ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Standard per il SGSI

La nuova famiglia ISO/IEC 27000 e

il BS 7799-2

(a cura di **M Cecioni** – CISA - Securteam)

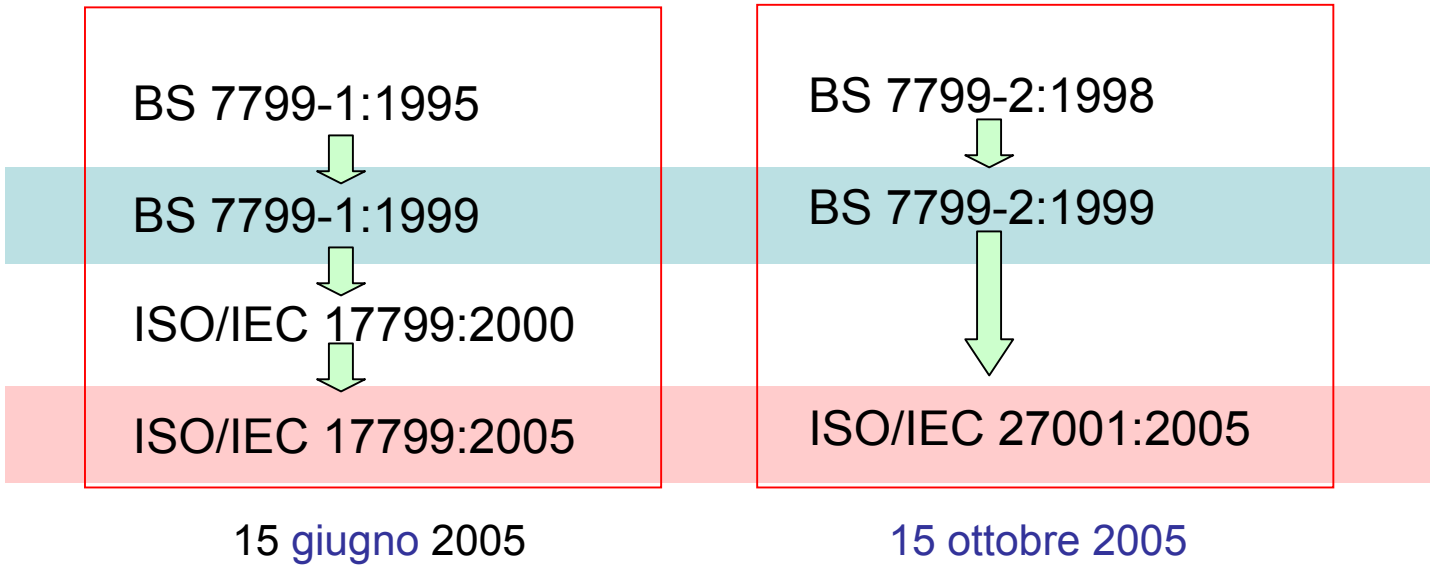
INDICE DELLA PRESENTAZIONE :

1. Situazione al momento degli standard per il SGSI
2. Scenario verso cui si tende
3. Novità nelle Code of Practice
4. Novità nei requisiti del SGSI

5. Riferimenti sitografici
6. Varie – Q&A

Situazione al momento

Situazione al momento degli standard per il SGSI



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Un po' di storia (1/2)

- Inizi degli anni 90'
  - il DTI (Department of Trade and Industry) britannico istituisce un Gruppo di Lavoro, finalizzato a fornire alle aziende una guida per il governo della sicurezza del loro patrimonio informativo

- 1993
  - Il Gruppo di Lavoro produce una raccolta di "best practice" per il governo della sicurezza dell'informazione in ambito industriale

- 1995
  - British Standard Institution (BSI) pubblica lo standard BS7799-1 "*Code of Practice for Information Security Management*" derivato dalla suddetta raccolta
  - La Gran Bretagna sottopone lo standard BS7799 all'ISO/IEC JTC1 SC27 affinché venisse approvato come standard ISO ma, seppure di stretta misura, la proposta non fu accettata.

- 1998
  - BSI aggiunge una seconda parte allo standard intitolata "*Specification for Information Security Management Systems*"

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Un po' di storia (2/2)

- aprile 1999
  - BSI pubblica una nuova versione delle due parti dello standard identificate come BS7799 -1 e BS7799 – 2
- autunno 1999
  - Viene risottoposta all'ISO la richiesta di trasformare il BS 7799 in uno standard internazionale
- dicembre 2000
  - la parte 1 dello standard BS7799 diviene uno standard internazionale ISO (ISO/IEC 17799:2000)
- settembre 2002.
  - rivisitazione della parte 2 dello standard anche per armonizzarla con gli Standard relativi alla Qualità (BS 7799-2:2002)
  - La parte 2 viene sottoposta all'ISO perché divenga anch'essa uno standard internazionale.

Code of Practice

- Non è uno standard da certificazione e non è auditabile

- Propone un catalogo di controlli derivati da pratiche consolidate in ambito industriale e costituiscono regole di buona condotta di applicabilità generale (code of practice)

- L'insieme dei controlli selezionati da un'azienda costituisce una sorta di piano di sicurezza che l'azienda si propone di attuare realizzando i controlli stessi attraverso, misure di sicurezza IT, fisica, procedurale, relativa al personale

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Requisiti del SGSI

- E’ uno standard da certificazione ed è auditabile
- Indica i requisiti per il Sistema di gestione per la sicurezza delle informazioni (SGSI) (Information Security Management System - ISMS)
- Per ottenere la certificazione l’azienda deve dimostrare di aver attivato un SGSI rispondente ai requisiti previsti dallo standard

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

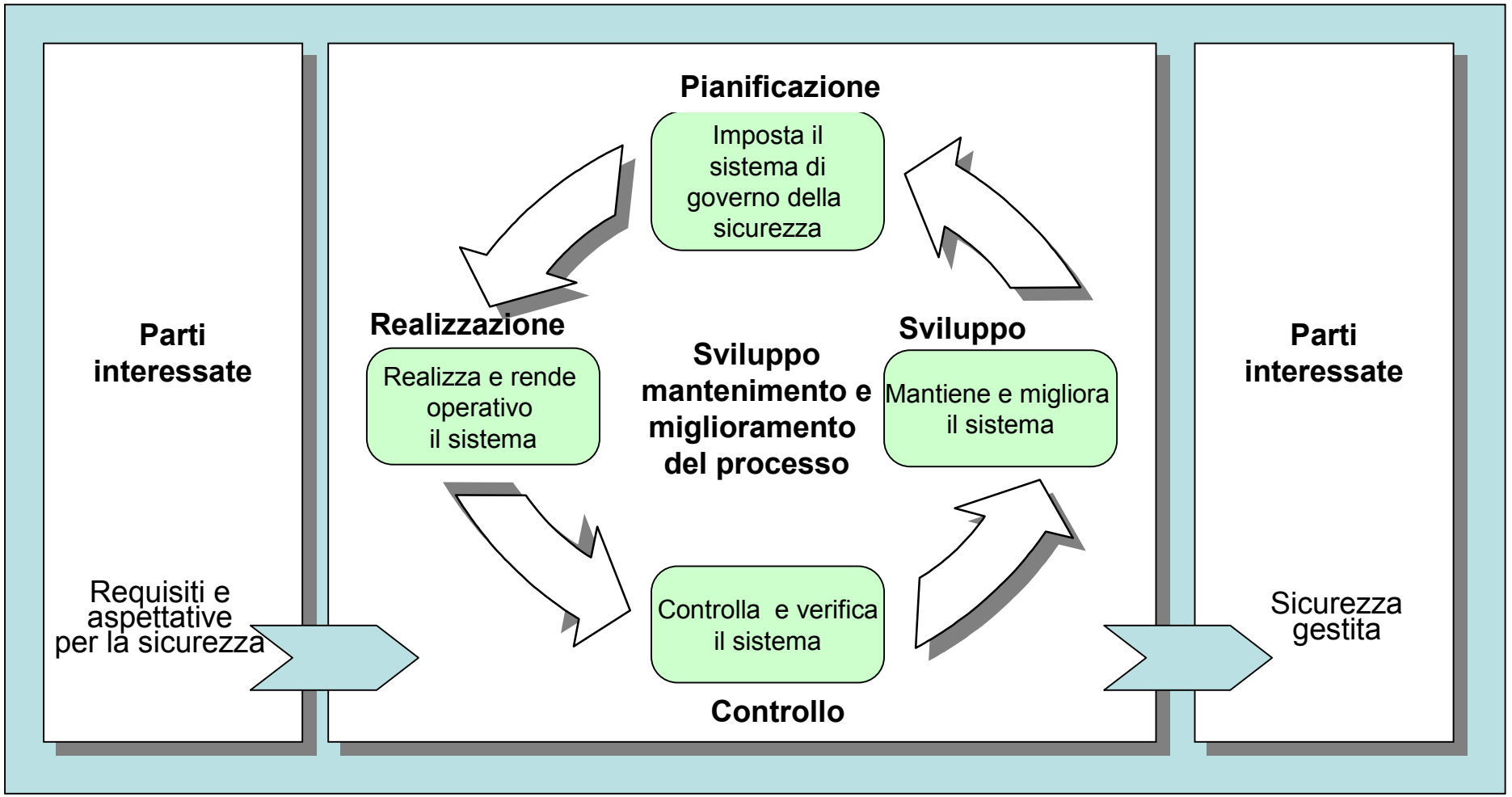
Requisiti del SGSI

- **SGSI -** Sistema di Gestione per la Sicurezza della Informazioni

- L'SGSI è l'insieme della struttura organizzativa, delle responsabilità, dei processi e delle risorse messe in atto per rispondere alle aspettative delle Parti interessate (clienti, utenti, direzione aziendale, istituzioni, ecc.) relativamente alla sicurezza delle informazioni

- L'SGSI ha il compito di assicurare che vengano selezionati e attuati controlli di sicurezza proporzionati ed adeguati al fine di proteggere i beni informativi e di fornire la necessaria confidenza alle parti interessate.

Ciclo di Deming



Situazione inizio 2005

ISO/IEC 17799:2000 Parte 1

Code of practice for information security management

Una raccolta di best practice in materia di sicurezza dell'informazione

BS 7799-2:2002 Parte 2

Information security management systems

Specification with guidance for use

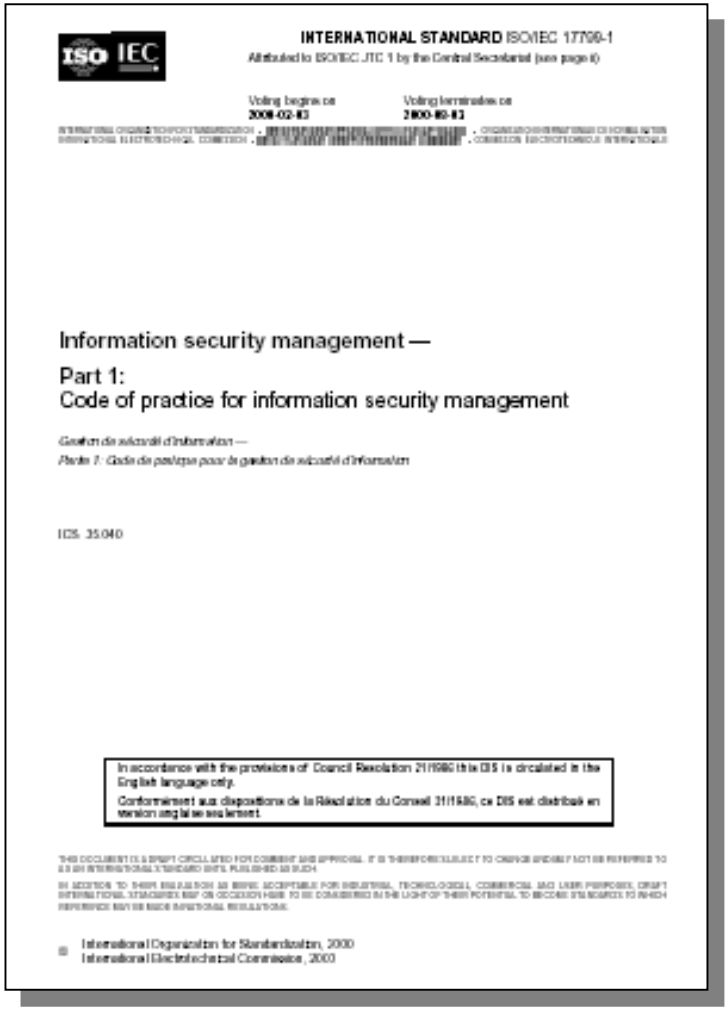
Specifiche del SGSI che costituiscono il riferimento per la certificazione della capacità di un'azienda di saper gestire il proprio patrimonio informativo.

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Linee guida DISC PD 3000

- Information Security Management: An Introduction
- Preparing for BS 7799 Certification
- Guide to BS 7799 Risk Assessment and Risk Management
- Are you ready for a BS 7799 Audit?
- Guide to BS 7799 Auditing

Lo standard ISO/IEC 17799:2000 Code of Practice



INTERNATIONAL STANDARD ISO/IEC 17799-1

Information security management —

Part 1:
Code of practice for information security management

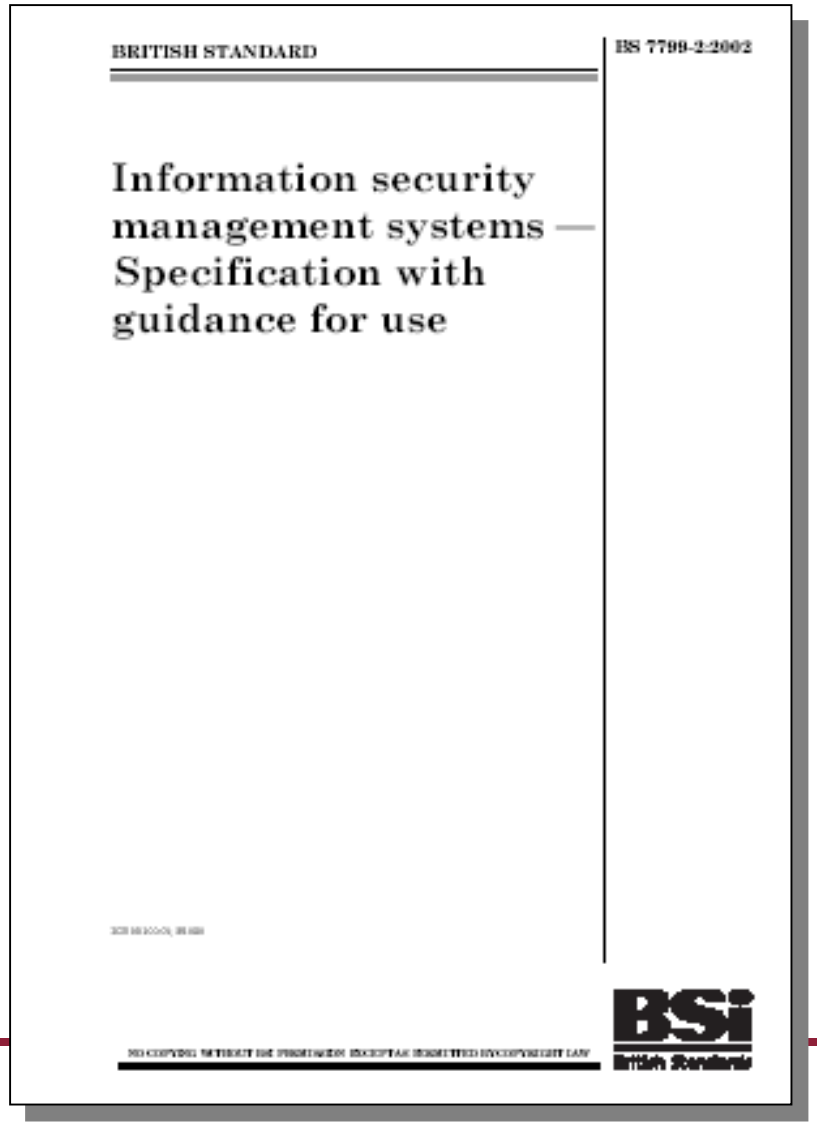
ICS 35.040

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Lo standard BS 7799-2:2002
Requisiti del SGSI

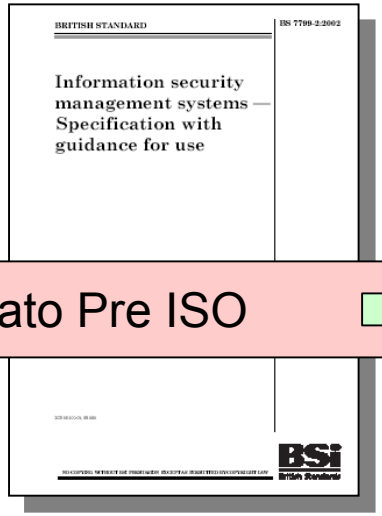


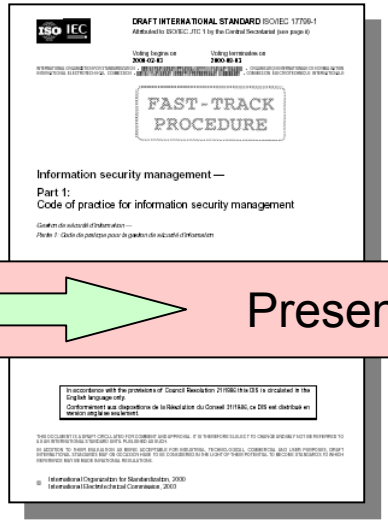
ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Lo standard BS 7799-2:2002
Normativa referenziata

- ISO 9001:2000, Quality management system – Requirements
- ISO/IEC 17799:2000, Information Technology – Code of practice for information security management
- ISO Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standard

Evoluzione degli standard verso ISO





Passato Pre ISO → Presente e futuro ISO

1995-1998 → 1999 → 2000 → 2005

BS 7799 Parte 1
Code of Practice
BS 7799 Parte 2
Requisiti del SGSI

Pubblicazione
Revisioni
Parti 1 & 2

BS 7799 Parte 1
Pubblicata come
ISO/IEC 17799

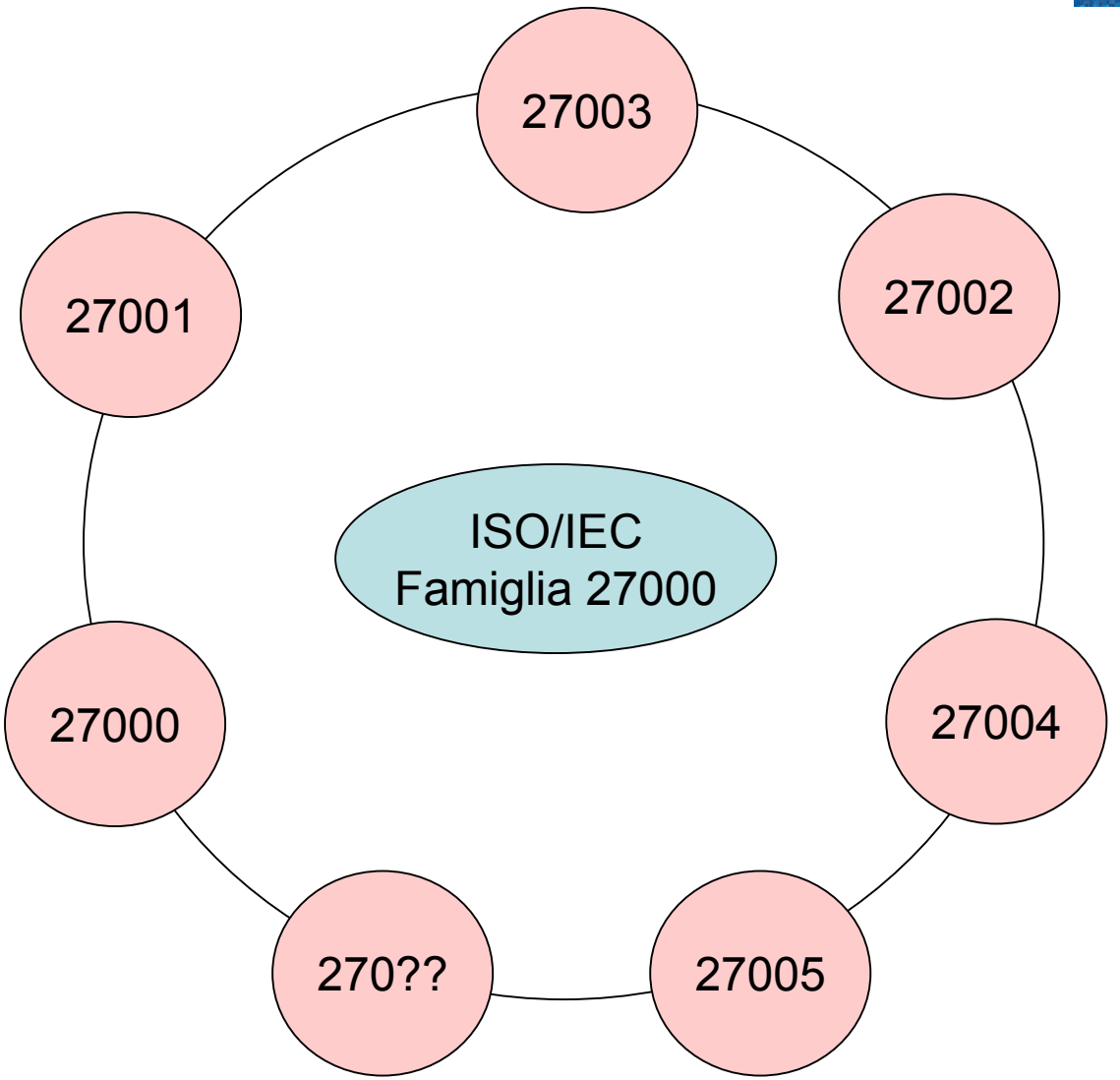
Prima revisione
ISO/IEC 17799
ISO/IEC 27001

INDICE DELLA PRESENTAZIONE :

1. Situazione al momento degli standard per il SGSI
2. Scenario verso cui si tende
3. Novità nelle Code of Practice
4. Novità nei requisiti del SGS

5. Riferimenti sitografici
6. Varie – Q&A

Scenario verso cui si tende



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

ISO/IEC 27000
Principles and vocabulary

- Dovrebbe includere il modello di riferimento per la serie 27000
- Accoglie la definizione dei principali termini e concetti
- Si prevede che venga rilasciato nel primo semestre 2006

ISO/IEC 27001
ISMS Requirements

- Gestione del rischio
  - Assessment del rischio
  - Trattamento del rischio
  - Decisioni da parte della Direzione
- Misurazione dell'efficacia
- Miglioramento continuo
- Specifiche auditabili

ISO/IEC 27002
Code of Practice

- Si prevede che ad aprile 2007 venga rilasciato tale standard forse semplicemente rinominando ISO/IEC 17799:2005
- Non è uno standard da certificazione e auditabile
- Propone un catalogo di controlli derivati da pratiche consolidate in ambito industriale e costituiscono regole di buona condotta di applicabilità generale (code of practice)
- I controlli proposti sono riportati nell'annex A dell'ISO/IEC 27001 come requisiti (*shall* anziché *should*)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

ISO/IEC 27003
ISMS Implementation Guide

- Ha l'obiettivo di fornire una guida operativa per la realizzazione dei requisiti dello standard 27001

- Consigli e aiuti dettagliati relativi a:
  - processo PDCA
  - Ambito del SGSI e politiche
  - Identificazione dei beni
  - Monitoraggio e revisione
  - Miglioramento continuo

- Si prevede che venga pubblicato a fine 2007

ISO/IEC 27004
Measurements

- Ha l'obiettivo di fornire una guida operativa su come misurare l'efficacia del SGSI sia dei processi che dei controlli.
- Affronta i seguenti aspetti
  - scopo degli indicatori
  - modalità di calcolo degli indicatori
  - determinazione dei valori obiettivo degli indicatori
  - cosa misurare, come e quando
  - Responsabilità nel raccogliere e gestire le misure
- Si prevede che venga pubblicato a fine 2007

ISO/IEC 27005
ISMS Risk Management

- Evoluzione dell'ISO/IEC 13335 (GMITS)

- ISO/IEC Technical Report 13335 ISO/IEC Technical Report 13335 Guidelines on the management of IT security (GMITS)
  - .Part 1: Concepts and models
  - .Part 2: Management and planning
  - .Part 3: Techniques for IT security management
  - .Part 4: Selection of safeguards
  - .Part 5: External connections

Management of ICT Security (MICTS)

MICTS Part 1
Nel 27000 e 27003

MICTS Part 2

27005

- Si prevede che venga pubblicato a fine 2007 (2008)

INDICE DELLA PRESENTAZIONE :

1. Situazione al momento degli standard per il SGSI
2. Scenario verso cui si tende
3. Novità nelle Code of Practice
4. Novità nei requisiti del SGSI

5. Riferimenti sitografici
6. Varie – Q&A

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice 2005
Esigenze di revisione

- Migliore leggibilità
- Migliore internazionalizzazione
- Migliore consistenza con l'Annex A 27001
- Tenere in conto le modalità di conduzione del business insorte negli ultimi 5 anni
  - Maggiore uso di servizi esterni
  - Gestione dell'erogazione di servizi
  - Gestione delle vulnerabilità (patch managment)
- Tenere in conto dei nuovi rischi, minacce,
  - Minacce dovute al codice mobile
  - Nuove tecnologie wireless e mobili

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice
Nuova struttura per i controlli

Controllo	Definisce lo specifico controllo Riportato nell'Annex A del 27001 come requisito ("*shall*" anziché "*should*")
Implementation Guide	Fornisce maggiori dettagli per l'attuazione del controllo. Tali informazioni non sono applicabili in tutti i casi.
Altre informazioni	Fornisce ulteriori informazioni ed eventuali fonti (standard, ecc). Non sempre presente.

Code of Practice
Modifica dei controlli

- I controlli sono passati da 127 a 133
- 17 nuovi controlli
- 116 sono direttamente refenziabili al precedente Standard.
  - 19 Identici
  - 74 Lievemente modificati
  - 23 Sostanzialmente modificati
- 8 nuovi obiettivi di controlli
- 5 obiettivi di controlli sono stati risistemati in altri

Code of Practice
Modifica dei controlli

- Allineamento con
  - ISO Guide 73
  - ISO/IEC TR 18044 (information Security Incident Management) introducendo il concetto di evento di sicurezza delle informazioni distinto dal concetto di incidente di sicurezza delle informazioni.
  - 27001 e 27005 (ISO/IEC 13335)

- Enfasi
  - sull'assessment del rischio
  - oltre che sui requisiti legali e normativi, anche sugli obblighi contrattuali in tutte le fasi del SGSI
  - sulla gestione incidenti
  - sui rischi indotti dalle terze parti

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice
Nuovi Capitoli

5	Politica di sicurezza	2
6	Organizzazione della sicurezza delle informazioni	11
7	Gestione dei beni	5
8	Sicurezza delle risorse umane	9
9	Sicurezza fisica e ambientale	13
10	Gestione delle comunicazioni e delle operazioni	32
11	Controllo accessi	25
12	Acquisizione, sviluppo e manutenzione dei sistemi inf.	16
13	Gestione degli incidenti di sicurezza delle informazioni	5
14	Gestione della continuità del business	5
15	Conformità	10

Code of Practice

5. Politica di sicurezza

- Richiede di comunicare la politica di sicurezza anche alle terze parti

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice

6. Organizzazione della sicurezza delle informazioni

- Non viene nominato il Security Forum
- Affidata alla Direzione la competenza a fornire supporto alle attività di sicurezza, a definire le politiche, ad allocare le risorse ecc. in linea con ISO 9001 e ISO 14000
- Accordi di riservatezza (da Sicurezza del Personale)
- Maggiore chiarezza sui rapporti con terze parti (concetto di outsourcing, clienti)

Code of Practice
7. Gestione dei beni

- Inseriti due nuovi controlli relativi a
  - 07.01.2 Proprietà dei beni
  - 07.01.3 Uso accettabile dei beni

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice

8. Sicurezza delle risorse umane

- Riorganizzato sulla base del ciclo di vita del personale
  - 08.01 Prima dell'impiego
  - 08.02 Durante l'impiego
  - 08.03 Fine o cambiamento di impiego

Code of Practice

9. Sicurezza fisica e ambientale

- Poche modifiche
  - Nuovo controllo

    09.01.4 Proteggere da minacce esterne e ambientali.
  - La Clear Desk Policy è stata ricollocata in Responsabilità degli utenti (11.03.3) Controllo Accessi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice

10. Gestione delle comunicazioni e delle operazioni

- Maggiore attenzione alle terze parti

  10.02 Gestione delle forniture di servizi da terze parti
- Nuovo controllo per il codice mobile

  10.04.2 Controllo contro il codice mobile
- Nuova sezione 10.09 dedicata al commercio elettronico
- Maggiore attenzione al monitoraggio dei sistemi (logging e auditing 10.10) con controlli che prima erano nel Controllo Accessi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice
11. Controllo accessi

- Stessa struttura di controlli
  - 11.01 Requisiti di business per il controllo degli accessi
  - 11.02 Gestione degli accessi degli utenti
  - 11.03 Responsabilità degli utenti
  - 11.04 Controllo degli accessi di rete
  - 11.05 Controllo degli accessi al Sistema Operativo
  - 11.06 Controlli degli accessi alle applicazioni e alle informazioni
  - 11.07 Computer portatili e telelavoro
- Eliminati
  - 9.4.2 Percorso obbligato
  - 9.5.1 Identificazione automatica del terminale
  - 9.5.6 Allarme per utente oggetto di coercizione
- Inseriti
  - 11.03.3 Politica di scrivania libera e schermo protetto

Code of Practice

12. Acquisizione, sviluppo e manutenzione dei sistemi informativi

- I controlli sulla crittografia sono ridotti da 5 a 2
  - 12.03.1 Politica sull'uso dei controlli crittografici
  - 12.03.2 Gestione delle chiavi
  - Eliminati Cifratura, Firma digitale e Servizi di non ripudio in quanto ritenuti più vivini alle tecnologie che al concetto di controllo
- Si è preferito non parlare di Autenticazione dei messaggi, ma piuttosto di Integrità dei messaggi (12.02.3)
- Nuovo obiettivo di controlli (12.06 Gestione delle vulnerabilità tecniche)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Code of Practice
13. Gestione degli incidenti di sicurezza delle informazioni

- Nuovo Capitolo
- Segnalazione degli eventi di sicurezza delle informazioni
- Raccoglie controlli già presenti (da Sicurezza del personale, Gestione delle comunicazioni e delle operazioni e Conformità)

Code of Practice

14. Gestione della continuità del business

- Stessa struttura
- Solo lievi variazioni

Code of Practice
15. Conformità

- Stessa struttura
- Solo lievi variazioni

Categoria / Obiettivo dei controlli		Num. Controlli
05	*Politica di sicurezza*	*2*
05.01	Politica di sicurezza delle informazioni	2
06	*Organizzazione della sicurezza delle informazioni*	*11*
06.01	Organizzazione interna	8
06.02	Parti esterne	3
07	*Gestione dei beni*	*5*
07.01	Responsabilità dei beni	3
07.02	Classificazione delle informazioni	2
08	*Sicurezza delle risorse umane*	*9*
08.01	Prima dell'impiego	3
08.02	Durante l'impiego	3
08.03	Fine o cambiamento di impiego	3
09	*Sicurezza fisica e ambientale*	*13*
09.01	Aree protette	6
09.02	Sicurezza degli apparati	7
10	*Gestione delle comunicazioni e delle operazioni*	*32*
10.01	Procedure operative e responsabilità	4
10.02	Gestione delle forniture di servizi da terze parti	3
10.03	Pianificazione e accettazione dei sistemi	2
10.04	Protezione dal codice malevolo e mobile	2
10.05	Back-up	1
10.06	Gestione della sicurezza delle reti	2
10.07	Trattamento dei supporti	4
10.08	Scambio di informazioni	5
10.09	Servizi per il commercio elettronico	3
10.10	Monitoraggio	6

Categoria / Obiettivo dei controlli		Num. Controlli
11	*Controllo accessi*	*25*
11.01	Requisiti di business per il controllo degli accessi	1
11.02	Gestione degli accessi degli utenti	4
11.03	Responsabilità degli utenti	3
11.04	Controllo degli accessi di rete	7
11.05	Controllo degli accessi al Sistema Operativo	6
11.06	Controllo degli accessi alle applicazioni ed alle informazioni	2
11.07	Computer portatili e telelavoro	2
12	*Acquisizione, sviluppo e manutenzione dei sistemi informativi*	*16*
12.01	Requisiti di sicurezza dei sistemi informativi	1
12.02	Corretta elaborazione nelle applicazioni	4
12.03	Controlli crittografici	2
12.04	Sicurezza dei file di sistema	3
12.05	Sicurezza nei processi di sviluppo e supporto	5
12.06	Gestione delle vulnerabilità tecniche	1
13	*Gestione degli incidenti di sicurezza delle informazioni*	*5*
13.01	Segnalazione degli eventi di sicurezza delle informazioni e delle debolezze	2
13.02	Gestione degli incidenti di sicurezza delle informazioni e miglioramenti	3
14	*Gestione della continuità del business*	*5*
14.01	Aspetti di sicurezza delle informazioni relativi alla gestione della continuità	5
15	*Conformità*	*10*
15.01	Conformità ai requisiti legali	6
15.02	Conformità alle politiche di sicurezza e agli standard, e conformità tecnica	2
15.03	Considerazioni sugli audit dei sistemi informativi	2
	Num. Controlli totale	**133**

INDICE DELLA PRESENTAZIONE :

1. Situazione al momento degli standard per il SGSI
2. Scenario verso cui si tende
3. Novità nelle Code of Practice
4. Novità nei requisiti del SGSI

5. Riferimenti sitografici
6. Varie – Q&A

Requisiti del SGSI
Maggior coinvolgimento della Direzione

- I ruoli precedentemente attribuiti al “Security Forum” diventano di competenza della Direzione.
- Resta ferma, comunque, la possibilità di costituire un “gruppo” con specifiche competenza in materia di sicurezza [cfr. Annex A controllo 6.1.1].
- La Direzione deve approvare il rischio residuo proposto [cfr. 4.2.1 h)]
- Deve essere ottenuta l’autorizzazione della Direzione per rendere effettivo ed operativo il SGSI [cfr. 4.2.1 i)]
- la Direzione deve decidere non solo i livelli di rischio accettabile, ma anche i “criteri” per l’accettazione dei rischi [cfr. 5.1 f)]
- la Direzione deve dimostrare il suo impegno anche garantendo che siano condotti audit interni sul SGSI [cfr. 5.1 g)]

Requisiti del SGSI
Ambito e confini del SGSI

Il nuovo standard, relativamente all'ambito del SGSI [cfr. 4.2.1 a)], sottolinea che devono essere definiti chiaramente l'ambito ed i confini del SGSI inclusi i dettagli e le motivazioni per qualunque esclusione dall'ambito

Requisiti del SGSI
Assessment del Rischio

- Deve essere definito e documentato sia l'approccio all'assessment del rischio [cfr. 4.2.1 c)] sia la relativa metodologia per produrre risultati comparabili e riproducibili [cfr. 4.3.1 d)]

- L'assessment del rischio deve essere revisionato a intervalli pianificati [cfr. 4.2.3 d)].

- La revisione Direzionale deve essere effettuata almeno una volta l'anno [cfr. 7.1] e deve prevedere la revisione dell'assessment del rischio ed il piano di trattamento del rischio [cfr. 7.3 b)]

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Requisiti del SGSI
Misurazione dell'efficacia dei controlli

Viene introdotto il concetto di misurazione dell'efficacia dei controlli e degli obiettivi di controllo. In particolare:

- l'Organizzazione deve definire come misurare l'efficacia dei controlli o degli obiettivi di controllo selezionati e deve specificare come queste misure saranno usate per valutare l'efficacia dei controlli al fine di produrre risultati paragonabili e riproducibili (cfr. 4.2.2)
- tali misure devono essere utilizzati nell'attività di monitoraggio e di revisione del SGSI (cfr. 4.2.3). In particolare:
  - tra i dati di input della revisione del SGSI devono essere inclusi i risultati derivanti dalla misurazione dell'efficacia [cfr. 7.2]
  - tra i dati di output della revisione del SGSI devono essere inclusi anche i miglioramenti da apportare alle modalità di misurazione dell'efficacia dei controlli [cfr. 7.3]
  - la documentazione del SGSI deve includere una descrizione delle modalità adottate per valutare l'efficacia dei controlli al fine di produrre risultati paragonabili e riproducibili [cfr. 4.2.2; 4.3.1 g)]

INDICE DELLA PRESENTAZIONE :

1. Situazione al momento degli standard per il SGSI
2. Scenario verso cui si tende
3. Novità nelle Code of Practice
4. Novità nei requisiti del SGSI

5. Riferimenti sitografici
6. Varie – Q&A

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Certificazione Transitorio

Il BSI si attende, per le organizzazioni già certificate BS 7799-2:2002, che le differenze tra il vecchio ed il nuovo standard vengano registrate dal valutatore durante la prossima visita ispettiva come osservazioni/commenti.

Una volta terminato il periodo di transizione (18 mesi) queste si trasformano in non conformità e la certificazione diventa a rischio.

www.asia.bsi-global.com/ India+InformationSecurity/ISO_27001v4.pdf

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Certificazione Transitorio

Il SINCERT ha comunicato agli Organismi di certificazione accreditati allo schema SSI BSI che:

- Fino al 31 marzo 2006 possono certificare secondo la norma BS 7799-2:2002

- Le certificazioni rilasciate ai sensi della norma BS 7799-2:2002 scadranno il 31 marzo 2007

www.sincert.it/docs/4072005UTC082.pdf

Riferimenti Sitografici

www.27000.org

asia.bsi-global.com/ India+InformationSecurity/ISO_27001v4.pdf
Illustrazione BSI delle novità 27001
www.sincert.it/docs/4072005UTC082.pdf

www.aiea.it/pdf/INFOAIEA/INFOAIEA20053b1.pdf -
Articolo di Gallotti

groups.yahoo.com/group/iso-27001
groups.yahoo.com/group/iso17799security
Gruppi di discussione

www.27001-online.com/
ISO 27001 Online

www.XISEC.com

Domande?

Grazie dell'attenzione