SECURITY SUMMIT

**Seminario associazioni:**
**Seminario a cura di *it*SMF Italia**

# Sistemi di gestione integrati
# Come la ISO/IEC 20000 può essere di supporto alla ISO/IEC 27001

Cesare Gallotti

Milano, 14 marzo 2011

itSMF ITALIA

# Agenda

- Presentazione
- Le norme ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27012
- Confronto tra le norme
- Alcune considerazioni

- Presentazione
- Le norme ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27012
- Confronto tra le norme
- Alcune considerazioni

# Cesare Gallotti

- Cesare Gallotti: dal 1999 nel campo della sicurezza delle informazioni, della qualità e dell'IT Management System.
- Dal 2008 è libero professionista: consulenza, formazione, Lead Auditor ISO/IEC 27001 e ISO 9001 per DNV Italia.
- Precedentemente, ha collaborato in Quint, in DNV Italia, in Intesis e Securteam.
- Ha pubblicato numerosi articoli e un libro (2002)
- Dal 2008 cura la newsletter IT Service Management News
- Per sito web, blog e newsletter: www.cesaregallotti.it

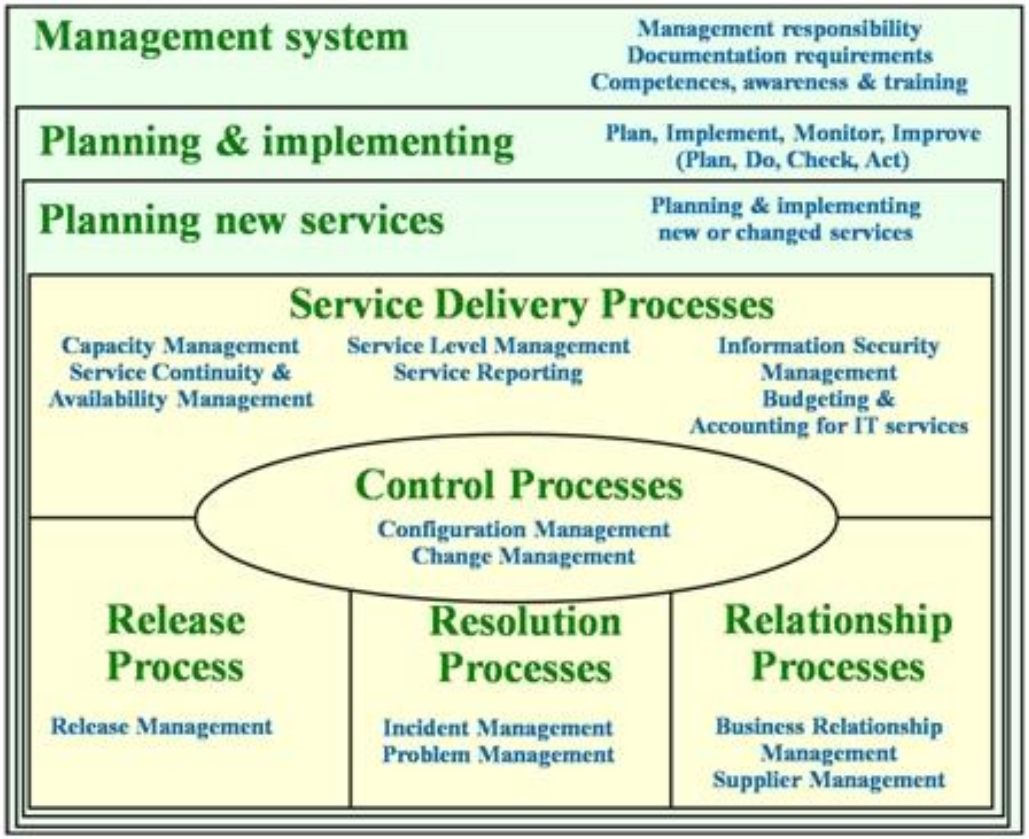
- Presentazione
- Le norme ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27012
- Confronto tra le norme
- Alcune considerazioni

# ISO/IEC 20000-1

- ISO/IEC 20000-1:2005: “Information technology — Service management — Part 1: Specification”
- Le altre parti:
  - part 2: Code of Practice
  - part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
  - part 4: Process reference model
  - part 5: Exemplar implementation plan for ISO/IEC 20000-1
- Il Final Draft della nuova ISO/IEC 20000-1 è stato approvato a inizio 2011 e quindi la norma dovrebbe essere pubblicata come ISO/IEC 20000-1:2011
  - estesi alcuni requisiti per renderli più chiari
  - tolte alcune incongruenze e refusi

# Struttura della ISO/IEC 20000-1

La “classica” figura per presentare come è strutturata la ISO/IEC 20000-1



# ISO/IEC 27001:2005

- ISO/IEC 27001:2005 “Information technology — Security techniques — Information security management systems — Requirements”
- La famiglia delle norme ISO/IEC 270xx comprende anche:
  - ISO/IEC 27000:2009 “Overview and vocabulary”
  - ISO/IEC 27002:2005 “Code of practice for information security management”
  - altre linee guida
- Stato di aggiornamento:
  - a novembre 2010 il ISO/IEC JTC 1/SC 27 ha emesso il 4WD della ISO/IEC 27001 (il percorso non si prevede breve)
  - la nuova versione si baserà sulla “Common Structure for Management Systems” della ISO

# Struttura della ISO/IEC 27001:2005

- La ISO/IEC 27001:2005 è suddivisa in più parti
- La prima parte (capitoli 0-3) è un'introduzione
- La seconda parte (capitoli 4-8) presenta i requisiti di sistema
  - riconoscibile l'impostazione sul ciclo PDCA
  - requisiti simili a quelli della ISO 9001:2000
- La terza parte (Annex A) presenta i controlli di sicurezza
  - 133 controlli suddivisi in 11 capitoli (da A.5 a A.15)
  - alcune ridondanze con i requisiti di sistema
- Infine, vi sono 2 allegati informativi e la bibliografia

# ISO/IEC 27013

- ISO/IEC 27013 “Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1”
- Novembre 2010: emissione del 3WD del ISO/IEC JTC 1/SC 27 basato sulle versioni del 2005 della 27k e 20k
- Il numero di contributi è abbastanza ridotto (i partecipanti saranno più interessati agli standard di requisiti...)

- Presentazione
- Le norme ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27012
- Confronto tra le norme
- Alcune considerazioni

# Nota

- La presentazione segue lo schema del 3WD della ISO/IEC 27013.
- Una parte delle riflessioni sono tratte dal 3WD della ISO/IEC 27013 e riassunte
- La sintesi esposta è necessariamente incompleta
- Un’altra parte delle riflessioni non sono riferibili al 3WD ISO/IEC 27013.
- La redazione di uno standard come la ISO/IEC 27013 deve prendere necessariamente in considerazione e consolidare il parere di molte parti interessate: in alcuni punti è generico e alcuni temi non sono ancora stati affrontati compiutamente

# Benefici di un'integrazione

- Dal 3WD della ISO/IEC 27013:
  - credibilità nei confronti dei clienti interni ed esterni di un'organizzazione e di un servizio corretto, eccellente e sicuro
  - l'abbassamento dei costi a fronte di due sistemi di gestione (da progettare, da implementare e da mantenere) integrati
  - la riduzione del tempo necessario per lo sviluppo e il mantenimento nel tempo di processi conformi ai due standard
  - l'eliminazione di duplicazioni non necessarie
  - una migliore relazione tra il personale dedicato alla gestione dei servizi e di quello dedicato alla sicurezza, grazie alla condivisione dei punti di vista
  - utilizzo delle best practices di tutti e due gli standard

# Diversi punti di partenza

1. Nessun Management System basato su uno dei due standard
2. Un Management System basato su uno dei due standard
3. Due Management System basati sui due standard ma non integrati

- Da considerare:
  - la presenza di altri Management System (es. QMS)
  - i servizi, i processi e le loro interdipendenze
  - gli elementi di ciascun standard e come questi possono essere condivisi o rimanere separati
  - gli impatti sulla tecnologia utilizzata
  - gli impatti e i rischi sui servizi e sulla loro gestione, sulla sicurezza e sulla sua gestione
  - le fasi di transizione
  - gli ambiti (scope): alcuni ISMS escludono la progettazione, alcuni ITSMS includono solo alcuni servizi

# Potenziali conflitti (1/2)

- Gli asset
  - ISO/IEC 27001:2005: “Anything that has value to the organization”
  - ITILv3: “Risorse e capacità. Gli asset includono ogni cosa che può contribuire alla gestione di un servizio.
  - ISO/IEC 20000-1:2005: “Configuration item (CI) - Component of an infrastructure or an item which is, or will be, under the control of configuration management”
  - un asset per l’ITSMS è ben diverso da un information asset.
- Progettazione e messa in produzione dei servizi IT
  - Quasi assente dalla 27k (è richiesta un’opportuna interpretazione dei controlli di sicurezza). Nel 3WD della ISO/IEC 27002 c’è un controllo “Information security in projects”
  - Presente nella 20k e molto migliorato nella versione ora approvata
  - La base della ISO 9001 (versione 2000 e 2008) è stata ignorata
  - La base fornita dalla 20k dovrebbe essere presa come base per gli analoghi processi della 27k, visto che si parte dalla RFC alla chiusura del change (Post Implementation Review), passando dalla determinazione dei requisiti e dai test

# Potenziali conflitti (2/2)

- Risk Assessment
  - Il risk assessment della ISO/IEC 27001:2005 (capitolo 4) è difficilmente correlabile alla gestione dei rischi presente nella ISO/IEC 20000-1:2005.
  - I risk assessment sono visti da diversi punti di vista (rischi "gestionali" rispetto alla sicurezza, rischi tecnologici, rischi di sostenibilità, eccetera)
- Incident management
  - ISO/IEC 27001:2005: "Information security incident - A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"
  - ISO/IEC 20000-1:2005: "Incident - Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service"
  - FDIS ISO/IEC 20000-1:2010: "Incident - Unplanned interruption to a service, a reduction in the quality of a service or a failure of a configuration item that has not yet impacted a service"
  - Domanda: quale incidente "di servizio" non è un incidente di sicurezza?

# Requisiti comuni (1/5)

- Uso del ciclo PDCA
  - tutti e due gli standard fanno esplicito riferimento al ciclo di Deming
  - deve essere posta attenzione ai diversi tempi di completamento dei diversi cicli
- Ruoli e responsabilità
  - i ruoli e le responsabilità descritti dalle due norme non sono in conflitto tra loro
- Service Level Management
  - non discusso dalla ISO/IEC 27001, ma è evidente come una contrattazione tra le diverse aree aziendali possa portare benefici nell'implementazione di controlli e processi di sicurezza
- Service reporting
  - la ISO/IEC 20000-1:2005 prevede un processo di service reporting
  - la ISO/IEC 27001:2005 richiede di misurare l'efficacia dei controlli (fortunatamente, l'attuale 4WD è meno stringente)
  - il requisito della ISO20k può integrare efficacemente quello della 27k, dandogli migliore significato

# Requisiti comuni (2/5)

- Continuity & Availability Management
  - I due standard affontano l'argomento da due punti di vista diversi ma coerenti tra loro
  - La ISO/IEC 27001 tratta l'availability in modo generale e come diretta conseguenza dei requisiti di disponibilità delle informazioni, e tratta la continuity come subordinata al business continuity management
  - La ISO/IEC 20000-1 restringe apparentemente l'ottica ai soli servizi e dettaglia bene alcuni aspetti, tra cui i punti minimi che devono essere coperti dai piani di continuità
  - Ulteriori considerazioni su questi aspetti possono essere tratti dalla ISO/IEC 27002. E' comunque evidente come l'uso dei due standard possa condurre ad adottare valide best practices

# Requisiti comuni (3/5)

- Budgeting and accounting
  - la ISO/IEC 27001 si limita a parlare di “risorse”
  - è noto che ogni progetto o attività ha dei costi
  - l’impostazione del budgeting e della rendicontazione proposta dalla 20k può portare indubbi benefici nella valutazione dell’accettabilità dei rischi e nella pianificazione del trattamento del rischio
- Capacity Management
  - il processo di Capacity Management della ISO/IEC 20000-1 comprende diversi requisiti e controlli della ISO/IEC 27001
  - è facile immaginare come alcuni requisiti della ISO/IEC 20000-1 possano aiutare nell’implementazione dei (sintetici) requisiti e controlli della ISO/IEC 27001, dando loro una più ampia prospettiva
  - una visione del Capacity Management come processo (requisito 20k) può portare maggiori benefici di una sua visione come controllo (requisito 27k)
- Information Security Management
  - il processo descritto dalla ISO/IEC 20000-1 è coerente con i requisiti della ISO/IEC 27001, ma è descritto in modo più sintetico

# Requisiti comuni (4/5)

- Business relationship management
  - La ISO/IEC 27001 nomina diverse volte “contractual security obligations”
  - Tradizionalmente, chi si occupa di sicurezza (imprese, specialisti, consulenti e auditor) non approfondisce gli aspetti contrattuali, se non su specifiche richieste. Anche nella pubblicistica in ambito sicurezza il “cliente” è poco nominato
  - La ISO/IEC 20000-1 è molto più orientata alla soddisfazione dei clienti e propone processi per questo obiettivo, certamente condivisibile anche quando si parla di sicurezza
- Supplier management
  - Partendo da due punti di vista diversi, i requisiti delle due norme sono indubbiamente complementari e una loro gestione integrata può portare benefici a chi li volesse adottare
  - L’approccio per SLAs (nominati UC) della 20k può essere utilmente integrato con i requisiti più specifici della sicurezza.
- Clienti e management commitment
  - la ISO/IEC 20000-1 è orientata ai clienti; la ISO/IEC 27001 agli “stakeholders” (più generale)
  - l’approccio ISO20k impone di trattare la sicurezza dando importanza ai requisiti dei clienti in fase iniziale e durante i riesami periodici (fasi importanti ma trascurate nell’ambito dell’ISMS)

# Requisiti comuni (5/5)

- Incident e Problem management
  - I potenziali problemi sono già stati discussi
  - Questi aspetti sono trattati in modo “implicito” dalla 27k. L’approccio più strutturato, rigoroso, efficace e, se ben gestito, efficiente, proposto dalla 20k dovrebbe essere adottato per un ISMS in tutti i casi
- Configuration management
  - La 20k tratta compiutamente il processo di configuration management
  - La ISO/IEC 27001 richiede di “identificare gli asset” in fase di risk assessment e di “gestire gli asset” come controllo di sicurezza (A.7)
  - Appare ovvio come il requisito della ISO/IEC 20000-1 possa dare benefici alla sicurezza delle informazioni
- Change Management
  - Già trattato
- Release and deployment management
  - Ognuno di questi può dare elementi aggiuntivi ai requisiti della ISO/IEC 27001.

- Presentazione
- Le norme ISO/IEC 20000-1, ISO/IEC 27001 e ISO/IEC 27012
- Confronto tra le norme
- Alcune considerazioni

# Terminologia

- Le due norme, nella versione del 2005 presentano dei problemi:
  - nella 27001 “appaiono” le azioni correttive e preventive senza una definizione di “non conformità”, probabilmente per inserire i punti comuni ad altre norme ISO
  - nella 27001, i requisiti sulla misurazione dell’efficacia dei controlli, oltre ad essere discutibili, sono posti in modo erroneo rispetto alle fasi del ciclo PDCA
  - nella 20000-1 sono utilizzati termini non definiti o incoerenti con altre norme ISO (per esempio, i termini di verifica, riesame e validazione sono ignorati in favore di altri; in modo simile, il termine “plan” è utilizzato in modi non sempre tra loro omogenei)
  - nella 20k alcuni requisiti comuni ad altre norme sono stati trasformati e il risultato non sempre è apprezzabile (p.e. gestione delle registrazioni e dei documenti)
- La terminologia, troppo spesso, ignora altre esperienze; ad esempio:
  - la definizione di “sistema di gestione” nella 27k è incoerente con altre norme
  - la definizione di “documentazione” nella 20k è incoerente con altre norme
- Le nuove versioni superano questi punti

# Tabelle di correlzione

- Non è facile mappare i requisiti della ISO/IEC 20000-1 con quelli della ISO/IEC 27001
- Ciascuna delle due norme ha due punti di vista diversi e alcune intersezioni non sono ben interpretabili se non approfondendo le due materie
- Meglio provare a leggere i requisiti dell'una confrontandoli di volta in volta con quelli della seconda e viceversa. Esempi:
  - il capacity management della 20k non è confrontabile con il A.10.3.1 della 27k
  - i requisiti della 27k sulla conduzione e sullo sviluppo dei sistemi (A.10 e A.12) sono difficilmente inquadrabili nei requisiti della 20k
- Le due norme partono da due storie diverse e i requisiti vanno letti anche tenendo conto di quelle storie. Rischiano di perdersi:
  - l'attenzione ai clienti e inquadramento di alcuni processi della 20k
  - l'estensione di alcuni controlli e il significato del risk assessment della 27k
- In altre parole: "Tabelle di correlazione? No, grazie" (meglio usare la testa)

# Per partecipare - UNINFO

- Ente di normazione federato all'UNI per le norme delle serie 15408, 20000, 27000. Mantiene contatti con ISO, ISO/IEC JTC, CEN
- E' attivo un GDL dedicato alle norme della serie 27000, con quote di iscrizione ridotte
- I soci hanno accesso ai draft degli standard per sottoporre i propri commenti ai Working Group dell'ISO
- Chiunque voglia contribuire alla redazione degli standard è benvenuto.

UNINFO

# Grazie!


- Cesare Gallotti
  Web: http://www.cesaregallotti.it
  Blog: http://blog.cesaregallotti.it
  Mail: cesaregallotti@cesaregallotti.it