



# IBM Service Management Roadshow

## Risk Management

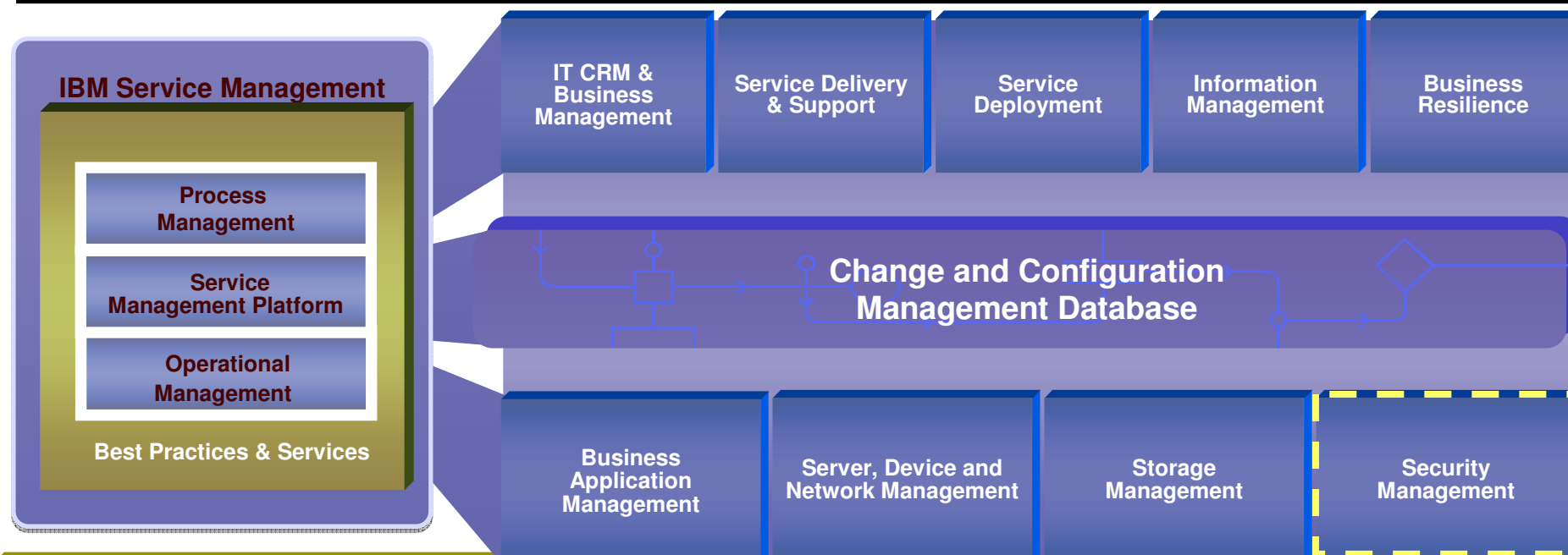
*Roma, Palazzo dell'Informazione, 13 Marzo 2007*

*Alessandro Faustini  
Tivoli Security Technical Sales*

# Agenda

- **Service Management & Security**
- **Consul Risk Management**
- **InSight**
- **zSecure**

# IBM Service Management e IT Security Management

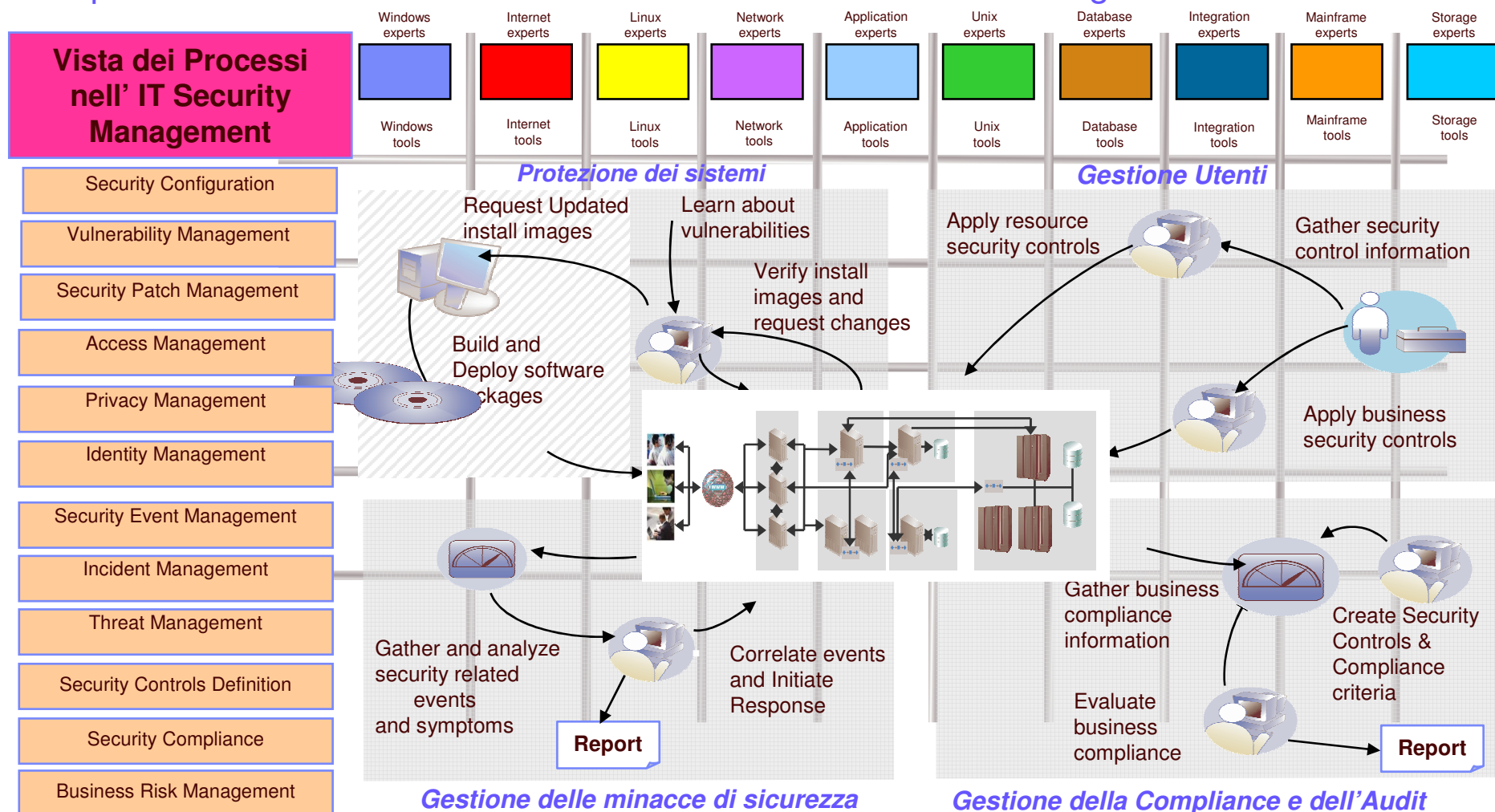


## Gestione della sicurezza e della compliance

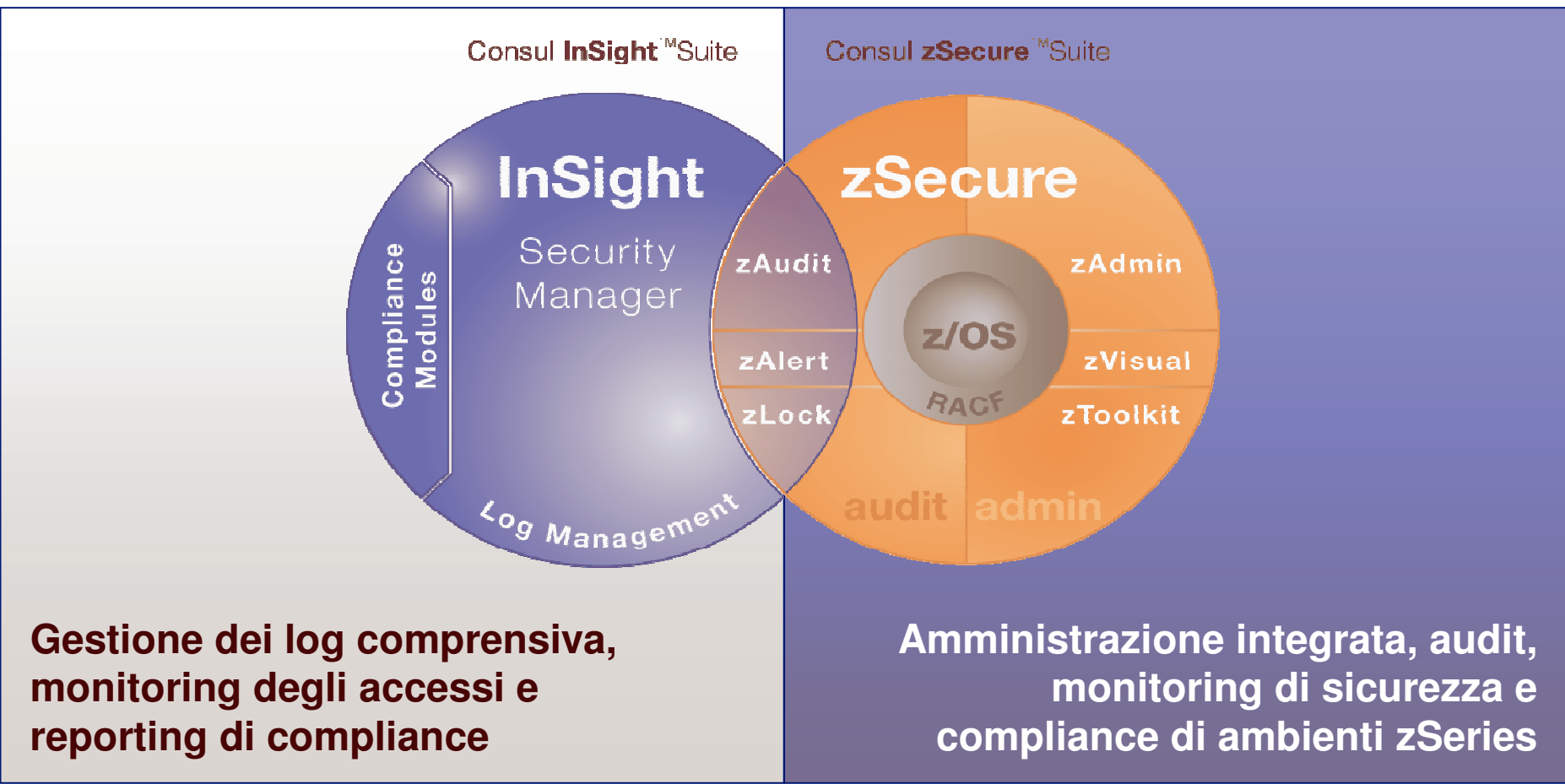
- Gestione della sicurezza IT, dell'audit e della compliance attraverso tutta la compagnia
- Gestione strutturata delle identità e degli accessi
- Gestione centralizzata delle minacce di sicurezza e degli incidenti
- Facilitare la valutazione degli impatti nella gestione dell'IT delle varie leggi e regolamentazioni come la SOX, GLBA, ISO17799, Basel II, Dlg. 196/2003, HIPAA
- Soluzioni comprensive, semplici da usare per gestire e monitorare l'attività utente attraverso tutta l'enterprise

# Processi chiave nell'IT Security Management

Le attività ed i processi associati con l'IT Security Management possono essere riassunti in quattro modelli che rimarranno attuali con i cambi della tecnologia.



# Consul Risk Management Audit & Compliance



# Audit & Compliance

- **Aumento degli obblighi**
  - Le normative sono ormai decine (Basilea II, ISO17799, Dlg. 196/2003, SOX...)
  - Le iniziative di compliance aumentano in ogni settore di industria
- **Aumento della complessità**
  - Le tecnologia e le infrastrutture disparate frammentano ed impediscono gli sforzi per la compliance
  - Il collegamento in termini di compliance tra il livello infrastruttura e il livello business è desiderabile, ma è una sfida spesso onerosa
- **Aumento dei costi**
  - Difficile sapere a priori il costo di un'attività di audit sulle moderne infrastrutture, eterogenee e distribuite
  - La cadenza periodica di un attività di audit impone costi fissi elevati
  - Il fallimento di un audit è nuovamente un costo da ripetere



**Il 43% dei CFO pensano che il miglioramento della governance, dei controlli e del risk management sia al top delle loro sfide.**

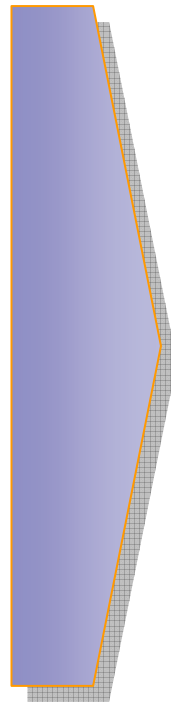
*CFO Survey: Current state & future direction,  
IBM Business Consulting Services*

# Audit & Compliance

Aumento degli  
obblighi

Aumento della  
complessità

Aumento dei  
costi



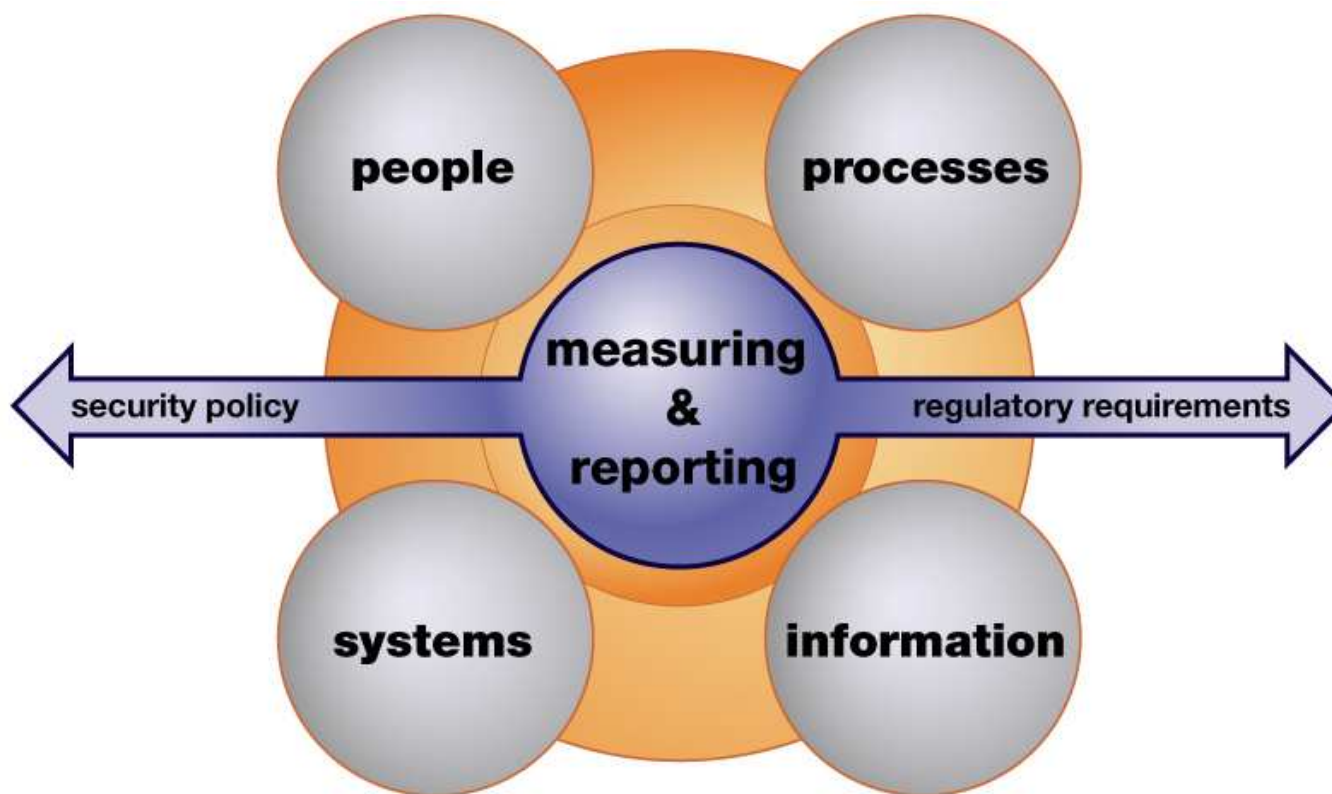
1. Le iniziative di Compliance richiedono processi strutturati e ripetibili
2. L'enfasi è sul controllo delle attività degli utenti privilegiati (*Privileged User Monitoring and Audit, PUMA*)
3. Facilità nel verificare gli accessi ai sistemi e applicazioni
4. Capacità di verificare la compliance degli asset strategici: z/OS, RACF, UNIX, monitoraggio e audit di database

# Cosa è importante

- **Violazioni alla Privacy**
  - DBA accedono informazioni riservate?
  - Ci sono usi impropri delle applicazioni HR?
  - Ci sono usi non legittimi di identità?
- **Violazioni alle politiche di sicurezza**
  - Ci sono modifiche ai sistemi non autorizzate?
  - Ci sono utenti root che hanno disattivato il tracciamento delle operazioni?
  - Quando sono stati cancellati i log di sistema?
  - Chi ha fermato quel processo importante senza permesso?
- **Amministratori che violano la separazione delle funzioni**
  - Ci sono utenti privilegiati che hanno effettuato transazioni su applicazioni in esercizio?
  - Ci sono utenti privilegiati che hanno creato e approvato nuove utenze e autorizzazioni sui sistemi?



## La Sfida dell'Audit & Compliance



*La sfida è misurare e visualizzare il comportamento delle persone sui sistemi e nell'accesso alle informazioni attraverso tutta l'enterprise senza inibire o degradare le performance del business*

# Personne

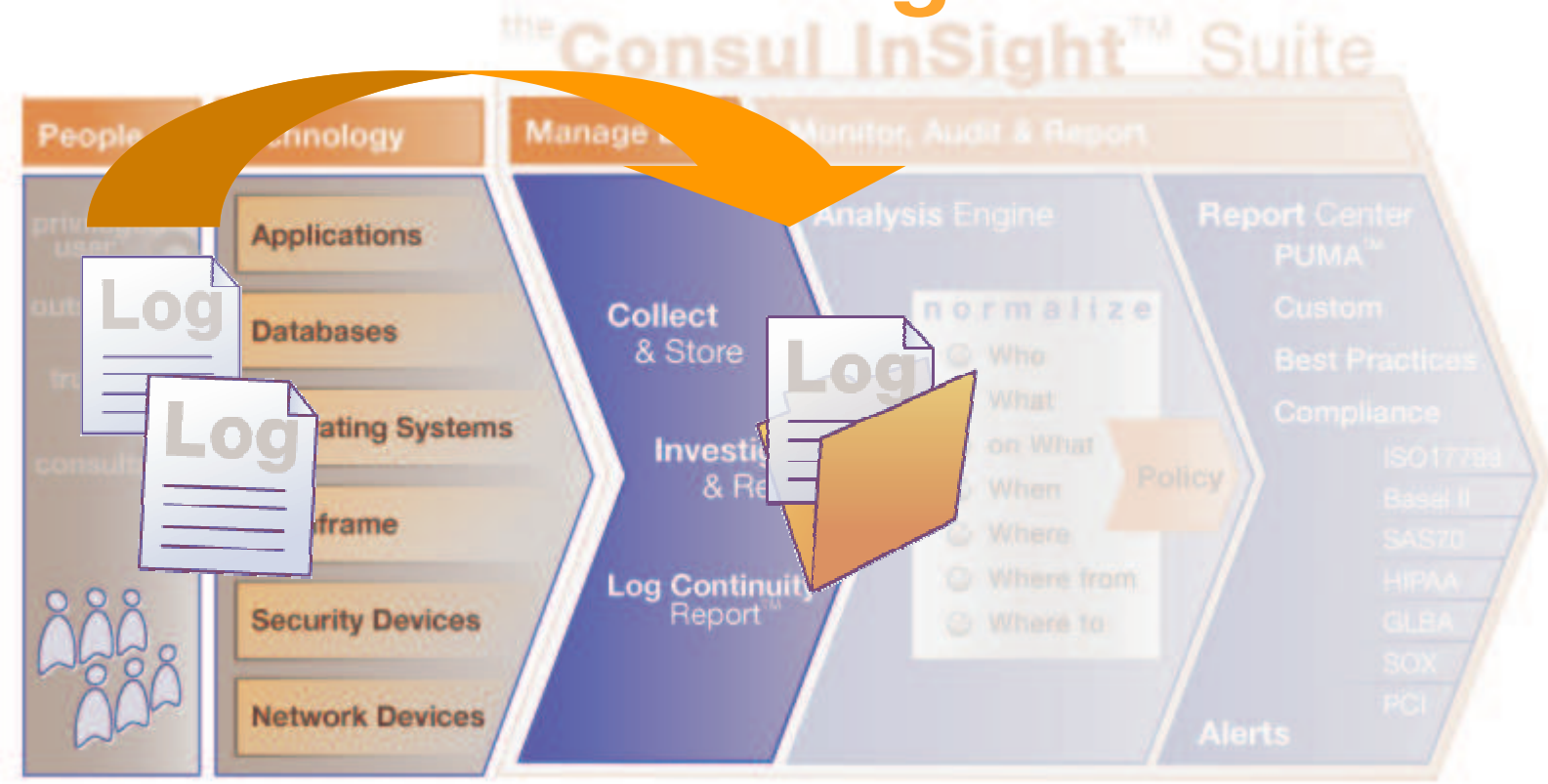
# the Consul InSight™ Suite



# Tecnologie the Consul InSight™ Suite



# Collezionamento dei file di Log the Consul InSight™ Suite



# Log Continuity Report the Consul InSight™ Suite

**People**

- privilege user
- outsourc
- trusted user
- consultan

**Technology**

- Applications
- Databases
- Operating System
- Mainframe
- Security Device
- Network Device

Dashboard
 History
 Continuity
 Activity
 Investigate
 Retrieval

**consul**

Portal > Log Manager > Continuity Report

### Log Continuity Report

> Graph

◀ June 24, 2005 ▶

location: Public Website (CRM007), Web Server Public, Internet Banking Public, Private Banking Server (CRM013), Private Banking Website, HR Data Server (CRM014), FTP server Partners (CRM015)

> List of Logfiles

<input type="checkbox"/>	#	Size	Start Date	Time	End Date	End Time	Eventsource Type	Eventsource Name	Machine
<input type="checkbox"/>	3	33 kb	June 25, 2005	10:00	June 25, 2005	12:00 (GMT +1)	IS	Public website	CRM007
<input type="checkbox"/>	5	21 kb	June 25, 2005	11:00	June 25, 2005	12:00 (GMT +1)	Windows Server	Web Server Public	CRM007
<input type="checkbox"/>	2	1.3 Mb	June 25, 2005	12:00	June 25, 2005	13:00 (GMT +1)	SAP	Internet Banking Public	CRM007
<input type="checkbox"/>	3	5 kb	June 25, 2005	13:00	June 25, 2005	13:17 (GMT +1)	Windows Server	Private Banking Server	CRM013

13

© 2007 IBM Corporation

# Benefici

## the Consul InSight™ Suite

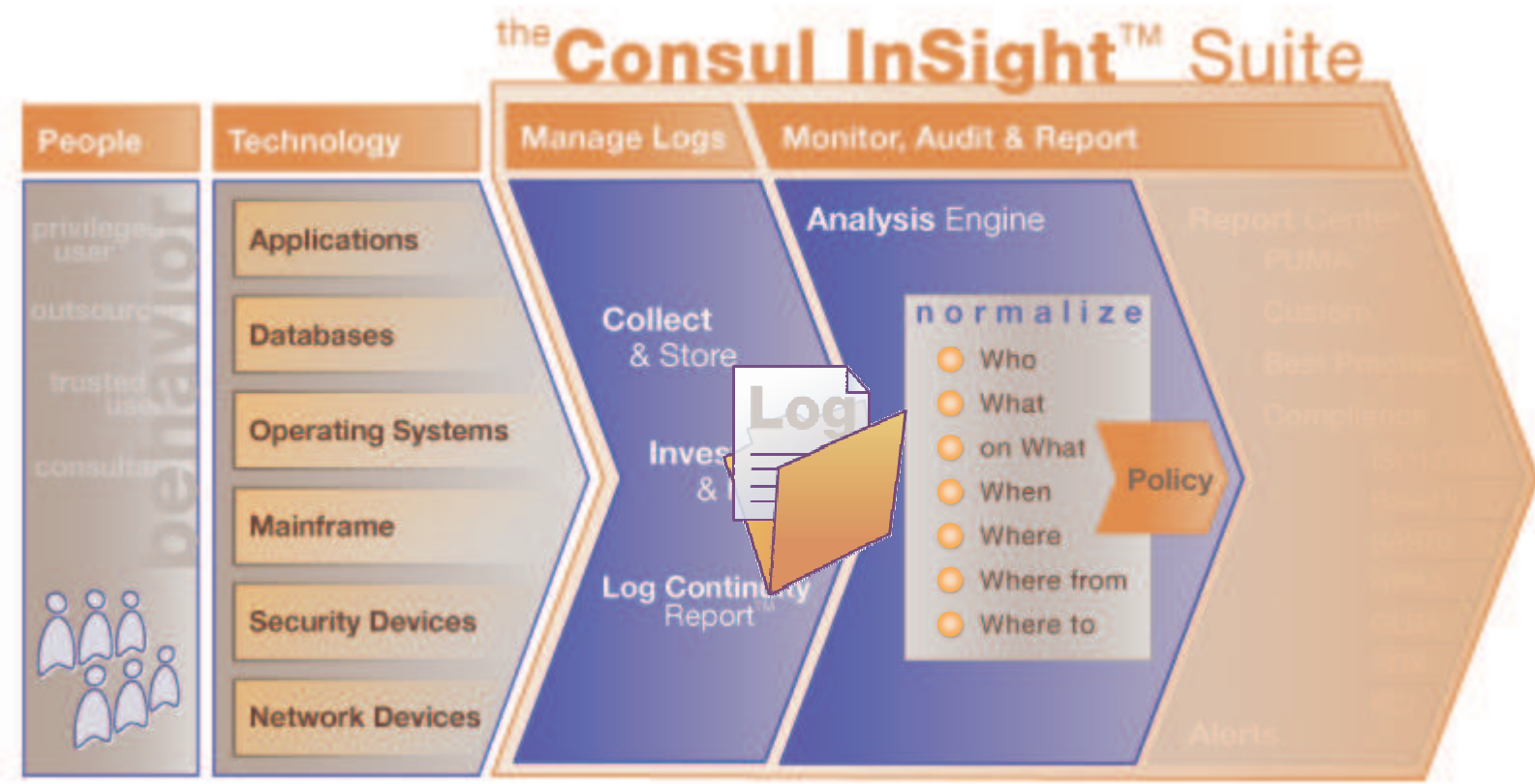


**Elimina le lunghe preparazioni per gli audit**

**Incrementa l'efficienza del team di audit**

**Soddisfazione degli auditor**

# Normalizzazione



# Report Center

People

Technology

privilege user

outsourc

trusted user

consultan

Application

Database

Operati

Mainfra

Security

Network

Dashboard Summary **Reports** Policies Groups Settings Regulations Log off

consul

> Dashboard > Reports Portal

### My Reports

[Add custom report](#) [Export custom reports](#)

Configuration tools

Type	Title	Description	Action
	Event Summary	Summary of all events	
	Events by Policy rules	List of events that comply with the Policy rules	
	Events by rule	List of events that comply with a W7 rule	
	Events by type	Summary of audited event types	
	Policy Wizard	Tool to help defining a policy and to verify the existing policy	
	Who accessing what frequency		
	Who realname by What triplet		

> Custom Report

> Daily verification

Detailed investigation

Type	Title	Description	Action
	Administration	List of administrative actions	
	Administration per user	List of administrative actions by user	
	Help Desk Activity	List of helpdesk security commands (enable/disable user)	



# Dashboard

Dashboard
Trends
Reports
Policies
Groups
Settings
Regulations
Log off

Dashboard Portal

People

Tech

privileges user

outsourc

trusted user

consultan

App

Data

Ope

Main

Sec

Net

## Compliance Dashboard

### Enterprise Overview

Events by top event count by "on What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.

**on What**

on What	Finance	Sales	Managers	Administrators	Marketing	Remote Users	Other
Finance high	High	High	Low	Low	Low	Low	Low
Finance low	Low	Low	Low	Low	Low	Low	Low
Client data	Low	Low	Low	Low	Low	Low	Low
HR data	Low	Low	Low	High	Low	Low	High
System data	High	Low	Low	Low	Low	Low	Low
Other	Low	Low	Low	Low	Low	Low	High

**Who**

### Trend graphic

Percentage of Exceptions for Oct 1, 2005 till Nov 28, 2005

### Database Overview

Database	Name	Status	Loading Date	Content
AggrDb	AggrDb	Loaded & Selected	Nov 29, 2005	Aggregation of all collected material for the last 90 days.
SOX				
Finance				
Basel II				
HR				
Banking				
Temp				

# Tipo di evento per utente

**Parameter Setup**

**What (event type)**

<input checked="" type="checkbox"/> Add : Privilege / Success	<input type="checkbox"/> Load : Module / Success	<input type="checkbox"/> Read : File / Success	<input type="checkbox"/> Stop : Service / Success
<input type="checkbox"/> Authenticate : User / Failure	<input type="checkbox"/> Logoff : User / Success	<input type="checkbox"/> Receive : Message / Success	<input type="checkbox"/> Update : Parameter / Failure
<input checked="" type="checkbox"/> Clear : Auditlog / Success	<input type="checkbox"/> Logon : User / Failure	<input type="checkbox"/> Restart : System / Success	<input type="checkbox"/> Use : Service / Success
<input type="checkbox"/> Complete : Process / Success	<input type="checkbox"/> Logon : User / Success	<input checked="" type="checkbox"/> Start : Process / Success	<input type="checkbox"/> Use : Service / Success
<input checked="" type="checkbox"/> Grant : Privilege / Failure	<input type="checkbox"/> Read : Access / Success	<input type="checkbox"/> Start : Service / Success	<input checked="" type="checkbox"/> Write : Config / Success
<input checked="" type="checkbox"/> Grant : Privilege / Success	<input type="checkbox"/> Read : Config / Success	<input checked="" type="checkbox"/> Start : System / Success	<input type="checkbox"/> Write : Log / Success

**Summary report**

Who (Name)	Logonname	What (Event type)	#Events
Administrator	WINDOWS_NT01\Administrator	Add: Privilege / Success	294
Administrator	WINDOWS_NT01\Administrator	Clear: Auditlog / Success	1150
Administrator	WINDOWS_NT01\Administrator	Grant: Privilege / Success	334
Administrator	WINDOWS_NT01\Administrator	Start: System / Success	7
ROOT	LN_SERV\ROOT	Add: Privilege / Success	5
ROOT	LN_SERV\ROOT	Grant: Privilege / Success	7
ROOT	LN_SERV\ROOT	Start: Process / Success	42
ROOT	LN_SERV\ROOT	Start: System / Success	306
ROOT	LN_SERV\ROOT	Write: Config / Success	10

# Dettagli sull'evento

Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off

Dashboard > Summary of Banking > Event List > Event Detail Portal

People

Tech

privileges user

outsourc

trusted user

consultan

## Event Detail

> Event information

Severity	Field	Group	
	70 (1x)	This is a policy exception This is a special attention	
When	Fri Nov 25, 2005 19:27:42 GMT -5	Week Evenings	50
What	Change : Auditlog / Success	Audit Log Actions	70
Where	Finance Server (OS/390)	Mainframe Finance	10
Who	Ross Hikkings	Administrators	10
From Where	WRKSTATIONSICRM007	Windows Workstations	10
On What	SYSTEM : FINANCE / SMF	Finance Data	10
Where To	Finance Server (OS/390)	Mainframe Finance	10

> Incident Tracking

> Additional information

Aspect	Value
Event :: command	6
Event :: logrecordtype	SMF, 90
Event :: miscellaneous	System status: operator command SWITCH SMF
Event :: subject	Ross Hikkings
Who :: originator	Ross Hikkings

# Sommario Utente

Navigation: Dashboard | Summary | Reports | Policies | Groups | Settings | Regulations | Log off

Breadcrumbs: Dashboard > Summary of Finance > Event List > Event Detail

Portal

### User Summary of Ross Hikkings as MAINFR\Admin\Ross001

▼ User information

Name	Ross Hikkings
Logonname	MAINFR\Admin\Ross001
#Events	15436
#Attention	245
#Exception	103
#Logon	21
#Logoff	20
#LogonFail	2
#Failure	65

▼ Who

Who (Source group)	Administrators
	Finance Admin

▼ When

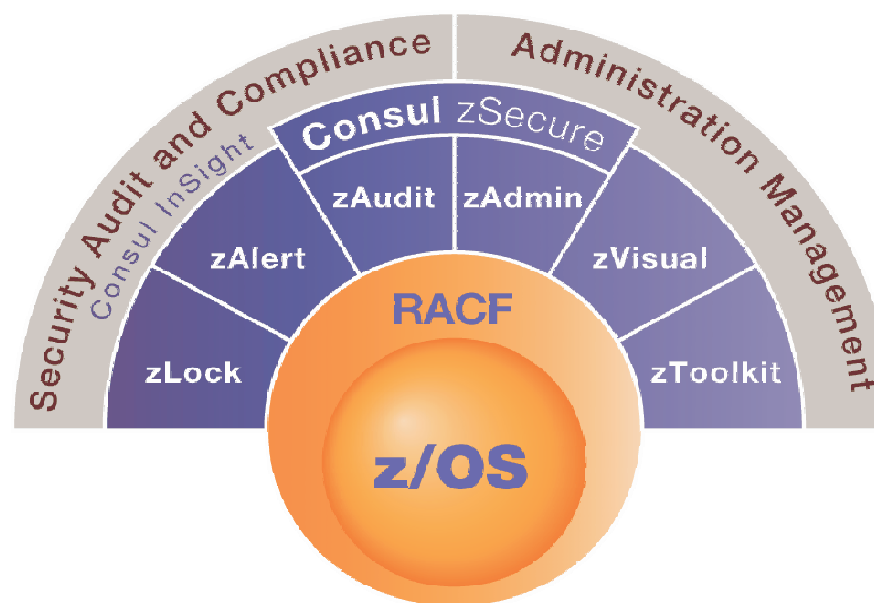
When (Period group)	#Events
Office Hours	10456
Week Evenings	3624
Weekend	1356

# Consul zSecure Suite

La suite Consul zSecure aggiunge strumenti user-friendly nel mainframe per facilitare l'amministrazione e fornire funzionalità di audit, alert e monitoring per z/OS Resource Access Control Facility (RACF)

## Funzionalità chiave

- La suite zSecure migliora la sicurezza del mainframe, migliora l'efficienza dell'amministrazione e consente di far diventare il mainframe l'hub per la sicurezza dell'enterprise.
- **Amministrazione e provisioning:**
  - **zAdmin** facilita e velocizza l'amministrazione del RACF
  - **zVisual** offre una Windows GUI per RACF
  - **zToolkit** è l'interfaccia CICS based per l'amministrazione del RACF
- **Audit, monitoring e compliance:**
  - **zLock** assicura la compliance alle politiche della compagnia e procedure per prevenire comandi errati
  - **zAlert** strumento di monitoraggio real-time delle intrusioni e delle attività indesiderate
  - **zAudit** fornisce strumenti per il detection degli eventi, l'analisi, il report, l'integrità del sistema e l'audit



## Benefici

- **Amministrazione e provisioning:**
  - Riduce il tempo, gli sforzi e i costi di amministrazione
  - Abilita un'amministrazione de-centralizzata
  - Tempi di risposta ridotti, facilitatori del business
  - Riduce il tempo di training necessario per i nuovi amministratori
- **Audit, monitoring e compliance:**
  - Passare audit più facilmente, migliorare la "posture" per la sicurezza
  - Risparmiare tempo e costi attraverso una migliorata gestione della sicurezza e degli incidenti
  - Incrementare l'efficienza operativa

## zSecure: Administration Management

- ➔ **zAdmin** – è lo strumento per facilitare e velocizzare l'amministrazione del RACF, evitando di usare farraginosi comandi nativi. zAdmin aggiunge un layer user-friendly sopra i tuoi RACF database. Attraverso questo software è possibile facilitare l'inserimento di comandi amministrativi, generare custom report ed eseguire clean-up di database.
- ➔ **zVisual** - è l'interfaccia grafica Windows based per l'amministrazione del RACF, di usare personale non specialistico o abilitare un'amministrazione centralizzata non basata su ISPF/TSO.
- ➔ **zToolkit** – Esegue semplici tak amministrativi da un ambiente CICS, liberando risorse con preziose competenze RACF da routine di amministrazione di base.

## zSecure: Administration Management

Migliorare la sicurezza del mainframe	<b>C'è sempre una possibilità per una breccia nel tuo sistema di sicurezza, ma con zAdmin la tua amministrazione più pulita e protetta ridurrà questa probabilità.</b>
Ridurre i tempi di amministrazione	<b>Con zAdmin il tempo richiesto per eseguire task di sicurezza è tipicamente ridotto del 50-75% permettendo alle tue ridotte risorse esperte mainframe di focalizzarsi nel miglioramento della qualità della sicurezza.</b>
Accelerare i tempi di risposta	<b>Gli utenti in attesa per la creazione di nuove userid ed altri task amministrativi verranno serviti più rapidamente grazie a zAdmin.</b>
Eliminare la necessità di soluzioni fatte in casa	<b>Molte compagnie hanno realizzato soluzioni sviluppate in casa per applicare le politiche di sicurezza. Tali soluzioni spesso costano di più per la realizzazione e il mantenimento di quanto le compagnie riescono a realizzare. zAdmin elimina questi costi.</b>
Abilitare la decentralizzazione delle risorse	<b>Operatori di Helpdesk e amministratori non-RACF sono generalmente 20-40% più economici. Consul abilita la decentralizzazione dei task amministrativi con minore impatto per l'amministrazione.</b>

## zSecure: Audit & Compliance

- ➔ **zAudit** – Audit e monitoraggio per gli eventi di sicurezza in ambiente mainframe. Analisi automatica delle esposizioni rispetto alle politiche definite. zAudit fornisce report standard e personalizzati, allarmi real-time sulla violazione delle policy.
- ➔ **zAlert** – zAlert è uno strumento di monitoring real-time per le minacce di sicurezza in ambiente mainframe che va ben oltre ad un tradizionale sistema di Intrusion Detection poichè è in grado di bloccare le azioni come un vero sistema di Intrusion Prevention. Gli allarmi sono scritti in un linguaggio di reporting semplice da utilizzare (CARLa), dando ai clienti la possibilità di personalizzare il “look and feel” delle e-mail e dei messaggi di testo da inviare a telefoni cellulari.
- ➔ **zLock** – permette di effettuare policy enforcement in modo che il sistema mainframe risulti protetto da operazioni accidentali o volute ma comunque dannose, limitando quindi le abilitazioni e le autorizzazioni degli utenti.



## Consul z/OS audit, monitoring e compliance

Passare gli audit e migliorare la sicurezza	<b>Avere i report che gli auditor e le regolamentazioni richiedono. Ridurre le possibilità di avere costose brecce di sicurezza attraverso una più sicura amministrazione del mainframe.</b>
Risparmiare tempi e costi	<b>zAudit può far risparmiare preziose ore-uomo necessarie per l'audit, la reportistica ed il clean-up dei database amministrativi. Realizzare significativi risparmi nell'utilizzo della CPU dovuti all'efficiente motore di reporting.</b>
Incrementare l'efficienza operativa	<b>zAudit mostra quali JCL, parametri e moduli caricati sono stati cambiati, quindi riduce il downtime delle applicazioni causate da modifiche inaspettate o improprie.</b>
Velocizzare la reazione agli incidenti di sicurezza	<b>Grazie ai dettagli presenti nelle e-mail di alert gli amministratori possono muoversi più rapidamente per diagnosticare e rimediare a failure o esposizioni.</b>
Eliminare la necessità di soluzioni fatte in casa	<b>Riduce o elimina la necessità di applicazioni home-made per forzare la compliance.</b>



धन्यवाद

Hindi

多謝

Traditional  
Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

Thank You

English

Obrigado

Brazilian  
Portuguese

شكراً

Arabic

多谢

Simplified Chinese

Danke

German

Grazie

Italian

Merci

French

நன்றி

Tamil

ありがとうございました

Japanese

감사합니다

Korean