Criteri di valutazione e certificazione della sicurezza delle informazioni

Cesare Gallotti - Lead Auditor, CISA

Milano, 16 maggio 2003

AGENDA

- Definizioni
- Valutazione dei prodotti
- Valutazione dello sviluppo del sw
- Valutazione dell'organizzazione per la sicurezza
- Percorso di certificazione BS 7799

- **Punti chiave:**
  - importanza dell'organizzazione
  - scopo di certificazione
  - approccio per processi
  - indicatori di processo

DEFINIZIONI

INFORMAZIONE - DEFINIZIONE

- L'*informazione* è un'aggregazione ed elaborazione di *dati elementari* di interesse per uno o più *destinatari* importante per il processo decisionale presente e futuro.

- L'aggregazione e l'elaborazione sono affidate al *sistema informativo* (ISM).

- Per l'ISO 9000:2000:
  - *informazione:* dati significativi
  - *documento* informazioni con il loro mezzo di supporto (IT e/o non-IT).

SICUREZZA – DEFINIZIONE

- Per *sicurezza delle informazioni* si intende l'attività volta a definire, conseguire e mantenere le seguenti proprietà:

  riservatezza: capacità di non rendere le informazioni disponibili a individui non autorizzati;

  integrità: impossibilità di alterare o distruggere le informazioni da parte di individui o entità non autorizzati;

  disponibilità: garanzia di potere accedere alle informazioni entro i tempi previsti e di utilizzarle da chi ne è autorizzato;

  autenticità: garanzia della provenienza delle informazioni;

  non ripudio: protezione da falsa negazione di ricezione, trasmissione, creazione, trasporto, consegna, ricevuta.

COME GARANTIRE LA SICUREZZA?

- La sicurezza si garantisce attraverso processi organizzativi e prodotti adeguati.
- Buoni processi organizzativi portano a scegliere ed usare buoni prodotti.
- Non è vero l'inverso.

L'ORGANIZZAZIONE E' IMPORTANTE PER LA SICUREZZA DELLE INFORMAZIONI?

- Controllo
- Pianificazione
- Assunzione di responsabilità
- Verifiche
- Riesami da parte degli utenti e della Direzione

Sistema di gestione

⇒ ?

- Creatività
- Alta specializzazione
- Continuo aggiornamento
- Cultura basata sulla diffusione delle conoscenze

Sistema di gestione delle informazioni (soprattutto IT)

VALUTAZIONE DEI PRODOTTI

STANDARD DI RIFERIMENTO

- 1983 TCSEC (Trusted Computer Security Evaluation Criteria)
- 1991 ITSEC (IT Security Evaluation Criteria)
- 1996 Common Criteria (ISO 15408)
- 2001 ISO 9126 (SW Quality)

COMMON CRITERIA

- Rivolto a sistemi e prodotti IT prevede 7 livelli crescenti (EAL 1 … EAL 7) di valutazione della correttezza.
- Simile a ITSEC, sviluppato dai Paesi autori di questo con Canada e Stati Uniti.
- Recepita dall'ISO come ISO 15408.
- http:\\www.commoncriteria.org

COMMON CRITERIA: DEFINIZIONI

- TOE (Target of Evaluation): oggetto di valutazione
- Funzionalità: requisiti di sicurezza del TOE;
  - Obiettivo: perché si vuole una funzionalità
  - Funzione di sicurezza: quale funzionalità è prevista
  - Meccanismo: come la funzionalità è realizzata
- Correttezza: quanto “bene” sono sviluppati i meccanismi
- Il Protection Profile è l’espressione di requisiti di sicurezza per una famiglia di TOE, coerenti con gli obiettivi di sicurezza stabiliti
- Il Security Target è l’espressione di requisiti di sicurezza per uno specifico TOE, più dettagliati rispetto a quelli espressi dal PP

CC: LIVELLI DI VALUTAZIONE

- La valutazione della funzionalità (Security Target) può avere risultato positivo o negativo (1, 0) e stabilisce se le funzioni di sicurezza soddisfano gli obiettivi.
- La valutazione della correttezza varia da 1 a 7 e dipende dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo.
- Più la documentazione è estesa e formale, più si ha la garanzia che il processo di sviluppo è stato rigoroso.
- Il livello EAL1 non richiede la valutazione della documentazione utilizzata e dell'ambiente di sviluppo. Gli altri sì, e richiedono la collaborazione degli sviluppatori.

COMMON CRITERIA: UN CASO

- Nell'ottobre 2002, Windows 2000 è stato certificato a livello EAL 4+ dei Common Criteria rispetto al Protection Profile *Controlled Access Protection Profile* (CAPP).

- I prodotti conformi al CAPP dispongono di un controllo degli accessi capace di far rispettare le limitazioni di accesso tra utenti (!!!) e data objects.

- Sicuro… sì, ma non da attacchi dei "blackhats"!

CC: DUE LEZIONI GENERALI

- Per i clienti: il termine “certificazione” (di qualità, di sicurezza) da solo non dice nulla: è sempre necessario verificare a cosa si riferisce.

- Per chi si certifica: il successo di un processo di certificazione dipende anche da *cosa* si certifica e da quali sono i suoi *confini*. In termini di certificazione BS 7799 e ISO 9001 ci si riferisce allo *scopo di certificazione.*

ISO 9126

Valutazione della qualità del software, sui requisiti:

- *funzionalità:* funzioni che soddisfano i bisogni per i quali il software è progettato;
- *affidabilità:* capacità del software di mantenere le prestazioni entro le condizioni indicate;
- *usabilità:* sforzo richiesto agli utenti per l'utilizzo;
- *efficienza:* relazione tra prestazioni del software e risorse impegnate;
- *manutenibilità:* lavoro occorrente per apportare successive modifiche;
- *portabilità:* possibilità di trasferire il software da un ambiente informatico a un altro.

- All'ISO 9126 è collegato l'ISO/IEC 14598 relativo alle attività di test.

VALUTAZIONE DELLO SVILUPPO DEL SW

STANDARD DI RIFERIMENTO

- 1993: SW CMM (Modello di maturità)
- 1995: ISO/IEC 12207 (SW life cycle)
- 1996: SSE-CMM (Security CMM)
- 1997: ISO 9000-3
- 1998: ISO/IEC 14598 (SW Evaluation)
- 1999: ISO/IEC 14764 (SW Maintenance)
- 2002: ISO/IEC 15288 (System life cycle)

SW CAPABILITY MATURITY MODEL

- Sviluppato dalla SEI CMU su richiesta del governo USA per valutare i fornitori software.

- Cinque livelli di maturità per l'azienda su capacità di gestione dei progetti e loro miglioramento:
  - *iniziale:* il successo dei progetti dipende dall'impegno di alcuni;
  - *ripetibile:* è definita una disciplina su pianificazione, calcolo dei costi e supervisione dei progetti, per ripeterne i successi;
  - *definito:* vi è uno standard aziendale per la gestione dello sviluppo;
  - *gestito:* controlli quantitativi della gestione dei processi di sviluppo del software;
  - *ottimizzato:* strategie di miglioramento progressivo e continuo dei progetti di sviluppo.

- Il Technical Report dell'ISO 15504:1998 (detto anche SPICE) riprende i concetti del CMM.

VALUTAZIONE DELL'ORGANIZZAZIONE DELLA SICUREZZA

STANDARD DI RIFERIMENTO

- 1987: ISO 9000
- 1995: BS 7799 parte 1
- 1996: Cobit
- 1996: GMITS (ISO TR 13335)
- 1998: BS 7799 parte 2

BS 7799-1: 1999 (ISO 17799)

- Nato dalla collaborazione tra aziende e Governo Inglese.
- E' una lista di "controlli" di sicurezza soprattutto di tipo gestionale (organizzativo) intesa come "best practice": non tutto va realizzato e può essere un valido spunto per le attività di sicurezza.
- È stata modificata nel 1999 per adeguarla all'evoluzione tecnologica
- È stata recepita dall'ISO come ISO 17799 nel 2000.
- Suggerisce degli *Starting Points* "normativi" (sui dati personali, registrazioni, diritto d'autore) e organizzativi (Politiche di Sicurezza delle informazioni, ruoli e responsabilità, formazione e sensibilizzazione, gestione degli incidenti, piano di continuità).

I CAPITOLI DEL BS 7799-1:1999

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

BS 7799 – 2: 2002

- Indica i requisiti per la certificazione di un sistema di gestione per la sicurezza delle informazioni (capitoli 1, ..., 7).
- È stata rivista nel 2002 per allinearsi alla ISO 9001:2000 ed essere approvata dall'ISO.
- Non esiste certificazione ISO17799.

APPROCCIO PER PROCESSI

- Il BS 7799 promuove l'approccio per processi per pianificare, realizzare, mantenere in opera, controllare e migliorare l'efficacia dell'ISMS.

- Processo è un'attività che usa risorse e viene gestita per trasformare elementi in entrata in elementi in uscita.

- Questo approccio implica l'identificazione dei processi, delle loro l'interrelazioni e modalità di gestione.

- L'approccio per processi è collegato al principio di "approccio sistemico":
  - identificare, capire e gestire (come un sistema) processi relativi alla sicurezza delle informazioni tra loro correlati, contribuendo all'efficacia ed efficienza di un'organizzazione nel conseguire i propri obiettivi.

ALCUNI PROCESSI PER LA SICUREZZA DELLE INFORMAZIONI

- gestire gli accessi e le autorizzazioni in ambito informatico
- gestire gli accessi e le autorizzazioni in ambito non informatico
- sviluppare le applicazioni software
- sviluppare e seguire le operazioni dei sistemi in esercizio (hardware e software)
- sviluppare e seguire le operazioni della rete
- assistere gli utenti
- mantenere gli impianti (riscaldamento, condizionamento, antincendio)
- sviluppare e seguire le operazioni dei sistemi di sicurezza fisica
- effettuare verifiche del sistema informativo
- sviluppare il Business Continuity Plan
- gestire i fornitori e l'approvvigionamento
- gestire il personale

COSA DESCRIVERE

- risorse (chi lo fa, chi ne è responsabile)
- input (da chi si ricevono indicazioni)
- attività o fasi
- output (il risultato)
- interdipendenze tra attività (anche all'esterno con clienti, fornitori, partner)
- controllo di gestione (indicatori di processo)

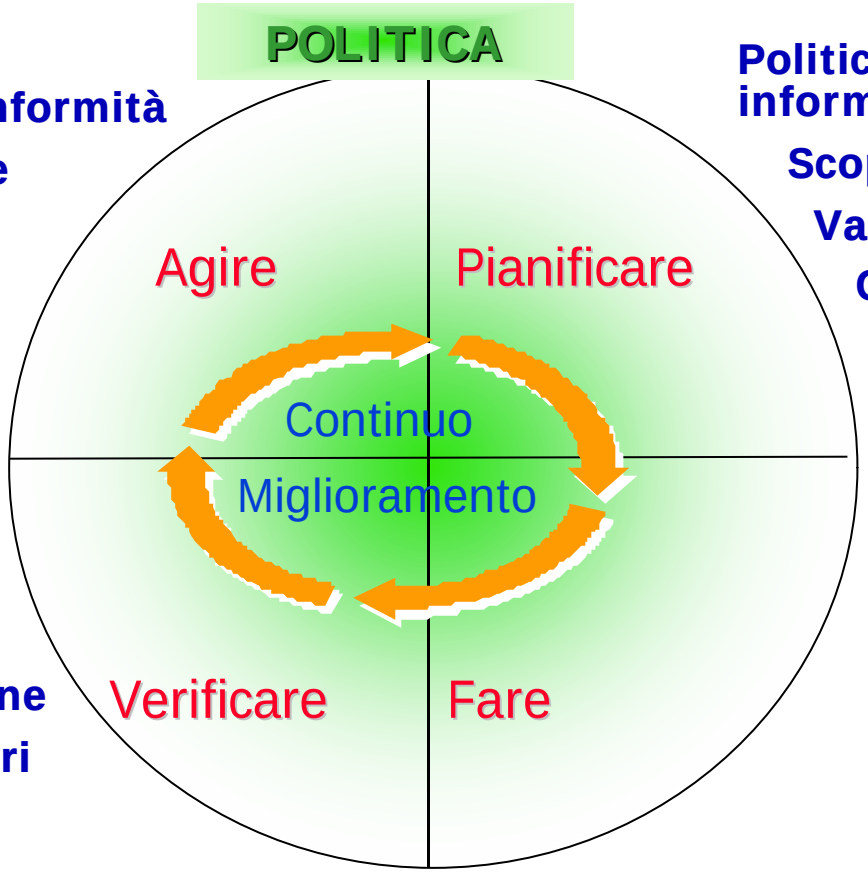
UN ESEMPIO

- Gestire le autorizzazioni
  - lo esegue l'amministratore di sistema
  - riceve indicazioni da HR e dal Responsabile di business
  - mantiene un registro delle richieste e uno delle eccezioni
  - riferisce al responsabile della sicurezza, ai responsabili di business, all'auditor interno.

UN ESEMPIO PIU' COMPLESSO

- Sviluppare sistemi software:
  - i resp. sviluppo ricevono i requisiti dai responsabili di business
  - gli analisti elaborano le specifiche
  - resp. sviluppo e analisti riesaminano le specifiche con i responsabili di business, della sicurezza, dei sistemi di esercizio, …
  - pianificano le fasi delle attività, indicano le scadenze, stabiliscono le risorse necessarie
  - i programmatori sviluppano l'applicazione
  - i responsabili dello sviluppo, gli analisti software e i programmatori riesaminano lo stato di avanzamento dei lavori ed i problemi
  - al termine dello sviluppo, i responsabili dello sviluppo, gli analisti e i programmatori revisionano il tutto
  - i programmatori e gli analisti eseguono i test negli ambienti di test
  - i programmatori e gli analisti riesaminano quanto realizzato con i responsabili di business, della sicurezza, dei sistemi di esercizio, …
  - i responsabili dello sviluppo richiedono ai responsabili della gestione dei sistemi di esercizio di installare su tali sistemi l'applicazione

PLAN DO CHECK ACT



Gestione non conformità
Azioni preventive
Azioni correttive
Manutenzione
Miglioramento

Politiche per la sicurezza delle informazioni
Scopo-dominio dell' ISMS
Valutazione del rischio
Gestione del rischio

Controlli tecnici
Visite ispettive
Riesame Direzione
Analisi indicatori di processo

Allocare le riscorse
Redigere la documentazione
Realizzare le misure di:
- **Sicurezza del Personale**
- **Sicurezza fisica**
- **Gestione comunicazioni,**
- **Controllo accessi**
- **Sviluppo e manutenzione**
- **Continuità del business**

PIANIFICARE

- Politica per la sicurezza delle informazioni
  - Responsabilità
- Scopo
- Identificazione e valutazione del rischio (risk identification and assessment)
- Piano di gestione del rischio (risk treatment)

PIANIFICARE 1 - POLITICHE

- Le politiche devono riportare:
  - una definizione di sicurezza delle informazioni,
  - uno schema per stabilire gli obiettivi e i principi da seguire,
  - un'indicazione per dare un orientamento alle attività e chiarire l'impegno della direzione,
  - i requisiti di business e i vincoli legali e contrattuali da rispettare,
  - definizione delle responsabilità.
- Per l'ampiezza, è possibile fare riferimento ad un *manuale per la sicurezza*, indicando come *politiche* solo i principi di base (anche per uniformità con l'ISO 9001).
- Esse sono uno strumento per evidenziare l'impegno della Direzione nella sicurezza delle informazioni.

PIANIFICARE 1A - RESPONSABILITA’

- Management information security forum
- Information security co-ordination
- Responsabili delle risorse (asset, informazioni)
- Amministratori di sistema
- Responsabili di processo
- Responsabile della sicurezza delle informazioni
- Responsabili per l’ampliamento del sistema informativo
- Auditor (interno, esterno)
- Custode delle password

PIANIFICARE 2 - SCOPO

- È il perimetro delle attività.
- Vanno identificate le caratteristiche di business e dell'organizzazione, le risorse fisiche, IT, non IT, umane e procedurali entro le quali valutare l'ISMS.
- Passo fondamentale per le attività di certificazione, perché in esso si deduce l'ampiezza delle attività.
- Vanno definite le relazioni con l'esterno: clienti, fornitori, partner, case madri, ...

PIANIFICARE 3 - IDENTIFICAZIONE E VALUTAZIONE DEL RISCHIO

- L'approccio per la valutazione del rischio deve basarsi su un metodo (ripetibile!) e identificare i livelli di rischio accettabili.
- Vanno documentati i seguenti dettagli:
  - valutazione delle risorse
  - vincoli (legali, contrattuali, ...)
  - minacce e vulnerabilità
  - valutazione delle minacce e degli impatti
  - calcolo del rischio e identificazione di quello residuale
- La ripetibilità del metodo si basa sulla descrizione delle scale di valutazione utilizzate.
- Questa fase serve anche per il Business Continuity Plan (di cui fa parte il DRP).

PIANIFICARE 4 - GESTIONE DEL RISCHIO

- Opzioni di trattamento del rischio: contrastare, trasferire, evitare, accettare.
- Selezionare i controlli, giustificandoli sulla base della valutazione del rischio e delle opzioni di trattamento scelte.
- Preparare una dichiarazione di applicabilità dei controlli scelti (Statement of Applicabiliy).
- Ottenere l'approvazione del management sul rischio accettato e per l'implementazione dei controlli (riesame).
- Pianificare le attività: azioni del management, responsabilità e priorità.

DICHIARAZIONE DI APPLICABILITA’

- Riferimenti a standard aziendali
- Dichiarazioni di adeguatezza o meno ai controlli BS
- Dettagli specifici dell’azienda rispetto ai controlli dello standard.
- È d’aiuto all’auditor perché così sa cosa aspettarsi.
- Serve come riferimento negli audit successivi.
- Può essere d’aiuto nella formazione del personale.
- Serve da riferimento anche per altri documenti più dettagliati
- Va approvata dalla Direzione.

FARE

- Allocare risorse
  - formazione e sensibilizzazione
  - gestione dei documenti
  - documenti “obbligatori”
- Gestire il rischio (risk treatment)

FARE 1 - RISORSE

- Per la realizzazione del piano vanno considerate le risorse necessarie in termini di personale, tempo e denaro.
- Devono anche essere allocate le risorse per:
  - garantire l'efficacia dell'ISMS,
  - seguire l'evoluzione dei vincoli legali e contrattuali,
  - garantire la correttezza dei controlli applicati,
  - condurre revisioni e reagire ai risultati,
  - migliorare l'efficacia dell'ISMS.

FARE 1a - FORMAZIONE

- Il personale, con responsabilità relative alla sicurezza, deve essere competente e consapevole (formato e sensibilizzato).
- Vanno *definite* le competenze necessarie per il personale coinvolto nell'ISMS.
- Deve essere valutata l'efficacia delle attività di formazione.
- Il personale deve essere sensibilizzato.

FARE 1b - DOCUMENTAZIONE

- Procedura documentata per la gestione dei documenti: approvazione, riesame, aggiornamento e riapprovazione, identificazione delle modifiche e revisioni, disponibilità delle versioni più recenti, garanzia di leggibilità e identificazione, identificazione dei documenti esterni, controllo della distribuzione, gestione documenti obsoleti.
- Procedura documentata per la gestione delle registrazioni: leggibilità, identificazione, reperibilità, conservazione, protezione, tempo di conservazione e distruzione.

FARE 1c – DOCUMENTI OBBLIGATORI

- Politica e obiettivi
- Scopo, procedure e controlli
- Valutazione del rischio
- Gestione del rischio
- Procedure documentate necessarie
- Registrazioni richieste dal BS.
- SoA.

FARE 2 – GESTIRE IL RISCHIO

- Deve essere realizzato il piano delle attività:
  - Realizzare i programmi di formazione e sensibilizzazione.
  - Gestire le operazioni.
  - Gestire le risorse.
  - Realizzare procedure (non necessariamente documentate) e altri controlli volti alla rilevazione e risposta agli incidenti.

VERIFICARE

- Controlli tecnici:
  - continui
  - allarmi
  - confronto con altre esperienze
- Visite ispettive interne
- Riesame della Direzione
- Indicatori di processo

VERIFICARE 1- CONTROLLI TECNICI

- Controlli tecnici possono essere
  - Continui: riconciliazioni, quadrature, controlli incrociati. Anche: risolvere reclami dei clienti.
  - Allarmi: da IDS, programmi di monitoraggio, rilevatori presenze, segnalazioni di incidenti.
  - Confronti: mailing list (cert cc, bugtraq), conferenze, periodici, articoli, Forze dell'ordine

VERIFICARE 2 - VISITE ISPETTIVE

- Vanno condotte visite ispettive interne periodiche secondo criteri di pianificazione, conduzione e riporto definiti in una procedura documentata.
- Va considerato: se la politica è adeguata, la metodologia di valutazione del rischio è adeguata, le procedure sono seguite e incontrano gli obiettivi, i controlli tecnici sono in ordine.
- Devono basarsi su evidenze oggettive.
- Non devono avere carattere punitivo.

VERIFICARE 3 - RIESAME DELLA DIREZIONE

- Va condotto regolarmente (almeno una volta all'anno) un riesame della direzione dell'ISMS. Deve essere documentato e con opportuni elementi in entrata e in uscita.
- Devono essere identificate le aree di miglioramento, deve essere posta attenzione sull'evoluzione delle tecnologie, delle attività aziendali e di possibili nuove minacce e vulnerabilità.
- Sulla base di queste analisi vanno rivisti i criteri di accettabilità del rischio.

VERIFICARE 4 - INDICATORI DI PROCESSO

- La norma (4.2.3.a.3) stabilisce che è necessario monitorare le procedure e i controlli al fine di consentire alla direzione di determinare se le attività delegate ad altri sono condotte come previsto (“obiettivi” oggettivi e misurabili).
- L’ISO 9001 (8.2.3) chiede di “adottare adeguati metodi per monitorare e, ove applicabile, misurare i processi del sistema di gestione [...]. Questi metodi devono dimostrare la capacità dei processi ad ottenere i risultati pianificati. Qualora tali risultati non siano raggiunti, devono essere adottate correzioni ed intraprese azioni correttive, come opportuno [...].

INDICATORI (piccola digressione 1)

- Gli “indicatori di processo” dell’ISO 9001:2000 rappresentano un grosso cambio di direzione rispetto all’ISO 9001:1994 tanto che il tempo di transizione tra le due norme è stato stabilito di tre anni.
- L’importanza dell’innovazione si riflette anche tra BS 7799:1999 e BS 7799:2002.
- Gli indicatori di processo riguardano le attività di carattere gestionale (non tecnico per le analisi del rischio quantitative!)

INDICATORI (piccola digressione 2)

- Gli indicatori di processo devono essere utili al personale operativo perché possa vedere quanto bene lavora.
- Gli indicatori di processo devono essere utili alla direzione per stabilire se il processo funziona (non per valutare il personale).
- L'analisi degli indicatori di processo può permettere la soluzione dei problemi prima che si verifichino incidenti o non conformità.

INDICATORI (piccola digressione 3a)

Processo	Indicatori
Gestire gli accessi e le autorizzazioni in ambito informatico	?numero medio di eccezioni al controllo degli accessi ?numero di variazioni dei privilegi affettuate ogni giorno
Gestire gli accessi e le autorizzazioni in ambito non informatico	?numero medio di eccezioni al controllo degli accessi ?numero di visitatori al giorno
Sviluppare i applicazioni software	?numero di incidenti rilevati ogni settimana ?numero di malfunzionamenti al software rilevate ogni mese ?tempo medio di risposta agli incidenti ?numero di modifiche correttive o evolutive apportate ad ogni applicazione ogni mese ?rapporto pianificato/effettivo sui tempi di progetto di sviluppo
Sviluppare e seguire le operazioni dei sistemi in esercizio (hardware e software)	?numero di incidenti rilevati ogni settimana ?numero di malfunzionamenti ai sistemi rilevate ogni mese ?tempo medio di risposta agli incidenti ?numero di modifiche correttive o evolutive apportate ai sistemi ogni mese ?rapporto pianificato/effettivo sui tempi di progetto di sviluppo ?tempo di indisponibilità dei sistemi al semestre

INDICATORI (piccola digressione 3b)

Processo	Indicatori
Sviluppare e seguire le operazioni della rete	?numero di incidenti rilevati ogni settimana ?numero di malfunzionamenti della rete rilevate ogni mese ?tempo medio di risposta agli incidenti ?numero di modifiche correttive o evolutive apportate alla rete ogni mese ?rapporto pianificato/effettivo sui tempi di progetto di sviluppo ?tempo di indisponibilità della rete al semestre
Assistere gli utenti	?tempo medio di risposta dell'help desk ?numero di problemi che hanno richiesto il coinvolgimento di personale esterno all'help desk ogni mese
Mantenere gli impianti (riscaldamento, condizionamento, antincendio)	?costo annuo delle manutenzioni ordinarie e straordinarie
Sviluppare e seguire le operazioni dei sistemi di sicurezza fisica	?numero di incidenti rilevati ogni settimana
Effettuare verifiche del sistema informativo	?rapporto tra miglioramenti pianificati/realizzati ogni anno
Sviluppare il Business Continuity Plan	?andamento dei test effettuati
Gestire i fornitori	?rispetto dei tempi di consegna (ritardo medio) ?qualità del prodotto (difetti) fornito o del servizio (adeguatezza) erogato

AGIRE

L’azienda deve migliorare l’efficacia dell’ISMS attraverso politiche, obiettivi, audit, analisi degli eventi, azioni correttive e preventive, riesami della direzione.

- Non conformità
- Azioni correttive e preventive
- Manuntenzione e miglioramento

AGIRE 1 – NON CONFORMITA’

- Una non conformità è:
  - l’assenza di uno o più requisiti dell’ISMS,
  - una situazione che pone il dubbio sull’efficacia dell’ISMS rispetto agli obiettivi.

- I controlli devono evidenziare un’area di non conformità e vanno poste in atto attività per risolvere il problema.

AGIRE 2 - AZIONI CORRETTIVE E PREVENTIVE

- Devono essere previste procedure documentate per la conduzione delle azioni correttive e preventive.
- Devono eliminare la causa di una [possibile] non conformità.
- Le attività devono essere riviste per valutarne l'efficacia.

AGIRE 3 – MANUTENZIONE E MIGLIORAMENTO

- Realizzare i miglioramenti identificati
- Intraprendere le appropriate azioni correttive e preventive. Applicare le lezioni da esperienze interne ed esterne.
- Riesaminare risultati e azioni con gli interessati
- Assicurarsi che i miglioramenti raggiungano gli obiettivi.
- Eventualmente riprendere dall'attività di pianificazione.

PERCORSO DI CERTIFICAZIONE

COS'E' LA CERTIFICAZIONE

- Per certificazione si intende la verifica ed attestazione, da parte di enti terzi indipendenti e competenti (*organismi di certificazione*), della conformità ai requisiti previsti dalla normativa di riferimento.

- Le attività di certificazione, oltre ad essere utili in termini di immagine, rappresentano per l'azienda anche un'opportunità di confrontarsi con un organismo esterno e raccogliere spunti per eventuali miglioramenti.

COME FUNZIONA (1/3)

- In linea di principio un certificato può essere rilasciato da chiunque, anche senza l'opportuna indipendenza e qualifica. Per questo sono in atto procedure di *accreditamento* per dimostrare la correttezza, trasparenza e professionalità dell'attività dell'organismo di certificazione.
- L’accreditamento avviene su specifici standard e settori industriali ed ogni organismo può essere accreditato per più standard e settori.

COME FUNZIONA (2/3)

- In Italia il compito di accreditare gli organismi di certificazione è affidato al Sincert.
- L'accreditamento avviene su specifici schemi emanati dall'ISO (guide 62) o dal CEN (EN 45012) o da altri basati sui sistemi di gestione qualità.
- Per il BS 7799 sono di riferimento le Guidelines for Certification- EA 7/03 (del 2000).
- Il compito dell'organismo di accreditamento è anche quello di uniformare l'approccio di valutazione degli organismi di certificazione. In Europa, il lavoro degli enti di accreditamento viene coordinato dall'EA.

COME FUNZIONA (3/3)

- Il sistema di accreditamento e certificazione ha come protagonisti quattro gruppi di attori:
  - gli enti normatori, come l'ISO, il BSI (British Standard Institute) o l'UNI (Ente Nazionale Italiano di Unificazione), che emettono standard;
  - gli enti di accreditamento; in Italia sono il Sincert (per gli organismi di certificazione), il Sinal (per i laboratori) e il Sit (per i centri taratura);
  - i soggetti accreditati, ossia organismi di certificazione, laboratori e centri di taratura;
  - i consumatori finali, intesi come aziende ed imprese.

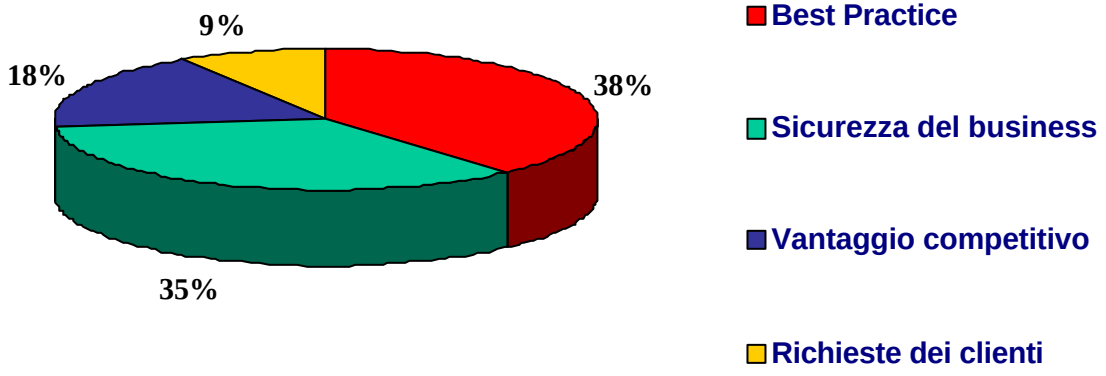
CERTIFICATI BS 7799
ACCREDITATI AL 31/12/2002

	Sum		Sum
Australia	1	Italy	3
Austria	2	Japan	17
Brazil	2	Korea	9
China	4	Malaysia	1
Egypt	1	Netherlands	0
Finland	8	Norway	6
Germany	8	Singapore	7
Greece	2	Spain	1
Hong Kong	6	Sweden	3
Hungary	2	Taiwan	3
Iceland	1	UAE	1
India	9	UK	77
Ireland	3	USA	2

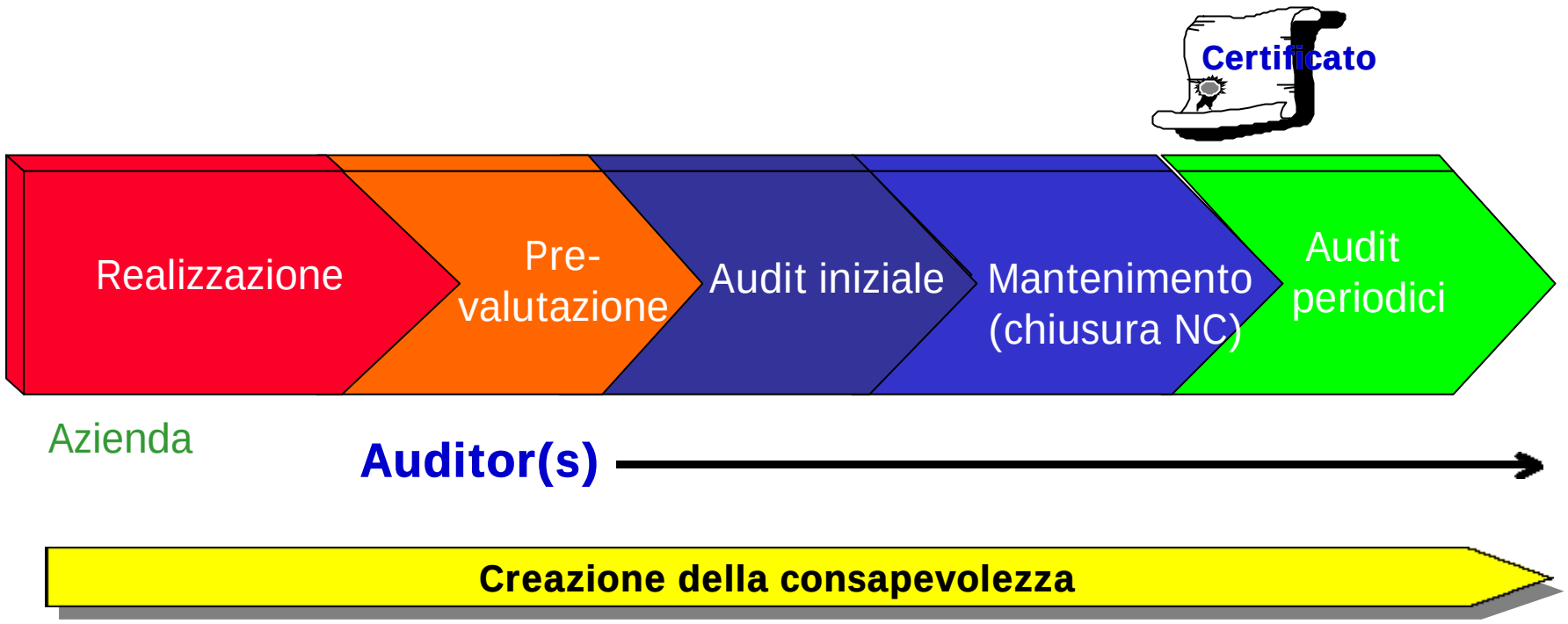
Totale: 179 (da www.xisec.com)

LE RAGIONI PER RICHIEDERE LA CERTIFICAZIONE

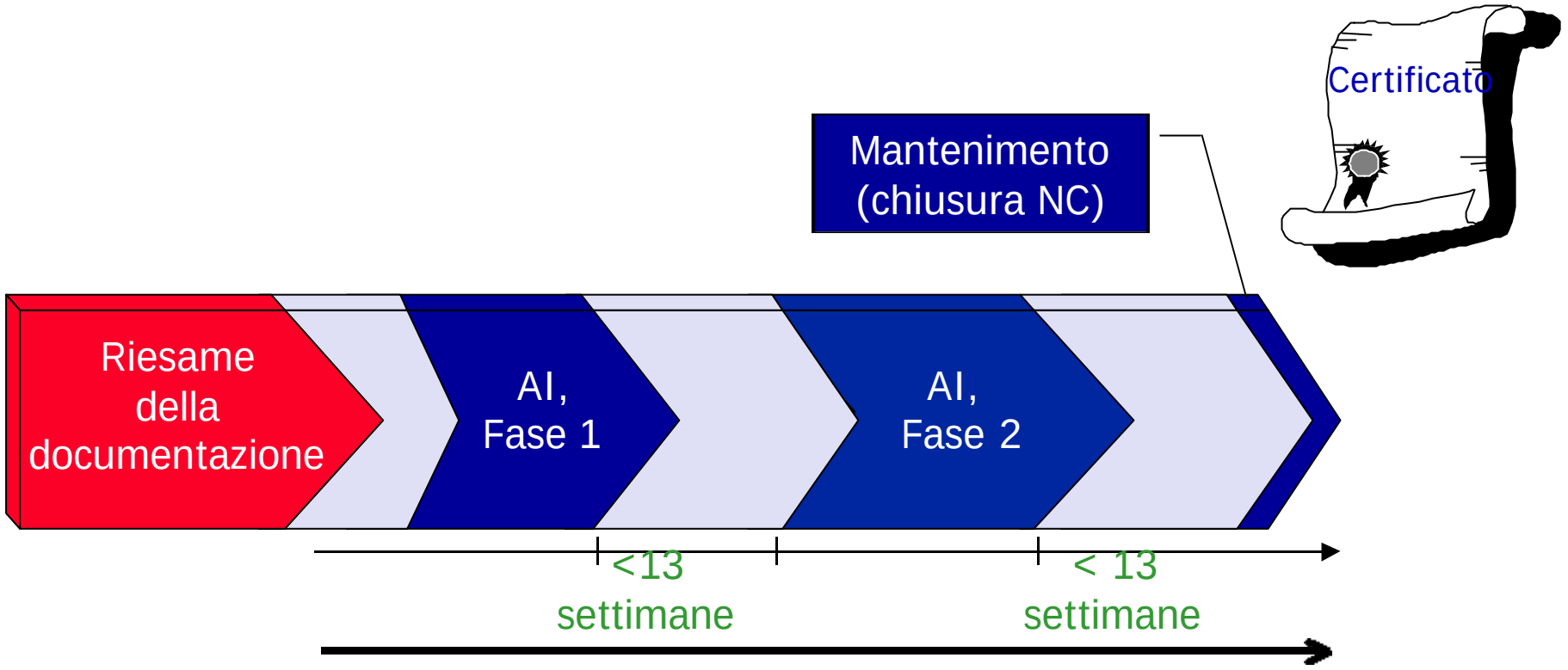
- Accresce la consapevolezza sulla sicurezza
- Individua i beni critici con l'Analisi del rischio
- Facilita il miglioramento continuo e sviluppi per l'impresa.
- Fornisce fiducia all'interno e all'esterno
- Arricchisce la conoscenza della direzione sulla sicurezza
- Assicura la conoscenza nell'azienda



QUANDO AVVIENE LA CERTIFICAZIONE?



AUDIT INIZIALE

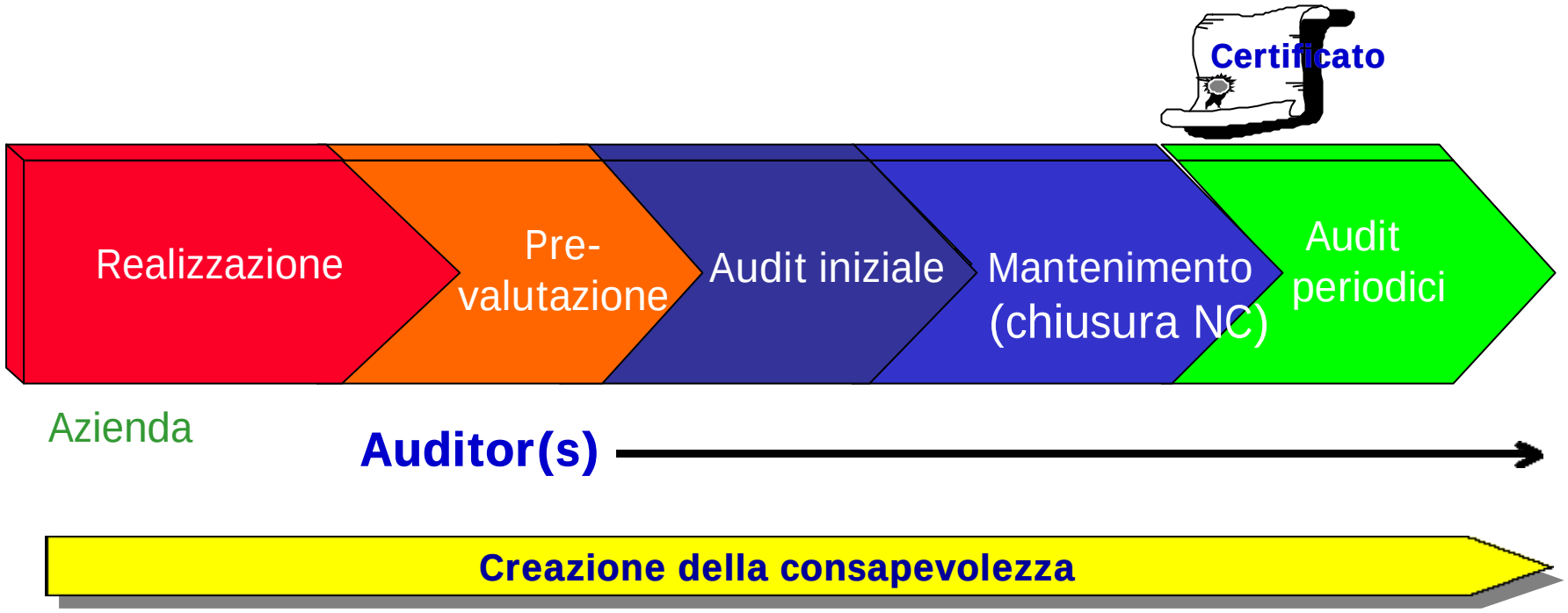


Gruppo di Audit
Esperti tecnici (ev.)

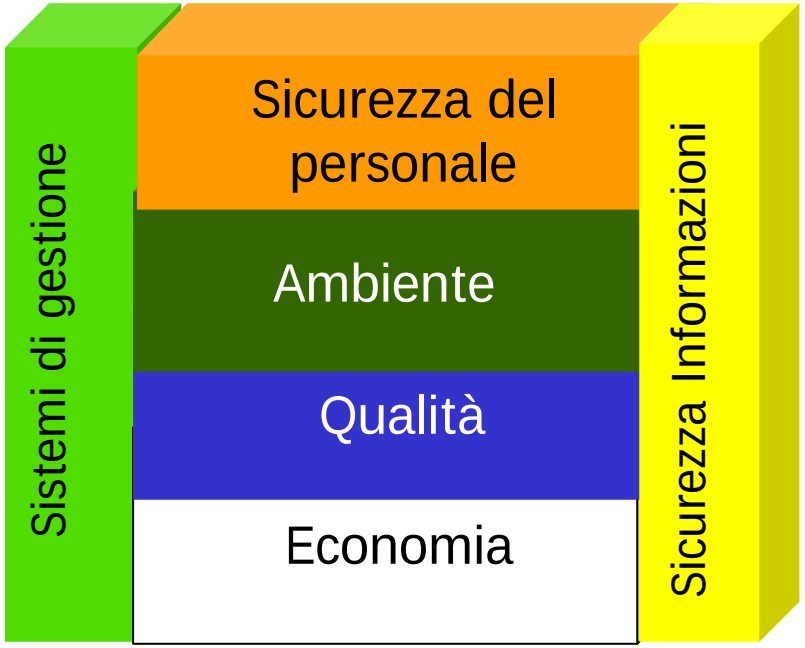
AUDIT INIZIALE

Riesame della documentazione	**Fase 1 (AI)**	**Fase 2 (AI)**
✍Documentazione ISMS ✍Politiche ✍Scopo ✍Descrizione ambiente IT ✍Descrizione ambiente non IT ✍Dichiarazione di Applicabilità ✍Valutazione del rischio ✍Piano di continuità	✍Riesame della documentazione a seguito della fase precedente. ✍Valutazione tecnica iniziale	✍Riesame di quanto emerso dalla fase 1 ✍Valutazione dell'ISMS realizzato ✍Validazione della conformità ai requisiti della norma
Risultato ✍Rapporto	**Risultato** ✍Rapporto ✍NC da chiudere prima della fase 2	**Risultato** ✍Rapporto ✍NC da chiudere prima dell'emissione del certificato ✍Proposta di Certificazione

QUANDO AVVIENE LA CERTIFICAZIONE?



COORDINAMENTO CON ALTRI STANDARD



- Sistema di gestione qualità
- Sistema di gestione ambientale
- Sistema di gestione della sicurezza delle persone
- Sistema di gestione della sicurezza delle informazioni

Un singolo gruppo di auditor

COSTO DELLA CERTIFICAZIONE INIZIALE

Dipende da

- dimensione dell’azienda
- scopo
- ambiente IT e non-IT
- certificazioni precedenti