L’approccio metodologico per l’analisi dei profili di accesso in ambiente SAP

VERONA

25 – 26 Maggio 2006

Agenda

- **Evoluzione di Sap in Poste Italiane**

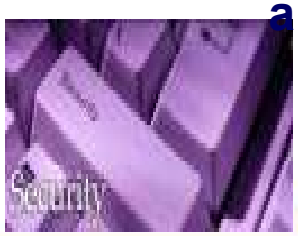
- **Logiche autorizzative e processo di costruzione di un profilo in ottica SOD (Segregation of Duties)**

- **Cause che hanno portato alla costruzione di profili non allineati**

- **Come si procede in questi casi:**

✓ *Analisi dei parametri di sistema che impattano sulla SOD*
✓ *Analisi delle utenze ad elevato rischio*
✓ *Analisi dei profili in ottica SOD attraverso l'analisi della reale operatività degli utenti*

- **Adozione di contromisure per la mitigazione dei rischi a breve e a medio termine e costruzione di un sistema di monitoraggio**



Sistemi SAP in Poste Italiane

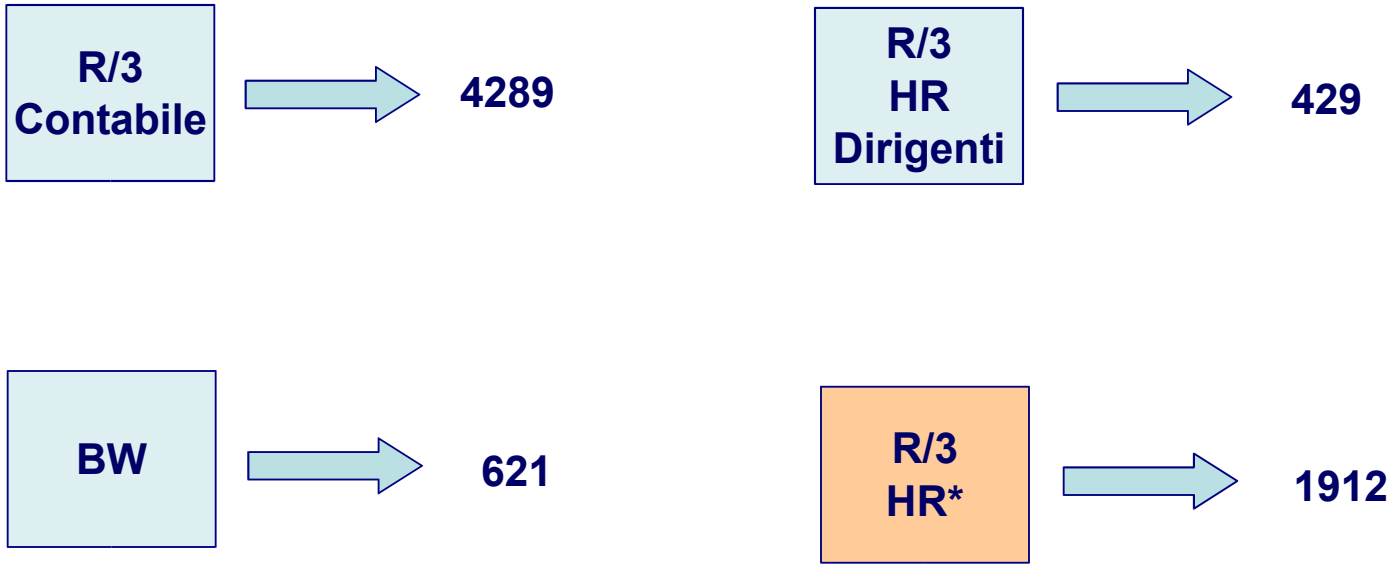
- **Il primo sistema SAP è andato in produzione nel 1998 con i moduli MM, FI e CO**
- **Oggi sono attivi i seguenti sistemi:**

R/3 Contabile	Contabilità Generale(FI) Ciclo Attivo (FI-CA) Ciclo Passivo (MM) Immobili (RE) Controllo di Gestione (CO) Vendita (SD) Tesoreria (TR)
BW	Datawarehouse aziendale.
R/3 Logistico	Rendicontazione approvvigionamento stampati e materiali di consumo negli UP.
R/3 Carrelli	Tracciatura dei carrelli che contengono la corrispondenza.
R/3 HR Dirigenti	Gestione personale dirigente
SRM	Elaborazione del processo acquisti
CRM	Gestione dei rapporti con il cliente
R/3 Carte Valori	Gestione delle carte valori postali
R/3 Poste Shop	Gestione delle vendite PT Shop
R/3 HR*	Anagrafica del personale, rilevamento presenze

* In outsourcing

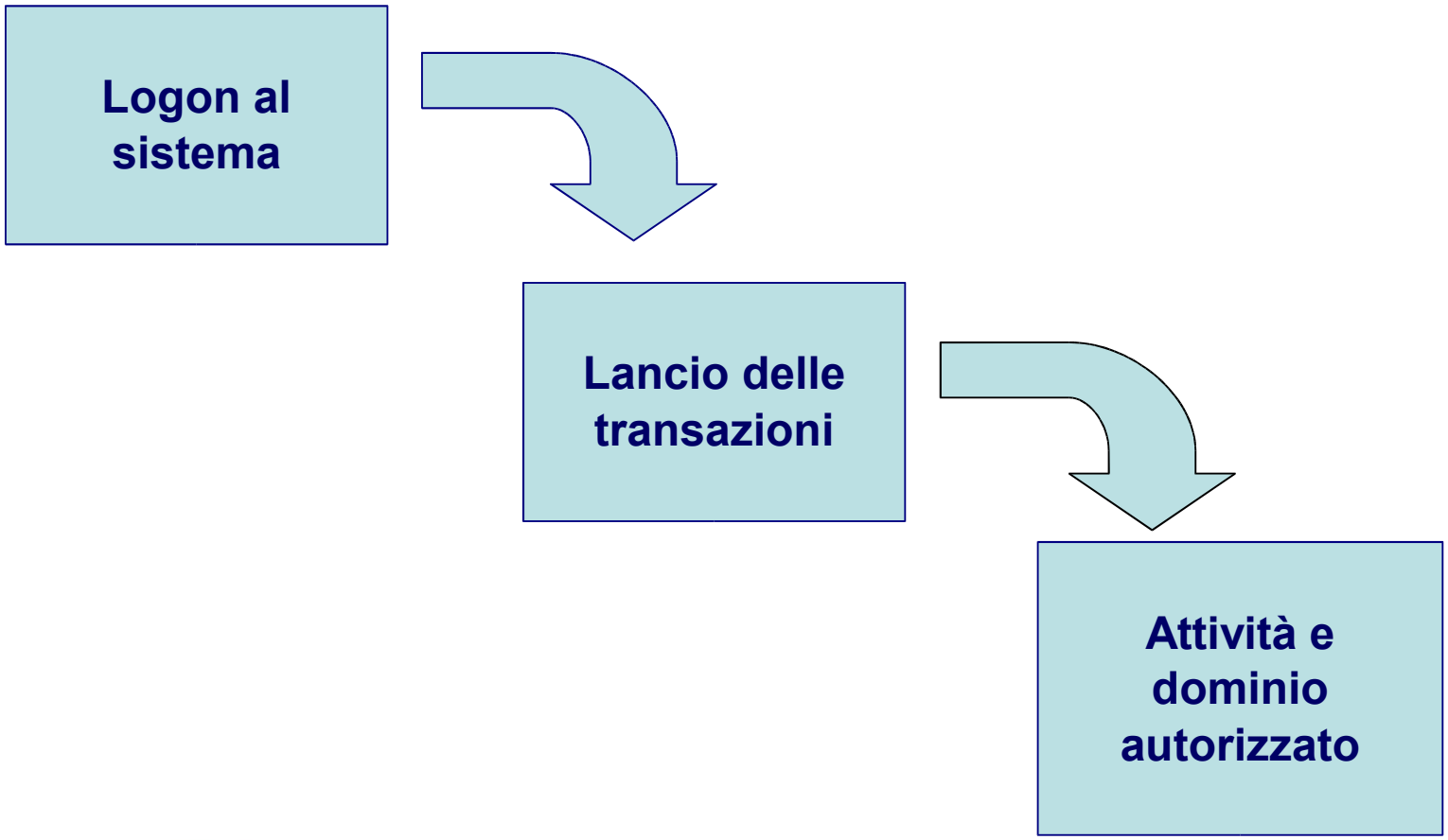
Sistemi SAP in Poste Italiane

- **Numero di utenze presenti sui principali sistemi**



* In outsourcing

Come si accede a SAP?



Segregation of Duties

Processo di costruzione dei profili in ottica di SOD

Authorization Profile Administrator

disegna la struttura dei profili autorizzativi,conoscendo bene i processi aziendali

Authorization data administrator

avendo skill prettamente tecnico, implementa la struttura autorizzativa sul sistema

User Administration

assegna le autorizzazioni e gestisce l'anagrafica degli utenti

Principali motivazioni per cui ciò non avviene:

- presenza di esiguo numero di risorse skill specifici
- spostamenti personale
- riorganizzazioni aziendali
- Implementazione di nuove funzionalità nei moduli SAP già attivi
- Attivazione di nuovi moduli

Rischio:

- profili non allineati al principio della separazione
- profili creati intorno alla persona e non al task

Attività di Audit

Come affrontare il processo di Audit in questi casi?

E' necessario adottare un approccio per step:

- **Verificando dei parametri di sistema che incidono sulla SOD**
- **Rilevando la presenza di utenze ad elevato rischio**
- **Analizzando le attività svolte da un gruppo di utenti in un certo arco temporale**

Parametro di sistema

Verificare dalla tabella RSPARAM :

- **la possibilità di cancellazione e riattivazione automatica, con password nota, della super utenza SAP***

Presenza di utenze ad elevato rischio

- presenza di utenze con privilegi troppi ampi SAP ALL e SAP NEW
- utenze create e mai utilizzate con password nota
- utenze anonime non facilmente riconducibili ad un responsabile
- utenze di “tipologia” non adeguata

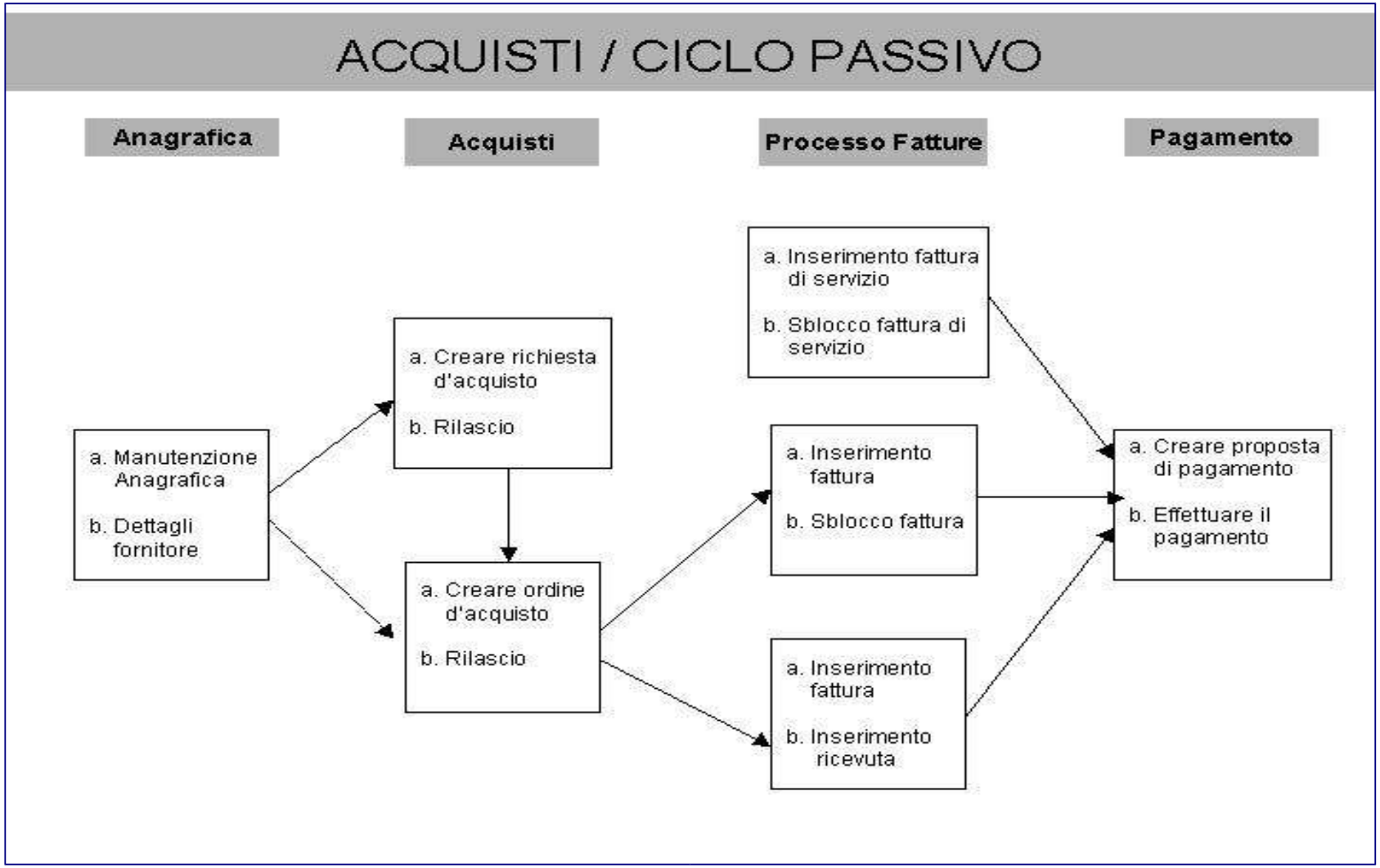
SAP permette la configurazioni delle seguenti tipologie di utenze:

- A = dialog , per l’accesso diretto al sistema
- B = di sistema, consente la comunicazione all’interno del sistema
- C= comunication, consente la comunicazione tra sistemi
- S= utenze di servizio

Analisi dei profili in ottica SOD

- **Si parte da un modello condiviso di separazione di ruoli e funzioni**
- **Si associano ad ogni attività le relative transazioni**
- **Si costruisce, sulla base delle reali attività svolte in un arco temporale, una matrice utente / transazioni lanciate**

Esempio Modello Organizzativo Separazione Ruoli Funzioni



Esempio Matrice Transazioni Processo Ciclo Passivo

		Manutenzione Anagrafiche											Creaz./Rilascio RDA						Creaz./Rilascio ODA						E/M - E/F												Reg. Pagamenti			
		Crea Materiale	Cambia materiale	Blocc/Sblocc Anagraf Fornit	Modif Blocc/Sblocc anag forn	Creare Anagraf Fornitì	Modif Anagraf Fornit	Creare Anagraf Fornit	Modific Anagraf Fornit	Blocc/Sblocc Anagraf Fornit	Cancellare Anagraf Fornit		Creare RDA	Creare RDA	Modifica RDA	Modifica RDA	Rilascia RDA	Rilascio collettivo di RDA	Creare ODA Forn Sconosciuto	Creare ODA	Modifica ODA	Modifica ODA	Creare ODA Forni.Sconosciuto	Rilascia ODA	E/M da ODA	E/M senza ODA	Entrata Merci	Stornare Entrata Merci	Acquisire Fattura Fornitori	Registra Fattura	Acquisire fattura in entrata	Acquisire fattura in entrata	Rilascia Fattura	Cancella Fattura	Rilasciare Fattura Bloccata	Modif Fattura	Registrare Uscita di Pag.	Creare parametri per il pag aut	Creare Parametri per il pag.	Creare Parametri per il pag.
	ACCOUNT	MM01	MM02	FK05	SM01	MK01	MK02	XK01	XK02	XK05	XK06		ME51	ME51N	ME52	ME52N	ME54	ME55	ME21	ME21N	ME22	ME22N	ME25	ME28	MB01	MB0A	MIGO	MBST	F-43	MRHR	MIRO	MR01	MR02	MR08	MRBR	FB02	F-07	F110	F111	F-28
2														6		4				6		3		6			6			6				2	4				
1																																			2				
1																																			1				
2														7		4			4	6	1	4		6			6			6									
3														2						3				3			3		2	6				4	4		2		
2														6	1	4				6		6		6			6			1									
1																					2																		
1																																			1				
1																																			1				
2														6		4				6	3	3		6			6		1								6			
2						6	6						1	9	1	4								1			6												
2														6		2				6		3	1	6			6												
2														6		2				6				6			6				6								
3														6	2	4				6	2	6		6			6		2		6			2			2		
1																																			1				
2														9		6				6		3		6			6		1										
4										2	2			1							2			3			3		2	1	6			2	4	2	2		
2																													2					3	2		2		
2														4		4				6				6			6		2		6				2				
2														6	2	4				6	1	6	1	6			6												
2														6					1	6		6		6			6				6								
2														9		4				6		6		6			6												
2														6		4				6		6		6			6												

A breve termine :

- eliminazione /modifica nel tempo più breve possibile le situazione più pericolose
- eliminazione user id che in un arco temporale concordato non abbiano mai lanciato transazioni
- portare all'attenzione del process owner tutti coloro che svolgono attività ad elevato rischio (più attività in conflitto o l'intero processo di business

Azioni Possibili

A Medio termine:

- **ridefinizione e nuova assegnazione agli utenti di profili costruiti secondo il modello della separazione**
- **normalizzazione di una procedura per la gestione del processo di assegnazione/modifica/cancellazione di profili SAP ed assegnazione delle responsabilità**
- **costruzione di un sistema di monitoraggio**