ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Dipartimento di Informatica
Facoltà di Scienze M.F.N.
Università di Roma "La Sapienza"

COBIT

CASE STUDY

Applicazione Pratica del Framework Cobit 4.1 nel mondo Assicurativo/Bancario

(a cura di – **Marco Tulliani CISA, ISO 27001 LA – Gruppo Sara Assicurazioni**)

Università degli Studi di Roma – Facoltà di Ingegneria
16 febbraio 2008

NOTE SUL RELATORE :

- Ing. Marco Tulliani – CISA, ISO 27001 LA
- Esperienza nell'area IT in aziende di consulenza (Next, Accenture)
- Esperienza nel campo delle Telecomunicazioni (Alenia Marconi System)
- Esperienza nell'ambito dell'IS Audit e Security Management (KPMG)
- Responsabile dell'IS Audit (Gruppo Sara Assicurazioni)

PROBLEMA :

Nel corso degli Audit eseguiti da Revisore Esterno si sono spesso individuate problematiche relative all'implementazione di adeguati controlli in SAP R/3 e l'adozione di un sistema di profilazione, in grado di garantire il corretto rispetto del principio di **Segregazione dei Compiti** all'interno del sistema informativo:

Separazione dei compiti in SAP (Segregation Of Duties)
Assicura che nessuno abbia la possibilità di svolgere più di una delle seguenti funzioni sull'input: generazione, autorizzazione, modifica, verifica o distribuzione

VINCOLI :

Il Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della Legge 19 settembre 2000, n. 300", ha introdotto per la prima volta nel nostro ordinamento la responsabilità in sede penale degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

- Nei lavori di compliance del sistema SAP al decreto lgsl. 231 sono state rilevate aree critiche nei seguenti moduli: acquisti (MM), vendite (SD), tesoreria (TR) e contabilità (FI).
- I punti di debolezza possono essere nel seguito riassunti:
  - Carenza o assenza di adeguati controlli autorizzativi per il processo di purchase order e di credit management
  - Carenza di controlli per il processo treasure
  - Bassa segregazione dei ruoli nella gestione dei processi di business

SOLUZIONE

Premessa: Regola aurea di COBIT

Al fine di fornire le informazioni necessarie alle aziende per conseguire i propri obiettivi, le risorse IT devono essere gestite con un insieme di processi naturalmente raggruppati

In linea con quanto disegnato fin'ora, sono stati identificati quattro ampi domini:

- Pianificazione ed organizzazione
- Acquisizione e realizzazione
- Erogazione e assistenza
- Monitoraggio

SCELTA DEGLI OBIETTIVI DI CONTROLLO

EROGAZIONE ED ASSISTENZA

In questo dominio si fa riferimento alla erogazione dei servizi richiesti, che vanno dalle operazioni tradizionali alla sicurezza e continuità del servizio, alla formazione. Per poter erogare i servizi devono essere creati i necessari processi di supporto.

"Questo dominio include le elaborazioni dei dati da parte dei sistemi applicativi, spesso classificati come controlli delle applicazioni"

SCELTA DEGLI OBIETTIVI DI CONTROLLO

EROGAZIONE ED ASSISTENZA

- DS1 Definire i livelli di servizio
- DS2 Gestire servizi acquistati da terzi
- DS3 Gestire prestazioni e volumi
- DS4 Garantire la continuità del servizio
- **DS5 Garantire la sicurezza dei sistemi**
- DS6 Identificare e attribuire i costi
- DS7 Istruire ed addestrare gli utenti
- DS8 Assistere e dare consulenza ai clienti
- DS9 Gestire la configurazione
- DS10 Gestire le anomalie
- DS11 Gestire i dati
- DS12 Gestire le apparecchiature
- DS13 Gestire il settore

SCELTA DEGLI OBIETTIVI DI CONTROLLO

Erogazione e Assistenza
Garantire la sicurezza dei sistemi

DS5

OBIETTIVI DI CONTROLLO DI ALTO LIVELLO

DS5 Garantire la sicurezza dei sistemi

La necessità di mantenere l'integrità delle informazioni e la protezione dei beni IT richiede un processo di gestione della sicurezza. Questo processo include la definizione e l'aggiornamento dei ruoli e delle responsabilità sulla sicurezza IT, politiche, standard e procedure. La gestione della sicurezza include anche controlli sulle prestazioni di sicurezza e periodici controlli e implementazioni di azioni correttive per identificare punti di debolezza o incidenti di sicurezza. Un'efficace gestione della sicurezza protegge tutti i beni aziendali e minimizza gli impatti aziendali sulle vulnerabilità e sugli incidenti di sicurezza.

SCELTA DEGLI OBIETTIVI DI CONTROLLO DI DETTAGLIO

DS5.4 Gestione degli identificativi utenti.

Assicurare che la richiesta, definizione, rilascio, sospensione, modifica e revoca degli identificativi utente ed i relativi privilegi siano indirizzati dalla Direzione degli identificativi utente. Dovrebbe essere inclusa una delineata procedura di approvazione e concessione dei privilegi di accesso al proprietario dei dati o sistemi. Questa procedura dovrebbe essere applicata per tutti gli utenti, inclusi gli amministratori (utenti privilegiati), utenti interni ed esterni sia per i casi normali che di emergenza. Diritti e obblighi relativi agli accessi alle informazioni e ai sistemi aziendali sono stabiliti contrattualmente per tutti i tipi di utente. Eseguire una regolare revisione di tutti gli identificativi ed i relativi privilegi.

DS5 Garantire la sicurezza dei sistemi

Da	Inputs
PO2	Architettura delle informazioni; classificazione assegnata ai dati
PO3	Standard tecnologici
PO9	Valutazione dei rischi
AI2	Specifiche su controlli di sicurezza alle applicazioni
DS1	OLAs

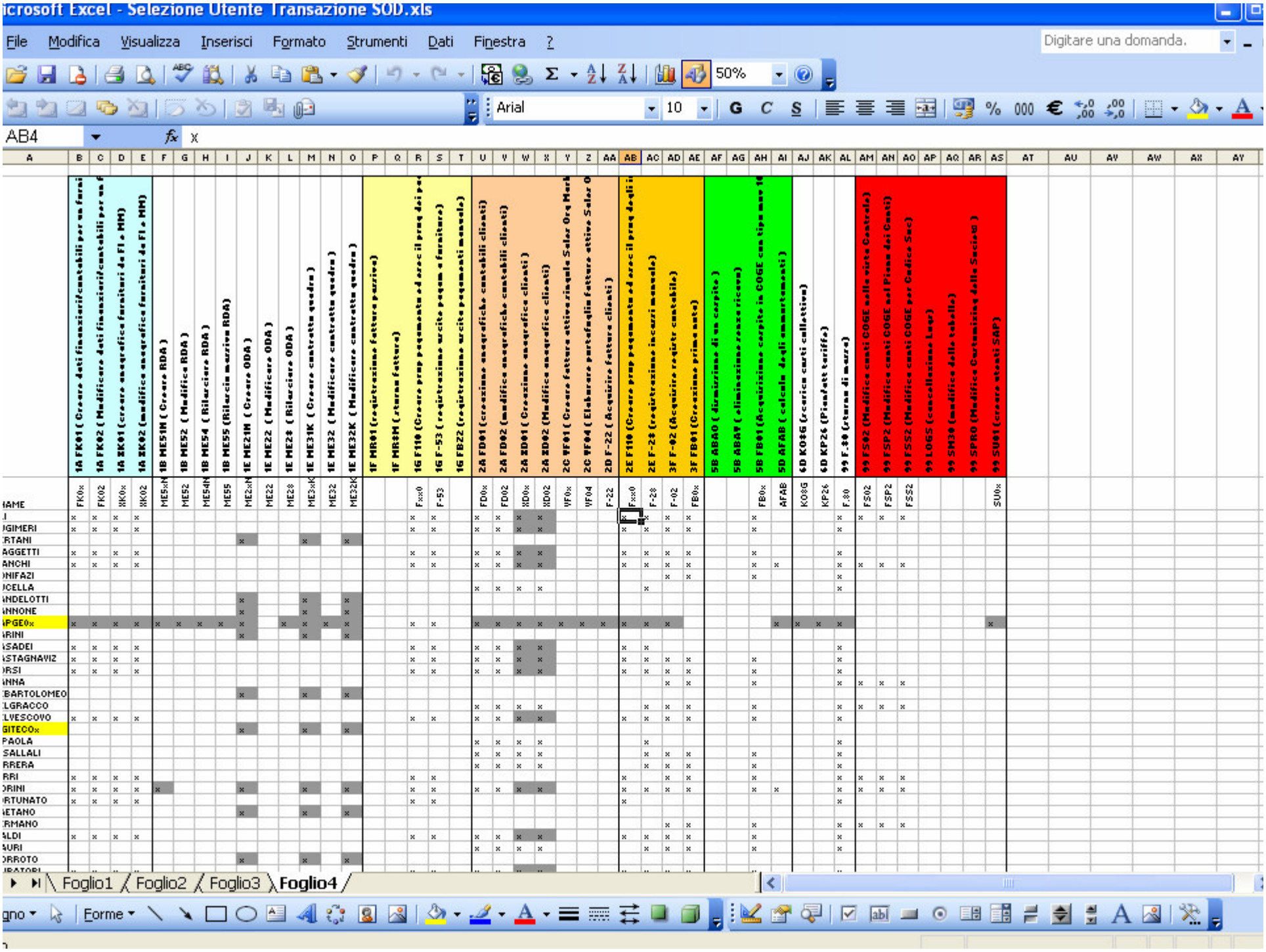
Outputs	a
Definizione degli incidenti di sicurezza	DS8
Richieste di addestramento specifico sulla consapevolezza della sicurezza	DS7
Relazione sulle prestazioni dei sistemi	ME1
Cambiamenti ai requisiti di sicurezza	AI6
Minacce e vulnerabilità alla sicurezza	PO9

RACI Chart — **Ruoli**

Attività	AD	Direttore Finanziario	Direttore Commerciale	Direttore IT	Responsabili di Settore	Direttore Operativo	Responsabile Architetture IT	Responsabile Sviluppo	Responsabile Amministrazione IT	PMO	Conformità, Audit, Gestione del Rischio e Sicurezza
Definire e aggiornare un piano di sicurezza IT		I	C	C	A	C	C	C	C	I	I
Definire, stabilire e rendere operativo un processo di gestione degli identificativi (account)				I	A	C	R	R	I		
Monitorare i potenziali e reali incidenti sulla sicurezza					A	I	R	C	C		
Periodicamente revisionare e convalidare i diritti di accesso e i privilegi degli utenti					I	A	C				
Definire e aggiornare una procedura per gestire e salvaguardare le chiavi crittografiche					A		R			I	
Implementare e aggiornare le tecniche e i controlli procedurali per proteggere il flusso di informazioni attraverso la rete					A	C	C	R	R		
Condurre una regolare valutazione delle vulnerabilità			I		A	I	C	C	C		

La RACI Chart identifica chi è Responsabile, Addetto, Consultato e/o Informato (vedi nota in Appendice IX)

Table\version	<= 3.1	4.0	4.5	4.6A/4.6B	>=4.6C
AGR_1016	-	-	X	X	X
AGR_1251	-	-	X	X	X
AGR_1252	-	-	X	X	X
AGR_AGRS	-	-	-	X	X
AGR_DEFINE	-	-	X	X	X
AGR_PROF	-	-	X	X	X
AGR_TCODES	-	-	X	X	X
AGR_TEXTS	-	-	X	X	X
AGR_USERS	-	-	X	X	X
PAT03	-	X	X	X	X
T000	X	X	X	X	X
TOBJT	X	X	X	X	X
TSTCT	X	X	X	X	X
USORG	X	X	X	X	X
USR02	X	X	X	X	X
USR03	X	-	-	-	-
USR11	X	X	X	X	X
USR40	X	X	X	X	X
USR41_MLD	-	-	-	-	X
USREFUS	-	-	-	-	X
UST04	X	X	X	X	X
UST10C	X	X	X	X	X
UST10S	X	X	X	X	X
UST12	X	X	X	X	X
USVART	X	X	X	X	X
V_USERNAME	-	X	-	-	-
V_USR_NAME	-	-	X	X	X


icrosoft Excel - Selezione Utente Transazione SOD.xls
File Modifica Visualizza Inserisci Formato Strumenti Dati Finestra ?
Digitare una domanda.
50%
Arial
10
AB4
1A FK01 (Creare dati finanziari/contabili per un forni
1A FK02 (Modificare dati finanziari/contabili per un f
1A EK01 (creare anagrafica fornitori da FI e MM)
1A EK02 (modifica anagrafica fornitori da FI e MM)
1B ME51M (Creare RDA)
1B ME52 (Modifica RDA)
1B ME54 (Rilasciare RDA)
1B ME55 (Rilascia manive RDA)
1E ME21M (Creare ODA)
1E ME22 (Modificare ODA)
1E ME23 (Rilasciare ODA)
1E ME31K (Creare contratto quadro)
1E ME32 (Modificare contratto quadro)
1E ME32K (Modificare contratto quadro)
1F MR01 (registrazione fattura passiva)
1F MR1M (storno fattura)
1G F110 (Creare prop pagamento d'acc il prog dei pa
1G F-53 (registrazione uscite pagam. effettuate)
1G FB22 (registrazione uscite pagamenti manuale)
2A FD01 (creazione anagrafiche contabili clienti)
2A FD02 (modifica anagrafiche contabili clienti)
2A XD01 (Creazione anagrafica clienti)
2A XD02 (Modifica anagrafica clienti)
2C VF01 (Creare fatture attive/cinquale Solar Org Mark
2C VF04 (Elaborare portafoglio fatture attive Solar O
2D F-22 (Acquisire fatture clienti)
2E F110 (Creare prop pagamento d'acc il prog degli i
2E F-28 (registrazione incassi manuale)
3F F-02 (Acquisire registr contabile)
3F FB01 (Creazione prima nota)
5B ABA0 (diminuzione di un carpite)
5B ABAV (eliminazione resse riceve)
5B FB01 (Acquisizione carpite in COGE con tipo mov 1
5D AFAB (calcolo degli ammortamenti)
6D K086 (carica carti collettive)
6D KP26 (Pianfatt tariffe)
99 F.80 (storno di massa)
99 FS02 (Modifica conti COGE nella vista Centrale)
99 FSP2 (Modifica conti COGE nel Piano dei Conti)
99 FSS2 (Modifica conti COGE per Codice Soc)
99 LOGS (cancellazione Logs)
99 SM30 (modifica della tabella)
99 SPRO (Modifica Customizing della Società)
99 SU01 (creare utenti SAP)
NAME
FK0x FK02 XK0x XK02 ME5x ME52 ME54 ME55 ME2x ME22 ME28 ME3x ME32 ME32K F-xx F-53 FD0x FD02 XD0x XD02 VF0x VF04 F-22 F-xx F-28 F-02 FB0x AFAB K086 KP26 F.80 FS02 FSP2 FSS2 SU0x
Foglio1 Foglio2 Foglio3 Foglio4
Forme

PROBLEMA :

Un'altra area di particolare interesse e su cui è possibile trovare dei problemi è quella relativa Data Quality/Integrity Controls.

L'area consiste nella valutazione, progettazione e implementazione dei controlli sulla qualità/integrità dei dati associati ai controlli sulle procedure di interfaccia da/verso gli altri sistemi e alle procedure di data conversion:

- Controlli sulla pulizia dei dati iniziali
- Controlli sui master data e sulle tabelle
- Controlli sulle parametrizzazioni
- Controlli di validazione e riconciliazione delle procedure di interfaccia da/verso altri sistemi
- Audit Trails delle procedure di Interfaccia
- Controlli di validazione e riconciliazione delle procedure di conversione dei dati
- Audit Trails delle procedure di conversione dei dati

Altri Controlli

- **Controllo di sequenza**

  I numeri di controllo si incrementano sequenzialmente e qualsiasi numero che risulti fuori sequenza o duplicato viene scartato o segnalato su un tabulato di eccezioni per le successive attività di verifica

- **Controllo di validità**

  Controlli programmati di validità dei dati in conformità a predeterminati criteri. Per esempio, un record del cedolino stipendi contiene un campo riguardante lo stato civile. Vengono acettati solo valori C/N e S. Se vengono incontrati altri valori, si dovrebbe scartare il record stesso

- **Controllo di esistenza**

  I dati sono correttamente introdotti e confrontati con criteri predeterminati validi. Per esempio, un codice di transazione valido viene introdotto nel campo codice di transazione

- **Controllo di completezza**

  Si esegue un controllo su ciascun byte di un dato campo per determinare che contenga valori significativi e non spazi o zeri

- **Controllo di duplicazione**

  Le nuove transazioni vengono confrontate con quelle già immesse per assicurare che non siano state già registrate

- **Controllo logico di relazione**

  Se una particolare condizione è vera allora anche una o più condizioni aggiuntive o relazioni di dati di input devono essere vere per considerare il dato valido

VINCOLI :

Legge 28 Dicembre 2005, n.262

"Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari"

(Art 14 che ha modificato l'articolo 154-bis del TUF)

Pubblicata dalla Gazzetta Ufficiale n.301 del 28 Dicembre 2005 – Supplemento ordinario n.208

Procedure Amministrativo Contabili

•Il fulcro delle innovazioni proposto dalla legge riguarda la predisposizione di "adeguate procedure amministrativo contabili per la formazione del bilancio…."

•In tale contesto, gli assetti aziendali e le procedure si configurano come la più rilevante esplicitazione del dovere di corretta amministrazione.

•Con l'espressione "Procedure Amministrativo Contabili" ci si riferisce:

- Ai processi di raccolta, elaborazione e distribuzione delle informazioni economiche finanziarie;
- Ai Sistemi Informativi inerenti l'acquisizione e lavorazione dei dati contabili;
- Alla valutazione delle attività e passività;
- In generale, a tutte le attività capaci di influire, positivamente o negativamente, sulla correttezza dei dati e quindi alla predisposizione dei bilanci e degli altri atti e comunicazioni finanziarie.

SCELTA DEGLI OBIETTIVI DI CONTROLLO

EROGAZIONE ED ASSISTENZA

- DS1 Definire i livelli di servizio
- DS2 Gestire servizi acquistati da terzi
- DS3 Gestire prestazioni e volumi
- DS4 Garantire la continuità del servizio
- DS5 Garantire la sicurezza dei sistemi
- DS6 Identificare e attribuire i costi
- DS7 Istruire ed addestrare gli utenti
- DS8 Assistere e dare consulenza ai clienti
- DS9 Gestire la configurazione
- DS10 Gestire le anomalie
- **DS11 Gestire i dati**
- DS12 Gestire le apparecchiature
- DS13 Gestire il settore

SCELTA DEGLI OBIETTIVI DI CONTROLLO

Erogazione e Assistenza
Gestione dei dati
DS11

OBIETTIVI DI CONTROLLO DI ALTO LIVELLO

DS11 Gestione dei dati

Una gestione efficace dei dati richiede l'identificazione dei fabbisogni informativi. Il processo di gestione dei dati include lo stabilire procedure efficaci per gestire la librerie dei supporti di memorizzazione, il salvataggio e il ripristino dei dati ed un'appropriata eliminazione dei supporti di memorizzazione. Un efficace processo di gestione dei dati aiuta ad assicurare la qualità, tempestività e disponibilità dei dati di business.

SCELTA DEGLI OBIETTIVI DI CONTROLLO DI DETTAGLIO

DS11.1 Fabbisogni di business per la gestione dei dati

Stabilire modalità operative per assicurare che siano ricevuti dal business i documenti originari corretti, che tutti i dati ricevuti dal business siano elaborati, che tutti gli output richiesti dal business siano preparati e distribuiti e che i fabbisogni di ripartenza e rielaborazione siano supportati.

LINEE GUIDA PER LA GESTIONE

DS11 Gestione dei dati

Da	Inputs
PO2	Dizionario dei dati; classificazione dei dati definita
AI4	Manuali utente, operativi, di supporto tecnici e amministrativi
DS1	OLA
DS4	Piano di memorizzazione e protezione dei salvataggi

Outputs	a						
Rapporti di performance dei processi	ME1						
Istruzioni per l'operatore per la gestione dati	DS13						

RACI Chart — **Ruoli**

Attività	AD	Direttore Finanziario	Direttore Commerciale	Direttore IT	Responsabili di Settore	Direttore Operativo	Responsabile Architetture IT	Responsabile Sviluppo	Responsabile Amministrazione IT	PMO	Conformità, Audit Gestione del Rischio e Sicurezza
Tradurre i fabbisogni di memorizzazione e conservazione dei dati in procedure					A	I	C	R			
Definire, aggiornare e implementare procedure per gestire la libreria dei supporti					A		R	C	C	I	
Definire, aggiornare e implementare procedure per rendere sicura l'eliminazione di supporti e dei dispositivi					A	C	R			I	
Salvare i dati secondo lo schema					A		R				
Definire, aggiornare e implementare procedure per il ripristino dei dati					A	C	R	C	C		

La RACI Chart identifica chi è Responsabile, Addetto, Consultato e/o Informato (vedi nota in Appendice IX)

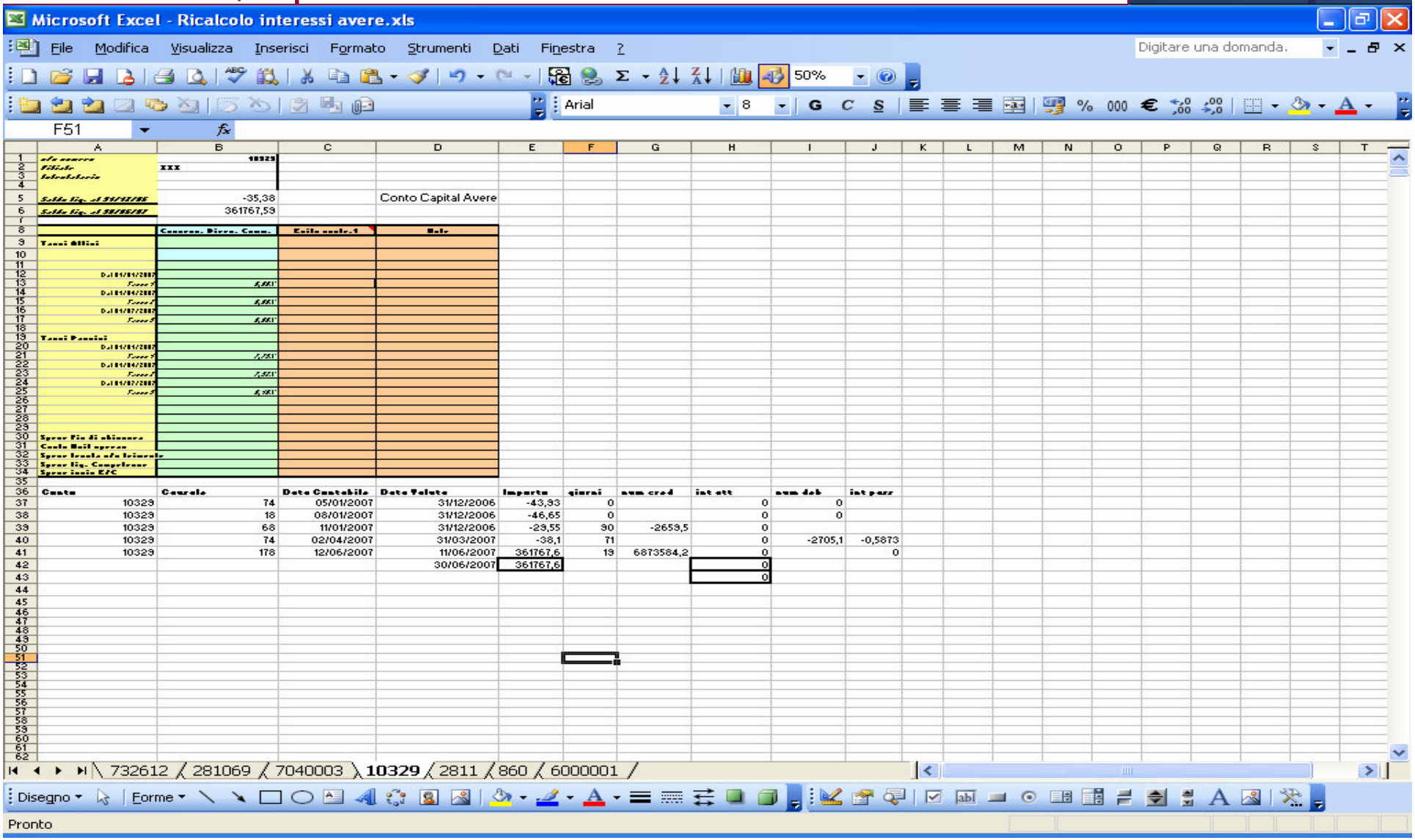
Controllo sulla corretta liquidazione degli interessi sui conti correnti fruttiferi

1. il controllo dei saldi per valuta: per ogni conto deve essere verificato che partendo dal saldo al 31 dicembre 200X, sulla base dei singoli movimento del semestre, devono essere corretti alle singole date, i singoli saldi e che fosse infine corretto il saldo del 30 giugno 2007;

2. la determinazione dei "*giorni*": per ogni conto, sulla base dei singoli movimenti, devono essere ricalcolati il totale dei giorni per i quali un singolo conto ha mantenuto un determinato saldo per valuta. Tale dato è la base per il conteggio degli interessi.

3. la determinazione dei "*numeri*" (creditori/debitori): tale dato è stato ottenuto moltiplicando i singoli saldi per valuta per il numero dei "giorni" precedentemente ricalcolati;

4. la determinazione degli interessi (creditori /debitori) in base alle condizioni applicate: per ogni tipologia di conto è stato riperformato il calcolo degli interessi (prodotto numeri -creditori o debitori- per tasso). I tassi sono stati estratti dal sistema che gestisce le condizioni dei conti (Tassi e decorrenze) per appurare che il ricalcolo delle competenze fosse eseguito in modo corretto in funzione anche delle Deroghe e delle promozioni correnti.



Conto	Causale	Data Contabile	Data Valuta	Importo	giorni	num cred	int att	num deb	int pass
10329	74	05/01/2007	31/12/2006	-43,93	0		0	0	
10329	18	08/01/2007	31/12/2006	-46,65	0		0	0	
10329	68	11/01/2007	31/12/2006	-29,55	90	-2659,5	0		
10329	74	02/04/2007	31/03/2007	-38,1	71		0	-2705,1	-0,5873
10329	178	12/06/2007	11/06/2007	361767,6	19	6873584,2	0		0
			30/06/2007	361767,6			0		
							0		

Microsoft Excel - Ricalcolo interessi avere.xls

File Modifica Visualizza Inserisci Formato Strumenti Dati Finestra ?

Digitare una domanda.

50%

Arial 8

G22

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1		2811															
2	*Filiale*	xxx															
3	*Intestatario*																
4																	
5	*Saldo fin. al 31/12/05*	42540,16		Conto Value Avere													
6	*Saldo fin. al 30/06/07*	311086,6															
7																	
8		Canone Di	Esito conto-1	Note													
9	Tassi Attivi																
10																	
11																	
12	Dal 01/01/2007																
13	Fino a	4,25%															
14	Dal 01/04/2007																
15	Fino a	4,25%		Proroga													
16	Dal 01/07/2007																
17	Fino a	4,50%		Proroga													
18	dal 01/10/2007	4,50%															
19	Tassi Passivi																
20	Dal 01/01/2007																
21	Fino a	4,25%															
22	Dal 01/04/2007																
23	Fino a	4,50%															
24	Dal 01/07/2007																
25	Fino a	4,50%															
26																	
27																	
28																	
29																	
30	Spese Fin di chiusura																
31	Costo Bail spread																
32	Spese Iscrizione Trimestrale																
33	Spese liq. Competenze																
34	Spese invio E/C																
35																	
36																	
37																	
38																	
39	Conto	Causale	Data Contabil	Data Valuta	Importo	giorni	num cred	int att	num deb	int pass							
150	2811	34	05/04/2007	05/04/2007	295860	8	2366880	176,705									
151	2811	27	16/04/2007	13/04/2007	306015	3	918045	68,539									
152	2811	152	27/04/2007	16/04/2007	305756	10	3057557	228,27									
153	2811	26	26/04/2007	26/04/2007	300756	1	300756	22,4537									
154	2811	48	23/04/2007	27/04/2007	302245	0	0	0									
155	2811	34	27/04/2007	27/04/2007	302456	18	5444202	406,451									
156	2811	27	16/05/2007	15/05/2007	312612	0	0	0									
157	2811	152	23/05/2007	15/05/2007	311970	0	0	0									
158	2811	152	23/05/2007	15/05/2007	311271	20	6225415	464,774									
159	2811	26	05/06/2007	05/06/2007	308767	7	2161367	161,362									
160	2811	13	13/06/2007	12/06/2007	306467	3	919400	68,6402									
161	2811	27	14/06/2007	15/06/2007	316623	0	0	0									
162	2811	152	25/06/2007	15/06/2007	316390	0	0	0									
163	2811	152	25/06/2007	15/06/2007	311087	15	4666239	348,374									
164				30/06/2007	311087			2220,37									
165					ok			2268,17									
166																	
167																	
168																	

732612 / 281069 / 7040003 / 10329 / **2811** / 860 / 6000001 /

Disegno Forme

Pronto

Sitografia

- www.aiiaweb.it
- www.isaca.org
- www.coso.org

Riferimenti

marco.tulliani@tin.it