

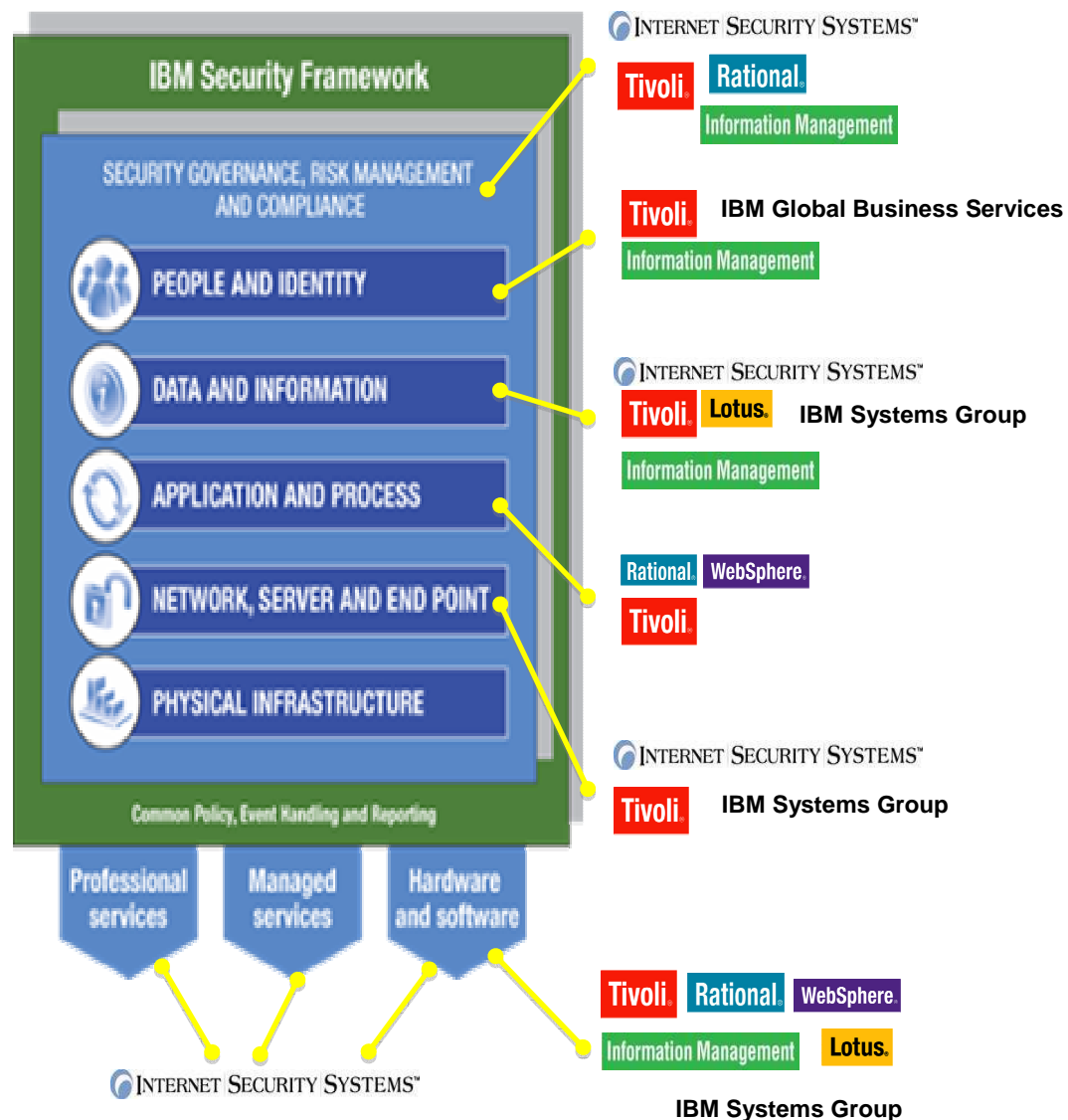


# Monitorización de usuarios y cumplimiento normativo

*Emmanuel Roeseler : Southwest Tivoli Security Sales Leader*  
*Emmanuel\_roeseler@es.ibm.com*



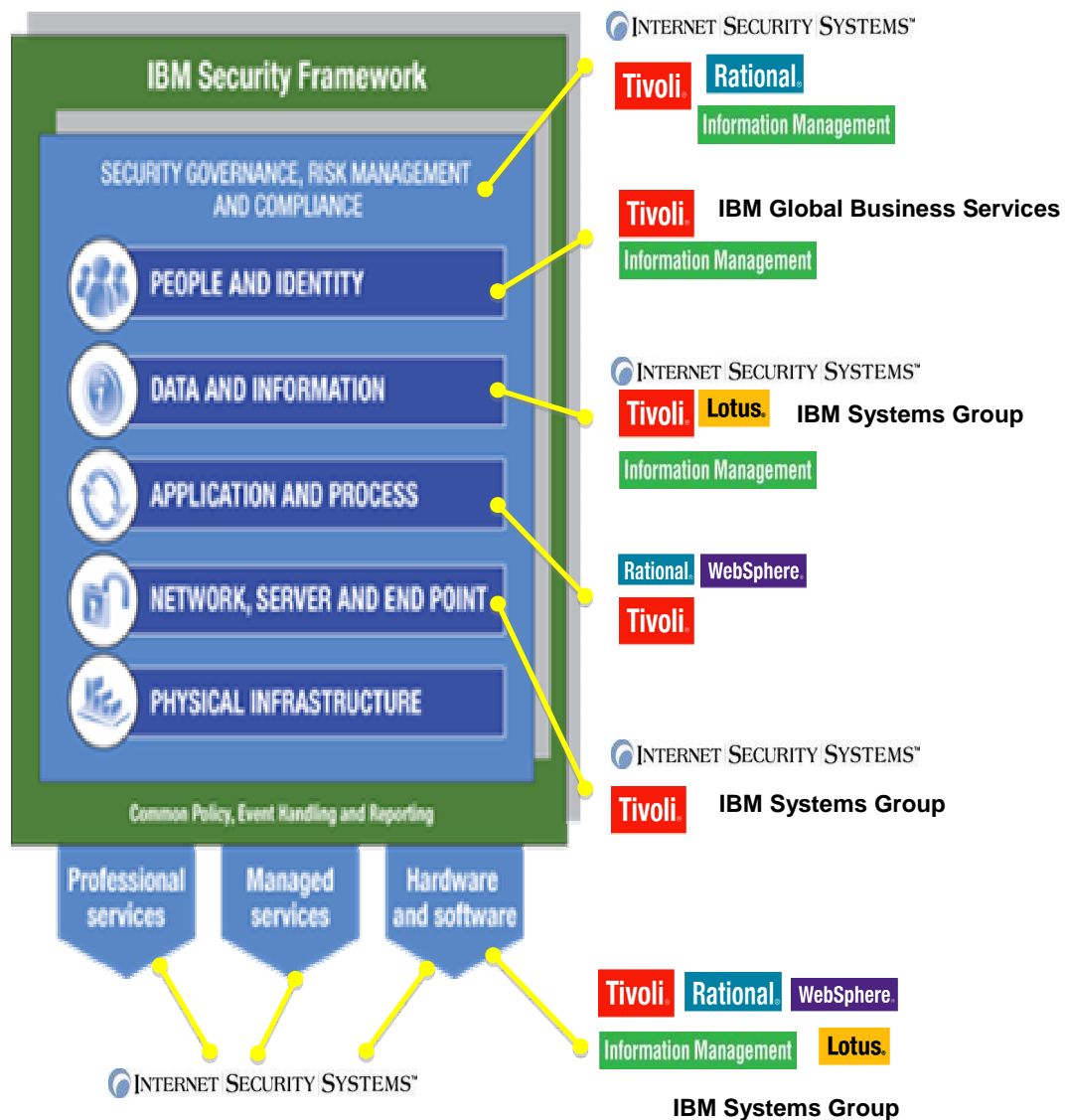
# Framework de Seguridad de IBM



## Seguridad en IBM

- 15,000 investigadores y desarrolladores involucrados en iniciativas de seguridad
- Más de 3,000 patentes de gestión de seguridad y de gestión de riesgo
- Más de 200 referencias cliente y 50 casos de estudio
- Más de 40 años de éxitos *securizando* el entorno *mainframe*
- Gestionando más de 2.5 billones de eventos de seguridad para nuestros clientes
- El *Framework* de seguridad IBM

# Framework de Seguridad de IBM



- **Medir grado de conformidad con soluciones Tivoli**
- **Otras Soluciones para el cumplimiento normativo**
- **Casos de éxito en la gestión de accesos**

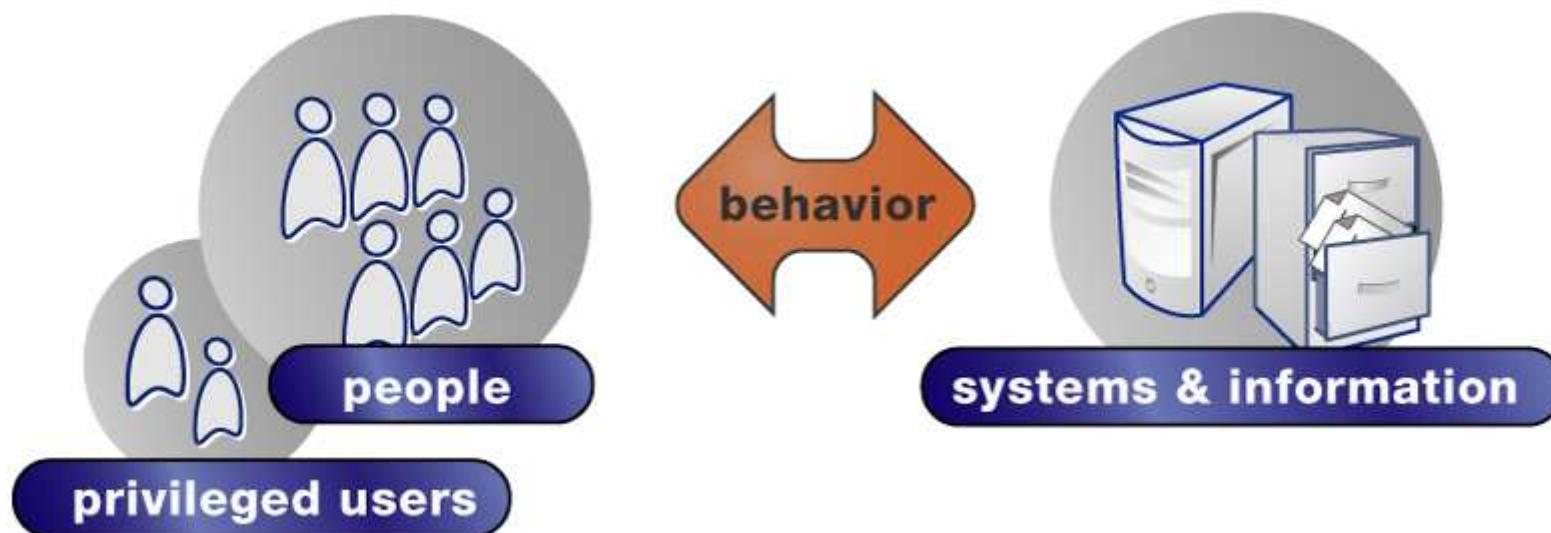
## Auditoria de Identidad

- **Auditoria del aprovisionamiento:** ¿Quién tiene que permisos? ¿Cuándo se modificó la cuenta?
- **Auditoria de acceso web :**¿Cuándo se cambió la contraseña? ¿Cuántos login se realizaron? ¿Cuál fue la URI accedida?
- **Auditoria de operaciones de logon:** ¿A que aplicaciones accedió el usuario?

## ¿QUE FALTA?

- **Auditoria de acceso al dato**
- **Correlar acciones**
- **Auditoria de la actividad en las aplicaciones**
- **Determinar que es “normal” y que no lo es**
- **Identificar comportamientos anómalos y riesgos potenciales**

## ¿Qué esta haciendo la gente en Mi Red?



***El 87% de los ataques internos están causados por usuarios privilegiados y técnicos.***

# ¿Como doy sentido a todo esto?

The screenshot displays a security audit log viewer with three main panes. The top-left pane shows a raw log stream with hex-encoded text. The bottom-left pane shows a filtered log stream with the following entries:

```

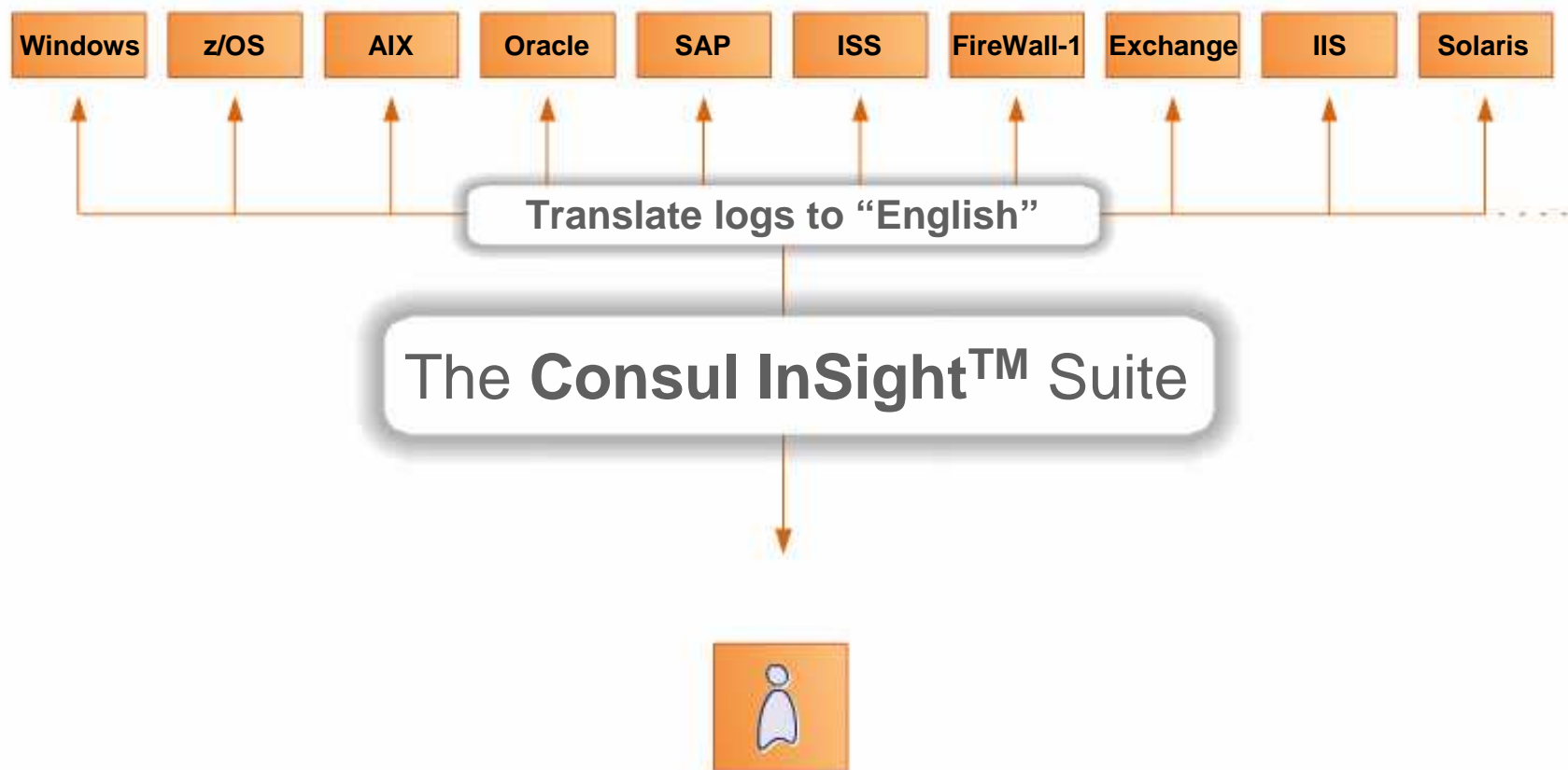
Apr 5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname=
tty=ruser=acristal rhost= user=MQM
Apr 5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acrist
Apr 5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr 5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr 5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr 5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr 5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr 5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr 6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr 6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr 6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr 6 03:01:01 syslog crond(pam_unix)[10477]: session closed for user MQM
Apr 6 03:33:29 syslog crond(pam_unix)[10479]: session closed for user MQM
Apr 6 04:01:02 syslog crond(pam_unix)[10509]: session closed for user MQM
Apr 6 04:03:46 syslog crond(pam_unix)[10511]: session closed for user MQM
Apr 6 04:30:02 syslog crond(pam_unix)[11012]: session closed for user MQM
Apr 6 05:01:01 syslog crond(pam_unix)[11031]: session closed for user MQM
Apr 6 06:01:01 syslog crond(pam_unix)[11033]: session closed for user MQM
Apr 6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr 6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr 6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr 6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname=
ruser= rhost=10.101.1.154 user=ebarrios
Apr 6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)
  
```

The right pane shows detailed security audit information for three events:

- Event 1:** Security audit (SECURITY) on APPLES, system id: 2074. Auditable event: Batch process login. Event time: 1-MAR-2005 00:02:09.84. PID: 20402B44. Process name: BATCH\_440. Username: SYSTEM. Process owner: [SYSTEM]. Image name: DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE. Posix UID: -2. Posix GID: -2 (%XFFFFFFFE).
- Event 2:** Security audit (SECURITY) on CYGNUS, system id: 2073. Auditable event: Network login. Event time: 1-MAR-2005 00:02:16.11. PID: 2021A46D. Process name: MQMTC\_P2\_BG164. Username: MQM. Process owner: [MQM\_SERVER]. Image name: DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE. Remote node id: 241859594. Remote node fullname: xyzzz.bananajunior.com. Remote username: MQM. Posix UID: -2. Posix GID: -2 (%XFFFFFFFE).
- Event 3:** Security audit (SECURITY) on CYGNUS, system id: 2073. Auditable event: Batch process login. Event time: 1-MAR-2005 00:02:32.61. PID: 20219477. Process name: BATCH\_443. Username: SYSTEM. Process owner: [SYSTEM].

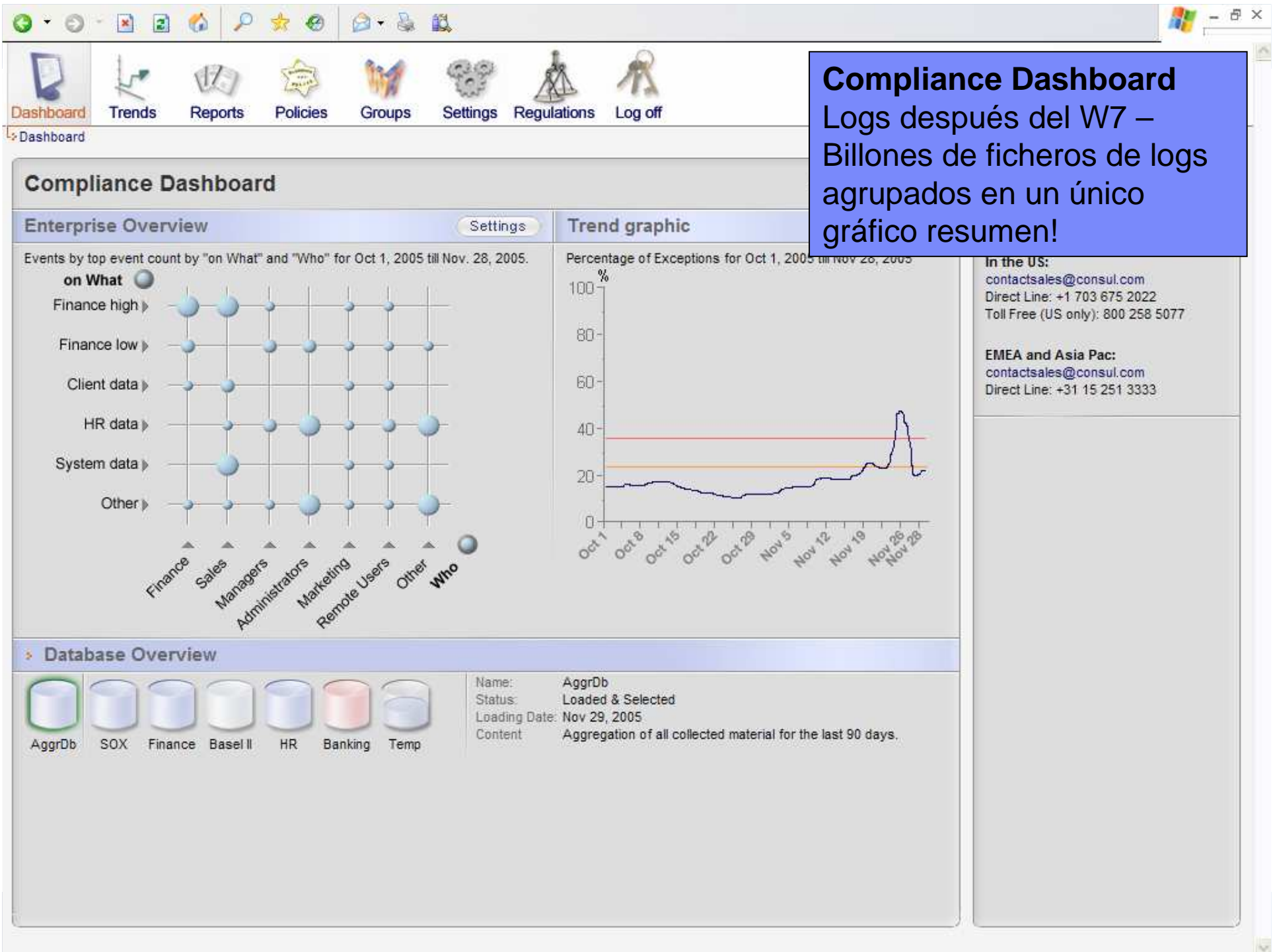
Red boxes and arrows highlight the correlation between the log entries and the audit details. For example, the log entry "authentication failure; logname= user=MQM" is linked to the audit details for the "MQM" user in the second event.

## Ahora los log de tu empresa en un único lenguaje



***Tivoli Compliance InSight Manager ahorra tiempo y dinero a tu departamento de seguridad de la información y cumplimiento mediante la automatización de la monitorización a través de la empresa.***







Dashboard History **Continuity** Activity Investigate Retrieval

Portal > Log Manager > Continuity Report

## Log Continuity Report

Graph

June 24, 2005

**Location**

- CRM007
  - Public Website
  - Web Server Public
  - Internet Banking Public
- CRM013
  - Private Banking Server
  - Private Banking Website
- CRM014
  - HR Data Server
- CRM015
  - FTP server Partners
- CRM023
  - Partner Webserver
  - IIS Partner Site
- CRM024
  - EMEA mail

**Type**

0:00 4:00 8:00 12:00 16:00 20:00

hour day week month year

**List of Logfiles**

#	Size	Start Date	Time	End Date	End Time	Eventsource Type	Eventsource Name	Machine
3	33 kb	June 25, 2005	10:00	June 25, 2005	12:00 (GMT +1)	IIS	Public website	CRM007
5	21 kb	June 25, 2005	11:00	June 25, 2005	12:00 (GMT +1)	Windows Server	Web Server Public	CRM007
2	1.3 Mb	June 25, 2005	12:00	June 25, 2005	13:00 (GMT +1)	SAP	Internet Banking Public	CRM007
3	5 kb	June 25, 2005	13:00	June 25, 2005	13:17 (GMT +1)	Windows Server	Private Banking Server	CRM013
3	213 kb	June 25, 2005	14:00	June 25, 2005	16:30 (GMT +1)	IIS	Private Banking Website	CRM013
1	94 kb	June 25, 2005	15:00	June 25, 2005	19:00 (GMT +1)	Windows Server	HR Data Server	CRM014

Export to PDF  
Export to Excel  
Retrieve selected Logfiles  
Regenerate Report  
Adjust Schedule

**View**

- Hide Timezone (GMT +1)
- By Audited Timezone
- By Browser Timezone
- By Other Timezone

**Filters**

**Sorting**

- Start Date
- Start Time
- Audited Machine

**Legend**

- Continuity Logfile
- Missing Logfile
- Missing Sub Logfile
- Failed collect, not collected yet
- Delayed collect, possible lost
- Archived Logfile
- Corrupt Logfile

**Report information**

Done My Computer

**Log Continuity Report**  
Prueba instantánea para los auditores y reguladores de que tu gestión de logs esta completa y es continua.

**W7 Eventlist**  
 Fíjate!: Mike Bonfire, un DBA, esta leyendo las nóminas

Dashboard Summary Reports Policy Groups Settings Regulations Portal

Portal > Dashboard > Reports > Database Top 10 Reports > Direct Database Access

### Direct Database Access Report

Time period setup

Start time: Month: September, Day: 3, Year: 2006, Hour: 1, Min: 0  
 End time: Month: September, Day: 7, Year: 2006, Hour: 16, Min: 0

Execute Reset

Time zone: Event time zone

### Event List

Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Sun Sep 03 2006 09:00:02 GMT-05:00	1	Logon : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	MS SQL Server
50	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Jim Hofferan	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Jim Hofferan	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Logon : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	MS SQL Server	Max Doane	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	DB2 Server	Jim Hofferan	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dboject / Success	DB2 Server	Jim Hofferan	DB2 Server	DBOBJECT : Finance/fn_op / Fn_op	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dboject / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	DB2 Server
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	DB2 Server	Mike Bonfire	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dboject / Success	MS SQL Server	Mike Bonfire	MS SQL Server	DBOBJECT : Finance/fn_lg / Fn_lg	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dboject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

1 2 3 4 5



consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations

### Compliance Modules

- Basel II
  - Introduction
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- Gramm-Leach-Bliley Act (GLBA)
  - Introduction
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- Health Insurance Portability and Accountability Act (HIPAA)
  - Introduction
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- ISO 17799
  - Introduction
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- Sarbanes Oxley (SOX)
  - Introduction
  - Classification Template
  - Policy Template
  - Reports
  - Documentation

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Classification Template

#### Classification Template

Download this template to use in the management Console.

Who

What

Group Name	Description
Alerts	Alerts generated by system devices resources
Alerts - High	Alerts generated by system devices resources - High
Alerts - Low	Alerts generated by system devices resources - Low
Alerts - Medium	Alerts generated by system devices resources - Medium
Exposure - High	description of Exposure - High
Exposure - Low	description of Exposure - Low
Exposure - Medium	description of Exposure - Medium
Exposure	description of Exposures
Intrusion - High	description of Intrusion - High
Intrusion - Low	description of Intrusion - Low
Intrusion - Medium	description of Intrusion - Medium
Intrusions	Intrusions reported by OS devices

on What

When

Group Name	Description
Office Hours	Normal working hours for staff
Out of Office Hours	Out of normal working hours
Weekend	Non-working days

Where

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Policy Template

#### Policy Template

Download this template to use in the management Console.

Policy Rules

Attention Rules

Who group	What group	When group	Where group	on/what group	from/where group	Where To Group ID	Severity	Description
HR Management	Intrusion - Medium		Customer Information Systems		Reside Workstation		medium	30 Review
Administrators			Financial - Medium	HR - Medium			access medium	40 Requires attention
Administrators			Customer Data - High				access 50	Requires attention
Administrators			Financial - Low				access high	70 Requires immediate attention
IT			Sensitive				access low	20 Review
Unknown	Customer							25

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

#### Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFEC 1.3.1.1) Classification report	No description supplied
Sarbanes Oxley (S.3.5.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (S.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (S.1.6) External contractors	Exceptions and failures caused by External Contractors.
Sarbanes Oxley (S.3) Malicious attacks	Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (S.4.5) Operator log	Actions performed by the IT Admin staff.
Sarbanes Oxley (S.5) Network management	Actions and events caused by users on Network Services.
Sarbanes Oxley (S.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (S.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (S.2.4.5.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (S.2.4.6.7) System access and use	Successes and failures against key assets.
Sarbanes Oxley (S.3) User responsibilities and password use	Login failures and successes either locally or remotely.
Sarbanes Oxley (S.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (S.4.4) Node authentication	Authentication of connections to remote computer systems.
Sarbanes Oxley (S.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (S.5.3) User identification and authentication	Login/Logout successes and failures.
Sarbanes Oxley (S.5.5) System utilities	Usage of system utilities.
Sarbanes Oxley (S.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (S.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (S.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset group User, HR Data, Source Code, and Financial Data.
Sarbanes Oxley (S.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the InSight system.
Sarbanes Oxley (S.8.1) Mobile worker	Exceptions and failures for mobile workers.

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

Extra Information

Help

Contact us

In the US:  
contactsales@consul.com  
Direct Line +1 703 675 2022  
Toll Free (US only) 800 258 5077

EMEA and Asia Pac:  
contactsales@consul.com  
Direct Line +31 15 261 3333

# Operational Change Control Report

Consulta el resumen de todos los cambios operacionales efectuados por los diferentes grupos

Dashboard Summary Reports Policy Groups Settings Regulations Portal

Dashboard > Regulations > Sarbanes Oxley Regulation Reports > Operational Change Control

## Operational Change Control of Finance database

### Time period setup

Month Day Year Hour Min.

Start time: October 1 2006 0 40

End time: November 1 2006 0 40

Execute Reset

Time zone: GMT-05:00 New\_York, Nipigon, Pangnirtung

### Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	System Administration	General Data	Finance Server	1256	15	145	12
Administrators	System Operations	Sensitive Data	Finance Server	1352	89	156	0
Administrators	System Updates	Financial Data	Finance Server	1543	154	456	45
FinAdmin Staff	System Updates	Sensitive Data	Finance Server	5644	16	165	0
IT	System Actions	Financial Data	Finance Server	5466	126	14	0
IT	System Operations	Sensitive Data	Mainframe FIN	8836	91	4	0
IT	System Updates	General Data	Mainframe FIN	4875	4	46	2
IT Admin	Authorization Objects	Financial Data	Finance Server	56	88	16	23
IT Admin	System Operations	Sensitive Data	Mainframe FIN	546	189	16	0
IT Admin	System Updates	General Data	Mainframe FIN	5165	48	54	0
Sales	System Actions	Financial Data	Finance Server	78	78	78	0
System	System Actions	Financial Data	Finance Server	15654	6	15	0
System	System Administration	Sensitive Data	Finance Server	546	15	45	0

The system update report shows changes to key system components. This report when used with the incident tracking report allows changes to be monitored and recorded and tracked via an external incident tracking system.

**Regulation**  
Paragraph 8.1.2

**Data Selection**  
This report is based on the following groups:

**What DBA Actions,**

- System Actions,
- System Administration,
- System Operations,
- System Updates

**Contact us**

**In the US:**  
[contactsales@consul.com](mailto:contactsales@consul.com)  
 Direct Line: +1 703 675 2022  
 Toll Free (US only): 800 258 5077

**EMEA and Asia Pac:**  
[contactsales@consul.com](mailto:contactsales@consul.com)  
 Direct Line: +31 15 251 3333



Severity	When	#	What	Where	Who			
2	Tue Oct 24 2006 14:32:44 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	(Windows)	David088	(Windows)
2	Tue Oct 24 2006 16:09:39 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferan	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:52 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferan	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:26 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferan	SRV_DC_034 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Unavailable / Unavailable	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferan	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferan	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Ralph037 / Ralph037	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034	USER : Ralph037 /	SRV_DC_034

**Event List**  
 Zoom sobre todas las acciones que los administradores IT hicieron en el servidor de Finanzas y descubre la creación de la cuenta de usuario Chin055

**An Event Detail Report**  
 Acceso a un evento específico y consulta todos sus detalles, y podemos acceder incluso al log original

Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-detail

### Event Detail

Event information

Field	Group	
Severity	2 (1x)	-
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10) 10
What	Grant : Privilege / Success	Security Changes Administration 50 40
Where	SRV_DC_034 (Windows)	Finance Server 50
Who	Jim Hofferma	Administrators 30 Database Admin 30 Finance Admin 20
From Where	XPWKST03 (Windows)	Workstation 10
On What	USER : Chin055 / Chin055	Authorization Objects 30 20
Where To	SRV_DC_034 (Windows)	Finance Server 50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute  
 Selected time zone: GMT+01:00 Rome, San\_Marino, Sarajevo

Filter by Platform: SRV\_DC\_034 (Windows)

Filter by User: Jim Hofferma

**Investigate**

Logrecords...

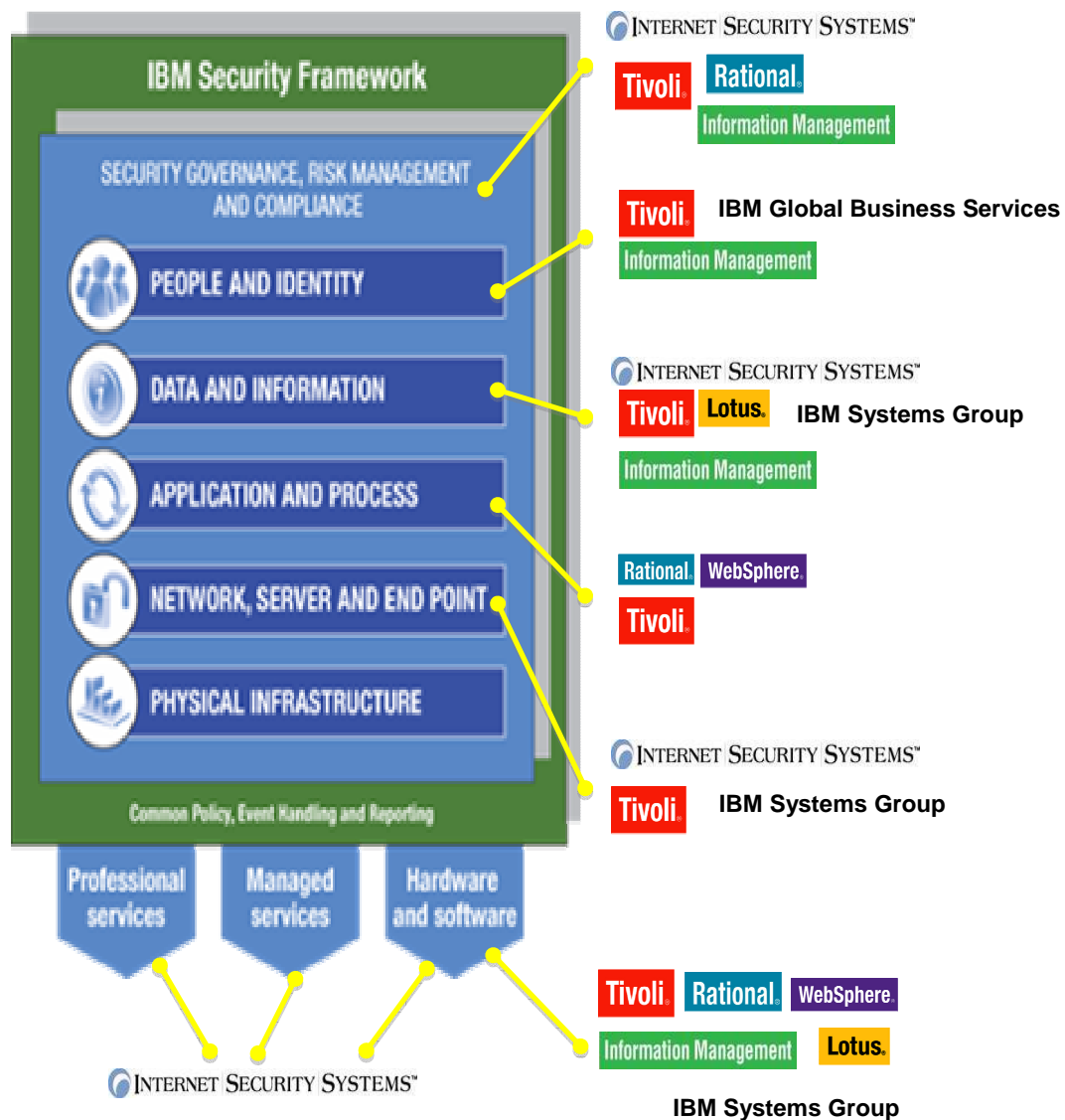
```

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
^F^A^T^K^e^c^e^e^L^F^SECURITY^L^2^s^z^A^H^)^@D+@ $^8^SYSTEM
^H^*^@BATCH_440^H^/^@D^A^H^W^Apjy^H^X^Apjy
^H^z^H^e^e
^G^APPLES.^@S^@:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^E^T^N^e^c^e^e^e^e
^L^F^SECURITY^H^+^
|j^N^G^e^@MQH^V^@^xyzz.bananajunior.com^L^2^@0dz^A^H^)^@m^! $^8^MQH
^R^*^@MQHTC_P2_B6164^H^/^@e^A^H^W^Apjy^H^X^Apjy
^H^v^H^e^e
^G^CYGNUS.^@S^@:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^A^T^K^e^c^e^e^e^e
^L^F^SECURITY^L^2^@Lanz^A^H^)^@w^! $^8^SYSTEM
^H^*^@BATCH_4
43^H^/^@D^A^H^W^Apjy^H^X^Apjy
^H^v^H^e^e
^G^CYGNUS.^@S^@:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^A^T^K^e^c^e^e^e^e
^L^F^SECURITY^L^2^@Lanz^A^H^)^@w^! $^8^SYSTEM
^H^*^@BATCH_
443^H^/^@D^A^H^W^Apjy^H^X^Apjy
^H^v^H^e^e
^G^CYGNUS.^@S^@:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^A^U^U^T^A^c^e^e^e^e^e
^L^F^SECURITY^H^@^m^;3^H^@^A^e^e^H^A^A^e^e^H^@^FILE
~
~
~
  
```

10,35-41 ALL



# Framework de Seguridad de IBM



- Medir grado de conformidad con soluciones Tivoli
- Otras Soluciones para el cumplimiento normativo
- Casos de éxito en la gestión de accesos

# Es necesario el cifrado de la información?



Format the drive or delete the data

- ***Doesn't remove the data - data is still readable***



Over-writing

- ***Takes hours-to-days***
- ***Error-prone; no notification from the drive of overwrite completion***



Shredding

- ***Very costly, time-consuming***
- ***Environmentally hazardous***



Degaussing

- ***Very costly, time-consuming***
- ***Difficult to ensure degauss strength matched type of drive***



Smash the disk drive

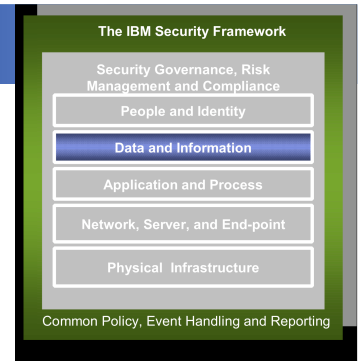
- ***Not always as secure as shredding, but more fun***



Professional offsite disposal services

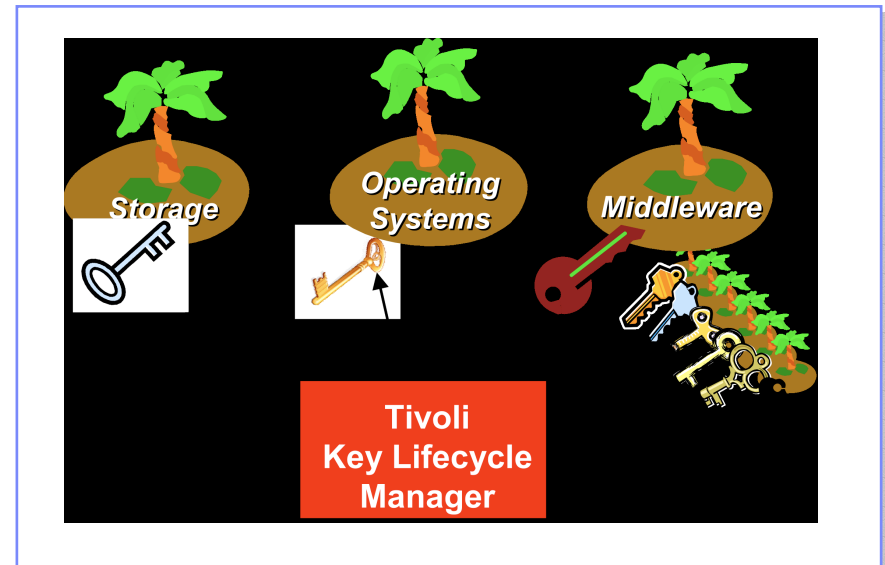
- ***Drive is now exposed to the tape's falling-off-the-truck issue***

# Tivoli Key Lifecycle Manager *Data & Information*



## What's new!

- Brand new offering! GA in 2H08
- Single GUI to simplify configuration & administration of key generation & management
- Easy to use Interface to do basic local Key Lifecycle Management
- Significantly simplifies set up and use of keys
- Key management can be centralized, distributed, or both
- Helps avoid key/certificate expiration problems
- Key retention/availability for backed-up data, to address regulations/discovery rules
- Can be used to manage many platforms, IBM storage, applications, and legacy system keys



## Beneficios

- **Proteger la propiedad intelectual y la imagen de la entidad**
- **Reducir costes de cifrado**
- **Cumplir las normativa legal**

# Analogia en el mundo mainframe

**Desde la administración de RACF a Tivoli Zsecure es como esto:**

```

COMMAND OUTPUT BROWSE -----
COMMAND ==> _
***** Top of Data *****
listuser ZPU001
USER=ZPU001 NAME=BANKING USER 1 OWNER=ZPDEPT31 CREATED=07.095
DEFAULT-GROUP=ZPDEPT31 PASSDATE=00.000 PASS-INTERVAL=120 PHRASEDATE=N/A
ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
LAST-ACCESS=UNKNOWN
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED (DAYS) (TIME)
-----
ANYDAY ANYTIME
GROUP=ZPDEPT31 AUTH=USE CONNECT-OWNER=ZPDEPT31 CONNECT-DATE=07.095
CONNECTS= 00 UACC=NONE LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
GROUP=ZPACC02 AUTH=USE CONNECT-OWNER=SYS1 CONNECT-DATE=07.095
CONNECTS= 00 UACC=NONE LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
***** Bottom of Data *****
  
```



```

Session A - [32 x 80]
zSecure Admin+Audit for RACF USER overview Line 1 of 54
Users like Z* 30 Jan 2008 14:35

- Identification of ZAADMIN ZT01
  User name WAS_ADMINISTRATOR
- Installation data
  Owner SENIOR KEVIN SENIOR ITALY
  User's default group ZACFG

Group Auth R SDA AG Uacc Revokedt Resumedt InstData
ZACFG USE NONE

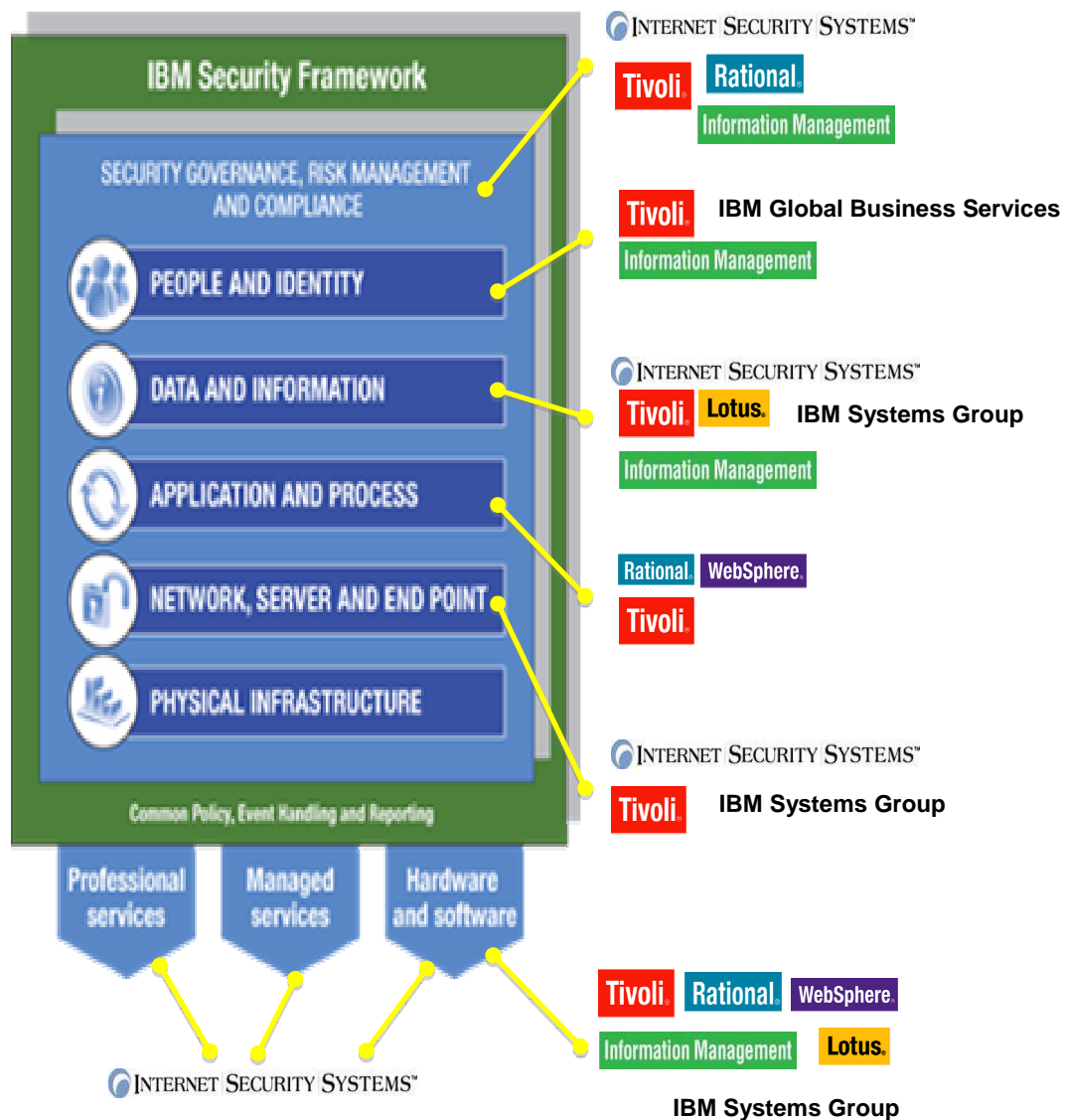
System access
Revoked (may be by date) No Statistics
Inactive, revoked or pending Yes Creation date 29Sep05
Days of week user can logon SMTWTES Last RACINIT current connects 11Sep07
Time of day user can logon User's last use date 11Sep07
Date user will be revoked (ddmmyyyy or NORESUME) 10:46
Date user will be resumed (ddmmyyyy or NORESUME)

Password
Has a password Yes Password phrase No
Expired password No Expired password phrase No
Password changed date 29Sep05 Password phrase change date
Password expiration date Password phrase expiry date
Old passwords present # 0 Old pass phrases present # 0
Failed password attempts # 0
Password interval
Password interval in effect
Mixed case password No

Command ==> _ Scroll==> CSR
  
```

**Viajar por el tiempo desde 1982 a hoy!**

# Framework de Seguridad de IBM



- Medir grado de conformidad con soluciones Tivoli
- Otras Soluciones para el cumplimiento normativo
- Casos de éxito en la gestión de accesos

# Gestion de Passwords

## Ministerio en Italia

- 20 aplicaciones por usuario
- expuestos a normas de protección de datos por mal uso de credenciales
- un pobre control de accesos



## Tivoli Compliance Value Proposition

Tivoli software BUILDING A SMARTER PLANET WITH A DYNAMIC INFRASTRUCTURE IBM  
**Simple Business Case**  
 (No discounting)

**"The average 10,000 user company spends \$1 to \$4 million on password resets per year."**  
Steve Hunt VP, Giga Information Group

Annual Password Resets Per Employee	Annual P/W Reset Cost Per Employee	Payback Period – Standard (\$69/user)	Year One ROI – Standard (\$69/user)	Payback Period – Suite (\$99/user)	Year One ROI – Suite (\$99/user)
2	\$50	16.6 months	73%	23.8 months	51%
4	\$100	8.3 months	145%	11.9 months	101%
6	\$150	5.6 months	215%	8.0 months	150%
8	\$200	4.2 months	286%	6.0 months	200%
10	\$250	3.4 months	353%	4.8 months	250%

➔ **Average reset cost per incident: \$25**

© 2008 IBM Corporation

## Single Sign On – business need

- Password management
  - Too many - complexity – policies (from "support" view)
  - Control + management : growing needs
  - Link to other department/applications (HR, TD, Med. Dept.)
  - €
- Login speed on shared pc + session management
- 1º step to identity & access management



## Single Sign On – business need

- Security
  - Too many – complexity (from "end user" view)
  - Use of 
  - Anybody sharing any user id
  - Use of default password
  - No log off

• Redujo carga del departamento IT en gestión de passwords

• Evitar fuga de datos sensibles

• Mejora productividad y satisfacción del usuario medical



# MUCHAS GRACIAS

*Emmanuel Roeseler : Southwest Tivoli Security Sales Leader  
Emmanuel\_roeseler@es.ibm.com*