Dalle BS 7799-2:2002 e ISO 17799:2005 alle ISO 17799:2005 e 27001:2005

Evoluzione delle normative di riferimento della Information Security ed analisi delle principali novità introdotte

di Cesare Gallotti

Il 15 giugno e il 15 ottobre 2005 sono state emesse rispettivamente la nuova versione dell'ISO 17799 che sostituisce quella del 2000 e la norma ISO 27001:2005 che sostituirà la BS 7799-2:2002. In seguito saranno stabilite le regole di transizione dalla BS 7799-2:2002 all'ISO 27001:2005.

L'ISO 17799 è una *linea guida* o "*code of practice*" (usa il verbo "should") che presenta in modo approfondito alcune misure per garantire la sicurezza delle informazioni. L'ISO 27001:2005 è, invece, lo standard di riferimento per le certificazioni dei Sistemi di Gestione per la Sicurezza delle Informazioni, o "*specifica*" (usa il verbo "shall").

Le due norme sono correlate e infatti la norma 27001 riporta nell'Allegato A i *controlli* indicati nell'ISO 17799:2005 e che dovranno essere utilizzati nello Statement of Applicability per descrivere le decisioni prese in merito al trattamento del rischio.

Per il 2006 è prevista la rinumerazione dell'ISO 17799:2005 in ISO 27002:2006 e verrà emessa l'ISO 27000 dedicata a "Terminologia e definizioni", seguendo così il modello già usato per le norme della serie ISO 9000 e ISO 14000.

Nel futuro si prevede l'emissione di nuove norme della serie 27000, dedicate alla gestione dei rischi, alle metriche e misurazioni dei processi di un Sistema di Gestione per la Sicurezza delle Informazioni, oltre a una guida per la loro implementazione.

Analisi dell'ISO 17799:2005

La nuova norma ISO 17799:2005 presenta una breve descrizione per ciascuna misura proposta, detta *controllo* di sicurezza, seguita da una descrizione più approfondita (*Implementation Guidance*) e da eventuali ulteriori considerazioni, riferimenti ad altri standard o richiami a possibili aspetti legali (nel paragrafo *Other information*).

La precedente versione della ISO 17799:2000 indicava come "controllo" sia la breve descrizione che la Implementation Guidance, lasciando agli estensori della BS 7799-2:2002 il compito di redigerne una sintesi da riportare nell'Allegato A. In questo modo alcune misure importanti (come, per esempio, la definizione di *Ownership of assets*), non erano riportate per quelli che potremmo definire *errori di sintesi*.

I controlli attualmente proposti sono 134, contro i 127 precedenti. Molti sono stati riformulati per aggiornare della terminologia, renderla omogenea e per garantire la completezza delle descrizioni. Altri controlli sono stati aggiunti per evitare *errori di sintesi*.

Non sono da segnalare modifiche tali da compromettere il lavoro svolto sin qui dalle aziende che hanno redatto uno Statement of Applicability conforme al BS 7799-2:2002, a parte la nuova numerazione e la maggiore attenzione ad alcuni argomenti, come verrà analizzato di seguito.

I capitoli iniziali ricalcano quanto già previsto dalla norma del 2000, con un'estensione del secondo capitolo dedicato alle definizioni, l'aggiunta di un breve capitolo (il quarto) dedicato alla valutazione e trattamento del rischio e uno (il terzo) di descrizione della struttura dello standard.

Agli *starting point* già proposti dall'ISO 17799:2000 ne viene aggiunto uno riguardante la correttezza di esecuzione delle applicazioni.

Per la successiva analisi, i capitoli saranno presentati secondo l'ordine della versione del 2000. Questo per facilitare chi ha lavorato sino ad oggi con questa.

Quasi tutti i titoli e descrizioni dei controlli sono stati modificati. Saranno di seguito segnalate le sole modifiche di rilevo agli scopi di questo articolo.

3 Security Policy

Una maggiore attenzione viene posta alle terze parti: l'ISO 17799:2005 richiede di comunicare la politica di sicurezza, oltre che al personale interno, anche alle "entità esterne rilevanti".

Questo aspetto era già presente nella norma del 2000, ma poco evidenziato dalla BS 7799-2:2002. La nuova organizzazione dei controlli e le relative descrizioni (anche se non saranno segnalate nel prosieguo dell'articolo) sottolineano questo argomento talmente importante da non richiedere ulteriori commenti.

4 Organizational Security

Al primo controllo è presente una novità: viene eliminato il "Security forum", entità organizzativa amatissima da quanti sino ad oggi si sono occupati di sicurezza delle informazioni.

Le responsabilità gestionali sono ora date alla Direzione Aziendale, uniformemente a quanto già previsto dalle attuali versioni di standard come l'ISO 9001 e l'ISO 14000. Il Security Forum veniva delegato dalla Direzione per fornire supporto alle attività di sicurezza, definire la politica di sicurezza e approvare gli investimenti di maggior portata: attività ora di competenza della stessa Direzione.

Viene comunque lasciata la possibilità di costituire un gruppo con competenze più specifiche e maggiore orientamento verso le tematiche di sicurezza.

Il controllo sugli accordi di riservatezza (6.1.3, per la ISO 17799:2000) non è più collocato nel capitolo dedicato alla gestione del personale, ma in questo sull'organizzazione della sicurezza perché riconducibile anche alla gestione delle "terze parti".

I controlli 4.1.5 e 4.1.6 della versione del 2000, ora numerati come 6.1.7 e 6.1.6, relativi al supporto di specialisti esterni e all'attivazione di contatti con altre organizzazioni, sono stati modificati e resi più chiari.

I controlli successivi, a cui è dedicata la Sezione 6.2, sono relativi alla gestione delle terze parti e sono stati riorganizzati. Viene chiarito meglio il concetto di outsourcing e le sue differenze rispetto ad altre tipologie di rapporti con terzi. Per questo motivo non è possibile trovare un corrispondente diretto del controllo 4.3.1 della precedente versione dell'ISO 17799.

Il nuovo controllo 6.2.2 esplicita la necessità di considerare, tra le terze parti, non solo i fornitori, ma anche i clienti.

5 Asset classification and control

Questo capitolo è stato rinominato "Asset management" e ha due controlli in più.

Il nuovo controllo 7.1.2 è dedicato alla "proprietà" degli asset (*Ownership of assets*). Tale argomento, benché presente nel controllo 4.1.3 dell'ISO 17799:2000, non era riportato nella BS 7799-2:2002 per *errore di sintesi.*

6 Personnel Security

La nuova norma dedica 3 nuovi controlli (8.3.1, 8.3.2, 8.3.3) alla gestione del personale interno o esterno in occasione della fine del rapporto con un'organizzazione. Queste misure, per *errori di sintesi,* non sono richiamate dall'Allegato A della BS 7799-2:2002.

Viene anche aggiunta la nuova misura 8.2.1, in cui viene specificato che è responsabilità della Direzione comunicare al personale, sia interno che esterno, l'obbligo di applicazione delle politiche e procedure di sicurezza.

Gestione degli incidenti

Le misure della ISO 17799:2000 da 6.3.1 a 6.3.4 riguardano la gestione degli incidenti, a cui la nuova norma del 2005 dedica un capitolo in più: il 13.

Per *errore di sintesi,* i controlli dell'Allegato A della BS 7799-2:2002 richiedevano di segnalare e analizzare gli incidenti, ma non contemplavano la gestione degli stessi. Una parziale eccezione a ciò è rappresentata dal controllo 8.1.3, limitato però ai soli incidenti informatici. Il controllo 13.2.1 della nuova norma richiede la gestione degli incidenti per tutti gli ambienti.

Il controllo della vecchia norma 6.3.3 sulle vulnerabilità software è collocato nel capitolo dedicato allo sviluppo e gestione dei sistemi.

Il controllo relativo alla raccolta di prove a scopi legali, precedentemente collocato nel capitolo *"Compliance"*, è stato ora più propriamente accorpato agli altri controlli di gestione degli incidenti.

7 Physical and environmental security

Si segnala l'aggiunta del controllo 9.1.4, che specifica meglio le misure da intraprendere contro le minacce ambientali, non riportate dall'Allegato A della BS 7799-2:2002 per *errore di sintesi.*

Il controllo 7.2.2, precedentemente dedicato alla protezione delle infrastrutture di erogazione di energia, è stato esteso a tutte le infrastrutture

Il controllo sulla Clear Desk Policy è stato ricollocato tra le "User responsabilities".

8 Communication and operations management

Per la nuova norma del 2005 sono stati ampiamente riscritti e aggiornati i controlli del 2000. In particolare, si nota una maggiore attenzione agli strumenti informatici esterni all'azienda, alle terze parti, al commercio elettronico (a cui è stata dedicata la nuova sezione 10.9) e all'evoluzione degli strumenti di automazione per l'ufficio.

E' stato aggiunto il controllo 10.8.1 relativo allo scambio di informazioni, mentre è interessante la riformulazione del vecchio controllo 8.7.7 sulla posta elettronica, che viene ora fatta rientrare come caso particolare di "Electronic messaging".

Una nuova sezione 10.10 è stata dedicata al monitoraggio dei sistemi (logging e auditing), raggruppando ed estendendo alcuni controlli precedentemente dedicati al solo monitoraggio dei sistemi o degli accessi. Alla protezione dei log, considerata precedentemente come caso particolare di sicurezza dei record aziendali, è ora dedicato il controllo 10.10.3.

9 Access Control

Le misure di controllo degli accessi sono in larga parte rimaste invariate o adeguate alle nuove tecnologie.

L'aggiornamento consiste nell'ammodernamento del linguaggio e nell'eliminazione di controlli specifici del solo mondo mainframe.

Sono stati eliminati i controlli 9.4.2 sull'*enforced path* (raramente applicato e meglio espresso come caso particolare di controllo delle trasmissioni), 9.5.1 sull'autenticazione automatica dei

terminali (più specifico per ambienti mainframe e ora caso particolare della 11.6.1), 9.5.6 sulla segnalazione automatica di transazioni effettuate sotto coercizione (ora caso particolare di segnalazione di incidenti)

10 System development and maintenance

In questo capitolo i controlli dedicati alla crittografia (quelli della sezione 10.3 della ISO 17799:2000) sono passati da cinque a due. Nella nuova versione, la crittografia è da intendersi più come tecnologia particolare che come controllo a sé stante. Rimangono i due controlli relativi alle politiche e alla gestione delle chiavi crittografiche.

Il vecchio controllo 10.2.3 è stato riformulato considerando l'autenticazione delle trasmissioni come caso particolare di integrità.

I restanti controlli sono stati resi più chiari e aggiornati.

11 Business continuity management

Capitolo largamente rimasto invariato. Da segnalare solo qualche aggiunta e precisazione.

12 Compliance

Anche questo Capitolo non ha subito variazioni di rilievo se non qualche aggiunta e precisazione.

Analisi della ISO 27001

La 27001:2005 riprende in larga parte la BS 7799-2:2002.

In particolare, i requisiti per la valutazione di un ISMS sono descritti nei primi capitoli da 4 a 8 (un capitolo è stato aggiunto perché il punto 6.4 è diventato il capitolo 6) e nell'Allegato A che riporta i controlli della ISO 17799:2005.

Tra le cose rilevanti si segnalano:

La descrizione dello Statement of Applicability: viene detto che il SoA "deve fornire un riassunto delle decisioni relative al trattamento del rischio" e viene anche richiesto di "dimostrare, per ciascun controllo, la sua relazione con i risultati del risk assessment e del risk treatment, con la politica e con gli obiettivi"; questo documento, quindi, non dovrà più riportare solo riferimenti a procedure o documenti di descrizione in dettaglio del controllo, ma anche una descrizione dei rischi che va a contrastare;

Misurazione dell'efficacia dei controlli di sicurezza: In più punti si fa riferimento alla richiesta di misurare l'efficacia dei controlli o di gruppi di controlli. Questo aspetto è sicuramente quello che rappresenta la maggiore innovazione della nuova norma e il maggiore impegno per chi implementa un ISMS. In particolare si potrà fare riferimento alla disponibilità dei sistemi e a statistiche sugli incidenti rilevati e gestiti, ma altri indicatori dovranno essere individuati dalle singole aziende sulla base dei dati e dei sistemi di monitoraggio che hanno a disposizione o compatibili con quelli già esistenti.

Come elementi di minor rilievo si segnalano:

- viene esplicitato che la metodologia di valutazione del rischio deve garantire risultati comparabili e riproducibili, ossia che i risultati di valutazioni del rischio in momenti diversi dell'azienda diano evidenza delle modificazioni eventualmente avvenute, e che la stessa metodologia applicata in condizioni simili dia gli stessi risultati
- viene esplicitata la necessità di rivedere periodicamente il risk assessment, mentre prima si chiedeva di rivedere il solo rischio accettabile
- viene esplicitamente richiesto un documento che descriva la metodologia di risk assessment.

Purtroppo i capitoli non sono allineati con l'ISO 9001:2000, e questo può rendere l'integrazione dei sistemi di gestione più laborioso di quanto auspicato.

Conclusioni

Le nuove ISO 17799:2005 e ISO 27001:2005 risultano essere più vicine alle esigenze del mercato e degli utilizzatori, grazie ai controlli più dettagliati, alla loro organizzazione più coerente e al loro aggiornamento.

Sicuramente, anche a fronte della richiesta di misurazione dell'efficacia dei controlli, la norma non perde la sua caratteristica di essere applicabile in tutte le realtà e sarà compito di ciascuna azienda individuare le modalità più adeguate per avere a disposizione dati utili al miglioramento continuo.

Queste norme, poi, dimostrano sempre più di migliorarsi tenendo conto dell'esperienza di quanti ne hanno utilizzato le precedenti versioni, in modo da renderle sempre più punto di riferimento per coloro che si occupano di sicurezza delle informazioni e dei sistemi di gestione ad essa dedicati.

*****

Cesare Gallotti attualmente lavora per l'organismo di certificazione Det Norske Veritas (www.dnv.it) come Lead Auditor BS 7799-2 e ISO 9001, oltre ad occuparsi di altri temi legati alla tecnologia dell'informazione. Ha lavorato precedentemente come consulente per Securteam e Intesis. È Certified Information System Auditor (CISA) e autore del libro *Sicurezza delle Informazioni - Analisi e gestione del rischio* (ed. FrancoAngeli, 2003).

Tabelle di correlazione

Di seguito viene proposta la correlazione tra i controlli dell'ISO 17799:2000 (corrispondenti a quelli dell'Allegato A della BS 7799-2:2002) con quelli dell'ISO 17799:2005 (corrispondenti a quelli dell'Allegato A della ISO 27001:2005), in modo che possa tornare utile a quanti hanno già esteso uno *Statement of Applicability* conforme alla Specifica.

La prima colonna riporta i controlli della ISO 17799:2000, ordinati e non ripetuti; la seconda colonna riporta i controlli corrispondenti dell'ISO 17799:2005, eventualmente ripetuti e accompagnati da una nota sulla colonna delle "Note" per facilitare chi vuole confrontare le versioni avendo come riferimento quella nuova.

Per motivi di diritto d'autore non verranno riportati né i testi né i titoli dei controlli. Si farà eccezione dei titoli dei capitoli, dato che sono ampiamente diffusi. Mi scuso con quanti non abbiano a disposizione i documenti di riferimento.

3 Security Policy

ISO 17799:2000	ISO 17799:2005	Note
3.1.1	5.1.1	
3.1.2	5.1.2	

4 Organizational Security

ISO 17799:2000	ISO 17799:2005	Note
4.1.1	6.1.1	
4.1.2	6.1.2	
4.1.3	6.1.3	
4.1.4	6.1.4	
	6.1.5	E' il controllo 6.1.3 della ISO 17799:2000
4.1.5	6.1.7	
4.1.6	6.1.6	
4.1.7	6.1.8	
4.2.1	6.2.1	
	6.2.2	
4.2.2	6.2.3	
4.3.1	-	

5 Asset classification and control

ISO 17799:2000	ISO 17799:2005	Note
5.1.1	7.1.1, 7.1.2	
5.2.1	7.2.1	
5.2.2	7.2.2, 7.1.3	

6 Personnel Security

ISO 17799:2000	ISO 17799:2005	Note
6.1.1	8.1.1	
6.1.2	8.1.2	
6.1.3	6.1.5	
6.1.4	8.1.3	
	8.2.1	
6.2.1	8.2.2	
6.3.5	8.2.3	
	8.3.1, 8.3.2, 8.3.3	
6.3.1	13.1.1	
6.3.2	13.1.2	
	13.2.1	E’ il controllo 8.1.3 della ISO 17799:2000
6.3.3	12.6.1	
6.3.4	13.2.2	
	13.2.3	E’ il controllo 12.1.7, della ISO 17799:2000

7 Physical and environmental security

ISO 17799:2000	ISO 17799:2005	Note
7.1.1	9.1.1	
7.1.2	9.1.2	
7.1.3	9.1.3	
	9.1.4	
7.1.4	9.1.5	
7.1.5	9.1.6	
7.2.1	9.2.1	
7.2.2	9.2.2	
7.2.3	9.2.3	
7.2.4	9.2.4	
7.2.5	9.2.5	
7.2.6	9.2.6	
7.3.1	11.3.3	
7.3.2	9.2.7	

8 Communication and operations management

ISO 17799:2000	ISO 17799:2005	Note
8.1.1	10.1.1	
8.1.2	10.1.2	
8.1.3	13.2.1	
8.1.4	10.1.3	
8.1.5	10.1.4	
8.1.6	10.2.1 10.2.2	
8.2.1	10.3.1	
8.2.2	10.3.2	
8.3.1	10.4.1 10.4.2	
8.4.1	10.5.1	
8.4.2	10.10.4	
8.4.3	10.10.5	
8.5.1	10.6.1	
	10.6.2	
8.6.1	10.7.1	
8.6.2	10.7.2	
8.6.3	10.7.3	
8.6.4	10.7.4	
	10.8.1	
8.7.1	10.8.2	
8.7.2	10.8.3	
8.7.3	10.9.1 10.9.2	
8.7.4	10.8.4	
8.7.5	10.8.5	
8.7.6	10.9.3	
8.7.7	10.8.4	

	10.10.1	E’ il controllo 9.7.1 della ISO 17799:2000
	10.10.2	E’ il controllo 9.7.2 della ISO 17799:2000
	10.10.3	
	10.10.4	E’ il controllo 8.4.2 della ISO 17799:2000
	10.10.5	E’ il controllo 8.4.3 della ISO 17799:2000
	10.10.6	E’ il controllo 9.7.3 della ISO 17799:2000

9 Access Control

ISO 17799:2000	ISO 17799:2005	Note
9.1.1	11.1.1	
9.2.1	11.2.1	
9.2.2	11.2.2	
9.2.3	11.2.3	
9.2.4	11.2.4	
9.3.1	11.3.1	
9.3.2	11.3.2	
	11.3.3	E’ il controllo 7.3.1 della ISO 17799:2000
9.4.1	11.4.1	
9.4.2	-	
9.4.3	11.4.2	
9.4.4	11.4.3	
9.4.5	11.4.5	
9.4.6	11.4.5	
9.4.7	11.4.6	
9.4.8	11.4.7	
9.4.9	10.6.2	
9.5.1	-	
9.5.2	11.5.1	
9.5.3	11.5.2	
9.5.4	11.5.3	
9.5.5	11.5.4	
9.5.6	-	
9.5.7	11.5.5	
9.5.8	11.5.6	
9.6.1	11.6.1	
9.6.2	11.6.2	
9.7.1	10.10.1	
9.7.2	10.10.2	
9.7.3	10.10.6	
9.8.1	11.7.1	
9.8.2	11.7.2	

10 System development and maintenance

ISO 17799:2000	ISO 17799:2005	Note
10.1.1	12.1.1	
10.2.1	12.2.1	
10.2.2	12.2.2	
10.2.3	12.2.3	
10.2.4	12.2.4	
10.3.1	12.3.1	
10.3.2	-	
10.3.3	-	
10.3.4	-	
10.3.5	12.3.2	
10.4.1	12.4.1	
10.4.2	12.4.2	
10.4.3	12.4.3	
10.5.1	12.5.1	
10.5.2	12.5.2	
10.5.3	12.5.3	
10.5.4	12.5.4	
10.5.5	12.5.5	

11 Business continuity management

ISO 17799:2000	ISO 17799:2005	Note
11.1.1	14.1.1	
11.1.2	14.1.2	
11.1.3	14.1.3	
11.1.4	14.1.4	
11.1.5	14.1.5	

12 Compliance

ISO 17799:2000	ISO 17799:2005	Note
12.1.1	15.1.1	
12.1.2	15.1.2	
12.1.3	15.1.3	
12.1.4	15.1.4	
12.1.5	15.1.5	
12.1.6	15.1.6	
12.1.7	13.2.3	
12.2.1	15.2.1	
12.2.2	15.2.2	
12.3.1	15.3.1	
12.3.2	15.3.2	