Criteri di valutazione e certificazione della sicurezza delle informazioni

Cesare Gallotti
Milano, 14 maggio 2004

AGENDA

- Introduzione
- Valutazione dei prodotti
- Valutazione dell'organizzazione per la sicurezza
- Percorso di certificazione BS 7799

Introduzione

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.
- Per l’ISO 9000:2000:
  - informazione*:* dati significativi (ossia che hanno significato per qualcuno)
  - documento*:* informazioni con il loro mezzo di supporto (IT e/o non-IT).
- Per sicurezza delle informazioni si intende l'attività volta a definire, conseguire e mantenere le seguenti proprietà: riservatezza, integrità, disponibilità, autenticità, non ripudiabilità.

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.

COSA SI VALUTA

- I punti chiave per valutare la sicurezza di “qualcosa” sono:
  - definire il “qualcosa”: di cosa si tratta e i suoi confini
  - definire cosa si intende per sicurezza di quel “qualcosa”
  - realizzare le misure di sicurezza previste
  - garantire il livello di sicurezza nel tempo

Valutazione dei prodotti

STANDARD DI RIFERIMENTO

- 1983: TCSEC (Trusted Computer Security Evaluation Criteria)
- 1991: ITSEC (IT Security Evaluation Criteria)
- 1996: Common Criteria (ISO 15408)
- Altri standard sulla qualità del software:
  - ISO 9126 e ISO/IEC 14598
  - Software CMM (Modello di maturità) e SSE-CMM (Security CMM)
  - ISO 90003
  - ISO/IEC 15288 e ISO/IEC 12207

1 - COSA SI VALUTA: IL TOE

- TOE (Target of Evaluation): oggetto di valutazione

- Può essere un sistema o un componente del sistema:
  - Sistema*:* specifica installazione informatica, con un determinato scopo e presente in un ambiente definito
  - Prodotto*:* pacchetto hardware e/o software acquistabile in un negozio e incorporabile in più sistemi.

2 - COSA È LA SICUREZZA DEL TOE

- 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
- Le funzionalità possono essere descritte in:
  - Protection Profile (PP): espressione di requisiti di sicurezza per una famiglia di TOE, coerenti con gli obiettivi di sicurezza
  - Security Target (ST): espressione di requisiti di sicurezza per uno specifico TOE, più dettagliati rispetto a quelli espressi dal PP
- La valutazione della funzionalità (PP e ST) può avere risultato positivo o negativo (1, 0) e stabilisce se le funzioni di sicurezza soddisfano gli obiettivi.

3 - REALIZZARE LE MISURE

- Correttezza: quanto “bene” sono sviluppati i meccanismi
- I Common Criteria prevedono 7 livelli crescenti (EAL 1 ... EAL 7) di valutazione della correttezza.
- 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.

4 - MANTENERE NEL TEMPO

- Parte dei requisiti per la valutazione della correttezza riguardano la gestione del ciclo di vita del TOE e della gestione dei fix.
- Lo standard, però, non garantisce il mantenimento del livello di sicurezza per versioni successive del TOE perché non si sa a priori che parti di codice sono state modificate.

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 nel 1995 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.

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.

1 - COSA SI VALUTA (1/3): LO 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 da esso si deduce l'ampiezza delle attività.
- Vanno definite le relazioni con l'esterno: clienti, fornitori, partner, case madri, ...

1 - COSA SI VALUTA (2/3): LO SCOPO

- La definizione dello scopo è fondamentale e in alcuni casi da esso dipende il successo di un processo di certificazione.
- Obiettivi troppo ambiziosi sono impossibili da raggiungere in un solo passo ed è preferibile un'estensione graduale del campo valutazione.
- In alcuni casi, è preferibile certificare una parte del sistema informativo piuttosto che niente: può servire da prototipo e aumenta la cultura aziendale in merito allo sviluppo e gestione dei sistemi informativi.

1 - COSA SI VALUTA (3/3): I 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. Vanno quindi definiti i processi:
  - 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)

2 - COS'È LA SICUREZZA (1/2): POLITICHE

- Le politiche devono riportare:
  - una definizione di sicurezza delle informazioni,
  - uno schema per stabilire gli obiettivi e i principi da seguire,
  - 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.
- Le politiche dovrebbero essere stabilite prima di decidere lo scopo.

2 - COS'È LA SICUREZZA (2/2): AN. RISCHIO

- L'approccio per la valutazione del rischio deve basarsi su un metodo ripetibile, ossia basato su scale di valutazione oggettive.
- Vanno identificati i livelli di rischio e confrontati con quelli accettabili.
- Opzioni di trattamento del rischio: contrastare, trasferire, evitare, accettare.
- Selezionare i controlli e preparare una dichiarazione di applicabilità (Statement of Applicability).

3 - REALIZZARE LE MISURE

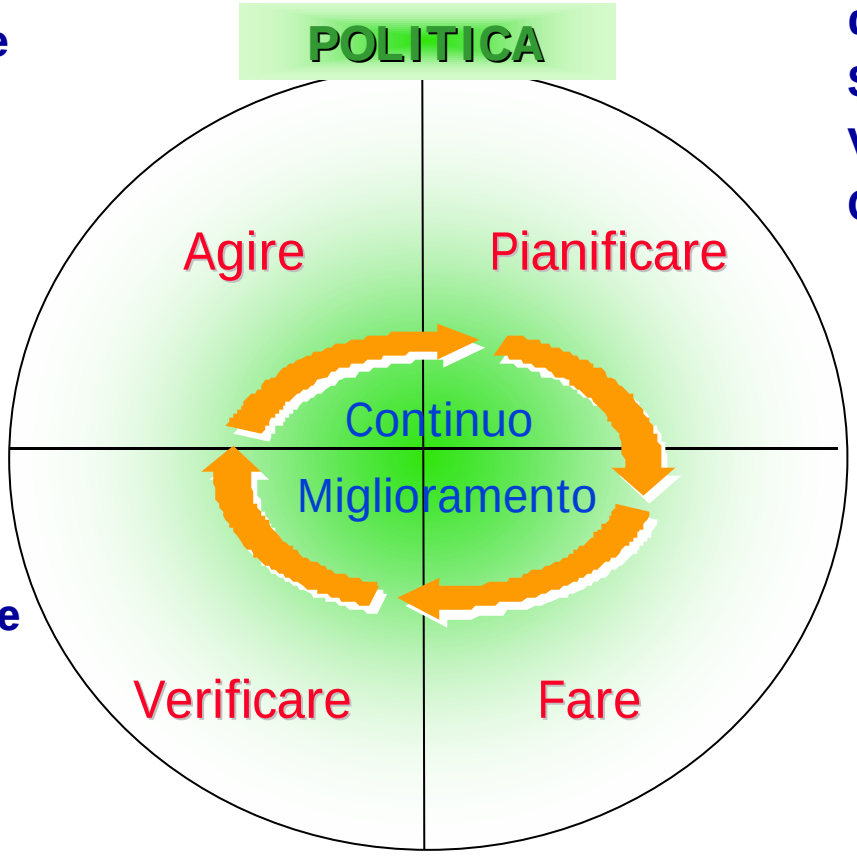
- Deve essere realizzato il piano delle attività, considerando le risorse necessarie in termini di personale, tempo e denaro.
- Devono essere allocate le risorse per:
  - garantire l'efficacia dell'ISMS,
  - seguire l'evoluzione dei vincoli legali e contrattuali,
  - garantire la correttezza dei controlli applicati,
  - condurre revisioni e reagire ai risultati,
  - migliorare l'efficacia dell'ISMS.

4 - MANTENERE NEL TEMPO

- Controlli tecnici:
  - continui
  - allarmi
  - confronto con altre esperienze
- Visite ispettive interne
- Riesame della Direzione
- Indicatori di processo
- Gestire gli incidenti, le azioni correttive e preventive

IL CICLO PLAN DO CHECK ACT

Gestione non conformità
Azioni preventive
Azioni correttive
Manutenzione
Miglioramento

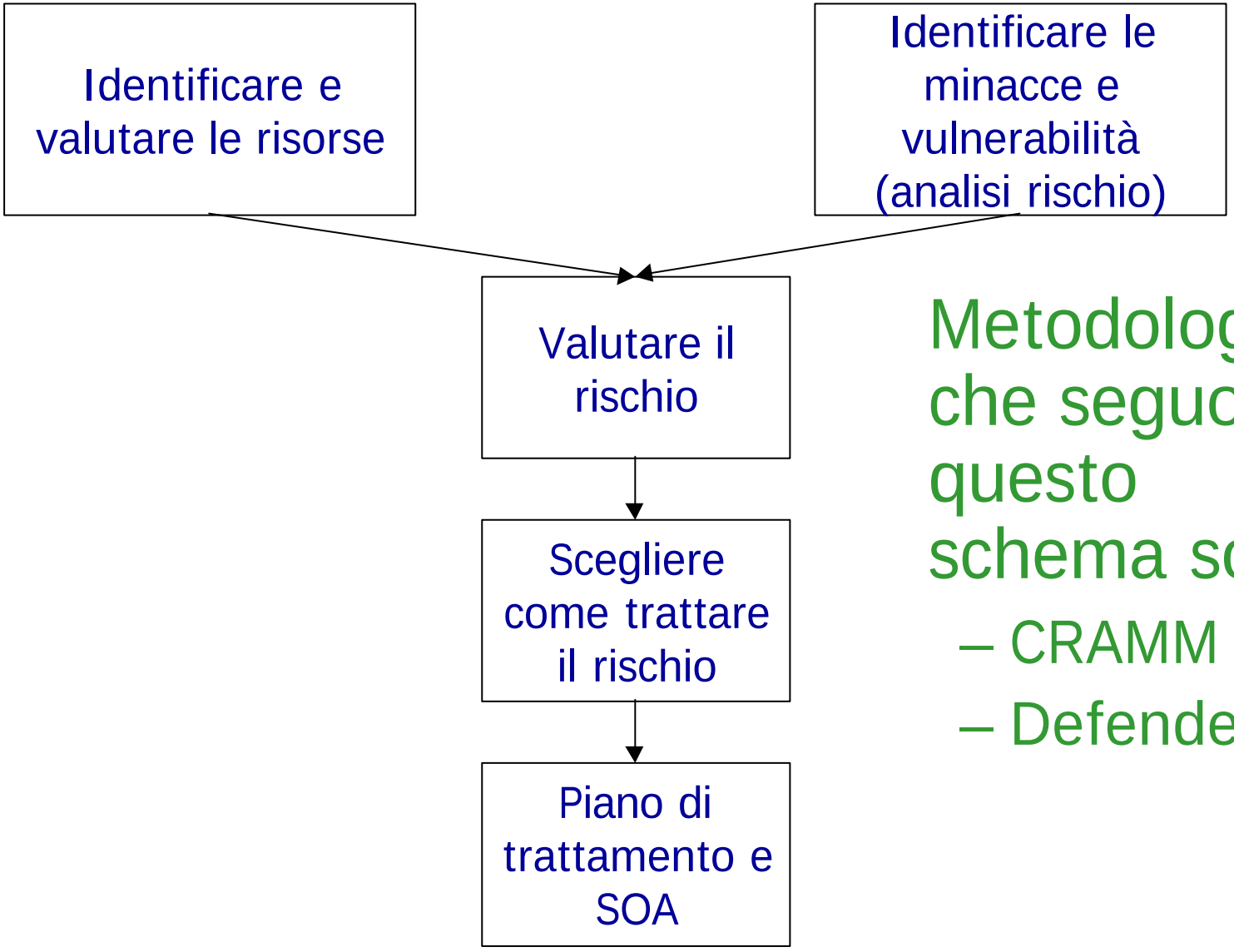


Politiche per la sicurezza delle informazioni
Scopo-dominio dell' ISMS
Valutazione del rischio
Gestione del rischio

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

Controlli tecnici
Visite ispettive
Riesame Direzione
Analisi indicatori di processo

SCHEMATICAMENTE: ANALISI DEL RISCHIO



Metodologie che seguono questo schema sono

- CRAMM
- Defender

UNA CONSIDERAZIONE

- Certamente l'analisi del rischio, la sua valutazione e la metodologia usata sono parti importanti del sistema di gestione.
- Non va però dimenticato che la valutazione del sistema riguarda anche (e soprattutto) come viene gestito nella pratica. E' quindi bene non focalizzarsi solo sulla parte formale.
- Dall'altra parte, l'auditor deve valutare la conformità rispetto ad una norma. Per questo l'azienda deve attenersi ad opportuni riferimenti (formali e sostanziali).

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

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

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

Sistema di gestione

Sistema di gestione delle informazioni (soprattutto IT)

Percorso di certificazione BS 7799-2

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.

CHI “CERTIFICA” I CERTIFICATORI

- 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 ed ogni organismo può essere accreditato per più standard.
- In Italia il compito di accreditare gli organismi di certificazione è affidato al Sincert.

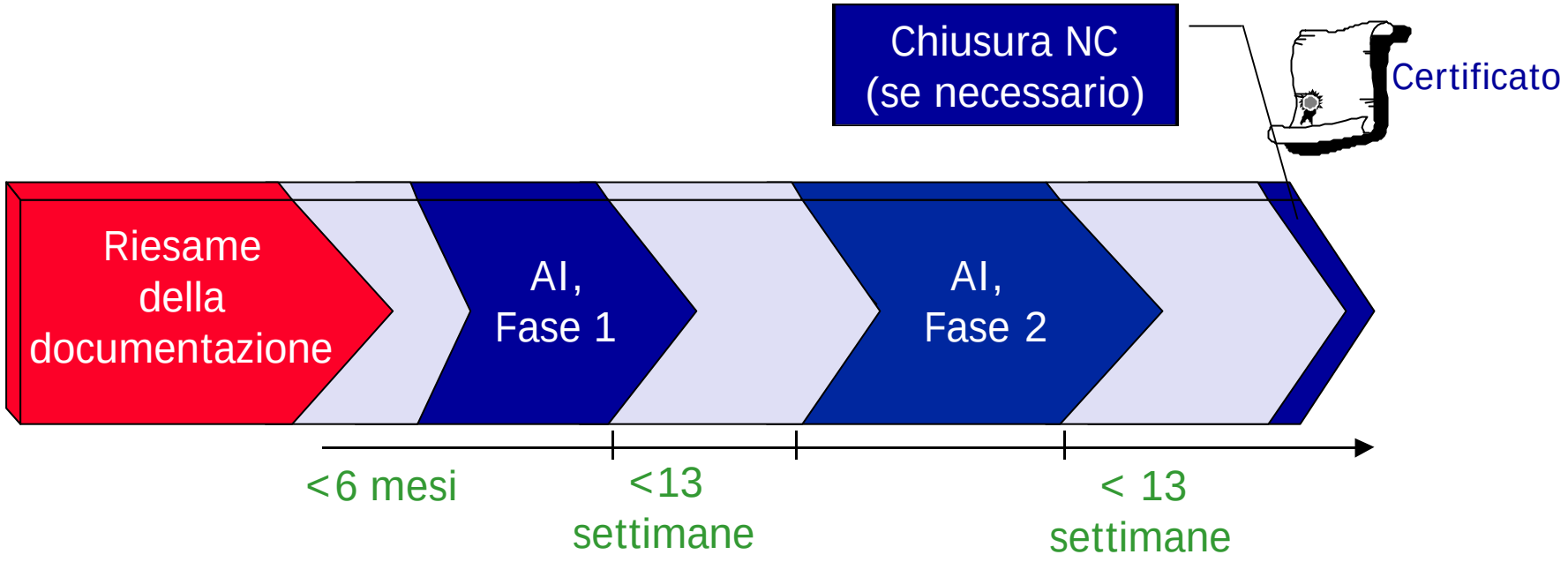
GLI ATTORI

- 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.

I CERTIFICATI BS 7799 AL 15/03/04 (www.xisec.com)

Japan	276	Ireland	7
UK	125	Hungary	6
India	24	China	5
Germany	22	Sweden	4
Korea	22	Austria, Brazil, Iceland, Mexico, Switzerland	3
Hong Kong	17		
Italy	12	Denmark, Greece, UAE	2
Finland	10	Argentina, Belgium, Egypt, Macau, Malaysia, Neth., Poland, Qatar, S. Arabia, Slovenia, S. Africa, Spain	1
Singapore	10		
Taiwan	10		
Norway	9		
USA	9		
Australia	7	**Totale**	**608**

IL PROCESSO DI CERTIFICAZIONE

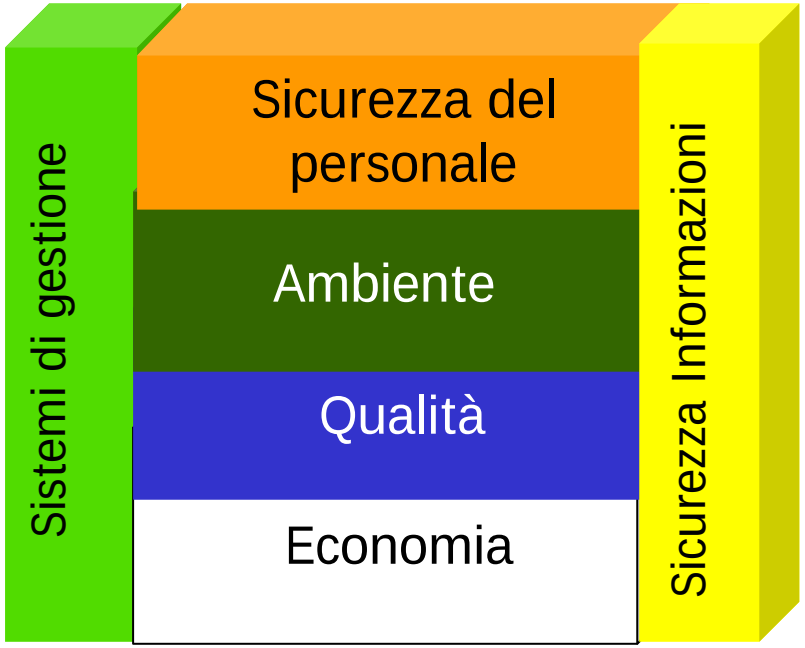


Il certificato ha validità pluriennale (3 anni).
Sono pianificate visite periodiche (almeno 1 all'anno) per confermare il mantenimento dei requisiti.

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	• Valutazione tecnica iniziale • Riesame della documentazione a seguito della fase precedente.	• 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

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