



Misure di Tutela e Aspetti Legali nel contesto del Cloud Computing

La certificazione di
sistema per aumentare il
“trust” cliente-fornitore



The speaker



- **Fabrizio Cirilli**

- Oltre 20 anni di esperienza nella gestione di progetti nell'ambito dell'ICT nella progettazione, sviluppo, gestione e audit per la sicurezza delle informazioni
- Lead auditor certificato ISO 27001, ISO 20000, ISO 9001 e TL 9000
- Opera in qualità di consulente ed auditor sia in Italia che all'estero
- Docente:
 - nei corsi accreditati per ISO lead auditor e security manager (CISM)
 - Al Master di 2^{do} livello in "gestione della sicurezza delle informazioni" dell'Università La Sapienza di Roma
- Membro IEEE, CLUSIT, ISACA, AIPSI, UNINFO
- Membro attivo e rappresentante per l'Italia ne:
 - Comitato ISO JTC1/SC27 per la famiglia ISO 27000
 - ISO/IAF Task Force group per la ISO 27006
 - UNINFO per la normalizzazione degli standard per la sicurezza delle informazioni
- ICT Product Manager per TÜV Italia Srl



Obiettivi dei capitoli

- favorire la divulgazione dello standard ISO 27000 in Italia e contribuire allo sviluppo e alla diffusione della cultura della sicurezza delle informazioni, organizzando o aderendo a *meeting*, *workshop*, pubblicazioni e 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.
- Sostenere il mercato (aziende, consulenti, organismi di certificazione e di accreditamento) nell'applicazione dello standard.
- Creare opportunità di lavoro garantendo processi di qualificazione / certificazione atti ad assicurare un costante ed elevato livello di professionalità ed etica



Gli altri chapters

<http://www.iso27001certificates.com/>

International Register of ISMS Certificates

Certificate Register
ISMS Standards
Certification Process
ISMS FAQs
ISMS IUG
Home

The grouping of international IUG chapters includes:

- Australia (contact john.snare@bigpond.com)
- Brazil (contact af15j@terra.com.br)
- France (contact Gerome.BILLOIS@solucom.fr)
- Germany (contact aaxisap@aol.com)
- Hong Kong (contact djo3500@hotmail.com)
- Iran (contact Info@scanit.ir)
- Italy (contact www.ismsiugitaly.net)
- Japan (contact ko-nakao@nict.go.jp)
- Korea (contact park.taewan@gmail.com)
- Poland (contact elzbieta.andrukiewicz@energotel.pl)
- Spain (contact www.ismsforum.es)
- Sweden (contact bengt.rydstedt@sis.se)
- UK (see [web page](#))



ISMS IUG ITALY in UNINFO

**Dal 2010 ISMS IUG ITALY
è in UNINFO!**

° Riunione

**Gruppo di lavoro
"Serie ISO/IEC 27000"**

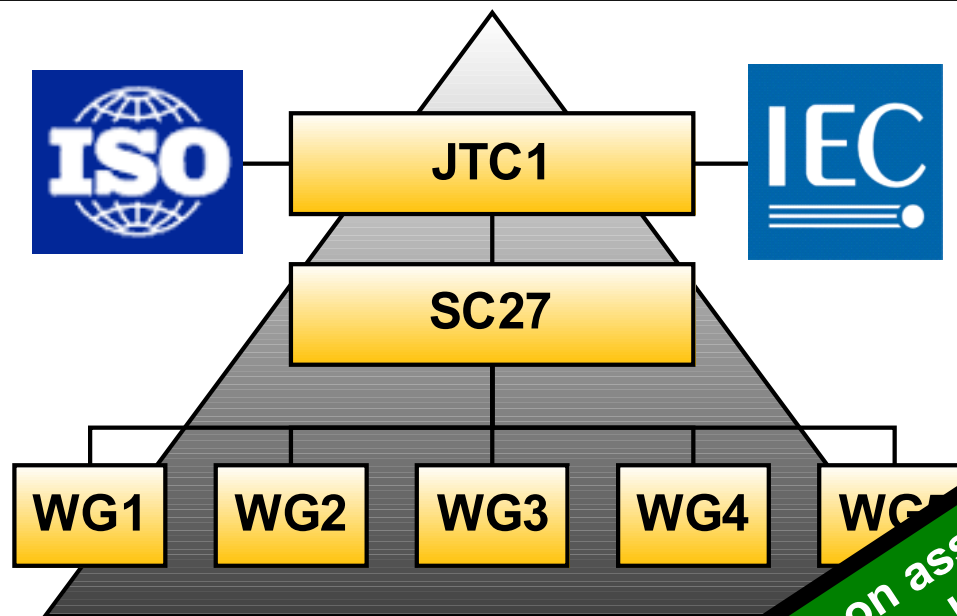
Milano

19 Maggio 2010



UNINFO

Organizzazione del JTC1 / SC27



- **WG1** ISMS Standards
- **WG2** Security Techni
- **WG3** Security Evalua
- **WG4** Security Controls
- **WG5** Privacy, Biometric,

Molte liason assicurano
L'integrazione e l'integrabilità
Della famiglia ISO 27xxx con
altri standard, modelli organizzativi
e tecnologie



Famiglia ISO/IEC 27xxx

- **27001:2005** ISMS requirements
- **27002:2005** Code of practice for ISM
- **27007** ISMS auditing guidelines
- **27008** Guidance for auditors on ISMS controls
- **27010** ISM for inter-sector and inter-organisational communications
- **27013** Guidance on the integrated implementation of ISO/IEC 20000 and ISO/IEC 27001
- **27014** Governance of information security
- **27015** Information security management guidelines for financial and insurance services



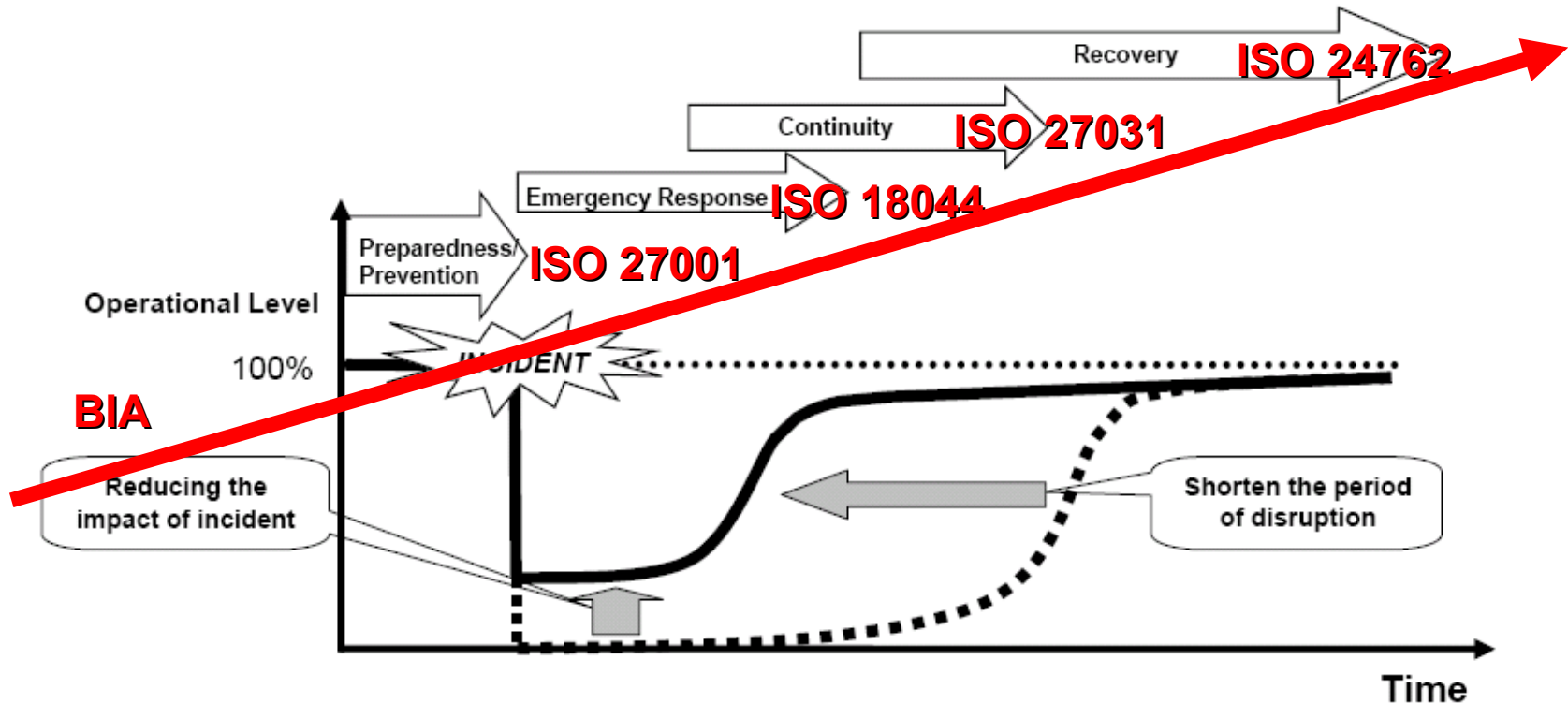
Famiglia ISO/ IEC 27xxx

- **27031** Guidelines for ICT readiness for Business Continuity
- **27032** Guidelines for Cybersecurity
- **27033-1** Guidelines for network security
- **27033-2** Guidelines for the design and implementation of network security
- **27033-3** Reference network scenarios – Risks, design techniques and control issues
- **27034** Application Security
- **27035** Information security incident management
- **27036 Guidelines for security of outsourcing**
- **27037** Guidelines for identification, collection and/or acquisition and preservation of digital evidence

ISMS: perchè?

- La ISO/IEC 27001:05
 - Ha l'obiettivo di assicurare:
 - **l'efficacia e**
 - **la conformità**della sicurezza delle informazioni in organizzazioni pubbliche e/o private.
 - E' focalizzata su:
 - **riservatezza,**
 - **integrità,**
 - **disponibilità**delle informazioni, secondo quanto necessario o richiesto a livello contrattuale o interno.
 - L'efficacia è intesa come:
 - **Business continuity,**
 - **Minimizzazione dei danni in caso di incidente,**
 - **Ottimizzazione degli investimenti e miglioramento dell'efficacia**

Parola d'ordine: continuità del servizio



- Before Introduction/Implementation of IPOCM
- After Introduction/Implementation of IPOCM

Integrare per competere

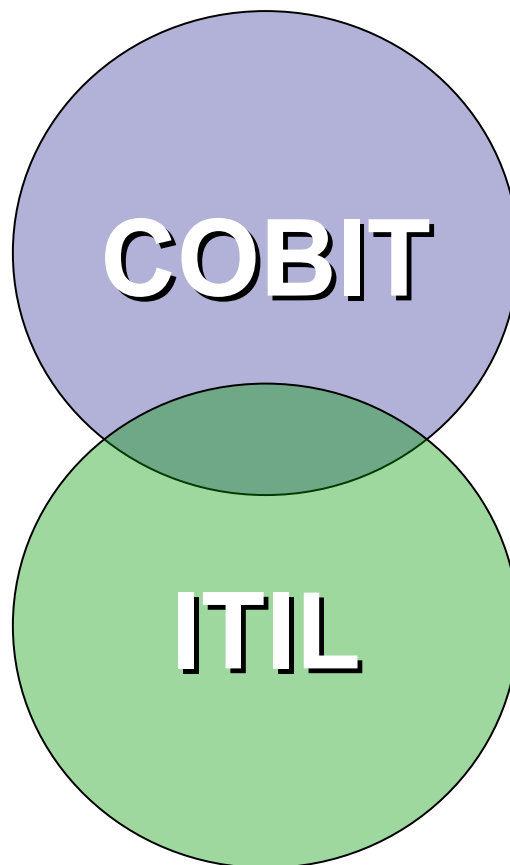
È uno dei modelli di ICT governance più diffusi nel mondo, proviene dagli USA creato da ISACA

COBIT
ICT Governance

È il modello per l'IT Service Delivery/Support per eccellenza, proviene dall'UK creato dall'OGC

ITIL
Service Delivery
&
Service Support

Integrare per competere





SISTEMA INTEGRATO AZIENDALE

La certificazione della qualità dei processi IT

La certificazione dell'IT Service Delivery (secondo ITIL v2)

La certificazione della sicurezza delle informazioni

L'ultimo "miglio" della sicurezza: ISO 27001 e OSSTMM



Livello strategico

**Approccio top down alla
Sicurezza delle Informazioni
dalla politica al rischio residuo**

ISO 27001

Livello tattico

OSSTMM ?

Livello operativo

**Approccio bottom up alla
sicurezza delle informazioni
dalle vulnerabilità agli asset**

- Come assicuro che gli investimenti abbiano realmente soddisfatto le attese?
- Quale sarà il reale grado di sicurezza del mio Sistema?
La certificazione ha realmente portato sicurezza o solo consapevolezza del tema?



Quanti certificati fino ad oggi?

Oltre 6000 nel mondo!



Perché certificarsi?

- Richiesta del mercato (PPAA in testa) o clienti strategici
- Fiducia e fidelizzazione dei clienti
- Obiettivo interno
- Dimostrazione verso shareholders/stakeholders
- Finanziamenti



Fattori che influenzano la certificazione

- Definizione
 - del perimetro
 - del campo di applicazione
 - del numero di persone incluse nel perimetro
 - dei siti inclusi nel perimetro
 - del grado di complessità in base ai processi produttivi e di sicurezza
- Presenza di una metodologia consolidata di risk assessment e di valutazioni ripetibili e confrontabili che dimostrino il miglioramento nella gestione dei rischi
- Definizione del livello di rischio accettabile e accettazione del livello di rischio residuo da parte della Direzione
- Dimostrazione dell'efficacia
 - delle contromisure adottate a fronte dei rischi valutati
 - del SGSI
- Completamento di almeno un programma di audit interni (che abbiano verificato e dimostrato la conformità ad ogni requisito della norma e ad ogni altro requisito definito)
- Completamento di almeno due cicli (PDCA) in modo da dimostrare il miglioramento continuo
- Disponibilità di almeno due riesami della Direzione



Le più comuni debolezze nei SGSI

- Scarsa conoscenza degli aspetti legali e contrattuali (dlg 196/03, dlg 231/01, L 262/05, L 48/2008, SLA, carte dei servizi ecc.) e delle interazioni con altre discipline (ad es. sicurezza sul posto di lavoro)
- Management “disattento” alla sicurezza delle informazioni (“è un costo”, “è un ostacolo”)
- Scarso collegamento della sicurezza con gli aspetti economico finanziari (tagli, budget insufficienti o inesistenti, ROI)
- Poco orientati agli utilizzatori ed al mercato (complessi e burocratici)
- + conformità – efficacia (certificazione invece che sicurezza)
- Troppo tecnicismo e poca organizzazione (+ firewall - cultura)
- Outsourcing “indiscriminato” inclusi audit interni (scarso controllo)
- Documentazione eccessiva (rispetto alle reali esigenze), obsoleta (rispetto al reale stato del SGSI) o incompleta (rispetto a quanto richiesto dalla norma)
- Scarsa disponibilità al confronto con altre realtà ed alla partecipazione a eventi e gruppi di studio
- Maggior orientamento alla gestione dell’incidente anziché alla prevenzione degli incidenti
- Scarsa propensione alle prove (*Murphy è in agguato!*)



Considerazioni

- **“La coperta è sempre (più) corta”**
 - Inseguendo le nuove vulnerabilità (pharming, phishing...) dimentichiamo i vecchi “trucchi” (ricordate il film: La stangata?)
- **Integrazione**
 - Approccio olistico alla sicurezza (sul lavoro, delle informazioni, ambientale, etica ecc.)
- **Risk awareness**
 - La sicurezza basata sulle persone è flessibile e dinamica, quella basata sui sistemi è rigida e statica
- **“Sicurezza invisibile”**
 - Approccio proattivo, diffuso, a basso costo, poche regole ma chiare
- **“Security by obscurity”**
 - Ti confido un segreto, prometti di non dirlo a nessuno...
- **“L’unione fa la forza”**
 - Azioni e reazioni coordinate, sinergie moltiplicano la forza
- **Quello che sei, quello che hai, quello che sai**
 - Un paradigma vincente ma poco conosciuto



Il ruolo del fornitore e gli strumenti

- **La sicurezza nei contratti**
 - Patti chiari amicizia lunga
- **Il peso degli UC sugli SLA**
 - Ciò che non puoi misurare...
- **Il contratto di outsourcing**
 - Come iniziare, come proseguire, come finire
- **L'audit in campo**
 - Lì tutto è diverso!
- **Il monitoraggio del servizio**
 - Vediamo come sta andando
- **Il miglioramento delle performances**
 - Cosa non va e cosa possiamo migliorare
- **La gestione degli errori**
 - Evoluzione o correzione



Domande?

Grazie per l'attenzione

Fabrizio Cirilli
cirillif@tin.it