N° 2 2009

di Lorenzo Caselli

Insegnare etica nelle Facoltà di Economia

saggi

working paper

< indietro

Reg. Tribunale di Genova, n. 11/2004 del 31 maggio 2004 ISSN 1824-3576 Cod. CINECA E187020 p.iva 00754150100

IMPRESAPROGETTO
RIVISTA ON LINE DEL DITEA n. 2 - 2009

Controlli interni e requisiti del Sarbanes-Oxley Act

Roberto Garelli

Sommario: 1. COBIT e i controlli IT – 2. Sarbanes-Oxley Act, PCAOB e COBIT – 3. I controlli relativi al dominio “acquisizione ed implementazione” – 4. I controlli relativi al dominio “erogazione ed assistenza-supporto” – 5. Alcune considerazioni conclusive - Bibliografia

Abstract

The Sarbanes-Oxley Act (SOX), approved in 2002 by the U.S. Congress after the well known Enron and Worldcom scandals, is focused on the necessity to give back credibility to American financial system. It requires SEC listed companies to document, evaluate and monitor on control of financial reports and on controls of the declarations and procedures expecially IT controls. In this context executives are considered responsible in defining and evaluating the effectiveness of internal controls related to financial report. The control objectives relevant for SOX purposes are a specific subset of the COBIT control objectives. In this subset 12 processes are identified in accordance with PCAOB principles and they are subdivided into 68 audit activity controls. All organizations should use SOX as a stimulus to improve their internal controls.

1. COBIT e controlli IT

L’annosa questione relativa all’individuazione e alla gestione degli indicatori quali-quantitativi per il monitoraggio delle performance acquista particolare rilevanza nell’ambito dei sistemi connessi con l’IT (anche con specifico riferimento al caso in cui questi ultimi siano correlati con la gestione della reportistica istituzionale) dove, la necessità di standardizzare i controlli – soprattutto alla luce della crescente complessità di tali sistemi – è sentita come esigenza irrinunciabile. La componente IT risulta oggi – innegabilmente - sempre più integrata nei processi aziendali per cui il costante monitoraggio degli elementi e delle procedure che ne permettono l’espletamento delle specifiche funzioni ha reso necessaria l’adozione di appositi framework di controllo. Tra i molteplici

standard e procedure utilizzate a tal fine emergono, in relazione alla loro diffusione:

- il COBIT, con specifico riferimento alla governance dell'IT; esso si inserisce nella gerarchia che parte dai business driver ed arriva sino ai processi ed alle procedure di governance;
- ISO/IEC 27000, focalizzati sugli aspetti della sicurezza dei sistemi informativi; ISO/IEC 27001, in particolare, è uno standard che inquadra i sistemi di gestione della sicurezza e ne stabilisce i requisiti per la definizione, la gestione e il sistematico monitoraggio[1].
- ITIL, sviluppato alla fine degli anni 80 per l'utilizzo da parte dell'Amministrazione Pubblica Inglese, può essere definito come un insieme di best practise per la razionale gestione dei servizi IT; si è rapidamente diffuso in tutti i contesti aziendali e, attualmente, rappresenta uno standard riconosciuto a livello internazionale;

A livello internazionale è stato individuato il COBIT come metodologia standard sia per la definizione, la gestione e il monitoraggio dei controlli connessi con i processi IT sia per promuovere specifiche azioni finalizzate alla riduzione – a livelli genericamente definiti come "accettabili" - dei rischi derivanti dagli errori di sistema.

COBIT, definito come "Control Objectives for Information and Related Tecnology", permette l'utilizzo di vere e proprie linee guida per la gestione e il controllo dei sistemi IT ed è uno dei modelli più noti a livello internazionale.

La prima versione del modello COBIT è stata ideata nel 1994. Negli anni successivi i molteplici studi e le plurime rivisitazioni hanno permesso di implementare versioni sempre più complete fino ad arrivare ad un consolidamento dei risultati da parte della COBIT Steering Commitee. Con la terza versione di COBIT, pubblicata nel 2000, sono stati ulteriormente rivisti alcuni elementi salienti e, in particolare, inserendo le linee guida per il corretto utilizzo e sviluppando ulteriormente la sezione dedicata all'IT governance, si è giunti ad un framework riconosciuto ed applicato dalle più importanti realtà aziendali. Lo strumento in esame viene costantemente revisionato e migliorato, dal momento che l'International Governance Institute, per mezzo del COBIT Steering Committee, intende far evolvere COBIT in relazione alle mutate esigenze del contesto[2]. La versione 4.0 di Cobit[3] è composta da quattro sezioni:

[1]Lo standard è noto anche come "ISMS: Information security management systems – Requirements".

[2]Si tratta di aggiornamenti basati sull'esperienza dei team di associati ISACA, degli utilizzatori in tutto il mondo di COBIT, di advisor esperti e di studiosi; inoltre gruppi di sviluppo locali formati da 6 - 10 esperti a Brussel (Belgio), Londra (UK), Chicago (USA), Canberra (Australia), Cape Town (Sud Africa), Washington DC (USA) e Copenhagen (Danimarca) si sono riuniti, in media, due o tre volte l'anno per collaborare su specifiche ricerche o per confrontarsi sui compiti loro assegnati dal COBIT Steering Committee. www.iasaca.org**.**

[3]La versione COBIT 4.1 è ad oggi presente sul mercato ma la versione 4.0 è sino ad ora la più utilizzata.

- l'executive overview,
- il framework,
- il core content dei nuovi contenuti (obiettivi di controllo, attività di controllo, linee guida),
- indici (diverse mappature e cross-references, maggiori informazioni sul maturity model, materiale per i riferimenti, descrizione del progetto ed un glossario).

Come si può notare nella figura 1 "COBIT Overview – Cobit cube", il "core content", che rappresenta l'elemento saliente ai fini di questa trattazione, è suddiviso in 34 processi, ciascuno dei quali risulta descritto in quattro sezioni dedicate a:

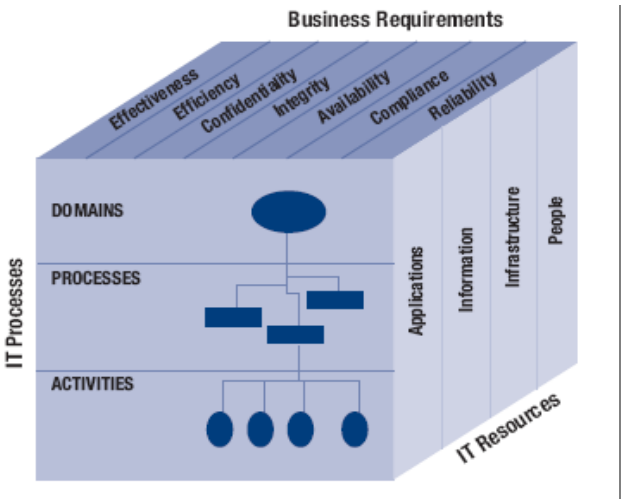
- obiettivi di controllo di alto livello - (descrizione, metriche, pratiche, mappature rispetto ai domini, risorse IT);
- management guideline[4]: input ed output del processo, schema RACI (responsible, accountable, consulted e/o informed), obiettivi e metriche;
- il maturity model di ogni processo.

I sopracitati processi, che danno origine a 318 attività di controllo (correlate agli obiettivi di dettaglio), sono raggruppati, nell'ambito del "core content" nei 4 domini di seguito descritti.

- Pianificazione e Organizzazione (Plan and Organize - PO). Questo dominio si riferisce agli aspetti, soprattutto di natura strategica, insiti nella funzione IT; con esso ci si propone di evidenziare come la funzione IT possa concorrere al raggiungimento degli obiettivi aziendali nel modo più efficace ed efficiente possibile. Acquista particolare rilevanza, in tale sede, la valutazione dei livelli di allineamento degli aspetti IT con la strategia aziendale.
- Acquisizione e Implementazione (Acquire and Implement - AI). Si tratta di monitorare i processi relativi sia all'identificazione, acquisizione o realizzazione delle soluzioni IT più opportune sia alla loro messa in opera nel contesto aziendale. E' oggetto di questo dominio anche il monitoraggio dei cambiamenti e la manutenzione dei sistemi IT.
- Erogazione ed Assistenza-supporto (Deliver and Support - DS), Vengono monitorati, in questa sede, i processi di erogazione dei servizi con particolare attenzione ai diversi gradi di disponibilità, ai livelli di sicurezza del servizio, al supporto agli utenti e ad ogni altro elemento che consenta l'erogazione dei servizi IT in linea con le priorità del contesto. Vengono altresì monitorate le condizioni di sicurezza che necessariamente devono esistere alla base di ogni "manipolazione" delle informazioni.
- Monitoraggio e Valutazione (Monitor and Evaluate - ME) Il dominio è dedicato sia alla valutazione sistematica della qualità dei processi IT sia alla conformità con le leggi ed i regolamenti.

[4]Sono inseriti in questo contesto gli input ed output del processo, lo schema RACI (responsible, accountable, consulted e/o informed) e metriche.

Figura 1 – COBIT Overview COBIT cube



Fonte: Obiettivi di controllo per la Sarbanes-Oxley (2008), www.isaca.org

La corretta applicazione del modello COBIT dovrebbe poter rendere possibile il raggiungimento dei seguenti obiettivi di governance dei sistemi IT:

- individuare e gestire in modo sistematico e coerente il collegamento tra gli tra gli obiettivi della funzione IT e gli obiettivi espressi a livello aziendale,
- organizzare sistematicamente le diverse attività della funzione IT secondo un modello generalmente accettato
- precisa definizione sia degli "obiettivi di controllo" da utilizzare a livello gestionale sia dei modelli di valutazione dei processi IT,
- specifica individuazione delle attività di controllo e dei target di riferimento.

2. Sarbanes-Oxley Act, PCAOB e COBIT

Il Sarbanes-Oxley Act (SOX), come noto, è stato approvato dal Congresso USA (2002) per migliorare la "corporate responsibility" delle aziende quotate nei mercati americani. Tale intervento, successivo ai noti scandali finanziari statunitensi (ci si riferisce in particolare agli scandali Enron e Worldcom), trova la sua ragion d'essere nel tentativo di ristabilire la fiducia nei confronti delle della coorporate goverance delle grandi compagnie americane; nel documento infatti, che si occupa sostanzialmente di regolamentare i comportamenti aziendali in tema di accountability, disclosure e reporting, è possibile leggere, tra l'altro, che:

"in azienda è obbligatoria una "corporate governance" efficace e sono richiesti comportamenti etici e conformi alle norme (compliance)"[5].

In particolare, il contesto estremamente complesso in cui si esplicano i processi che generano i report istituzionali impone, sempre più frequentemente, l'utilizzo di sistemi ERP in tutte le fasi delle transazioni di natura economico-finanziaria; ne consegue che l'applicazione di un sistema di verifiche sistematiche dei controlli IT rappresenta dunque una notevole opportunità per tutte quelle aziende che intendono attivare o mantenere comportamenti "compliant" ai requisiti SOX.

Con riferimento al sopracitato "Act", ai fini della trattazione in esame, è possibile rammentare alcune considerazioni, originarie o interpretative, che informano il sistema dei controlli connessi con le relazioni che si instaurano tra i sistemi IT e la gestione del reporting istituzionale (financial reporting).

- Il documento è rivolto a chi deve soddisfare i requisiti di conformità IT in ambito SOX ma può anche essere usato come supporto per le attività generali di IT compliance di aziende che non sono soggette al Sarbanes-Oxley Act e che tuttavia vogliono migliorare il proprio sistema di controlli IT.
- Alle aziende quotate e registrate presso la SEC[6] è richiesto di effettuare annualmente un assessment sul proprio sistema di controllo interno e sottoscrivere un rapporto sulla efficacia dei controlli relativi al financial reporting (sezioni 302 e 404)
- L'affidabilità del financial reporting è strettamente correlata ad un sistema IT controllato e coordinato con finalità aziendali; i controlli IT devono essere opportunamente verificati nel contesto della rendicontazione istituzionale.
- Si pone l'accento sul fatto che i controlli IT indicati dalle pubblicazioni citate riguardano ovviamente solo gli aspetti del financial reporting.
- Tutti gli apprezzamenti relativi ai controlli non devono considerati staticamente poiché la materia (così come il contesto di applicazione) è sempre in evoluzione e richiede continue rivisitazioni delle indicazioni generali.
- Si considerano gli excutives direttamente responsabili del processo di valutazione e monitoraggio relativo all'efficacia del sistema dei controlli interni correlati con la gestione della reportistica istituzionale. "Senior" e "owners" hanno dunque l'obbligo sia di stabilire e mantenere un'adeguata struttura di controllo sia di valutarne sistematicamente l'efficacia.
- I soggetti interessati (interni o consulenti) devono quindi migliorare la conoscenza dei controlli interni, conoscere e condividere il piano aziendale di compliance alla Sarbanes-Oxley, sviluppare un proprio compliance-plan per i controlli IT, integrare tale piano con i quanto richiesto dalla Sarbanes-Oxley.

Per meglio comprendere, da un punto di vista operativo, quali siano i controlli applicabili nel contesto esaminato occorre ricorrere all'Auditing Standard n. 2, intitolato "Audit dei controlli interni sul financial reporting in congiunzione con

[5]Obiettivi di controllo IT per la Sarbanes-Oxley – Il ruolo dell'IT nella progettazione ed implementazione dei controllli interni rispetto al financial reporting. – Edizioni ISACA 2006 (ingl) e 2008 (ita).
[6]U.S. Securities and Exchange Commission.

l'audit dei financial statements", emanato dal PCAOB ed approvato dalla SEC nel 2004[7]. In estrema sintesi, lo standard:

- individua i requisiti necessari per l'audit dei controlli interni sul financial reporting;
- fornisce direttive in merito all'approccio richiesto agli auditors;
- evidenzia requisiti specifici per gli auditor onde permettere la reale comprensione di operazioni quali: inizializzazione, autorizzazione, registrazione delle transazioni, processing e comunicazione dei risultati;
- fa specifico riferimento al fatto che la registrazione e il processing delle informazioni di business richiedono spesso peculiari applicazioni finanziarie;
- richiama il concetto di "affidabilità dell'informazione" sottolineando come esso dipenda – anche se non in via esclusiva – dall'utilizzo di sistemi IT (database, network, sistemi operativi).

In estrema sintesi, lo Standard n. 2 ribadisce che la reportistica istituzionale può raggiungere un determinato livello di affidabilità solo se tutti i sistemi IT coinvolti sono opportunamente monitorati a partire dalla fase di progettazione per arrivare ai momenti di manutenzione o di cambiamento e se, contemporaneamente, esiste uno specifico insieme di controlli interni volto a valutarne sistematicamente l'allineamento con gli obiettivi di fondo. Si tratta della c.d. pervasività che l'IT esplica sui controlli interni relativi al financial reporting. Si riconosce quindi l'estrema rilevanza del sistema dei controlli IT nell'ambito del più ampio sistema (complessivo) dei controlli e si ribadisce l'importanza di comprendere il ruolo dell'IT nei processi di rendicontazione.

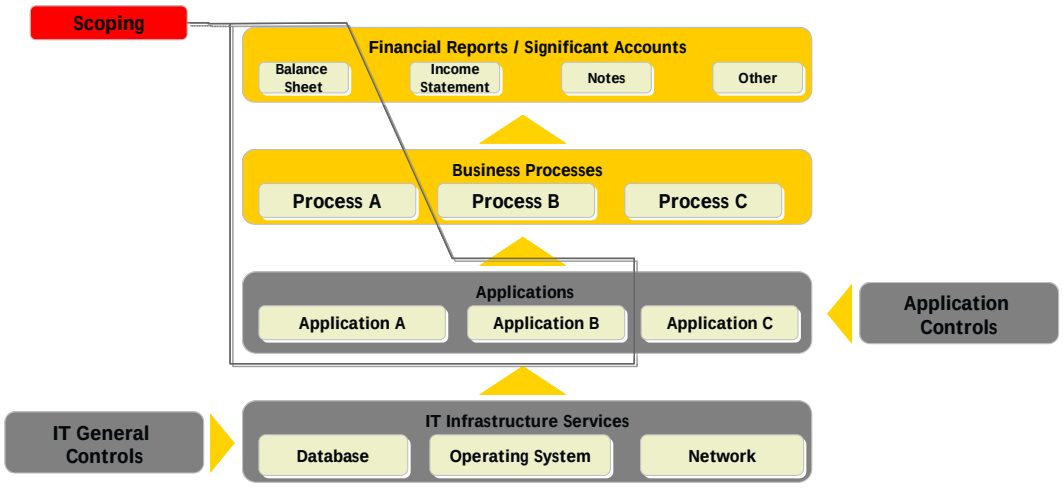
Concretamente, lo Standard n. 2 richiede quattro tipologie di controlli IT che devono necessariamente essere presi in considerazione per il Sarbanes-Oxley Act; esse riguardano:

- modalità di sviluppo dei programmi;
- procedure automatizzate;
- accesso gestione delle modifiche dei programmi;
- ai programmi ed ai dati.

L'allocazione dei controlli specifici – sia oggetti di controllo che attività di controllo - è chiaramente dipendente dalla definizione del perimetro dell'audit (scope) e quest'ultimo viene determinato in seguito alla comprensione del business e dei processi IT ad esso correlati (vedi figura 2).

[7] Il PCAOB (Public Company Accounting Oversight Board), società privata senza scopo di lucro, è stata generata dal Sarbanes-Oxley Act, per sorvegliare i revisori dei conti delle aziende pubbliche e per proteggere gli interessi degli investitori. Emanazione della SEC (l'ente di controllo della borsa statunitense) per la verifica delle società che si occupano della certificazione dei bilanci, la PCAOB è composta di cinque membri, dei quali solo due possono essere revisori contabili di professione, al fine di evitare collusioni e rapporti ambigui nella categoria (www.pcaobus.org).

Figura 2 – Il perimetro dei controlli in ambito sistemi IT – reporting (balance sheet)



Fonte: Obiettivi di controllo per la Sarbanes-Oxley (2008), www.isaca.org

Più in particolare, occorre porre l'attenzione sul fatto che i controlli trovano allocazione, nel contesto aziendale, in almeno tre ambiti diversi:

- direzione generale, con riferimento ai cd. controlli di "entity level" riferiti all'impostazione generale dell'organizzazione (essi riguardano le strategie e i piani, le politiche e le procedure, la valutazione del rischio, la formazione, la qualità e l'audit interno);
- processi di business, dove si individuano i controlli - insiti nelle applicazioni correlate al processo di business – che supportano gli obiettivi di controllo economico e finanziario (sono controlli relativi alla completezza, all'accuratezza, alla creazione e alla trasparenza, generalmente inclusi nella maggioranze delle applicazioni finanziarie utilizzate in azienda);
- IT services, in cui vengono individuati i cd. controlli "IT general" (essi comprendono lo sviluppo di programmi e le eventuali modifiche, le procedure di accesso ai dati e ai programmi e tutto quanto risulti collegato con l'operatività informatica).

La scelta degli oggetti di controllo interno per l'IT nei confronti del financial reporting è stata effettuata tenendo conto del necessario allineamento tra il Sarbanes-Oxley Act, il PCAOB Auditing Standard n.2 e COBIT[8].

[8]SOX fa riferimento sia a controlli generali (entity level) da definirsi a livello di azienda o di organizzazione sia controlli a livello di attività (activity level). La presente trattazione, per motivi di semplicità, si concentra esclusivamente sui secondi. Occorre inoltre rammentare che i controlli di entity level attengono la cultura e lo stile operativo dell'azienda e mal si prestano ad essere esplicitati. In: Obiettivi di controllo IT per la Sarbanes-Oxley, vedi citazioni precedenti.

Si sono individuati 12 processi, 62 oggetti di controllo e 106 attività specifiche di controllo (testing). Nella tabella 1 si evidenzia un riferimento incrociato tra gli obiettivi IT del Sarbanes-Oxley Act e i processi descritti in ambito COBIT.

E' possibile quindi notare che (tralasciando i controlli di entity level):

- i 62 oggetti di controllo, utilizzati per i fini di cui trattasi, sono collocati in 12 processi, a loro volta collocati in due dei quattro domini di COBIT; non vengono considerati, questa sede, i domini relativi a "Pianificazione e Organizzazione" e "Monitoraggio e Valutazione";
- con riferimento al dominio "Acquisizione ed implementazione" si prendono in considerazione 5 dei 6 processi COBIT e 18 oggetti di controllo;
- con riferimento al dominio "Erogazione ed assistenza-supporto" si utilizzano 7 dei 13 processi previsti nel modello COBIT e 44 oggetti di controllo.

Vale la pena ribadire che tutti i controlli presi in esame in questo contesto sono finalizzati al monitoraggio dei sistemi informativi dal momento che è proprio in questo ambiente (costituito da base dati, applicazioni, strumenti tecnologici diversi) che si possono evidenziare i punti di forza e le debolezze che incidono sull'efficacia ed efficienza del data processing.

Si ritiene che gli oggetti così identificati possano costituire una valida guida applicativa per il controlli IT insiti nell'insieme di operazioni, di varia natura, correlate con la produzione della reportistica istituzionale. Ogni attività di controllo dovrebbe essere opportunamente supportata da specifici indicatori di performance, espressi in apposite misure, per consentire il monitoraggio degli andamenti dei controlli. Con riferimento a oggetti di controllo e attività di controllo, in SOX si sottolinea che, in ogni caso, l'elenco fornito non rappresenta che un punto di partenza per eventuali ulteriori percorsi di analisi.

Tabella 1 – COBIT overview – COBIT for SOX – Processi e oggetti di controllo

Plan and Organze	PO.1	Definizione di un piano strategico per l'IT	
	PO.2	Definizione dell'architettura del Sistema Informativo	
	PO.3	Definizione degli indirizzi tecnologici	
	PO.4	Definizione dei processi, dell'organizzazione e delle relazioni dell'IT	
	PO.5	Gestione degli investimenti IT	
	PO.6	Comunicazione degli obiettivi e degli orientamenti della direzione	
	PO.7	Gestione delle risorse umane dell'IT	
	PO.8	Gestione della qualità	
	PO.9	Valutazione e gestione dei rischi informatici	
	PO.10	Gestione dei progetti	
Acquire and Implement	AI.1	Identificazione delle soluzioni informatiche	
	AI.2	Acquisizione e manutenzione dei software applicativi	X
	AI.3	Acquisizione e manutenzione delle infrastrutture tecnologiche	X
	AI.4	Sviluppo e gestione delle procedure	X
	AI.5	Installazione e validazione di soluzioni e cambiamenti	X
	AI.6	Gestione del cambiamento	X
Deliver and Support	DS.1	Definizione e gestione dei livelli di servizio	X
	DS.2	Gestione dei servizi delle parti-terze	X
	DS.3	Gestione delle prestazioni e della capacità produttiva	
	DS.4	Assicurazione sulla continuità di servizio	
	DS.5	Garanzia di sicurezza dei sistemi	X
	DS.6	Identificazione ed attribuzione dei costi	
	DS.7	Formazione e addestramento degli utenti	
	DS.8	Gestione del service desk e degli incidenti	
	DS.9	Gestione delle configurazioni	X
	DS.10	Gestione dei problemi e degli incidenti	X
	DS.11	Gestione dei dati	X
	DS.12	Gestione dell'ambiente fisico	
	DS.13	Gestione delle procedure di sistema	X
Monitor and Evaluate	ME.1	Monitorare e valutare le prestazioni dell'IT	
	ME.2	Monitorare e valutare i controlli interni	
	ME.3	Garantire la conformità ai regolamenti	
	ME.4	Istituzione dell'IT governance	
X = Oggetti di controllo previsti in SOX e loro collocazione in COBIT			

Fonte: Obiettivi di controllo per la Sarbanes-Oxley (2008), www.isaca.org

3. I controlli relativi al dominio "acquisizione ed implementazione"

Con riferimento al dominio "Acquire & Implement" – "AI", che si concentra sulle acquisizioni e sulle implementazioni delle procedure correlate alle nuove applicazioni e/o nuovi sistemi, l'attenzione è focalizzata su 5 dei 6 processi inseriti nella versione originale, in particolare[9]:

- acquisizione e manutenzione dei software applicativi - AI2;
- acquisizione e manutenzione delle infrastrutture tecnologiche - AI3;
- sviluppo e gestione delle procedure - AI4;
- installazione e validazione di soluzioni e cambiamenti - AI5;
- gestione del cambiamento - AI6.

Rientrano in tale dominio anche i controlli relativi al cambiamento e/o al mantenimento di procedure pre-esistenti; il fine è cercare di garantire un corretto ciclo di vita e di sviluppo del software (SDLC)[10].

Nell'impalcatura concettuale esaminata i 18 oggetti di controllo si traducono, a titolo esemplificativo, in 33 specifiche attività di controllo finalizzate al sistematico monitoraggio.

Processo di acquisizione e manutenzione dei software applicativi

I controlli sono effettuati tenendo conto che i processi di acquisizione e di mantenimento del software sono riferiti alla progettazione, all'acquisizione all'eventuale creazione-realizzazione, e allo sviluppo di tutti i sistemi che supportano il raggiungimento degli obiettivi di business.

Gli obiettivi di controllo di tale processo riguardano la coerenza dei sistemi applicativi con l'insieme dei requisiti richiesti al sistema di reporting istituzionale dell'azienda (inizializzazione, registrazione, processing, comunicazione); in altre parole, ci si domanda se effettivamente il software applicativo sia allineato alle esigenze della reportistica istituzionale. Sono previsti 7 oggetti di controllo e 10 attività specifiche di controllo.

Oggetto n.1 - L'azienda usa una metodologia per l'intero ciclo di vita di sviluppo del software ed essa tiene in considerazione i requisiti per la sicurezza e l'integrità del processing.

Attività n. 1/1 - Ottenere una copia della metodologia SDLC dell'organizzazione.

Attività n. 1/2 - Rivedere la metodologia per determinare se, e come, sono gestiti i requisiti in relazione alla sicurezza ed all'integrità del processing.

Attività n. 1/3 – Considerare se sono previste attività specifiche per valutare se tali requisiti sono rispettati lungo l'intero ciclo di sviluppo o acquisizione, cioè se, in particolare, la sicurezza e l'integrità del processing sono presi in

[9]Gli oggetti di controllo e le attività specifiche ivi menzionati sono opportunamente esposti e descritti in: Obiettivi di controllo IT per la Sarbanes-Oxley, vedi citazioni precedenti.
[10]Con l'acronimo SDLC si intende: software system development life cycle.

considerazione durante la fase di definizione dei requisiti della nuova applicazione.

Oggetto n.2 - Le politiche e procedure SDLC aziendali prendono in considerazione lo sviluppo e l'acquisizione dei nuovi sistemi ed i principali cambiamenti ai sistemi esistenti?

Attività n. 2/1 - Rivedere la metodologia SDLC aziendale per determinare se essa considera sia le fasi di acquisizione e sviluppo di nuovi sistemi sia i cambiamenti significativi ai sistemi esistenti.

Oggetto n. 3 - La metodologia SDLC esplicita i requisiti necessari ed i controlli applicativi nel processing delle transazioni affinché quest'ultimo sia completo, accurato, autorizzato e valido?

Attività n. 3/1 - Rivedere la metodologia SDLC aziendale per determinare se essa considera sia le fasi di acquisizione e sviluppo di nuovi sistemi sia i cambiamenti significativi ai sistemi esistenti.

Oggetto n. 4 - L'azienda ha un processo di acquisizione e pianificazione che sia conforme ed allineato rispetto alla strategia generale?

Attività n. 4/1 - Review della metodologia SDLC per determinare se sono prese in considerazione le linee strategiche generali aziendali, attraverso ad esempio, un coinvolgimento dei responsabili IT per rivedere ed approvare i progetti così da garantirne l'allineamento con i requisiti di business strategici (e per verificare che si utilizzino solo nuove tecnologie approvate).

Oggetto n. 5 - Per mantenere un ambiente affidabile, l'IT management coinvolge gli utilizzatori nel design delle applicazioni nella selezione dei software e dei relativi test?

Attività n. 5/1 - Review della metodologia SDLC per determinare se gli utilizzatori sono coinvolti in modo appropriato nel design delle applicazioni, nella selezione dei package software e nel test.

Oggetto n. 6 - Effettuazione di review di post implementazione per verificare che i controlli sono operativi in modo efficace.

Attività n. 6/1 - Determinare se le review di post implementazione sono sviluppate su nuovi sistemi e se i cambiamenti significativi sono riportati e opportunamente valutati.

Oggetto n. 7 - L'azienda acquisisce/sviluppa sistemi software applicativi in accordo con i processi di acquisizione, sviluppo e pianificazione?

Attività n. 7/1 - Selezionare un esempio di progetti che riguardano i sistemi finanziari.

Attività n. 7/2 - Rivedere la documentazione ed i deliverable di questi progetti per determinare se essi sono stati completati in accordo con i processi di acquisizione, sviluppo e planning dei progetti.

Processo di acquisizione e manutenzione delle infrastrutture tecnologiche

E' il processo dedicato alle infrastrutture tecnologiche; l'attenzione è posta alla progettazione, acquisizione e/o realizzazione e gestione dei sistemi correlati alle applicazioni riguardanti la reportistica in oggetto.

In tale processo gli obiettivi di controllo riguardano la coerenza tra l'acquisizione, o la realizzazione, delle infrastrutture tecnologiche (a piattaforme software ed hardware) e le applicazioni del sistema di reporting dell'azienda. Il controllo del processo è dunque finalizzato ad accertare se le infrastrutture vengono acquisite e gestite in modo tale da supportare effettivamente le funzionalità richieste al sistema di reporting.

Nel modello di cui trattasi si prevede un "oggetto di controllo" esplicitato da una singola specifica attività di controllo.

Oggetto n. 8 - Esistono procedure documentate ed esse sono seguite in modo tale che i sistemi infrastrutturali, compresi i network devices ed il software, siano acquisiti sulla base dei requisiti delle applicazioni finanziarie che essi devono supportare?

Attività n. 8/1 – Verificare, eventualmente anche attraverso campionamento, se la documentazione prende in opportuna considerazione i requisiti di infrastruttura nel contesto del processo di acquisizione.

Processo di sviluppo e gestione delle procedure

In questo processo trovano allocazione:

- i controlli relativi al corretto sviluppo o gestione di tutte quelle procedure o politiche necessarie al corretto svolgimento delle attività di acquisizione e manutenzione (service level agreement, prassi operative, training)
- i controlli necessari per assicurare che esistano le documentazioni necessarie al corretto funzionamento delle diverse soluzioni applicative (applicazioni e soluzioni tecnologiche).

Sono previsti due "oggetti di controllo", ciascuno esplicitato da una specifica attività di controllo.

Oggetto n. 9 – Nel contesto delle metodologie SDLC ci sono politiche e procedure che vengono regolarmente aggiornate e revisionate, nonché approvate dal management?

Attività n. 9/1 – Verificare se esistono procedure che descrivono la coerenza del percorso di aggiornamento di tali procedure.

Oggetto n. 10 - L'azienda assicura che i sistemi e le applicazioni siano effettivamente sviluppati in modo coerente con le procedure e le politiche documentate.

Attività n. 10/1 - Selezionare un campione di progetti e determinare se sono stati predisposti i manuali utente (user reference) ed i manuali di supporto, la documentazione di sistema e la documentazione delle procedure.

Processo di installazione e validazione di soluzioni e cambiamenti

In tale ambito i controlli si riferiscono alle fasi di testing e di validazione dei sistemi prima che questi ultimi vengano messi in produzione. Eventuali soluzioni o modificazioni apportate devono essere in grado di supportare coerentemente il

sistema di reporting. Il controllo del processo risulta particolarmente importante poiché la mancanza di test "ante-applicazione" di nuovi sistemi è una delle cause più frequenti di produzione di informazioni non attendibili.

Gli "oggetti di controllo" sono quattro e ciascuno di essi prevede almeno due specifiche attività.

Oggetto n. 11 – È sviluppata ed utilizzata una strategia di test per tutti i cambiamenti significativi nelle applicazioni e infrastrutture tecnologiche che comprende test a livello di unità, sistema, integrazione e accettazione da parte degli utenti così che il deployment dei sistemi operi come previsto?

Attività n. 11/1 - Determinare se è stata predisposta ed utilizzata una strategia formale di testing.

Attività n. 11/2 - Considerare se questa strategia prende in considerazione i rischi potenziali connessi allo sviluppo ed implementazione e gestisce tutte le componenti necessarie per gestire tali rischi (esempio: accuratezza delle interfacce).

Oggetto n. 12 – Il load and stress testing è effettuato in accordo al piano di test e agli standard di testing prestabiliti?

Attività n . 12/1 - Selezionare un campione di progetti di sistema in sviluppo ed in aggiornamento che sono significativi per il reporting istituzionale..

Attività n. 12/2 - Dove sono vitali fattori come capacità e performance rivedere l'approccio al load and stress testing. Considerare se è stato applicato un approccio strutturato adeguatamente modellato in relazione al volume dei dati e che prende in considerazione i tipi di transazione che devono essere processati e l'impatto sulla performance degli altri servizi che devono girare in modo concorrente.

Oggetto n. 13 – Le interfacce con gli altri sistemi devono essere testate per confermare che le trasmissioni dati siano complete, accurate e valide.

Attività n. 13/1 - Determinare se le interfacce con gli altri sistemi sono state effettivamente testate per confermare che i dati trasmessi siano completi cioè che i record, complessivamente considerati, siano accurati e validi.

Attività n. 13/2 - Considerare se l'estensione del testing è sufficiente ed include il recovery nel caso che i dati trasmessi non siano completi.

Oggetto n. 14 – La conversione dei dati è testata all'origine e alla destinazione per confermare che i dati sono completi, accurati e validi?

Attività n. 14/1 – Determinare se la strategia di conversione è stata documentata. Considerare se sono state prese in considerazione strategie per la cancellazione (scrub) dei dati nel vecchio sistema prima della conversione.

Attività n. 14/2 – Rivedere sistematicamente il piano di test della conversione dati.

Processo di gestione del cambiamento

In questo ultimo processo del primo gruppo AI i controlli sono da riferirsi "al come" viene gestito il cambiamento delle funzionalità del sistema, tenendo conto ogni variazione non dovrebbe peggiorare il livello di soddisfacimento degli

obiettivi di reporting istituzionale. I controlli, in questa sede, sono fondamentali per l'attendibilità dell'informazione (si pensi ai casi di modifica nelle classificazioni di bilancio e alle relative attribuzioni).

Gli "oggetti di controllo" di tale processo sono quattro e prevedono dodici attività specifiche.

Oggetto n. 15 – Le richieste di cambiamenti dei programmi dei sistemi e di manutenzione (inclusi i cambiamenti al software di sistema) sono standardizzate, registrate con i log, approvate, documentate e soggette alle procedure formali di change management.

Attività n. 15/1 - Determinare se esiste un processo documentato di change management che è mantenuto per riflettere i processi correnti.

Attività n. 15/2 - Considerare se le procedure di change management esistono per tutti i cambiamenti relativi all'ambiente di produzione, compresi i cambiamenti ai programmi in produzione, la manutenzione dei sistemi ed i cambiamenti alle infrastrutture.

Attività n. 15/3 - Determinare se i cambiamenti di programmi sono sviluppati in un ambiente segregato e controllato. Valutare se le procedure sono disegnate per determinare se solo i cambiamenti autorizzati/approvati sono trasferiti alla produzione.

Oggetto n. 16 – Le richieste di cambiamenti di emergenza sono documentate e soggette alle procedure formali di change management?

Attività n. 16/1 - Determinare se esiste un processo per controllare e supervisionare i cambiamenti in emergenza.

Attività n. 16/2 - Valutare le procedure che assicurano che tutti i cambiamenti in emergenza siano testati e soggetti alle procedure di approvazione standard.

Oggetto n. 17 – Sono posti in essere controlli per limitare la migrazione dei programmi in produzione alle sole persone autorizzate?

Attività n. 17/1 - Valutare le approvazioni richieste prima che il programma sia spostato in produzione.

Attività n. 17/2 - Considerare le approvazioni da parte degli owner del sistema, lo staff di sviluppo ed i responsabili delle procedure di sistema.

Attività n. 17/3 - Confermare che esiste una appropriata relazione tra lo staff responsabile di spostare i programmi in produzione e lo staff di sviluppo.

Attività n. 17/4 - Ottenere le evidenze per convalidare tali asserzioni.

Oggetto n. 18 – L'IT management implementa sistemi software che indeboliscono la sicurezza dei dati e dei programmi che devono essere memorizzati nel sistema?

Attività n. 18/1 - Determinare se il risk assessment del potenziale impatto dei cambiamenti al software di sistema è stato effettuato.

Attività n. 18/2 - Rivedere le procedure per testare i cambiamenti al software di sistema in un ambiente di sviluppo prima che essi siano applicati in produzione.

Attività n. 18/3 - Verificare che le procedure di backout esistano.

4. I controlli relativi al dominio "erogazione ed assistenza-supporto"

Nel dominio "Deliver & Support" – "DS" che si riferisce alle procedure di erogazione dei servizi collegati con le operazioni IT, alla sicurezza e all'assistenza-supporto agli utenti, ci si concentra seguenti processi di controllo interno[11]:

- definizione e gestione dei livelli di servizio - DS1;
- gestione dei servizi delle parti-terze - DS2;
- assicurazione sulla sicurezza dei sistemi - DS5;
- gestione delle configurazioni - DS9;
- gestione dei problemi e degli incidenti - DS8 e DS10;
- gestione dei dati - DS11;
- gestione delle procedure di sistema - DS13.

L'attenzione è focalizzata su 7 dei 13 processi originari di COBIT e i 44 oggetti di controllo sono esplicitati da 73 attività di controllo (inserite in SOX a titolo di esempio).

Processo di definizione e di gestione dei livelli di servizio

In questo processo si parte dall'assunto che efficaci comunicazioni tra la Direzione IT ed i clienti interni - relativamente ai servizi richiesti - sono rese possibili solo attraverso una precisa configurazione e gestione dei livelli dei servizi IT. I controlli dunque riguardano i livelli di servizio e la loro coerenza con i requisiti dei sistemi connessi col reporting istituzionale. I controlli sono altresì riferibili alla misurazione del livello di performance relativo alla qualità dei servizi. Trovano allocazione in questa sede otto "oggetti di controllo".

Obiettivo n. 19 - I livelli di servizio sono definiti e gestiti per supportare i requisiti del sistema di financial reporting.

Attività n. 19/1 - Ottenere un campione dei service level agreement e rivedere gli specifici contenuti dal punto di vista della chiara definizione della descrizione dei servizi e delle aspettative degli utenti.

Attività n. 19/2 – Attivare momenti di confronto tra i responsabili per il service level management e testare l'evidenza per determinare se i service level sono gestiti in maniera coerente.

Attività n. 19/3 - Ottenere e testare l'evidenza che i service level sono gestiti in maniera attiva in accordo con i service level agreement.

Attività n. 19/4 - Discutere con gli utilizzatori se i sistemi di financial reporting sono stati supportati ed erogati in accordo con le loro aspettative ed i service level agreements.

[11]Gli oggetti di controllo e le attività specifiche menzionati nel dominio DS sono opportunamente esposti e descritti in: Obiettivi di controllo IT per la Sarbanes-Oxley, vedi citazioni precedenti.

Obiettivo n. 20 - È definito un framework per stabilire gli indicatori di performance per gestire i service level agreement, sia internamente che esternamente.

Attività n. 20/1 - Ottenere i report relativi alle service level performance e confermare che essi includono indicatori di key performance.

Attività n. 20/2 - Rivedere i risultati di performance, identificare le problematiche di performance e valutare come i service level gestiscono questi temi.

Processo di gestione dei servizi delle parti-terze

I controlli sono, in questo processo, finalizzati ad assicurare sia l'inserimento negli accordi con le terze parti di una chiara definizione dei ruoli, delle responsabilità e delle aspettative sia la revisione ed il monitoraggio di tali accordi quando necessario per garantire la coerenza con l'integrità del processing. Particolare attenzione è data anche alla valutazione dei parametri di performance inseriti in tali contratti. Sono individuabili sei oggetti di controllo.

Obiettivo n. 21 – E' designato un responsabile per il monitoraggio sistematico della coerenza del reporting rispetto degli obiettivi di performance, con attenzione ai servizi delle terze parti.

Attività 21/1 - Determinare se la gestione dei servizi delle terze parti è stato assegnata alle persone appropriate.

Obiettivo n. 22 - Selezione dei vendor per i servizi in outsourcig sviluppati in accordo con le politiche aziendali.

Attività n. 22/1 - Ottenere la politica aziendale di gestione dei vendor e discutere con i responsabili dei servizi delle terze parti se tali standard sono seguiti.

Attività n. 22/2 - Ottenere evidenze, attraverso test specifici, che la selezione dei vendor per i servizi in outsourcing è sviluppata in accordo con la politica aziendale di gestione dei vendor.

Obiettivo n. 23 - L'IT management determina che, prima della selezione, le terze parti potenziali sono qualificate; tale giudizio avviene in modo appropriato attraverso un assessment delle loro capacità di delivery dei servizi richiesti e una review della loro affidabilità finanziaria.

Attività n. 23/1 - Ottenere i criteri ed i business case usati per selezionare i fornitori di servizi di terse parti.

Attività n. 23/2 - Valutare che questi criteri comprendano la considerazione della stabilità finanziaria delle terze parti, skill e conoscenze del sistema sotto gestione e controlli sulla sicurezza e l'integrità del processing.

Obiettivo 24 - I contratti per i servizi delle terze parti prendono in considerazione i rischi, i controlli di sicurezza e le procedure dei sistemi informativi ed i network.

Attività 24/1 - Selezionare un campione di contratti di servizi di terze parti e determinare se essi comprendono controlli per supportare la sicurezza e l'integrità di processing in accordo con le politiche e le procedure dell'azienda.

Obiettivo n. 25 - Esistono e sono seguite procedure che includono requisiti relativi alla stipulazione di contratti formali con le terze parti;

Attività n. 25/1 - Rivedere il campione di contratti per determinare se esiste una definizione sia dei servizi da sviluppare sia delle responsabilità per i controlli sui sistemi di financial reporting.

Obiettivo n. 26 - È effettuata una review regolare della sicurezza e della integrità di processing dei fornitori di servizi di terze parti (usando SAS 70, Canadian 5970 e ISA 402).

Attività n. 26/1 - Indagare se i fornitori di servizi di terze parti effettuano review indipendenti sulla sicurezza e l'integrità del processing (cioè un service auditor report).

Attività n. 26/2 - Ottenere un campione delle review più recenti e determinare se ci sono altre criticità nei controlli che possono avere impatto sul financial reporting.

Processo volto ad assicurare la sicurezza dei sistemi

Sono inseriti, in questo processo, controlli relativi alla necessità di mantenere l'integrità delle informazioni e la protezione dei beni IT. Si tratta di valutare come vengono gestite le attività inerenti la sicurezza del sistema (rientrano in questo ambito anche i controlli sulle prestazioni di sicurezza e i periodici controlli e implementazioni di azioni correttive per identificare punti di debolezza o incidenti di sicurezza). Si elencano 13 oggetti di controllo.

Obiettivo n. 27 - Esiste una politica di sicurezza ed essa è stata approvata dall'appropriato livello dell'executive management.

Attività n. 27/1 - Ottenere una copia delle politiche di sicurezza aziendali e valutarne l'efficacia (SOA evidenzia alcuni punti da prendere in considerazione).

Obiettivo n. 28 - Viene utilizzato un framework per gli standard di sicurezza che supporta gli obiettivi della politica di sicurezza.

Attività n. 28/1 - Ottenere una copia degli standard di sicurezza. Determinare se il framework degli standard garantisce in modo effettivo gli obiettivi della security policy.

Attività n. 28/2 – Considerare, per gli standard di sicurezza, i seguenti punti: organizzazione, ruoli e responsabilità, sicurezza ambiente, sistema operativo, reti, applicazioni e database.

Attività n. 28/3 - Determinare se esistono processi per comunicare e gestire tali standard.

Obiettivo n. 29 - Esiste un IT security plan che è allineato con i piani strategici IT aziendali.

Attività n. 29/1 - Ottenere una copia dei piani di sicurezza o delle strategie per i sistemi di financial reporting ed i relativi sottosistemi e valutare la loro adeguatezza in relazione al piano generale aziendale.

Obiettivo n. 30 - L'IT security plan è aggiornato per riflettere sia cambiamenti significativi nell'ambiente IT sia i requisiti di sicurezza dei sistemi IT specifici.

Attività n. 30/1 - Confermare che il piano di sicurezza riflette i requisiti di sicurezza dei sistemi e sottosistemi di financial reporting.

Obiettivo n. 31 - Esistono e sono osservate procedure per l'autenticazione di tutti gli utilizzatori (interni od esterni) dei sistemi IT per supportare la coerente gestione delle transazioni.

Attività n. 31/1 - Valutare i meccanismi di autenticazione di validazione delle credenziali del sistema di financial reporting, nonché le scadenze delle sessioni.

Attività n. - 31/2 Verificare che non siano stati profili di accesso condivisi tra più utilizzatori.

Processo n. 32 - Esistono e sono osservate procedure per mantenere nel tempo l'efficacia dei meccanismi di autenticazione e di accesso ai sistemi IT (es. cambiamento password).

Attività n. 32/1 - Rivedere le procedure di sicurezza per confermare che i controlli di autenticazione sono usati in modo appropriato e sono soggetti ai requisiti di confidenzialità comunemente in uso.

Obiettivo n. 33 - Esistono e sono osservate procedure in relazione ad azioni tempestive da compiere per richiedere, stabilire, fornire, sospendere e chiudere gli account utente

Attività n. 33/1 - Confermare che le procedure per la registrazione, le modifiche e la cancellazione degli utenti dai sistemi e sottosistemi di financial reporting esistano; rivisitare periodicamente tali conferme.

Attività n. 33/2 - Selezionare un campione di nuovi utilizzatori e determinare se il management ha approvato i loro accessi e se i privilegi accordati sono in accordo con le loro funzioni lavorative.

Attività n. 33/3 - Selezionare un campione di operatori non più in forza all'azienda e determinare se i loro diritti di accesso sono stati rimossi e se ciò è stato fatto in modo tempestivo.

Attività n. 33/4 - Selezionare un campione di utenti con accessi privilegiati e di utenti normali e rivedere i loro diritti di accesso sulla base della loro funzioni lavorative.

Obiettivo n. 34 - Esiste ed è seguito un processo di controllo per effettuare periodicamente una review e confermare i diritti di accesso.

Attività n. 34/1 - Indagare se i controlli di accesso per i sistemi e sottosistemi di financial reporting sono rivisti dal management periodicamente.

Attività n. 34/2 - Valutare l'adeguatezza di come le eccezioni sono riesaminate e se il followup viene svolto in modo tempestivo.

Obiettivo n. 35 - Dove appropriato, esistono controlli per valutare la coerenza dell'inserimento o del ripudio di specifiche transazioni.

Verifica n. 35/1 - Determinare come l'azienda stabilisce precise responsabilità per l'inizializzazione e l'approvazione delle transazioni.

Verifica n. 35/2 - Testare l'uso dei controlli di accountability osservando un utilizzatore che cerca di inserire una transazione non autorizzata.

Verifica n. 35/3 - Ottenere un campione di transazioni ed identificare l'evidenza della accountability o l'origine di ciascuna transazione.

Obiettivo n. 36 - Esistono controlli appropriati, inclusi firewall, intrusion detection e vulnerabilità assessment, per prevenire l'accesso non autorizzato attraverso i network pubblici.

Verifica n. 36/1 - Determinare la efficacia dei controlli di sicurezza perimetrale inclusi i firewall e gli intrusion detection systems.

Verifica n. 36/2 - Indagare se il management ha effettuato un assessment indipendente dei controlli dell'anno precedente (ad esempio attraverso: ethical hacking o social engineering).

Verifica n. 36/3 - Ottenere una copia dell'assessment e rivedere i risultati, in particolare verificare le rivisitazioni dei follow-up in relazione alle debolezze identificate.

Verifica n. 36/4 - Determinare se sono usati sistemi antivirus per proteggere l'integrità e la sicurezza dei sistemi finanziari e dei sottosistemi.

Verifica n. 36/5 - Se appropriato, determinare se tecniche di cifratura sono usate per supportare la riservatezza delle informazioni finanziarie inviate da un sistema all'altro.

Obiettivo n. 37 – Nell'ambito della gestione della sicurezza IT si monitorizzano e si conservano i log delle attività di sicurezza sul sistema operativo

Attività n. 37/1 - Indagare se esiste un responsabile della sicurezza (security office) che monitorizza le vulnerabilità di sicurezza a livello di applicazione/database e le relative possibili minacce.

Obiettivo n. 38 - Esistono e sono in opera controlli relativi all'appropriata segregazione di responsabilità sugli accessi richiesti ed accordati.

Attività n. 38/1 - Rivedere il processo per richiedere ed ottenere i diritti di accesso ai sistemi ed ai dati e confermare queste funzioni non vengano svolte da una stessa persona.

Obiettivo n. 39 - L'accesso alle facility di sistema è ristretto al personale autorizzato e richiede una specifica identificazione ed autorizzazione.

Attività n. 39/1 - Ottenere una copia delle politiche e delle procedure relative alla facility security, key e card reader access e determinare se siano previste account specifici per una la corretta identificazione.

Attività n. 39/2 - Osservare il traffico in entrata ed uscita delle facility security aziendali per stabilire se esiste un controllo sul corretto accesso.

Attività n. 39/3 - Selezionare un campione di utilizzatori e determinare se i loro accessi sono appropriati rispetto alle loro responsabilità lavorative.

Processo di gestione delle configurazioni

I controlli sono finalizzati ad evidenziare come le componenti IT siano ragionevolmente protette da eventuali cambiamenti non autorizzati. Essi attengono inoltre alla sistematica verifica dell'avvenuta registrazione della configurazione corrente. Gli "oggetti di controllo" sono cinque, abbinati ad undici tipologie di attività.

Obiettivo n. 40 - Al personale è permesso di utilizzare solo il software autorizzato e solo per mezzo delle risorse IT aziendali.

Attività n. 40/1 – Determinare se esistono procedure per intercettare e prevenire l'uso di software non autorizzato.

Attività n. 40/2 - Ottenere una review delle politiche aziendali in relazione all'uso del software per verificare se sono chiaramente espresse.

Attività n. 40/1 - Considerare l'opportunità di rivedere un campione delle applicazioni e dei computer per determinare se sono conformi alle politiche aziendali.

Obiettivo n. 41 - Le infrastrutture di sistema sono opportunamente configurati per prevenire accessi non autorizzati.

Attività n. 41/1 - Determinare se le politiche aziendali rendono obbligatoria la documentazione delle configurazioni correnti così come delle configurazioni di sicurezza da implementare.

Attività n. 41/1 Rivedere un campione di server, firewall, router, etc. e valutare se sono stati configurati in accordo con le politiche aziendali.

Obiettivo n. 42 - Il software applicativo ed i sistemi di data storage sono propriamente configurati sulla base della necessità dimostrata di ciascun operatore di visualizzare, aggiungere, modificare e cancellare i dati.

Attività n. 42/1 - Condurre una valutazione della frequenza e della tempistica delle review del management sui record di configurazione.

Attività n. 42/2 - Valutare se il management ha documentato la configurazione delle procedure specifiche.

Attività n. 42/3 - Rivedere un campione dei cambiamenti, delle aggiunte, delle cancellazioni in ambito di configurazione per valutarne appropriatamente le modalità di svolgimento (e valutarne la necessità).

Obiettivo n. 43 - L'IT management ha stabilito procedure per tutta l'azienda per proteggere i sistemi informativi e la tecnologia dai virus informatici.

Attività n. 43/1 - Rivedere le procedure aziendali per intercettare i virus informatici.

Attività n. 43/2 - Verificare che l'azienda abbia installato e abbia in uso software antivirus su tutti i personal computer, stand alone o connessi

Obiettivo n. 44 - Test periodici ed assessment sono effettuati per confermare che il software ed le infrastrutture di network siano configurati in modo appropriato.

Attività n. 44/1 - Rivedere le infrastrutture software e di network per stabilire che siano configurate in modo appropriato e mantenute in conformità ai processi documentati aziendali.

Processo di gestione dei problemi e degli incidenti

Vengono suggeriti, in questa sede, controlli per accertare che i problemi e gli incidenti, sia nel contesto infrastrutturale che nell'ambito dei servizi, vengano gestiti in modo opportuno. Sono previsti tre "oggetti di controllo" e un minimo di sei attività.

Obiettivo n. 45 – L'IT management ha definito ed implementato un sistema di gestione degli incidenti e dei problemi tale che gli incidenti relativi all'integrità dei

dati ed al controllo di accesso siano registrati, analizzati, risolti in modo tempestivo.

Attività n. 45/1 - Determinare se esiste un sistema per la gestione degli incidenti e se le modalità di utilizzo dello stesso sono state formalizzate.

Attività n. 45/2 - Rivedere come il management ha documentato le modalità d'uso del sistema.

Attività n. 45/3 - Rivedere un campione di rapporti di incidenti al fine di considerare se tutte le fasi previste sono state gestite in modo tempestivo.

Obiettivo n. 46 – Il sistema di gestione dei problemi fornisce utilità di audit trail adeguate che permettono il tracciamento di problemi o incidenti per individuarne le cause.

Attività n. 46/1 - Determinare se le procedure aziendali includono strumenti di audit trail e tracking dei problemi e degli incidenti.

Attività n.46/2 - Rivedere un campione dei problemi registrati sul sistema di gestione degli incidenti al fine di considerare se esiste un appropriato audit trail e se è utilizzato.

Obiettivo n. 47 - Esiste un processo di security incident response per supportare in modo tempestivo la risposta e per investigare eventuali attività non autorizzate.

Attività 47/1 - Verificare se le attività non autorizzate sono prese in carico in modo tempestivo e se esiste un processo per supportare le disposizioni da adottare.

Processo di gestione dei dati

Questi controlli riguardano in primo luogo l'identificazione dei fabbisogni informativi, in secondo luogo le modalità di registrazione (es. salvataggi e ripristini), manipolazione e comunicazione dei dati considerando sia gli aggiornamenti che le memorizzazioni. Sono presenti sei "oggetti di controllo".

Obiettivo n. 48 - Esistono politiche e procedure per la distribuzione e conservazione dei dati e il relativo reporting.

Attività n. 48/1 - Rivedere le politiche e le procedure per la distribuzione e la conservazione dei dati del reporting. Valutare l'adeguatezza delle procedure/politiche rispetto alla protezione dei dati.

Attività n. 48/2 - Ottenere e testare le evidenze che i controlli relativi alla protezione dei dati ed alla distribuzione tempestiva dei report finanziari al personale appropriato operano in modo efficace.

Obiettivo n. 49 - Il management protegge le informazioni sensibili – logicamente e fisicamente sia nello storage sia durante la trasmissione – contro l'accesso non autorizzato o la modifica.

Attività n. 49/1 - Rivedere i risultati dei test di sicurezza.

Attività n. 49/2 - Determinare se esistono controlli adeguati per proteggere le informazioni sensibili – logicamente e fisicamente sia nello storage sia durante la trasmissione - contro l'accesso e la modifica non autorizzati.

Obiettivo n. 50 - Il periodo di conservazione ed i termini di storage sono definiti per i documenti, dati, programmi, report e messaggi (in entrata ed uscita), così come per gli elementi (chiavi, certificati) usati per la cifratura e l'autenticazione.

Attività n. 50/1 - Ottenere copia delle procedure di gestione della distribuzione e conservazione dei dati.

Attività n. 50/2 - Trovare conferma che le procedure definiscono i periodi di conservazione e di storage per i documenti, i dati, i programmi, i report ed i messaggi (in entrata ed in uscita), così come per gli elementi (chiavi, certificati) usati per la cifratura e l'autenticazione.

Attività n. 50/3 - Ottenere conferma che i periodi e le modalità di conservazione sono in conformità al SOA (utilizzando anche campioni specifici).

Obiettivo n. 51 - Il management ha implementato una strategia per il back-up ciclico dei dati e dei programmi.

Attività n. 51/1 - Determinare se esistono procedure aziendali per il back up dei dati e dei programmi sulla base dei requisiti sia dell'IT sia degli utilizzatori.

Attività n. 51/2 - Selezionare un campione dei file dei dati e dei programmi e determinare se il loro back up è stato effettuato come richiesto.

Obiettivo n. 52 - Il restore dei dati è periodicamente testato.

Attività n. 52/1 - Verificare che la conservazione e lo storage dei messaggi, documenti, programmi, eccetera, sono stati testati durante l'ultimo anno.

Attività n. 52/2 - Ottenere e rivedere i risultati delle attività di testing.

Attività n. 52/3 - Stabilire se ogni criticità è nota e se è stata riesaminata.

Attività n. 52/4 - Ottenere le politiche per l'accesso in condizioni di sicurezza e discutere con il responsabile se esse seguono gli standard e linee guida anche per il backup dei dati sensibili.

Obiettivo n. 53 - I cambiamenti alle strutture dati sono autorizzati ed effettuati in accordo con i requisiti di progettazione e sono implementati in modo tempestivo.

Attività n. 53/1 - Ottenere un campione dei cambiamenti alle strutture dati e determinare se sono aderenti alle specifiche; chiarire se le strutture modificate sono state implementate nei tempi previsti.

Processo di gestione delle procedure di sistema

In questo processo sono considerate le politiche e le procedure operative per la gestione delle elaborazioni schedulate, la protezione dell'output, il monitoraggio delle infrastrutture e la manutenzione preventiva dell'hardware.

I controlli inseriti in questo ambito mirano a valutare se lo svolgimento dei programmi autorizzati è allineato a quanto programmato: ne consegue che ogni deviazione dal percorso stabilito deve essere identificata, monitorata sistematicamente. Si possono identificare nove "oggetti di controllo" che originano tredici attività (esemplificative) specifiche.

Obiettivo n. 54 - Il management ha stabilito e documentato procedure standard per le operazioni IT (e le segue sistematicamente), inclusi il job

scheduling ed il monitoraggio degli eventi relativi alla sicurezza e alla integrità del processing.

Attività n. 54/1 - Determinare se il management ha documentato le sue procedure per le operazioni IT e se le operazioni sono riviste periodicamente per la compliance.

Attività n. 54/2 - Rivedere un campione di eventi per confermare il corretto funzionamento dei ripristini.

Attività n. 54/3 - Rivedere il processo di job scheduling e le procedure usate per monitorare la completezza dei job.

Obiettivo n. 55 - I dati relativi agli eventi significativi dei sistemi ed i log sono conservati per permettere la ricostruzione dei sistemi e dati processati in caso di necessità.

Attività n. 55/1 - Determinare se sono registrate informazioni cronologiche sufficienti e log per ripristinare, se necessario, l'intero sistema.

Attività n. 55/2 - Ottenere un campione dei log per determinare se permettono la ricostruzione del sistema secondo quanto previsto.

Obiettivo n. 56 - I dati relativi agli eventi significativi dei sistemi sono progettati per fornire una ragionevole assurance sulla completezza e tempestività del sistema e del data processing.

Attività n. 56/1 - Indagare sul tipo di informazioni che è usato dal management per determinare la completezza e tempestività del processing dei dati.

Attività 56/2 - Rivedere un campione dati relativi agli eventi significativi dei sistemi per confermare la completezza e tempestività del processing.

Obiettivo n. 57 - Esistono e sono seguite politiche e procedure per l'end-user computing che riguardano la sicurezza e l'integrità del processing.

Attività n. 57/1 - Ottenere una copia delle politiche e procedure relative all'end-user computing ed avere conferma che esse prevedano controlli per gestire la sicurezza e l'integrità del processing.

Attività n. 57/2 - Selezionare un campione di utilizzatori e verificare che essi conoscano tali politiche.

Obiettivo n. 58 - L'end-user computing, inclusi i fogli elettronici ed altri programmi sviluppati da e per gli utenti, sono documentati e rivisti regolarmente dal punto di vista dell'integrità dei processi comprese le funzionalità di sort, calcolo e reporting .

Attività n. 58/1 - Verificare che il management conosca i piani per l'end-user programme.

Attività n. 58/2 - Verificare la frequenza e gli approcci seguiti per la review dei programmi end-user dal punto di vista dell'integrità del processing e fare una review di un campione per avere conferma dell'efficacia del programma.

Attività n. 58/3 - Rivedere i sistemi user-developed e testare la loro capacità di sort, calcolo e reporting in accordo con le indicazioni del management.

Obiettivo n. 59 – I sistemi sviluppati dagli utenti ed i relativi dati sono regolarmente salvati e le copie sono conservate in un'area sicura.

Attività n. 59/1 - Indagare sulle modalità di back-up dei sistemi end-user anche riguardo al luogo in cui le copie sono conservate.

Obiettivo n. 60 - Sistemi sviluppati direttamente dagli utenti, come fogli elettronici ed altri programmi end-user, sono messi in sicurezza rispetto all'uso non autorizzato.

Attività n. 60/1 - Rivedere le chiavi di sicurezza usate per proteggere i sistemi user-developed contro l'accesso non autorizzato.

Attività n. 60/2 - Osservare uno user che cerchi di accedere in modo non autorizzato ai sistemi userdeveloped.

Attività n. 60/3 - Verificare che il management sia in grado di intercettare accessi non autorizzati ed esaminare le procedure di follow-up usate per valutare l'impatto di tali accessi.

Attività n. 60/1 - Selezionare un campione dei sistemi userdeveloped e determinare chi ne ha accesso (valutando l'appropriatezza di tale accesso).

Obiettivo n. 61 – L'accesso ai sistemi user-developed è ristretto ad un limitato numero di persone.

Attività n. 60/1 - Selezionare un campione dei sistemi userdeveloped e valutare se chi ne ha accesso è effettivamente autorizzato.

Obiettivo n. 62 - Input, processing ed output relativi ai programmi sviluppati direttamente dagli utenti sono verificati in modo indipendente dal punto di vista della completezza e accuratezza.

Attività n. 62/1 - Verificare come il management controlla l'accuratezza e la completezza delle informazioni processate e oggetto di reporting da parte dei sistemi user-developed.

Attività n. 62/2 - Indagare su chi effettua la review ed approva gli output dei sistemi user-developed prima che tali sistemi processino i dati.

Attività n. 62/3 - Rivedere la logica usata nei sistemi userdeveloped ed arrivare ad una conclusione sulla loro capacità di processare in modo completo ed accurato i dati.

5. Alcune considerazioni conclusive

Da quanto detto emerge chiaramente l'elevato livello di responsabilità dei vertici aziendali in tema di controlli interni legati al rapporto che si instaura tra sistemi IT e reportistica istituzionale. In tal senso, il management deve preoccuparsi di garantire il funzionamento del sistema di controllo, valutarne l'efficacia attraverso appositi framework e documentare i risultati utilizzando le procedure identificate.

L'applicazione di un framework così articolato consente, tra l'altro:

- lo svolgimento di una vera e propria attività di risk assessment mediante l'individuazione dei processi rilevanti rispetto agli obiettivi definiti.
- l'assegnazione di specifiche responsabilità in merito al livello di coerenza delle politiche e procedure anche in relazione a particolari programmi sociali quali codici di comportamento e altri;

- la corretta predisposizione dei report economico-finanziari coerenti con quanto previsto dai contesti legislativi in vigore;
- la consapevole gestione del rischio di misstatements collegati a comportamenti erronei o fraudolenti, con riferimento sia agli schemi di bilancio sia alle singole poste in esso contenute;
- di soddisfare, almeno a livello nazionale, i requisiti richiesti dalla legge 262/2005 di trasparenza contabile e di adeguatezza della struttura organizzativa e del sistema dei controlli interni

Occorre tuttavia rammentare che l'effettiva implementazione dei modelli SOX e COBIT comporta un notevole investimento in termini sia di risorse finanziarie sia di impegno manageriale il cui ritorno economico-finanziario è difficilmente valutabile; tale circostanza costituisce indubbiamente un deterrente all'applicazione volontaria in tutte quelle organizzazioni che non sono quotate, o emittenti, sui mercati borsistici statunitensi.

In ultima analisi occorre sottolineare che, in ambito nazionale, i controlli richiesti dalla legge 262/2005 sono meno stringenti rispetto a quelli previsti in ambito SOX per cui sembra poco probabile l'applicazione rigorosa di tale modello. Le aziende che intendono instaurare percorsi virtuosi di controllo interno IT connesso alle procedure contabili e di reporting, ancorché non sottoposte ad obblighi o comunque rientranti nell'ambito di applicazione della legge 262/2005, potranno quindi optare per l'utilizzazione di uno specifico sottoinsieme di oggetti di controllo opportunamente scelto nel contesto del più ampio insieme offerto da COBIT o da SOX[12].

Bibliografia

Brown A., Grant G. (2005), "*In answer to Carr: Reflections on the strategic value of IT*" – 12th European Conference on Information Technology Evaluation, Turku, Finland.

COBIT® e ITIL®; Due framework complementari (2007) - www.innovativeconsulting.it

Dameri R. P., Privitera S. (2009), "*IT governance. Concetti teorici e implementazione* - Franco Angeli, Milano.

Debreceny R., (2006) "*COBIT in Academia*" - COBIT Focus, vol. 1 www.isaca.org

Dizionario dei profili di competenza per le professioni ICT (2009) – www.cnipa.gov.it.

[12]In SOX si legge infatti che: "le aziende più piccole possono trovarsi in difficoltà anche nell'applicare i requisiti del controllo IT che sono richiesti dal Sarbanes-Oxley Act. E' dunque importante non teorizzare una strategia di intervento uguale per tutti ma, invece, usare un approccio risk based ed implementare solo quei controlli IT che sono necessari e rilevanti per il proprio contesto". In: Obiettivi di controllo IT per la Sarbanes-Oxley, vedi citazioni precedenti.

Harley-Davidson – Using COBIT to Simplify Compliance (2006) - COBIT Focus, vol. 2 - www.isaca.org
Heschl J., (2004) "*COBIT in Relation to Other International Standards*" – Information System Control Journal, Vol 4. – www.isaca.org
ITGI Global Survey - An Executive View of IT Governance (2009) – www.itgi.org
Le best practice e gli standard di mercato per l''efficacia, l'efficienza ed il governo dell'IT (2004) – www.adfor.it
Obiettivi di controllo per la Sarbanes-Oxley – Il ruolo dell'IT nella progettazione dei controlli interni rispetto al financial reporting (2006 e 2008), – www.isaca.org
Van Grembergen W., Saull R., De Haes S. (2001), "*Linking the IT BSC to the business objectives at a major canadian financial group"*, Journal of Information Technology and Cases Applications (JITCA), vol.5.
Weill P., Ross M., (2005), "*A Matrixed Approach to Designing IT Governance*" – MIT Sloan Management Review, Winter Vol. 46 n. 2.

Editoria elettronica

Ulteriori informazioni sul modello COBIT e sull'applicazione del Serbanes-Oxley Act sono state reperite sui seguenti siti:

www.coso.org
www.isaca.org
www.isacaroma.it
www.itgi.org
www.sarbanes-oxley.com/
www.sec.gov
www.s-ox.com

Roberto Garelli
Ricercatore confermato in Economia Aziendale
Dipartimento di Tecnica ed Economia delle Aziende
Università degli Studi di Genova
Via Vivaldi, 1
16126 Genova
mail: rgarelli @ economia.unige.it