ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

ISO/IEC 20000: la Norma per la qualità dell'erogazione dei Servizi IT

Attilio Rampazzo, Antonio Piva, David D'Agostini

1. Introduzione

La gestione di un'organizzazione moderna è un'attività complessa: deve rispondere in maniera sistematica e documentata del rispetto di leggi, di norme settoriali e volontarie, di impegni contrattuali, di attese della proprietà, dei clienti e della comunità e lo deve fare operando in un contesto sempre più dinamico; deve gestire e far coesistere interessi economici con requisiti relativi alla sicurezza delle persone e dei prodotti, alla qualità e rispetto di tutte le parti interessate.

Tra le varie incombenze la gestione e l'erogazione dei servizi IT (conosciuta come *IT Service Management*) si dimostra sempre più come una necessità per tutte le organizzazioni, pubbliche e private, sia che si tratti di servizi destinati all'interno dell'organizzazione, sia che i servizi vengano rivolti al cliente/utente.

Tra le varie proposte introdotte da IBM, HP, Microsoft e altre organizzazioni del mondo IT, il modello *IT Infrastructure Library* (ITIL) ha dimostrato la sua validità ed efficacia rappresentando un framework e un approccio internazionalmente condivisi per una corretta gestione ed erogazione dei servizi IT. Partendo da questo modello è nata una Norma Internazionale, l'ISO/IEC 20000, che costituisce un valido strumento per l'ottimizzazione degli aspetti di gestione dei servizi per l'IT e per la progettazione dei processi di business correlati[1].

ITIL è un insieme di consigli partici (*best practice*), mentre la ISO/IEC 20000 è un insieme formale di specifiche di cui un fornitore del servizio deve tendere per essere in grado di fornire un'elevata qualità dei servizi[2] (nella Figura 1 sono illustrate le relazioni fra la ISO/IEC 20000 e ITIL).

Prima d'ora, chi erogava servizi IT per manifestare la sua capacità si certificava ISO 9001 settore EA 33 (Servizi IT), mentre adesso ha una nuova e valida possibilità di dimostrare il controllo efficace e il miglioramento continuo dell'intero complesso di prestazioni dell'IT Service Management grazie alla Norma ISO/IEC 20000, che prevede l'implementazione di un **Sistema di Gestione dei Servizi IT** (SGSIT). Infatti l'ISO/IEC 20000 è una norma dedicata alla valutazione delle organizzazioni che erogano servizi IT che riconosce l'importanza dei servizi IT, ne individua le specificità e stabilisce l'esigenza di una risposta adeguata ai problemi che le tecnologie dell'informazione comportano nella impostazione e nell'esercizio di un Sistema di gestione del servizio.

La Norma ISO/IEC 20000, applicabile a organiz-

[1] In merito alle normativa ISO/IEC si ricorda che questa rubrica ha già preso in esame la famiglia ISO 27000 nell'articolo pubblicato su Mondo Digitale di settembre 2008.

[2] L'applicazione dei "consigli pratici" ITIL potrà supportare un fornitore del servizio nel raggiungere la qualità del servizio così come richiesto dalla ISO/IEC 20000.

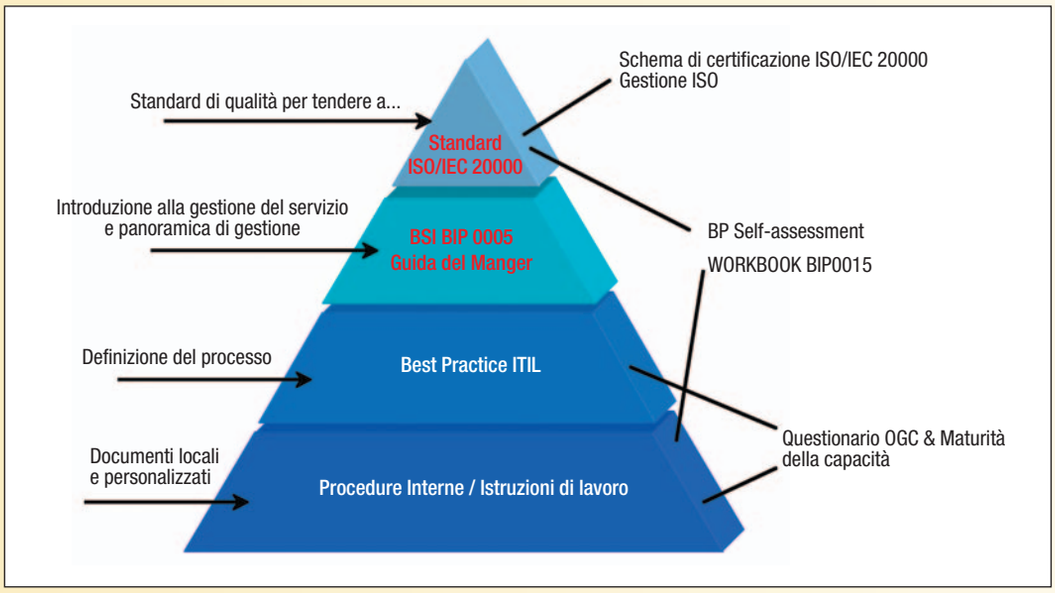

FIGURA 1
Relazioni fra la ISO/IEC 20000 e ITIL

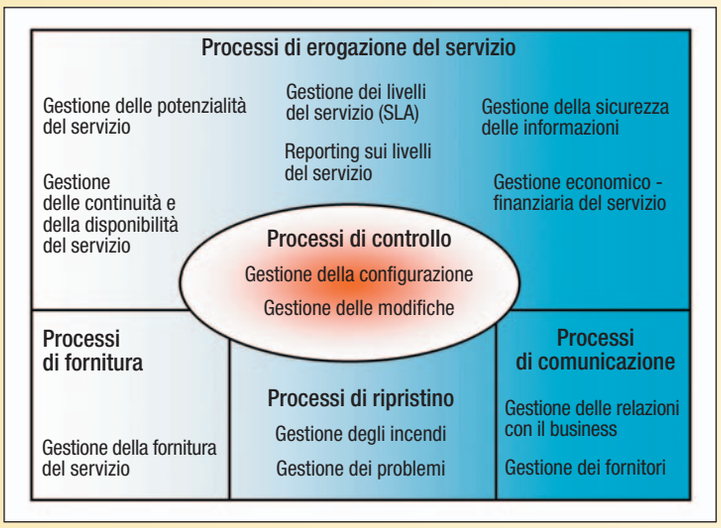

FIGURA 2
Processi del Service Management

zazioni di tutte le dimensioni, si compone di due parti:

- parte 1 *Specification*: ovvero la ISO/IEC 20000-1:2005. Contiene le specifiche (o requisiti) per l'implementazione di un Sistema di Gestione per l'Erogazione dei Servizi IT;
- parte 2 *Code of practice*: ovvero la ISO/IEC 20000-2:2005. Contiene linee guida, raccomandazioni utili per la corretta implementazione di quanto specificato nella parte 1.

L'ISO/IEC 20000 si configura, quindi, come una nuova famiglia di Norme.

La prima parte della Norma (ISO/IEC 20000-1) si pone l'obiettivo di promuovere un approccio integrato alla gestione di un'organizzazione erogatrice di servizi IT[3] con l'idea che una buona qualità del processo di erogazione implichi una buona qualità del servizio erogato. La capacità dell'organizzazione consiste nel saper coniugare in modo equilibrato efficienza ed efficacia, profitto economico, vantaggi per il cliente e miglioramento continuo.

La ISO/IEC 20000-1 impone una lista di obiettivi e controlli[4] ed evidenzia i processi strettamente collegati alla gestione del servizio, in sinergia a ITIL (la Figura 2 rappresenta lo schema dei processi). Esprime i requisiti dei processi di erogazione attraverso precise prescrizioni elementari[5].

La seconda parte della Norma (ISO/IEC 20000-2) si pone l'obiettivo di affiancare la prima parte della Norma fornendo linee guida e raccomanda-

[3] L'organizzazione erogatrice è un insieme complesso di processi, di relazioni, di flussi, di competenze, di risorse, di tecnologie. L'approccio integrato proposto dalla norma consente l'impostazione del controllo sui flussi ciclici di erogazione del servizio e delle opportunità di miglioramento continuo.

[4] Possono risultare non esaustivi: ogni organizzazione, in base alle proprie necessità, può considerare obiettivi e controlli che si aggiungono a quelli previsti dalla norma.

[5] *Shall*: i requisiti espressi devono applicarsi al sistema di erogazione del servizio IT quando l'organizzazione erogatrice si ponga l'obiettivo di realizzare un servizio gestito con una predefinita (e accettabile) qualità per i propri clienti.

zioni, descrizione di buone pratiche e consigli pratici connessi alle possibili applicazioni dei requisiti espressi nella prima parte. La norma individua le aree critiche della progettazione e dell'erogazione dei servizi IT e richiede che persone, processi e tecnologie (ICT) interagiscano e si mantengano costantemente coordinati sui fini stabiliti per l'organizzazione. Tra i fattori che determinano il successo di un'organizzazione erogatrice di servizi IT si riconosce la preponderanza del fattore umano, ovvero le persone che governano i processi di erogazione dei servizi[6].

L'uso congiunto di seconda e prima parte della norma mette l'organizzazione erogatrice in condizione di progettare e realizzare il miglioramento della qualità del servizio erogato in modo strutturato e proattivo anziché sporadico e reattivo[7].

Al di là del regolare uso combinato, si potrebbe anche affermare che l'ambito di applicazione della seconda parte della norma sia progettazione ed amministrazione del sistema di gestione piuttosto che la valutazione di conformità (di prima, seconda e terza parte[8]) trattata e resa praticabile dalla prima parte della norma.

La Norma ISO/IEC 20000, come già accennato, è sostanzialmente allineata con l'*Information Technology Infrastructure Library* (ITIL), nonostante non ne includa formalmente l'approccio. Il contenuto della norma è comunque tale da poter supportare altri frameworks e approcci simili (per esempio *MOF Microsoft Operational Framework* (Microsoft), *HP ITSM Reference Model* (Hewlett Packard), IT Process Model (IBM) ecc.).

2. Origine ed evoluzione della famiglia di Norme ISO/IEC 20000

Le origini di ISO/IEC 20000:2005 sono abbastanza recenti e affondano le proprie radici negli anni '80 quando nasce il progetto *Information Technology Infrastructure Library* (ITIL) per iniziativa del Governo Britannico.

ITIL v.1 (1989 – inizialmente "*Guide for Government*") è stato sviluppato sotto gli auspici del CCTA *Central Computer and Telecommunications Agency* (CCTA) oggi conglobata nell'*Office of Government Commerce* (OGC) in risposta alla crescente difficoltà di azione delle agenzie governative britanniche nella gestione dell'innovazione della tecnologia dell'informazione. I lavori del gruppo ITIL, inizialmente orientati sulla costruzione di un metodo formale, è decisamente cambiata in corso d'opera concentrando l'attenzione verso le "best practices". In tal modo i consigli e linee guida di ITIL sono stati implementati in diverse organizzazioni ed utilizzati nei settori più disparati (amministrazioni pubbliche locali e centrali, industrie e imprese di servizi). Sebbene sviluppato durante gli anni 80, ITIL ha raggiunto grande popolarità solo dopo la metà degli anni 90.

Il *British Standards Institute* (BSI) organizzazione britannica fondata nel 1901 e operante oggi nello sviluppo di norme nazionali e internazionali, nella certificazione di terza parte indipendente di prodotti e sistemi di gestione e nella formazione manageriale - ha pubblicato "*A Code of Practice for IT Service Management* - DISC PD0005:1998". La norma documenta l'approccio alla gestione del servizio IT basato sui principi stabiliti da ITIL e sulle esperienze consolidate nell'industria. Nella norma si può trovare una prima definizione dei processi chiave della gestione dei servizi: *service design & management, control, release, resolution, supplier*.

Nel 2001 OGC ha rilasciato ITIL v.2 concentrando il focus sull'approccio per processi; *Service Support* & *Service Delivery* costituiscono la macro area fondamentale per la gestione e l'erogazione dei servizi IT e sono il cuore della seconda versione la cui struttura si completa con altre sei aree:

- *ICT Infrastructure Management*;
- *Planning To Implement Service Management*;
- *Applications Management*;
- *The Business Perspective*;

[6] L'applicazione delle prescrizioni della norma alla gestione del servizio ed alla evoluzione del sistema di gestione è affidata all'attenzione di persone competenti.

[7] Naturalmente l'adozione della norma nella progettazione organizzativa richiede all'Alta Direzione le capacità interpretative che consentono la costruzione di un sistema di gestione in funzione delle specifiche caratteristiche dell'organizzazione erogatrice (dimensioni, struttura, competenze, personale, strategia ecc.).

[8] Di prima parte mediante Audit interni dell'organizzazione; di seconda parte mediante verifiche effettuate dall'organizzazione nei confronti dei fornitori; di terza parte indipendente per esempio nel processo di certificazione.

- *Software Asset Management*;
- *Security Management*.

Nel Novembre 2000 BSI ha pubblicato la prima norma che stabilisce i requisiti del sistema di gestione dei servizi IT: la BS15000:2000 è stata sviluppata sulla base della precedente pubblicazione DISC PD005:1998. La seconda edizione è uscita nel 2002: l'aggiornamento è stato fatto raccogliendo l'esperienza degli utilizzatori della prima edizione. La struttura della seconda edizione anticipa la 20000 con una prima parte che definisce i requisiti (BS15000-1 IT service management Part 1: *Specification for service management*) e una seconda parte che fornisce raccomandazioni (BS15000-2 IT service management Part 2: *Code of practice for service management*).

Nel 2004 l'*International Organization for Standardization* (ISO) - organismo internazionale per la definizione delle norme a livello mondiale - e l'*International Electrotecnical Commission* (IEC) - Commissione Elettrotecnica Internazionale - attraverso il comitato tecnico congiunto JTC1/SC7, responsabile dello sviluppo delle norme nell'area dell'ingegneria del software e dei sistemi, hanno accolto la norma nazionale BS15000 e l'hanno promossa il 15 dicembre 2005 a Norma Internazionale ISO/IEC 20000:2005[9].

Questa breve cronologia mostra come la nascita e l'evoluzione della Norma ISO/IEC 20000:2005 si intreccino con l'evoluzione di ITIL. Norma e ITIL si sviluppano in maniera complementare e non costituiscono alternativa[10]. La norma formalizza in termini di requisiti del sistema di gestione gli elementi chiave descritti nelle "Buone Pratiche" raccolte in ITIL. Le organizzazioni che adottano lo schema ITIL pubblicizzano tale scelta per distinguersi nello scenario competitivo di interesse. Da qui nasce l'esigenza di poter verificare in modo obiettivo e imparziale un'affermazione di conformità di un'organizzazione allo schema dichiarato: in altre parole nasce l'esigenza di una norma che possa funzionare da metro per la verifica in analogia a quanto avviene con la Norma ISO 9001. Nella tabella 1 possiamo trovare una sintesi dei principali eventi che hanno caratterizzato l'evoluzione della normativa su IT Service Management.

TABELLA 1
Sintesi dei principali eventi che hanno caratterizzato l'evoluzione della normativa su IT Service Management

Anno pubblicazione	Norma/Proposta pubblicata
1998	BS DISC PD0005:1998 – "A Code of Practice for IT Service Management"
2000	BS 15000:2000 – "Specification for IT Service Management"
2002	BS 15000-1:2002 – "IT service management. Specification for Service Management"
2003	BS 15000-2:2003 – "IT service management. Code of practice for Service Management"
2005	ISO/IEC 20000-1, Information technology — Service Management — Part 1: Specification – Stabilisce i requisiti del sistema di gestione
2005	ISO/IEC 20000-2, Information technology — Service Management — Part 2: Code of Practice – Raccomanda buone pratiche per la gestione
2008	ISO/IEC CD TR 20000-3 - Information technology — Service Management — Part 3: Guidance on compliance with ISO/IEC 20000-1
2008	ISO/IEC CD TR 20000-4 - Information Technology – Service Management — Process Reference Model

[9] Secondo la procedura "*fast track*" (percorso abbreviato – tre passi invece dei sei canonici, che mediamente consente in poco meno di un anno di lavoro la pubblicazione di una norma internazionale a partire da un consolidata norma nazionale).

[10] Il primo giugno 2007 OGC ha pubblicato la nuova versione ITIL v3 concentrando il focus sull'intero ciclo di vita del servizio e sull'allineamento tra la gestione del servizio e la gestione dell'impresa. I nuovi volumi coprono i seguenti temi: *Strategy, Design, Transition, Operation, Continual Improvement*.

3. Contenuti della Norma ISO/IEC 20000-1:2005

La Norma ISO/IEC 20000-1 è composta da 10 capitoli in cui sono specificati i requisiti che possono essere classificati in tre macro categorie:

- i requisiti di carattere generale dell'organizzazione – capitoli 3, 4, 5;
- i requisiti dei processi primari di erogazione – capitoli 6, 7;
- i requisiti dei processi di supporto – capitoli 8, 9, 10.

La parte iniziale della norma fino al capitolo 2 ha un carattere introduttivo come in tutte le norme. Di particolare interesse sono le ultime tre definizioni tratte dal glossario, parte integrante della norma, in quanto anticipatrici del principio della norma ovvero il concetto di livello di servizio:

❑ **SLA - Service Level Agreement** - Accordo sui livelli di servizio: accordo documentato fra il fornitore di servizi e il cliente che descrive il servizio e ne definisce i livelli concordati.

❑ **Service Management** - Gestione del servizio: le attività di organizzazione/pianificazione/controllo che mirano a soddisfare le esigenze di business (fornire valore ai clienti) attraverso un servizio.

❑ **Service Provider** - Erogatore del servizio (Fornitore): organizzazione che fornisce servizi a uno o più clienti (interni o esterni).

I caratteri generali della norma prendono corpo nei capitoli 3, 4 e 5.

Nel *capitolo 3* sono riportati i requisiti generali per implementare un Sistema di Gestione che permetta la progettazione-erogazione di tutti i servizi IT.

La realizzazione del sistema di gestione si basa su tre fattori chiave:

- responsabilità dell'Alta Direzione;
- documentazione;
- competenza, consapevolezza e formazione del personale.

Nel *capitolo 4* sono riportati i requisiti per la pianificazione e l'implementazione della gestione del servizio e si adotta la metodologia "*Plan-Do-Check-Act*" (PDCA – ciclo di DEMING) per tutti i processi organizzativi e gestionali (Figura 3).

Il processo direzionale viene messo in relazione con il ciclo evolutivo del sistema di gestione:

- pianificazione della gestione del servizio (*Plan*);
- implementazione della gestione ed erogazione dei servizi (*Do*);
- monitoraggio, misurazioni e revisioni (*Check*);
- miglioramento continuo (*Act*).

Nel *capitolo 5* sono riportati i requisiti per la pianificazione e l'implementazione dell'innovazione (servizi nuovi o cambiamenti a servizi attivi); la gestione corrente del servizio, impostata secondo il metodo PDCA, consente un primo livello di governo orientato al miglioramento continuo.

L'Organizzazione deve mantenere attivo un sistema per il monitoraggio delle situazioni di crisi (opportunità e minacce) cui rispondere

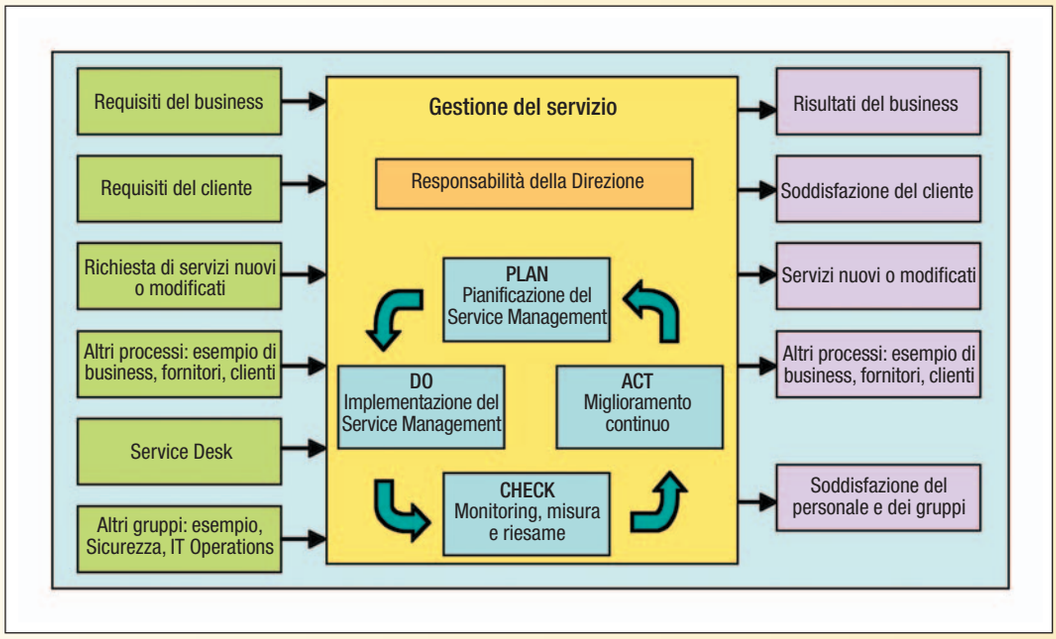

FIGURA 3
Ciclo PDCA del Sistema di Gestione dei Servizi IT

con un approccio all'innovazione radicale e settoriale[11].
In questo contesto si intende per innovazione quel cambiamento del servizio e del sistema di gestione del servizio finalizzato alla massimizzazione dei benefici attesi per una data configurazione di risorse (finanziarie e di conoscenza). Così come per il miglioramento anche per l'innovazione l'iniziativa deve essere gestita come un programma-progetto i cui elementi devono costantemente essere allineati alla strategia e obiettivi dell'Organizzazione.
Nei successivi capitoli vengono esposte le specificità di un Sistema di Gestione dei Servizi IT.
Nel *capitolo 6* sono riportati i requisiti per l'erogazione del servizio, vengono trattati tutti quei processi che negoziano, definiscono e concordano gli effettivi livelli di servizio e che riportano le prestazioni raggiunte rispetto a tali obiettivi. Rientrano a far parte dell'ambito di erogazione del servizio i seguenti processi:
- *Service Level Management*;
- *Service Reporting*;
- *Capacity Management*;
- *Service Continuity and Availability Management;*
- *Information Security Management*;
- *Budgeting and Accounting for IT services*.

Nel *capitolo 7* sono riportati i requisiti relativi alla gestione dei subfornitori e alla gestione delle relazioni di business. Rientrano a far parte dell'ambito di gestione delle relazioni del servizio i seguenti processi:
- *Business Relationship Management*;
- *Supplier Management*.

Sia il subfornitore che il cliente possono essere sia interni che esterni all'organizzazione del fornitore del servizio, ma mentre le relazioni esterne vanno formalizzate anche attraverso contratti di subfornitura, per le relazioni interne bastano accordi sui livelli operativi o di servizio. Al fine di stabilire e mantenere buone relazioni dovrebbero essere definite le figure di interfaccia per tutte le parti, che dovrebbero definire e concordare i bisogni di business, l'ambito, i ruoli e le responsabilità delle relazioni e i canali e la frequenza di comunicazione.
Nel *capitolo 8* sono riportati i requisiti relativi alla risoluzione attraverso i processi di risoluzione, incident e problem management, processi separati, benché strettamente collegati.
Rientrano a far parte dell'ambito di risoluzione del servizio i seguenti processi:
- *Incident Management*;
- *Problem Management*.

Nel *capitolo 9* sono riportati i requisiti che permettono al fornitore del servizio di controllare i componenti del servizio dell'infrastruttura e di mantenere informazioni accurate sulla configurazione. Questa accuratezza delle informazioni è un requisito fondamentale per il processo decisionale interno al processo di *change management* così come per tutti gli altri processi dell'organizzazione di servizio IT. Nell'alveo del controllo del servizio vi sono i processi:
- *Configuration Management*;
- *Change Management*.

Nel *capitolo 10* sono riportati i requisiti per il rilascio dei cambiamenti pianificati. Alla messa in produzione del servizio appartiene il processo:
- *Release Management*.

La norma evidenzia l'importanza che il processo di *release management* sia integrato con i processi di *configuration* e *change management*, al fine di assicurare la sintonia e l'accordo dei rilasci e dei cambiamenti eseguiti.

4. Futuro ed evoluzione

La versione attuale della norma internazionale riflette la struttura della BS15000:2002 (originaria norma britannica) la quale era già in fase di sperimentazione nel contesto anglosassone. Si può ritenere, pertanto, che il livello di penetrazione della certificazione sia in una fase evolutiva e ciò è testimoniato anche dal numero di certificazioni a livello mondiale (Tabella 2). Le prospettive della norma sono, poi, delineate all'interno dei progetti del Comitato Tecnico congiunto ISO &IEC JTC1/SC7: riguardano una revisione per adeguamento a ITIL v.3 e la redazione della terza e della quarta parte della Norma ISO 20000.
La parte 3 (*Guidance on Compliance with ISO/IEC 20000-1*) fornirà linee guida addizionali per la definizione dei contenuti (campi di applicazione) della gestione dei servizi IT con il duplice scopo di sostenere l'approccio sia alla pianificazione dei sistemi, sia alla verifica di conformità da parte degli auditors (di prima, seconda e terza parte). La ISO/IEC 20000-3

[11] In quanto l'approccio graduale del miglioramento continuo potrebbe non essere sufficiente: la risposta ad una aggressività tecnologica potrebbe arrivare in ritardo.

sarà indirizzata alle organizzazioni erogatrici di servizi e prenderà la forma di una raccolta di spiegazioni, raccomandazioni ed esempi sulla definizione del campo di applicazione della gestione. Si prevede l'uso congiunto delle parti terza e prima, senza escludere l'utilità di un affiancamento con la seconda.
La parte 4 (*Process Reference Model for Service Management*) fornirà un modello di processo utilizzabile come riferimento per la valutazione del livello di capacità dei processi di gestione dei servizi implementati da un'organizzazione erogatrice che ha adottato la ISO/IEC 20000-1. ISO/IEC 20000-4 sarà fedele alla impostazione data alla nuova Norma ISO/IEC 12207 (pubblicata nel marzo 2008) e consentirà sia di stabilire l'organizzazione dei processi del ciclo di vita dei servizi IT, sia di classificare la capacità del processo di gestione dei servizi IT sulla scala dei livelli di maturità.

5. Collegamenti con altre Norme

La Norma ISO/IEC 20000-1, attraverso le evoluzioni seguite alla pubblicazione nel 2002 della prima release del predecessore BS 15000, ha visto una migliore armonizzazione dei processi, inglobando anche il noto paradigma *Plan-Do-Check-Act* (PDCA) e, quindi, risulta allineata alle altre norme che adottano un Sistema di Gestione (vedi ISO 9001, ISO 14001, ISO 27001).
Molte organizzazioni IT[12] sono certificate secondo la ISO 9001 nel settore EA 33, quindi la ISO/IEC 20000-1 potrebbe sostituire o meglio integrare molte di queste certificazioni.
Uno dei processi del *Service Delivery* della ISO/IEC 20000-1 è l'*Information Security Management*. La ISO/IEC 27002:2005[13] fornisce delle indicazioni o *best practice* sulla Gestione della Sicurezza delle Informazioni atte a implementare questo processo. Le organizzazioni già certificate ISO/IEC 27001:2005 possono soddisfare i requisiti di sicurezza propri della ISO/IEC 20000-1, sempre che gli scopi di certificazione coincidano o comunque siano nel perimetro di certificazione.
Ulteriore processo del *Service Delivey* della

[12] Al giorno d'oggi se ne contano circa 2800 (Fonte: sito SINCERT al 31dicembre 2008).

[13] Rinumerazione della ISO/IEC 17799:2005.

Nazione	Nr. Aziende Certificate
UK United Kingdom	52
Japan	50
India	42
China	35
South Korea	35
Germany	20
Taiwan	14
Switzerland	12
USA	18
Hong Kong	7
Austria	8
Czech Republic	8
France	4
Poland	4
Australia	3
Denmark	3
Netherlands	3
Spain	3
Thailand	3
Brazil	2
Ireland	2
Malaysia	2
Philippines	2
Saudi Arabia	2
Singapore	2
Slovakia	2
Turkey	2
United Arab Emirates	2
Botswana	1
Colombia	1
Finland	1
Kuwait	1
Italy	1
Latvia	1
Liechtenstein	1
Qatar	1
Russia	1
Sri Lanka	1
Totale	**352**

TABELLA 2
Aziende certificate ISO 20000-1 suddivise per Nazione (Fonte: www.isoiec20000-certification.com al 10/marzo/2009)

ISO/IEC 20000-1 è il *Service Continuity Management*. La BS 25999-1:2006 del British Standard fornisce delle indicazioni o *best practice* sulla Gestione della *Business Continuity*, nota come BCM. A dicembre 2007 è stata pubblicata la BS 25999-2:2007 che permette alle organizzazioni di certificare il Sistema di Gestione della *Business Continuity* aziendale soddisfacendo così anche i requisiti propri della ISO/IEC 20000-1 in questo particolare argomento[14].
La normativa ISO/IEC esaminata, in tutta evidenza, presenta tratti di forte connessione con la disciplina legislativa in materia di trattamento dei dati personali e della sicurezza informatica di cui al d.lgs. 196/03 (cosiddetto Codice della privacy) e relativo Allegato B.
Tali disposizioni (già trattate approfonditamente in questa rivista nel numero di giugno 2007) hanno naturalmente forza imperativa di legge, a differenza della ISO/IEC a cui si può liberamente scegliere di sottostare; tuttavia, considerato che quest'ultima contiene previsioni a tratti più rigorose di quelle dettate dal legislatore, appare evidente che l'ottenimento della certificazione implica l'ottemperanza (ovvero favorisce il rispetto) di determinate norme del Codice della privacy o, quantomeno, una rivisitazione dei relativi adempimenti in ambito aziendale (si pensi alle misure minime di sicurezza in riferimento ad accessi abusivi o a danneggiamenti informatici).

6. Conclusioni

Nel business di oggi giorno è evidente la necessità di dimostrare la capacità di fornire servizi che soddisfino i requisiti dei clienti sia interni che esterni all'organizzazione: ciò può essere ottenuto attraverso la standardizzazione dei processi di gestione del servizio. L'approccio è teso a enfatizzare i benefici per l'utente finale e rappresenta un risultato condiviso relativamente agli standard di qualità per i processi di gestione dei servizi IT.
La ISO/IEC/IEC 20000-1 rappresenta un grandissimo balzo in avanti, che supera i precedenti tentativi di gestione dei servizi IT come attività individuali separate e distinte. Il nuovo approccio si concentra invece sulla fornitura di servizi *end-to-end* mediante l'applicazione dei modelli e *best practice* o consigli pratici per l'implementazione e gestione dei processi.

Bibliografia

[1] ISO/IEC 20000-1:2005 *Information technology – Service management* – Part 1: *Specification*.

[2] ISO/IEC 20000-2:2005 *Information technology – Service management* – Part 2: *Code of practice*.

[3] ISO/IEC 20000 *Pocket Guide* – ITSMF ITALIA - Van Haren Publishing.

[14] Sempreché gli scopi di certificazione coincidano.

Attilio Rampazzo, consulente di Sistemi Informativi e Sicurezza delle Informazioni in AlmavivA Finance Spa. Ha maturato un'esperienza più che trentennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. È Vice Presidente del Comitato AICQ "Qualità del Software e dei Servizi IT", valutatore Sistemi di Sicurezza delle Informazioni R.G.V.I. (AICQ_SICEV certificato n.3), socio AIPSI-Associazione Italiana Professionisti Sicurezza Informatica.
E-mail: attilio@rampazzo.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

David D'Agostini avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it