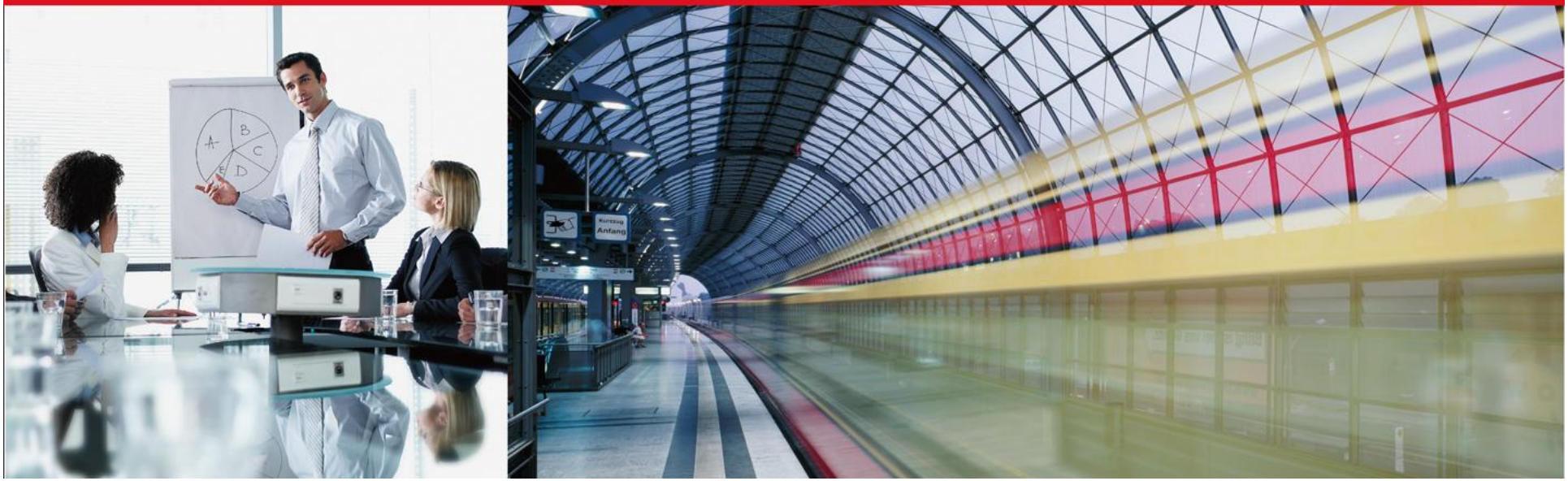
EXPO 2010 SHANGHAI CHINA

IBM

中国2010年上海世博会高级赞助商

IBM服务管理体验之旅

高效管理随需而变 优化服务实践共赢



Title ： IBM Tivoli安全軟件銷售經理

姓名　　金 天 威 (Eric Chin)
联系方式　echin@tw.ibm.com

演讲主题：**IBM Tivoli身份管理解决方案**

- 集中身份管理
- 集中访问授权
- 用户行为审计

信息安全成为企业CTO/CEO最为头疼的问题

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach at DuPont

February 15, 2007 – A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more …

"The best way to guard against insider breaches is for companies to ***monitor database and network access for unusual activity*** and set thresholds that represent acceptable use for different users."

Source: InformationWeek, Feb. 15, 2007

发生的安全问题:

- 数据被窃取
- 访问关键数据库
- 账号多人共用

Carnegie Mellon CERT Comments:

- "75% of … confidential information thefts studied … were committed by current employees"
- "45% had already accepted a job offer with another company"

如何处理：

- 对于内部访问有更为清晰的了解
- 增加身份控制
- 集中化的监控和审计

身份管理与访问控制

- **身份管理 (Identity Management)** - 建立身份和帐号的关联关系；管理每个用户的整个生命周期以及围绕用户管理的各种自动化的业务流程。它包括了：
  - 用户帐号的供应与管理，包括创建、修改、检查、删除等
  - 用户自我服务 (如更改用户个人信息或密码)
  - 工作流(Workflow)支持不同的用户管理及审批条件
  - 删除用户帐号，当该用户不再需要访问系统时

- **访问管理 (Access Management)** - 实现用户对应用资源和系统资源的访问与授权。
  - 什么人(by role)可以用什么资源？
  - 该角色被授权执行何种作业？
  - 该角色有什么样的授权和限制？

身份管理与访问控制的价值

- 账号、授权管理将纳入统一。实现对各业务支撑系统的帐号、认证、授权和审计的集中控制和管理。
- 实现集中化、基于角色的的帐号管理。用户权限的分配符合安全策略要求，拥有完成任务所需要的最小权限。
- 用户生命周期的管理，均可在一个平台上进行管理。用户的工作变动情况及时在支撑系统中得到体现。
- 用户一次登录即可方便地访问被授权的系统，提高工作效率。
- 实现安全审计管理，收集、记录、管理用户对业务支撑系统的高敏感度的数据访问和关键操作行为记录。

身份和访问管理方案的主要组件

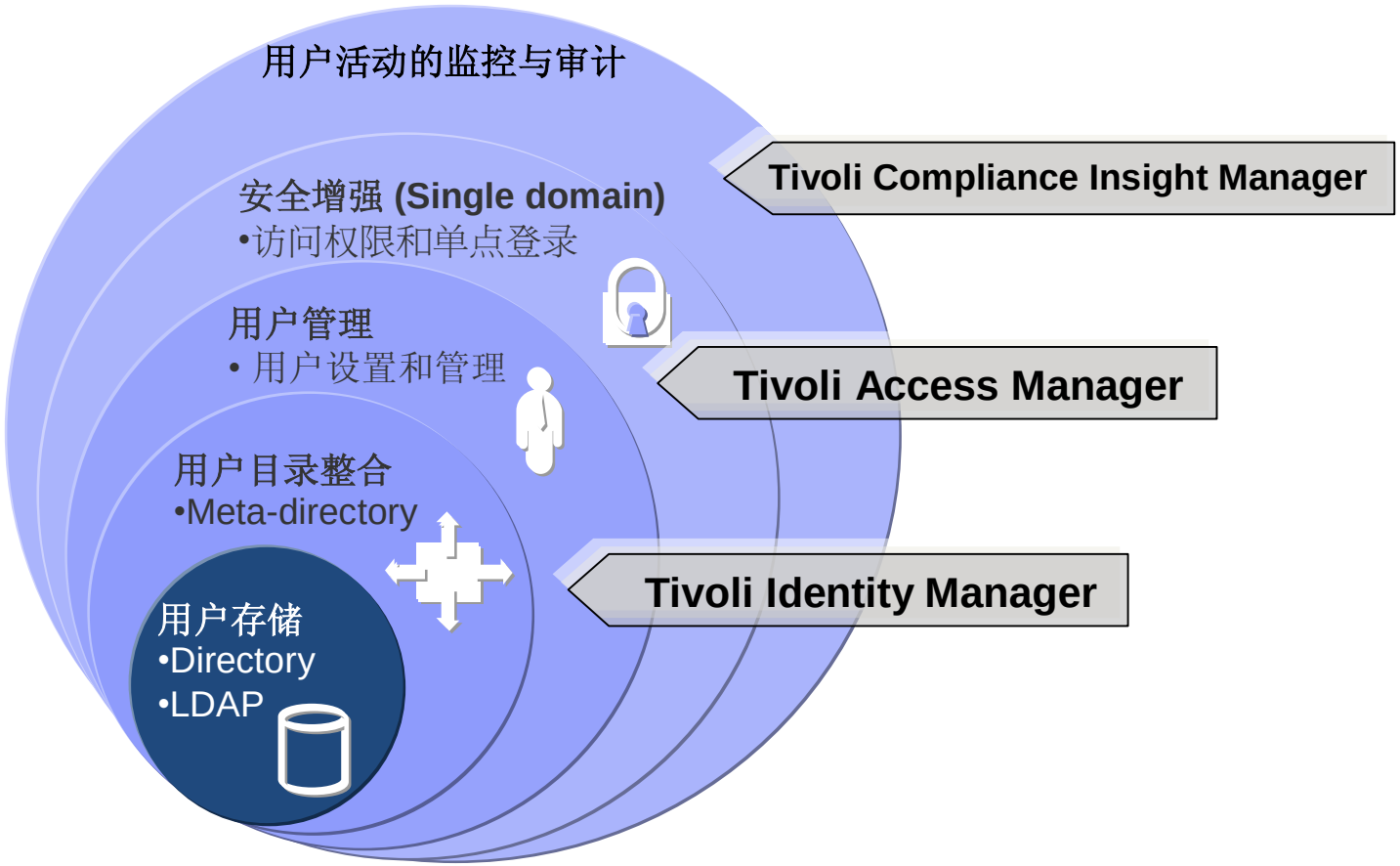
- 目录
  - 必须扩展至几万至百万个用户
  - 需要复制和分发目录数据，以提高可用性

身份管理

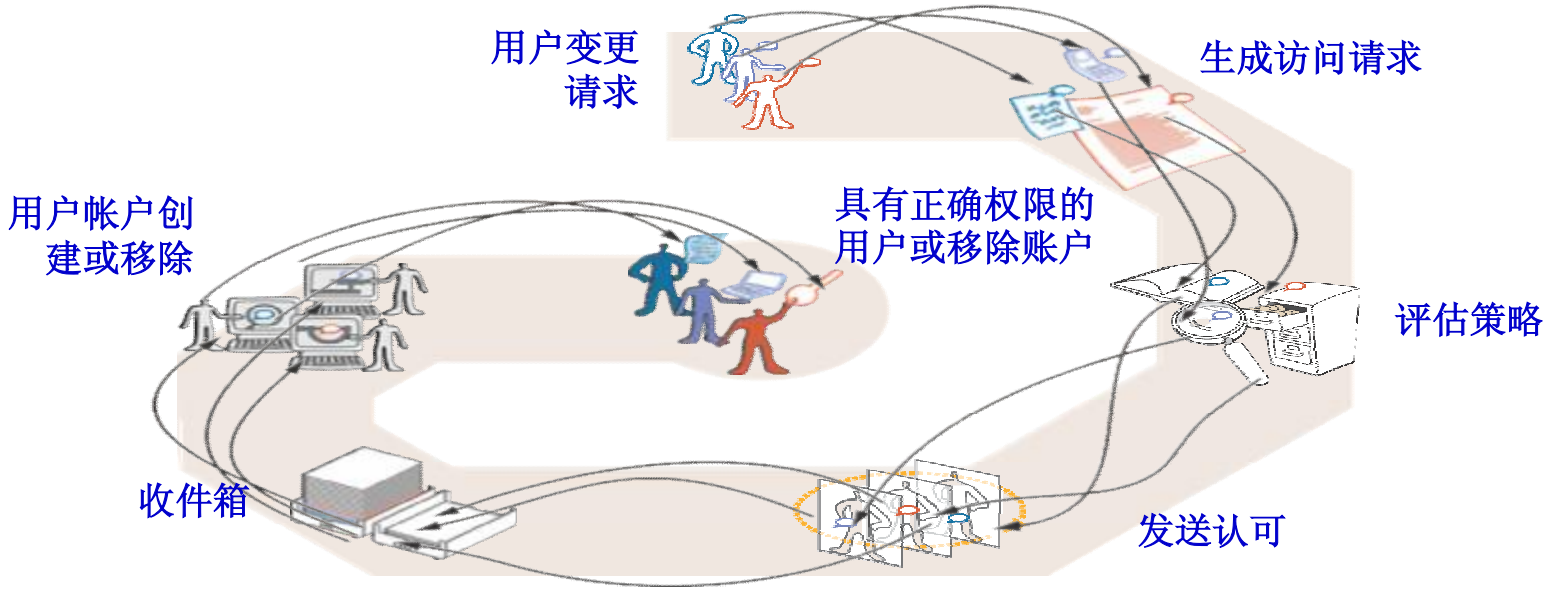
- IT系统（操作系统、目录、数据库）的界面应该可以测试并支持各种选项和场景
- 能以灵活的方式处理复杂供应场景

- 访问管理
  - 必须能支持高身份验证率
  - 单点登录和访问控制对于应用程序非常关键，必须具有高度可用性

Tivoli 身份管理和访问授权解决方案构建模块

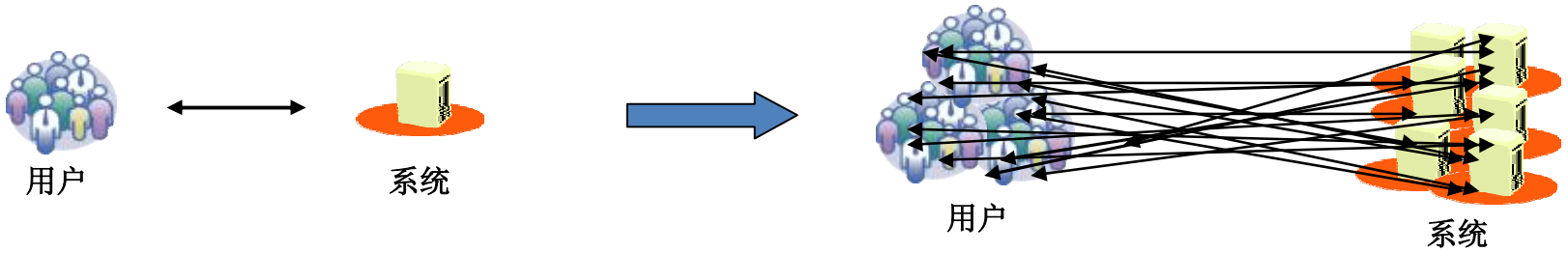


低效率的身份管理：帐户啟用、异动、删除 ...

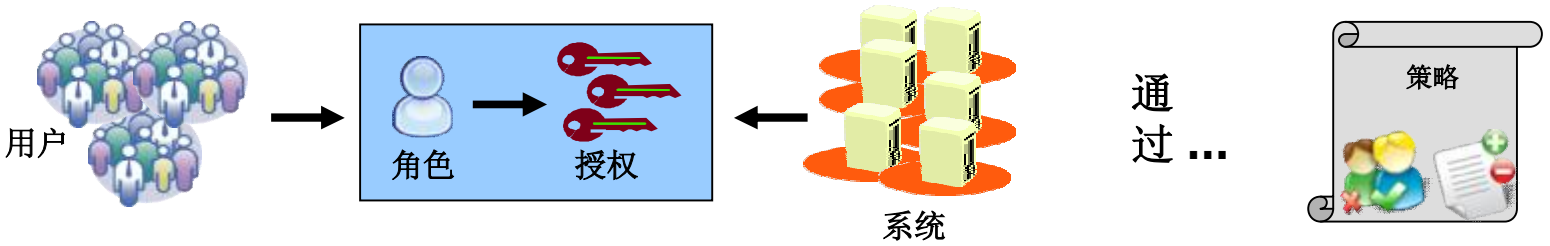


- 用户管理
  - 高度手动化的流程，往往需要多方参与，用户入职往往需要数周的时间
  - 成本高，每 300-500 名用户预计需要一名全职管理员
- 遵从性
  - 法规增加了用户和授权数据透明度的要求
  - 审计记录的收集是在各目标系统独立运行、维护。缺乏集中统一的访问审计系统。
- 安全性
  - 安全风险加速、糟糕的密码管理、孤儿帐户、无权威数据源

身份管理需具备自动化及高度的扩展性



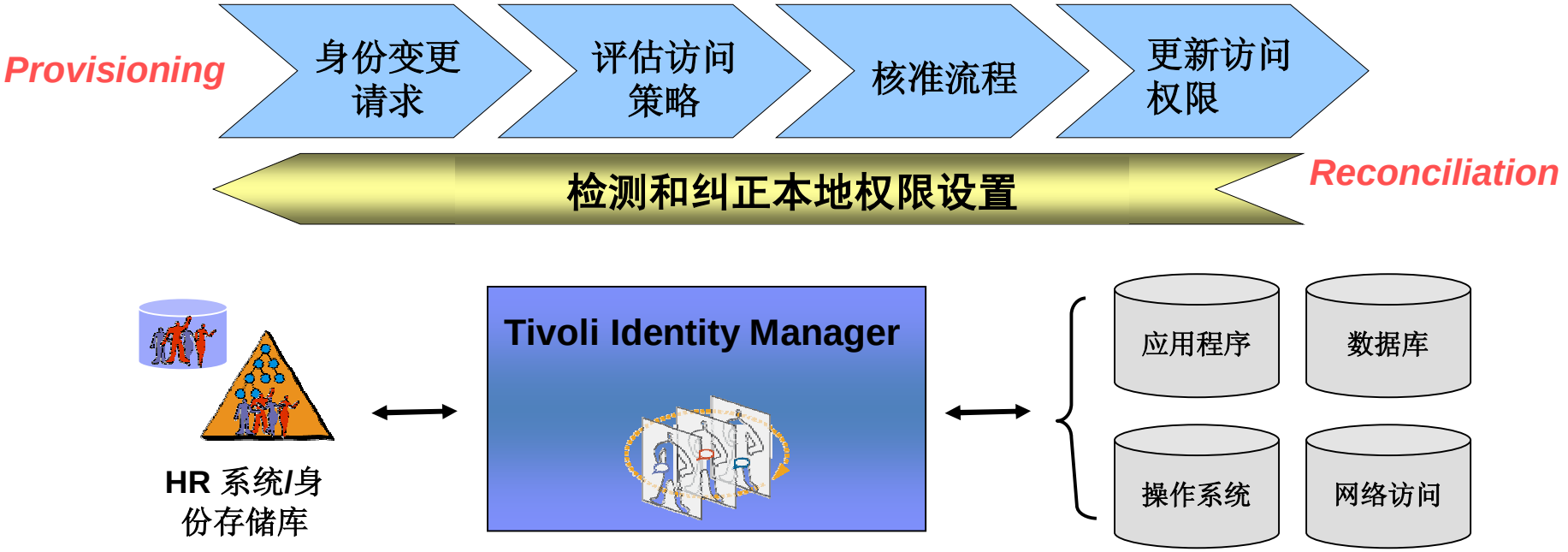
- 在用户/系统增加时，系统用户的自动提供将变得极为复杂
- 用户访问认证耗时且复杂



§ 角色和授权简化了身份管理，同时改善了组织扩展中的可见性和访问控制

§ 将规则与工作流关联的策略可简化自动化

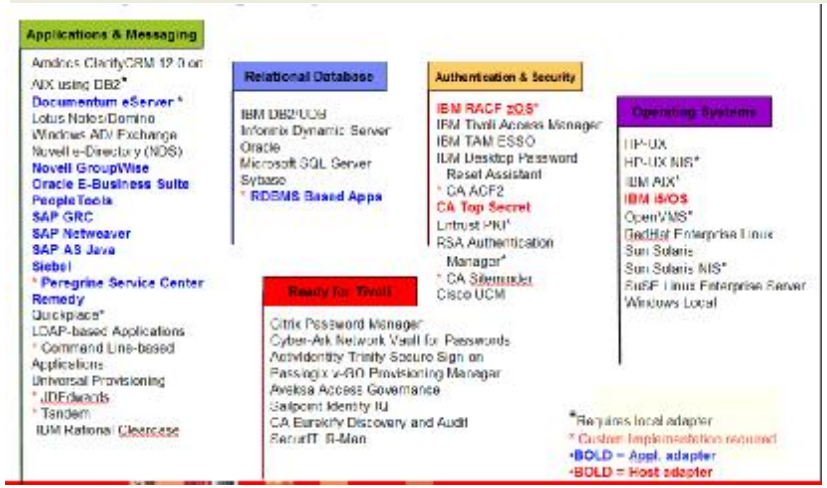
Tivoli Identity Manager (TIM) ：自動化用户身份生命周期管理



- 提高效率 - 用户的工作变动情况及时在支撑系统中得到体现
- 降低成本 - 将用户入职访问权限的配置缩短到几分钟内，通过自助服务减少人力成本
- 提高安全性 - 通过周期性的续验证和修正用户访问权限
- 管理遵从性 -了解谁有访问权限；为什么这些人拥有访问权限

Tivoli Identity Manager 的集成广度和深度是快速实现价值的关键所在

对预先打包的适配器的最广泛支持

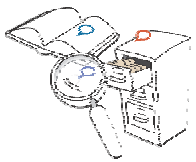


用于自定义适配器的快速、可调整的工具

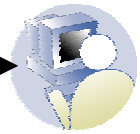
- 快速集成自主开发的应用程序
- 简单的驱动模板可将开发时间缩短 **75%**
- 需要的专业技能更少

提供多种管理用户访问权限的方法

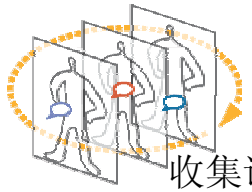
基于请



发布服务目录



用户发起访问请求

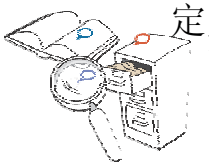


收集许可

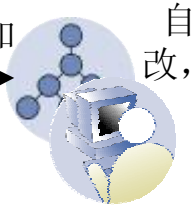
提供访问权限

周期性地重新认证

混合方



定义大致的角色和可选访问权限

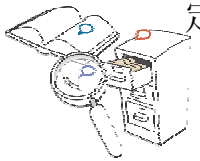


自动化主要更改，请求次要更改

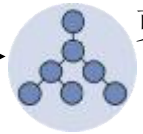
提供访问自动化、认可异常

仅重新确认异常

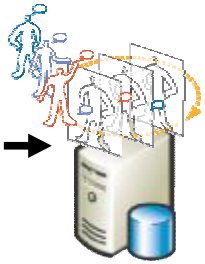
基于角



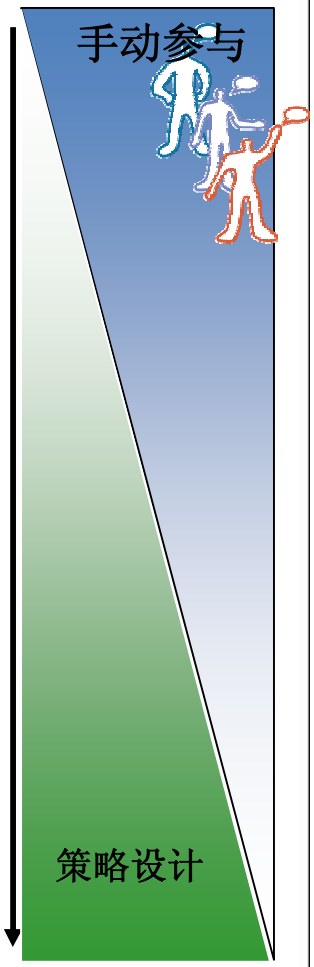
定义基于角色的访问控制模型/策略



更新用户属性，发起访问更改



自动提供和权限验证



集中的密码管理可增强安全性，并降低帮助台成本

- 跨所有系统的自助服务密码管理
  - 应用有针对性或全局的密码规则
  - 根据目标系统验证遵从性
- 密码同步
- 用户遗忘 ID 和/或密码时的密码回复及更新
  - 用户或站点定义的问题
  - 电子邮件通知
- 集成Tivoli Access Manager
  - 根据 Windows 登录提示进行桌面密码重设/解锁
  - 提供 TAM ESSO 的用户访问权限

Tivoli Identity Manager：提高安全性和遵从性

1

一致性 (Reconciliation)

谁有权访问什么？身份孤儿和休眠账户 - 严重的安全隐患！

2

重新认证 (Recertification)

用户是否依然需要此帐户或访问权限？建立自动流程来评审和实施。

3

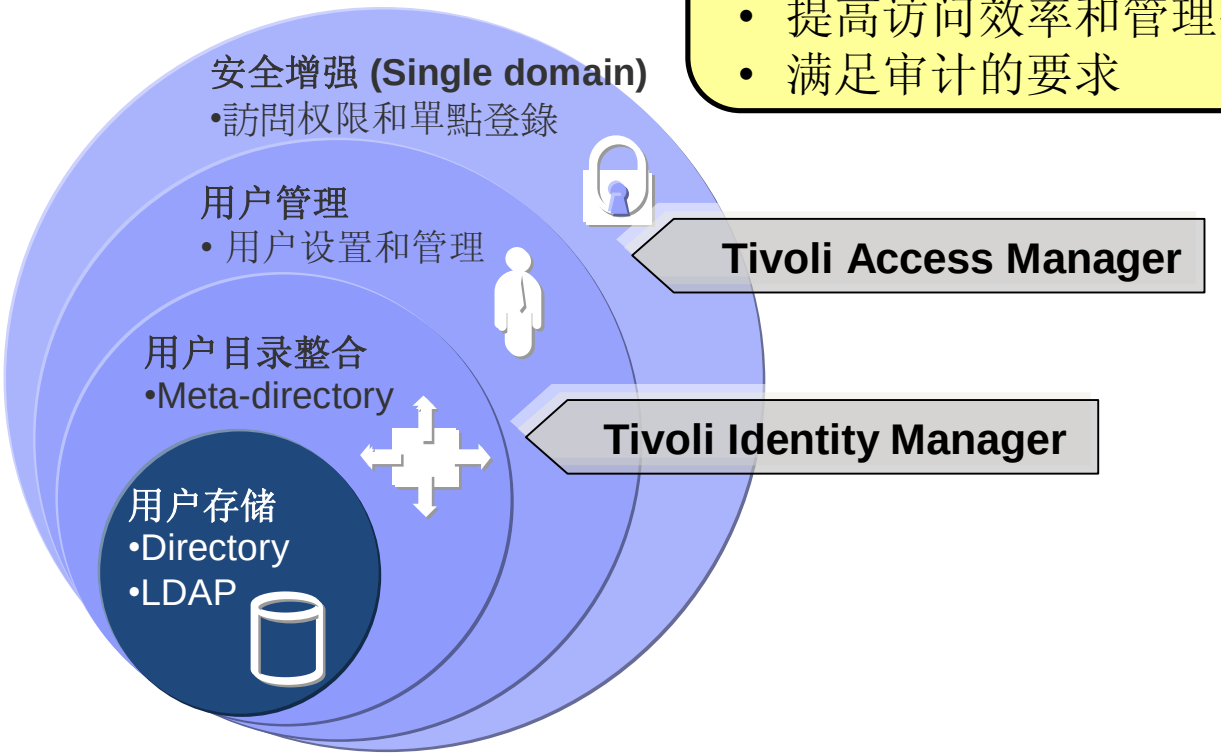
报告 (Reporting)

为审计人员展示谁有权访问哪些内容，以及他们是如何获得访问权限的。

身份管理应用模式：安全访问和认证授权

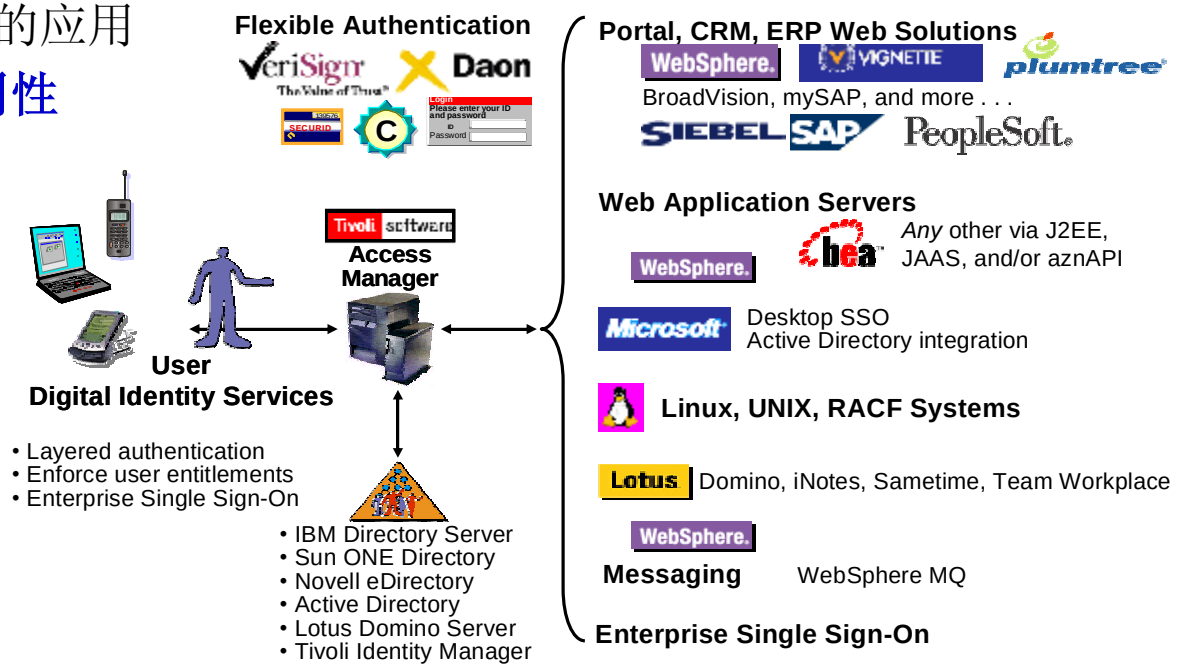
解决客户问题

- 薄弱的/不一致的管理
- 分散的, 不一致的授权/访问控制
- 提高访问效率和管理效率
- 满足审计的要求

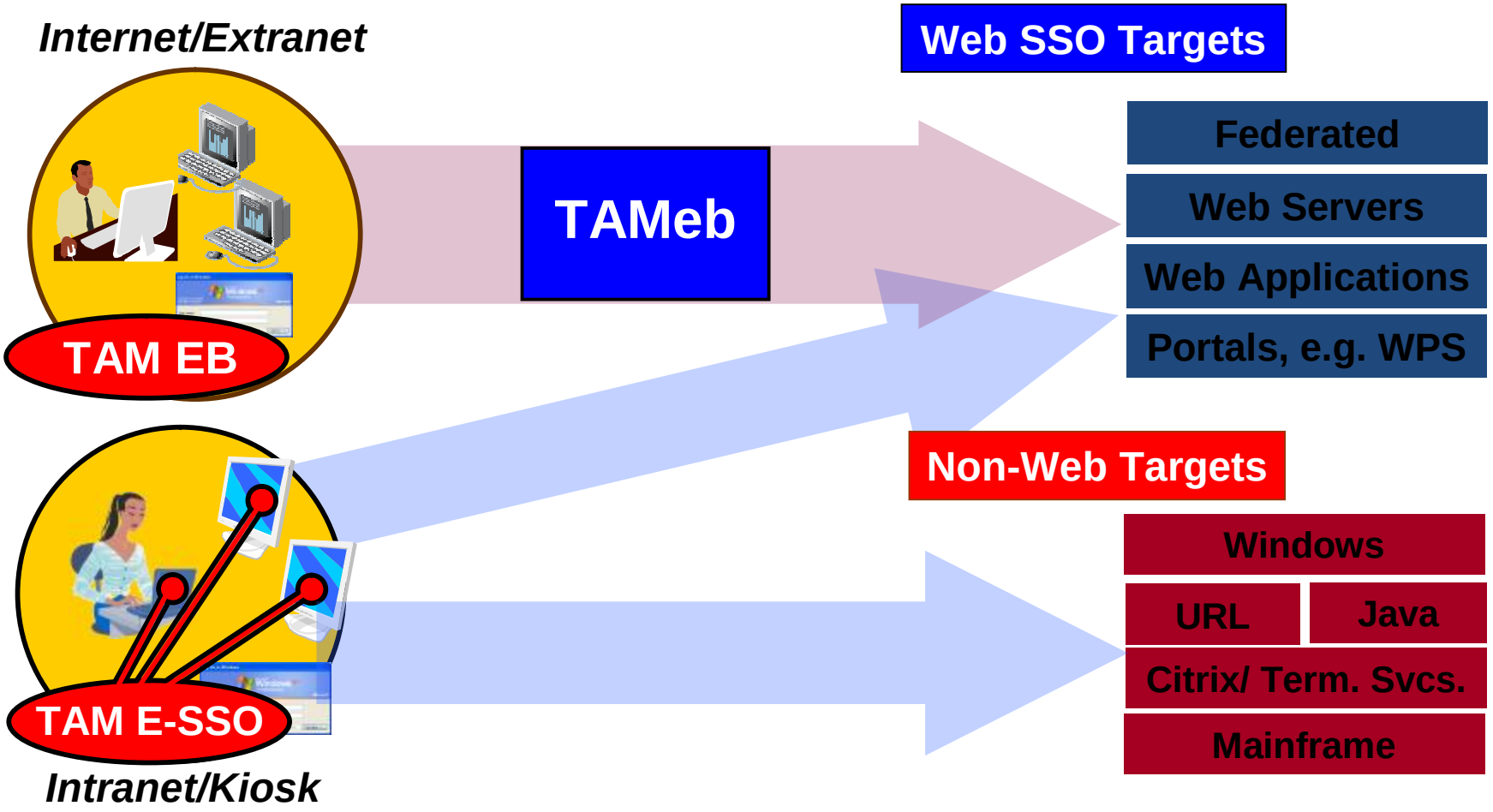


Tivoli Access Manager for e-Business (TAMeB) ：集中的应用访问认证和授权服务

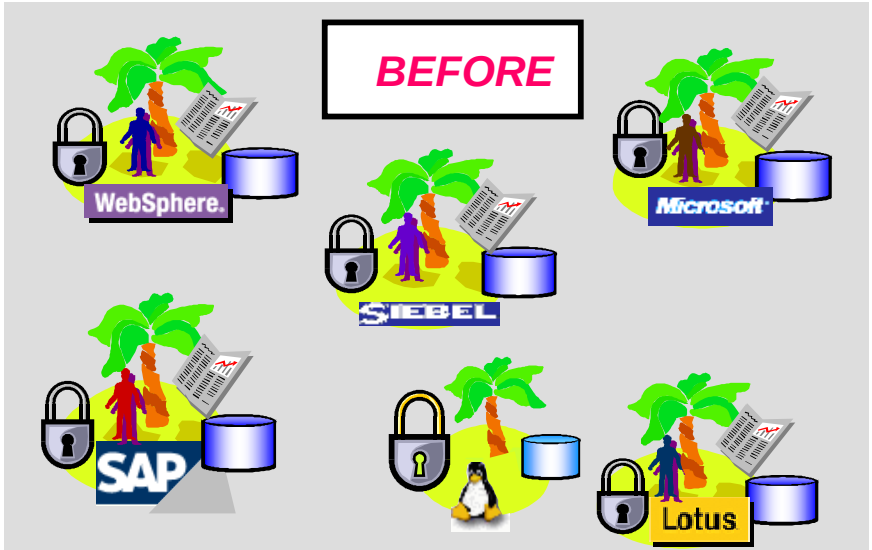
- 控制对系统、应用、数据和信息的访问
- 面向多种应用，提供统一身份认证授权服务
  - 用户、门户、Web 应用、定制应用
- 支持单一登录基于 Web 的应用
- 解决安全问题并确保可用性



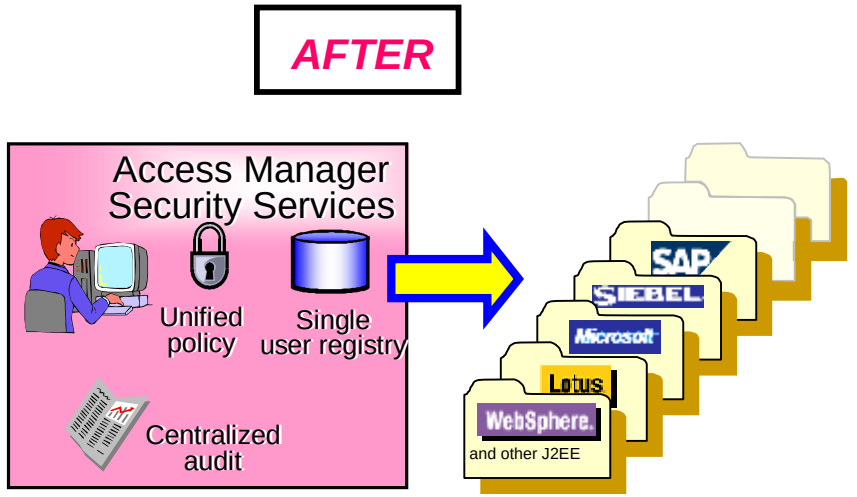
Tivoli Access Manager：完整的单点登录解决方案



Tivoli Access Manager – 功能与价值



§太多的口令需要记忆
§多个管理域，多个访问控制工具
§到处都是用户和访问控制信息
§安全成为应用开发者的任务
§策略依从性?

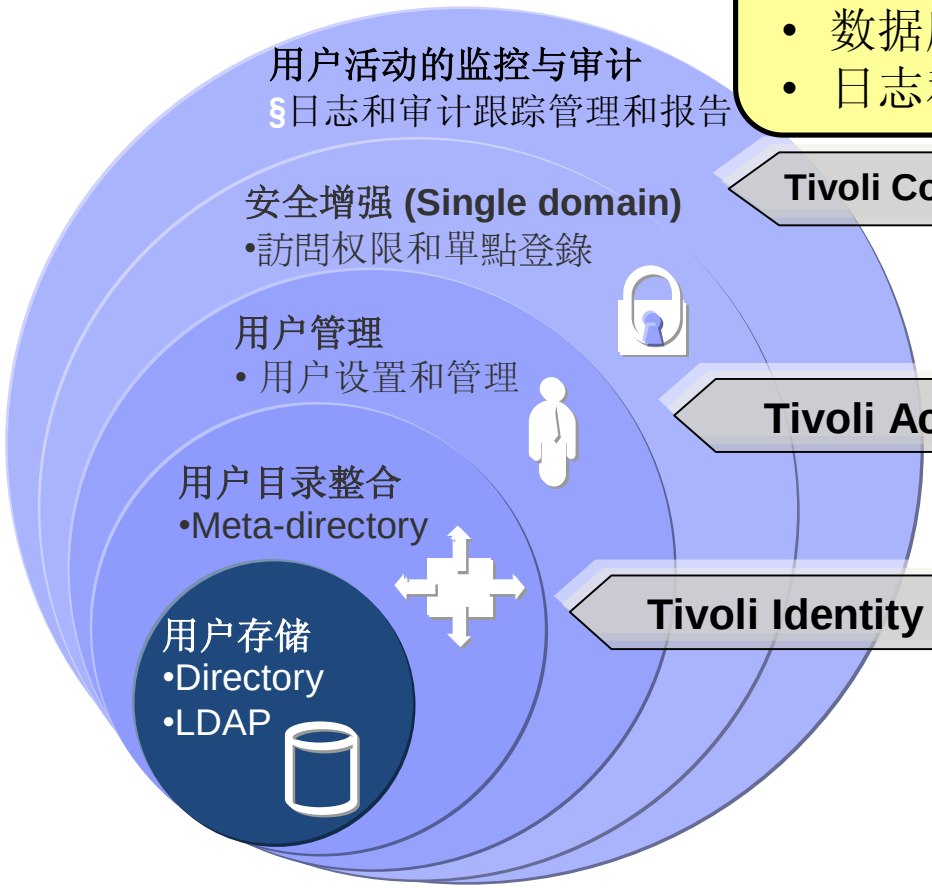


§Web单点登录，单一工具完成访问控制
§单一安全域，或是基于单一工具的委派管理
§集中的用户和安全信息
§策略+审计=策略依从
§建立安全标准，具有高度扩展性

= 安全策略　　= 用户和组的信息　　= 审计

身份管理应用模式：用户安全审计

- 安全制度遵从情况的显示板和报告
- 特权用户的监控与审计
- 数据库的监控和审计
- 日志和审计跟踪管理



Tivoli Compliance Insight Manager

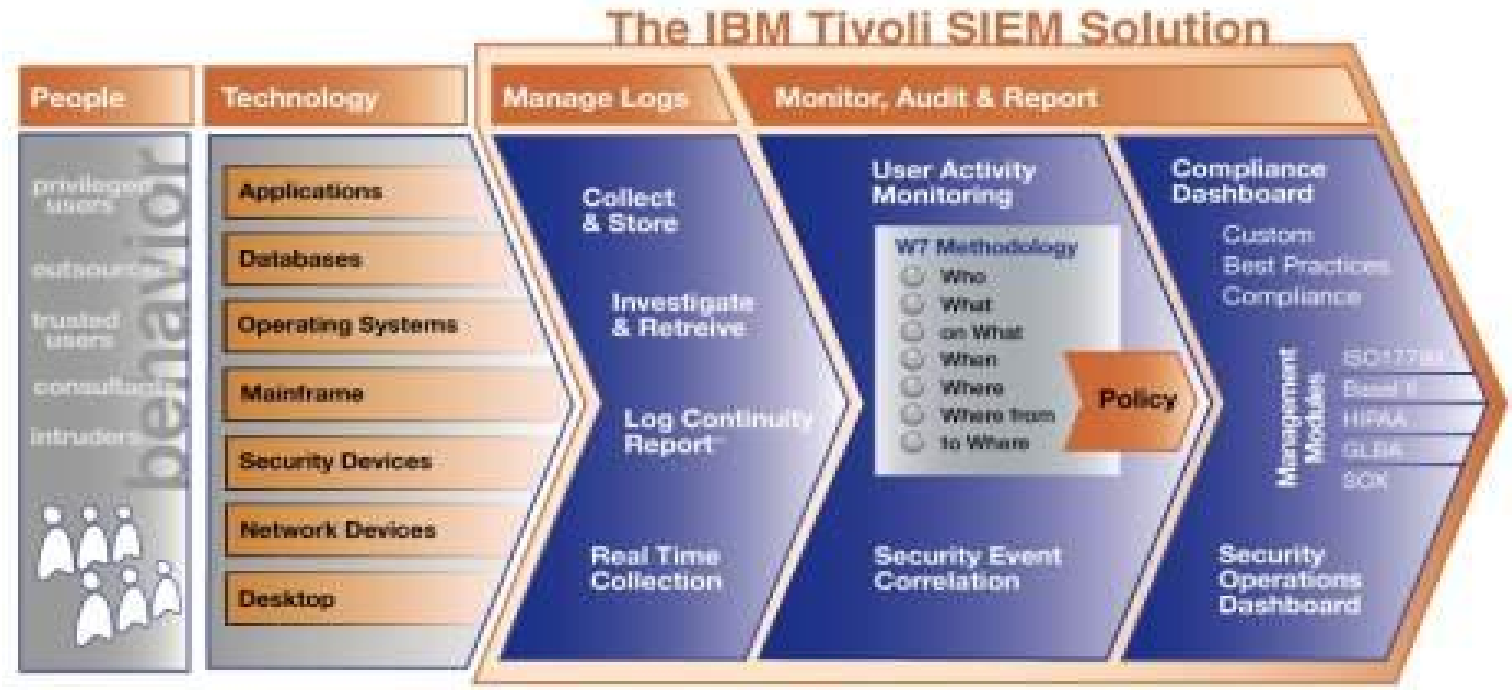
Tivoli Access Manager

Tivoli Identity Manager

作为安全管理员，需要如何完成繁重的审计工作？

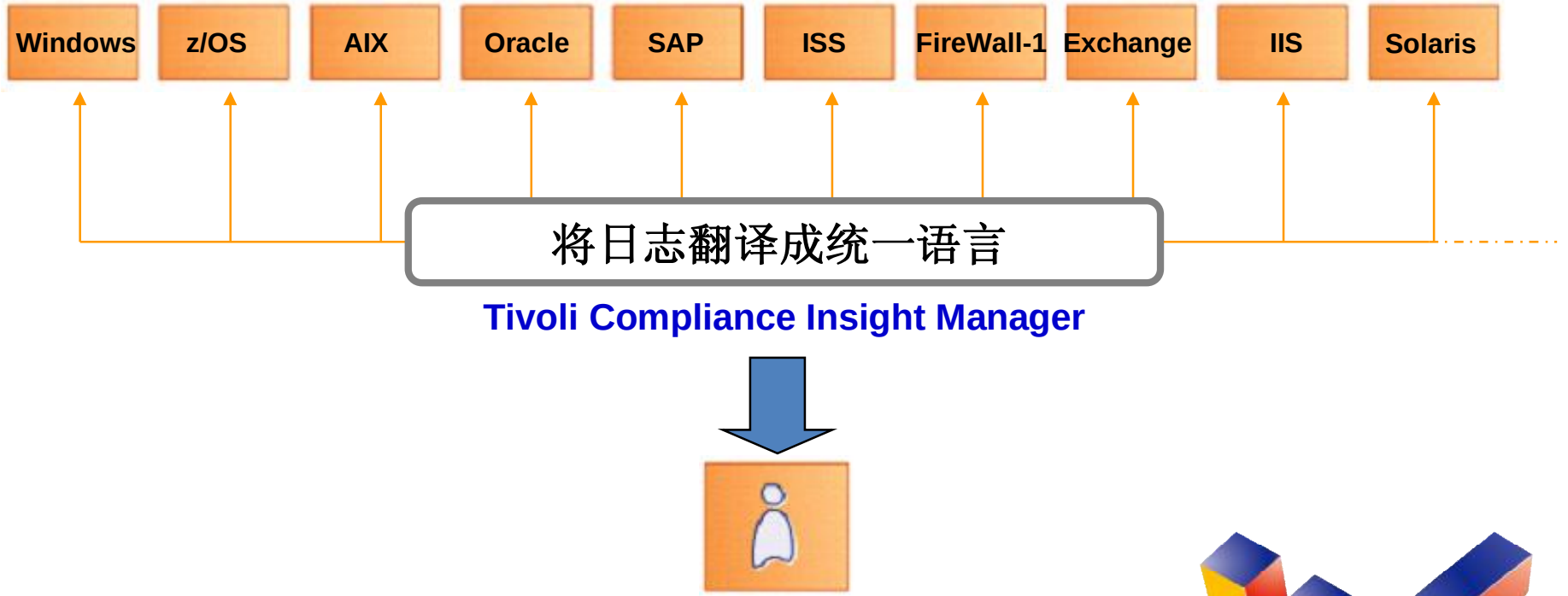
- 对海量原始日志文件的调查
  - 我需要审计系统本身就可以提供对原始日志文件的调查能力，而不是我自己打开每个文件去查询
- 理解每种系统的日志信息，从而找到安全隐患
  - 我需要审计系统提供对日志的自动翻译到标准格式的能力，而不是我自己来翻译
- 自动完成对违规行为的发现、严重级别定义
  - 我需要可以在审计系统中定义规则，同时审计系统需要根据我定义的规则对每条日志进行自动分析和安全级别定义
- 能否第一时间得到告警
  - 我希望审计系统和企业的IT运维中心进行连接，统一发送告警
- 完成合规报告
  - 我需要审计系统自动生成我企业需要合规报告，而不是我自己来做！

Tivoli Compliance Insight Manager (TCIM)：一专业的审计管理平台

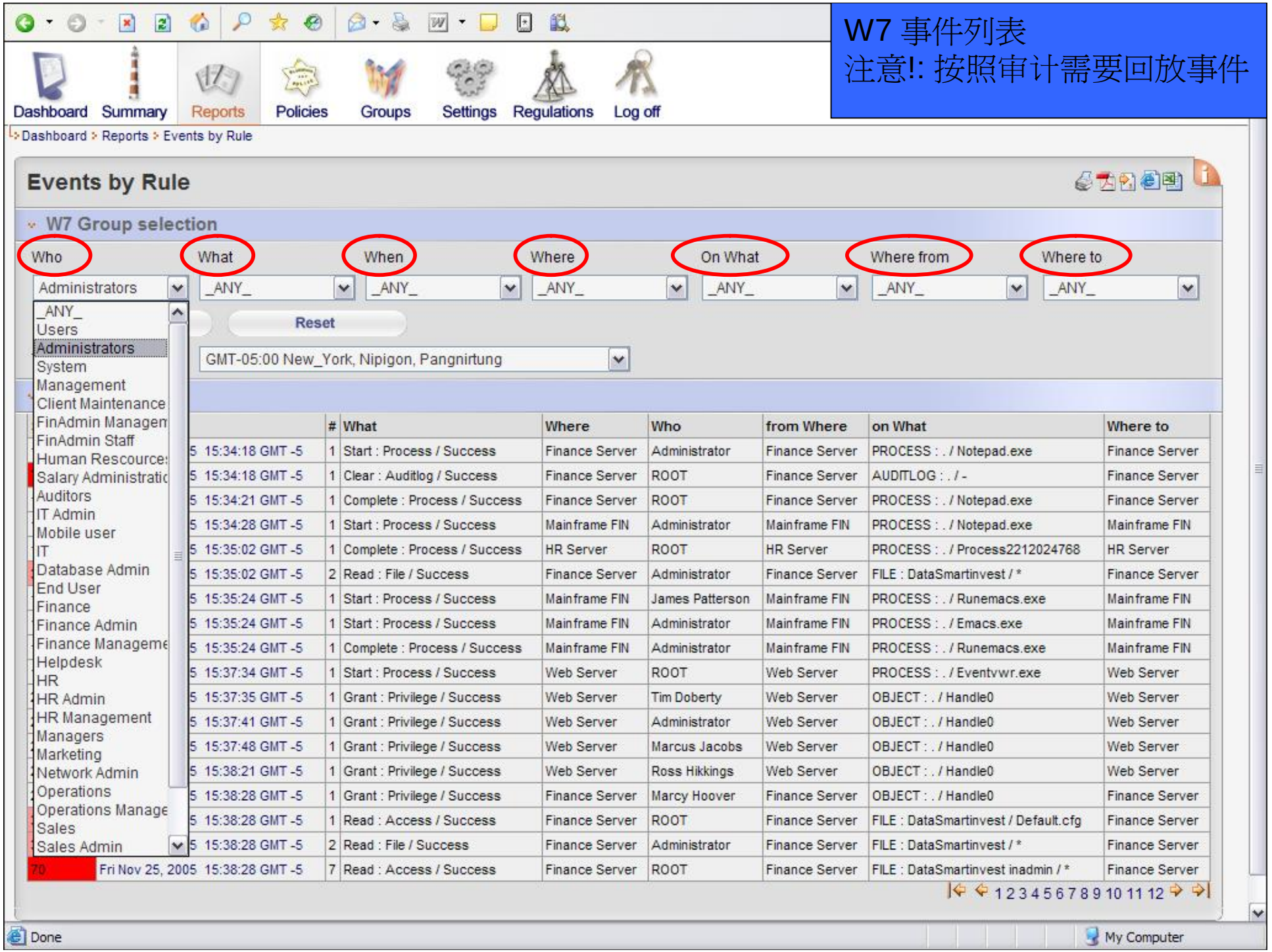


- 捕获（Capture）：企业日志收集和管理
- 理解（Comprehend）：精准的日志翻译和解释
- 了解（Communicate）：全面的审计和合规性报告

统一所有企业日志的语言

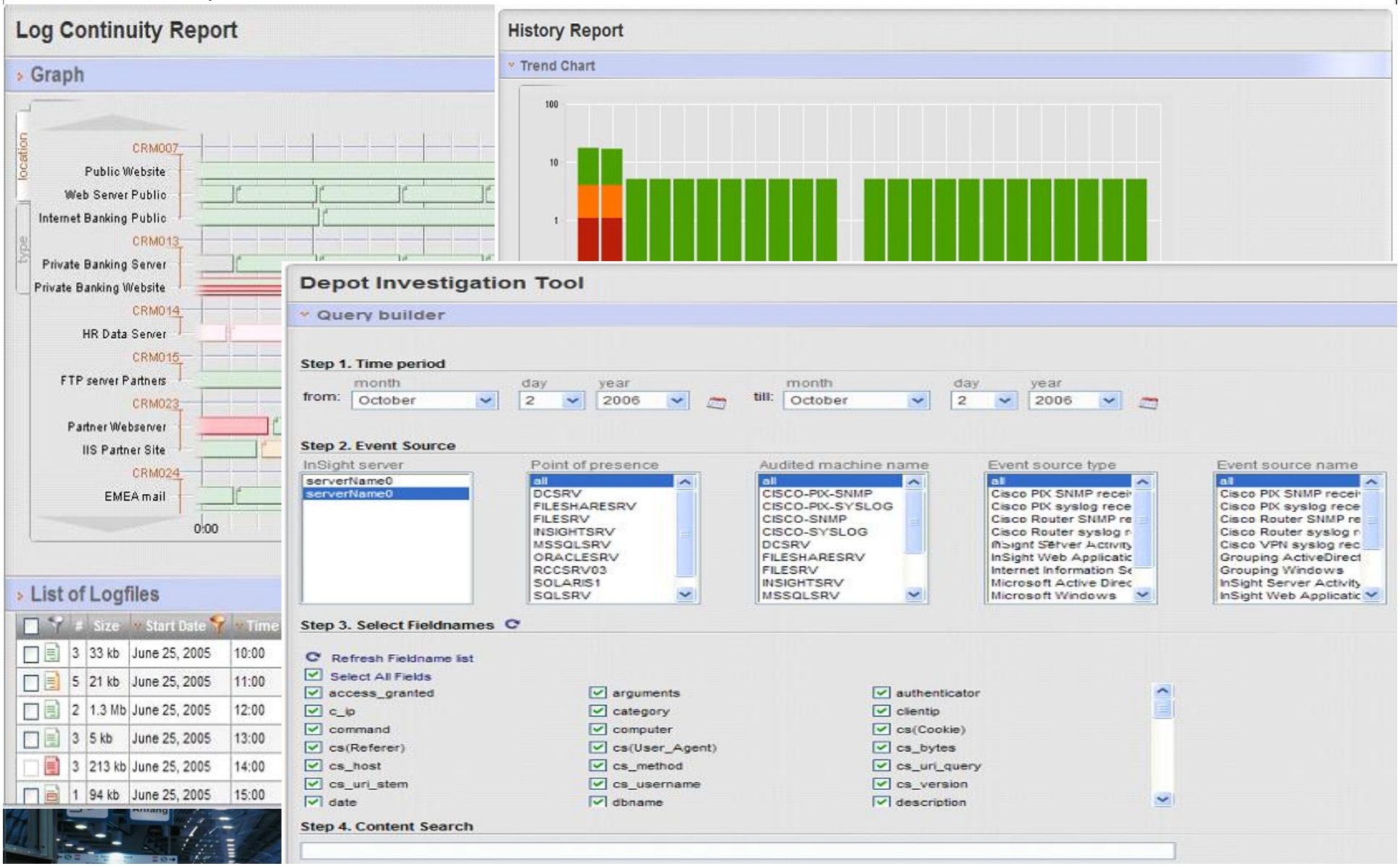


基于一种“标准”的格式来描述事件：***Who did What, When, Where, From Where, Where To, and on What***。从而使管理员可以更为直观了解事件的内容。


W7 事件列表
注意!: 按照审计需要回放事件
Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard > Reports > Events by Rule
Events by Rule
W7 Group selection
Who
What
When
Where
On What
Where from
Where to
Administrators
ANY
Reset
GMT-05:00 New_York, Nipigon, Pangnirtung
ANY
Users
Administrators
System
Management
Client Maintenance
FinAdmin Managen
FinAdmin Staff
Human Rescource:
Salary Administratic
Auditors
IT Admin
Mobile user
IT
Database Admin
End User
Finance
Finance Admin
Finance Manageme
Helpdesk
HR
HR Admin
HR Management
Managers
Marketing
Network Admin
Operations
Operations Manage
Sales
Sales Admin
| What | Where | Who | from Where | on What | Where to
5 15:34:18 GMT -5 | 1 | Start : Process / Success | Finance Server | Administrator | Finance Server | PROCESS : . / Notepad.exe | Finance Server
5 15:34:18 GMT -5 | 1 | Clear : Auditlog / Success | Finance Server | ROOT | Finance Server | AUDITLOG : . / - | Finance Server
5 15:34:21 GMT -5 | 1 | Complete : Process / Success | Finance Server | ROOT | Finance Server | PROCESS : . / Notepad.exe | Finance Server
5 15:34:28 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Notepad.exe | Mainframe FIN
5 15:35:02 GMT -5 | 1 | Complete : Process / Success | HR Server | ROOT | HR Server | PROCESS : . / Process2212024768 | HR Server
5 15:35:02 GMT -5 | 2 | Read : File / Success | Finance Server | Administrator | Finance Server | FILE : DataSmartinvest / * | Finance Server
5 15:35:24 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | James Patterson | Mainframe FIN | PROCESS : . / Runemacs.exe | Mainframe FIN
5 15:35:24 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Emacs.exe | Mainframe FIN
5 15:35:24 GMT -5 | 1 | Complete : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Runemacs.exe | Mainframe FIN
5 15:37:34 GMT -5 | 1 | Start : Process / Success | Web Server | ROOT | Web Server | PROCESS : . / Eventvwr.exe | Web Server
5 15:37:35 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Tim Doberty | Web Server | OBJECT : . / Handle0 | Web Server
5 15:37:41 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Administrator | Web Server | OBJECT : . / Handle0 | Web Server
5 15:37:48 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Marcus Jacobs | Web Server | OBJECT : . / Handle0 | Web Server
5 15:38:21 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Ross Hikkings | Web Server | OBJECT : . / Handle0 | Web Server
5 15:38:28 GMT -5 | 1 | Grant : Privilege / Success | Finance Server | Marcy Hoover | Finance Server | OBJECT : . / Handle0 | Finance Server
5 15:38:28 GMT -5 | 1 | Read : Access / Success | Finance Server | ROOT | Finance Server | FILE : DataSmartinvest / Default.cfg | Finance Server
5 15:38:28 GMT -5 | 2 | Read : File / Success | Finance Server | Administrator | Finance Server | FILE : DataSmartinvest / * | Finance Server
70 Fri Nov 25, 2005 15:38:28 GMT -5 | 7 | Read : Access / Success | Finance Server | ROOT | Finance Server | FILE : DataSmartinvest inadmin / * | Finance Server
1 2 3 4 5 6 7 8 9 10 11 12
Done
My Computer

日志连续性及历史报告，
可即刻向管理及审计人員证明日志管理程序的完整性和持续性。

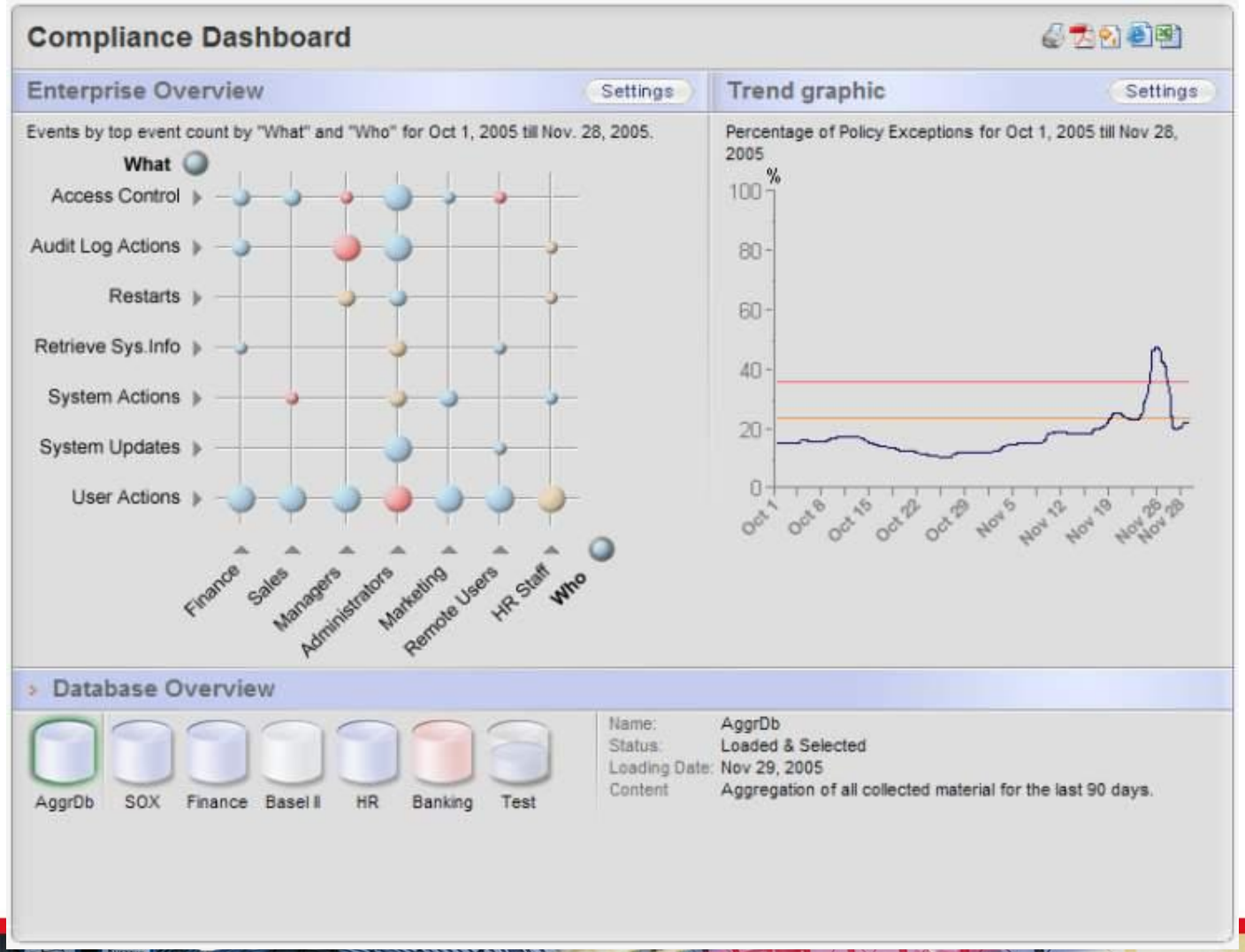
日志管理



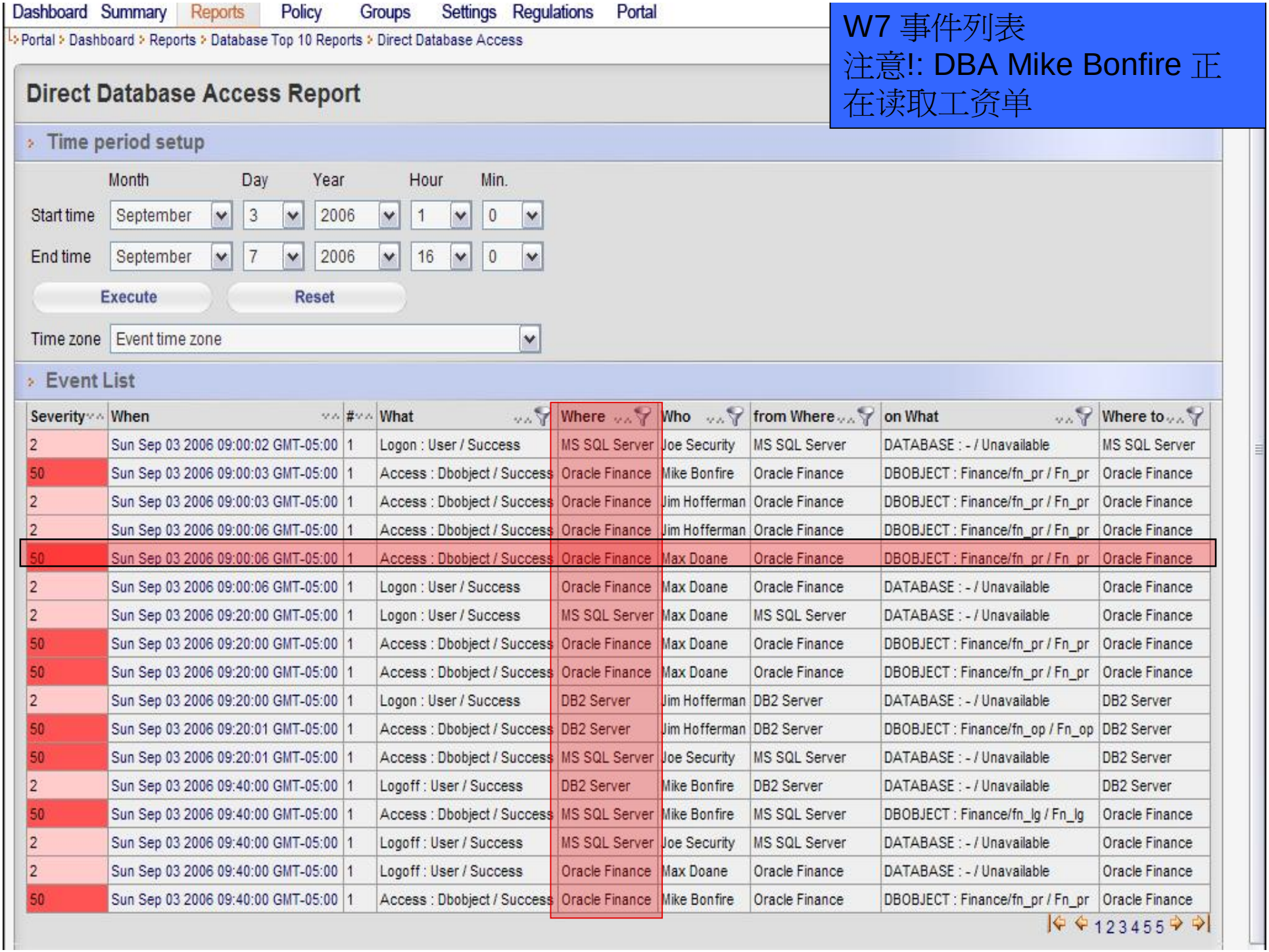
制度遵从显示板

W7 处理器后的日志– 通过一个简单的图形汇总几亿个日志文件！

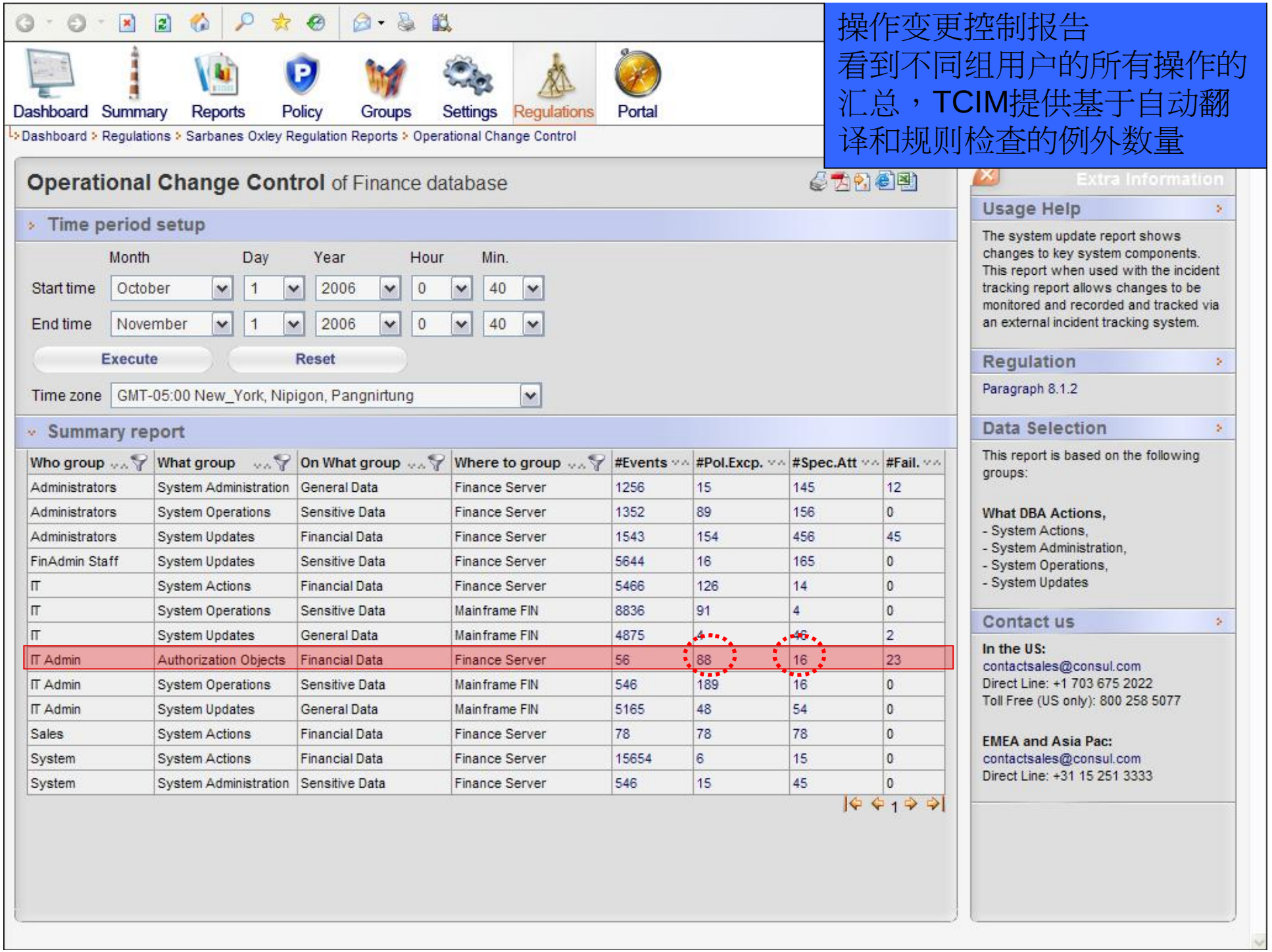
制度遵从显示板提供监控 / 报告



- 快速深入察看细节
- 违规
- 特别提示
- 故障
- 报告数据库
- 汇聚数据库
- 企业概述
- 报告分发



W7 事件列表
注意!: DBA Mike Bonfire 正在读取工资单


操作变更控制报告
看到不同组用户的所有操作的汇总，TCIM提供基于自动翻译和规则检查的例外数量
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
1
Extra Information
Usage Help
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
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

事件具体报告
可深入到具体事件并察看所有事件的具体情况，甚至能够深入察看原始的日志文件

Dashboard | Summary | Reports | Policy | Groups | Settings | Regulations | Portal

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 Hofferman	Administrators Database Admin Finance Admin	30 30 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 Hofferman

Investigate

Logrecords...

Extra Information

Help

Contact us

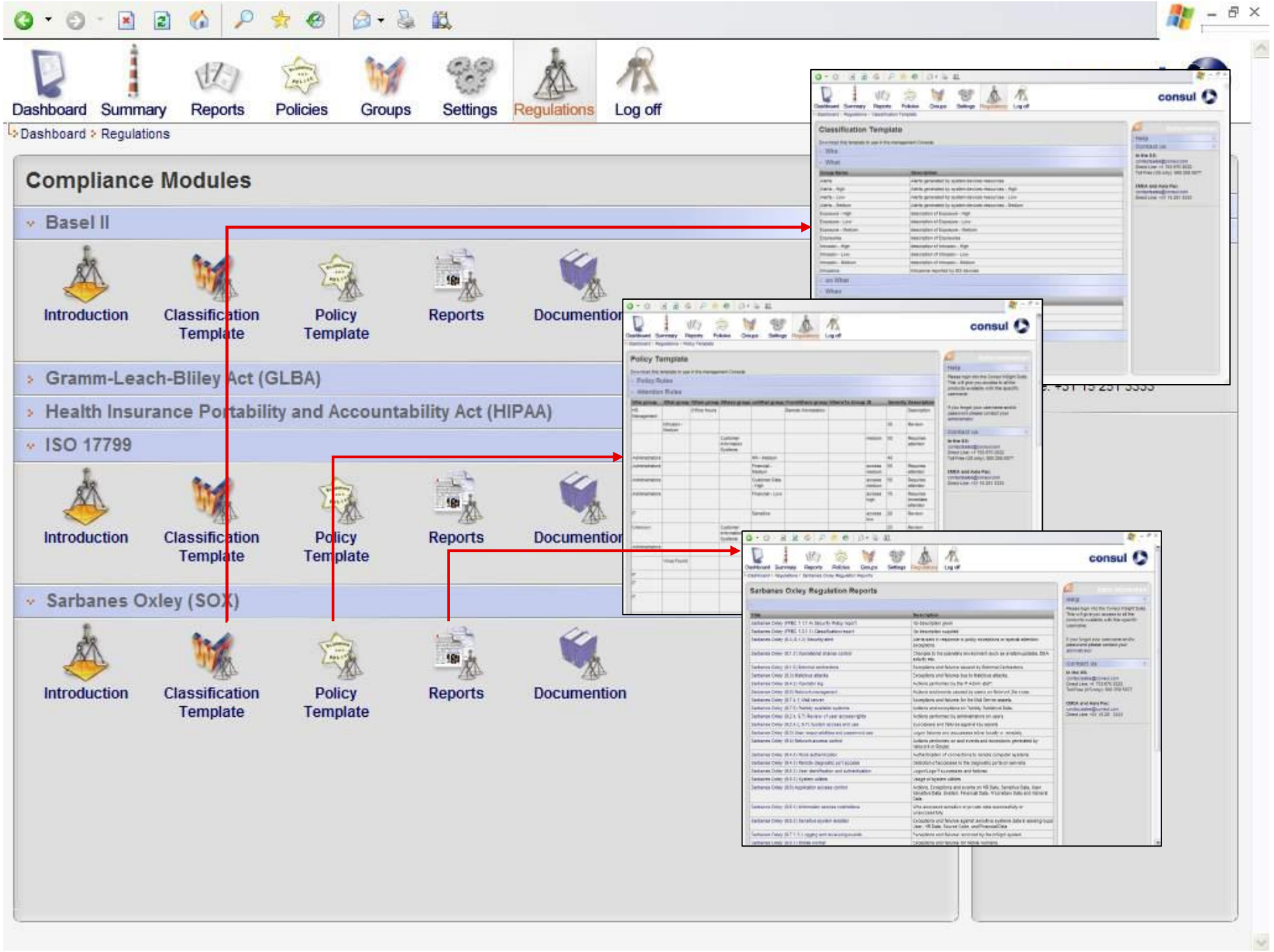
In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333

AUDIT_280503.AUDIT (C:\Documents and Settings\voss\Desktop) - GVIM2

File Edit Tools Syntax Buffers Window Help

My Computer


Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
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
consul
Classification Template
consul
Policy Template
consul
Sarbanes Oxley Regulation Reports

IBM Tivoli身份管理解决方案优势

- Tivoli 安全解决方案包括构建解决方案所需的IBM中间件
  - 數據庫(DB2)、应用服务器(WAS)、目录服务(TDS/TDI)
- 功能完善，一个方案解决所有关键需求
  - 集中用户访问和单点登录
  - 集中用户管理
  - 集中日志审计
- 利用即成产品缩短实现价值的时间
  - 通过配置可以实现更多的定制功能，不需要开发新软件组件
  - 丰富的API集合可供客户环境所需的定制集成所用
  - 高可用性、可扩展性、稳定性、审计和日志等非功能需求会大大提高开发成本，这些功能都已经在产品中提供
- IBM专业安全服务团队，长期的安全伙伴
  - 无论行业或地理位置，IAM要求跨组织的高度通用性


Thank
You


Kurzzug
Anfang