HSPI

Rubrica ISO-IEC 20000

Parlano gli esperti

Fabrizio Cirilli
Marcus Giese
Sadao Fukatsu
Paul Barrett

HSPI

INDICE

INTRODUZIONE

Sotto la spinta del governo britannico sono stati sviluppate diverse best practice e standard, tra gli altri ITIL e BS 15000.
La best practice ITIL (Information Technology Infrastructure Library), la raccolta strutturata ed organica delle linee guida per la definizione, la realizzazione, il passaggio in produzione e l'erogazione dei Servizi IT, giunta alla sua terza versione, è diffusa a livello internazionale, in organizzazioni di medie e grandi dimensioni appartenenti ad ogni settore produttivo.
A fianco della best practice ITIL l'iniziativa di politica industriale del ministero del commericio e dell'industria inglese ha ritenuto opportuno far nascere e diffondere uno standard, il British Standard 15000 - IT Service Management, ed uno schema per la certificazione delle aziende inglesi. Tale standard verifica la corretta implementazione di un Sistema per la Gestione dei Servizi IT (IT Service Management System - ITSMS), analizzando:

- Il coinvolgimento del management (impegno di gestione);
- l'implementazione di processi trasversali all'organizzazione, con l'individuazione di ruoli e responsabilità per ogni processo e delle interrelazioni tra i processi;
- l'impostazione e misurazione degli obiettivi di gestione di servizio e degli indicatori di prestazioni chiave (KPI) di ogni processo.

Nel 2005 lo standard BS 15000 viene recepito dagli organismi internazionali di standardizzazione ISO, che emanano la norma ISO/IEC 20000 e supportano l'affermazione a livello internazionale dell'IT Service Management.
Recentemente, si sta assistendo alla diffusione della norma ISO/IEC 20000 anche in Italia, con la certificazione di quasi una ventina di organizzazioni.
Non sempre, tuttavia, l'acquisizione della certificazione si traduce in un reale miglioramento della qualità dei servizi offerti, al di là dei costosi formalismi adottati; il rischio è quello di focalizzarsi sul raggiungimento della certificazione, confondendo il mezzo con il fine e non creando valore.
Perché le organizzazioni si sottopongono ad un processo di certificazione? Qual è l'effettiva utilità della certificazione e come vengono impostati i progetti di miglioramento? Quali sono gli effettivi risultati ottenibili col raggiungimento delle certificazione? Quali le difficoltà che si incontrano?
Quanto le organizzazioni che aspirano alla certificazione si mettono realmente in discussione?
Cerchiamo di capirlo intervistando alcuni lead auditor ISO/IEC 20000 dei principali organismi certificatori operanti a livello internazionale (TÜV, DNV e BSI), analizzando come vengono affrontate le certificazioni in Germania, Giappone e Regno Unito, indagando insieme le ragioni per cui le organizzazioni decidono di intraprendere il percorso di certificazione ISO 20000, il loro atteggiamento nei confronti dell'adozione dello standard e le principali debolezze e non conformità rispetto ai requisiti riscontrate nel corso degli audit.
In questo numero la rubrica presenta il punto di vista di Marcus Giese, Product Manager e Lead Auditor ISO/IEC 20000 e ISO/IEC 27001 di TÜV SÜD, di Sadao Fukatzu, Lead Auditor ISO/IEC 20000 di DNV e di Paul Barrett, Strategic Accounts Team Leader di BSI UK.
Prima della presentazione delle interviste, riportiamo a chiarimento della nomenclatura utilizzata una breve premessa di Fabrizio Cirilli, Lead Auditor di TÜV Italia, che ci introdurrà alla norma e al ruolo dei diversi soggetti coinvolti nel percorso di certificazione.

Premessa a cura di Fabrizio Cirilli

L'attività di certificazione è svolta da un Organismo di Certificazione (OdC) indipendente, che verifica l'efficacia e la conformità di un Sistema di Gestione rispetto ad una norma di riferimento (o schema di certificazione).
Nel caso dei Sistemi di Gestione per i Servizi (SGS) la norma di riferimento (o schema di certificazione) è la ISO/IEC 20000-1.
Una volta terminata la certificazione l'OdC rilascia un certificato, cioè l'attestazione che il SGS verificato, rispetta, con ragionevole certezza (si tratta di audit su base campionaria), i requisiti descritti nella ISO/IEC 20000-1.
Il processo di certificazione dura generalmente tre anni e prevede, oltre alla verifica iniziale, almeno altre due verifiche di sorveglianza la cui funzionalità è quella di attestare che il SGS continui a mantenere le caratteristiche di efficacia e conformità necessarie a garanzia della validità del certificato. Al termine del triennio sarà prevista un'ulteriore verifica di rinnovo che riattiverà il ciclo triennale.
Le certificazioni, rilasciate dagli OdC, possono essere accreditate. Ciò significa che gli stessi OdC si sottopongono annualmente ad una verifica da parte di un Organismo di Accreditamento, generalmente nazionale, il quale attesta che l'OdC opera secondo determinati standard (nel caso della certificazione dei SGS si tratta della ISO/IEC 17021) e regolamenti nazionali. In Italia questo ruolo è svolto da Accredia.
Un altro aspetto fondamentale dell'accreditamento è garantire tutti i processi di aggiornamento normativo a tutela delle organizzazioni certificate perché ricevano servizi adeguati in condizioni di trasparenza e di etica.
Ad esempio, in questo momento sono in fase di aggiornamento: le norme per la certificazione delle aziende (ISO/IEC 17021:11), quelle per la qualificazione degli auditor (ISO 19011:11) e quelle per la certificazione dei SGS (ISO/IEC 20000-1:11).

Ad oggi, sul territorio nazionale, opera un solo OdC accreditato da Accredia per la certificazione dei SGS (TUV Italia con 20 certificati).
Un OdC può operare in Italia anche per effetto del Multi Lateral Agreement (o MLA), sotto egida dell'European Accreditation, e/o del Multilateral Recognition Arrangement (o MRA) sotto l'egida dell'International Accreditation Forum.
In questi casi, la ricerca delle aziende certificate diventa molto più articolata, dovendo necessariamente reperire le informazioni sui siti dei membri aderenti agli accordi (ad esempio, UKAS per il territorio britannico), tramite cui identificare gli OdC accreditati, per poi visitare i siti di questi ultimi e visionare i data base delle aziende certificate per la ISO/IEC 20000-1.
Esiste un'ulteriore categoria di certificazioni: sono quelle rilasciate da organizzazioni autonome, non aderenti a nessuno degli schemi di accreditamento sopra citati, è il caso di APM Group-itSMF, la cui ricerca sul sito riporta 14 certificazioni in Italia distribuite tra DNV (4), RINA (8), IMQ (1) , SQS (1).
Le certificazioni con accreditamento internazionale e/o proprietario pongono qualche problema nella comprensione della loro validità e, soprattutto, riconoscibilità al di fuori dei confini nazionali poiché sfuggono ai controlli incrociati previsti dagli accreditamenti. Ciò non significa però che i SGS e le certificazioni che ne derivano siano di dubbia validità, poiché si tratta di un puro e semplice problema di tracciabilità delle competenze degli auditor impegnati e delle procedure di gestione della certificazione stessa.
Le interviste realizzate da HSPI, ponendo per la prima volta la questione su un piano internazionale, potranno agevolare la comprensione e la conoscenza degli aspetti tecnici della certificazione dei SGS secondo la ISO/IEC 20000-1,al momento tanto complessi ed eterogenei.

2 marzo 2012

Intervista a Marcus Giese

Marcus Giese lavora come Product Manager e lead auditor all'interno del TÜV SÜD per gli standard IT ISO 20000 e ISO 27000, secondo lo schema di certificazione del TGA, uno dei principali organi di certificazione nazionale.
Ha iniziato a svolgere l'attività di audit in Germania nel 2006, dopo la formazione condotta presso l'itSMF, in Inghilterra , dove ha ottenuto le certificazioni da Lead Auditor.

Quante sono le organizzazioni certificate in Germania?

Per il TÜV SÜD, le organizzazioni certificate risultano 14.
Vi è un altro grande organismo competitor nel mercato tedesco, il DQS, che rimane ancora affiliato all'AMPG. Il TÜV e il DQA sono i due protagonisti del mercato tedesco e hanno il 90% delle quote di mercato in Germania: ci sarebbero altri 3 o 5 certificati non seguiti dal DQS né dal TÜV: Per quanto riguarda la Fujitsu, conta già di per sé 6 o 7 certificazioni in Germania, poiché molte organizzazioni appartengono a questo gruppo.
In linea generale, suppongo vi siano 35-40 organizzazioni certificate, solo in Germania.

Quali sono i settori maggiormente interessati all'ISO 20000?

Dei nostri 18 clienti all'interno dell'Europa abbiamo:

- 13 server provider interni (reparto IT di organizzazioni il cui core business non è l'ICT management, che vanno dai 30 impiegati all'interno del reparto IT fino a, forse, 500 o 600 impiegati, complessivamente compagnie dai 3000 ai 14000 dipendenti, quindi da medie a grandi) incluse:
- 4 organizzazioni che si occupano di banking;
- 3 compagnie di fornitura elettrica.
- 5 service provider esterni (outsourcers).

Non vi sono, di conseguenza, dei settori predominanti, ma tra i servizi e il manifatturiero è sicuramente l'ambito dei servizi a prevalere.

Qual è il numero di lead auditors per la ISO 20000 in Germania (non solo appartenenti al TÜV SUD)?

Il TÜV SÜD ha in Germania più di 3 lead auditors e ulteriori 3 sono in arrivo. Complessivamente direi che in Germania abbiamo più o meno 10 lead auditors che conducono audits (provenienti dal TÜV e dal DQS), ma non dedicati unicamente alla certificazione ISO 20000.

Per quanto riguarda le certificazioni rilasciate in Germania, quali appartengono al Sistema di Accreditamento APMG, quanti al TGA?all'ISO 20000?

In prima istanza, a proposito del BS 15000, vi era la richiesta di creare uno schema di certificazione per il BS 15000, quindi l'itSMF U.K. si rivolse allo UKAS, l'ente nazionale di certificazione del Regno Unito, per prendere lo schema di accreditamento dallo UKAS; lo UKAS non era molto interessato perché aveva precedentemente creato lo schema ISO 27000, che non aveva riscosso il successo sperato, per cui lo UKAS decise di non procedere nemmeno con il BS 15000; l'itSMF

U.K. decise allora di creare il proprio schema di accreditamento.
Negli ultimi anni abbiamo avuto accreditamenti itSMF e TGA; il TGA fa parte del governo: era della Repubblica Federale Tedesca e l'ente di accreditamento era all'interno del governo tramite il DAR quindi il TGA rappresentava la parte operativa del DAR. Alla fine del 2010, l'itSMF U.K. vendette il suo schema di accreditamento all'AMPG. Dopo aver ceduto lo schema all'AMPG, nel 2011, il TÜV, che era accreditato dall'itSMF U.K., decise di non proseguire con l'APMG e di ottenere solo una certificazione ufficiale dall'ente certificatore nazionale.
L'AMPG è una compagnia privata e a mio parere non ha la reputazione che l'organismo nazionale, il TGA, possiede.
Inoltre, fino ad ora, nessun controllo è stato fatto dall'itSMF/APMG eccezion fatta per due aree:

- Pagate la quota?
- L'auditor ha passato il corso itSMF Auditor?

Ovviamente vi era anche un controllo su altri aspetti, ma cercando alcuni ambiti elencati sul sito ufficiale, non si sapeva esattamente cosa venisse certificato. Oltre a ciò, non veniva fatto alcun controllo dei file o controllo dei CV di un auditor.
Poco tempo dopo l'ente di certificazione nazionale prese in consegna anche l'ISO 20000 nel proprio portfolio; per cui dal mio punto di vista non c'è una forte domanda per ottenere uno schema di accreditamento privato.

Quali pensa che siano le ragioni per cui un'organizzazione decida di ottenere la certificazione ISO 20000?

- ***fornire più valore al business attraverso***
- ***efficacia***
- ***qualità***
- ***velocità nell'adattarsi***
- ***integrazione con i service providers***
- ***ridurre i costi***
- ***l'analisi comparativa***
- ***essere in grado di fornire servizi e partecipare alle gare (solo service providers)***

La ragione per i service provider esterni è avere un certificato perché è richiesto nelle gare; la ragione per i service provider interni è mostrare il business e che il reparto IT interno sta svolgendo un buon lavoro e sta implementando il Service Management e concentrarsi per migliorarsi anno dopo anno.
Se si intraprende un procedimento di certificazione, ovviamente il primo punto è ottenere la certificazione: nel caso si ottenga, il primo punto è mantenerla, dopo di che, bisogna migliorarsi e gli auditor devono controllare l'effettivo migliormaneto anno dopo anno: perdere la certificazione equivarrebbe a perdere la faccia. Per il CIO la certificazione rappresenta un altro modo di chiedere alle sue persone o al suo provider interno di rispettare gli SLA, di lavorare coordinati e di raggiungere il top, delegando una minima parte di responsabilità al mettere pressione all'auditor o ad un soggetto esterno che arriverà ogni anno.

Quanto spesso le organizzazioni decidono di intraprendere la certificazione ISO 20000 senza identificarne il valore per il loro business? Senza un business case? E senza una sufficiente condivisione del valore atteso con i più importanti stakeholders dei processi collegati all'ISO 20000?

Suppongo che molte compagnie non abbiano un business case realizzato in maniera ottimale: molti dei nostri clienti dovrebbero essere visti come "early adopters". Troverete qualcuno all'interno dell'organizzazione che spinge sul questo argomento: può anche essere proprio il CIO oppure il Service Manager dell'azienda; queste persone hanno una visione chiara della strategia per l'IT e la certificazione è per loro un passo per raggiungere quest'obiettivo. Alle volte fare pressione sull'organizzazione aiuta su base annua per mantenere lo slancio e migliorare l'IT anno dopo anno.

Ha notato qualche miglioramento anno dopo anno nelle organizzazioni che hanno ottenuto la certificazione ISO 20000?

Sì, assolutamente!!
Vi sono processi come il capacity management

e l'availability continuity management che sono, più o meno, processi di pianificazione; nella maggior parte dei casi le compagnie definiscono il processo di capacity e individuano un capacity manager, che è in carica per creare piani di capacity per tutti i servizi, ma quando si ha una compagnia un po' più grande, il capacity manager non può avere una conoscenza completa di tutti i servizi. In questi casi è pertanto indispensabile individuare per ciascun servizio un responsabile, che si occupi anche della reportistica sui livelli di servizio, sui possibili OLA e UC per quel servizio e sulla pianificazione di capacity ed availability.
È necessario avere un responsabile del processo di capacity planning, ma la conoscenza appartiene al service manager; è quindi necessario coordinamento tra il Capacity Planning Manager, che ha la responsabilità sul processo ed i service manager, uno per ogni gruppo di servizi IT, reponsabili di fornire informazioni su ciò che necessita il processo di capacity planning. Abbiamo quindi una persona che si occupa unicamente di definire il nostro piano di capacity ed una persona responsabile del servizio, la quale deve ora soddisfare i requisiti, ma che responsabile di provvedere al piano di capacity, ai dettagli di availability, per fornire i dettagli di servizio al service manager appropriato.

Quali sono gli eventi più critici che minacciano la certificazione? Come ad esempio un'acquisizione, nuova linea di business, un cambiamento organizzativo…

Un cambiamento nell'organizzazione e successivamente la perdita dello sponsor!

Quanto la creazione di valore* del percorso di certificazione è guidata dall'esperienza e conoscenza del lead auditor?
(*Non solo la correttezza della decisione finale).

C'è bisogno di un buon lead aditor: dal mio punto di vista, il lead auditor per l'ISO 20000 dovrebbe avere una conoscenza più approfondita rispetto al mero controllo dei requisiti. Per esempio, in riferimento allo schema di accreditamento di APMG, la richiesta per gli auditors è di essere auditor per qualsiasi standard e di partecipare a due giorni di corsi per auditor dell'APMG.
Per aiutare un'organizzazione a cambiare non devi solo conoscere un procedimento specifico, ma anche come aiutare l'organizzazione ad integrare i processi uno con l'altro e fornire un'organizzazione adatta, capendo l'impatto e tenendo conto delle risorse davverso disponibili all'interno di quella specifica organizzazione. Quindi conoscere un particolare processo non è sufficiente, ma bisogna anche sapere come mettere in moto i processi e l'organizzazione e definire un piano di gestione del cambiamento che sia compatibile con lo starting point dell'organizzazione.
Un buon lead auditor dovrebbe inoltre ispirare il consulente a fare meglio il suo lavoro e l'organizzazione a cercare il consulente adatto; quindi è un problema di conoscenza dei consulenti?
Sì, penso che il problema maggiore è che tutti i consulenti IT service management sanno come implementare tutti i processi, ma non hanno idea del sistema di gestione: si ha bisogno di sapere cosa sia un internal audit, cos'è il riesame della direzione, quale sia l'ambito di applicazione, quindi questi argomenti vanno affrontati e poi essere realizzati se si vuole ottenere la certificazione.

Quali sono i trend e le aspettative per il 2012? Più o meno organizzazioni che intraprendono la certificazione, nessun cambiamento nel livello di interesse, crescita di interesse per specifici mercati, una crescita globale dell'interesse…

Sto ancora aspettando il momento in cui l'ISO 20000 sarà un requisito richiesto per le grandi gare d'appalto. Fino ad ora, suppongo che le grandi compagnie stiano aspettando che più service providers abbiano un certificato ISO 20000; quando ciò succederà, allora l'ISO 20000 sarà un must per i service providers e ci sarà una pubblicità enorme. Credo che questo avverrà nei prossimi 5 anni.
In Germania, fino ad ora la certificazione ISO 27000 non è molto richiesta come requisito

nelle gare; nei prossimi 5 anni, suppongo, sarà richiesta nelle grandi gare e vi sarà una forte domanda di certificazioni ISO 20000 e ciò porterà molti service provider a ottenere questo certificato.

Quali requisiti più di altri riveleranno le debolezze e le non conformità?

- ***il commitment del management***
- ***policy e comunicazione***
- ***PDCA - internal audit e revisione del SMS (Service Management System)***
- ***gestione delle risorse***
- ***documentazione dei processi***
- ***registrazioni dei processi***
- ***i processi più critici (più alto numero di non conformità)***

La mia classifica personale sarebbe:

- PDCA - internal audit e riesame della direzione
- Vision -> mission -> obiettivi annuali per l'IT -> obiettivi per i processi
- Qualità delle registrazioni dei processi

I processi più critici sono: il Capacity Management, l'Availability Management e il Problem Management. Anche l'interfaccia tra Change & Release e Capitolo 5 non è ben compresa e dovrebbe essere spiegata in maggior dettaglio, dal mio punto di vista: non ho mai visto un processo di release ben eseguito. Molte aziende attuano davvero i change, ma rilasciano poi meno di ciò che hanno implementato nei change.
Nei primi anni di una certificazione indirizziamo sempre verso un'attenzione alla qualità delle registrazioni.I KPI identificati non sono sempre adatti ad essere utilizzati, ma questo potrebbe andare bene, perché l'organizzazione deve allenarsi per segnalare KPI indipendentemente dal senso: nella fase iniziale della certificazione ISO 20000 le organizzazioni non sono molto brave a scegliere il modo giusto per misurare il processo. Il senso dei KPI diventerà più cruciale quando l'organizzazione sarà più matura e avrà una buona qualità nei loro confronti e nello svolgimento dei processi. Giusto per darvi un suggerimento del modello di "maturità" cui stiamo portando i nostri clienti lungo l'arco di questi anni:

- ottenere una buona qualità di record, descrizione di processo e ruoli
- organizzare gli obiettivi di processo, ottenere dei buoni KPI
- usare i processi per ogni attività

Quale delle seguenti aree ha bisogno di più tempo per essere analizzata e potrebbe dare più valore all'organizzazione?

- ***processi***
- ***organizzazione***
- ***strumenti***

A mio parere: tutte quelle sopra menzionate! Credo che il più importante anzitutto sia pensare per prima cosa al processo, poi all'organizzazione.

Ho un reparto IT che è un provider interno che ha molti tasks affidati in outsourcing ad un service provider esterno; questo reparto vuole ottenere la certificazione, che tipo di requisiti elencati nella domanda 11 trova più critici?

Ovviamente è necessario dimostrare controllo e governo sugli outsources; essere owner del sistema di gestione e del processo di miglioramento continuo.

Se fossimo nel caso citato sopra, quando trova i seguenti problemi:

- ***un adeguato modello di governance (processi e responsabilità definiti ed adeguatamente suddivisi tra Dipartimento IT e service provider)***
- ***adeguate competenze e dimensioni mantenute all'interno delle organizzazioni***
- ***contratti allineati con SLA e OLA***
- ***strumenti integrati***
- ***log dei dati e dati sulle configurazioni non disponibili al Dipartimento IT***

Quando si dipende in maniera massiccia da un outsourcer e si vuole ottenere una certificazione, allora bisogna mostrarmi il governo sugli outsourcers, quindi bisogna essere owner del processo, non degli strumenti, e bisogna come minimo fornire

dei report. Ad oggi, non ho dei clienti che facciano fortemente ricorso all'outsourcing. Se vuoi ottenere una certificazione, devi sedere davvero al posto di guida, devi definire il processo, i KPI, mostrare una governance adeguata. Ovviamente devi avere per davvero un degli incontri di revisione regolari con l'outsourcer. Ciò che noto di più è una mancanza di government.
Se il dipartimento IT interno ha differenti strumenti rispetto al service provider esterno, l'integrazione di questi strumenti risulta essere qualcosa di importante, ma se ho una grande azienda, come usare i miei strumenti dipende un po' dalla misura del contratto.

Basandosi sulla sua esperienza, il processo di certificazione (incluso il mantenimento) è in grado di fornire in modo chiaro all'organizzazione la capacità di passare da un fornitore di servizi ad un altro? Quante volte le organizzazioni rinnovano i contratti senza una gara?

Con la certificazione l'azienda ottiene una panoramica più dettagliata delle proprie attività. Con ciò, si possono definire requisiti più precisi per il proprio fornitore.
Posso portarvi l'esempio di uno dei miei clienti che ha esternalizzato il supporto di primo livello: Aveva definito con precisione cosa voleva ottenere e le interfacce. Un altro cliente stava cercando un nuovo strumento ITSM e aveva prodotto una outline per la gara molto precisa. Uno dei topic della gara era anche quello di dare al fornitore qualche ora di tempo per sistemare il suo strumento per un processo speciale (ad esempio: incident) sulle premesse del cliente. Quindi la certificazione ISO 20000 aiuta nel conoscere cosa stia facendo il fornitore di servizi e aiuta ad identificare i modi per ottenere efficacia nei costi attraverso l'outsourcing dei processi o attività di out tasking.
Il processo di certificazione è decisamente la chiave per rendere l'organizzazione più matura, abbastanza da cambiare da un outsourcer ad un altro, perché il cliente conosce il processo e che cosa vuole dall'outsourcer; definisce in modo molto preciso le interfacce e come lavora.

Quando incontrate pratiche di body-rental, che cosa fate?

Sono parte della normale organizzazione. Si deve conoscere e seguire la normale descrizione di processo.

Qual è la sua opinione riguardo al rapporto tra servizi cloud-type e la ISO 20000? Come può la certificazione ISO 20000 aiutare il Dipartimento IT di un'organizzazione a gestire meglio i servizi cloud-type e a fornire più valore al loro cliente interno? Come può la certificazione ISO 20000 aiutare le organizzazioni ad acquistare ed integrare meglio i servizi cloud-type?

A mio parere un certificato ISO 20000 dovrebbe essere un must per avere la conferma che un cloud provider stia svolgendo un buon lavoro. Ma non solo l'ISO 20000, anche l'ISO 27000.

Quante volte rilevate violazioni SLA su quanti audits?

Sempre. Le violazioni SLA non sono l'argomento cruciale se si riporta la violazione e se si fanno dei miglioramenti: è normale. Un comportamento normale si ha quando all'interno degli SLA ci sono alcune misure definite che non sono riportate nello SLA reporting né internamente. Tipico esempio: l'80% degli incidents a priorità 2 e 3 sono risolti all'interno del tempo SLA.

Ci piacerebbe sapere se il processo di certificazione sia in grado di rendere chiara la capacità/maturità dell'organizzazione, una volta che gli incidents sono stati analizzati, di risolvere i problemi in modo definito e strutturato (policies, processi, ruoli, responsabilità, accordi interni), facendo ricorso ad un team ridotto e multi-disciplinare (Dev+Ops) in modo da identificare la root-cause, trovare soluzioni ed emettere la change request.

Non ho mai assistito ad un buon processo di problem management; credo che sia un processo davvero complicato: si ha un problema perché si sono verificati un paio di incidents e bisogna definire un cambiamento che gestisca questo problema quando si trova la root-cause, ma allora quanti costi ho in meno? Di solito le organizzazioni hanno un documento dei processi, ma non viene fatto in una forma adeguata; hanno una procedura formale e questo è buona cosa, ma quando vai a controllare davvero i records dei incident vedi che non sempre vengono fatte le cose giuste. Non ho davvero visto un'rganizzazione dove si realizza una buona analisi degli incident.

Quante volte il campo di applicazione della certificazione è limitato ad alcuni servizi IT / alcune unità organizzative / alcuni siti piuttosto che a tutti i servizi IT forniti dall'organizzazione?

La maggior parte dei nostri campi di applicazione sono ristretti ad un catalogo di servizi definito. Questo è un buon aiuto per ottenere la certificazione in anticipo e per incrementare il numero di servizi certificati anno dopo anno.
Questo aiuta anche il cliente.

Per quanto riguarda le organizzazioni che non sono IT Service Provider e che vogliono certificare il loro Dipartimento IT, che tipo di servizi IT sono maggiormente inclusi nell'ambito di certificazione?

- *ICustomer-facing-Services, servizi IT end-to-end che includono infrastrutture,applicazioni e componenti di supporto al servizio, quali ad esempio:*
  - *order processing*
  - *CRM,*
  - *SAP*
  - *i Servizi Tecnici:*
  - *service desk,*
  - *applicazione di sviluppo*
  - *fleet management*

Iniziano con un catalogo molto breve (2 o 3 servizi) e poi viene esteso anno dopo anno. Ciò aiuta a non porre troppa pressione sull'organizzazione. All'interno del catalogo vi sono più servizi per il cliente.

Quanto spesso l'organizzazione utilizza soluzioni che implicano processi di time-consuming solo per essere conforme all'ISO 20000 (e molto spesso abbandona queste soluzioni immediatamente dopo la revisione audit)? Per esempio:

- *Change record registrati attraverso documenti cartacei anziché strumenti di workflow*
- *CMDB multipli non integrati, alcuni dei quali realizzati attraverso file Excel*

Ovviamente si può non identificare questa situazione nell'audit di certificazione, lo standard non dice qualcosa su dove bisogna immagazzinare i dati CMDB, per esempio. Ma ovviamente se mi accorgo, almeno nella verifica di sorveglianza, l'anno dopo, che non sono avvenuti i cambiamenti necessari, allora mi innervosisco e li richiedo.

Potrebbe fornirci qualche esempio di queste non-soluzioni? Quando sono efficaci? Quanto incrementano i costi di gestione giorno dopo giorno (o diminuiscono l'efficacia)?

In molti casi, le organizzazioni non sono completamente pronte ad ottenere la certificazione e quando l'auditor entra nel posto dove hanno dei punti deboli, cercano di nasconderli. Ma questo non è un comportamento critico credo, poiché è normale, quindi voglio aiutarli a migliorare, l'importante è che il secondo anno riescano a gestire questi punti deboli.

Quali sono i principali errori che i professionisti IT commettono a causa della mancanza di conoscenza del processo di audit? (ad esempio: formalizzazione del documento non richiesta, design di metrics non implementato)

Gli errori principali riguardano:

- Contestualizzazione
- Documenti troppo formali
- Processi troppo legati allo standard ITIL

Una cosa che dico sempre al mio cliente, "Fate ciò che scrivete e scrivete ciò che fate". Ciò che noto è che scrivono ciò che suggerisce ITIL ma mettono in atto i loro processi.

SMS dopo la certificazione: mantenere la certificazione attraverso il cambiamento di servizio, come gestire variazione/estensione del campo di applicazione, come e quando rivedere il sistema.

Dev'esserci una verifica di sorveglianza ogni anno così che si debano per forza mostrare i miglioramenti.
Il piano di gestione dei servizi dovrebbe anche avere una sorta di time-frame sul come migliorare questi servizi.

Sviluppo di un sistema integrato di gestione per essere conformi alle norme ISO90001, ISO/IEC20000 e ISO/IEC27001. Quali sono i benefici di un sistema integrato di gestione? Com'è possibile integrare questi tre framework?

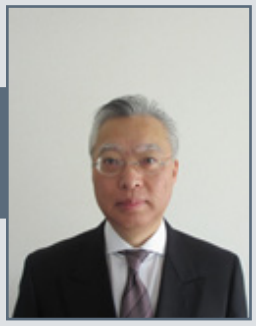
A mio parere solo un'integrazione di questi due o tre standard acquisisce significato. Almeno per i service provider l'integrazione dell'ISO 20000 e dell'ISO 27000 dovrebbe essere un obbligo: l'ISO 9000 è necessaria solo se sei un fornitore di servizi e hai un tuo reparto di sviluppo software perché non rientra nell'ambito dell'ISO 20000. Inoltre vi sono alcuni processi, come il Change Management, il Release Management e il Capacity Management che possono essere usati per entrambi gli standard. All'interno dei miei audit, cerco di combinare questi processi solo per condurre un'unica intervista con le persone responsabili e non avere due o tre sessioni di intervista per ogni standard, ma so che è un po' una sfida progettare un buon piano di audit per tutti e due/tre gli standard. Inoltre, vi è uno standard ISO DIS 27013 disponibile che è il risultato della combinazione dell'ISO 27000 e l'ISO 20000. Ho già dato un'occhiata veloce a questo standard e mi è parso molto buono.
Ho un paio di clienti che hanno tutti e 3 gli standard e ciò che cerco di fare è combinare questi standard in un approccio integrato, vorrei realizzare un audit gestendo tutti e tre gli standard; una gestione di sistema per tutti gli standard, un unico sistema di gestione.

Quali sono, secondo Lei, gli impatti più rilevanti della nuova versione ISO/IEC 20000:2011?

Secondo me la nuova verisone è un miglioramento della vecchia nella definizione di alcuni argomenti non specifici e ora più precisi. I più importanti sono il Capacity Plan, l'interfaccia tra Change& Release e il Capitolo 5. Ad essere onesto, ho puntato parecchio con i miei clienti su questo argomento, poiché lo reputo un punto cruciale.
La governance, introdotta nella nuova versione, non è proprio un concetto nuovo, poiché era già accennato nel documento di scoping dell'itSMF e dello standard ISO 20000-3. Penso che l'impatto più rilevante sia nel cambiamento del Capitolo 5, poiché vi si trovano più dettagli nella nuova versione dell'ISO 20000.

9 maggio 2012

Intervista con Sadao Fukatsu



Laureato in scienze informatiche, Sadao Fukatsu ha lavorato per circa dieci anni per uno dei più grandi laboratori di produzione di computer giapponesi, specializzato anche insistemi operativi, processori di linguaggio e intelligenza artificiale.
I dieci anni successivi sono stati investiti in progetti di sviluppo di notebook commerciali che lo hanno visto collaborare con Microsoft, Intel, BIOS e diverse compagnie di grafica. Ha presieduto uno degli standard di gestione del risparmio energetico per notebooks negli Stati Uniti.
Negli ultimi dieci anni, si è dedicato agli audit per le certificazioni ISO presso DNV per le ISO 9001, ISO 27001 ed ISO 20000.

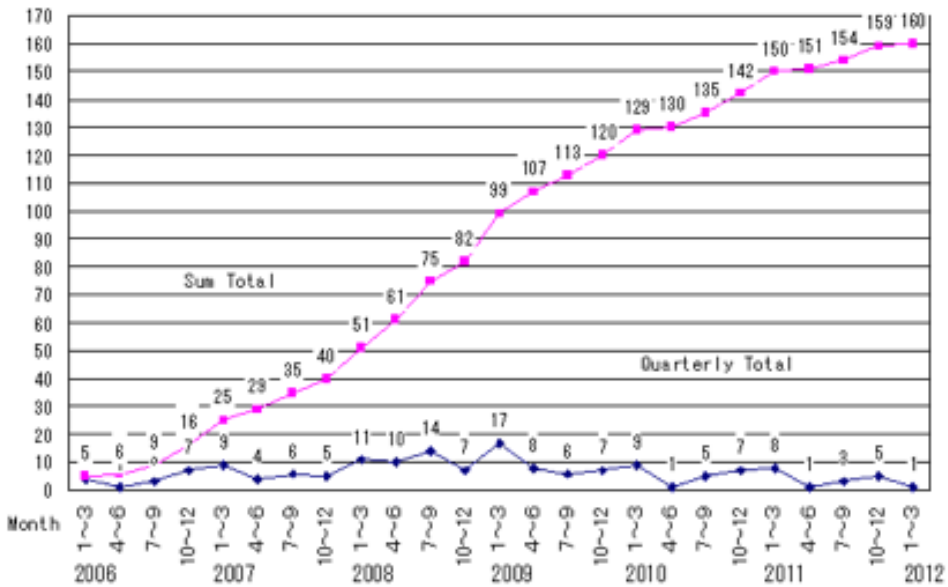
Quante organizzazioni certificate sono presenti in Giappone?

Più o meno 160. In Giappone, vi sono due diverse tipologie di compagnie, una è quella internazionale e l'altra quella nazionale. Potete vedere il grafico delle organizzazioni che sono certificate dal JIPDEC.
http://www.isms.jipdec.or.jp/english/itsms/lst/ind/org2.html

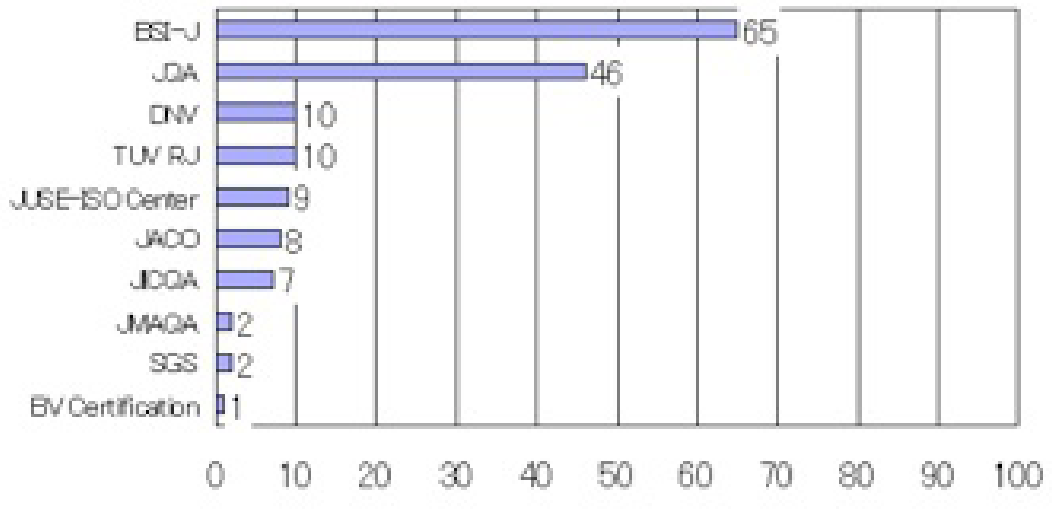
I Numeri dei Certificati ITSMS

20 Gennaio 2012
IMSPC, JIPDEC

ITSMS Certified Organizations by Quarter



ITSMS Certified Organizations
by Certification Body



Al 20 Gennaio 2012, il numero delle organizzazioni certificate ci risulta essere pari a 160.
La lista di tali organizzazioni è consultabile in "*List of ITSMS certified organizations*"
NOTA: I grafici sono stati creati sulla base dei dati riportatici dagli enti certificatori ITSMS.

http://www.isms.jipdec.or.jp/english/itsms/lst/isr/isr.html

Certification bodies accreditati ITSMS

Reg.#	Nome/Indirizzo	Data accreditam
ITR001	Japan Quality Assurance Organization (JQA) 2-5-2, Marunouchi, Chiyoda-ku, Tokyo, 100-8308, Japan	23 February 2009
ITR002	JIC Quality Assurance Ltd. (JICQA) 15-5, Shintomi 2-chome, Chuo-ku, Tokyo, 104-0041, Japan	18 May 2007
ITR004	BSI Group Japan K.K. (BSI-J) Seizan Bldg. 5F, 2-12-28, Kita-Aoyama, Minato-ku, Tokyo, 107-0061, Japan	18 December 2006
ITR005	Union of Japanese Scientists and Engineers ISO Center (JUSE-ISO Center) 5-10-11 Sendagaya, Shibuya-ku, Tokyo, 151-0051, Japan	12 November 2007

ITR007	Japan Audit and Certification Organization for Environment and Quality (JACO) 2-2-19 Akasaka, Minato-ku, Tokyo, 107-0052, Japan	15 October 2007
ITR008	DNV Business Assurance Japan KK (DNV) Sannomiya Chuo Bldg.,9th Floor, 4-2-20 Goko-dori, Chuo-ku, Kobe, 651-0087, Japan	14 September 2007
ITR011	JMA QA Registration Center (JMAQA) 105-8522 3-1-22 Shiba Koen, Minato-ku, Tokyo	28 March 2011
ITR015	TUV Rheinland Japa Ltd. (TUV RJ) Shin Yokohama Daini Center Bldg., 3-19-5, Shin Yokohama Kohoku-ku, Yokohama, 222-0033, Japan	23 July 2008
ITR018	Bureau Veritas Japan Co., Ltd. System Certification Services Headquarter (BV Certification) Silk Building, 1 Yamashita-cho, Naka-ku, Yokohama, Kanagawa, 231-0023, Japan	21 December 2009
ITR021	SGS Japan Inc. Systems & Services Certification (SGS) THE LANDMARK TOWER YOKOHAMA 38F 2-2-1,Minatomirai,Nishi-ku, Yokohama, 220-8138, Japan	11 January 2008

Se una compagnia volesse ottenere la certificazione dal DNV, potrebbe scegliere tra tre opzioni di certificazione: tramite il JIPDEC, attraverso UKAS ovvero combinando le prime due.

Quali settori risultano maggiormente interessati alla certificazione ISO 20000?

Principalmente gli IT outsourcer, ma vi sono diversi tipi di outsourcer, quali ,quelli di Facility Management, che alle volte si dedicano anche alla gestione dei software degli hardware e sono provider dei Data Center. Vi sono anche i servizi finanziari (banking, borsa valori, …)

Quanti ISO 20000 lead auditors conta il Giappone (non solo all'interno del DNV)?

Il numero non è facile da stimare, probabilmente un centinaio di lead auditor ricopre tale posizione, non dedicandosi tuttavia esclusivamente alle certificazioni ISO 20000. Già solamente in DNV è possibile contare 10 lead auditor; questo perché necessitiamo di più persone che si occupino del processo di certificazione ISO 20000, essendo presenti circa 160 compagnie certificate e non possiamo dedicarci esclusivamente all'ISO 20000. Al momento non possiamo permetterci di avere lead auditors dedicati esclusivamente all'ISO 20000.

Per quanto riguarda le certificazioni rilasciate in Giappone, quante risultano appartenere allo UKAS Accreditation Service e quante al JIPDEC?

Non conosciamo le cifre delle certificazioni UKAS; per il JIPDEC, le certificazioni rilasciate alla fine di Marzo 2012 sono pari a 160.

Quali pensa che siano le ragioni migliori per cui un'organizzazione decida di ottenere la certificazione ISO 20000?
fornire più valore al business attraverso:

- ***efficacia***
- ***qualità***
- ***velocità nell'adattarsi***
- ***integrazione con i service providers***
- ***ridurre i costi***
- ***l'analisi comparativa***
- ***essere in grado di fornire servizi e partecipare alle gare (solo service providers)***

La qualità è la ragione principale.

Quante sono le organizzazioni che decidono di intraprendere la certificazione ISO 20000 senza identificarne il valore per il loro business? Senza un business case? E senza una sufficiente condivisione del valore atteso con i più importanti stakeholders dei processi collegati all'ISO 20000?

Nessuna: tutte le organizzazioni eseguono un business case (processo formale molto strutturato nel quale si valutano costi e benefici di un progetto), riunendo un team per valutare costi e benefici del progetto stesso. In Giappone non è possibile intraprendere un progetto senza aver precedentemente realizzato un business case.

Ha notato qualche miglioramento anno dopo anno nelle organizzazioni che hanno ottenuto la certificazione ISO 20000?

Sì; ho costatato una maggiore efficienza per quanto riguarda la raccolta dei dati, la loro analisi, il loro miglioramento, la comprensione degli incidents; le organizzazioni hanno iniziato a distinguere alert, richieste e guasti. (es.) Un semplice esempio di miglioramento percepito è che ogni compagnia possiede un PC e deve avere una password per effettuare il log in; periodicamente, ogni tre mesi, è necessario forzare le persone a cambiare la propria password e alcuni la dimenticano, così risulta necessario per loro richiedere al Dipartimento IT di inizializzare la password così da poterne creare una nuova. Se hai un organico di 10000 persone, molte di esse possono venire al Dipartimento IT per cambiare o inizializzare la loro password; se non avessimo una modalità standard per poter gestire questa richiesta, sarebbe necessario ricorrere a procedure formali ed ottenere il permesso ogni volta che si riscontra questo tipo di problema, il che porterebbe via molto tempo prima di poter usare nuovamente il computer.
Così, al Dipartimento IT, si può ricorrere ad una speciale procedura dedicata all'inizializzazione della password e non risulta necessario ricorrere al Problem Solving o alla Negoziazione o al Change Management o a cose di questo genere: possono ricorrere una apposita procedura per il cambio password.

Tutto ciò non solo rende il tutto più sicuro, ma anche più veloce e quindi più efficiente per la compagnia.

Qual è l'elemento più critico che risulta essere una minaccia per l'organizzazione che vuole ottenere la certificazione?

L'acquisizione da parte di altre organizzazioni, ma è un fenomeno cui in Giappone non siamo molto avvezzi. In realtà, non percepiamo questa minaccia poiché in Giappone il modus decidendi è totalmente differente rispetto agli altri paesi: le nostre decisioni si fondano infatti sul consenso di gruppo, così il cambiamento di pochi manager solitamente non compromette le decisioni precedentemente prese.
Ad esempio, ipotizziamo che lei sia il mio capo e che dieci persone lavorino per lei, sapendo che domani qualcun altro verrà ad occupare la sua posizione; questo nuovo capo chiederà al gruppo cosa fare e come farlo, presenterà se stesso e le sue idee, confrontandosi con il gruppo sulle cose da cambiare.

Quanto sono importanti la conoscenza e l'esperienza del lead auditor per guidare la creazione di valore* per il percorso

di certificazione? (*Non unicamente la decisione finale per la certificazione)

I lead auditors non sono consulenti, quindi ufficialmente non forniscono aiuto o consigli per migliorare le organizzazioni nei metodi o processi, o simili: essi forniscono semplicemente risposte alle domande e valutano se le organizzazioni siano o meno conformi agli standard. In questi termini non necessitiamo di particolari competenze; dovremmo essere capaci di valutare il sistema di gestione e di trovare le debolezze dell'organizzazione. Dobbiamo avere esperienza e conoscenza per interpretare correttamente gli standard per i vari tipi e livelli di clienti con i rischi stimati. Ci è inoltre richiesta una vasta gamma di esperienze per essere in grado di valutare i nostri clienti dal miglior punto di vista pratico per i loro stakeholders. Anche un background nell'ambito de software development è molto importante, per comprendere la gestione degli incident e dei problemi, dei cambiamenti e delle configurazioni.

Quali sono i trend e le aspettative per il 2012? (Più o meno organizzazioni che intraprendono la certificazione, nessun cambiamento nel livello di interesse, crescita di interesse per specifici mercati, una crescita globale dell'interesse…)

Nessun cambiamento rilevante.

Quali requisiti più di altri riveleranno le debolezze e le non conformità?

- ***il commitment del management***
- ***policy e comunicazione***
- ***PDCA - internal audit e revisione del SMS (Service Management System)***
- ***gestione delle risorse***
- ***documentazione dei processi***
- ***registrazioni dei processi***
- ***i processi più critici (più alto numero di non conformità)***

L'efficacia dei processi, le misurazioni, le analisi e i miglioramenti.

Su quali delle seguenti aree crede sarebbe meglio spendere più tempo per dare più valore all'organizzazione?

- ***Processi***
- ***Organizzazione***
- ***Strumenti***

Processi anzitutto, ma c'è bisogno di equilibrio tra le tre. Se dovessi necessariamente prediligere un'area, sarebbe quella dei Processi, pur non ritenendo meno importanti le relative aree di Organizzazione e Strumenti.

Quali sono gli aspetti più critici quando l'organizzazione dipende in maniera massiccia dagli IT outsourcers?

Le organizzazioni hanno bisogno di una buona Governance degli outsourcers: sono molto importanti i contratti, gli SLA, gli audit interni, incontri regolari con gli outsourcers… questa è Governance!

(Nel caso di un'organizzazione fortemente dipendente da un IT provider esterno) Quali criticità trova maggiormente probabili tra le seguenti categorie:

- ***un adeguato modello di governance (processi e responsabilità definiti ed adeguatamente suddivisi tra Dipartimento IT e service provider)***
- ***adeguate competenze e dimensioni mantenute all'interno delle organizzazioni***
- ***contratti allineati con SLA e OLA***
- ***strumenti integrati***
- ***log dei dati e dati sulle configurazioni non disponibili al Dipartimento IT***

Un adeguato modello di governance (processi e responsabilità definiti ed adeguatamente suddivisi tra Dipartimento IT e service provider)

(Nel caso di un'organizzazione fortemente dipendente da un IT provider esterno) Basandosi sulla sua esperienza, il processo di certificazione (incluso il mantenimento) è in grado di fornire in modo chiaro all'organizzazione la capacità di passare da un fornitore di servizi ad un altro? Quante volte le organizzazioni rinnovano i contratti

senza una gara?

Quasi mai: gli outsourcers non hanno alcun concorrente; quasi tutti gli IT outsourcers sono sussidiari dell'organizzazione che compie l'outsourcing, lavorano insieme ad essa e non possono essere sostituiti.

Quando incontrate pratiche di body-rental (man-power), che cosa fate?

Controlliamo il piano di formazione e le relative registrazioni con un processo di screening. Dipende dal livello di lavoro che andranno ad intraprendere: il body-rental è molto diffusa in Giappone; la maggior parte delle società di servizi fanno ricorso alla pratica di man-power. La responsabilità di sviluppare un piano formativo per le persone che appartengono ad un provider esterno, ma che lavorano per l'organizzazione, è sostanzialmente una responsabilità delle compagnie, ma molto spesso: se assumi una persona individualmente, hai la responsabilità della sua formazione, poiché questa persona deve lavorare secondo le tue procedure; se assumi più di una persona, allora potresti aver bisogno di fornire anche un piano di formazione esterno nonostante la provata esperienza dei soggetti presi. I lead auditors possono controllare il tipo e grado di formazione in questione impartito dalla compagnia.

Qual è la sua opinione riguardo al rapporto tra servizi cloud-type e la ISO 20000? Come può la certificazione ISO 20000 aiutare il Dipartimento IT di un'organizzazione a gestire meglio i servizi cloud-type e a fornire più valore al loro cliente interno? Come può la certificazione ISO 20000 aiutare le organizzazioni ad acquistare ed integrare meglio i servizi cloud-type?

SLA e Business Continuity Management sono processi che potrebbero aiutare le organizzazioni a ad un miglior ricorso e gestione dei servizi cloud-type. Il configuration management è un processo chiave, ma occultato dal service provider: non è possibile vedere come siano gestite internamente le organizzazioni di servizi cloud-type; e se esse avessero eventuali incongruenze con il sistema, ci influenzerebbero negativamente dal punto di vista della configurazione. L'organizzazione non può vedere nulla a proposito della gestione delle configurazione. Ciò che si può vedereè probabilmente lo SLA, questo è quanto!

Quante volte rilevate violazioni SLA su quanti audits?

Nessuna violazione ingente: 5 o 6 su 10 audits e, tra queste, la maggior parte delle volte si tratta di violazioni minori, nella manutenzione (non è un gran problema).

Ci piacerebbe sapere se il processo di certificazione sia in grado di rendere chiara la capacità/maturità dell'organizzazione, di risolvere i problemi in modo definito e strutturato (policies, processi, ruoli, responsabilità, accordi interni) una volta analizzati gli, facendo ricorso ad un team ridotto e multi-disciplinare (Dev+Ops) in modo da identificare la root-cause, trovare soluzioni ed emettere la change request, lo è.

Sì, lo è.

Quante volte il campo di applicazione della certificazione è limitato ad alcuni servizi IT / alcune unità organizzative / alcuni siti piuttosto che a tutti i servizi IT forniti dall'organizzazione?

Per il 2012, per quanto riguarda i clienti DNV, il 90% ha un sevizio IT all'interno della ambito di certificazione ISO 20000 che include tutti i servizi IT, le organizzazioni IT e tutti i siti in cui l'IT è gestito. Questo significa che solo 1 società su 10 dei clienti di DNV che mantiene la certificazione ha un campo limitato; la pratica comune è quella di iniziare con un piccolo campo d'applicazione per poi allargarlo anno dopo anno.

Per quanto riguarda le organizzazioni (che non sono IT Service Provider) che vogliono certificare il loro Dipartimento IT, che tipo

di servizi IT sono maggiormente inclusi nell'ambito di certificazione?
I Customer-facing-Services, servizi IT end-to-end che includono infrastrutture, applicazioni e componenti di supporto al servizio, quali ad esempio:
- ***order processing***
- ***CRM,***
- ***SAP***

o i Servizi Tecnici:
- ***service desk,***
- ***applicazione di sviluppo***
- ***fleet management***

Nelle nostre organizzazioni il gruppo di application development costituisce il centro delle operazioni. E' responsabile di tutto, dallo sviluppo applicativo fino al funzionamento del sistema e solitamente gestisce lo sviluppo dell' IT Service Provider. Prima di tutto necessita di occuparsi dei Customer-facing-Services ed in seguito di estendere l'ambito ai Servizi Tecnici.

Preparare l'organizzazione per la certificazione: passaggi, raccomandazioni, principali errori da evitare…
- ***ruoli e responsabilità che vanno definiti, competenze e formazione necessari, strumenti utili, budget relativi alle risorse richieste***
- ***un modo migliore di gestire il processo di documentazione e registrazione per l'audit ai fini della certificazione***
- ***Pianificazione per la certificazione: tempi, principali milestones, raccomandazioni***
- ***Come l'audit interno influenza l'audit ai fini della certificazione***
- ***Utilizzo ottimale delle altre parti dell'ISO/IEC 20000 (2, 3, 4 ecc.)***
- ***Ruolo del consulente prima e durante l'audit ai fini della certificazione***

Se l'organizzazione non è sicura del proprio livello di maturità, è raccomandato avere un pre-audit. L'organizzazione deve inoltre avere un piano il quale specifichi quando si voglia ottenere la certificazione, quando si vogliano attuare tutti i processi, quando avere un internal audit, il riesame della direzione,…

Soliti passi/approcci usati in un audit per valutare la conformità del SMS

Processo per processo, processi incrociati…

Quanto spesso l'organizzazione utilizza soluzioni che implicano processi di time-consuming solo per essere conforme all'ISO 20000 (e molto spesso abbandona queste soluzioni immediatamente dopo la revisione audit)? Per esempio:
Change record registrati attraverso documenti cartacei anziché strumenti di workflow CMDB multipli non integrati, alcuni dei quali realizzati attraverso file Excel

Nessuna, grazie ai consulenti. Questo tipo di cose succedevano solo una volta, quando attuavamo l'ISO 90001 per il settore delle costruzioni, dove è obbligatorio avere il certificato partecipare ad appalti pubblici e le organizzazioni hanno bisogno di un riconoscimento scritto. Ma per l'ISO 20000 non abbiamo questo tipo di richieste in Giappone, ecco perché il numero di organizzazioni certificate è molto piccolo, perché nessuno vuole perdere tempo per ottenere un certificato senza svolgere attività di valore. Non riscontriamo nessun caso di società che vogliano solo ottenere un certificato.

Potrebbe fornirci qualche esempio di queste soluzioni? Quando sono efficaci? Quanto incrementano i costi di gestione giorno dopo giorno (o diminuiscono l'efficacia)?

NON APPLICABILE

SMS dopo la certificazione: mantenere la certificazione attraverso il cambiamento di servizio, come gestire variazione/ estensione del campo di applicazione, come e quando rivedere il sistema.
Una volta che l'organizzazione è certificata, come mantiene i service change, l'estensione del campo di applicazione, ecc. Quando lo attua?

Attraverso un audit periodico (annuale o semi-annuale). Se i cambiamenti di servizio sono estensioni ai servizi correnti, allora dovremo effettuare un ulteriore audit per quei servizi.

Sviluppo di un sistema integrato di gestione per essere conformi alle norme ISO90001, ISO/IEC20000 e ISO/IEC27001. Quali sono i benefici di un sistema integrato di gestione? Com'è possibile integrare questi tre framework? Quali sono i requisiti o le aree da cui crede che l'organizzazione tragga benefici quando vengono integrati sistemi di gestione?

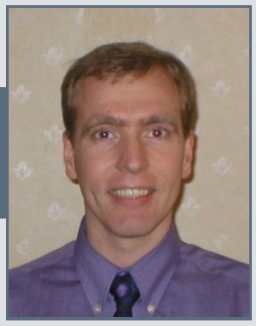
I benefici saranno l'eliminazione di duplicati di processi simili come i controlli della documentazione, i controlli di risorse,il Risk Management, l'Outsource Management, la formazione, le azioni correttive e preventive, ecc. TrickITPlus (schema UK per il settore ICT) fornisce esempi di framework per alcune integrazioni.

Quali sono, secondo Lei, gli impatti più rilevanti della nuova versione ISO/IEC 20000:2011?

Alcuni requisiti dettagliati sono chiariti. I miglioramenti per l'organizzazione verranno incrementati.

15 marzo 2012

Intervista con Paul Barrett



Paul Barrett si è laureato in Fisica ed Elettronica presso l'università del Kent a Canterbury .
Dopo alcuni anni come ingegnere di Produzione e di Qualità, dal 2003 diventa BSI Client Manager per la norma ISO9001.
Nel 2006 diviene BSI Key Account Client Manager, focalizzato su due grandi clienti IT & Technology-based e Lead assessor per i Sistemi ISO27001 Information Security Management.
Nel 2009 entra a far parte del BSI EMEA Key Account team, con responsabilità di delivery per EMEA, un key account globale e due UK-based.
Dal 2011 è inoltre Team Manager per lo Strategic Accounts Programme del BSI in Inghilterra.

Quante sono le organizzazioni certificate in Inghilterra?

L'APMG conta 60 organizzazioni nel Regno Unito elencate sul loro sito web, anche se non si tratta di una lista completa, in quanto non tutte le organizzazioni scelgono questa certificazione.
In Inghilterra il BSI ha 42 certificati che coprono 85 locations specifiche e le ricerche di mercato indicano che abbiamo approssimativamente il 45% delle quote di Mercato nel Regno Unito. Di conseguenza, la stima complessiva si aggira intorno alle 90 certificazioni.

Quali sono i settori maggiormente interessati all'ISO 20000?

I Governi Locali, l'Assistenza Sanitaria e le organizzazioni di IT Outsourcing.

Qual è il numero di lead auditors per la ISO 20000 in Inghilterra (non solo appartenenti al BSI-UK)?

Non abbiamo informazioni complete, comunque vi sono dieci Lead Auditor che lavorano con il BSI e ulteriori due Assessor in formazione. Alcuni soggetti tra quelli che lavorano con il BSI lavorano anche per altri organismi di audit, quindi una stima realistica sarebbe meno di venti lead auditor in Inghilterra. Molti dei nostri clienti hanno, tuttavia, lead auditors appartenenti al BSI o all'itSMF che lavorano internamente, o usano per gli audit consulenti specializzati.
L'itSMF potrebbe avere figure provenienti dai propri corsi di formazione.

Per quanto riguarda le certificazioni rilasciate nel Regno Unito, quante appartengono al Servizio di Accreditamento APMG, quante allo UKAS o ad altri Servizi di Accreditamento?

10 dei nostri certificati sono accreditati con l'AMPG; tutti i 42 con lo UKAS.

Quali pensa che siano le ragioni per cui un'organizzazione decida di ottenere la certificazione ISO 20000?

- ***fornire più valore al business attraverso***
  - ***· efficacia***
  - ***· qualità***
  - ***· velocità nell'adattarsi***

- ***integrazione con i service providers***
- ***ridurre i costi***
- ***l'analisi comparativa***
- ***essere in grado di fornire servizi e partecipare alle gare (solo service providers)***

Tutti questi fattori; ad ogni modo, da una limitata ricerca generale, l'efficacia delle performance operative e gli aspetti di conformità incidono sulla decisione in maniera più elevata della riduzione dei costi o delle maggiori opportunità di vendita.

Quanto spesso le organizzazioni decidono di intraprendere la certificazione ISO 20000 senza identificarne il valore per il loro business? Senza un business case? E senza una sufficiente condivisione del valore atteso con i più importanti stakeholders dei processi collegati all'ISO 20000?

Sulla base della nostra esperienza non spesso, anche se le organizzazioni a livello globale hanno un numero più alto di certificazioni rispetto a quelle che abbiamo noi in Inghilterra. Di solito la certificazione ISO 20000 rappresenta una decisione di livello strategico, che ha chiari obiettivi di business associati.

Ha notato qualche miglioramento anno dopo anno nelle organizzazioni che hanno ottenuto la certificazione ISO 20000?

Il miglioramento è una parte molto importante del modello di gestione del sistema e viene verificato durante il periodo di certificazione. Generalmente molti dei nostri clienti dimostrano miglioramenti anno dopo anno e la transizione all'ISO20000-1:2011 sta portando un cambiamento netto verso il miglioramento.

Quali sono gli eventi più critici che minacciano la certificazione? Come ad esempio un'acquisizione, nuova linea di business, un cambiamento organizzativo…

L'Acquisizione/fusione e il cambiamento organizzativo significativo si sono rivelati essere gli eventi critici per una certificazione continua.

Quanto la creazione di valore* del percorso di certificazione è guidata dall'esperienza e conoscenza del lead auditor? (*Non solo la correttezza della decisione finale).

Il ruolo di un team di audit dell'organismo di certificazione è anzitutto quello di verificare la conformità agli standard nel sistema di gestione. Ad ogni modo, le capacità e il background di un IT Service Management System Auditor risultano di solito nell'identificazione di opportunità per il miglioramento, all'interno delle costrizioni di imparzialità a cui siamo obbligati.

Quali sono i trend e le aspettative per il 2012? Più o meno organizzazioni che intraprendono la certificazione, nessun cambiamento nel livello di interesse, crescita di interesse per specifici mercati, una crescita globale dell'interesse…

Ci attendiamo una crescita in tutti i nostri mercati per il 2012 e anche oltre. La versione 2011 dell'ISO20000-1 sembra possa portare a più attività di certificazione, in quanto allineata in maniera più stretta agli standard dei sistemi di gestione esistenti a cui molte organizzazioni sono già adeguate.

Quali requisiti più di altri riveleranno le debolezze e le non conformità?

- ***il commitment del management***
- ***policy e comunicazione***
- ***PDCA - internal audit e revisione del SMS (Service Management System)***
- ***gestione delle risorse***
- ***documentazione dei processi***
- ***registrazioni dei processi***
- ***i processi più critici (più alto numero di non conformità)***

Dalla nostra analisi degli audit le seguenti condizioni sono state identificate come le maggior ragioni di

non conformità:

- Configuration Management
- Change Management
- Service Continuity e Availability Aanagement
- Document Management
- Supplier Management
- Problem Management
- Service Level Management
- Service Reporting

Quale delle seguenti aree ha bisogno di più tempo per essere analizzata e potrebbe dare più valore all'organizzazione?

- ***processi***
- ***organizzazione***
- ***strumenti***

Capire le strutture organizzative e l'interazione dei processi risultano aspetti chiave per un assessment efficace di un Sistema di IT Service Management.

Quali risultano essere i requisiti più critici quando l'organizzazione dipende in maniera massiccia da un outsourcer IT?

Con la versione 2011 degli standard, la clausola 4.2, che riguarda la Governance verso le terze parti (provider esterni), è un requisito critico laddove i processi di IT Service management sono esternalizzati.

(Nel caso in cui l'organizzazione dipendesse fortemente da un service provider IT esterno) Quando trova i seguenti problemi:

- ***un adeguato modello di governance (processi e responsabilità definiti ed adeguatamente suddivisi tra Dipartimento IT e service provider)***
- ***adeguate competenze e dimensioni mantenute all'interno delle organizzazioni***
- ***contratti allineati con SLA e OLA***
- ***strumenti integrati***
- ***log dei dati e dati sulle configurazioni non disponibili al Dipartimento IT***

Non possediamo un'analisi specifica per questi fattori, comunque la clausola 4.2 della versione 2011 dello standard è molto più specifica circa i requisiti per la Governance dei fornitori. L'esperienza attuale è che siamo soliti trovare accordi contrattuali ben allineati con gli SLAs e l'adozione di strumenti integrati non è inusuale – il che facilita la condivisione dei log e dei dati sulle configurazioni.

(Nel caso in cui l'organizzazione dipendesse fortemente da un service provider IT esterno) Basandosi sulla sua esperienza, il processo di certificazione (incluso il mantenimento) è in grado di fornire in modo chiaro all'organizzazione la capacità di passare da un fornitore di servizi ad un altro? Quante volte le organizzazioni rinnovano i contratti senza una gara?

Il pricing è diventato sempre più competitivo e frequentemente le organizzazioni ri-appaltano e cambiano fornitori di servizi non appena giunge il momento di rinnovare un contratto. Spesso troviamo ci sia una limitata pianificazione anticipata di questo cambiamento, nonostante sia un requisito dello standard ISO 20000.

Quando incontrate pratiche di body-rental, che cosa fate?

Il bisogno di Governance dei fornitori esterni generalmente preclude l'abilità di certificare organizzazioni che stanno utilizzando pratiche di body-rental. Abbiamo bisogno di stabilire con chiarezza le responsabilità di gestione quando si considerano le registrazioni e abbiamo rifiutato di certificare elementi delle organizzazioni laddove la responsabilità di risultava non essere all'interno dell'organizzazione che forniva le risorse.

Qual è la sua opinione riguardo al rapporto tra servizi cloud-type e la ISO 20000? Come può la certificazione ISO 20000 aiutare il Dipartimento IT di un'organizzazione a gestire meglio i servizi cloud-type e a fornire

più valore al loro cliente interno? Come può la certificazione ISO 20000 aiutare le organizzazioni ad acquistare ed integrare meglio i servizi cloud-type?

L'obiettivo primario per il Cloud Computing è quello di fornire un metodo cost effective ed efficiente nel rilasciare servizi IT. I benefici del Cloud Computing vengono ottenuti una volta che il fornitore di servizi ha ottenuto visibilità e controllo sui propri servizi. Un sistema di Service Management rispettoso delle norme monitora e controlla le attività di gestione dei servizi e può essere usato da fornitori di Cloud Service per accompagnare il raggiungimento di elevati livelli di qualità dei servizi. La parte 7 pianificata per la serie dello standard 20000 fornisce linee guida sull'applicazione dell' ISO/IEC 20000 al Cloud.

Quante volte rilevate violazioni SLA su quanti audits?

Non possediamo analisi specifiche a riguardo.

Ci piacerebbe sapere se il processo di certificazione sia in grado di rendere chiara la capacità/maturità dell'organizzazione, una volta che gli incidents sono stati analizzati, di risolvere i problemi in modo definito e strutturato (policies, processi, ruoli, responsabilità, accordi interni), facendo ricorso ad un team ridotto e multi-disciplinare (Dev+Ops) in modo da identificare la root-cause, trovare soluzioni ed emettere la change request.

Il processo di certificazione vuol stabilire la conformità all'ISO/IEC 20000-1 e a tutti quegli aspetti che sono parzialmente coperti e il processo di certificazione guarda all'efficacia del Sistema di Gestione dei Servizi per raggiungere gli obiettivi prefissati. In termini di capacità/maturità, ciò non è al momento previsto dal processo di certificazione ISO/IEC 20000-1, ad ogni modo vi sono frameworks di assessment e modelli che sono stati sviluppati e che renderanno possibile tutto ciò in futuro.

Quante volte il campo di applicazione della certificazione è limitato ad alcuni servizi IT / alcune unità organizzative / alcuni siti piuttosto che a tutti i servizi IT forniti dall'organizzazione?

- ***Le migliori pratiche per definire lo scopo della certificazione SMS***

Non è cosa inusuale per le organizzazioni limitare il loro ambito di certificazione soltanto a quei servizi forniti ad un cliente specifico, spesso a causa di un requisito contrattuale. Questo non significa necessariamente che i servizi al di fuori dell'ambito di certificazione non siano controllati e monitorati usando il Sistema di Service Management, è solo che le organizzazioni non desiderano averli certificati esternamente, generalmente per ragioni di costi. L'ISO/IEC 20000-3 fornisce linee guida sulla definizione dell'ambito e dell'applicazione dell' ISO/IEC 20000-1.

Per quanto riguarda le organizzazioni che non sono IT Service Provider e che vogliono certificare il loro Dipartimento IT, che tipo di servizi IT sono maggiormente inclusi nell'ambito di certificazione?

- ***I Customer-facing-Services, servizi IT end-to-end che includono infrastrutture, applicazioni e componenti di supporto al servizio, quali ad esempio:***
  - ***order processing***
  - ***CRM,***
  - ***SAP***
- ***i Servizi Tecnici:***
  - ***service desk,***
  - ***applicazione di sviluppo***
  - ***fleet management***

Spesso sono inclusi nell'ambito di certificazione i servizi associati all'infrastruttura IT, ai Network e al supporto di sistemi operativi e applicazioni di business. E' quasi sempre

Preparare l'organizzazione alla certificazione: fasi, raccomandazioni, errori principali da evitare…

- ***Ruoli e responsabilità da definire, capacità e formazione necessarie, strumenti utili, budget relative alle risorse di cui si ha bisogno***
- ***Miglior modo di gestire la documentazione di processo e dei record per la certificazione audit***
- ***Pianificare la certificazione: tempi, principali milestones, raccomandazioni***
- ***Come l'audit interno abbia effetti sulla certificazione audit***
- ***Utilizzo ottimale delle altre parti dell'ISO/IEC 20000 (2, 3, 4, ecc.)***
- ***Ruolo del consulente prima e durante la certificazione audit***

Le comuni attività del framework del sistema di gestione spesso non ricevono sufficiente considerazione – inclusi il controllo dei documenti e delle registrazioni, il riesame della direzione e l'audit interno – così come la definizione dei ruoli e delle responsabilità e i requisiti di competenza associata. Lo standard ISO20000-1:2011 ha valorizzato questi requisiti in modo che la situazione possa migliorare.

Fasi/approcci tipici usati in un audit per verificare la conformità dell'SMS:

- ***(processo dopo processo, processo incrociato, ..)***
- ***Gestire e indirizzare non-conformità maggiori e minori: il come***
- ***Quali sono gli errori maggiori che i professionisti IT commettono a cause di una mancanza conoscenza del processo audit? (ad esempio, formalizzazione del documento non richiesta, progettazione delle metriche non implementata)***

Il processo di Assessment segue un programma che esamina l'organizzazione del Service Management, il Sistema di Service Management e l'implementazione dei relativi processi sull'intero ambito di certificazione; le non conformità sono portate all'attenzione dell'organizzazione non appena vengono identificate e devono essere oggetto di revisione per determinare le cause di origine e le azioni correttive appropriate. Le non conformità maggiori richiederanno ulteriore momento di verifica per confermarne la chiusura; le non conformità minori, invece, richiederanno un piano di azione correttivo formale, che sarà revisionato in termini di pertinenza prima dell'emissione del certificato e controllato per verificare l'eliminazione delle non conformità durante le attività di verifica di sorveglianza. Errori comuni commessi risultano essere legati alla tenuta di documentazione con un eccessivo livello di formalismo o alla disponibilità di registrazioni che evidenzino conformità con processi documentati.

Quanto spesso l'organizzazione utilizza soluzioni che implicano processi di time-consuming solo per essere conforme all'ISO 20000 (e molto spesso abbandona queste soluzioni immediatamente dopo la revisione audit)? Per esempio:

- ***Change Record registrati attraverso documenti cartacei anziché strumenti di workflow***
- ***CMDB multipli non integrati, alcuni dei quali realizzati attraverso file Excel***

Le organizzazioni generalmente non implementano soluzioni che richiedono tempo per conformarsi all'ISO 20000-1, in quanto sarebbe in contrasto con gli obiettivi di migliore efficacia che di norma applicano quando si implementa il Sistema di Service Management. La maggior parte delle nostre organizzazioni certificate usano strumenti di Service Management che sono stati disegnati avendo in mente la conformità all'ISO/IEC 20000-1.

Potrebbe fornirci qualche esempio di queste

soluzioni? Quando sono efficaci? Quanto incrementano i costi di gestione giorno dopo giorno (o diminuiscono l'efficacia)?

Si veda la risposta alla domanda precedente: non è una cosa che riscontriamo.

SMS dopo la certificazione: mantenere la certificazione attraverso il cambiamento di servizio, come gestire variazione/estensione del campo di applicazione, come e quando rivedere il sistema.

Le organizzazioni sono incoraggiate a gestire proattivamente i cambiamenti del loro sistema di gestione IT. Il riesame della direzione richiede cambiamenti che avranno effetti sul sistema di gestione che vanno identificati ed azioni ben determinate. Tali aspetti saranno rivisti continuamente lungo tutto il percorso di sorveglianza della certificazione.

Sviluppo di un sistema integrato di gestione per essere conformi alle norme ISO90001, ISO/IEC20000 e ISO/IEC27001. Quali sono i benefici di un sistema integrato di gestione? Com'è possibile integrare questi tre framework?

Sistemi di gestione integrati riducono il duplicarsi dei documenti e forniscono una visione comprensibile più ampia dell'utente, dell'organizzazione e dei suoi processi. La guida verso l'implementazione integrata dell'ISO/IEC 27001 e dell'ISO/IEC 20000-1 sarà contenuta nello standard ISO/IEC 27013 e l'ISO/PDTR 90006 fornirà linee guida all'applicazione dell'ISO 9001 per il service management.

Quali sono, secondo Lei, gli impatti più rilevanti della nuova versione ISO/IEC 20000:2011?

La Governance sui fornitori, la progettazione dei processi di Transition di servizi nuovi e modificati e più chiari requisiti per i processi documentati.

HSPI SpA - Consulenti di Direzione
Viale Aldo Moro 16 - 40127 Bologna (Italy)
P.IVA 02355801206

Tel. +39 051 509861 | Fax. +39 051 509737
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it