delle categorie di controlli definiti nella norma ISO/IEC 27001 che fanno riferimento a sistemi e/o prodotti ICT
  - **10 – Communications and operations management**
  - **11 – Access Control**
  - **12 – Information systems acquisition, development and maintenance**

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006

Organismo di Certificazione della Sicurezza Informatica

Classifica Controlli ISO 27001

- Nell'ambito di queste categorie, è utile definire tre tipologie di controlli
  1. Controlli di carattere organizzativo/procedurale
  2. Controlli di carattere tecnologico che riguardano sistemi e/o prodotti ICT per i quali l'Auditor ISO 27001 dovrebbe limitarsi a verificare, analizzando documenti, intervistando il personale o, al più, eseguendo semplici prove, la sola presenza di funzionalità di sicurezza
  3. Controlli di carattere tecnologico che riguardano sistemi e/o prodotti ICT per i quali l'Auditor ISO 27001 dovrebbe limitarsi a verificare, analizzando documenti, intervistando il personale o, al più, eseguendo semplici prove, che le caratteristiche e le modalità di utilizzo delle funzionalità di sicurezza soddisfino i requisiti espressi nei controlli

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Prima Tipologia

- Esempio

11.1.1 Access control policy
An access control policy should be established, documented, and reviewed based on business and security requirements for access.

- L'Auditor ISO 27001 deve verificare che sia stata definita, documentata e sottoposta a revisione una politica per il controllo dell'accesso alle informazioni e alle strutture per l'elaborazione delle stesse.

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Prima Tipologia

- Alcuni controlli, classificati nella prima tipologia, sono da ritenersi parzialmente soddisfatti qualora il prodotto risulti iscritto ad un programma di mantenimento del certificato:
  - 10.1.2, relativo al controllo delle modifiche effettuate alle strutture per l'elaborazione delle informazioni (sistemi operativi, applicativi software);
  - 10.3.2, relativo alla definizione di criteri di approvazione e di eventuali test per nuovi sistemi informativi, aggiornamenti e nuove versioni di software in uso presso l'organizzazione
  - 12.4.1, relativo al controllo dell'installazione del software operativo
  - 12.5.2, relativo alla definizione di test per le applicazioni critiche per il business dell'organizzazione nel caso in cui siano effettuate modifiche ai sistemi operativi.

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Seconda Tipologia

- Esempio

> **11.7.1 Mobile computing and communications**
> A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

- L'auditor ISO 27001 in questo caso deve verificare, tra l'altro, la presenza di misure IT per la protezione delle informazioni gestite dai dispositivi mobili, e per l'accesso remoto alle informazioni di business dell'azienda attraverso reti pubbliche (ISO/IEC 17799:2005)

- La verifica dell'effettiva affidabilità delle funzionalità di sicurezza adottate non è richiesta dalla norma ISO/IEC 27001

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Terza Tipologia

- Controlli di carattere tecnologico per i quali l'attività degli Auditor ISO 27001 è affine allo svolgimento di azioni di valutazione definite in ISO/IEC 15408
- Rispettando lo spirito della norma, tali attività di auditing possono al più arrivare a verificare le impostazioni di configurazione di programmi come gli antivirus oppure ad eseguire semplici prove finalizzate a verificare la presenza di funzionalità di sicurezza
- In ogni caso quindi le attività svolte dagli Auditor ISO 27001 non sono mai comparabili per livello di approfondimento con le attività svolte dal valutatore ISO/IEC 15408

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Terza Tipologia

- Esempio

> **10.4.1 Controls against malicious code**
> Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

- L'Auditor ISO 27001 deve verificare se l'organizzazione ha installato e mantiene regolarmente aggiornato un software per il rilevamento di codice malevolo. In particolare lo standard ISO/IEC 17799:2005 richiede, tra le altre, una verifica che tale software sia configurato in modo tale da effettuare tre specificati tipi di scansione
- La verifica dell'affidabilità delle suddette scansioni non è compito dell'Auditor ISO 27001

Massimiliano Orazi
Fondazione Ugo Bordoni

Organismo di Certificazione della Sicurezza Informatica

Conclusioni

Quella dell'OCSI è una importante sfida che viene condotta per innalzare il livello di sicurezza dell'intero Paese.

Certificare con l'OCSI deve poter significare "**proteggere veramente**"

Massimiliano Orazi
Fondazione Ugo Bordoni
31 Gennaio 2006