IBM Tivoli IAM Governance

Juan Nemiña Gantes

juannemina@es.ibm.com

Seguridad y servicio en el Sector Público

Posibilitar el despliegue de servicios seguros controlando el coste y el riesgo procedente tanto de usuarios internos como de usuarios externos y protegiendo los datos confidenciales de la corporación y del usuario

Verificar Identidad

Partners…
Service providers…
Patients...
Doctors...
Specialists…
Employees...

Gestionar Acceso

Securizar Servicios

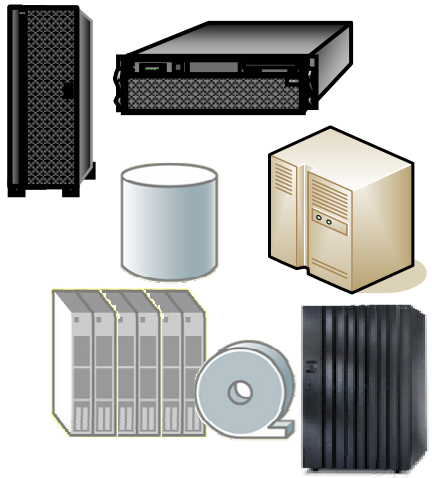
Aplicaciones Internas

Relación con otras entidades

Acceso de Proveedores

Acceso del ciudadano

Proteger Datos



Problemáticas comunes

Cumplir normativas y ofrecer mas servicios… Controlando el coste, manteniendo la calidad del servicio y proporcionando acceso rápido y seguro a aplicaciones y datos

- **Nuevas aplicaciones**
- **Gestión de contraseñas**
  - De 8 a 10 contraseñas en promedio por usuario
- **LOPD**
- **Reducción de costes de HelpDesk**
  - El reset de contraseñas es un 25% de la actividad del HelpDesk
  - Mejora de la eficiencia y productividad
- **Acceso seguro y rápido**
  - Muchos datos gestionados son confidenciales. Los usuarios son profesionales de su actividad, no guardianes de datos.
  - Usuarios temporales: Subcontratación, suplencias, etc…necesidad de asignar y retirar accesos temporales de forma rápida y eficiente
- **Movilidad**
  - Usuarios desplazandose entre centros, entre plantas, etc. Necesidad de acceso desde distintas estaciones de trabajo, en muchas ocasiones compartidas.

Visión de IBM para solventar esta problemática

Solución centralizada de Gestión de Identidades y Políticas

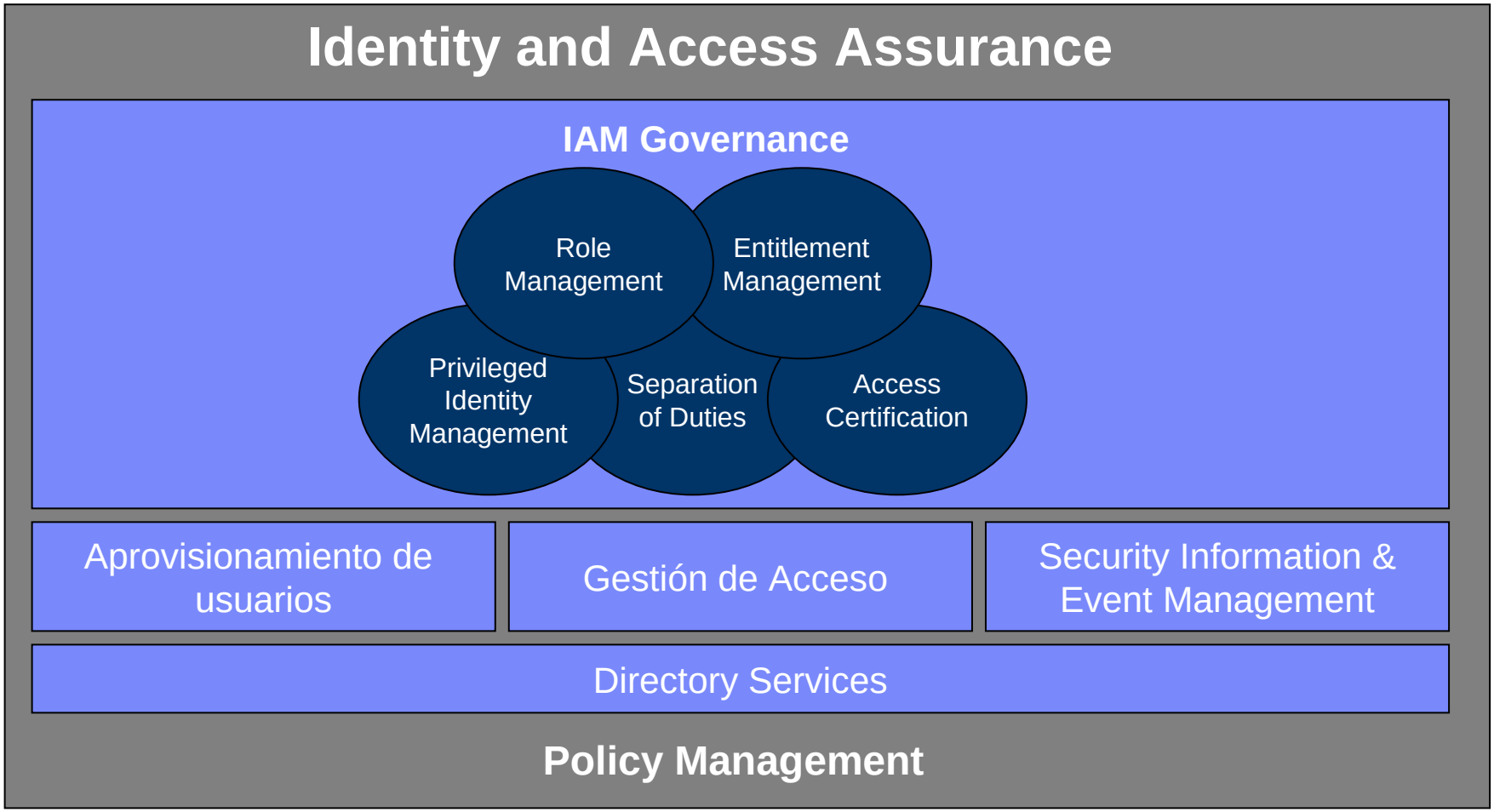
Reduccción de costes y mejora de productiviad mediante la automatización de los procesos de aprovisionamiento y el autoservicio

Acceso seguro y rápido mediante mecanismos de autenticación fuerte combinado con SSO. Reducción de pérdidas de contraseña

SSO y cambio rápido de sesión en estaciones de trabajo multi-usuario y combinado con autenticación fuerte si se desea.

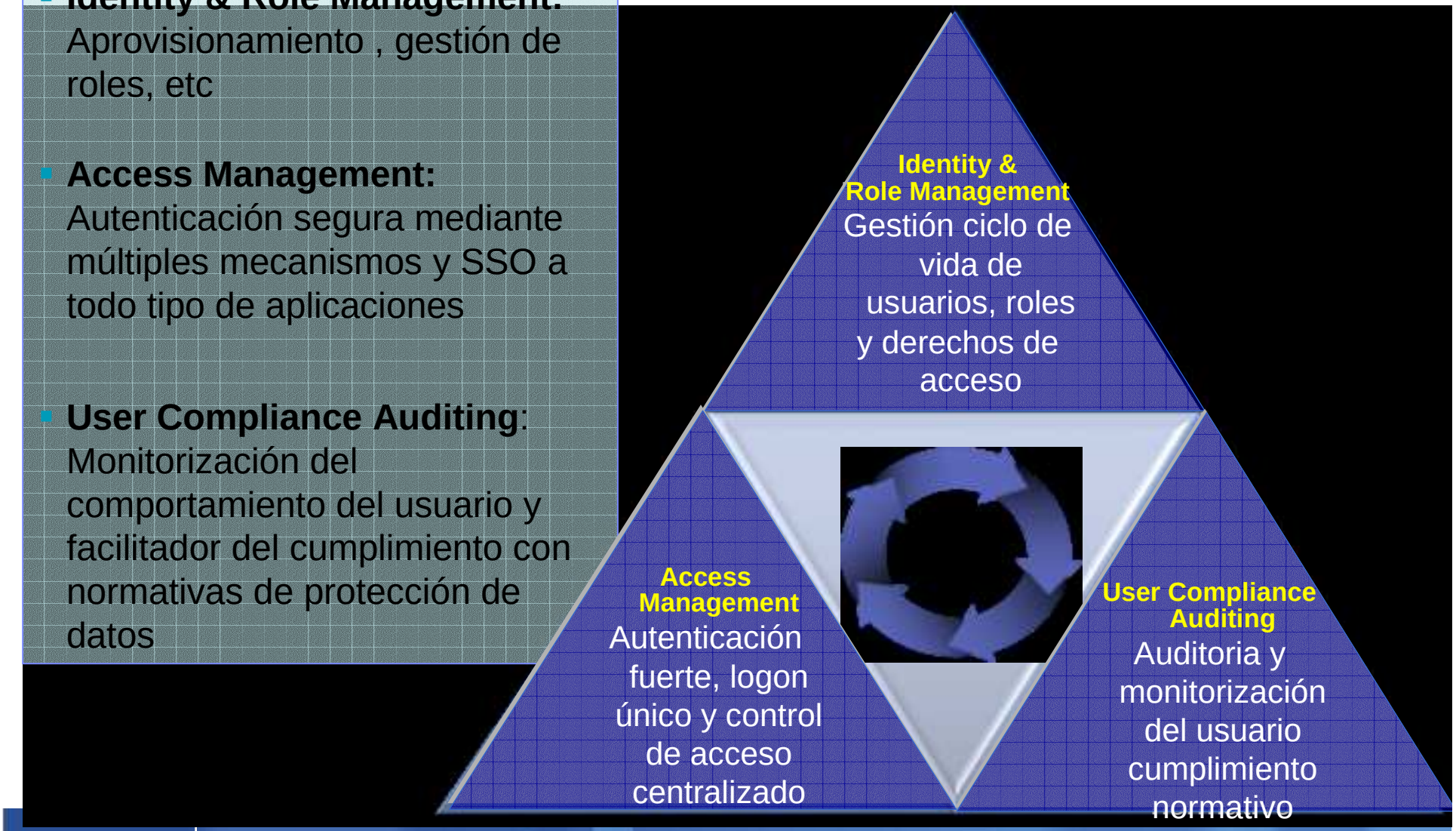
Monitorización y auditoria del comportamiento del usuario.

Tivoli Identity and Access Assurance



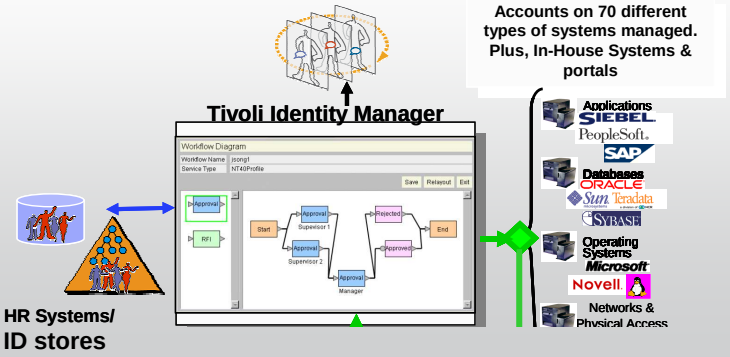
Tivoli Identity and Access Assurance

- **Identity & Role Management:** Aprovisionamiento , gestión de roles, etc
- **Access Management:** Autenticación segura mediante múltiples mecanismos y SSO a todo tipo de aplicaciones
- **User Compliance Auditing**: Monitorización del comportamiento del usuario y facilitador del cumplimiento con normativas de protección de datos



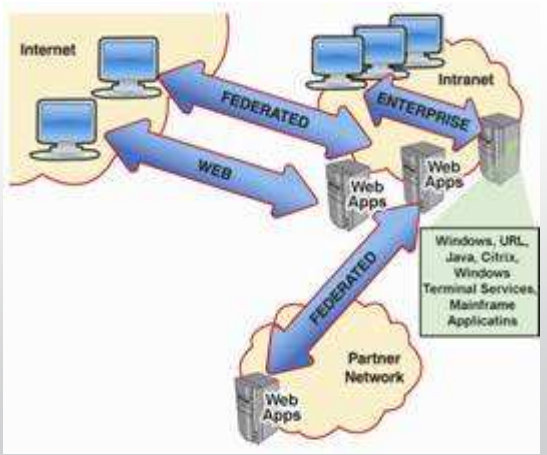
Identity and Access Assurance

User Provisioning / Role Management

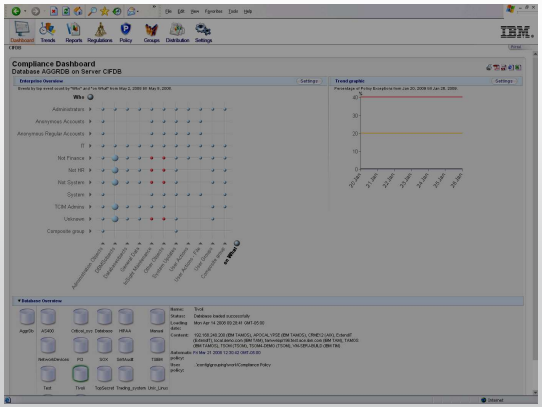


Single Sign On

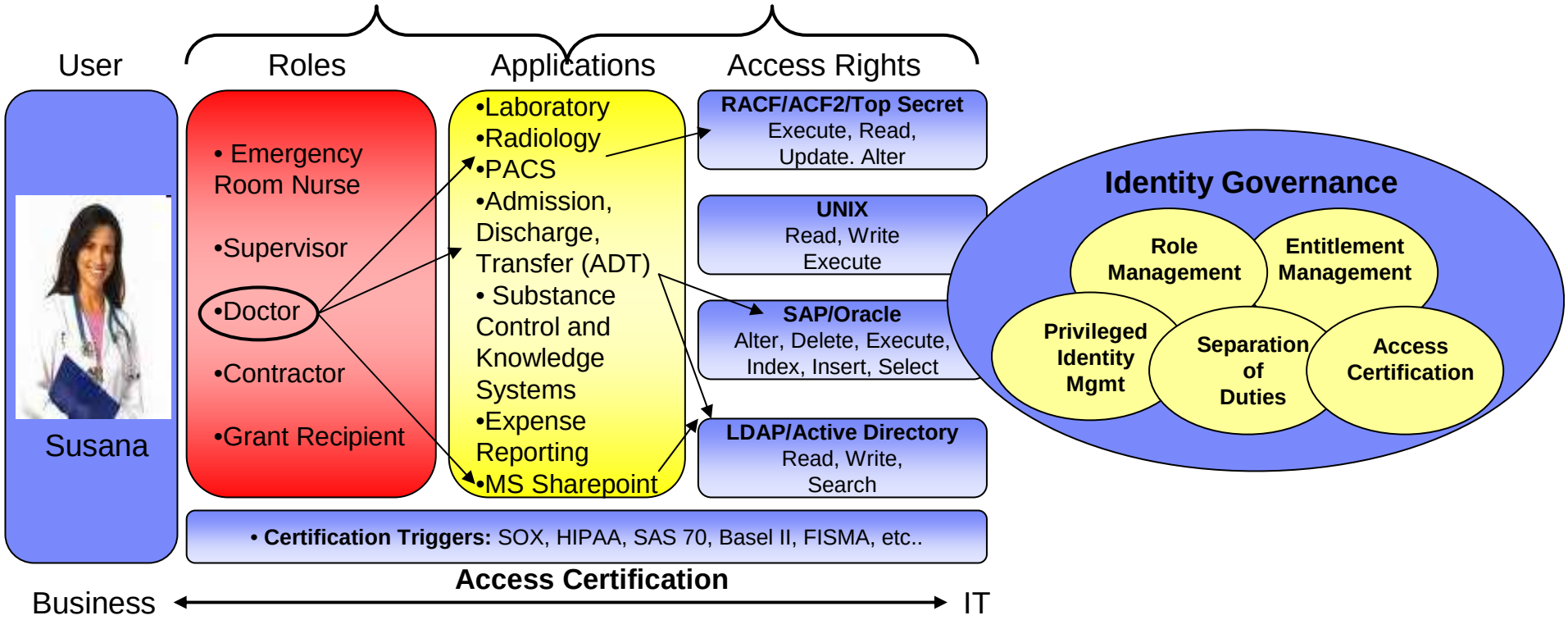
& Password Management



Security log management & reporting



Ejemplo de Identity Governance en acción



Ejemplo: JK Enterprise Hospital

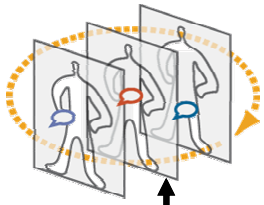
- El rol de Doctor implica que Susana necesita acceso a las aplicaciones de Radiologia, ADT y Sharepoint
- Ello implica que Susana necesita un usuario en AD, RACF y SAP
- Los usuarios de Susana se crean automáticamente con los accesos necesarios
- La pertenencia de Susana al rol de Doctor se chequea (es re-certificado) periódicamente

Tivoli Identity Manager gestiona el ciclo de vida del usuario

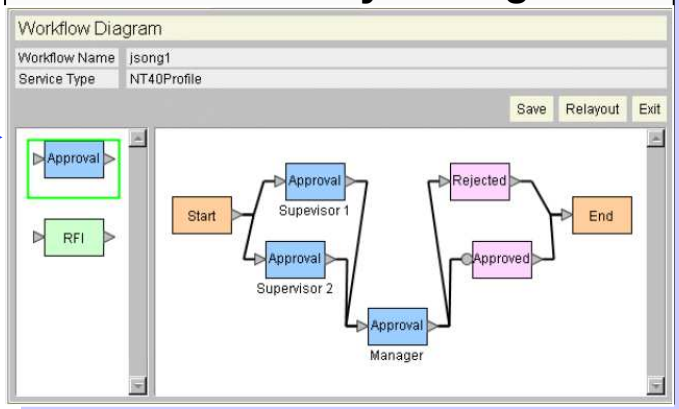
Cambio en personal (add/del/mod) → **Evaluación políticas de acceso** → **Circuito de aprobación** → **Actualización cuentas**

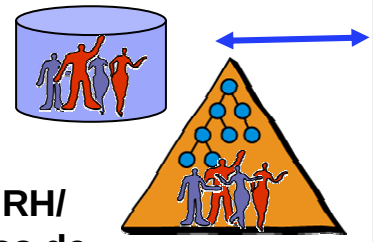
Detecta y corrige privilegios establecidos localmente

Aprovisionamiento basado en Politicas para toda la infrastructura IT



Tivoli Identity Manager





Sistemas RH/ Repositorios de Usuarios

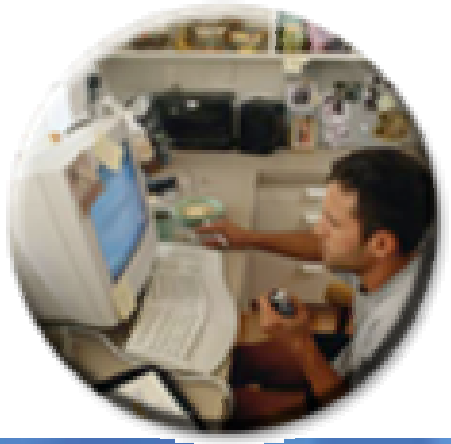
Gestión de cuentas en 70 tipos distintos de sistemas, aplicaciones de negocio, portales, etc

Applications
SIEBEL
PeopleSoft
SAP
Databases
ORACLE
Sun
Teradata
SYBASE
Operating Systems
Microsoft
Novell.
Networks & Physical Access
Cisco Systems
ActivCard

IBM Tivoli Identity Manager v5.1 y IAM governance

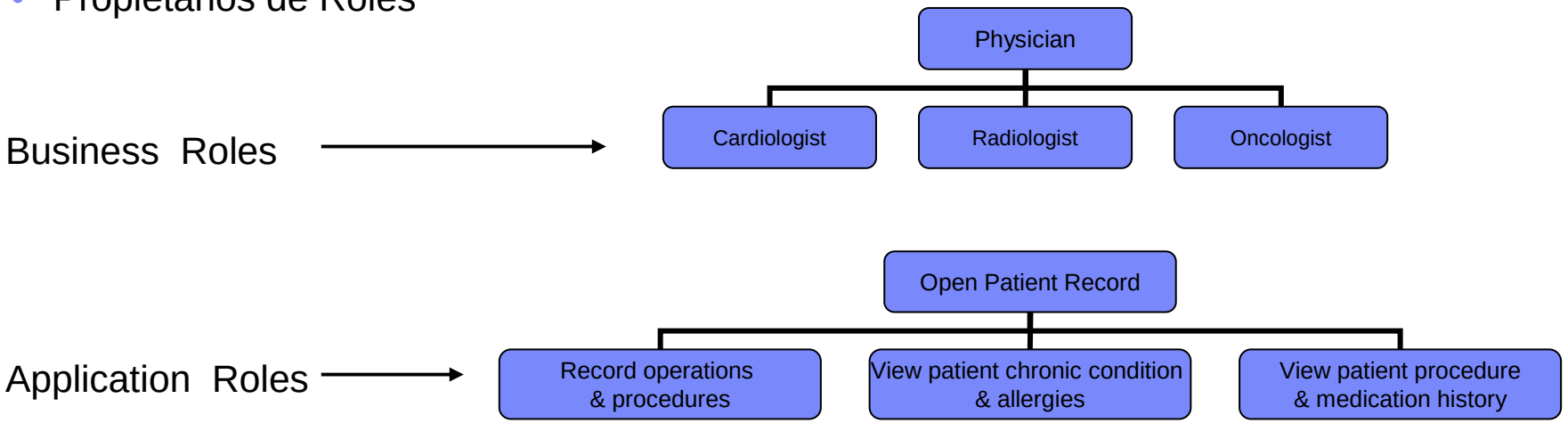
IBM Tivoli Identity Manager v5.1	
Funcionalidad	**Beneficio**
Roles Jerárquicos	Simplifica la definición y la visibilidad de los accesos del usuario
Segregacion de deberes	Fortalece la seguridad y la conformidad previniendo conflictos entre los procesos de negocio
Re-certificación de Accesos	SImplifica la gestión del ciclo de vida de los accesos del usuario dentro y fuera del mapa de roles garantizando el cumplimiento
Gestión de grupos	Simplifica la administración de nuevos permisos
Informes de Cumplimiento	Facilita el cumplimiento, permite el análisis

Asistentes para la gestión de Roles	
Role Modeling Assistant	Role Management Assistant
Descubrimiento, Mineria e Ingenieria de Roles	Gestión del ciclo de vida de Roles



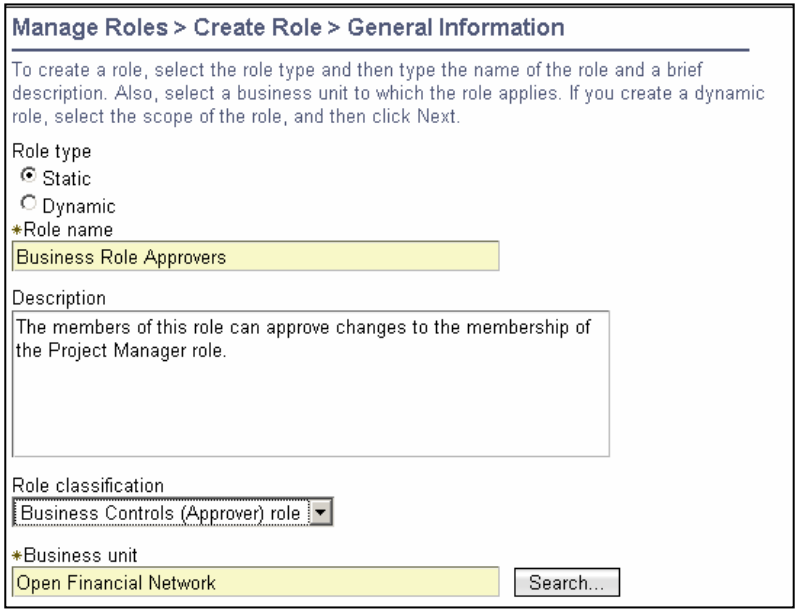
Roles jerárquicos simplifica la definición del mapa de roles

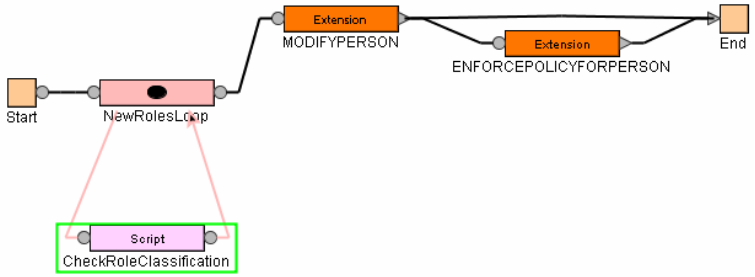
- **Capacidades TIM**
  - Establecimiento de relaciones padre/hijo entre roles y aplicación de herencia a través de la relación de pertenecia
    - Capacidad de añadir y retirar roles como miembreo de otros roles
  - Los Roles padre pueden tener múltiples jijos
    - Medico = role padre
    - Cardiologo, Radiologo = roles hijo
  - Los Roles hijo pueden tener múltiples padres
    - Cardiologo = role hijo
    - Medico, Empleado = roles padre
  - La herencia se aplica a todos los objetos/procesos que usan roles
    - Provisioning policy
    - Aprobaciones
    - Propietarios de Roles



Tipificacíon o clasificación de Roles

- **Capacidades TIM**
  - ***Tipificación de Roles*** clasificación de roles, no solo desde el punto de vista organizativo sino para el uso en los flujos de trabajo y la particularización de políticas
  - Tipos de role “por defecto” son: business and application, típicamente
    - ***Roles de negocio*** relacionados con el tipo de trabajo que una persona hace
    - ***Roles de Aplicación*** relacionados con el tipo de acceso que una persona necesita
  - Se permite la definición de tipo adicionales de roles
  - El tipo de role se consulta en los flujos de trabajo y aprobación para permitir la uso de flujos comunes con acciones diferenciadas

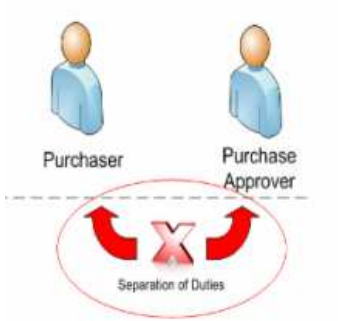




Segregación de deberes para mejorar la seguridad y la conformidad

- **Segregación de deberes (SoD)**
  - Habilidad para impedir que los usuarios tengan derechos de acceso que puedan generar conlictos en el negocio

- **Capacidades TIM**
  - Proporciona detección y control preventivo sobre conflictos de roles mediante la creación/modificación/borrado de politicas que evitan que el usuario perteneca a distintos roles que pueden generar conflictos de negocio, por ejemplo:
    - Usario no puede ser miembro del Rol A y Rol B al mismo tiempo
  - En los procesos de petición o asignación de acceso TIM detectará si hay reglas SoD aplicables y previene la ocurrerencia del conflicto
  - Los workflow de aprobación permiten la existencia de excepciones cuando ocurre una violación de la regla
  - Los informes proporcionan listas de violaciones y exenciones de las reglas para prevenir y monitorizar el uso inadecuado de privilegios



Separation of Duty Policy Violations

The request when adding members to the role Log Receipt of Medications on February 16, 2009 has caused separation of duty policy violations.

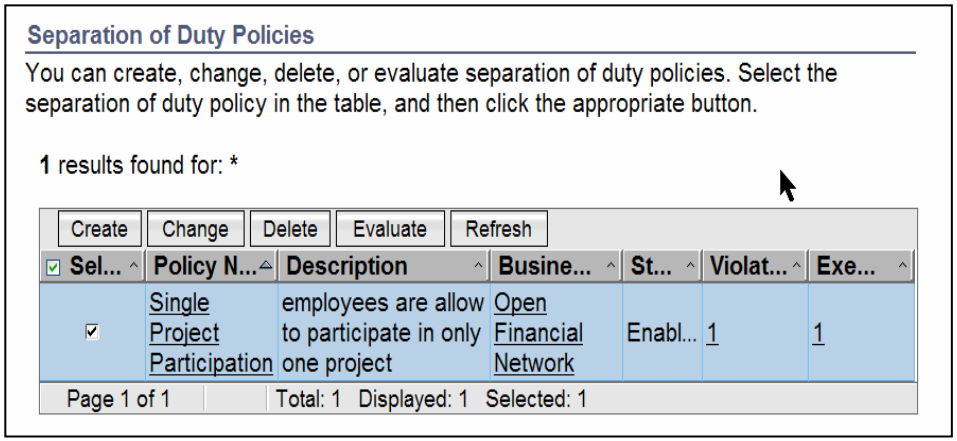
Separation of Duty Policy Violation Details

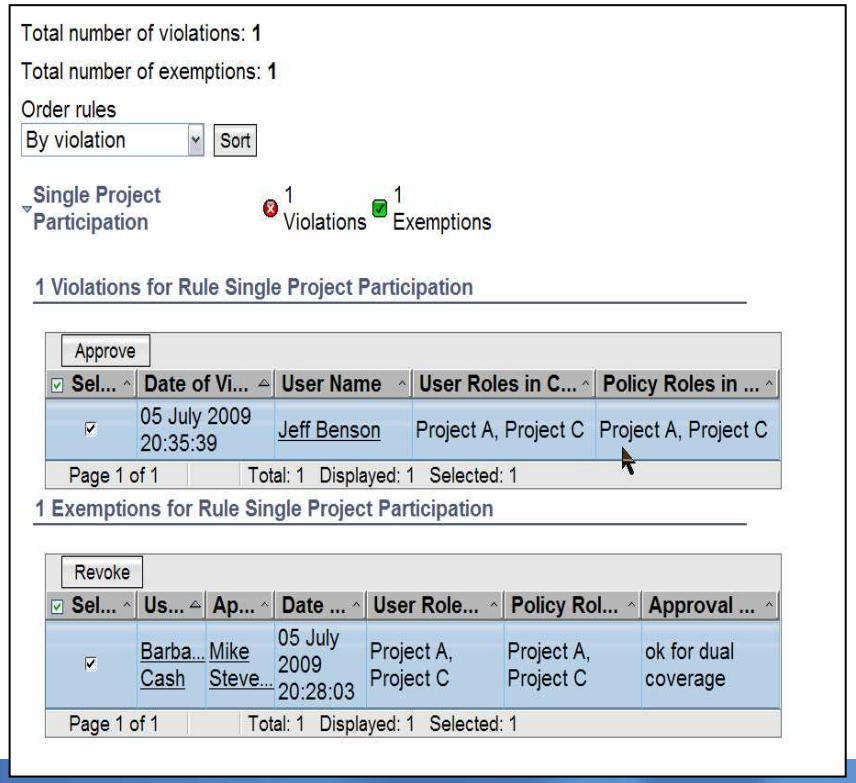
The separation of duty policy violation details are specified in the following table. Click Submit to add members to this role with separation of duty policy violations.

Person Name	Rule	Roles in Conflict
Judith Hill	Controlled Substances Inventory Mgmt	Log Receipt of Medications, Dispense Medication App Authority

Visibilidad de la exposición al riego mediante vistas de status de Políticas SoD

- **Cuadro de mandos de Administración**
  - Proporciona vista de status con la lista de violaciones detectadas y excepciones aprobadas
  - Vista de detalle “Drill down” para la revisión del conflicto y el status de excepción





Recertificacion de accesos en TIM

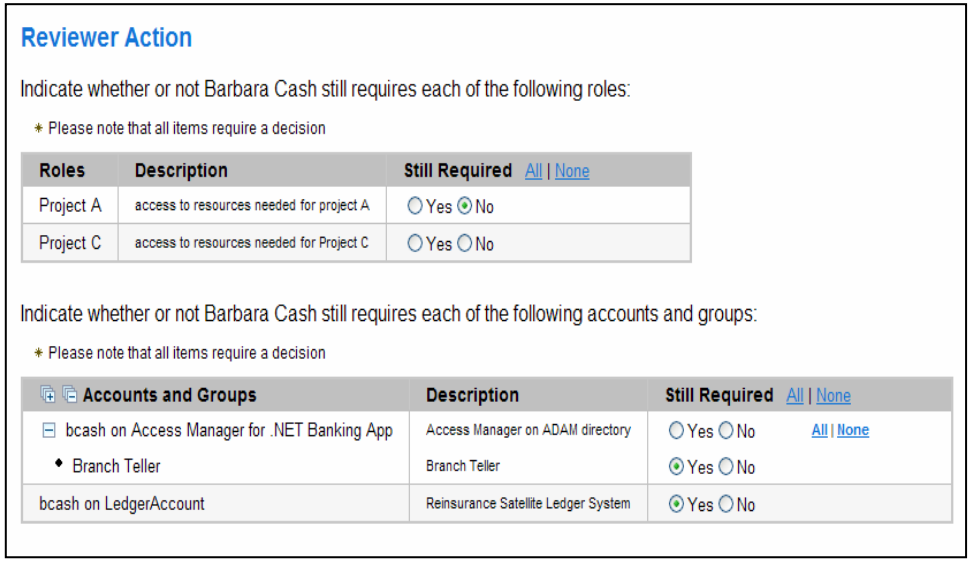
- **Capacidades TIM**
  - 3 tipos de políticas de recertificación para validar que los accesos a los recursos continuan siendo necesarios

1. Politicas de recertificación de cuentas

2. Políticas de recertificación de Accesos

3. Políticas de recertificación de Usuarios
   - Un tipo de proceso de certificación de que combina la certificación de los roles de un usuario, sus cuentas y la lista de grupos a la que pertenece en una sola operación

NEW



Reviewer Action

Indicate whether or not Barbara Cash still requires each of the following roles:

* Please note that all items require a decision

Roles	Description	Still Required All | None
Project A	access to resources needed for project A	Yes No
Project C	access to resources needed for Project C	Yes No

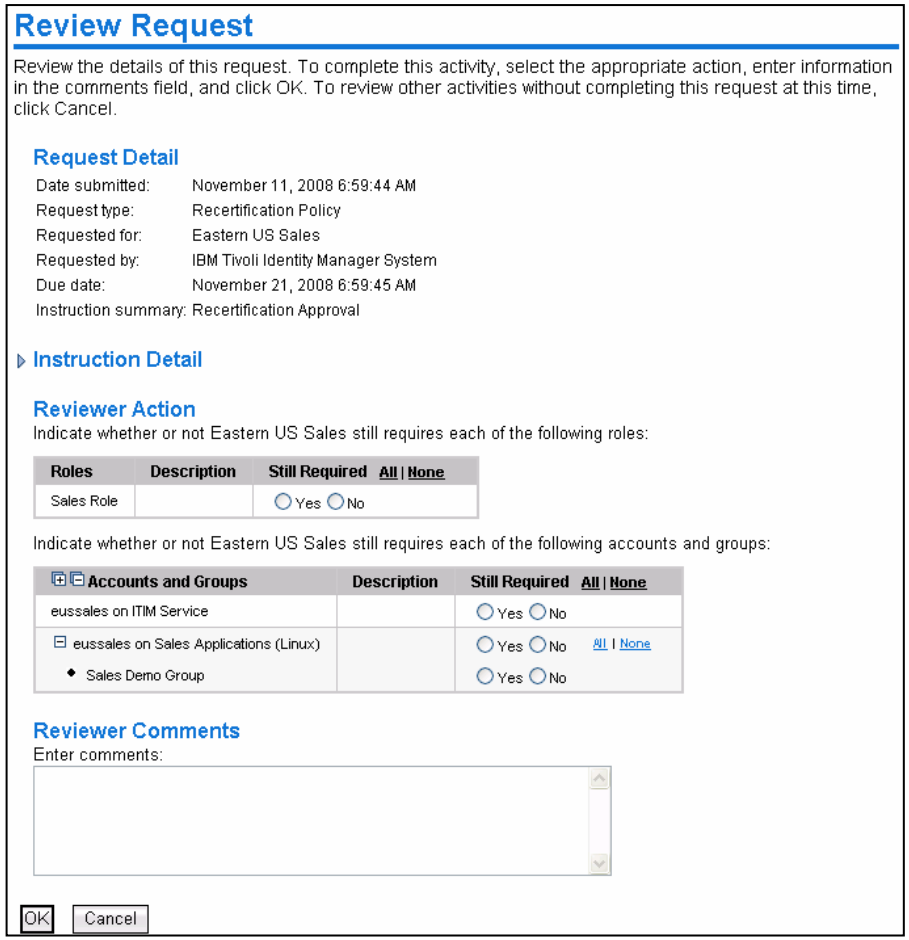
Indicate whether or not Barbara Cash still requires each of the following accounts and groups:

* Please note that all items require a decision

Accounts and Groups	Description	Still Required All | None
bcash on Access Manager for .NET Banking App	Access Manager on ADAM directory	Yes No All | None
Branch Teller	Branch Teller	Yes No
bcash on LedgerAccount	Reinsurance Satellite Ledger System	Yes No

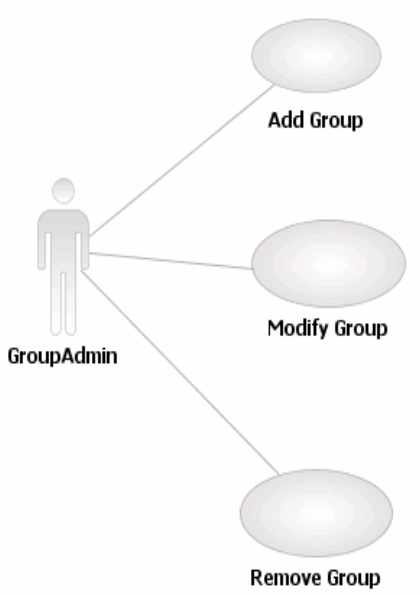
Recertificacion de usuarios ➔ Conformidad simplificada

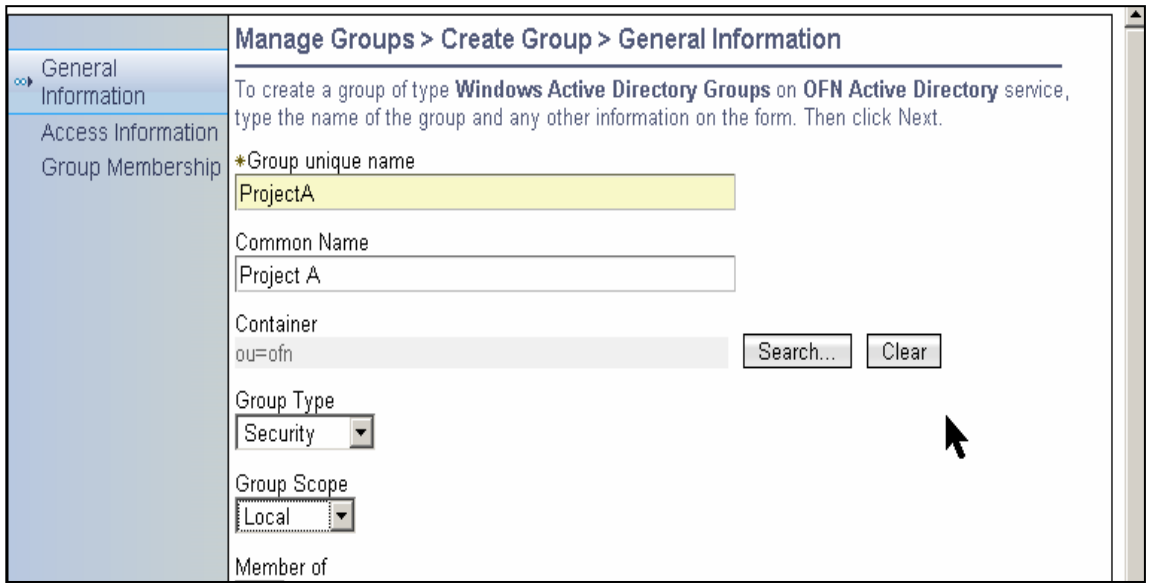
- **El procesos User recertification presenta al aprobador una única actividad de aprobación para todos o varios de los accesos y privilegios asociados a un usuario:**
- **El certificador puede tomar decisiones diferentes para cada recurso y enviar una respuesta consolidada**
  - El impacto de las descisiones de recertificación pueden ser pre-vistas antes de ser enviadas
  - Es posible realizar una operación progresiva y salvar como borrador
- **Una "Política de Recertificación de Usuarios" define la poblacion de usuarios, la planificación, los recursos y el workflow a utilizar**
  - Los flujos de trabajo pueden definirse en modo asistido y en modo avanzado
  - El modo asistido incluye selección del aprobador, desinatario de la notificación de la denegación, rejection action, due date, overdue behavior (new), and notification templates

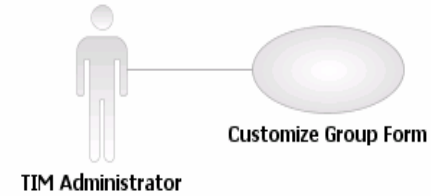


Gestión de grupos

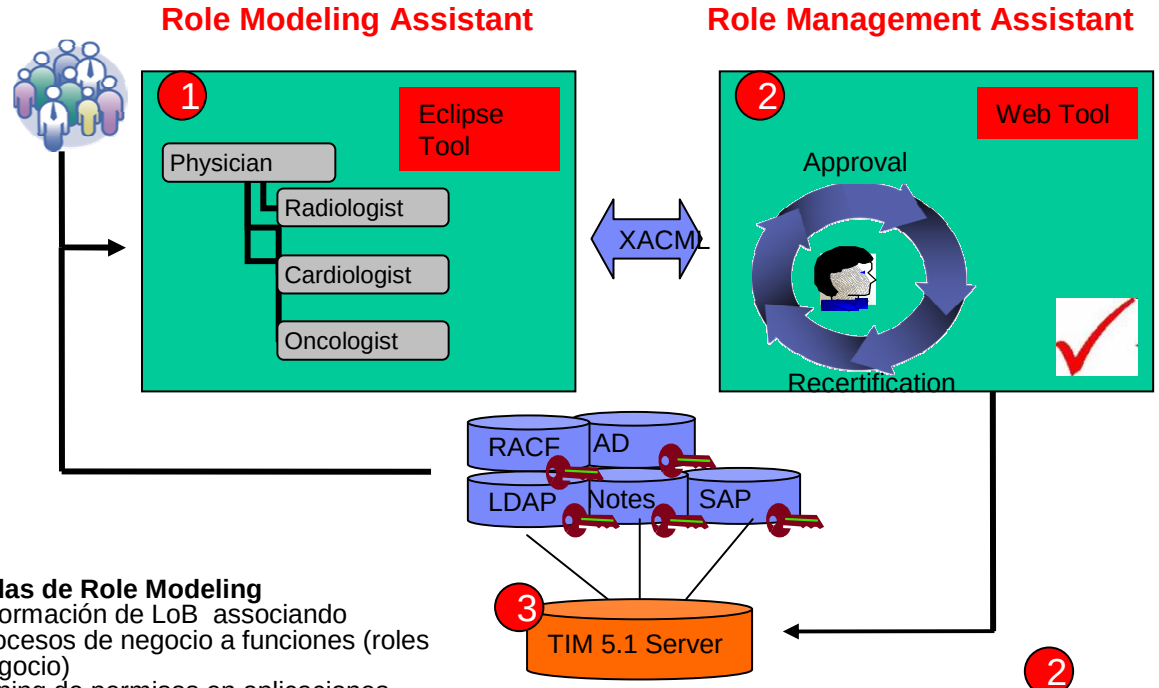
- **Capacidades TIM**
  - Administracion de Groups en el repositorio gestionado
    - Creación de Nuevos Groupos
    - Borrado de Groupos existentes
    - Modifación de la lista de miembros
  - Anidado de grupos en los sistemas gestionados que lo soportan







Asistentes para la gestión de roles



1

Entradas de Role Modeling
- Información de LoB asociando procesos de negocio a funciones (roles negocio)
- Mining de permisos en aplicaciones (app roles)

Salidas de Role Modeling
- Borradores para la estructura de rolesque asocia funciones de negocio con permisos
- Mapeo de roles entre negocio y aplicaciones y simulación para el refinamiento de la estructura

Valor de Role Modeling Assistant:
- Permite el diseño de estructuras de roles de grano fino
- Proporciona mayor visibilidad de la granularidad de acceso

Entrega
- Descarga de OPAL soporte desde el foro gestionado de Opal

2

Role Management Assistant:
- Importar roles creados en Role Modeling Assistant, ficheros CSV u otras herramientas de role modeling
- Aprobar y certificar definiciones de políticas y roles
- Exportar roles y políticas a TIM 5.1

Valor de Role Management Assistant:
- Simplifica la gestión del ciclo de vida de roles y politicas
- Elimina aprobaciones y certificaciones

Entrega
- Descarga gratuita de OPAL , soporte standar de IBM

TIM 5.1

3

TIM 5.1 :
- Consumidor de la estructura jerarquica de roles
- Establecimiento de políticas de separación de deberes, de contraseña, etc
- Gestión de cuentas y grupos.
- Certificación de la signación del rol

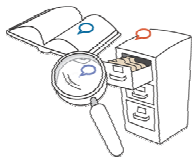
Valor deTIM 5.1 :
- Mejora de la seguridad.
- Incremento de productivodad
- Automatización del aprovisionamiento
- Simplificación de la gestión de roles

Entrega
- Passport Advantage

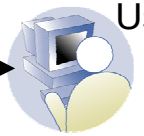
TIM 5.1 – Posibilitar soluciones rápidas y una aproximación por fases a IAM Governance

Simplify Complexity

Request Based



Publish Service Catalog



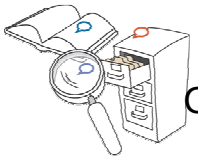
User Initiates Access Request

Approvals Gathered

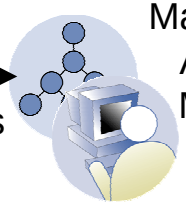
Access Provisioned

Periodic Recertification

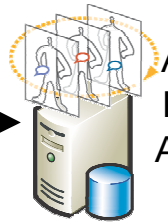
Hybrid Approach



Define Coarse Roles Plus Optional Access



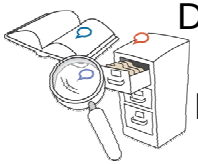
Major Changes Automated, Minor Ones Requested



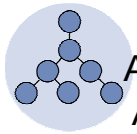
Access Auto Provisioned, Approvals for Exceptions

Recertify Exceptions Only

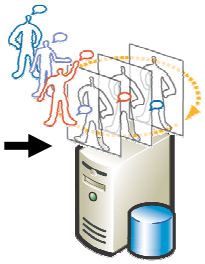
Role Based



Define Role Based Access Control Model & Policies

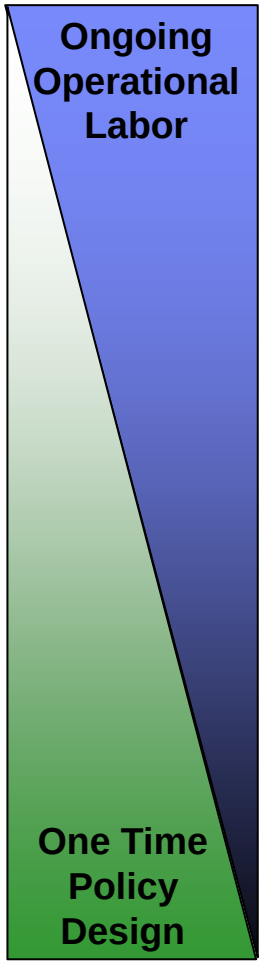


Update to User Attribute Initiates Access Change



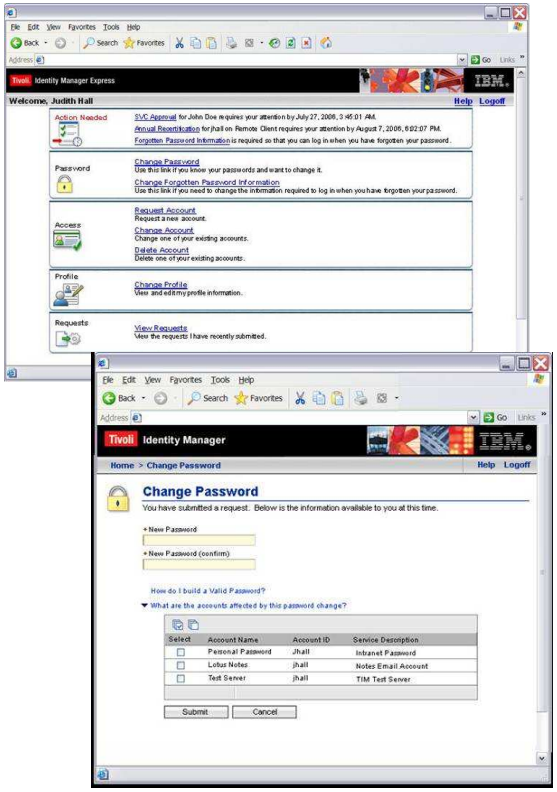
Automatic Provisioning and Rights Verification

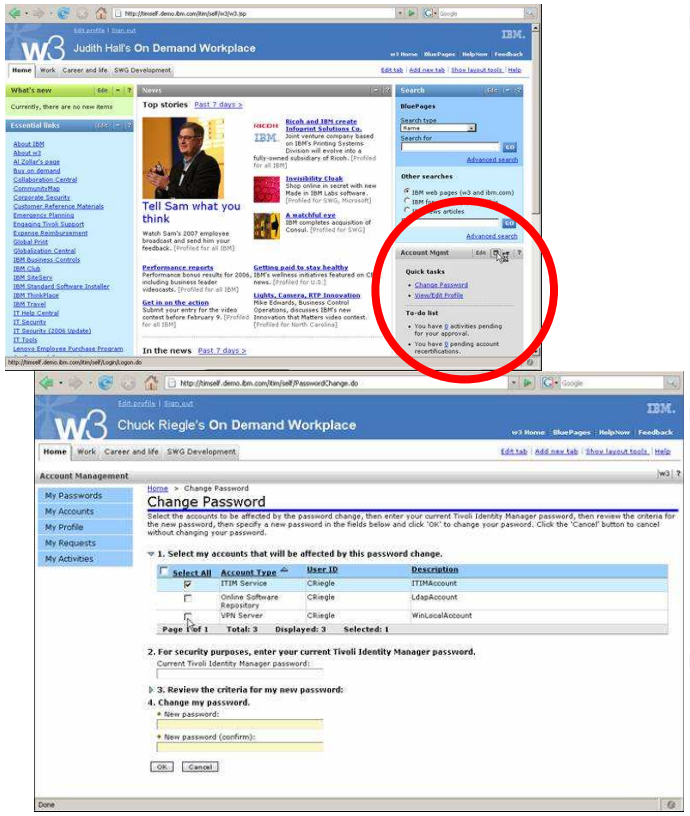
Automation



Soluciones Orientadas a la petición → Interface de autoservicio customizable out-of-the box– ROI rápido, soluciones mas simples

Lower Cost

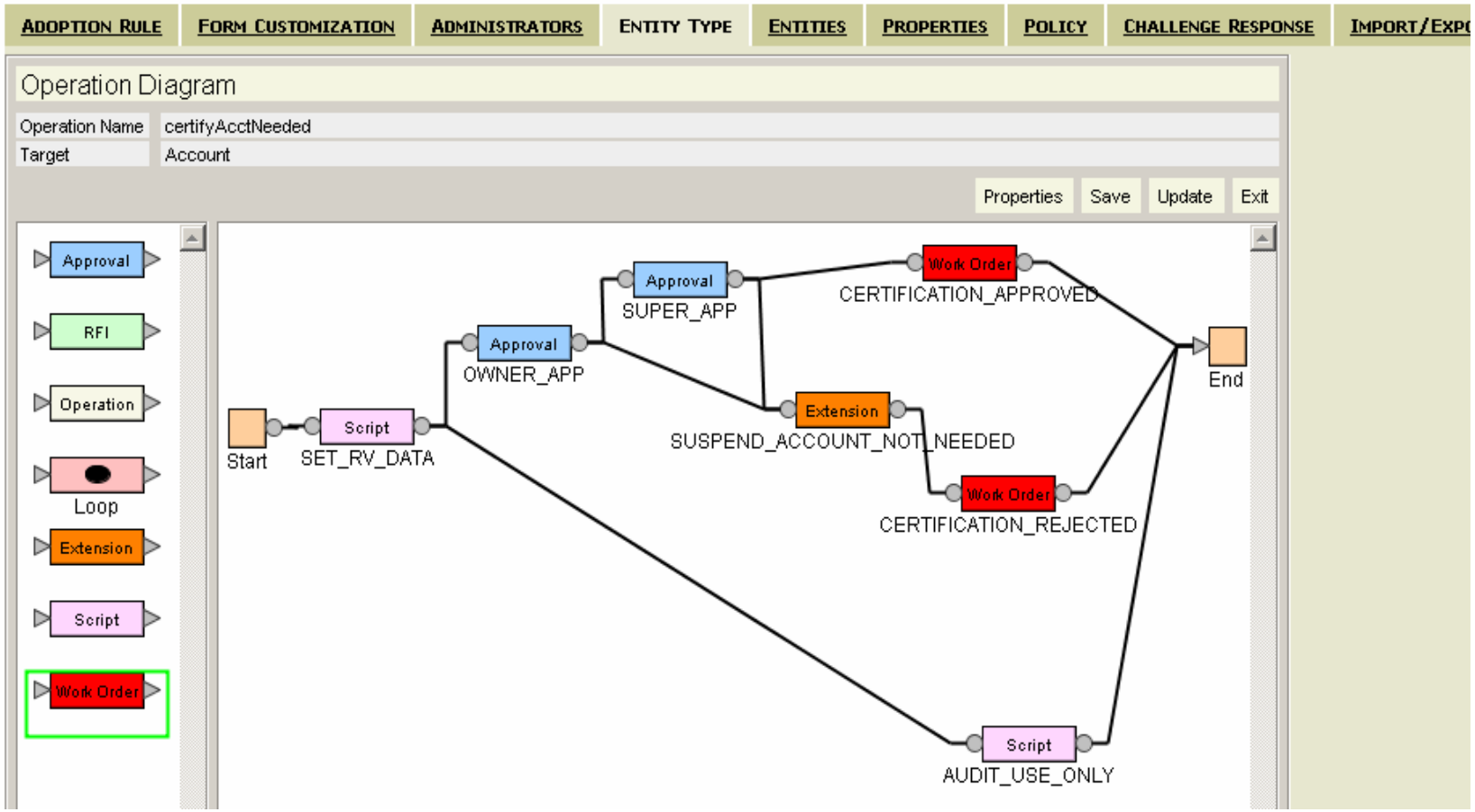




- **Autoservicio del usuario final:**
  - Petición de Cuenta o de Acceso
  - Reset Password
  - Approvals
- **Customizable**
  - Update via style sheets
  - Portal-friendly
- **Upgrade-friendly**
  - Customizations maintained
  - New features added

SOPORTE de soluciones basadas en la petición

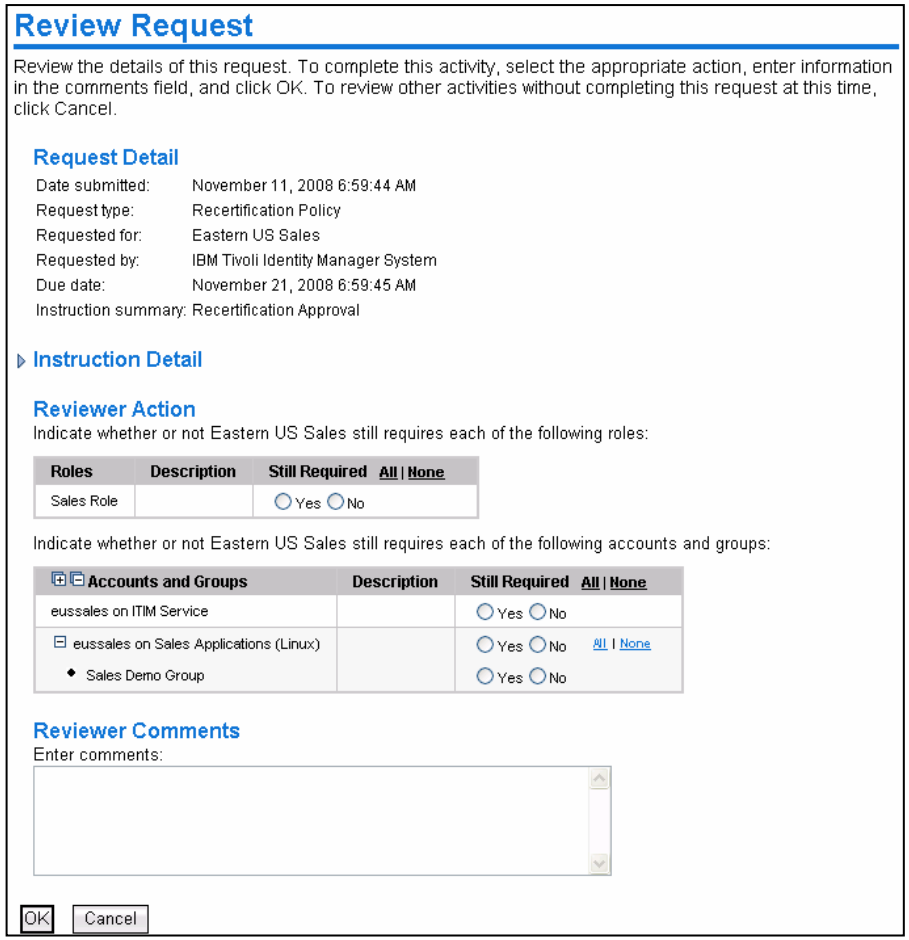
Flujos de aprobación y trabajo en modo asistido o en modo avanzado



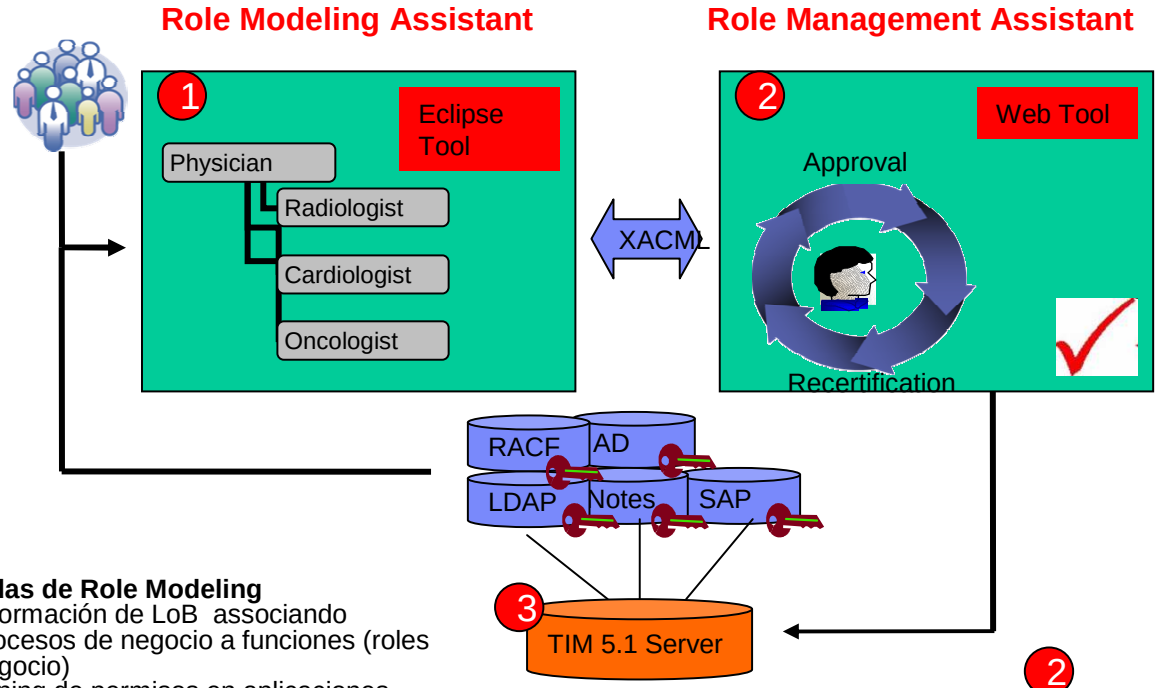
Permite definir facilmente flujos de aprobación complejos y ciclos de recertificación

Recertificacion de usuarios ➔ Conformidad simplificada

- **El procesos User recertification presenta al aprobador una única actividad de aprobación para todos o varios de los accesos y privilegios asociados a un usuario:**
- **El certificador puede tomar decisiones diferentes para cada recurso y enviar una respuesta consolidada**
  - El impacto de las descisiones de recertificación pueden ser pre-vistas antes de ser enviadas
  - Es posible realizar una operación progresiva y salvar como borrador
- **Una "Política de Recertificación de Usuarios" define la poblacion de usuarios, la planificación, los recursos y el workflow a utilizar**
  - Los flujos de trabajo pueden definirse en modo asistido y en modo avanzado
  - El modo asistido incluye selección del aprobador, desinatario de la notificación de la denegación, rejection action, due date, overdue behavior (new), and notification templates



Solución orientada a Roles



1

Entradas de Role Modeling
- Información de LoB asociando procesos de negocio a funciones (roles negocio)
- Mining de permisos en aplicaciones (app roles)

Salidas de Role Modeling
- Borradores para la estructura de rolesque asocia funciones de negocio con permisos
- Mapeo de roles entre negocio y aplicaciones y simulación para el refinamiento de la estructura

Valor de Role Modeling Assistant:
- Permite el diseño de estructuras de roles de grano fino
- Proporciona mayor visibilidad de la granularidad de acceso

Entrega
- Descarga de OPAL soporte desde el foro gestionado de Opal

2

Role Management Assistant:
- Importar roles creados en Role Modeling Assistant, ficheros CSV u otras herramientas de role modeling
- Aprobar y certificar definiciones de políticas y roles
- Exportar roles y políticas a TIM 5.1

Valor deRole Management Assistant:
- Posibilita la gestión del ciclo de vida de roles y politicas
- Elimina aprobaciones y certificaciones

Entrega
- Descarga gratuita de OPAL , soporte standar de IBM

TIM 5.1

3

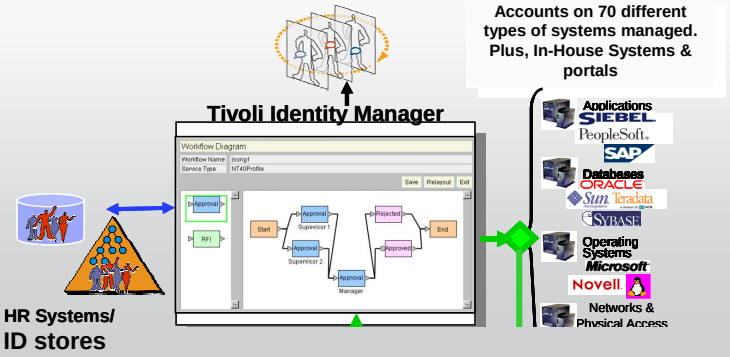
TIM 5.1 :
- Consumidor de la estructura jerarquica de roles
- Establecimiento de políticas de separación de deberes, de contraseña, etc
- Gestión de cuentas y grupos.
- Certificación de la signación del rol

Valor deTIM 5.1 :
- Mejora de la seguridad.
- Incremento de productivodad
- Automatización del aprovisionamiento
- Simplificación de la gestión de roles

Entrega
- Passport Advantage

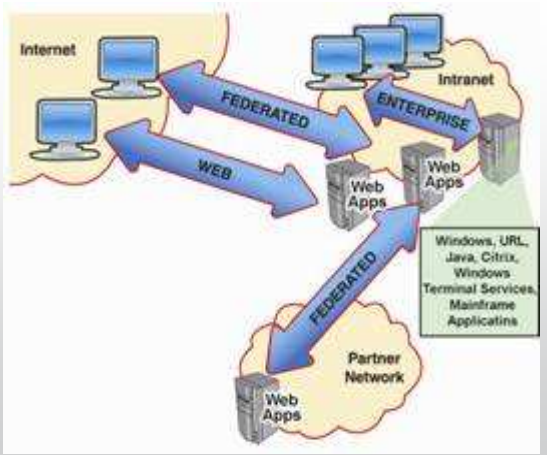
Identity and Access Assurance

User Provisioning / Role Management

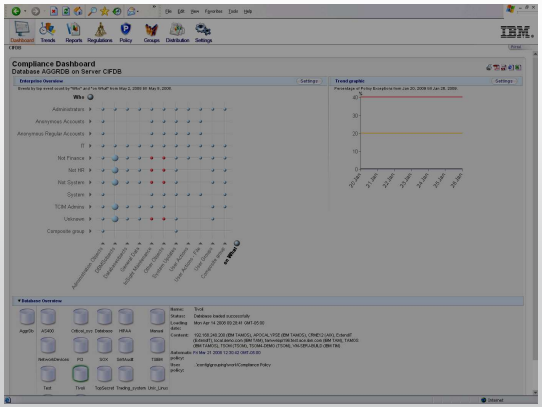


Single Sign On

& Password Management



Security log management & reporting



Banco de España

- Roles aditivos
- Conjunto de roles comunes
- Conjuntos de roles departamentales
- El usuario de un departamento solicita que se le asigne un rol departamental
- El responsable del departamento tramita la aprobación
- Tivoli Identity Manager realiza el aprovisionamiento automático de los accesos y cuentas asociados con dicho rol
- El departamento de seguridad obtiene informes semanales de conformidad

IBM Tivoli IAM Governance

Juan Nemiña Gantes

juannemina@es.ibm.com