Cesare Gallotti

From: it_service_management-news-bounces@mailman.cesaregallotti.it on behalf of IT Service Management NewsLetter [it_service_management-news@mailman.cesaregallotti.it]

Sent: Sunday, 15 November, 2009 09:33

To: it_service_management-news@mailman.cesaregallotti.it

Subject: [IT Service Management] Newsletter del 15 novembre 2009

Attachments: ATT00008.txt

****
IT SERVICE MANAGEMENT NEWS
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza http://creativecommons.org/licenses/by-nc/2.5/it/.
E' possibile iscriversi, disiscriversi e modificare le proprie opzioni, oltre a vedere l'informativa sul trattamento dei dati personali, all'indirizzo
http://mailman.ipnext.it/mailman/listinfo/it_service_management-news

****
Indice

****
01- Qualità (ISO 9004 e facilitazioni per aziende certificate)

ISO 9004:2009

E' stata pubblicata il 30 ottobre la nuova versione della norma ISO 9004. Non l'ho letta, ma il titolo dice già molto: "Managing for the sustained success of an organization -- A quality management approach".

In altre parole, non si tratta più della linea guida per approfondire la ISO 9001, ma una linea guida con ambizioni ben più ampie, trattando la qualità come elemento fondante della sostenibilità di un'azienda.

Si tratta di argomenti noti agli "esperti", ma ahimé troppo spesso dimenticati da alcuni auditor (che richiedono adempimenti senza riflettere sul loro impatto) e auditee (che pensano solo a passare la verifica, senza riflettere che la ISO 9001 è fatta per le aziende e non viceversa).

Certificazioni qualità e controlli amministrativi

(Ringrazio Edmea de Paoli della segnalazione) La Legge 133/2008 recita, all'articolo 30 comma 1:
"1. Per le imprese soggette a certificazione ambientale o di qualità rilasciata da un soggetto certificatore accreditato in conformità a norme tecniche europee ed internazionali, i controlli periodici svolti dagli enti certificatori sostituiscono i controlli amministrativi o le ulteriori attività amministrative di verifica, anche ai fini dell'eventuale rinnovo o aggiornamento delle autorizzazioni per l'esercizio dell'attività. Le verifiche dei competenti organi amministrativi hanno ad oggetto, in questo caso, esclusivamente l'attualità e la

completezza della certificazione. Resta salvo il rispetto della disciplina comunitaria."

Come commentare senza rischiare querele questa norma?

E' ovviamente ben noto, a chiunque l'avesse letta, che la ISO 9001 non tratta assolutamente di "attività amministrative". E quindi, come pensare che un auditor qualità (ovviamente non necessariamente formato in materia) possa condurre verifiche che coprano i controlli amministrativi?

****

02- Cancellazione di ITILv2

La newsletter di EXIN International segnala la decisione di OGC di cancellare ITILv2, in favore di ITILv3.

La cancellazione di ITILv2 procederà per fasi e si concluderà a giugno 2011. Si inizierà con la indisponibilità degli esami ITIL Foundation da giugno 2010 (con l'eccezione delle sessioni di recupero) e si continuerà, via via, con gli altri.

Le pubblicazioni in formato cartaceo non saranno più disponibili da Giugno 2011.

Maggiori dettagli su http://www.exin-exams.com/exams/it-standards/itil.aspx

****

03- Conferenza e materiale itSMF

Il 19 novembre a Milano si terrà la Conferenza Annuale di itSMF. Una buona occasione per discutere di Service Management.
http://www.itsmf.it/index.php?lng=1&method=section&action=zoom&id=1123

Segnalo, per chi non potesse parteciparvi, la pagina con le presentazione delle precedenti edizioni. Non sempre di livello omogeneo, ma interessanti
http://www.itsmf.it/index.php?method=section&id=229

****

04- Privacy e biometria
(Dalla Newsletter Giuridica di Filodiritto)

Finalmente il Garante dà un parere favorevole sui dati biometrici! Una buona lettura per cercare di capire cosa fare per avere il parere positivo.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=1557&newsfrom=2045

Continuo la mia polemica sull'Ufficio del Garante: sulla newsletter istituzionale non viene segnalato nulla di tutto ciò. Chi può fare qualcosa, lo faccia.

****

05- Lavori ISO per la nuova ISO/IEC 27001

Ricevo (e riassumo, probabilmente male) da Fabio Guasconi di Uninfo.

Vi riassumo gli argomenti di interesse trattati nelle sessioni plenarie del WG1 e del WG4:

- la 27001 può (ma non è obbligata) ad usare la nuova struttura per TUTTI i sistemi di gestione in corso di definizione da parte del JTCG; saranno approntati due WD (draft) paralleli prima del prossimo meeting, uno con la vecchia e uno con la nuova struttura
- nella 27001 compare ora esplicitamente il concetto di controllo degli outsourcers
- la 27002 vedrà la sua struttura modificata attraverso due sessioni specifiche nel prossimo meeting
- la 27013 (confronto tra norme 20000 e 27001) ha finalmente due editor definiti, uno dal SC27 e uno dal SC7 (ISO 20000) e possono iniziare i lavori veri e propri
- la 27005 vedrà iniziare uno study period per una sua revisione motivata dalla necessità di allineamento con la neo pubblicata 31000
- sono partiti dei contatti per verificare l'interesse dei Brand delle carte a un documento di linee guida per

l'approccio combinato a 27001 e PCI-DSS
- la 27008 includerà parte del testo di OSSTMM
- il prossimo meeting (plenaria) si terrà in Malaysia (Malaka)

Per quanto concerne i commenti italiani, vi anticipo che:
- l'approccio alla sicurezza nativa è stato accettato e comparirà nella parte iniziale della 27001 (anche se non usando il termine "nativa")
- si aggiungerà la definizione di "non conformità" alla 27001
- le procedure documentate della 27001 sono state riesaminate; le misurazioni di efficacia non necessitano più una procedura documentata (ma "solo" una procedura)
- si è proposto del testo integrativo per i dispositivi mobile e la loro sicurezza
- assieme agli USA è passata la necessità di nuove contromisure sulle verifiche tecniche di sicurezza

Mentre per la 27001 i commenti sono stati tutti indirizzati, quelli sulla
27002 erano molto più numerosi (270 pagine) e sono stati visionati per circa metà. Gli editor si sono offerti di valutarli offline e di sottoporre un testo modificato ai NB entro metà dicembre, termine entro il quale saranno resi disponibili i documenti ufficiali relativi alla risoluzione di ogni singolo commento.

Fabio Guasconi

****

06- Metodologie di Risk Assessment

Angelo Chiarot commenta il mio articolo su VERA.

"A suo tempo, avevo prodotto, insieme a persone di Spike Reply, il NERA: Not Easy Risk Analysis... :)
Era un approccio alla Risk Analysis (non Assessment) di mia concezione che diversamente da VERA affrontava la tematica con logica fisica, cioè non partendo dai processi ma dagli asset... dove veniva preferita una referenziazione di PROCESSI >> SERVIZI puntualmente elencati a fianco degli asset, piuttosto che una continua replicazione degli asset per dettagliare le risorse di processo.

Ad esempio, partendo dall'ambito 'building' si avevano le seguenti catene:
a) BUILDING >> CED >> SERVER >> APPLICATIVO/DB >> INFORMAZIONE (+appartenenza a processo e servizio)
b) BUILDING >> UFFICIO >> PERSONE >> STRUMENTI >> INFORMAZIONE (+appartenenza a processo e servizio)

In effetti, come presagivi fondatamente, questo approccio è in effetti un po' una bomba ad orologeria, quanto a dati prodotti. Una grande massa di informazioni pronta ad esploderti in faccia, ma molto parlante con un'eccellente granularità.

Quindi, pur trovando VERA molto interessante, resto sempre un po' dell'idea d'essere 'contrario alla pentola a pressione, perchè non si vede la cottura'".

Ringrazio molto Angelo, perché ha colto il mio invito a riflettere sulle metodologie di Risk Assessment. Non penso esista un'unica soluzione per tutte le esigenze, ma sono sicuro che il dibattito è importante affinché ciascuno di noi possa poi adottare, di volta in volta, l'approccio più corretto.

PS: Qualcun altro mi aveva accennato ad una sua riflessione su "metodologie vecchie e nuove"; quando mi scriverà due righe in merito, ve le girerò. Chiunque è invitato a condividere le proprie riflessioni.

****

07- Perché i progetti falliscono

Questo articolo (segnalato dalla ITSM Newsletter) illustra molto bene perché i progetti ITIL falliscono. Il titolo è simpatico (richiama Shakespeare) e l'articolo molto buono: "ITSM Projects: A Tragedy in Five Acts". Applicabile, purtroppo, anche ad altri ambiti (sicurezza, qualità, business process reengineering, eccetera)
http://s236467555.onlinehome.us/2009/11/02/itsm-projects-a-tragedy-in-five-acts/

Ovviamente, l'ultimo paragrafo pubblicitario può essere ignorato.

****

08- Mutuo riconoscimento delle certificazioni del personale

L'IRCA annuncia la sua prossima uscita dall'ICP.

L'ICP è una sorta di accordo di mutuo riconoscimento delle qualifiche del personale. In particolare per quanto riguarda le qualifiche di Lead Auditor ISO 9001, ISO/IEC 27001 e altri. In Italia, l'ente di riferimento in ambito ICP è il CEPAS.

Per quanto riguarda le certificazioni aziendali ISO, esiste un accordo simile a livello europeo e internazionale.

Mi preoccupa molto il fatto che IRCA, uno degli organismi più importanti di qualifica del personale, voglia uscire da questo accordo. Infatti, anche da alcuni esempi raccolti all'estero, sembra che sia difficile già ora far accettare qualifiche non-IRCA, anche se perfettamente equivalenti ad essa.

Purtroppo, questa notizia mi fa temere o ad un futuro monopolio o ad una futura confusione: già oggi quasi tutti i bandi, quando riportano i requisiti di qualificazione del personale, lasciano a desiderare. Ora sarebbe già stata una conquista vedere un requisito del tipo "Lead Auditor ISO/IEC 27001 qualificato IRCA o equivalente"; nel futuro, però, il termine "equivalente" non potrà più essere facilmente definito.

http://www.irca.org/inform/issue23/IPCauditors.html?dm_i=4VM,1RE3,HZSOT,5MGC,1

****

09- Novità tecniche (BCM e sourcing)

NIST e Business Continuity

Il NIST annuncia la pubblicazione della bozza della "Guida per il Contingency Planning" SP 800-34 rev1. Io sono un grande fan di questa guida e ne raccomando la lettura a quanti vogliono imparare o approfondire le tecniche di Business Continuity e Disaster Recovery.
http://csrc.nist.gov/publications/PubsDrafts.html#800-34-Rev1

eSourcing Capability Model for Client Organizations (eSCM-CL)

Grazie alla newsletter di Quint Wellington Redwood Italy dell'Ottobre 2009, sono venuto a sapere della presenza dell'eSourcing Capability Model for Service Providers (eSCM-SP) e dell'eSourcing Capability Model for Client Organizations (eSCM-CL). Gli attuali modelli furono pubblicati a fine 2006 (anche se li presento come "novità tecniche").

Le tematiche del sourcing sono sempre più importanti per le strategie delle aziende. Segnalo pertanto il link da cui scaricarli e dove trovare ulteriori informazioni
http://itsqc.cmu.edu/

****

10- Cloud Computing

Il Cloud Computing è la nuova moda in materia di tecnologia. Io ho fatto un po' di fatica a capire esattamente di cosa si tratta e qualche chiaccherata con altri colleghi mi conferma che non è così semplice definirlo.

E la definizione data da Whatis.com, in effetti, fornisce tanti tipi di Cloud Computing che questa confusione è comprensibile.
http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html

In termini di sicurezza, il Cloud Computing presenta certamente alcuni aspetti da tenere sotto controllo. Ma, mi viene da pensare, quanti di questi aspetti sono comuni all'hosting dato in outsourcing? Tante aziende danno in hosting i loro sistemi e non hanno assolutamente il controllo degli amministratori di sistema, di come vengono effettuati i backup e di come è effettivamente gestita la rete; non hanno mai fatto audit ai fornitori, eccetera. Mi chiedo il perché di tutta questa preoccupazione solo quando si parla di Cloud.

E' vero che il Cloud Computing oggi offre molte possibilità nuove, ma già vecchie (seppure in modi diversi) negli

ambiti AS/400 (eSeries) e OS390 (zSeries), grazie alla più veloce interfaccia a carattere. E infatti ho buona memoria di un progetto che ho gestito per il quale abbiamo impiegato parecchio tempo a capire se i dati erano in Italia, Olanda o USA.

Questo articolo presenta una visione meno drammatica della realtà:
http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1370646,00.html?track=NL-1329&ad=728897&asrc=EM_NLN_9520382&uid=5093788

L'articolo di Fred Cohen & Associates è più equilibrato
http://www.all.net/Analyst/2009-08.pdf

Ma non dimentichiamoci i rischi. Il caso di Sidekick (una forma di Cloud Computing per utenti consumer) può essere emblematico (da SANS NewsBites Vol. 11 Num. 81)
http://www.computerworld.com/s/article/9139261/T_Mobile_sidelines_Sidekick_in_wake_of_data_debacle?taxonomyId=1
http://www.msnbc.msn.com/id/33278150/ns/technology_and_science-security/

In definitiva, è sicuramente bene studiare correttamente la tecnologia offerta e i relativi contratti.
http://www.isaca.org/Template.cfm?Section=Research2&CONTENTID=53050&TEMPLATE=/ContentManagement/ContentDisplay.cfm

****

11- Certificazione slot machines (e caso giudiziario)

Su Certinews (www.certinews.it) del novembre 2009 si trovano gli aggiornamenti su una faccenda non edificante: nel 2007 il PM di Venezia dispose il sequestro di più di 100mila slot machines non rispondenti alla normativa vigente e indagò, tra gli altri, l'azienda produttrice delle slot e l'ente di certificazione delle slot stesse.
http://www.acmi.ws/20070911497/notizie/bologna-i-noleggiatori-rischiano-il-sequestro.html

Stando alla normativa (http://www.aams.it/site.php?page=20050516155011121&op=download) l'Amministrazione autonoma dei Monopoli di Stato dovrebbe aver copia del sistema certificato, in modo da poter verificare se non fosse stato modificato in fase di vendita delle slot.

Stando al Cermet, sembra che il giudice non voglia aver troppo a che fare con perizie tecniche. Ma gli articoli letti non aiutano a capire la situazione, comunque potenzialmente interessante in ambito computer forensics.
http://www.gioconews.it/generale/black-slot-il-gup-rigetta-le-istanze-delle-difese-l11-dicembre-parte-il-processo-2982.html

Faccenda inquietante, comunque vada a finire. E fa riflettere sui rischi, i limiti e le difficoltà delle verifiche ispettive.

****

12- Errata Corrige

Mauro Cicognini, facendo riferimento alla mia segnalazione del mese scorso sulla "Introduzione alla BS 25999" organizzata dal Clusit, mi ricorda che "le slide ovviamente saranno disponibili con il consueto calendario: in breve tempo per i soci Clusit nell'area riservata, per tutti invece soltanto dopo almeno due anni dalla pubblicazione".

_____
Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italy)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it

No virus found in this incoming message.
Checked by AVG - www.avg.com
Version: 9.0.707 / Virus Database: 270.14.65/2503 - Release Date: 11/14/09 20:42:00