

Panorama legislativo: ambito volontario

Sistemi di Gestione per la Sicurezza delle Informazioni

Perché parliamo di sicurezza delle informazioni

- Rischio reale
- Effetto *media*
- Diffusione ICT
- Evoluzione tecnologica
- Protezione delle informazioni del paziente
- Responsabilità e conseguenze legali

La legislazione in materia

- D. Lgs 518/92 (L. 633/41)
- L. 547/93
- L. 513/97
- D. Lgs 318/99
- L. 248/00 (L. 633/41)
- Reg. 338/01 (S.I.A.E)
- D. Lgs 231/01
- D. Lgs 70/2003 (Artt. 14 e segg.)
- D. Lgs. 196/03
- D. Lgs. 30/05 (Art. 98)
- D. Lgs 82/05 (Ammin. Digit.)
- L. 155/05 (Pacchetto Pisanu)

La serie ISO 27000

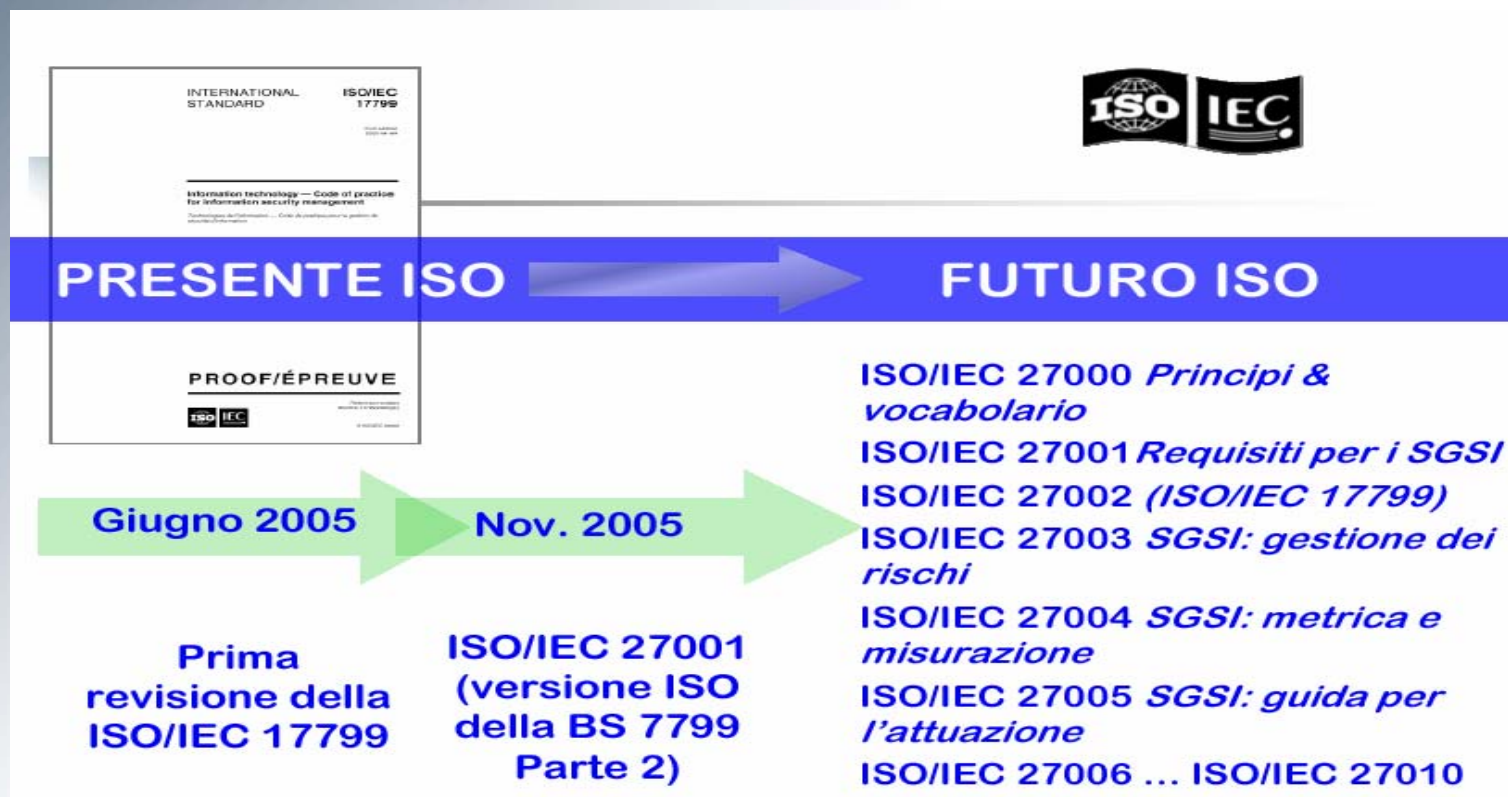
- L'adozione della ISO 27001:05 ha lo scopo di garantire:
 - **la conformità,**
 - **l'efficacia,**della sicurezza delle informazioni all'interno di una organizzazione (pubblica o privata).
- Sicurezza delle informazioni intesa come:
 - **Riservatezza,**
 - **Integrità,**
 - **Disponibilità.**
- Efficacia intesa come:
 - **continuità del business,**
 - **minimizzazione dei danni in caso di incidenti,**
 - **massimizzazione degli investimenti e miglioramento dell'efficacia.**

Fasi dello sviluppo

- Politica
- Campo di applicazione e perimetro
- Inventario
- ***Valutazione dei rischi***
- Contromisure
- Piano trattamento dei rischi
- Dichiarazione applicabilità
- Formazione
- Attuazione
- Monitoraggio
- Miglioramento



L'evoluzione della norma



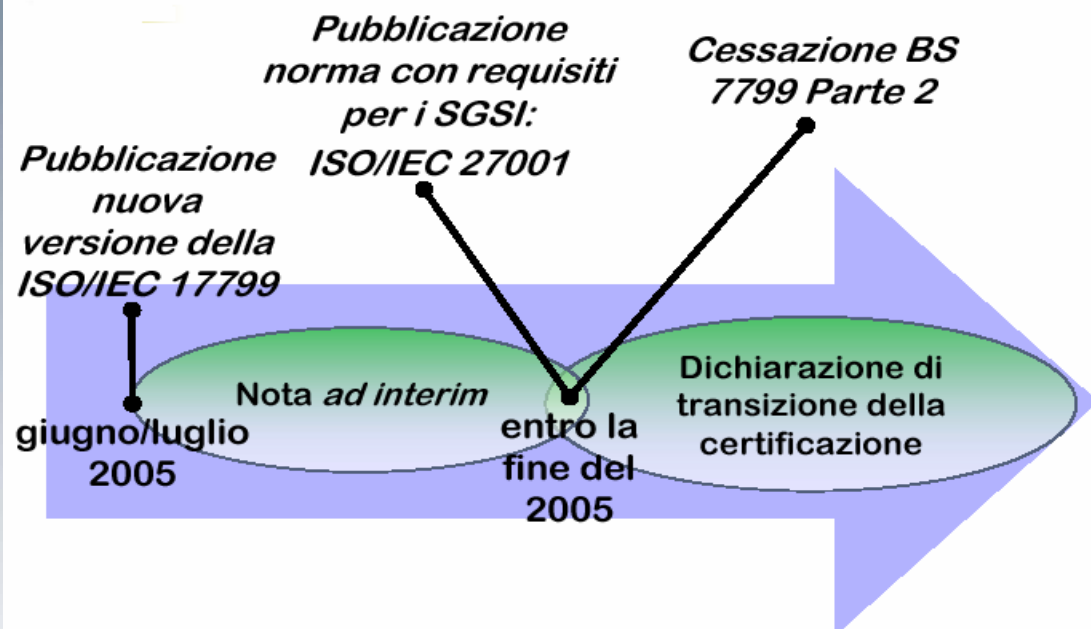
La certificazione dei SGSI



La certificazione dei SGSI

Dichiarazione di transizione della certificazione

(Definisce il periodo durante il quale si trasferiranno le conformità delle certificazioni dalla BS 7799 Parte 2 alla ISO/IEC 27001)



SINCERT 13/12/05

- **03/2006: STOP a BS7799**
- **03/2007: fine transizione**

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

Trend certificazioni nel mondo


- Circa 2500 certificazioni già emesse (BS7799)

*Si stima che il recepimento
ISO possa portare i certificati
a 5.000 unità entro 18 mesi!!*

Situazione certificazioni in Italia

- Ad oggi sono stati rilasciati 158 certificati corrispondenti a circa 50 aziende
- L'Italia è uno dei primi paesi al mondo ad aver rilasciati certificati ISO 27001 sotto accreditamento SINCERT
- Il trend è in crescita costante
- La richiesta di certificazione da parte delle Pubbliche Amministrazioni potrebbe far crescere ulteriormente il trend

International User Group (www.xisec.com)



Information Security Management Systems ISO 27000 Series (including ISO/IEC 27001 (revised BS 7799 Part 2) and ISO/IEC 17799)

Welcome to the official web site of the

ISMS International User Group (established 1997) and the World of Information Security Management Systems


[REVISION OF ISO/IEC 17799 'HOT OFF THE PRESS' TUTORIALS see 7799 events page.](#) [Visit the Certificate Register](#)

Responding to demands from the international community over the last twelve years for best practice and certification of information security management the standards ISO/IEC 17799, the (revised version of BS 7799 Part 2:2002) and BS 7799 Part 2:2002 have developed and evolved. The application and use of these standards has been taken up by organisations small, medium and large in many parts of the world as a "common language" for information security management *to ensure business continuity, minimise business damage by preventing and minimising the impact of information security incidents and to maximise business investments and opportunities.* The ISMS International User Group is a business-led, international network of users of ISO/IEC 17799 and BS 7799 Part 2. It was established (Department of Trade and Industry) in 1997 to facilitate a means of sharing experiences in the use of these standards. The ISMS International User Group and this web site continues to be successful as part of their wider promotion of best practice to the business community.

Ted Humphreys, Director and Founder of the ISMS International User Group

On this web site you will find a vast range of information relating to ISO/IEC 17799, the NEW ISO/IEC 27001 (revised version of BS 7799 Part 2:2002) and BS 7799 Part 2:2002

The official ISMS IUG web site.



ISMS IUG & info

Home
News
About the IUG
IUG Membership
ISMS Foundation
ISMS FAQs
7799 Events
Certificate Register
Certification Portal
Members Page
Related Sites

IN COLLABORAZIONE CON



Consulta Nazionale Atop Giovani

Capitoli internazionali



Information Security Management Systems ISO 27000 Series (including ISO/IEC 27001 (revised BS 7799 Part 2) and ISO/IEC 17799)

- Home
- News
- About the IUG
- IUG Membership
- ISMS Foundation
- ISMS FAQs
- 7799 Events
- Certificate Register
- Certification Portal
- Members Page
- Related Sites

IUG CHAPTERS

The following is a list of National ISMS International User Group

Australia	John Snare Chair
Brazil	Ariosto Farias jr Chair
Canada	Marc-André Léger Chair (www.leger.ca) Web site www.ismsiug.ca
France	
Germany	Angelika Plate Chair Web site www.aexis.de
Hong Kong & Macau	Dale Johnstone Chair
Italy	N Sathyan Chair Chair Fabrizio Cirilli Web site www.ismsiugitaly.net

The official ISMS IUG

Capitolo italiano
www.ismsiugitaly.net

[ISMS IUG Aims](#)



Italian ISMS Chapter
Reg. 05/017

- Le coordinate bancarie del Capitolo sono: BANC

Italian ISMS Chapter

[chi siamo](#)
[news](#)
[organizzazione](#)
[links](#)
[contatti](#)
[adesione](#)

HOME

L'International User Group (IUG) riunisce gli utilizzatori dei sistemi di gestione della sicurezza delle informazioni (ISMS) secondo lo standard ISO 27000 (ex BS7799) e norme collegate. Il Capitolo Italiano si pone in modo specifico i seguenti obiettivi:

- Favorire la divulgazione dello standard ISO 27000 e delle norme collegate in Italia e contribuire allo sviluppo e alla diffusione della cultura della sicurezza delle informazioni, organizzando o aderendo a meeting, workshop, pubblicazioni, corsi
- Scambiare esperienze e informazioni con chiunque (associazioni, gruppi di ricerca, università, scuole, amministrazioni pubbliche, aziende, professionisti, ecc.) abbia interesse verso i sistemi di gestione per la sicurezza delle informazioni e nelle tematiche connesse.
- Interagire con tutti i capitoli esteri su problematiche applicative della serie ISO 27000, sui risultati delle applicazioni e diffondere tali informazioni nel mercato italiano.
- Sostenere il mercato (aziende, consulenti, organismi di certificazione e di accreditamento, associazioni, università ecc.) nell'applicazione dello standard.
- Creare opportunità di lavoro garantendo processi di qualificazione/certificazione del personale atti ad assicurare un costante ed elevato livello di professionalità.

Il Capitolo è aperto a chiunque voglia contribuire allo sviluppo delle tematiche oppure essere informato in materia di sicurezza delle informazioni. La regolamentazione del

Composizione del Capitolo

- Presidente (chairman)
- Vice Presidente
- Segretario generale
- Revisore dei conti

- Membro del comitato ISO WG1/SC27
- Membro del comitato IAF “task force ISO 27001” per la definizione della ISO 27006

Fabrizio Cirilli

Nico Mastrorillo

Sergio Boero

Ottorino Pomilio



Grazie per l'attenzione.
Per qualsiasi ulteriore informazione e chiarimento:

Fabrizio Cirilli

www.xisec.com
www.ismsiugitaly.net
chairman@ismsiugitaly.net