

# Quaderni Clusit

500

Implementazione e  
certificazione dei  
sistemi di gestione  
per la sicurezza  
delle informazioni

Fabrizio Cirilli

# Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni

*Fabrizio Cirilli*

*Comitato Tecnico Scientifico*



---

Quaderni CLUSIT – Febbraio 2007

## CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

## Copyright e Disclaimer

Copyright © 2007 Fabrizio Cirilli

Copyright © 2005-2007 CLUSIT

Tutti i diritti sull'Opera sono riservati all'Autore e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito [www.clusit.it](http://www.clusit.it) in area pubblica.

Gli Autori e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

Gli Autori e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne.

In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato.

Il contenuto dell'Opera non costituisce un parere di tipo professionale o legale.

Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

## Presentazione

In questi ultimi dieci anni il settore della sicurezza delle informazioni e dei sistemi è stato caratterizzato da un flusso continuo di evoluzioni e miglioramenti, che hanno contraddistinto tutte le diverse componenti della disciplina, quella tecnologica e quella organizzativa e di processo.

Dal punto di vista tecnologico sistemi di prevenzione e rilevamento sempre più precisi e sofisticati, accompagnati da un costante miglioramento della qualità del codice hanno contribuito ad accrescere sensibilmente la robustezza dei sistemi alle intrusioni. Certo la strada da percorrere è ancora lunga, ma credo che nessuno possa negare che oggi un sistema informatico aggiornato con le ultime patch ed opportunamente protetto da firewall e IDS, è di gran lunga molto più difficile da attaccare di quanto non lo fosse una decina di anni fa.

Un ruolo importante in questo processo evolutivo è stato svolto anche dai progressi fatti nel settore della governance della Sicurezza. Poco meno di dieci anni fa la documentazione a disposizione di una qualunque organizzazione che volesse affrontare sistematicamente questo problema, la cui complessità è spesso sottostimata, non aveva altra fonte disponibile che il famoso BS7799:1, uno standard britannico costituito da una raccolta di buone pratiche su come amministrare la sicurezza in azienda. Con l'andare del tempo e con l'affermarsi della Società dell'Informazione quelli che oramai sono diventati i Sistemi di Gestione per la Sicurezza delle Informazioni (o SGSI) hanno assunto un rilievo sempre maggiore, e oggi disponiamo di due corposi standard ISO (ISO/IEC 17799:05 e ISO 27001:05) legati alla realizzazione e certificazione di SGSI. Altri standard "di processo" sono all'orizzonte.

Ad onor del vero il processo che ha portato dallo standard britannico BS7799 agli standard ISO è stato un po' caotico, inizialmente solo la componente BS7799:1 dello standard è stata adottata come ISO 17799:2000, successivamente la stessa è stata rivista (ISO 17799:2005) e affiancata dallo standard ISO 27001:05 che costituisce a sua volta una revisione della versione più aggiornata di BS7799:2. Ovviamente non è facile districarsi in tutti questi standard e soprattutto riuscire a cogliere gli aspetti salienti che li differenziano, per contro è estremamente importate per chiunque voglia seriamente occuparsi di sicurezza ICT in ambito aziendale cogliere appieno questi aspetti.

Per far fronte a questa esigenza il CLUSIT ha deciso di affidare a Fabrizio Cirilli, presidente del capitolo italiano del Information Security Management System International User Group, un autore sicuramente tra i più rappresentativi in tema di SGSI nel nostro paese, il compito di predisporre un documento che consentisse di avere un panorama sui diversi processi di standardizzazione in corso presso l'ISO in materia di sicurezza informatica, e di avere una breve panoramica sulle diverse tematiche trattate dagli standard già approvati, sottolineandone aspetti unificanti e non.

Il risultato ottenuto è questa guida dedicata agli addetti ai lavori, estremamente chiara nell'esposizione e di facile lettura. Direi che il pregio principale di questo lavoro, oltre a cogliere appieno gli obiettivi prefissati, è quello di fornire al lettore gli elementi necessari per leggere in modo critico il contenuto degli standard ed apprezzare il significato intrinseco del processo di certificazione proposto. A questo proposito mi sembra importante richiamare due paragrafi del manoscritto che possono fornire al lettore, in estrema sintesi, il tipo di contenuto

che potrà trovare all'interno dello stesso. Ad esempio, in relazione ai contenuti da ricercarsi all'interno degli standard analizzati l'autore ribadisce con estrema chiarezza:

*“... lo standard costituisce un modello organizzativo piuttosto che uno standard tecnico. Non vi troveremo quindi il come fare ma solo il cosa fare in materia di gestione della sicurezza delle informazioni. Ogni organizzazione trova nello standard un riferimento per organizzare la propria sicurezza delle informazioni e non le soluzioni migliori o più innovative. Questa è nel contempo la forza ed il limite di ciascun standard ISO.”*

Ancora più preciso è l'inquadramento che si fornisce del processo di certificazione e del suo valore:

*“L'audit di certificazione consente al team di audit dell'OdC di valutare la conformità (e l'efficacia) del SGSI dell'organizzazione. E' importante ricordare che gli audit degli OdC si svolgono “a campione”, cioè le valutazioni si riferiscono solamente alle parti di SGSI verificate direttamente e che, pertanto, la valutazione non è da considerarsi esaustiva o affidabilistica<sup>1</sup>. Come si dice “l'audit dà confidenza che il SGSI sia conforme ed efficace nel campione esaminato” e non vi è presunzione di affidabilità nella valutazione eseguita<sup>2</sup>. Forse è questo il tallone d'Achille del sistema di certificazione ma dobbiamo anche ricordare che si tratta pur sempre e comunque di un processo volontario a fronte di uno standard “gestionale” e non tecnologico. L'esaustività della valutazione non solo comporterebbe costi rilevanti ma soprattutto condurrebbe alla “clonazione” dei SGSI con ovvio irrigidimento organizzativo e tecnico delle soluzioni ed interpretazioni della norma stessa.”*

In conclusione, ci troviamo di fronte ad un testo sintetico e alla portata di chiunque abbia un decoroso bagaglio di nozioni in materia. Un testo che non si limita a elencare e descrivere i contenuti dei diversi standard legati alla realizzazione di un SGSI, come il titolo potrebbe suggerire, ma entra nel merito degli stessi fornendone una chiave di lettura ed interpretazione. Un testo che va nella direzione di dare il giusto peso agli sforzi compiuti in sede di standardizzazione evitando toni trionfalistici, e la diffusione di miscredenze o cattive interpretazioni, spesso alimentate da improvvisatori dell'ultima ora, che a lungo andare non possono che nuocere all'intero comparto della Sicurezza ICT.

*Prof. Danilo Bruschi  
Presidente del  
Comitato Tecnico-Scientifico Clusit*

---

<sup>1</sup> Il concetto di campionamento si riferisce a documenti, registrazione e/o interviste rilevate durante l'audit.

<sup>2</sup> Le attività di audit per i SGSI si svolgono secondo quanto indicato da: UNI EN ISO 19011:03, ISO 27006 (dal 2007), EA 7/03 e dai documenti tecnici SINCERT.

## **Abstract**

Breve excursus nel mondo della certificazione dei Sistemi di Gestione per la sicurezza delle informazioni e delle norme della famiglia ISO 27000.

Il primo capitolo introduce l'argomento della sicurezza delle informazioni con una rapida analisi del mercato seguita da una breve storia sulla normazione relativa e dal richiamo ai principi ispiratori, delineando così lo scenario di base per una corretta comprensione dei capitoli successivi.

Il secondo capitolo analizza in dettaglio la struttura ed i contenuti della norma. Ciascun argomento è trattato in modo pragmatico individuando le richieste della norma ed i relativi documenti da produrre.

Il terzo capitolo descrive il contenuto ed il significato della ISO/IEC 17799:05 analizzando il collegamento alla ISO/IEC 27001:05.

Il capitolo quattro schematizza il corollario delle norme della famiglia ISO 27000 in fase di pubblicazione.

Il capitolo cinque permette una rapida comprensione delle differenze esistenti tra BS7799-2:02 e ISO/IEC 27001:05 , questo capitolo è di particolare interesse per tutte le organizzazioni che si trovano a dover convertire la propria certificazione entro il 31/3/2007.

I capitoli sei e sette introducono il lettore nel mondo della certificazione dei sistemi ed in particolare dei Sistemi per la Gestione per la Sicurezza delle Informazioni, ponendo l'enfasi sugli aspetti operativi e cercando, nel contempo, di sfatare "miti e leggende" della certificazione.

Il capitolo otto affronta invece il complesso aspetto dell'accreditamento fornendo al lettore gli strumenti per orientarsi nel vasto mondo delle certificazioni dei SGSI e dell'accreditamento degli Organismi di Certificazione.

I capitoli nove e dieci sono di particolare utilità per le organizzazioni che devono affrontare o completare il percorso conversione della propria certificazione verso la ISO/IEC 27001:05 . In particolare il capitolo dieci suggerisce un pratico approccio per guidare il lettore verso l'obiettivo finale.

Infine il capitolo 11 presenta il capitolo italiano del gruppo utenti internazionali della ISO/IEC 27001:05 ed i legami esistenti tra l'associazione e lo sviluppo della norma a livello internazionale e nazionale.

## **L'autore**

Fabrizio Cirilli

Consulente e auditor dei sistemi di gestione per la sicurezza delle informazioni, docente presso il Master di II livello dell'Università La Sapienza di Roma Dipartimento di Informatica (Direttore Prof. L.V.Mancini) , progettista e docente di corsi nazionali ed internazionali per la qualifica degli auditor ISO 27001, lead auditor certificato IRCA e RICEC, membro del comitato ISO JTC1/SC27/WG1 per le norme della famiglia ISO 27000 e membro della task force ISO/IAF per la ISO 27006. Attualmente collabora con organismi di certificazione ed aziende in ambito nazionale ed internazionale sui temi della sicurezza delle informazioni, della qualità dei servizi e dei processi dell'ICT. Socio CLUSIT, AIEA-ISACA e IEEE. Chairman del capitolo italiano degli utilizzatori della ISO 27001 ISMS IUG ITALY

▪

# SOMMARIO

<b>1. INTRODUZIONE.....</b>	<b>9</b>
1.1. IL MERCATO DI RIFERIMENTO .....	9
1.2. BREVI CENNI SUL CONTENUTO DELLO STANDARD.....	9
1.3. LA STORIA DELLA ISO/IEC 27001:05.....	10
1.4. PRINCIPI ISPIRATORI DELLO STANDARD .....	11
1.5. IL CICLO PLAN-DO-CHECK-ACT.....	13
<b>2. LA ISO/IEC 27001:05.....</b>	<b>14</b>
2.1. OBIETTIVI DELLO STANDARD.....	14
2.2. SPECIFICITÀ DELLO STANDARD .....	14
2.3. STRUTTURA .....	14
2.4. INTRODUZIONE AI REQUISITI DELLO STANDARD .....	15
2.5. ANALISI DEI REQUISITI – PDCA .....	15
2.6. ANALISI DEI REQUISITI – DOCUMENTAZIONE.....	16
2.7. DOCUMENTAZIONE OBBLIGATORIA .....	17
2.8. ASPETTI SPECIFICI DEI REQUISITI 4.2 E 4.3.....	17
2.9. ANALISI DEI REQUISITI – 5 RESPONSABILITÀ DELLA DIREZIONE.....	17
2.10. ANALISI DEI REQUISITI – 6 AUDIT INTERNI.....	18
2.11. ANALISI DEI REQUISITI – 7 RIESAME DELLA DIREZIONE .....	18
2.12. ANALISI DEI REQUISITI – 8 MIGLIORAMENTO DEL SGSI.....	19
2.13. L’ALLEGATO A – I CONTROLLI.....	19
2.14. L’ALLEGATO B – L’INTEGRAZIONE PRINCIPI-PDCA-REQUISITI .....	20
<b>3. COSA È ED A COSA SERVE LA ISO/IEC 17799:05 .....</b>	<b>21</b>
3.1. OBIETTIVO .....	21
3.2. STRUTTURA .....	22
3.3. ALTERNATIVE.....	23
<b>4. LE ALTRE NORME DELLA FAMIGLIA ISO 27000 .....</b>	<b>24</b>
4.1. PROSSIME SCADENZE.....	24
<b>5. COSA CAMBIA RISPETTO ALLA BS7799-2:02 .....</b>	<b>25</b>
5.1. LE INNOVAZIONI .....	25
5.2. LE DIFFERENZE.....	25
5.3. LA MISURABILITÀ .....	25
<b>6. LA CERTIFICAZIONE DEI SGSI.....</b>	<b>27</b>
6.1. OBIETTIVO .....	27
6.2. SIGNIFICATO .....	27
6.3. VALENZA.....	28
6.4. EFFICACIA VS CONFORMITÀ .....	28
<b>7. COME CERTIFICARSI ISO/IEC 27001:05 .....</b>	<b>29</b>
7.1. I PASSI DA FARE PER IMPLEMENTARE IL SGSI.....	29
7.1.1. <i>Campo di applicazione</i> .....	29
7.1.2. <i>Ampiezza</i> .....	30
7.1.3. <i>Politica</i> .....	30
7.1.4. <i>Analisi e valutazione dei rischi</i> .....	30
7.1.5. <i>Dichiarazione di applicabilità</i> .....	30
7.1.6. <i>La scelta dei controlli</i> .....	31
7.2. I PASSI PER IDENTIFICARE E SCEGLIERE L’ORGANISMO DI CERTIFICAZIONE (ODC) .....	31

7.3.	AUDIT PRELIMINARE .....	31
7.4.	IL PROCESSO DI CERTIFICAZIONE.....	32
7.4.1.	<i>Quanto può durare un audit</i> .....	32
7.4.2.	<i>Fase 1 (o audit documentale)</i> .....	34
7.4.3.	<i>Fase 2 (o audit di certificazione)</i> .....	34
7.5.	SORVEGLIANZA E RINNOVO.....	35
7.6.	VALENZA DEGLI AUDIT .....	36
<b>8.</b>	<b>LA CERTIFICAZIONE ACCREDITATA .....</b>	<b>37</b>
8.1.	PERCHÉ ACCREDITATA.....	37
8.2.	CHI ACCREDITA .....	38
8.2.1.	<i>SINCERT</i> .....	38
8.2.2.	<i>EA</i> .....	39
8.2.3.	<i>IAF</i> .....	40
8.3.	COME ACCREDITA .....	40
8.4.	IL MULTI LATERAL AGREEMENT EUROPEO .....	41
8.5.	IL MULTI RECOGNITION ARRANGMENT MONDIALE .....	41
<b>9.</b>	<b>IL PERIODO DI TRANSIZIONE.....</b>	<b>42</b>
9.1.	QUANDO SCADA LA BS7799-2:02 .....	42
<b>10.</b>	<b>COME CONVERTIRE I CERTIFICATI DA BS7799-2:02 A ISO/IEC 27001:05.....</b>	<b>43</b>
10.1.	CONVERTIRE IL SGSI ALLA NUOVA NORMA.....	43
10.2.	CONVERTIRE IL CERTIFICATO .....	44
<b>11.</b>	<b>IL GRUPPO UTENTI INTERNAZIONALI (ISMS IUG).....</b>	<b>45</b>
11.1.	RUOLO DEL ISMS IUG ITALY NEL COMITATO ISO JTC1/SC 27/WG 1 .....	45

## 1. Introduzione

Questo quaderno si pone l'obiettivo di fornire informazioni in relazione alla certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni (o SGSI<sup>3</sup>) secondo lo standard ISO/IEC 27001 edizione 2005. Per raggiungere tale obiettivo dovremo però necessariamente parlare:

- del mercato di riferimento
- dello standard stesso e della sua storia
- dei principi cui si ispira
- del modello organizzativo in esso proposto.

Solo a questo punto la certificazione assumerà un senso compiuto e si potrà avere una visione chiara del significato di tale azione e delle sue conseguenze su un'organizzazione.

### 1.1. Il mercato di riferimento

L'attuale scenario mondiale vede le informazioni, di ogni genere, sempre più al centro dell'interesse di tutti: stampa, aziende, pubbliche amministrazioni, borsa, cittadini ecc. La globalizzazione ed internet hanno enormemente allargato la possibilità di raccogliere informazioni, sia in senso positivo (si pensi alla possibilità di prenotare visite specialistiche presso un ospedale) sia in senso negativo (si pensi alla possibilità di intercettazione delle proprie credenziali di home banking nel corso di una transazione).

Lo standard ISO/IEC 27001:05, pur non volendo costituire la panacea dei mali della sicurezza delle informazioni, costituisce senz'altro il punto di partenza per impostare un sistema organizzativo che abbracci tutti gli aspetti della sicurezza delle informazioni e che si inserisca in un contesto di IT governance evoluto<sup>4</sup>.

In Italia è previsto un uso massiccio di questo standard all'interno di bandi di gara e licitazioni private, infatti nell'ultimo anno si è avuto un incremento significativo dell'interesse nei confronti dello standard (sebbene ciò non implichi necessariamente l'incremento del numero di certificazioni emesse).

Inoltre non va trascurato l'effetto trascinatore provocato dalla legislazione vigente in materia di privacy, proprietà intellettuale, responsabilità amministrativa e disposizioni antiterrorismo; queste hanno contribuito certamente ad avvicinare ulteriori organizzazioni all'applicazione dello standard in contesti diversi, permettendone così una *validazione* a livello nazionale.

A livello applicativo si possono ipotizzare le seguenti fasce di interesse nel prossimo biennio: sanità, banche e assicurazioni, telecomunicazioni, servizi al pubblico. A tal fine lo standard verrà appositamente contestualizzato in specifici standard applicativi di settore (come vedremo in uno dei capitoli successivi), l'uscita di tali personalizzazioni è prevista nell'arco del biennio 2007-2008.

### 1.2. Brevi cenni sul contenuto dello standard

La ISO/IEC 27001:05 nasce come standard per gestire la sicurezza delle informazioni e come tutti gli standard ISO certificabili non si riferisce ad un contesto specifico, vale a dire che lo standard è applicabile anche al di fuori dei sistemi informatici, essendo l'informazione intesa come indipendente dai supporti e dalle infrastrutture (sebbene al di fuori di un contesto

---

<sup>3</sup> ISMS nella versione inglese (Information Security Management System).

<sup>4</sup> In tal senso è facilmente comprensibile la forte interazione con altri modelli di gestione IT: COBIT, ITIL e ISO 20000-1.

informatico risulti piuttosto complesso comprenderne alcuni contenuti specifici che vedremo più avanti).

In generale possiamo affermare che lo standard è applicabile a qualsiasi contesto produttivo ed a qualsiasi tipo di organizzazione: semplice o complessa, pubblica o privata, informatizzata e non. L'esperienza ci insegna però che a fruirne con maggior frequenza ed efficacia sono le aziende e le organizzazioni per le quali l'ICT costituisce un asse portante di rilievo (amministrazioni pubbliche centrali e locali, fornitori di servizi telefonici e di telecomunicazioni, dipartimenti/divisioni IT di banche ed assicurazioni ecc.).

Bisogna anche sottolineare come lo standard costituisca un modello organizzativo piuttosto che uno standard tecnico. Non vi troveremo quindi il *come* fare ma solo il *cosa* fare in materia di gestione della sicurezza delle informazioni. Ogni organizzazione trova nello standard un riferimento per organizzare la propria sicurezza delle informazioni e non le soluzioni migliori o più innovative.

Questa è nel contempo la forza ed il limite di ciascun standard ISO.

La lettura e l'analisi dello standard apre varchi, nuovi confini, evidenzia opportunità e possibilità in materia di sicurezza delle informazioni, offrendo praticamente nessuna soluzione operativa, che deve invece essere maturata internamente tenendo conto delle proprie necessità e risorse disponibili.

E' indispensabile sottolineare come l'adozione della ISO/IEC 27001:05 non escluda l'integrazione di altri standard o modelli per la gestione della sicurezza (ad esempio COBIT di ISACA ed altri).

### **1.3. La storia della ISO/IEC 27001:05**

Nel 1990 il DTI (*Department of Trade and Industry*) del governo britannico istituisce un gruppo di lavoro finalizzato a fornire alle aziende una guida per la gestione della sicurezza del loro patrimonio informativo.

Nel 1993 viene pubblicato il documento: *Code of Practice for Information Security Management* che contiene una raccolta di pratiche utili per affrontare temi specifici della sicurezza.

Nel 1995 *British Standard Institution* pubblica lo stesso documento come standard BS7799-1:1995.

Nel 1996 la ISO (*International Standard Organization*) costituisce il comitato JTC1 SC27 che ha il compito di trasformare lo standard britannico in standard mondiale.

Nel 1998 BSI pubblica lo standard BS7799-2:1998 *Specification for Information Security Management Systems* che pone le basi per la gestione dei sistemi per la sicurezza delle informazioni e sancisce l'avvio della certificazione secondo standard BSI (limitatamente ai paesi che intendano sfruttarne volontariamente i contenuti senza velleità di standardizzazione internazionale).

Nel 1999 BSI pubblica un aggiornamento dei due standard generando una versione allineata e congruente dei due documenti.

Nel 2000 il comitato ISO rilascia la prima versione del documento ISO/IEC 17799:2000 (emissione ISO dello standard BS7799-1:1995).

Nel 2005 lo stesso comitato, recependo la più recente versione dello standard BS del 1999, pubblica la versione definitiva ed attuale dello standard ISO/IEC 27001:05 e della ISO/IEC 17799:05 avviando la certificazione secondo standard ISO e decretandone l'internazionalizzazione e l'utilizzabilità in ambito internazionale e contrattuale.

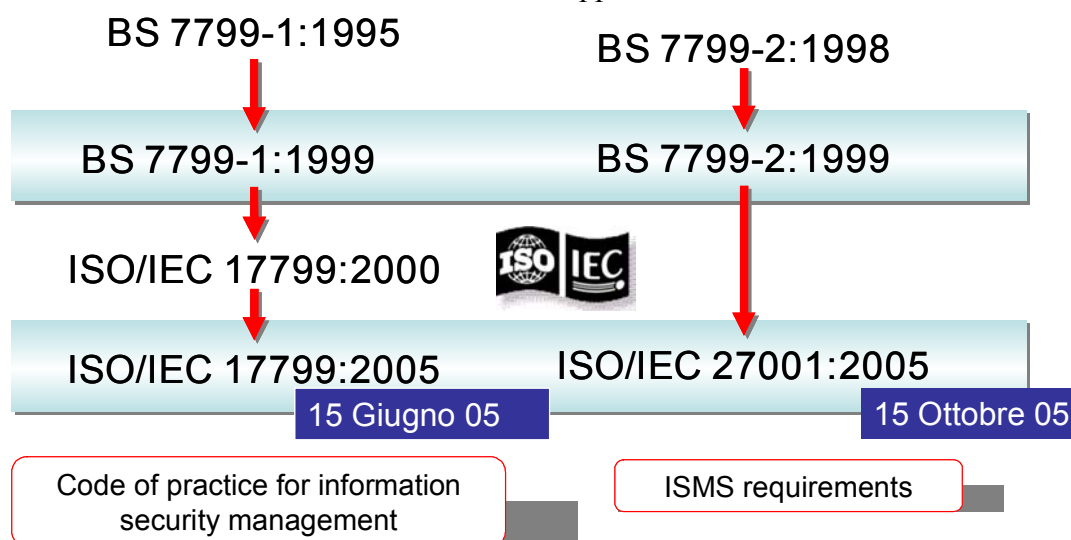
Il recepimento ISO sancisce anche la normalizzazione delle certificazioni, emesse fino a quel momento in un regime di libertà totale. Viene così definito il periodo di transizione, cioè

vengono definiti i criteri per convertire le certificazioni esistenti da BS 7799-2 a ISO/IEC 27001; ciascun paese definisce i propri criteri salvo quanto concerne la data ultima che viene fissata a livello mondiale al 30 aprile 2007.

In Italia, il SINCERT pubblica i propri criteri il 13 dicembre 2005, fissando al 31 marzo 2007 la data ultima per la conversione dei certificati emessi posizionando le aziende italiane in situazione favorevole rispetto al mercato internazionale: infatti, così facendo, le aziende italiane potranno, ad esempio, rispondere con un mese di anticipo ad eventuali gare pubblicate in G.U.C.E. nelle quali si faccia richiesta di certificazioni ISO 27001.

Nello stesso documento sono prescritti i principi che gli Organismi di Certificazione devono adottare per l'aggiornamento del proprio accreditamento e per la formazione degli auditor.

Lo schema successivo riassume brevemente le tappe dello standard:



L'interesse suscitato da questo standard è l'applicabilità ai diversi ambiti produttivi ha avviato un vero e proprio processo di specializzazione ed espansione dello standard che condurrà a breve ad un quadro come quello presentato in uno dei capitoli successivi

#### 1.4. Principi ispiratori dello standard

Come molti altri standard ISO anche la ISO/IEC 27001:05 è ispirata a principi guida generalmente riconosciuti a vario titolo nel mondo.

Le "linee guida sulla sicurezza dei sistemi e delle reti di informazione. Verso una cultura della sicurezza" sono state adottate sotto forma di Raccomandazione in occasione della 1037<sup>a</sup> sessione del Consiglio dell'OCSE<sup>5</sup>, il 25 luglio 2002.

Gli obiettivi della guida sono<sup>6</sup>:

- estendere all'insieme delle parti interessate una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti d'informazione.
- Rafforzare la sensibilità rispetto ai rischi per i sistemi e le reti d'informazione, alle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi, nonché alla necessità di adottarli e di attuarli.
- Favorire una maggiore fiducia delle parti nei confronti dei sistemi e delle reti d'informazione e nel modo in cui sono forniti ed utilizzati.

<sup>5</sup> Organizzazione per la Cooperazione e lo Sviluppo Economico, nella versione inglese Organization for Economic Co-operation and Development (o OECD) per maggiori informazioni consultare il sito [www.oecd.org](http://www.oecd.org).

<sup>6</sup> Dalla traduzione a cura di AICQ ([www.aicq.it](http://www.aicq.it)).

- Creare un assetto generale di riferimento che aiuti le parti interessate a comprendere la natura dei problemi legati alla sicurezza e a rispettare i valori etici nell'elaborazione e nell'attuazione di politiche, pratiche, azioni e procedure coerenti per la sicurezza dei sistemi e reti d'informazione.
- Incoraggiare fra tutte le parti interessate, la cooperazione e la condivisione d'informazioni adeguate all'elaborazione e all'attuazione di politiche, pratiche, azioni e procedure intese alla sicurezza.
- Promuovere la presa in considerazione della sicurezza quale obiettivo rilevante per tutte le parti interessate associate all'elaborazione e all'attuazione di norme.

“I nove principi di seguito presentati sono complementari e devono essere considerati come un insieme. Essi riguardano le parti interessate a tutti i livelli, compreso quello politico e operativo. Secondo quanto indicato dalle Linee guida, le responsabilità delle parti interessate variano secondo il ruolo da loro assunto. Tutte le parti interessate saranno assistite con interventi di sensibilizzazione, d'istruzione, di scambi d'informazione e di formazione per facilitare una migliore comprensione degli argomenti di sicurezza e l'adozione di migliori pratiche in tale settore. Gli sforzi tesi a rafforzare la sicurezza dei sistemi e delle reti d'informazione devono rispettare i valori di una società democratica, in particolare l'esigenza di una libera ed aperta circolazione dell'informazione e i principi di base del rispetto della vita privata delle singole persone.”<sup>7</sup>

Vediamo ora i 9 principi, in termini di enunciati:

**1) Sensibilizzazione**

Le parti interessate devono essere consapevoli della necessità di tutelare la sicurezza dei sistemi e delle reti d'informazione e delle azioni che possono intraprendere per rafforzare la sicurezza.

**2) Responsabilità**

Le parti interessate sono responsabili della sicurezza dei sistemi e delle reti d'informazione.

**3) Risposta**

Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.

**4) Etica**

Le parti interessate devono rispettare i legittimi interessi delle altre parti.

**5) Democrazia**

La sicurezza dei sistemi e delle reti d'informazione deve essere compatibile con i valori fondamentali di una società democratica.

**6) Valutazione dei rischi**

Le parti interessate devono procedere a valutazioni dei rischi.

**7) Concezione e applicazione della sicurezza**

Le parti interessate devono integrare la sicurezza quale elemento essenziale dei sistemi e delle reti d'informazione.

**8) Gestione della sicurezza**

Le parti interessate devono adottare un approccio globale della gestione della sicurezza.

**9) Rivalutazione**

Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti di informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e le procedure di sicurezza.

---

<sup>7</sup> Dalla traduzione a cura di AICQ.

Tutti i principi (ad eccezione del 4° etica e del 5° democrazia) sono stati integrati nello standard ISO/IEC 27001:05. Le motivazioni per l'esclusione dei due principi non risultano apertamente documentate (anche se da un'attenta lettura dei due principi, dall'analisi dei paesi aderenti all'OCSE e stante la dichiarazione degli obiettivi generali è possibile intuirne le problematiche attuative in alcune delle nazioni elencate).

### **1.5. Il ciclo Plan-Do-Check-Act**

Gli standard ISO adottano il ciclo PDCA<sup>8</sup> come modello di riferimento per la descrizione dei processi e dei requisiti dello standard.

Il ciclo PDCA, sviluppato negli anni 1920 da Walter Shewhart, è stato successivamente reso popolare da W. Edwards Deming. Il concetto PDCA è presente in tutte le aree della nostra vita personale o professionale e viene utilizzato continuamente, formalmente o informalmente, coscientemente o non, in qualunque cosa noi facciamo. Ogni attività, sia essa semplice o complessa, ricade sotto questo schema, di fatto un ciclo senza fine:

- **Plan**  
Cosa fare e come per soddisfare politica e obiettivi per la sicurezza delle informazioni?
- **Do**  
Porre in atto quanto pianificato
- **Check**  
Verificare se si è fatto quanto pianificato e se quanto fatto risulta efficace
- **Act**  
Come e cosa migliorare?

Ciascuna attività all'interno dello standard ISO/IEC 27001:05 ricade sostanzialmente in questo ciclo, come vedremo in uno dei capitoli successivi.

In buona sostanza il ciclo PDCA è il motore dello standard ISO/IEC 27001:05 mentre i principi OCSE sono le strade attraverso le quali si raggiunge la sicurezza delle informazioni.

---

<sup>8</sup> Cfr. documento ISO/TC 176/SC 2/N 544R2 reperibile nel sito [www.iso.ch](http://www.iso.ch).

## 2. La ISO/IEC 27001:05

A questo punto dobbiamo guardare più da vicino il contenuto dello standard (o norma) per poter proseguire nel nostro percorso di analisi del processo di certificazione.

### 2.1. Obiettivi dello standard

Lo standard ISO/IEC 27001:05 definisce i requisiti applicativi per un SGSI. Tali requisiti sono utilizzabili sia per l'implementazione sia per l'audit dei SGSI.

Gli obiettivi di un SGSI sostanzialmente possono essere riassunti come segue:

- dimostrare la **conformità** e l'**efficacia** delle scelte organizzative e delle attività operative poste in atto per garantire la:
  - **riservatezza**
  - **integrità**
  - **disponibilità**delle informazioni incluse nel perimetro coperto dal SGSI
- assicurare la:
  - **continuità del business**;
  - **minimizzazione dei danni in caso di incidenti** (essendo questi di fatto inevitabili);
  - **massimizzazione degli investimenti** effettuati per l'implementazione e la gestione della sicurezza;
  - **miglioramento continuo dell'efficacia** organizzativa ed operativa.

### 2.2. Specificità dello standard

*Chiave di volta* dello standard è la valutazione dei rischi sulla base della quale viene organizzato un SGSI.

Lo standard introduce però altri aspetti caratteristici tipici di un SGSI:

- il concetto di asset (o bene) con relativa valorizzazione;
- gli aspetti economico-finanziari inerenti la sicurezza delle informazioni;
- l'aspetto organizzativo (e non solo tecnologico) della sicurezza delle informazioni;
- l'efficacia del SGSI e delle contromisure adottate per trattare i rischi.

In tal senso siamo di fronte ad uno standard "rivoluzionario" che pone le basi per una reale utilizzabilità e comprensione all'interno di una organizzazione. Altri standard hanno infatti sofferto dell'astrattismo tipico di uno standard ISO e della completa assenza di riferimenti economico-finanziari, che li hanno resi alla lunga poco graditi al management ed agli imprenditori.

Altra importante caratterizzazione è il corollario di standard che affiancano la ISO/IEC 27001:05 per supportare le organizzazioni nell'attuazione dello stesso, per citarne alcune a titolo esemplificativo: lo standard per la valutazione e gestione dei rischi, lo standard per la misurazione dell'efficacia della sicurezza, le personalizzazioni settoriali previste e già accennate all'inizio di questo documento.

### 2.3. Struttura

La ISO/IEC 27001:05 è strutturata macroscopicamente in 3 blocchi di requisiti:

- Dal cap. 0 al cap. 3: requisiti introduttivi e di spiegazione della norma (come quasi tutte le norme ISO);
- Dal cap. 4 al cap. 8: requisiti applicativi del SGSI;

➤ Allegati: normativi e descrittivi a supporto di quanto citato nei capitoli precedenti. L'allegato A, in particolare, ricopre un ruolo fondamentale nelle fasi di implementazione operativa e audit del SGSI, come vedremo nei capitoli successivi.

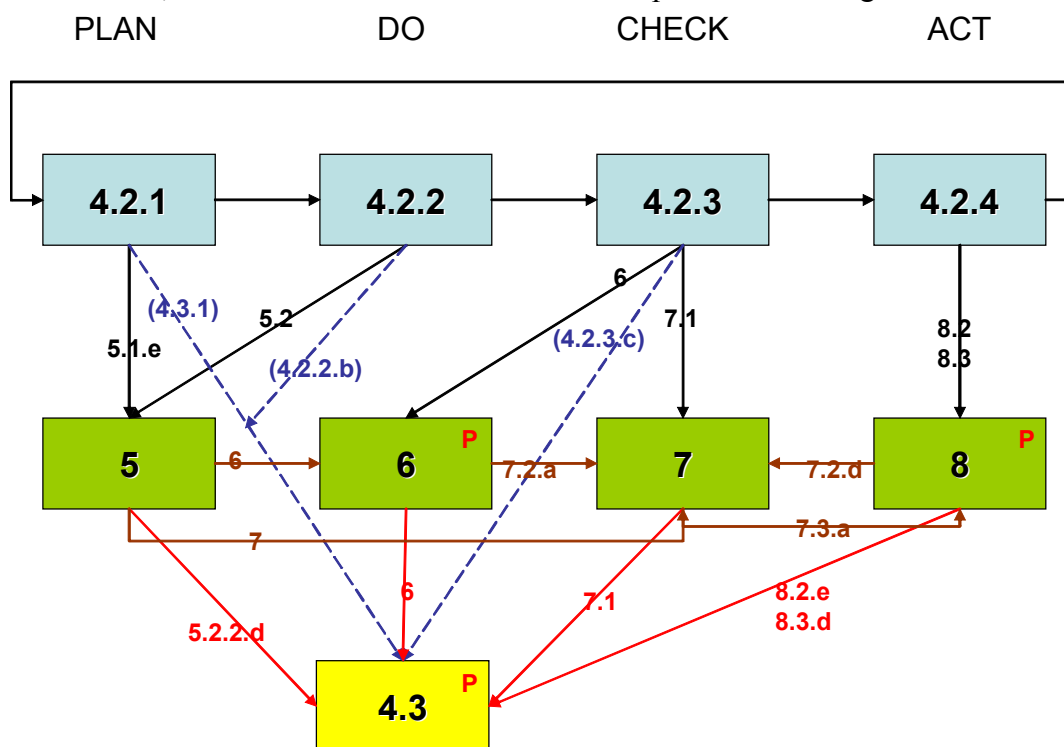
## 2.4. Introduzione ai requisiti dello standard

All'interno dei capitoli (detti anche *requisiti* o *clausole*) dal 4 all'8 sono distribuiti i requisiti applicativi per i SGSI.

Questi capitoli possono essere schematizzati come segue:

- Il cap. 4.2 contiene le fasi di progettazione, sviluppo, verifica e miglioramento del SGSI (il ciclo Plan-Do-Check-Act).
- Il cap. 4.3 contiene gli aspetti di gestione documentale del SGSI.
- Il cap. 5 contiene gli aspetti organizzativi e di Direzione del SGSI.
- Il cap. 6 contiene gli aspetti legati alle attività di audit sul SGSI.
- Il cap. 7 fissa gli aspetti necessari al riesame dell'andamento del SGSI a cura della Direzione.
- Il cap. 8 contiene gli aspetti inerenti il miglioramento continuo.

Lo schema seguente, sebbene non esaustiva, fornisce una indicazione di massima della struttura delle norme, delle interazioni esistenti tra i vari capitoli e dei collegamenti con il ciclo PDCA:



## 2.5. Analisi dei requisiti – PDCA

Il cap. 4.2 costituisce (per così dire) il motore del SGSI, in particolare:

- il cap. 4.2.1 definisce i passi per la pianificazione del SGSI:
  - definizione dell'ampiezza e dei confini,
  - stesura della politica per la sicurezza delle informazioni,
  - valutazione dei rischi,
  - trattamento dei rischi,

- scelta delle contromisure,
- approvazione della Direzione per i rischi residui e per l'attuazione del SGSI,
- preparazione della dichiarazione di applicabilità.
- il cap. 4.2.2 definisce i passi per l'attuazione del SGSI:
  - formulazione e attuazione del piano di trattamento dei rischi,
  - attuazione delle contromisure scelte,
  - definizione criteri di misurazione dell'efficacia dei controlli,
  - attuazione dei programmi di formazione,
  - gestione delle attività del SGSI,
  - individuazione incidenti e pronta risposta.
- il cap. 4.2.3 definisce i passi per il controllo, la misurazione ed il monitoraggio del SGSI:
  - attuazione attività di monitoraggio e riesame,
  - esecuzione riesami di efficacia del SGSI
  - misurazione efficacia contromisure,
  - riesame della valutazione dei rischi,
  - conduzione degli audit interni,
  - riesame della Direzione sul SGSI,
  - aggiornamento dei piani sicurezza,
  - registrazione azioni ed eventi inerenti efficacia e prestazioni del SGSI.
- il cap. 4.2.4 definisce i passi per il miglioramento del SGSI:
  - attuare i miglioramenti individuati,
  - intraprendere azioni correttive e preventive<sup>9</sup>,
  - comunicare azioni e miglioramenti alle parti interessate,
  - assicurare che i miglioramenti raggiungano gli obiettivi prestabiliti.

Gli altri capitoli sono in effetti richiamati dai requisiti del cap. 4.2 per approfondire e/o specializzare alcuni aspetti puntuali (ad esempio: il riesame, gli audit, le azioni correttive e preventive ecc.).

## **2.6. Analisi dei requisiti – Documentazione**

Il cap. 4.3 costituisce il framework strutturale della documentazione necessaria per il corretto funzionamento del SGSI.

Documentazione in questo caso va inteso nel termine più ampio del termine, includendo qualsiasi tipo di documento su qualsiasi supporto (magnetico o cartaceo che sia).

I sistemi di gestione comprendono sostanzialmente due ordini di documenti:

- quelli che descrivono attività da condurre per la sicurezza delle informazioni (politiche, procedure, istruzioni ecc.);
- quelli che dimostrano l'effettiva attuazione di quanto prescritto (o registrazioni).

Il cap. 4.3 elenca le attività che devono essere poste in atto per assicurare un efficace controllo e gestione dei documenti e delle registrazioni del SGSI.

Nel capitolo viene richiesta l'implementazione di una procedura documentata<sup>10</sup> che descriva quanto posto in atto per la gestione dei documenti del SGSI.

L'estensione della documentazione di un SGSI è posta in relazione con:

- dimensioni dell'organizzazione,
- tipologia di attività,

<sup>9</sup> Un'azione correttiva rimuove la causa del problema evitando che questo si ripeta, un'azione preventiva invece rimuove le cause potenziali del problema evitando che questo si verifichi.

<sup>10</sup> Con procedura documentata si intende procedura scritta.

- ampiezza e complessità dei requisiti per la sicurezza.

Pertanto organizzazioni diverse possono avere diverse strutture documentali senza per questo compromettere l'efficacia e la conformità del SGSI.

### **2.7. Documentazione obbligatoria**

La documentazione obbligatoria è stata ridotta allo stretto necessario e prevalentemente orientata a sfruttare quanto già in atto presso qualsiasi organizzazione orientata alla sicurezza delle informazioni:

- *politica* ed obiettivi per il SGSI;
- descrizione del *perimetro* applicativo del SGSI;
- metodologia e rapporto sulla *valutazione dei rischi*;
- piano per il *trattamento dei rischi*,
- *procedure documentate* per la gestione:
  - della documentazione,
  - degli audit,
  - delle azioni correttive e preventive,
  - dei criteri di valutazione dell'efficacia del SGSI e delle contromisure adottate;
- registrazioni (prove oggettive) del funzionamento efficace e conforme del SGSI;
- *Dichiarazione di Applicabilità*, cioè l'elenco delle contromisure adottate, incluse i motivi di scelta/esclusione dei controlli citati nell'allegato A dello standard;
- eventuali documenti dell'organizzazione per la pianificazione, gestione e controllo della sicurezza delle informazioni ed del SGSI.

Sostanzialmente vengono richiesti pochi elementi aggiuntivi rispetto a quelli normalmente necessari o utilizzati per la sicurezza anche senza uno standard di riferimento!

### **2.8. Aspetti specifici dei requisiti 4.2 e 4.3**

Il cap. 4.2 e il cap. 4.3 sono indispensabili per l'implementazione del SGSI mentre i restanti capitoli lo diventano per permetterne la standardizzazione verso la valutazione e la certificazione.

In linea teorica un'organizzazione potrebbe adottare inizialmente i soli due capitoli iniziali per assicurare il corretto funzionamento del proprio SGSI; successivamente potrebbe essere prevista l'inclusione dei restanti capitoli avviando così il SGSI alla certificazione.

### **2.9. Analisi dei requisiti – 5 Responsabilità della Direzione**

Il cap. 5 definisce le responsabilità della Direzione in relazione al SGSI:

- stabilire una politica per il SGSI;
- assicurare che siano stabiliti obiettivi e piani per il SGSI;
- stabilire ruoli e responsabilità per la sicurezza delle informazioni;
- comunicare all'organizzazione l'importanza del conseguimento degli obiettivi relativi alla sicurezza delle informazioni e conformandosi alla politica per la sicurezza delle informazioni, alle sue responsabilità di fronte alla legge e alle necessità di miglioramento continuo;
- fornire risorse sufficienti per istituire, attuare, operare, monitorare, riesaminare, mantenere e migliorare il SGSI;
- decidere i criteri per accettare i rischi e per l'accettabile livello di rischio;

- assicurare che siano condotti gli audit interni sul SGSI;
- condurre riesami da parte della direzione del SGSI.

Inoltre il capitolo delinea gli aspetti inerenti le risorse, in termini di:

- messa a disposizione delle risorse necessarie affinché il SGSI raggiunga gli obiettivi prefissati;
- formazione e consapevolezza del personale in relazione alla sicurezza delle informazioni, competenze necessarie per la corretta gestione del SGSI.

### **2.10.      *Analisi dei requisiti – 6 Audit interni***

Il capitolo 6 introduce gli audit interni come potente strumento per la dimostrazione dell'efficacia e della conformità<sup>11</sup> del SGSI.

Inoltre viene qui delineata la necessità di una procedura documentata<sup>12</sup> per assicurare l'efficace gestione degli audit interni, ivi inclusa la necessità di assicurare l'indipendenza di giudizio degli auditor utilizzati.

Per la gestione degli audit interni è possibile utilizzare la linea guida UNI EN ISO 19011:03 che costituisce il modello di riferimento per ogni tipologia di audit sui sistemi di gestione ISO.

### **2.11.      *Analisi dei requisiti – 7 Riesame della Direzione***

Il capitolo 7 definisce gli elementi in ingresso/uscita per il riesame della Direzione.

Il riesame della Direzione deve essere condotto con frequenza almeno annuale al fine di assicurare che il SGSI sia: idoneo, adeguato ed efficace secondo quanto prescritto nei documenti e nelle politiche per la sicurezza delle informazioni dell'organizzazione.

Tra gli elementi in ingresso:

- risultati degli audit interni e dei riesami del SGSI;
- feedback provenienti dalle parti interessate;
- tecniche, prodotti o procedure, utilizzabili per migliorare le prestazioni e l'efficacia del SGSI;
- stato delle azioni preventive e correttive;
- vulnerabilità o minacce non adeguatamente affrontate della precedente valutazione del rischio;
- risultati delle misurazioni dell'efficacia;
- azioni a seguire dai precedenti riesami da parte della Direzione;
- cambiamenti che potrebbero avere effetto sul SGSI;
- raccomandazioni per il miglioramento.

Tra gli elementi in uscita:

- attività per il miglioramento dell'efficacia del SGSI;
- aggiornamento della valutazione dei rischi e del piano per il trattamento dei rischi;
- modifiche delle procedure e dei controlli che incidono sulla sicurezza delle informazioni per rispondere a eventi interni o esterni che possono avere un impatto sul SGSI, compresi cambiamenti;
- eventuali necessità di risorse;
- miglioramento della misura dell'efficacia dei controlli.

---

<sup>11</sup> La dimostrazione di efficacia è parte integrante del SGSI pertanto la conformità può essere ottenuta solo a fronte della dimostrazione di efficacia del SGSI e delle contromisure attuate.

<sup>12</sup> In generale le procedure documentate sono richieste a fronte di attività/processi normalmente estranei alle organizzazioni o comunque strettamente collegate all'adozione di uno standard ISO senza il quale tali attività/processi non è detto che siano presenti.

## 2.12. **Analisi dei requisiti – 8 Miglioramento del SGSI**

Il capitolo 8 include gli aspetti inerenti:

- Il miglioramento continuo:
  - della politica per la sicurezza delle informazioni,
  - degli obiettivi per la sicurezza delle informazioni,
  - dei risultati degli audit,
  - dell'analisi degli eventi monitorati,
  - delle azioni correttive e preventive,
  - del riesame da parte della direzione.
- La gestione delle azioni correttive e preventive, per entrambe viene richiesta la preparazione di una procedura documentata.

## 2.13. **L'allegato A – I controlli**

L'allegato A è l'unico allegato “normativo” cioè obbligatorio per la corretta implementazione e certificazione del SGSI. In sostanza rappresenta:

- 11 macrocategorie di aspetti inerenti la sicurezza delle informazioni;
- 39 obiettivi (a loro volta suddivisi in 133 contromisure o controlli) utili per la riduzione/mitigazione dei rischi individuati nella fase di valutazione dei rischi.

Ciascuna macrocategoria fissa un argomento (ad esempio A.8 sicurezza delle risorse umane) ed all'interno di questo definisce gli obiettivi per la sicurezza (nel nostro esempio definisce 3 obiettivi di controllo: prima, durante e dopo l'impiego della persona all'interno del SGSI). Ciascun obiettivo è quindi esploso in dettagli operativi (ad esempio: A.8.1.1 Ruoli e responsabilità).

Quindi una struttura logica orientata ad individuare potenziali soluzioni organizzative (e talvolta tecniche) a fronte di rischi valutati e relativi danni potenziali alle informazioni.

La seguente figura raccoglie gli esempi sopra citati:

<b>A.8 Sicurezza delle risorse umane</b>		
<b>A.8.1 Prima dell'impiego</b> <i>Obiettivo:</i> garantire che impiegati, contraenti e utenti comprendano le proprie responsabilità, e siano idonei per i ruoli per i quali sono presi in considerazione, e per ridurre il rischio di furto, frode o uso improprio degli impianti.		
A.8.1.1	Ruoli e responsabilità	<i>Controllo</i> Si devono definire e documentare i ruoli e le responsabilità per la sicurezza degli impiegati, dei contraenti e degli utenti terze parti secondo la politica per la sicurezza delle informazioni dell'organizzazione.
A.8.1.2	Scrutinio	<i>Controllo</i> Si devono fare dei controlli di verifica sui dati di tutti i candidati per l'impiego, i contraenti e gli utenti terze parti secondo le leggi, i regolamenti e l'etica pertinenti, e in proporzione ai requisiti aziendali, alla classificazione delle informazioni cui avere accesso e ai rischi percepiti.
A.8.1.3	Condizioni di impiego	<i>Controllo</i> Impiegati, contraenti e utenti terze parti devono concordare e firmare le condizioni d'impiego che dovrebbero enunciare le responsabilità loro e dell'organizzazione in merito alla sicurezza delle informazioni.

Inoltre l'allegato A costituisce il collegamento con lo standard ISO/IEC 17799:05, l'uso di quest'ultimo standard deve essere considerato come una raccolta di best practice cui riferirsi per trarre idee e spunti in tema di contromisure.

Lo standard ISO/IEC 17799:05 *non è in alcun modo certificabile*, pertanto la sua utilizzazione è assolutamente libera e priva di legami obbligatori nei confronti di ISO/IEC 27001:05. Anzi, in tal senso è possibile utilizzare standard diversi per coprire gli aspetti citati nell'allegato A della ISO/IEC 27001:05.

#### 2.14. L'allegato B – L'integrazione principi-PDCA-requisiti

Uno degli aspetti innovativi introdotti dallo standard ISO/IEC ISO 27001:05 sta nel fatto che il Comitato normatore ha predisposto una matrice che pone in diretta relazione: le fasi del ciclo PDCA, i principi OCSE ed i requisiti applicativi dello standard; sollevando di fatto gli utilizzatori dello standard dalla ricerca spasmodica, e talvolta infruttuosa, delle interconnessioni e dei legami, creando nel contempo una eccezionale opportunità per progettare e verificare i contenuti del SGSI.

Infatti, l'allegato B contenuto nella ISO/IEC 27001:05 permette di verificare continuamente se il SGSI soddisfa contemporaneamente i tre aspetti: ciclo PDCA, principi OCSE e requisiti applicativi.

La tabella seguente schematizza in breve quanto sopra esposto:

<b>Tabella correlazione: Requisiti ISO 27001:05 - principi OCSE - ciclo PDCA</b>	<b>Consapevolezza</b>	<b>Responsabilità</b>	<b>Risposta</b>	<b>Valutazione rischio</b>	<b>Progettazione e sviluppo della sicurezza</b>	<b>Gestione sicurezza</b>	<b>Rivalutazione</b>
<b>4 Information security management system</b>						<b>PDCA</b>	
4.1 General requirements							
<b>4.2 Establishing and managing the ISMS</b>							
4.2.1 Establish the ISMS			P	P	P		
4.2.2 Implement and operate the ISMS	D				D		
4.2.3 Monitor and review the ISMS		C		C			C
4.2.4 Maintain and improve the ISMS		A					
<b>4.3 Documentation requirements</b>							
4.3.1 General							
4.3.2 Control of documents							
4.3.3 Control of records							
<b>5 Management responsibility</b>							
5.1 Management commitment							
5.2 Resource management					D		
5.2.1 Provision of resources							
5.2.2 Training, awareness and competence	D						
<b>6 Internal ISMS audits</b>		C		C			C
<b>7 Management review of the ISMS</b>							
7.1 General							
7.2 Review input							
7.3 Review output		C		C			C
<b>8 ISMS improvement</b>							
8.1 Continual improvement		A					A
8.2 Corrective action							
8.3 Preventive action		A				A	

### 3. Cosa è ed a cosa serve la ISO/IEC 17799:05

#### 3.1. Obiettivo

È in buona sostanza una raccolta di obiettivi di controllo (finalità) e controlli (contromisure) utilizzabili per ridurre e/o mitigare i rischi individuati.

*Non è uno standard certificabile e non è indispensabile per l'implementazione del SGSI. Deve invece essere considerato come un supporto (o linea guida) per la comprensione ed individuazione delle attività da porre in atto a fronte delle scelte effettuate in materia di riduzione/mitigazione dei rischi valutati.*

Ciascun controllo (o contromisura) citato dall'allegato A della ISO/IEC 27001:05 trova un corrispettivo capitolo di spiegazione e dettaglio nella ISO/IEC 17799:05. Ciascun capitolo è organizzato in modo da definire:

- l'obiettivo del controllo, cioè cosa si vuole ottenere;
- i controlli (o contromisure), cioè quali aspetti occorre considerare per soddisfare l'obiettivo di controllo, ivi inclusi rimandi e riferimenti ad altra letteratura.

Ad esempio, nella ISO/IEC 27001:05 troviamo:

<b>A.10.9 Servizi per il commercio elettronico</b> <i>Obiettivo: garantire la sicurezza dei servizi per il commercio elettronico e il loro uso sicuro.</i>		
A.10.9.1	Commercio elettronico	<b>Controllo</b> <i>Le informazioni coinvolte nel commercio elettronico che passano in reti pubbliche devono essere protette da attività fraudolenta, dispute contrattuali, e da divulgazione e modifica non autorizzate.</i>

Nel corrispondente capitolo della ISO/IEC 17799:05 troveremo:

#### **10.9 Servizi per il commercio elettronico**

*Obiettivo: garantire la sicurezza dei servizi per il commercio elettronico e il loro uso sicuro.*

*Si dovrebbero prendere in considerazione le implicazioni per la sicurezza associate all'uso dei servizi per il commercio elettronico, comprese le transazioni on-line, e i requisiti per i controlli. Si dovrebbero prendere in considerazione anche l'integrità e la disponibilità delle informazioni pubblicate elettronicamente tramite sistemi disponibili al pubblico.*

#### **10.9.1 Commercio elettronico**

##### Controllo

*Le informazioni coinvolte nel commercio elettronico che passano in reti pubbliche dovrebbero essere protette da attività fraudolenta, dispute contrattuali, e da divulgazione e modifica non autorizzate.*

##### Guida all'attuazione

*Le considerazioni inerenti la sicurezza per il commercio elettronico dovrebbero comprendere quanto segue:*

- a) *Il livello di riservatezza che ogni parte richiede relativamente all'identità dichiarata reciprocamente, p.e. tramite autenticazione*
- b) *Processo di autorizzazione associato a chi può stabilire i prezzi, emettere o firmare documenti commerciali chiave;*
- c) *Garantire che i contraenti siano informati appieno delle loro autorizzazioni;*
- d) *Determinare e soddisfare i requisiti di riservatezza, integrità, prova di consegna e ricevimento dei documenti chiave e del non misconoscimento dei contratti, p.e. associati a processi d'asta e contrattuali;*
- e) *Il livello di fiducia necessario nell'integrità dei listini prezzi pubblicizzato;*
- f) *La riservatezza di eventuali informazioni o dati delicati;*
- g) *Riservatezza e integrità degli ordini, delle informazioni di pagamento, dell'indirizzo di consegna e della conferma di ricevimento;*

- h) Il grado di verifica appropriato per controllare le informazioni di pagamento fornite da un cliente;
- i) Scegliere la forma più appropriata di pagamento per salvaguardarsi contro la frode;
- j) Il livello di protezione necessario per mantenere la riservatezza e l'integrità delle informazioni dell'ordine;
- k) L'evitare la perdita o la duplicazione delle informazioni della transazione;
- l) Responsabilità associata a eventuali transazioni fraudolente;
- m) Requisiti assicurativi.

Molte delle considerazioni qui sopra possono essere affrontate con l'applicazione di controlli crittografici (v. 12.3), tenendo conto della conformità ai requisiti legali (v. 15.1, in particolare 15.1.6 per la legislazione sulla crittografia).

Le disposizioni per il commercio elettronico tra parti dovrebbero essere sostenute da un accordo documentato che impegni entrambe le parti ai termini concordati, compresi i dettagli sull'autorizzazione [vedi item b) sopra]. Possono essere necessari ulteriori accordi con i servizi d'informazione e con i fornitori di reti apportatrici di valore.

I sistemi di commercio pubblici dovrebbero pubblicare i propri criteri/requisiti ai clienti.

Si dovrebbe prendere in considerazione la resistenza agli attacchi dello host usato per il commercio elettronico, e alle implicazioni per la sicurezza di eventuali interconnessioni di rete necessarie per l'attuazione dei servizi per il commercio elettronico (v. 9.4.7).

#### Altre informazioni

Il commercio elettronico è vulnerabile a numerose minacce di rete possono avere come conseguenza attività fraudolenta, dispute contrattuali, e da divulgazione o modifica delle informazioni.

Il commercio elettronico può avvalersi di metodi per l'autenticazione sicura, p.e. usando chiavi crittografiche pubbliche e firme digitali (v. anche 12.3) per ridurre i rischi. Inoltre, se tali servizi sono necessari, si possono usare terze parti fidate.

Come si può facilmente notare il contenuto della ISO/IEC 17799:05 è fortemente esplicativo e pone in relazione il controllo (o contromisura) con altri controlli o aspetti del SGSI. Quindi una valida guida per una efficace comprensione ed applicazione di un aspetto specifico della sicurezza delle informazioni.

### **3.2. Struttura**

Questa guida è strutturata in 15 capitoli, i primi 4 capitoli introducono all'utilizzazione del documento mentre gli altri 11 richiamano i controlli (o contromisure) dell'allegato A della ISO/IEC 27001:05.

Ciascuno degli 11 capitoli (dette *clause*) affronta un tema della sicurezza delle informazioni:

- **5 Politica della sicurezza**
- **6 Organizzazione della sicurezza delle informazioni**
- **7 Gestione dei beni**
- **8 Sicurezza delle risorse umane**
- **9 Sicurezza fisica e ambientale**
- **10 Gestione delle comunicazioni e delle operazioni**
- **11 Controllo accessi**
- **12 Acquisizione, sviluppo e manutenzione dei sistemi informativi**
- **13 Gestione degli incidenti della sicurezza delle informazioni**
- **14 Gestione della continuità del business**
- **15 Conformità**

Ciascun capitolo a sua volta si compone di più paragrafi (detti *categorie*), in totale sono state definite 39 categorie. All'interno di ciascun paragrafo (o categoria) vengono trattati i controlli (o contromisure), che in totale risultano essere 133.

Ciascun controllo (o contromisura) può a sua volta richiamare altri controlli per ampliare la trattazione del tema.

### **3.3. Alternative**

Non essendo uno standard obbligatorio per l'implementazione del SGSI possiamo affermare che potenzialmente esistono infinite alternative, tante quante sono le libere interpretazioni dell'allegato A della ISO/IEC 27001:05.

Piuttosto potrebbe essere interessante valutare le contromisure suggerite in documenti di settore, di mercato e/o derivanti da letteratura internazionale.

#### 4. Le altre norme della famiglia ISO 27000

Il Comitato ISO JTC1 SC27 WG1 ha pianificato i successivi sviluppi della famiglia ISO 27000. L'attuale situazione è in sostanza rappresentabile come segue:

ISO 27000	Principi e vocabolario (aprile 2007)
ISO 27002	Ex ISO/IEC 17799:05 (aprile 2007)
ISO 27003	Guida all'implementazione (aprile 2007)
ISO 27004	Misura della sicurezza delle informazioni (aprile 2007)
ISO 27005	Gestione del rischio per i SGSI (aprile 2007)
ISO 27006	Guida per gli OdC/OdA alla valutazione di conformità dei SGSI (gennaio 2007)
Da ISO 27007 a ISO 27009	Non ancora assegnate
Da ISO 27010 a ISO 27019	Normazione della sicurezza delle informazioni in settori specifici (sanità, finanza, industria, aerospaziale, automobilistico ecc.) <sup>13</sup> assegnazioni e tempi da definire
Da ISO 27030 a ISO 27044	Normazione di aspetti tecnici della sicurezza delle informazioni (IT network security, Intrusion Detection Systems, Disaster Recovery, Business Continuità, Cyber Security, Outsourcing, Trusted Third Party ecc.) <sup>14</sup> assegnazioni e tempi da definire

Sono inoltre in fase di definizione accordi (liaison) con associazioni e gruppi di interesse internazionali per l'integrazione della famiglia ISO 27000 con altri standard (ad es. IEEE).

##### 4.1. Prossime scadenze

Le prossime scadenze (e impegni) del Comitato ISO sono disponibili on line all'indirizzo [www.iso.ch](http://www.iso.ch).

---

<sup>13</sup> Alcuni gruppi sono già al lavoro, ad esempio: ISO TC 68 sugli aspetti bancari-finanziari.

<sup>14</sup> Alcune norme sono già state pubblicate sotto altri numeri e verranno trasferite per mantenere il riferimento al tema sicurezza delle informazioni.

## 5. Cosa cambia rispetto alla BS7799-2:02

### 5.1. Le innovazioni

Come abbiamo visto nei paragrafi precedenti la norma del British Standard è stata convertita in ISO e pubblicata nel dicembre del 2005.

La pubblicazione come norma ISO comporta l'automatico allineamento ad altre norme inerenti i sistemi di gestione (come ad esempio quelle per la qualità e l'ambiente) ed in particolare:

- Adozione del modello PDCA
- Approccio per processi
- Introduzione di procedure documentate a supporto dell'approccio sistemico

Inoltre sono state apportate modifiche derivanti da aggiornamenti tecnici ed eventuali errori della precedente versione.

### 5.2. Le differenze

La sostanziale differenza è incentrata sulla *misurabilità*:

- del rischio,
- dell'efficacia del SGSI,
- dell'efficacia delle contromisure adottate a fronte dei rischi individuati.

Sono stati chiariti ed implementati gli aspetti inerenti:

- ruolo della Direzione nella fase di progettazione del SGSI;
- la definizione dello scopo, con particolare enfasi:
  - alla politica sulla sicurezza per le informazioni,
  - al perimetro del SGSI,
  - all'identificazione degli assets (beni) inclusi nel SGSI,
  - alle interfacce,
  - alle interdipendenze organizzative,
  - all'outsourcing;
- l'approccio alla valutazione dei rischi, in termini di:
  - comparabilità e riproducibilità dei risultati ottenuti,
  - perdite e impatti sul business,
  - esposizione al rischio,
  - livello di rischio residuo ed accettabile;
- le opzioni per il trattamento dei rischi;
- la selezione delle contromisure;
- la dichiarazione di applicabilità;
- il piano di trattamento dei rischi;
- il riesame dei rischi (in termini di ripetibilità del processo e congruità dei risultati).

### 5.3. La misurabilità

L'aspetto della misurabilità del SGSI è stato fortemente enfatizzato, tanto da prevedere:

- un documento del British Standard di supporto: *BIP 074 Guidelines on Measuring the Effectiveness of ISMS (Information security management system) Implementations*
- una linea guida ISO 27004 prevista per il prossimo aprile 2007.

La misurabilità è intesa come:

- identificazione:
  - degli oggetti di misurazione:
    - un particolare processo del SGSI,
    - una contromisura o un gruppo di contromisure adottate;

- dei metodi di misura;
- della frequenza di misurazione;
- dei criteri di misura;
- procedure per la definizione dei dati da raccogliere, delle analisi da condurre e dei report da produrre;
- misurazione ed eventuale miglioramento.

## 6. La certificazione dei SGSI

### 6.1. Obiettivo

La certificazione di un Sistema di Gestione per la Sicurezza delle Informazioni (o SGSI) è un passo importante per qualunque tipo di organizzazione: pubblica o privata, piccola o grande. E' il primo passo verso una visione consapevole della sicurezza delle informazioni e verso la valorizzazione commerciale del livello di sicurezza raggiunto.

Un SGSI viene implementato principalmente per permettere alla propria azienda di avere una visione "sistemica" della sicurezza delle informazioni, basandosi su uno o più standard internazionali. La certificazione è quindi, prima di tutto, una necessità interna.

L'aspetto commerciale non è però del tutto trascurabile, anzi il più delle volte costituisce la spinta principale per "investire in sicurezza".

Formalmente la certificazione permette *l'inserimento dell'organizzazione (o azienda) all'interno di un "registro delle organizzazioni certificate"*.

Vale a dire che il nome ed i dati dell'azienda (ragione sociale, indirizzo dei siti, attività certificata) vengono pubblicati mediante collocazione all'interno di registri pubblici gestiti dagli Organismi di Certificazione (OdC) e/o dagli Organismi di Accreditamento (OdA).

Tale operazione fornisce visibilità all'azienda collocandola in una vetrina per un mercato potenziale esteso oltre i confini nazionali. I registri infatti sono solitamente pubblicati su web o comunque facilmente accessibili mediante richiesta diretta agli OdC e/o agli OdA.

Nel caso dei SGSI la pubblicazione di tali dati potrebbe però costituire una prima informazione utilizzabile da malintenzionati o da "dilettanti allo sbaraglio" il cui unico obiettivo è l'introduzione in un Sistema per potersene vantare all'interno delle comunità underground. Per questo motivo alcune certificazioni, su richiesta dell'organizzazione, non vengono pubblicate; la prima certificazione ISO/IEC 27001:05 rilasciata in Italia è stata posta sotto veto dall'organizzazione stessa proprio perché consapevole del rischio insito nella pubblicazione di alcune informazioni che avrebbero potuto "svelare" le attività ed i siti in cui queste si svolgono. Certificazione quindi come conoscenza della propria sicurezza, come valorizzazione dei propri sforzi di implementazione del SGSI, come opportunità di ampliamento del mercato e soprattutto come consapevole visibilità dell'azienda nel mercato.

### 6.2. Significato

Certificarsi significa:

- aderire ad uno standard di riferimento (la ISO/IEC 27001:05 nel nostro caso),
- analizzare, interpretare ed implementare quanto richiesto dallo standard,
- dimostrare la conformità allo standard per mezzo di "evidenze oggettive";
- dimostrare l'efficacia del SGSI nel raggiungere quanto definito in materia di sicurezza delle informazioni.

Questi semplici passi sono in realtà costituiti da una serie di attività che occorre porre in atto affinché tutto vada nel verso giusto.

E' lo stesso standard che in generale mette a disposizione le informazioni necessarie per poter operare al meglio, ad esempio la sequenza dei requisiti della ISO/IEC 27001:05 è sviluppata proprio in tal senso ed è prevista la pubblicazione dello standard ISO/IEC 27003 per guidare le organizzazioni interessate verso l'implementazione di un SGSI e per la sua certificazione.

In generale tutti gli standard prevedono delle guide a corollario della norma principale, tali guide non risultano utilizzabili per la certificazione ma costituiscono un valido aiuto per il lavoro operativo. In alternativa ci si dovrà avvalere di consulenti competenti che possano guidare in egual misura l'organizzazione lungo il cammino della certificazione.

### **6.3. Valenza**

Parlando degli obiettivi abbiamo già accennato alla valenza commerciale della certificazione. Qui vogliamo riprendere il discorso sotto un punto di vista puramente speculativo, elaborando alcune riflessioni e riportando esperienze raccolte in campo.

La certificazione dei SGSI si connota, per ora, come una anomalia all'interno del mondo delle certificazioni, principalmente perché la certificazione ISO/IEC 27001:05 non è richiesta per gare o contratti. Ciò la rende qualcosa di utile per l'organizzazione al di là delle possibilità di sfruttamento offerte dal mercato.

Almeno questo è il parere di molti degli imprenditori e dei manager a capo di organizzazioni certificate.

La carenza di consulenti, competenti in materia, e la fortissima influenza dell'ICT completano il quadro di un mercato emergente con potenzialità rilevanti.

Ovviamente la trasformazione da BS7799-2:02 a ISO/IEC 27001:05 comporta una visione ed una valutazione diversa dello standard e del suo potenziale sfruttamento.

Il fatto stesso che si tratti di una norma internazionale a livello ISO la rende appetibile anche per gli usi contrattuali poiché applicabile e riconosciuta in tutto il mondo. Ciò significa che a breve anche questo standard entrerà a far parte delle richieste di routine per bandi e appalti pubblici così come di contrattazione tra privati.

### **6.4. Efficacia vs conformità**

Lo standard ISO/IEC 27001:05 prevede sia la conformità sia l'efficacia di un SGSI, cioè non si limita alla mera rispondenza delle attività con la norma ma anche, e soprattutto, all'efficacia della sicurezza, laddove per efficacia si intende la capacità del SGSI di raggiungere gli obiettivi ed i livelli di sicurezza definiti dall'organizzazione e da essa ritenuti consoni in relazione al mercato, alle proprie esigenze economiche e tecnologiche, alle leggi applicabili ecc.

Un SGSI deve prima di tutto essere efficace, cioè utile all'organizzazione per assicurare la sicurezza delle informazioni necessaria, successivamente si potrà parlare di conformità alla norma.

“Un sistema inefficace ma conforme è certificabile?” ovviamente non dovrebbe esserlo visto che soddisfa solo una delle condizioni tracciate dalla stessa norma. Il condizionale è però d'obbligo essendo l'efficacia definita dall'organizzazione stessa e non strettamente collegata a parametri comuni.

La conformità è invece l'aspetto più plastico dello standard: poche cose sono rese obbligatorie dall'adozione di uno standard ISO, il resto è per lo più lasciato all'inventiva ed alla capacità dell'organizzazione di collegare, sfruttare al massimo quanto in suo possesso per dimostrare il rispetto di regole generali e/o convenzionali. Ad esempio: questo standard non prevede l'uso di un “manuale”, le “procedure” obbligatorie sono ridotte al minimo indispensabile proprio per favorire e sviluppare le capacità delle organizzazioni di produrre e raccogliere evidenze oggettive che comprovino quanto posto in atto in termini di sicurezza delle informazioni.

Di contro il concetto di efficacia è richiamato più volte proprio per sviluppare la consapevolezza e lo spirito critico dell'organizzazione sui temi della sicurezza, della valutazione del rischio, sui risultati ottenuti, sui costi, sui rischi residui e su quelli accettabili ecc.

A titolo informativo si consideri la possibilità di utilizzare la ISO/IEC 27004 (di prossima pubblicazione) per maggiori informazioni circa la misurazione della sicurezza di un SGSI.

## 7. Come certificarsi ISO/IEC 27001:05

### 7.1. I passi da fare per implementare il SGSI

Come abbiamo detto l'implementazione del SGSI è un passo importante, sia in termini economici sia in termini di immagine.

I passi per l'implementazione del SGSI sono direttamente tracciati dallo standard (nel req. 4.2.1) che guida in modo puntuale nella corretta sequenza delle fasi:

- Definire l'ampiezza ed i confini del SGSI.
- Definire una politica.
- Identificare una metodologia per la valutazione del rischio.
- Sviluppare criteri per l'accettazione del rischio (sfruttando ad esempio la ISO/IEC 27005 di prossima pubblicazione).
- Identificare i livelli di rischio accettabili.
- Identificare i beni all'interno dell'ampiezza del SGSI e i responsabili di tali beni.
- Identificare le minacce, le vulnerabilità e gli impatti che la perdita di riservatezza, integrità e disponibilità potrebbe avere sui beni.
- Valutare le realistiche probabilità che si verificano avarie della sicurezza.
- Stimare i livelli dei rischi.
- Determinare se il rischio sia accettabile o richieda un trattamento.
- Identificare e stimare le opzioni per il trattamento dei rischi.
- Scegliere controlli e obiettivi del controllo per il trattamento dei rischi.
- Ottenere l'approvazione da parte della direzione per i rischi residui.
- Ottenere l'autorizzazione da parte della direzione per attuare e operare il SGSI.
- Preparare una Dichiarazione di Applicabilità.

Alcuni di questi argomenti meritano un approfondimento per evitare errori nelle fasi di implementazione.

In generale la ISO 13335 contiene informazioni sufficienti in materia, tuttavia si ritiene utile una breve sintesi dettata dall'esperienza internazionale.

#### 7.1.1. Campo di applicazione

Per campo di applicazione si intende generalmente il testo che verrà inserito all'interno del certificato e che descriverà al mondo esterno quali attività, processi, servizi e/o applicazioni sono oggetto di certificazione. Quindi si tratta di un dato rilevante, sia per gli scopi commerciali sia per l'esatta calibratura del SGSI e dei relativi aspetti tecnico-gestionali.

L'esperienza raccomanda una attenta individuazione sulla base delle esigenze aziendali, del mercato, delle tecnologie e dalle legislazioni applicabili in materia di sicurezza delle informazioni.

Non vi sono obblighi formali, il campo di applicazione deve essere sostanzialmente credibile e riferibile alle attività dell'organizzazione anche in riferimento alle politiche definite.

Il campo di applicazione può essere via via ridefinito, aggiustato mano a mano che si acquisisce maggior consapevolezza dell'importanza di questo dato. Vale a dire che il campo di applicazione può essere ridefinito più volte fin quando non coincide con le necessità dell'organizzazione. Vista l'impostazione della norma è possibile certificare anche processi interni (gestione del personale, contabilità ecc.) essendo la sicurezza delle informazioni riferibile a qualsiasi contesto.

Il campo di applicazione di un SGSI raramente coincide con eventuali processi certificati con altri standard ISO (ISO 9001, ISO 14001, ISO 18001 ecc.). Infatti non è detto che il flusso delle informazioni da porre in sicurezza si riferisca ad un processo produttivo "visibile" dal mondo esterno.

### **7.1.2.Ampiezza**

L'ampiezza di un SGSI definisce gli aspetti fisici e logici, i siti, le infrastrutture e tutto quanto necessario per definire un "perimetro" all'interno del quale varranno le regole definite dall'implementazione del SGSI. Ivi inclusi gli aspetti di interazione con entità esterne (fornitori, clienti, outsourcer ecc.). La definizione corretta dell'ampiezza può comportare vari cicli di analisi fino a far combaciare le aspettative dell'organizzazione con gli aspetti tecnici, organizzativi e gestionali del SGSI. Campo di applicazione ed ampiezza dipendono spesso l'uno dall'altro, pertanto modificando l'uno si ottiene la modifica indotta dell'altro.

### **7.1.3.Politica**

La politica della sicurezza di un'organizzazione può andare dalle declaratorie generali, definite dal top management, fino alle politiche operative. Comunque si potrebbe parlare di politica. Molte organizzazioni stratificano la politica in più livelli: strategico, tattico e operativo. Aziende piccole tendono invece ad avere una sola politica.

In ogni caso le informazioni minime che la politica deve evidenziare sono:

- 1) gli obiettivi per la sicurezza delle informazioni;
- 2) le linee di indirizzo ed i principi generali per quanto riguarda la sicurezza delle informazioni;
- 3) i requisiti aziendali, legali/coagenti e obbligazioni contrattuali inerenti la sicurezza delle informazioni;
- 4) i riferimenti alla gestione dei rischi;
- 5) i criteri a fronte dei quali si stimeranno i rischi;

La politica deve essere approvata dalla Direzione<sup>15</sup> e riesaminata periodicamente.

### **7.1.4. Analisi e valutazione dei rischi<sup>16</sup>**

Definizione dei criteri e delle modalità per l'identificazione, per l'analisi e la valutazione dei rischi inerenti i beni all'interno del perimetro (per maggiori informazioni su tali attività riferirsi alla ISO/IEC 27005 di prossima pubblicazione).

Spesso le organizzazioni impiegano metodologie e/o prodotti per supportare l'analisi e la valutazione dei rischi, in questi casi si potrà far riferimento al manuale d'uso o comunque alla letteratura di riferimento, purché se ne comprendano effettivamente limiti e scelte. Troppo spesso infatti si è assistito a valutazioni eseguite senza aver compreso i meccanismi adottati generando così scelte ambigue (se non controproducenti in termini economici e di sicurezza) per un semplice errore di impostazione o di setting del modello/software utilizzato.

### **7.1.5.Dichiarazione di applicabilità**

E' il documento che descrive quanti e quali contromisure sono state adottate per far fronte ai rischi individuati. Dovrebbe essere riferita all'allegato A della norma o comunque farvi riferimento in modo tale da permetterne la verifica.

E' previsto altresì che la Dichiarazione di Applicabilità (detta SoA da Statement of Applicability) evidenzi anche le motivazioni per l'esclusione e per la scelta delle contromisure.

Da notare che, per effetto dell'attuale sistema di accreditamento e certificazione, i riferimenti di questo documento vengono inseriti nell'eventuale certificato, in tal modo una informazione del SGSI viene trasmessa al mondo esterno e potenzialmente potrebbe aprire una nuova vulnerabilità (i potenziali attaccanti saprebbero quale documento cercare per

---

<sup>15</sup> Per direzione si intende il livello gerarchico-funzionale più alto dell'organizzazione, generalmente interna al perimetro.

<sup>16</sup> Per una maggior chiarezza terminologica si consideri la ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards e la ISO/IEC 27000 di prossima pubblicazione.

capire le contromisure attivate e non!). Molte organizzazioni hanno quindi posto in atto degli artifici che rendono di fatto inutilizzabile il riferimento posto sul certificato.

#### **7.1.6. La scelta dei controlli**

La scelta dei controlli dall'allegato A deve essere effettuata sulla base dei risultati della valutazione dei rischi e sulla base delle opzioni di trattamento (elusione, trasferimento, accettazione e/o riduzione/mitigazione del rischio) decise in sede di gestione del rischio. Ciascuno dei controlli dell'allegato A può essere utilizzato, eventualmente combinato con ulteriori trattamenti, per ridurre i fattori di rischio oppure per mitigare gli effetti di eventuali impatti.

Possono anche essere inserite contromisure "proprietarie", cioè create ad hoc per la gestione di determinati rischi. In tal caso queste sono considerate aggiuntive a quelle già previste nell'allegato A.

Naturalmente non è obbligatorio utilizzare i controlli descritti nell'allegato A, in tal caso occorrerà però giustificarne l'esclusione.

La dichiarazione di applicabilità ha proprio il compito di raccogliere i controlli (o contromisure) adottate rispetto all'allegato A incluse le motivazioni di inclusione ed esclusione.

### **7.2. I passi per identificare e scegliere l'Organismo di Certificazione (OdC)**

Alla luce di quanto esposto nei capitoli precedenti risulta chiaro quanto possa essere critica la scelta dell'OdC appropriato. Come districarsi in questo mercato?

Prima di tutto dobbiamo distinguere tra OdC accreditati e non<sup>17</sup>. Il peso di tale informazione sarà chiarito nei capitoli successivi.

In seconda istanza occorrerà valutare le "referenze" dell'OdC, cioè il numero e la tipologia dei certificati già emessi. Maggiore è la varietà e la quantità maggiore sarà la capacità degli auditor di "leggere" e comprendere la sicurezza dell'organizzazione, prescindendo da preconcetti e fraintendimenti di interpretazione dello standard.

Infine occorrerà accertarsi delle reali competenze possedute dal potenziale team di audit: qualifiche, eventuali certificazioni possedute, esperienze pregresse nell'audit dei SGSI, tipo di relazioni con l'OdC (alcuni auditor non sono dipendenti dell'OdC e pertanto alcune limitazioni contrattuali sulla sicurezza e riservatezza potrebbero non essere sufficienti a tutelare l'organizzazione da "fughe di notizie" in merito al proprio SGSI).

### **7.3. Audit preliminare**

In tal senso potrebbe essere utile prevedere un audit preliminare (detto anche pre audit o pre assessment) per "misurare" in qualche modo il team di audit in relazione alle necessità dell'organizzazione e per ricevere un primo feedback sul SGSI. L'audit preliminare non fa parte del processo di certificazione e può essere eseguito solo in determinate circostanze (essendo particolarmente critico per un OdC) infatti viene contrattualizzato in modo diverso e generalmente deve essere eseguito prima dell'inizio del processo di certificazione.

L'audit preliminare è una splendida opportunità per vedere il team all'opera e per ottenere una prima valutazione senza l'ansia della certificazione. In generale l'audit preliminare permette di intraprendere il processo di certificazione senza sorprese e può rivelarsi particolarmente utile quando l'azienda deve raggiungere l'obiettivo entro tempi definiti (ad esempio per soddisfare una richiesta contrattuale).

---

<sup>17</sup> Per maggiori informazioni consultare il sito [www.sincert.it](http://www.sincert.it) nell'area: banca dati, organismi di certificazione.

L'audit preliminare ha una durata inferiore rispetto a quello che sarà poi l'audit di certificazione e produce, in genere, un rapporto di massima sui vari aspetti del SGSI evidenziando eventuali criticità che possano in qualche modo ostacolare il processo di certificazione.

#### 7.4. Il processo di certificazione

Una volta identificato l'OdC e stipulato il contratto di certificazione si avrà di fronte un processo sostanzialmente indipendente dall'OdC, derivante dall'applicazione di vari standard internazionali (descritti nella ISO/IEC 27006 di prossima pubblicazione).

Tutti gli audit per i Sistemi di gestione (inclusi i SGSI) si svolgono secondo quanto prescritto:

- dalla linea guida UNI EN ISO 19011:03
- dal regolamento dell'OdC riguardo i SGSI
- dai regolamenti tecnici dell'Oda (generali e specifici per il settore).

Nei prossimi paragrafi analizzeremo alcune fasi tipiche degli audit applicabili ai SGSI.

##### 7.4.1. Quanto può durare un audit

Il numero di “giorni persona” necessari per la valutazione di un SGSI dipende da vari fattori: numero di persone coinvolte, numero di siti, complessità dei processi ecc. Esiste un algoritmo per il calcolo dei gg/p cui tutti gli OdC devono attenersi, è pertanto possibile ipotizzare una quantificazione di massima degli impegni semplicemente applicando una formula<sup>18</sup>. La tabella di base per il calcolo è la seguente:

people	man days
1-10	2
11-25	3
26-45	4
46-65	5
66-85	6
86-125	7
126-175	8
176-275	9
276-425	10
426-625	11
626-875	12
876-1175	13
1176-1550	14
1551-2025	15
2026-2675	16
2676-3450	17
3451-4350	18
4351-5450	19
5451-6800	20
6801-8500	21
8501-10700	22
>10700	follow progression above

Come è possibile notare si tratta di fasce numeriche entro le quali collocare il numero di persone coinvolte nel SGSI e sulla base del numero ottenuto inserire i fattori correttivi per complessità e numero di siti.

Il costo giornaliero per auditor è invece dipendente da vari fattori tra i quali: la competenza del team di audit, le politiche dell'OdC in materia di trattamento economico degli auditor, la richiesta e l'offerta del mercato ecc.

<sup>18</sup> Per maggiori informazioni riferirsi al regolamento dell'OdC, alla EA-7/01 • EA Guidelines on the Application of EN 45012; ed alla EA-7/03 - EA Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems

E' possibile cambiare OdC in qualsiasi momento esistendo un protocollo internazionale che regola il passaggio tra OdC diversi, può quindi essere valutata la possibilità di cambiare l'OdC in modo ciclico per valutare le diverse competenze e conoscenze mettendo così a frutto i risultati degli audit e l'esperienza dei vari team di audit. In tal senso c'è comunque da evidenziare come un team di audit possa impiegare più audit per comprendere pienamente un SGSI e come l'apporto positivo possa emergere solo a valle di un ciclo di audit.

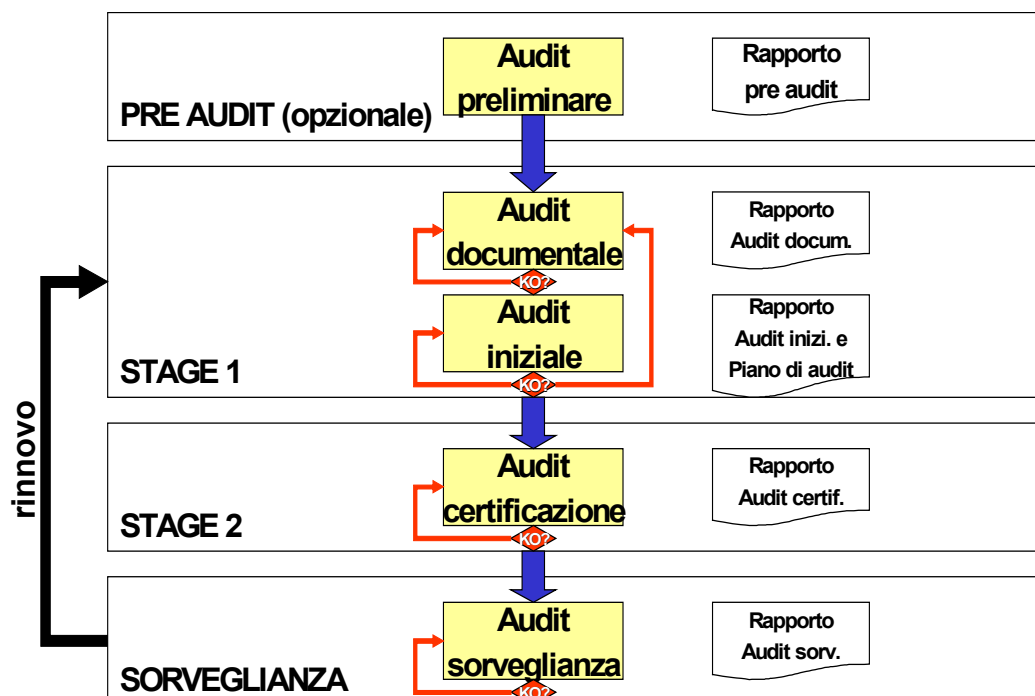
Le valutazioni degli OdC possono dunque differire anche in modo sensibile in termini di costo economico ed approccio mentre saranno sostanzialmente identiche in termini di "effort" operativo, essendo legato ad una formula.

Diverso invece è il discorso di competenze del team, l'unico modo per ovviare è cercare di ottenere quante più informazioni possibili sulle competenze dei singoli membri del team di audit in materia di sicurezza delle informazioni.

Altro fattore da tenere in considerazione è il numero di auditor nel team: un numero maggiore di auditor può abbreviare il numero complessivo di giorni solari in campo sebbene questo possa costituire un fattore di appesantimento nelle attività di allineamento tra gli auditor (maggiori momenti di scambio di informazioni per "incrociare" i dati raccolti ed avere una visione più congrua del SGSI).

Il processo di audit è suddiviso in due macro fasi, ciascuna fase produce una valutazione che ammette alla fase successiva del processo. Il lasso di tempo massimo che intercorre tra le fasi è generalmente fissato a livello contrattuale e corrisponde all'incirca ad un semestre. Per entrambe le fasi è ovviamente prevista l'esecuzione "in campo", cioè presso l'organizzazione.

Schema di massima del processo di certificazione:



#### 7.4.2.Fase 1 (o audit documentale)

Durante questa fase vengono eseguite:

- la valutazione del sistema documentale dell'organizzazione, secondo quanto richiesto dal req. 4.3.1 dello standard e dal regolamento dell'OdC (il regolamento viene fornito all'atto della stipula del contratto ed è parte integrante di questo).
- La valutazione iniziale del SGSI per valutare gli aspetti legali/cogenti applicabili e se sussistano le condizioni per proseguire nel processo di certificazione.

L'esito di queste valutazioni viene solitamente inserito in un apposito rapporto che conterrà punti di forza e di debolezza del SGSI.

Ne consegue che in caso di esito negativo si dovrà ripetere la fase fino alla completa risoluzione delle situazioni che ostano al proseguimento del processo.

In caso di esito positivo verrà redatto il piano per l'esecuzione della fase 2 (piano dell'audit di certificazione) che costituirà l'agenda degli incontri e degli argomenti per l'audit di certificazione.

Di particolare rilievo è il fatto che il SGSI deve dimostrare di essere conforme ed efficace in ogni suo aspetto, deve cioè dimostrare di aver completato un numero di cicli sufficienti a dimostrare anche la capacità di migliorarsi.

In ogni caso l'audit di certificazione di fase 2 è possibile se e solo se:

- sono stati effettuati tutti gli audit interni programmati e necessari affinché la Direzione abbia una corretta visione e consapevolezza dello stato del SGSI in termini di conformità ed efficacia;
- la Direzione ha eseguito il *riesame* del SGSI durante il quale la Direzione diviene effettivamente consapevole della situazione, soprattutto in termini di livelli di rischio (residuo e accettabile).
- 

#### 7.4.3.Fase 2 (o audit di certificazione)

L'audit di certificazione consente al team di audit dell'OdC di valutare la conformità (e l'efficacia) del SGSI dell'organizzazione. E' importante ricordare che gli audit degli OdC si svolgono "a campione", cioè le valutazioni si riferiscono solamente alle parti di SGSI verificate direttamente e che, pertanto, la valutazione non è da considerarsi esaustiva o affidabilistica<sup>19</sup>. Come si dice "l'audit dà confidenza che il SGSI sia conforme ed efficace nel campione esaminato" e non vi è presunzione di affidabilità nella valutazione eseguita<sup>20</sup>. Forse è questo il tallone d'Achille del sistema di certificazione ma dobbiamo anche ricordare che si tratta pur sempre e comunque di un processo *volontario* a fronte di uno standard "gestionale" e non tecnologico. L'esaustività della valutazione non solo comporterebbe costi rilevanti ma soprattutto condurrebbe alla "clonazione" dei SGSI con ovvio irrigidimento organizzativo e tecnico delle soluzioni ed interpretazioni della norma stessa.

Al termine dell'audit verrà redatto un rapporto di audit che conterrà l'esito della valutazione eseguita. In ogni caso il rapporto di audit verrà sottoposto al Comitato di Certificazione dell'OdC, organo preposto alla effettiva decisione in merito alla certificazione.

E' quindi ovvia la posizione del team di audit, relegata alla sola raccolta e verifica in campo delle evidenze oggettive che comprovano la conformità e l'efficacia del SGSI. Sarà invece il Comitato a decidere sull'esito finale

<sup>19</sup> Il concetto di campionamento si riferisce a documenti, registrazione e/o interviste rilevate durante l'audit.

<sup>20</sup> Le attività di audit per i SGSI si svolgono secondo quanto indicato da: UNI EN ISO 19011:03, ISO 27006 (dal 2007), EA 7/03 e dai documenti tecnici SINCERT.

In caso di esito negativo si dovrà provvedere a correggere le anomalie riscontrate (dette in genere non conformità o osservazioni) prima di poter ripetere l'audit.

In caso di esito positivo l'organizzazione riceverà "certificato ISO/IEC 27001:05" per il proprio SGSI, per le attività citate dal campo di applicazione e riferito al perimetro in esso descritto.

Solo da questo momento l'organizzazione potrà proclamarsi certificata, o meglio potrà dichiarare di avere un *SGSI certificato in conformità allo standard ISO/IEC 27001:05*.

Il tempo che intercorre tra il termine dell'audit di fase 2 ed il rilascio del certificato può variare in funzione dell'OdC, in genere i Comitati si riuniscono mensilmente, è però possibile attivare procedure d'urgenza per abbreviare i tempi di emissione (ovviamente previa pagamento di un supplemento di costo).

### **7.5. Sorveglianza e rinnovo**

La certificazione ha una durata predeterminata a livello contrattuale, in Italia tale periodo è fissato in tre anni nel corso del quale si riceveranno almeno due/tre audit di sorveglianza. Gli audit di sorveglianza hanno l'obiettivo di verificare che il SGSI mantenga conformità ed efficacia nel periodo di validità del certificato (oltre che migliorare in modo continuativo la sicurezza). Ovviamente nel corso degli audit di sorveglianza è possibile "incappare" in situazioni tali da dover inserire audit supplementari per la verifica di situazioni critiche o particolarmente complesse. Pertanto il numero di audit di sorveglianza può variare in funzione della gravità delle eventuali non conformità rilevate nel corso di tali audit.

In caso di problemi sistematici e permanenti gli OdC possono innescare un meccanismo di escalation che può condurre, in caso di mancata risoluzione dei problemi, fino alla sospensione e revoca del certificato. Si tratta prevalentemente di situazioni al limite della legalità o del danno verso terzi, in ogni caso tali situazioni sono chiaramente previste nel regolamento dell'OdC (che deve essere attentamente letto e studiato prima di sottoscrivere il contratto per evitare brutte sorprese in corso d'opera).

Allo scadere del periodo di validità del certificato si può procedere all'audit di rinnovo, cioè alla ripetizione di un ciclo molto simile a quello della prima certificazione, solo leggermente diverso. Anche in questo caso esistono algoritmi che permettono di ricalcolare le durate dei singoli audit tenendo conto di un'aliquota di riduzione dettata dalla maturità del Sistema e dall'esperienza acquisita dall'OdC nella conoscenza dell'organizzazione e del SGSI.

In genere la durata delle sorveglianze e dell'audit di rinnovo è proporzionalmente inferiore all'audit di certificazione. Nell'audit di rinnovo può essere rieseguita la valutazione documentale ripetendo così il percorso già effettuato per la certificazione iniziale.

## 7.6. Valenza degli audit

Una volta compresi gli aspetti contrattuali ed operativi della certificazione cerchiamo di analizzare più a fondo l'audit. Gli audit vengono gestiti secondo la ISO 19011:02 (UNI EN ISO 19011:03 in Italia). Questo standard detta le modalità di gestione degli audit di qualsiasi genere riferibili ai Sistemi di Gestione, inclusi i SGSI.

Il lavoro di audit è basato sulla raccolta di evidenze che possano permettere di valutare la conformità e l'efficacia di un Sistema a fronte di uno o più standard di riferimento (è il caso dei sistemi di gestione integrati<sup>21</sup>).

La competenza del team di audit può però contribuire in modo significativo alla "crescita" del SGSI, pur nel rispetto dei ruoli e mantenendo l'indipendenza e l'etica professionale richiesta. Esiste infatti la possibilità, da parte del team di audit, di identificare dei punti di miglioramento (dette raccomandazioni). In genere si tratta di segnalazioni sul "cosa" migliorare e non "come", il team di audit identifica cioè delle aree di miglioramento potenziali sulla base delle conoscenze pregresse in materia di SGSI e/o sulla base della comprensione e maturità del SGSI. Tali raccomandazioni possono essere recepite oppure ignorate dall'organizzazione senza incidere sull'esito dell'audit. La capacità e la competenza di un auditor sono spesso misurate attraverso le raccomandazioni che esso riesce ad individuare e che l'organizzazione riesce a recepire ricavandone vantaggio.

Altro aspetto caratteristico degli audit sono le non conformità e le osservazioni, che chiameremo rilievi per semplicità. Spesso l'apertura di rilievi da parte dell'OdC diviene occasione per la revisione di alcune parti del SGSI innescando una vera e propria spirale di crescita nella ricerca delle soluzioni.

Ogni OdC ha una propria classificazione e solo la lettura del regolamento permette di comprenderne le differenze e le diverse modalità di gestione. Ogni organizzazione potrebbe ricevere uno o più rilievi in funzione delle "evidenze oggettive" raccolte dal team di audit. Ogni rilievo dovrà essere gestito secondo le modalità contrattuali previste dall'OdC (tempi, documentazione di supporto, obblighi di follow up ecc.).

Indipendentemente dalla classificazione e dal nome attribuitogli si tratta di situazioni che pregiudicano l'efficacia del sistema (in termini di funzionamento e di sicurezza) e/o di conformità alla norma, pertanto vengono considerate dagli OdC come situazioni per le quali si dovranno avviare opportune indagini (per determinare le cause) e quindi azioni per la loro rimozione (dette azioni correttive).

In generale una non conformità rileva qualcosa già avvenuto e pertanto si dovrà procedere con la correzione. Le osservazioni invece rilevano, in genere, potenziali problemi cui rispondere con azioni di prevenzione. Ma le cose possono sensibilmente cambiare di OdC in OdC!

I rilievi di maggior gravità comporteranno l'esecuzione di un audit straordinario per dimostrare che le situazioni origine del problema siano state effettivamente risolte.

In definitiva gli audit degli OdC possono divenire una rilevante opportunità di crescita se ben compresi e gestiti.

---

<sup>21</sup> Per i Sistemi di Gestione integrati riferirsi al documento PAS 99:2006 del British Standards Institution [www.bsi-global.com](http://www.bsi-global.com)

## **8. La certificazione accreditata**

### **8.1. Perché accreditata**

L'accREDITAMENTO è assicurato dagli OdA. In ciascuna nazione possono operare uno o più OdA in funzione delle scelte operate a livello di mercato e/o di governo. Alcuni OdA sono componenti governative, in altri casi si tratta di organizzazioni con varia forma giuridica (di solito associativa) cui spetta il compito di sorvegliare l'operato degli OdC accreditati.

Non tutti gli OdC operanti nel mercato risultano accreditati, cioè soggetti a loro volta ad un meccanismo di controllo simile a quello da loro operato sulle organizzazioni certificate.

“Chi controllerà il controllore?” questa è in definitiva la posizione dell'OdA rispetto agli OdC ed al mercato.

L'OdA esegue audit sugli OdC accreditati, seguendo standard ISO di riferimento, in modo analogo a quello operato dagli OdC sulle organizzazioni certificate. Processi e modalità simili, finalità diverse.

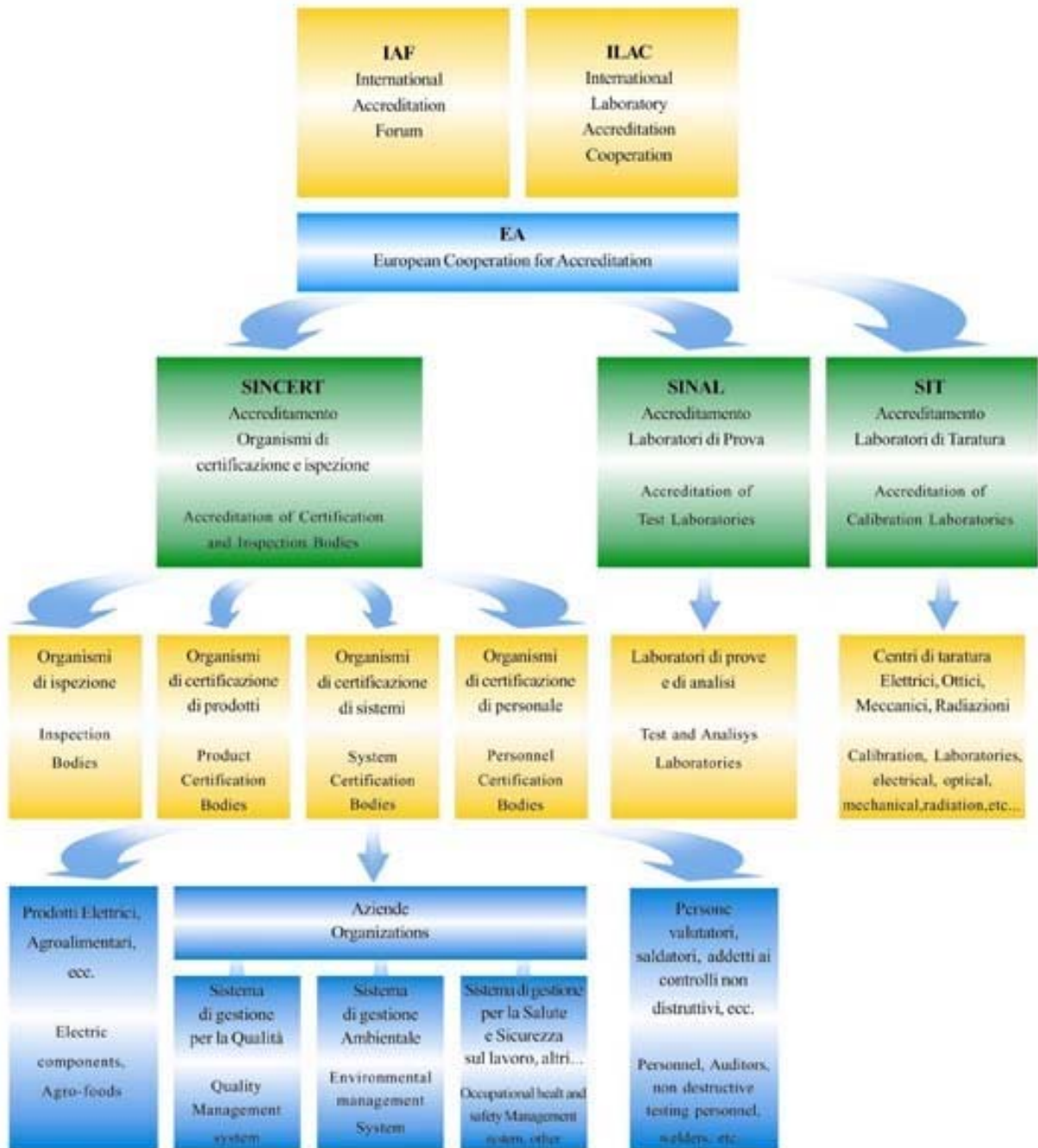
Da quanto appena descritto risulta evidente la valenza di un accREDITAMENTO per assicurare un meccanismo credibile di concessione delle certificazioni ISO/IEC 27001:05.

Ad oggi il numero di OdC accreditati è piuttosto limitato (6 a livello mondiale alla data di redazione del documento), è però auspicabile e prevedibile un numero maggiore in relazione alla richiesta di certificazioni da parte del mercato. Un maggior numero di OdC accreditati amplia l'offerta e avvia il meccanismo della concorrenza a favore del mercato (sebbene si rischi un declassamento delle competenze dei team di audit per compensare i minori ricavi).

I siti web degli OdA permettono non solo di identificare quali siano gli OdC accreditati a livello nazionale ma anche di verificare quante e quali siano le certificazioni rilasciate.

## 8.2. Chi accredita

La seguente figura sintetizza la “piramide” del sistema di accreditamento:



Fonte SINCERT

### 8.2.1. SINCERT<sup>22</sup>

“... costituito nel 1991, in forma di Associazione senza scopo di lucro, legalmente riconosciuta dallo Stato Italiano con Decreto Ministeriale del 16 Giugno 1995. La compagine associativa di SINCERT comprende attualmente 36 Associati, fra cui rientrano i principali Soggetti istituzionali, scientifici e tecnici, economici e sociali aventi

<sup>22</sup> [www.sincert.it](http://www.sincert.it)

*interesse diretto e indiretto nelle attività di accreditamento e certificazione, quali: le Pubbliche Amministrazioni e i maggiori Enti Pubblici Tecnici e di Ricerca, le Associazioni dei Consumatori, le Associazioni di categoria della industria, commercio e agricoltura, le Camere di Commercio, i grandi Fornitori di servizi di pubblica utilità (energia e trasporti), le Associazioni rappresentative degli Organismi di Certificazione e Ispezione e delle Società e Professionisti della consulenza, nonché numerosi altri Soggetti facenti riferimento a o riponenti affidamento su le attività di accreditamento.*

*L'Associazione ha come finalità l'accREDITAMENTO di:*

- *Organismi di Certificazione di sistemi di gestione aziendale, quali sistemi di gestione per la qualità, sistemi di gestione ambientale, sistemi di gestione per la sicurezza e salute sul lavoro ed altri;*
- *Organismi di Certificazione di prodotti;*
- *Organismi di Certificazione di personale;*
- *Organismi di Ispezione”*

### **8.2.2.EA<sup>23</sup>**

EA nasce dall'unificazione di EAC (European Accreditation of Certification) ed EAL (European co-operation for Accreditation of Laboratories) e copre tutte le attività europee di valutazione della conformità:

- certificazione di laboratori di prova e centri di taratura
- ispezione
- certificazione di sistema
- certificazione di prodotto
- certificazione di personale
- verifiche ambientali in conformità allo schema europeo EMAS.

Dal 26 giugno 2000 EA è diventata un'entità legale (associazione senza fini di lucro), con sede in Olanda.

I membri dell'EA sono gli Enti di accreditamento, riconosciuti a livello nazionale, degli stati membri (o candidati ad esserlo) della Comunità Europea e dell'EFTA.

La più alta autorità decisionale dell'EA è l'Assemblea Generale, costituita dal Presidente, dal/la Segretario/a e dai delegati degli Organismi membri EA. L'organo operativo dell'EA è il Comitato Esecutivo, che è supportato dalla segreteria e dai Comitati Tecnici. Gli stakeholders possono esprimere il proprio punto di vista attraverso le discussioni del Consiglio EA, organo indipendente, gestito e composto dai rappresentanti di tutte le parti interessate all'accREDITAMENTO e dai rappresentanti degli Enti di accREDITAMENTO.

Possono diventare Membri Associati gli Enti di accREDITAMENTO, riconosciuti a livello nazionale, di stati Europei che siano in grado di dimostrare che operano in conformità alle norme per l'accREDITAMENTO dei laboratori o per l'accREDITAMENTO degli organismi di certificazione.

Obiettivo primario di EA è svolgere un ruolo chiave nell'eliminazione delle barriere tecniche agli scambi commerciali, attraverso:

- un approccio uniforme all'accREDITAMENTO in tutta l'Europa
- l'accettazione universale dei certificati e dei rapporti coperti da accREDITAMENTO
- la creazione di un clima di fiducia reciproca tra gli enti di accREDITAMENTO
- il supporto ad un'implementazione condivisa delle norme relative all'accREDITAMENTO
- lo scambio di conoscenze tecniche fra membri firmatari dell'accordo di mutuo riconoscimento ([MLA](#)) e membri associati

---

<sup>23</sup> [www.european-accreditation.org](http://www.european-accreditation.org)

- il raggiungimento della riferibilità delle prove
- il mantenimento e l'implementazione di accordi MLA sia all'interno dell'EA stesso sia con enti di accreditamento non membri o gruppi regionali.

### 8.2.3. IAF<sup>24</sup>

L'International Accreditation Forum, Inc. (IAF) è l'associazione mondiale degli Organismi di accreditamento di Organismi di certificazione e di altri Enti interessati alle attività di Conformity Assessment.

Lo IAF raggruppa Enti di accreditamento di tutto il mondo, rappresentanti del mondo dell'industria e degli Organismi di certificazione accreditati, in un'organizzazione internazionale che cerca di incoraggiare lo sviluppo di un unico sistema mondiale di mutuo riconoscimento dei certificati di conformità.

Tutti i membri dello IAF si impegnano ad adottare delle politiche e procedure che facilitino il commercio, in conformità con l'accordo relativo alle Barriere Tecniche al Commercio, definito dall'Organizzazione Mondiale per il Commercio.

Sia gli Enti di accreditamento sia gli Organismi di certificazione si impegnano a basare le proprie procedure di conformity assessment su norme o guide sviluppate dall'ISO/CASCO e adottate in accordo con le regole stabilite da ISO/IEC.

Qualora dei membri dello IAF, per esigenze di mercato, svolgano attività di conformity assessment con riferimento a settori/servizi per i quali non esistano norme o guide sviluppate dall'ISO/CASCO e adottate in accordo con le regole stabilite da ISO/IEC, tali membri si impegnano ad assicurare l'utilizzo di norme conformi ai principi definiti negli articoli 5 e 6 sul Conformity Assessment (consensus driven open process) dell'accordo relativo alle Barriere Tecniche al Commercio, definito dall'Organizzazione Mondiale per il Commercio.

Tra i compiti dello IAF citiamo:

- Sviluppare un programma mondiale di valutazione della conformità che promuova l'eliminazione delle barriere tecniche al commercio.
- Facilitare gli scambi e il commercio, in accordo con le politiche dell'Organizzazione Mondiale del Commercio (WTO), attraverso la definizione di accordi multilaterali di mutuo riconoscimento (MLA), che si basano sull'equivalenza dei programmi di accreditamento definiti dagli enti di accreditamenti membri IAF, e che vengono verificati attraverso visite ispettive reciproche fra questi enti.

L'accREDITAMENTO è sempre più visto e utilizzato dai governanti e dal mercato come uno strumento imparziale, indipendente e trasparente di valutazione delle competenze degli Organismi di certificazione. Lo IAF fornisce le basi tecniche per il riconoscimento mondiale delle competenze degli Organismi accreditati dai suoi membri, dando forma al seguente concetto: "testato o certificato una volta - accettato dappertutto".

### 8.3. Come accredita

La ISO 17021 (e la linea guida ISO/IEC 27006 di prossima pubblicazione) forniscono informazioni circa i meccanismi generali di accreditamento e certificazione.

Ogni OdC riceve periodicamente visite di sorveglianza da parte dell'OdA. Il processo di accreditamento e di sorveglianza periodica è analogo a quello della certificazione per le organizzazioni. Unica eccezione è che le sorveglianze per l'accREDITAMENTO si ripetono in funzione degli schemi e dei settori di accREDITAMENTO concessi, vale a dire che più un OdC estende il proprio campo di azione più sorveglianze riceverà nel periodo.

<sup>24</sup> [www.compad.com.au/clients/iaf](http://www.compad.com.au/clients/iaf)

#### **8.4. Il Multi Lateral Agreement europeo**

I firmatari degli accordi di mutuo riconoscimento garantiscono l'uniformità delle attività di accreditamento attraverso una sorveglianza continua e rigorosa.

L'attività di sorveglianza si basa sul "peer assessment" fra gli Enti firmatari degli accordi MLA e comprende sia visite presso l'Organismo di accreditamento, sia visite di accompagnamento presso gli Organismi di certificazione da esso accreditati.

Durante queste visite viene valutato il rispetto dei criteri condivisi, compreso il criterio di indipendenza. Il risultato positivo di queste visite è necessario per ottenere e mantenere l'accREDITAMENTO EA.

#### **8.5. Il Multi Recognition Arrangement mondiale**

Procedimento analogo al MLA su scala mondiale.

## 9. Il periodo di transizione

### 9.1. Quando scade la BS7799-2:02

Il SINCERT ha definito il periodo di transizione con un documento del 13/12/05 nel quale sono state delineate due date limite:

- **31/3/2006**: cessazione emissioni certificati BS7799-2:02; significa che a partire da questa data non è più possibile richiedere certificazioni o rilasciare nuove certificazioni secondo la BS7799-2:02.
- **31/3/2007**: cessazione validità della BS7799-2:02; significa che tutti i certificati devono essere stati convertiti in ISO/IEC 27001:05 e non sarà più possibile gestire certificazioni BS7799-2:02 accreditate.

Da notare che la scadenza in Italia è anticipata di un mese rispetto a molte altre nazioni europee, ciò pone le organizzazioni italiane in posizione di vantaggio verso potenziali clienti e/o per la risposta a bandi di gara sul territorio internazionale.

## 10. Come convertire i certificati da BS7799-2:02 a ISO/IEC 27001:05

### 10.1. Convertire il SGSI alla nuova norma

La prima considerazione da fare è la peculiare differenza di impostazione del SGSI derivante da alcuni requisiti modificati nella ISO/IEC 27001:05 (ad esempio: la misurabilità dell'efficacia del SGSI e delle contromisure adottate).

La seconda considerazione è l'impatto derivante dalle modifiche apportate all'allegato A con riflessi sia sul trattamento dei rischi sia sulla dichiarazione di applicabilità.

La terza considerazione si riferisce alla valutazione del rischio che dovrà necessariamente dimostrare di essere ripetibile e di produrre risultati congruenti.

A parte questi aspetti puntuali il resto del SGSI non dovrebbe subire modifiche sostanziali modifiche.

Ipotizzando un percorso *generalizzato* potremmo azzardare le seguenti tappe:

1. **Gap analysis:** cioè eseguire un audit interno utilizzando la ISO/IEC 27001:05 evidenziando i *sol*i punti disallineati rispetto alla situazione attuale.
2. **Impact analysis:** cioè definire le attività necessarie per adeguare il SGSI alla nuova norma.
3. **Risk analysis:**
  - ridefinire i criteri di valutazione del rischio secondo le richieste della nuova norma, ivi inclusi i criteri di accettabilità;
  - eseguire la valutazione dei rischi utilizzando i nuovi criteri, evidenziando le eventuali differenze con le precedenti valutazioni.
4. **Risk treatment:** cioè ridefinire i criteri e le modalità di trattamento dei rischi evidenziati, selezionando le opportune contromisure dall'allegato A della nuova norma.
5. **Statement of Applicability:** la dichiarazione di applicabilità dovrà essere aggiornata in funzione dei trattamenti definiti e delle scelte effettuate.
6. **Risk Treatment Plan:** cioè definire un piano di trattamento dei rischi che tenga conto delle differenze derivanti dall'applicazione delle contromisure selezionate sulla base della nuova norma. In particolare si dovrà porre attenzione:
  - alle contromisure soppresse rispetto all'allegato A della vecchia norma;
  - alle nuove contromisure previste dall'allegato A della nuova norma, di particolare rilievo è l'aspetto inerente alla gestione degli incidenti;
  - alle contromisure modificate rispetto all'allegato A della vecchia norma.
7. **Transition Plan:** cioè definire le attività operative per implementare il nuovo SGSI e per dimostrarne/misurarne la conformità e l'efficacia.
8. **Training Plan:** cioè definire un piano di aggiornamento del personale affinché siano recepite (ed attuate) le differenze derivanti dall'adozione della nuova norma.
9. **Risk Assessment Plan:** cioè definire un piano<sup>25</sup> per la ripetizione della valutazione dei rischi e per la dimostrazione della congruenza delle valutazioni eseguite.
10. **Monitor Plan:** cioè pianificare attività di misurazione continua che permettano di dimostrare l'efficacia del SGSI e delle contromisure adottate.
11. **Audit Plan:** cioè definire un nuovo programma di audit in modo da verificare l'applicazione e l'efficacia del SGSI.
12. **Management review:** definire almeno un riesame annuale del SGSI a valle del quale produrre eventuali documenti per la gestione del miglioramento.

---

<sup>25</sup> Un'analisi approfondita della nuova norma (e dei documenti richiamati) prospetta la possibilità di pianificare analisi bimestrali per ottenere un numero minimo di rilevazioni significative nell'arco di un periodo di riferimento.

I passi esposti non devono essere considerati come obbligatori o applicabili a tutte le realtà, sono solo la trasposizione in chiave operativa di quanto suggerito dalla norma stessa e dalle esperienze internazionali maturate ad oggi. Le organizzazioni già certificate sono libere di adottare qualsiasi approccio purché al termine del percorso siano stati soddisfatti tutti i criteri previsti dalla nuova norma.

## **10.2. Convertire il certificato**

Innanzitutto occorre verificare se il proprio OdC sia accreditato per l'emissione dei certificati in conformità alla ISO/IEC 27001:05, in caso contrario occorrerà identificarne uno diverso oppure predisporre l'aspetto contrattuale come necessario (tempi per l'accreditamento, validità dei certificati rilasciati ecc.).

La conversione della norma obbliga (in genere) alla revisione del contratto con l'OdC che utilizzerà questo passaggio per adeguare costi e durate alle più recenti disposizioni in atto presso gli OdA e derivanti dalle direttive internazionali (ad esempio dalla ISO/IEC 27006).

In genere la conversione del certificato avviene nel corso di uno degli audit di sorveglianza periodica. Per far ciò occorre concordare con l'OdC i tempi e la modalità per lo svolgimento delle varie fasi del processo: analisi documentale (o fase 1) e audit in campo (o fase 2).

Alcuni OdC prevedono uno specifico audit di conversione, altri invece considerano tale passo come una "estensione" del certificato preesistente. In ogni caso la durata dell'audit sarà simile a quella della prima certificazione.

Particolarmente consigliabile è l'esecuzione di un preaudit (o assessment preliminare) in modo da valutare preventivamente l'allineamento del SGSI alla norma, prima di ingaggiare il processo di certificazione vero e proprio.

## 11. Il gruppo utenti internazionali (ISMS IUG)

Gli utilizzatori della ISO 27001 (e delle linee guida collegate) sono riuniti all'interno di un Gruppo Utenti Internazionali (IUG) con sede a Londra<sup>26</sup>, gestito dal "padre" della norma. Ogni nazione può esprimere un Capitolo locale coordinato da un chair di riferimento. L'organizzazione dei Capitoli può essere diversa di nazione in nazione ma le finalità devono invece essere comuni.

I Capitoli si incontrano una volta l'anno in occasione dell'International Meeting che si svolge a Londra nel mese di dicembre.

Ciascun Capitolo ha come obiettivo principale sostenere la diffusione e l'utilizzazione della ISO 27001 supportando e/o organizzando eventi in materia di sicurezza delle informazioni.

Il Capitolo italiano, attivo dal settembre 2005, provvede a tale scopo mediante il proprio sito<sup>27</sup> e le proprie iniziative, spesso in collaborazione con altre associazioni.

### 11.1. *Ruolo del ISMS IUG Italy nel Comitato ISO JTC1/SC 27/WG 1*

Nel 2005 il Capitolo italiano ha avuto accesso ai comitati ISO della norma come punto di riferimento per l'Italia. In tal modo si è dato atto della posizione dell'Italia nel quadro mondiale della ISO 27001, delle competenze e dell'esperienza maturata dal 1999 in tale campo da tutti i professionisti e le organizzazioni coinvolte nella implementazione e nella certificazione dei SGSI.

Il Capitolo contribuisce attivamente alla scrittura delle norme ed alla loro diffusione, anche per mezzo di eventi pubblici, comunicazioni ufficiali, interventi informativi e per mezzo della gestione delle prove sulle norme in via di approvazione.

Il Capitolo organizza annualmente (in genere nel mese di settembre) un Forum annuale sull'andamento dei SGSI e della norma, sia a livello nazionale che internazionale. A questo appuntamento vengono invitati relatori nazionali ed internazionali e le associazioni i cui impegni ed interessi gravitano nell'orbita della sicurezza delle informazioni.

---

<sup>26</sup> [www.xisec.com](http://www.xisec.com)

<sup>27</sup> [www.ismsiugitaly.net](http://www.ismsiugitaly.net)

CLUSIT

**Associazione Italiana per la Sicurezza Informatica**

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

[www.clusit.it](http://www.clusit.it) – [info@clusit.it](mailto:info@clusit.it)

tel. 347 23 19 285