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 exito en la gestión de accesos**

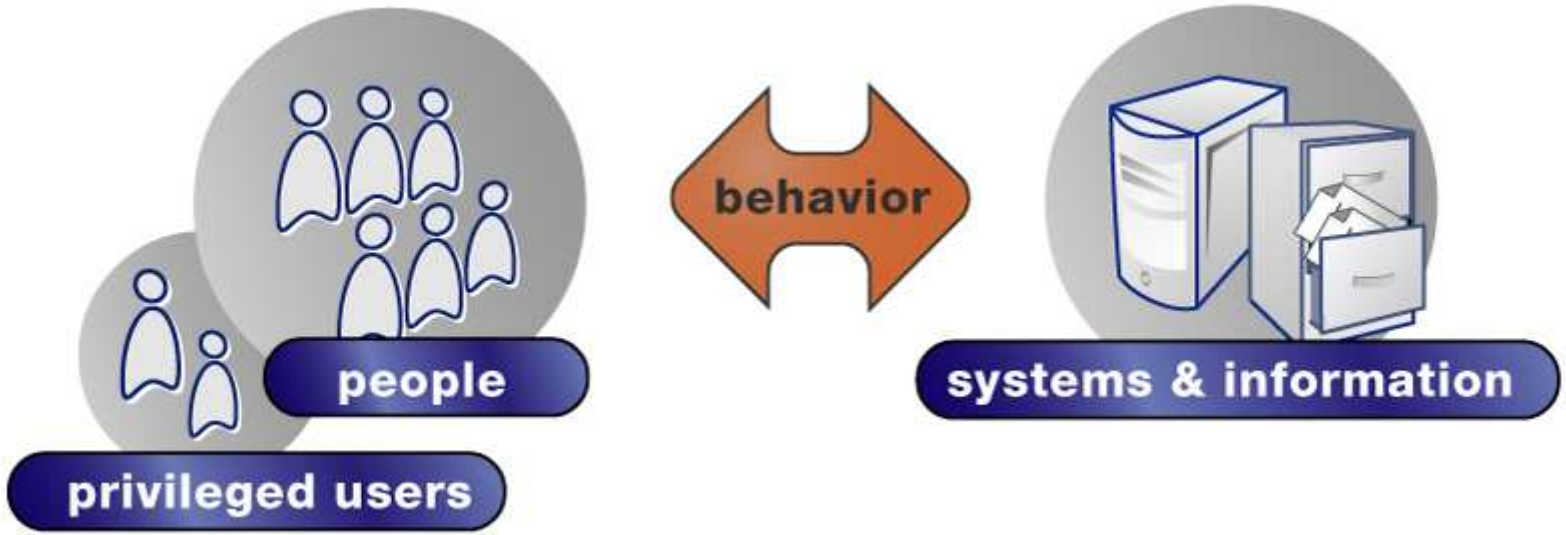
Auditoria de Identidad

- **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 aplicaciónes accedió el usuario?**

¿QUE FALTA?

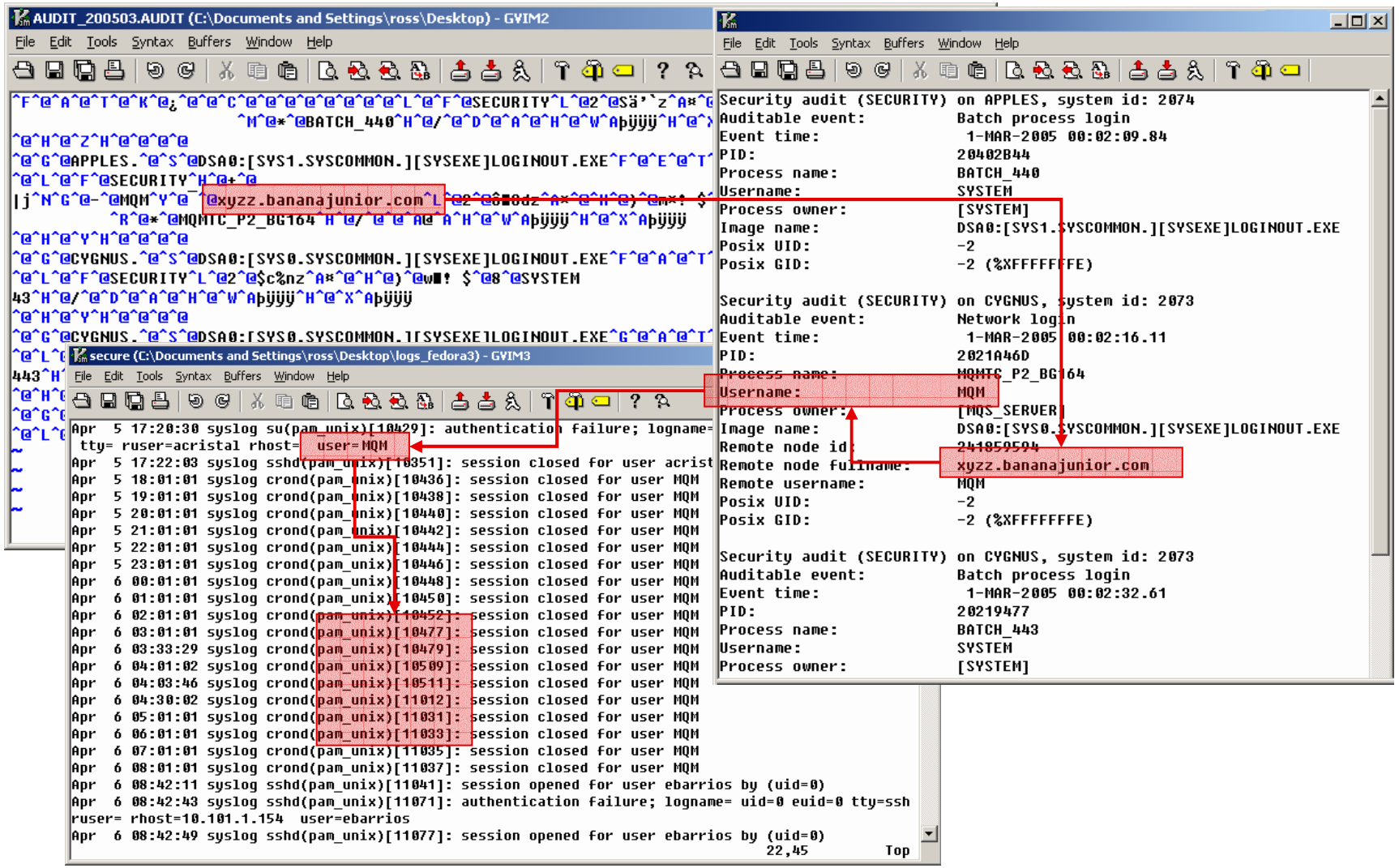
- **Auditoria de acceso al dato**
- **Correlar acciones**
- **Auditoria de la actividad en las aplicaciones**
- **Determinar que es “normal” y que no lo es**
- **Identificar comportamientos anómalos y riesgos potenciales**

¿Qué esta haciendo la gente en Mi Red?

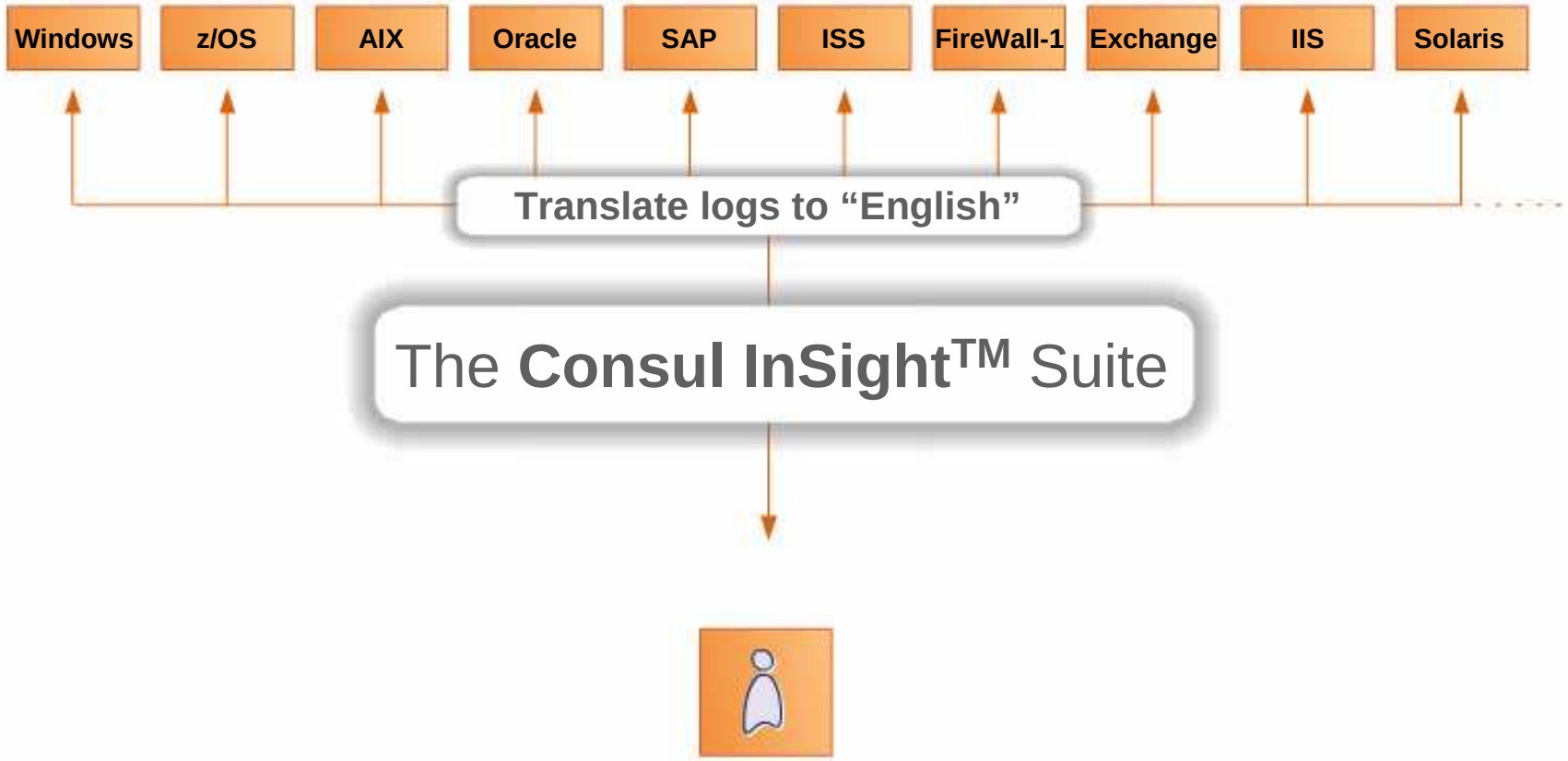


El 87% de los ataques internos están causados por usuarios privilegiados y técnicos.

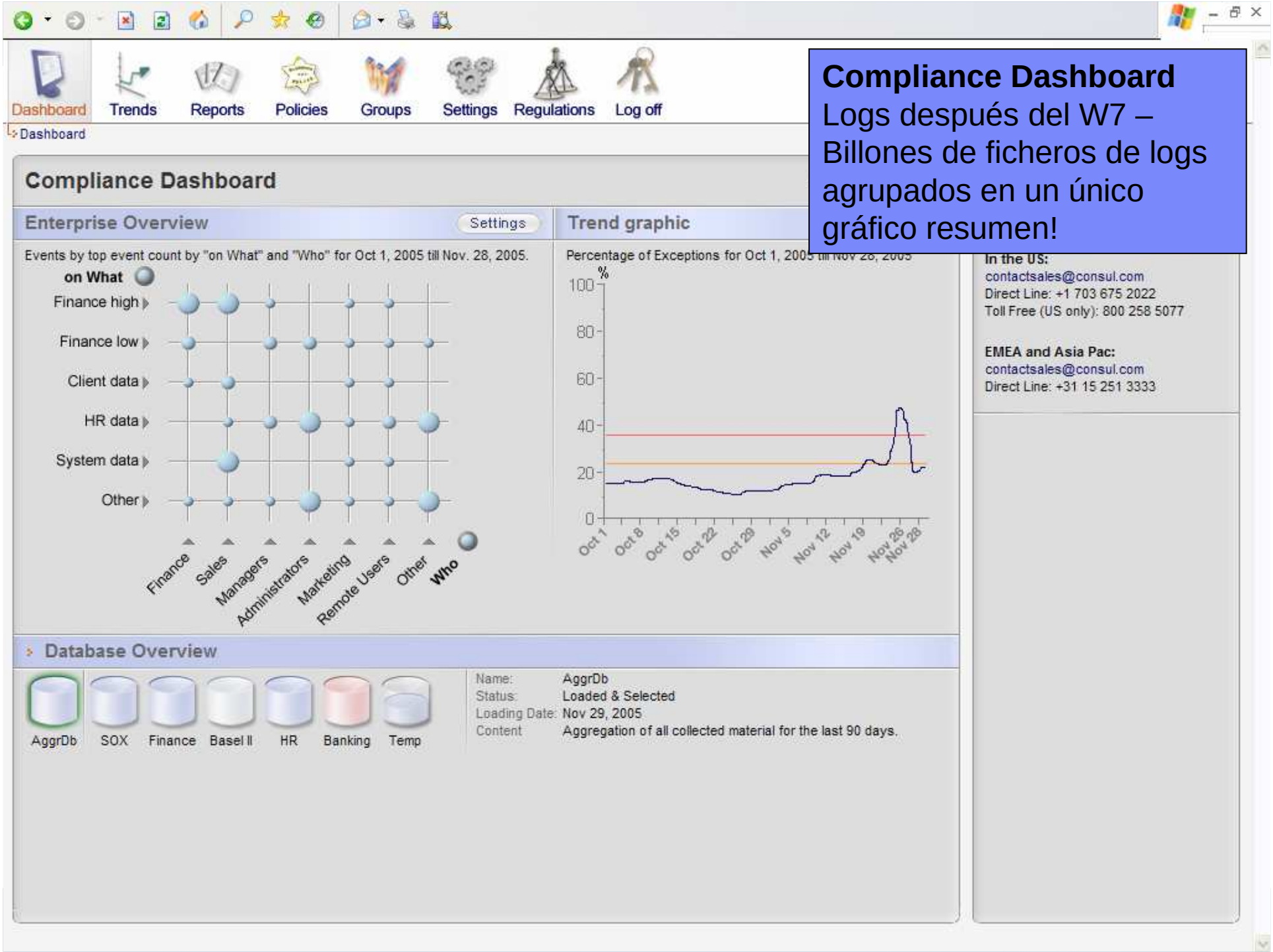
¿Como doy sentido a todo esto?

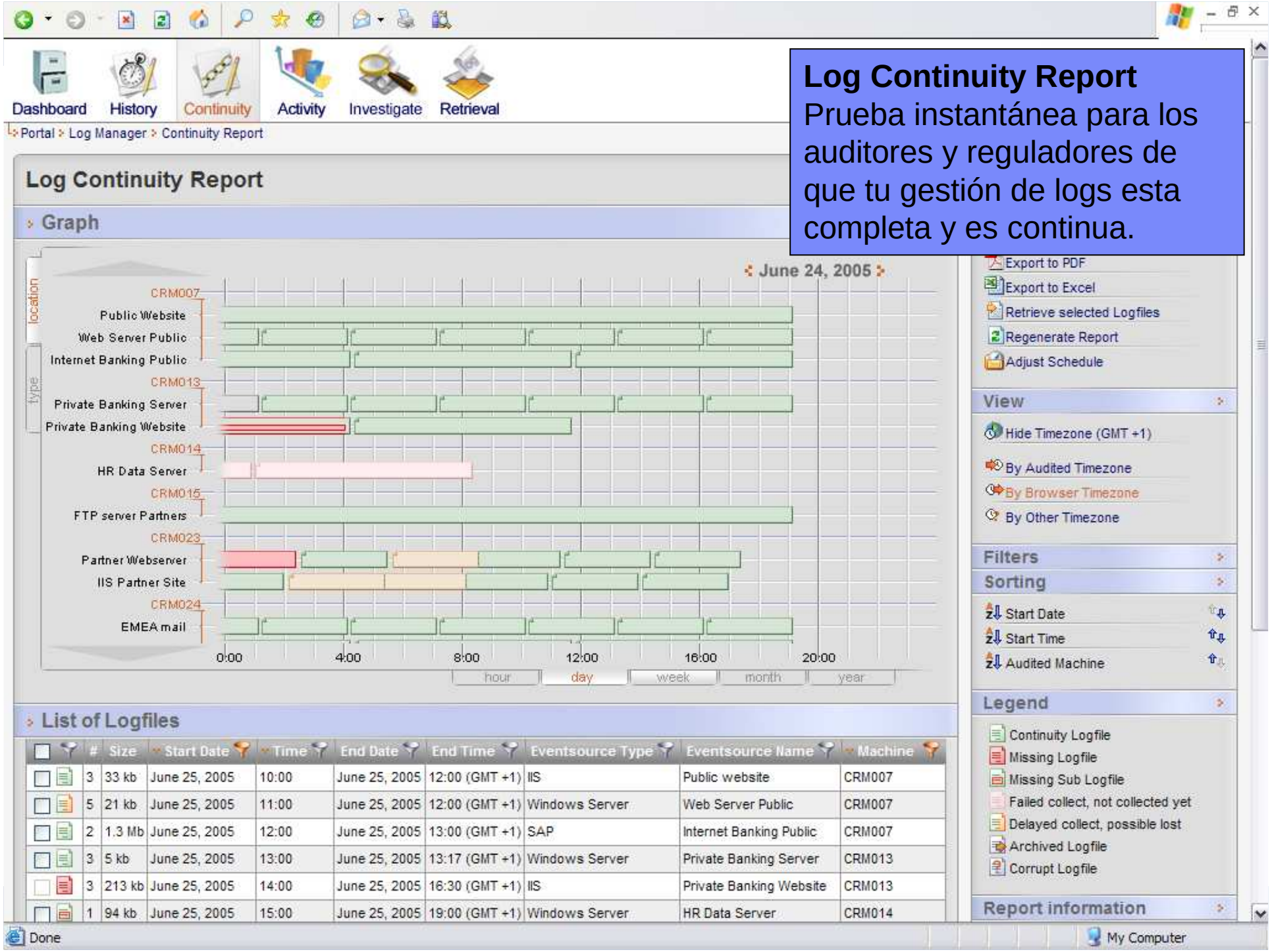


Ahora los log de tu empresa en un único lenguaje

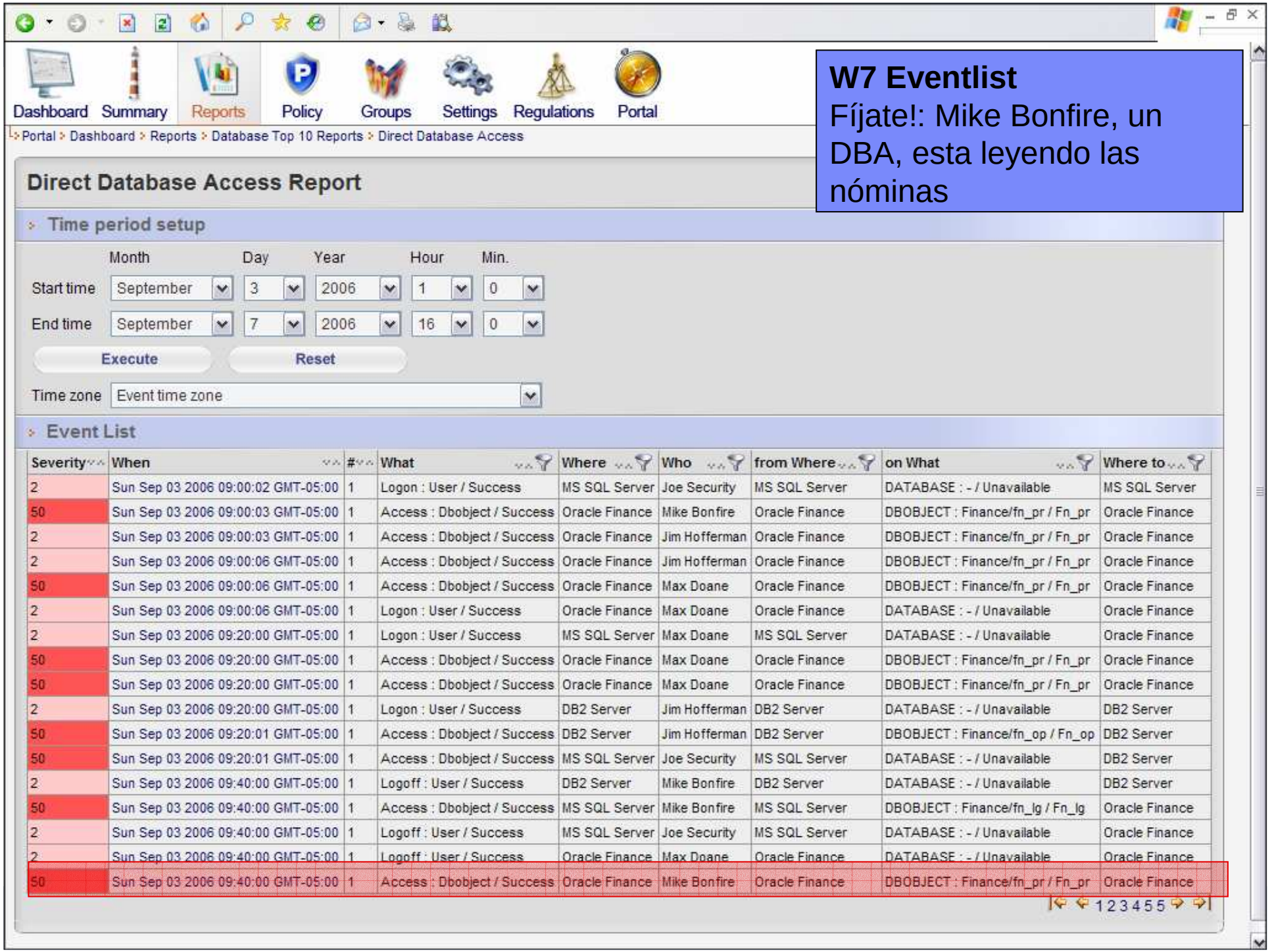


Tivoli Compliance InSight Manager ahorra tiempo y dinero a tu departamento de seguridad de la información y cumplimiento mediante la automatización de la monitorización a través de la empresa.


Dashboard
Trends
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard
Compliance Dashboard
Logs después del W7 – Billones de ficheros de logs agrupados en un único gráfico resumen!
Compliance Dashboard
Enterprise Overview
Settings
Events by top event count by "on What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.
on What
Finance high
Finance low
Client data
HR data
System data
Other
Finance
Sales
Managers
Administrators
Marketing
Remote Users
Other
Who
Trend graphic
Percentage of Exceptions for Oct 1, 2005 till Nov 28, 2005
%
100
80
60
40
20
0
Oct 1
Oct 8
Oct 15
Oct 22
Oct 29
Nov 5
Nov 12
Nov 19
Nov 26
Nov 28
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 15 251 3333
Database Overview
AggrDb
SOX
Finance
Basel II
HR
Banking
Temp
Name: AggrDb
Status: Loaded & Selected
Loading Date: Nov 29, 2005
Content Aggregation of all collected material for the last 90 days.

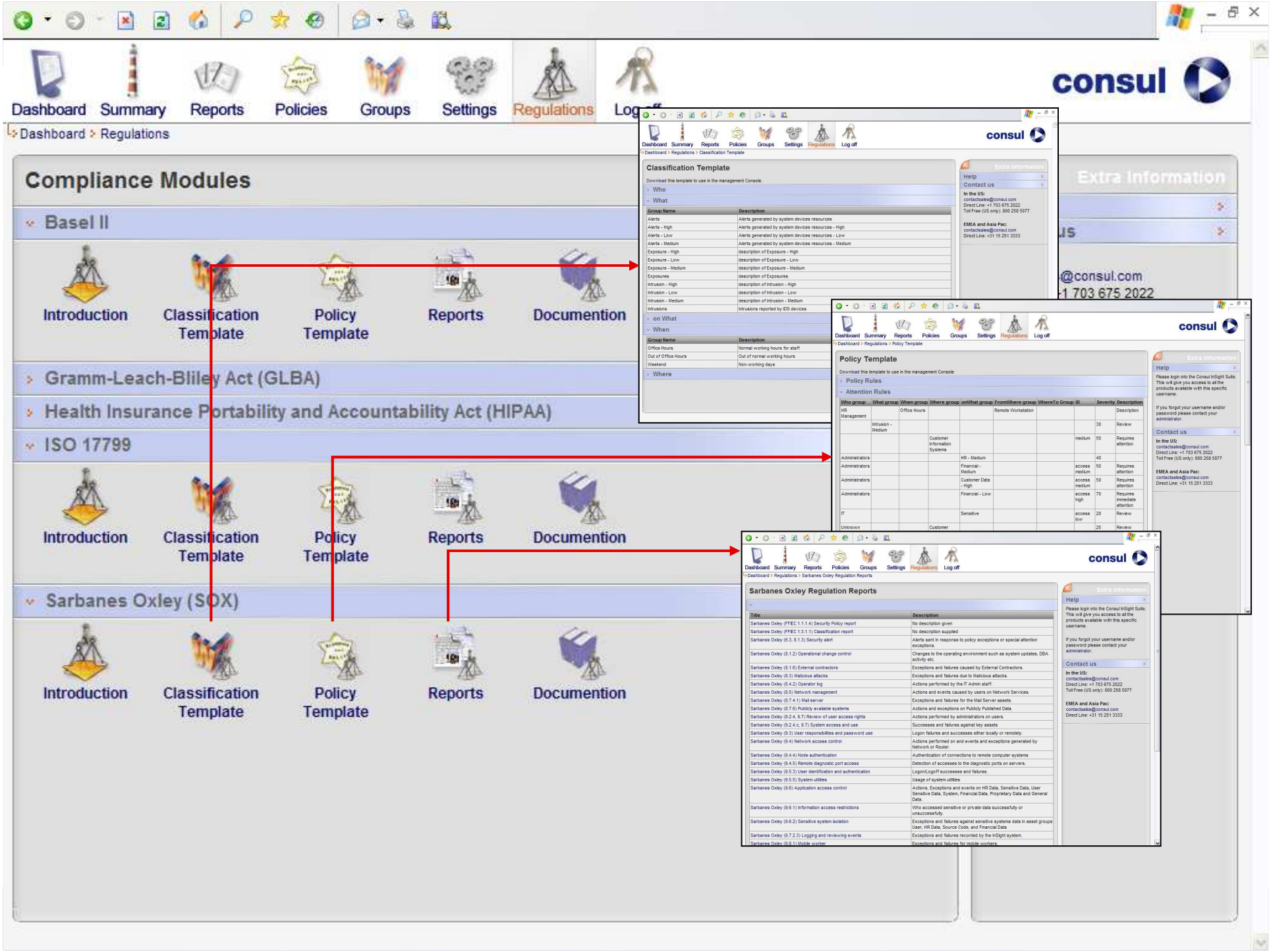


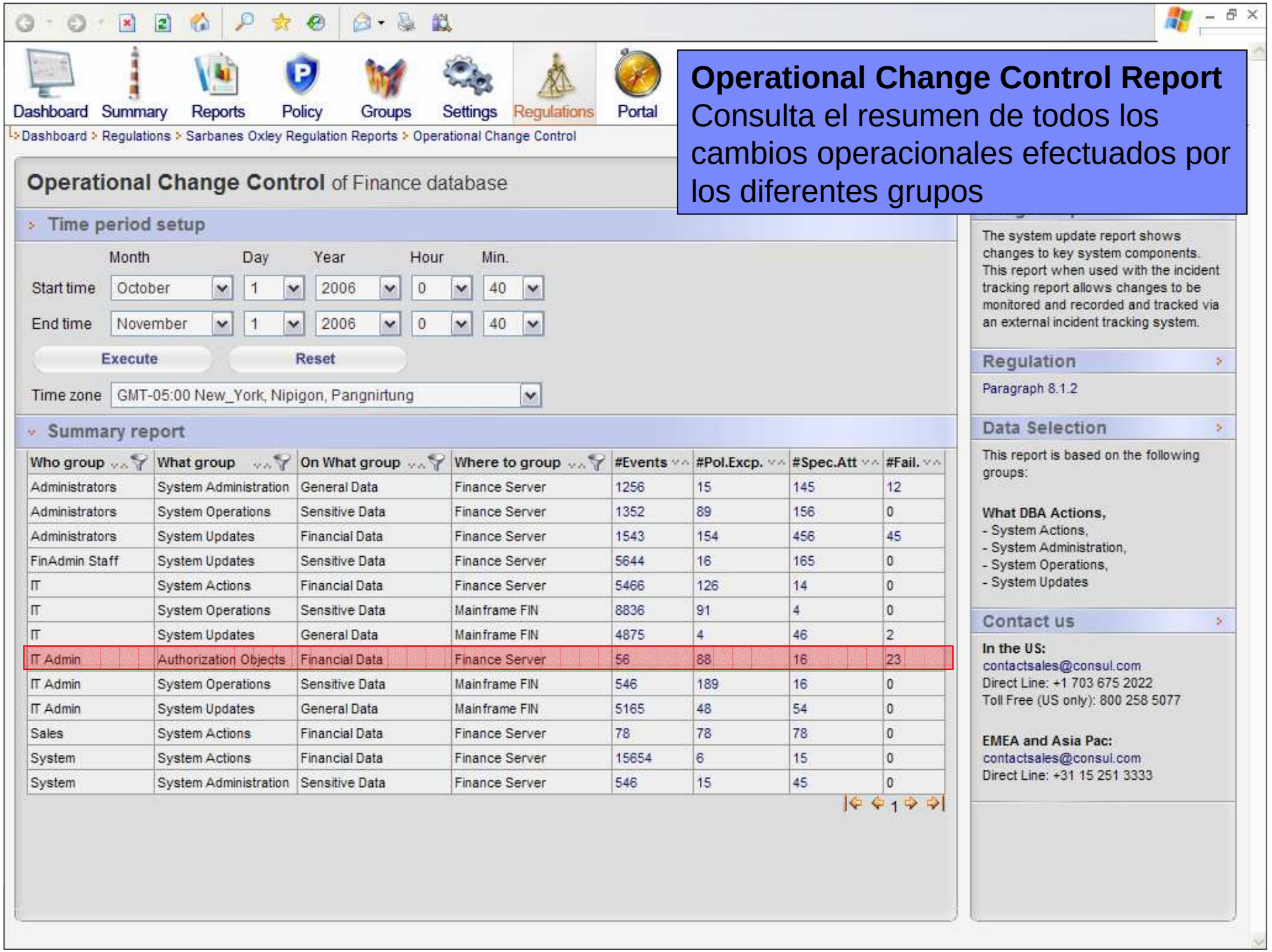
Log Continuity Report
Prueba instantánea para los auditores y reguladores de que tu gestión de logs esta completa y es continua.



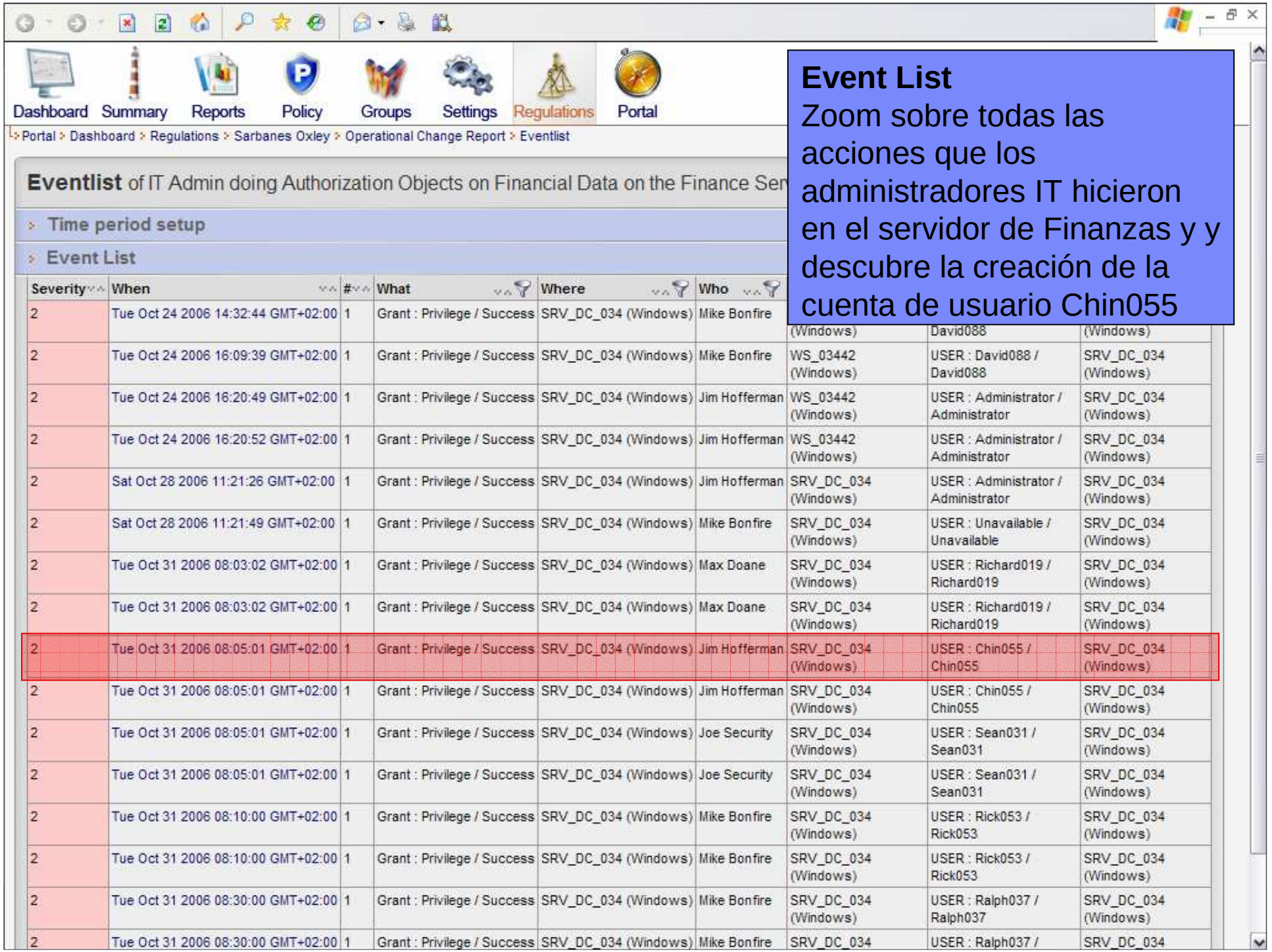
W7 Eventlist

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


Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
consul
Dashboard > Regulations
Compliance Modules
Basel II
Introduction
Classification Template
Policy Template
Reports
Documention
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
ISO 17799
Introduction
Classification Template
Policy Template
Reports
Documention
Sarbanes Oxley (SOX)
Introduction
Classification Template
Policy Template
Reports
Documention
Extra Information
Classification Template
Policy Template
Sarbanes Oxley Regulation Reports

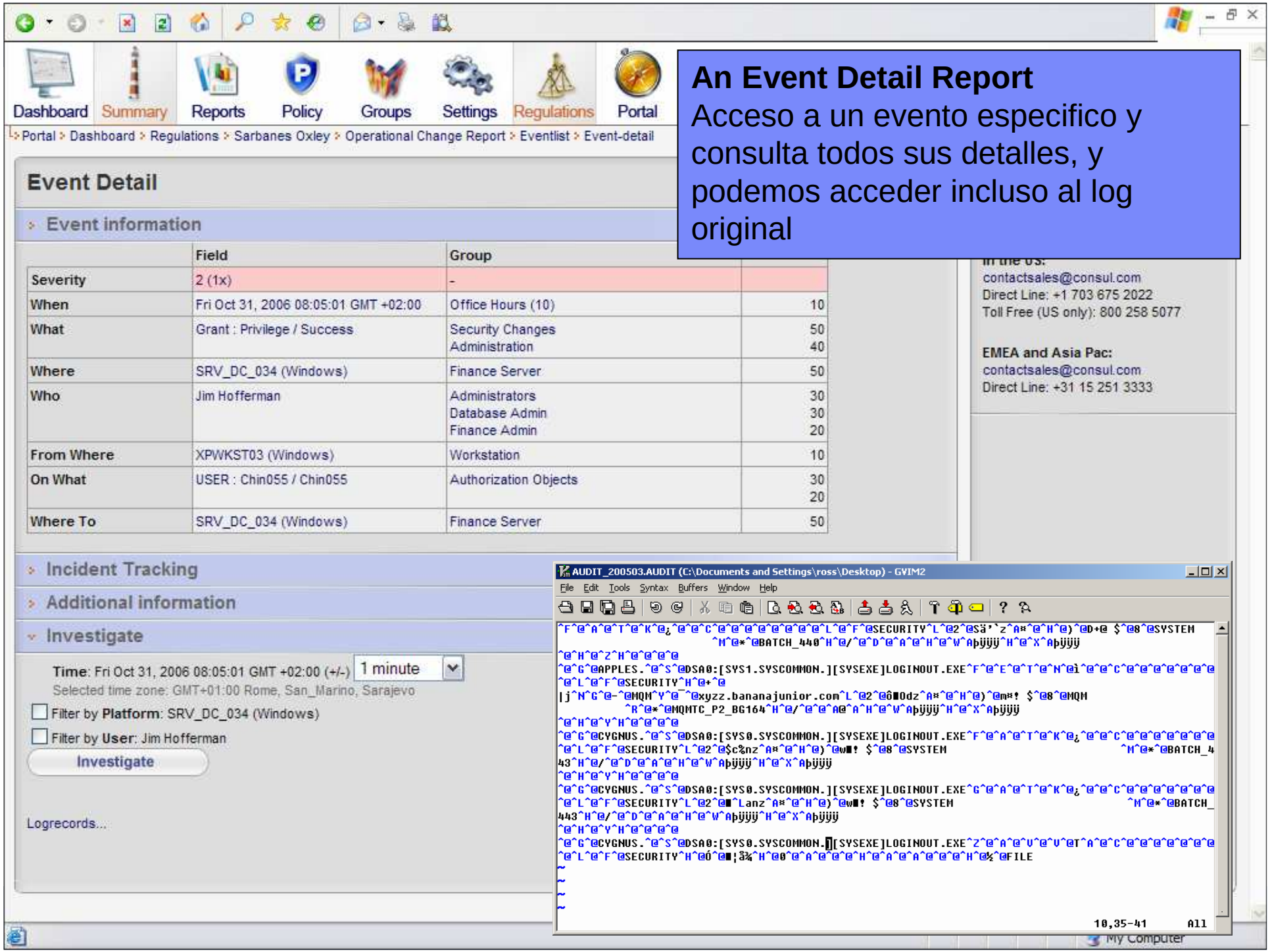


Operational Change Control Report
Consulta el resumen de todos los cambios operacionales efectuados por los diferentes grupos



Event List

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



An Event Detail Report

Acceso a un evento especifico y consulta todos sus detalles, y podemos acceder incluso al log original

Framework de Seguridad de IBM

- Medir grado de conformidad con soluciones Tivoli
- **Otras Soluciones para el cumplimiento normativo**
- Casos de exito 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***

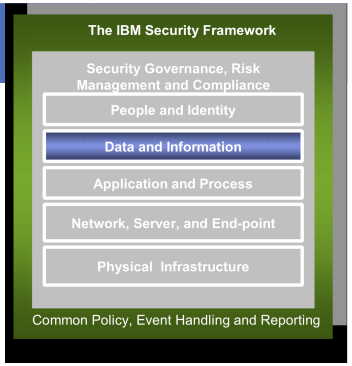
Smash the disk drive

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

Professional offsite disposal services

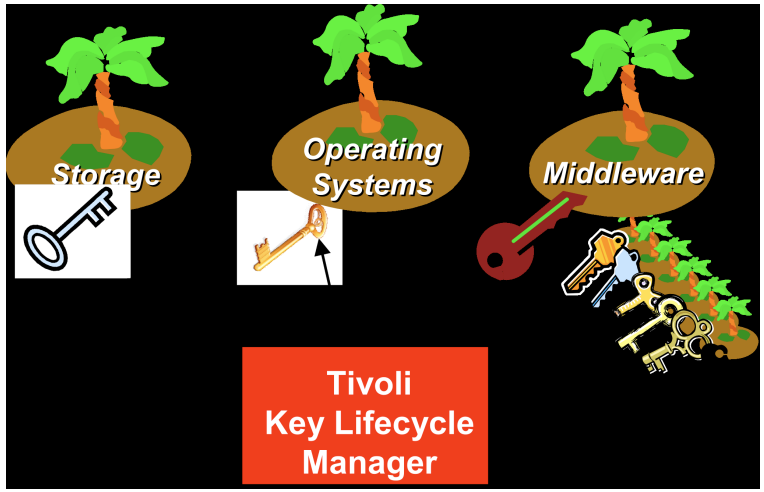
- *Drive is now exposed to the tape's falling-off-the-truck issue*

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

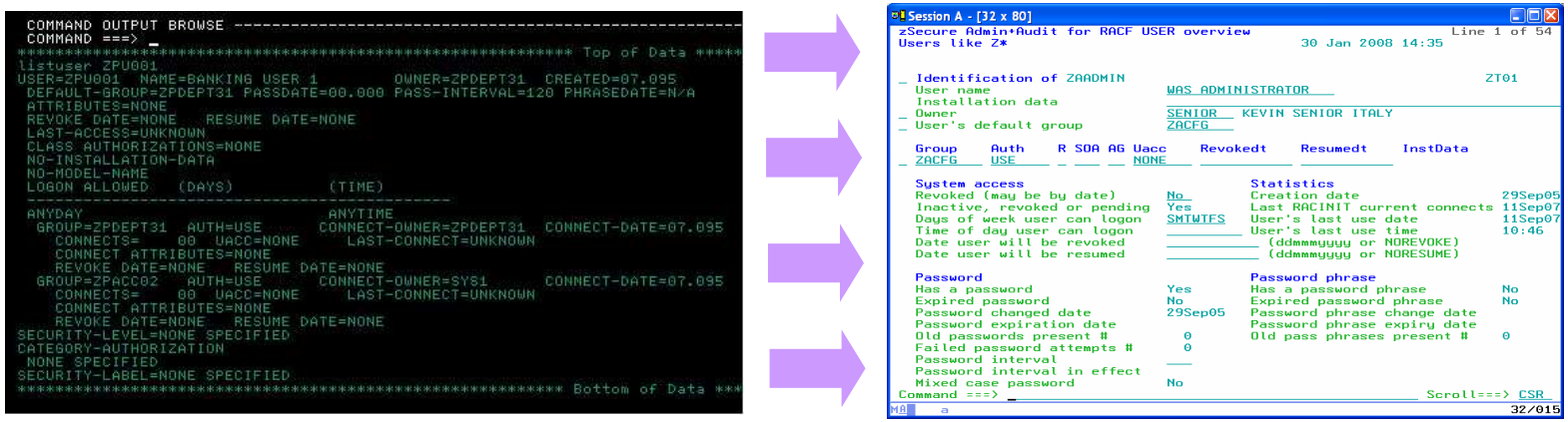


Beneficios

- **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:



Viajar por el tiempo desde 1982 a hoy!

Framework de Seguridad de IBM

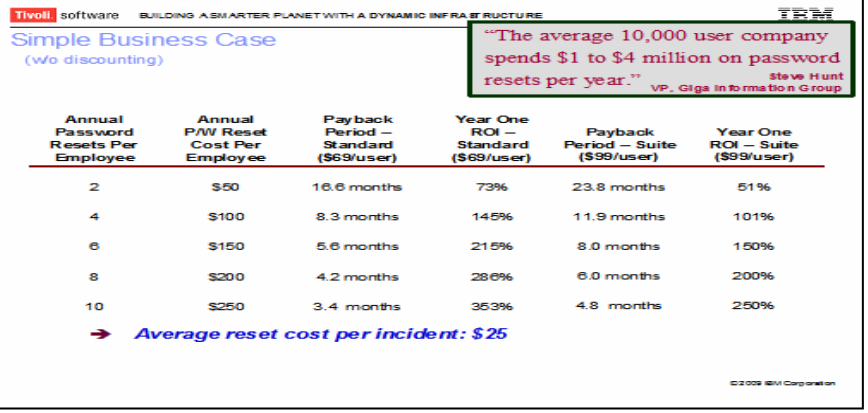
- Medir grado de conformidad con soluciones Tivoli
- Otras Soluciones para el cumplimiento normativo
- **Casos de exito en la gestión de accesos**

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



- **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