

BS 7799 e contratti ICT



Seminario CLUSIT "La sicurezza nei contratti ICT"
Milano 16 Giugno 2003

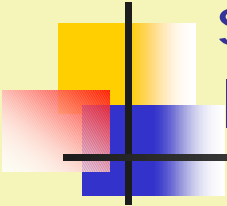
Vittorio Asnaghi

Comitato Direttivo CLUSIT
vittorio.asnaghi@virgilio.it



Scenario normativo ICT security

- Norme (o meglio criteri) per valutare il grado di Assurance (garanzia, oppure fiducia) della sicurezza di prodotti o sistemi informatici.
 - TCSEC (Trusted Computing Security Evaluation Criteria, 1985).
 - ITSEC (Information Technology Security Evaluation Criteria, 1992, Europa).
 - Common Criteria o ISO/IEC 15408 (1999, Internazionali. www.common-criteria.org).
- Norme dedicate al sistema di gestione della sicurezza delle informazioni (SGSI). Argomento è la gestione dei sistemi informativi.
 - BS7799 (UK, 1995)
 - BS7799 Part. 1 (UK, 1999)
 - BS7799 Part. 2 (UK, 2002)
 - ISO/IEC 17799 (Internazionale, 2000)
- Norme funzionali sui prodotti ICT.



Norme per il sistema di gestione della sicurezza delle informazioni (SGSI o ISMS)

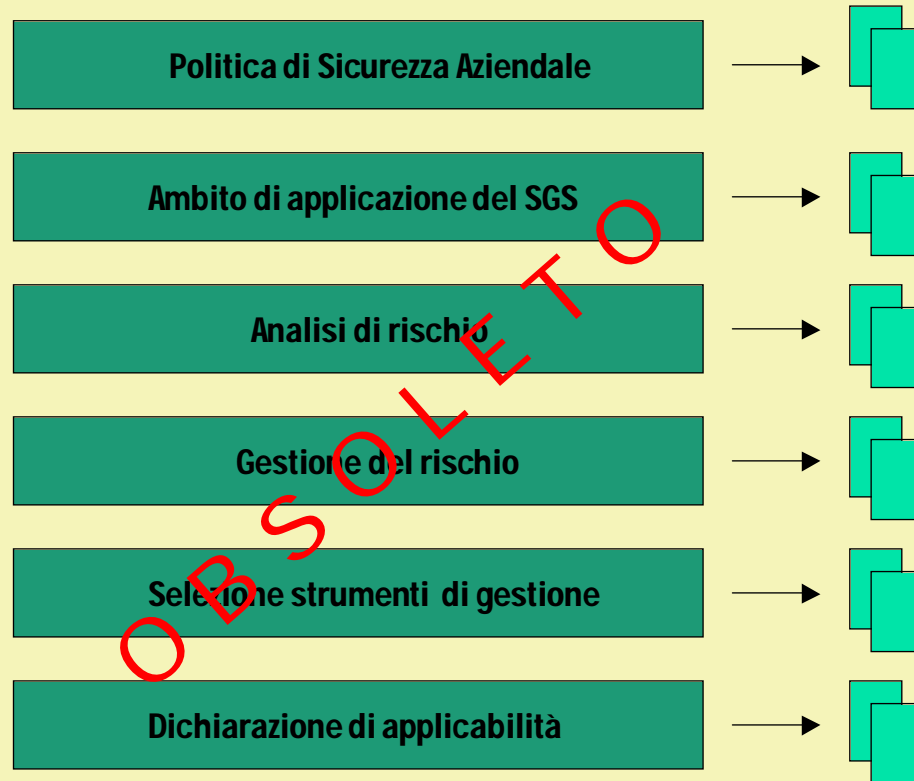
- Hanno per oggetto le organizzazioni (azienda o porzione di essa).
- BS7799 (1995, 1999, 2002) è configurata in due parti:
 - Parte 1: Code of Practice (regole di buon comportamento), non mandatoria, recepita nell'ISO/IEC 17799.
 - Parte 2: Requisiti normativi per il sistema di gestione, rimasta allo stato di norma britannica, ultima versione 2002.
- E' in definizione, a cura di SINCERT uno schema italiano per la certificazione rispetto ai contenuti di BS 7799 parte 2.



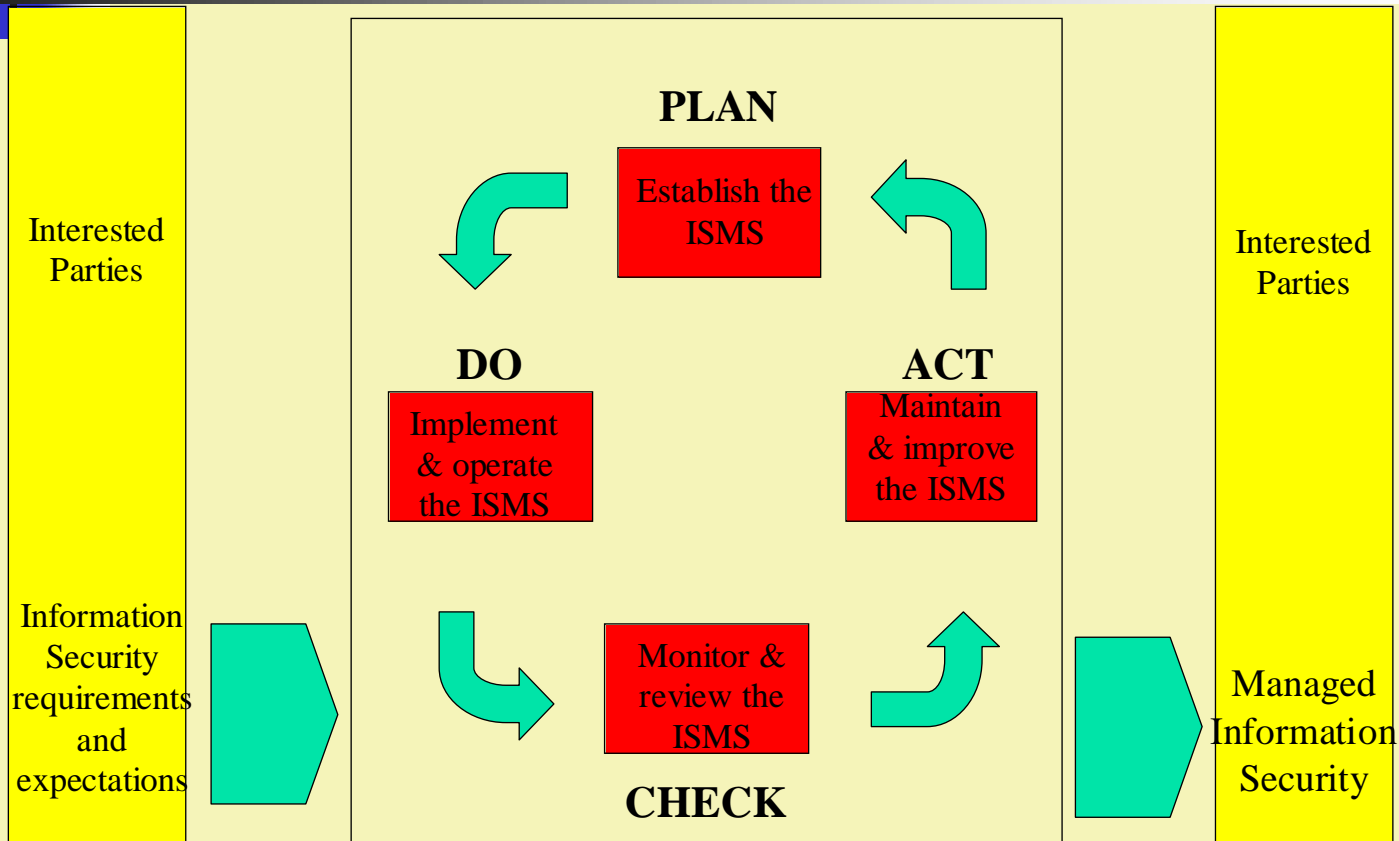
BS7799 parte 2 – Appendice A : Controls (strumenti di gestione) selezionabili

- Politiche di sicurezza
- Organizzazione per la sicurezza
- Classificazione e controllo degli “asset”
- Sicurezza del personale
- Sicurezza fisica e ambientale
- Gestione delle operazioni e delle comunicazioni
- Controllo degli accessi
- Sviluppo e manutenzione del sistema
- Gestione della continuità delle operazioni
- Conformità ai requisiti (di legge, delle policy, etc..)

BS7799 1999 part. 2: infrastruttura del SGSI (vecchia versione 1999)



BS 7799 part.2 2002 – modello di gestione del SGSI





BS 7799 part. 2 2002: PLAN

- Definizione dell'ambito di applicazione del SGSI.
- Definizione di una politica di sicurezza di alto livello
- Definizione di un approccio sistematico per l'analisi dei rischi
- Identificazione dei rischi
- Valutazione dei rischi
- Identificazione delle opzioni per il trattamento (eliminazione, cessione, riduzione) dei rischi
- Selezione delle contromisure per il controllo dei rischi
- Redazione della dichiarazione di applicabilità, comprendente l'esplicitazione delle ragioni che hanno portato alla selezione delle contromisure e alla non applicazione di misure indicate nell'appendice A della norma



BS 7799 part. 2 2002: DO

- Formulazione di un piano di trattamento dei rischi
- Implementazione del piano
- Implementazione delle contromisure selezionate
- Svolgimento di programmi di informazione e formazione
- Gestione delle operazioni connesse con la fase
- Gestione delle risorse connesse con la fase
- Implementazione di procedure e altre misure che assicurino la rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza



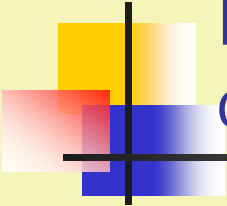
BS 7799 part. 2 2002: CHECK

- Esecuzione delle procedure di monitoraggio dell'SGSI
- Esecuzione di revisioni per l'accertamento del rischio residuo
- Conduzione di audit interni all'SGSI
- Esecuzione di review al massimo livello dirigenziale dell'SGSI
- Registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'SGSI



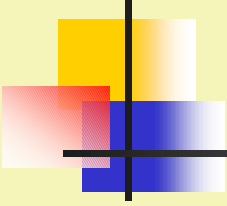
BS 7799 part. 2 2002: ACT

- Implementazioni delle azioni migliorative dell'SGSI identificate
- Implementazione delle azioni correttive e preventive
- Comunicazione dei risultati
- Verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base



BS7799 parte 2: che cosa è mandatorio e che cosa non lo è

- La lista dei “controls” (strumenti di gestione) presente nell’appendice A è per esplicita ammissione non esaustiva.
- Non è obbligatorio implementare tutti i “controls”. Per esplicita ammissione ogni caso specifico va valutato.
- Le quattro fasi della gestione dell’infrastruttura debbono essere compiute e se ne deve fornire l’evidenza.



Aspetti legati all'outsourcing

BS 7799-2:2002 – Appendice A

- Cap. A.4.2 La sicurezza negli accessi da Terze Parti
 - A.4.2.1 Identificazione dei rischi connessi con accessi delle T.P.
 - Il rischio connesso con l'accesso delle T.P. deve essere valutato e devono essere prese opportune contromisure.
 - A.4.2.2 Requisiti di sicurezza nei contratti con T.P.
 - Accordi relativi all'accesso di T.P. all'IS devono essere formalizzati in contratti contenenti opportuni requisiti di sicurezza
- Cap. A.4.3 Outsourcing
 - A.4.3.1 Requisiti di sicurezza nei contratti di outsourcing.
 - I requisiti di sicurezza di un'organizzazione che demandi ad altri la gestione ed il controllo di tutto o parte del suo sistema informativo, rete e/o installazioni desk-top, devono essere indirizzati in un contratto concordato tra le parti.



Aspetti legati all'outsourcing BS 7799 p.1

- La BS 7799 parte 1 (Code of Practice) è specifica al riguardo nel capitolo 4, dedicato all'organizzazione per la sicurezza.
 - 4.2.2 Requisiti di sicurezza nei contratti con terze parti che includano l'accesso al sistema informatico: vi vengono descritti gli aspetti che dovrebbero essere presenti, in particolare:
 - Politica generale di sicurezza
 - Protezione degli "asset"
 - Descrizione di ciascun servizio richiesto
 - Livello target di servizio e livelli non accettabili
 - Trasferimenti di staff qualora richiesti
 - Responsabilità relative dei due contraenti
 - Responsabilità indotte dall'applicazione delle leggi
 - Proprietà intellettuale
 - Accordi sul controllo degli accessi
 - Definizione di criteri verificabili di performance



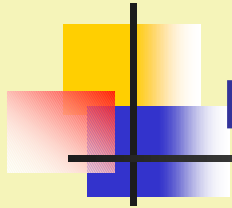
Aspetti legati all'outsourcing BS 7799 p.1

- Cap. 4 Organizzazione della sicurezza
 - 4.2.2 Requisiti di sicurezza nei contratti con T.P.(continua)
 - Diritti di verifica e di revoca di attività degli utenti
 - Diritti di verifica di requisiti contrattuali o di affidarli a terze parti
 - Definizione di un processo di escalation per la risoluzione di problemi
 - Definizione di responsabilità relative allo h/w e al s/w
 - Definizione della struttura di riporto
 - Definizione del processo di gestione dei cambiamenti
 - Eventuali requisiti di protezione fisica
 - Training per gli utenti e l'amministratore di sistema per la sicurezza
 - Modalità di assicurare protezione da "malicious software"
 - Modalità per riportare, notificare e investigare incidenti
 - Gestione dei subfornitori



Aspetti legati all'outsourcing BS 7799 p.1

- Capitolo 4 Organizzazione della sicurezza
 - 4.3 Outsourcing: Nel caso in cui la responsabilità dell'IS venga affidata a terzi, oltre ai punti citati al par. 4.2.2, dovrebbero essere considerati nel contratto:
 - Come i requisiti di legge vengono rispettati
 - Quali accordi per assicurarsi che tutte le parti coinvolte (collaboratori, subcontractors) siano a conoscenza delle proprie responsabilità
 - Come mantenere e testare la confidenzialità e l'integrità dei dati aziendali
 - Quali misure fisiche e logiche verranno adottate per restringere l'accesso agli operatori autorizzati
 - Come sarà assicurata la continuità delle operazioni in caso di disastri
 - Quale livello di protezione fisica assicurare all'h/w parte del servizio
 - Il diritto di verificare il rispetto dei requisiti contrattuali



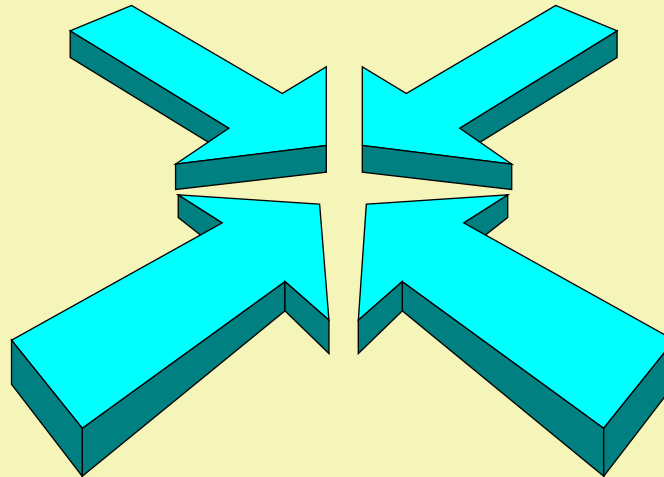
Punti di forza della BS7799

- Impone un'infrastruttura organizzativa che si renda responsabile della sicurezza delle informazioni in tutti i suoi aspetti.
- Impone la continuità nella gestione della sicurezza delle informazioni.
- **Rende possibile un linguaggio comune tra Aziende diverse .**



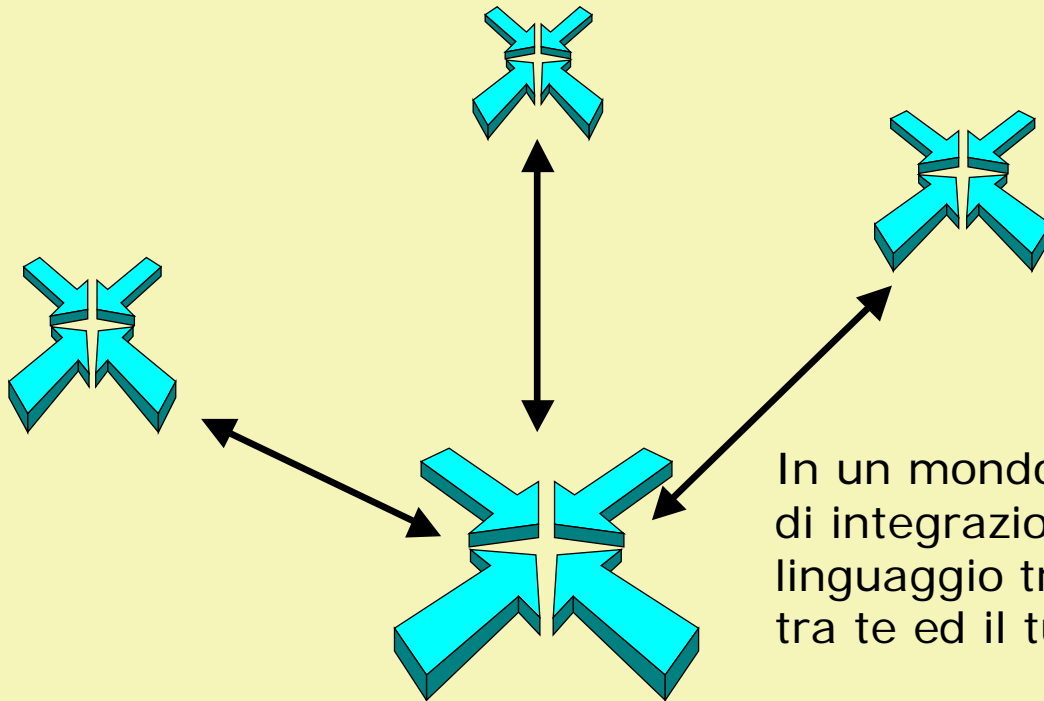
Analogie con la genesi della serie ISO 9000

Il sistema di gestione della Qualità



La *struttura organizzativa*, le *procedure*, i processi e le risorse necessarie ad attuare la gestione per la qualità.

Analogie con la genesi della serie ISO 9000



In un mondo fatto sempre di più di integrazione, lo stesso linguaggio tra te ed il tuo cliente, tra te ed il tuo fornitore.



Quali garanzie per il cliente?

- La norma BS 7799 parte 1 (code of practice) stabilisce alcuni criteri di buon governo della sicurezza.
- La norma BS 7799 parte 2 (utilizzabile per la certificazione) stabilisce alcuni passi formali per l'implementazione di un SGSI.
- Tra i passi formali (obbligatorie) è inclusa la produzione di
 - Un documento di Politiche di Sicurezza
 - Un documento di analisi di rischio
 - Un documento che stabilisca l'applicazione ragionata di una serie di contromisure (Dichiarazione di applicabilità).
- Esistono i presupposti per un linguaggio comune



Quali garanzie per il cliente?

- La decisione del fornitore di accedere ad un processo di certificazione BS7799 è indicazione della volontà della Direzione di curare gli aspetti di sicurezza.
- L'ottenimento della certificazione è indicativo del fatto che esistono le evidenze della conclusione dei sei passi che costituiscono l'infrastruttura di gestione della sicurezza.
- Esistono quindi documenti che potrebbero essere consultati.
- La varietà delle situazioni (campo di applicazione della norma e oggetto del certificato, selezione libera dei "controls", etc..) indurrebbe a considerare le differenze.



Conclusione

- I contenuti della norma sono condivisibili e il raggiungimento dei requisiti impone alle Aziende uno sforzo notevole.
- Documenti “semipubblici” come le politiche di sicurezza o la dichiarazione di applicabilità aiutano nella fase di procurement.
- Sicuramente una certificazione facilita il raggiungimento di un buon contratto sottoscrivibile da entrambe le parti.
- Il dettaglio dei requisiti per il cliente in fase contrattuale (che il fornitore conosce, essendo certificato) è una guida per un buon contratto.