Pulse
Comes to You

IBM
Managing the World's Infrastructure

Privileged Identity Management

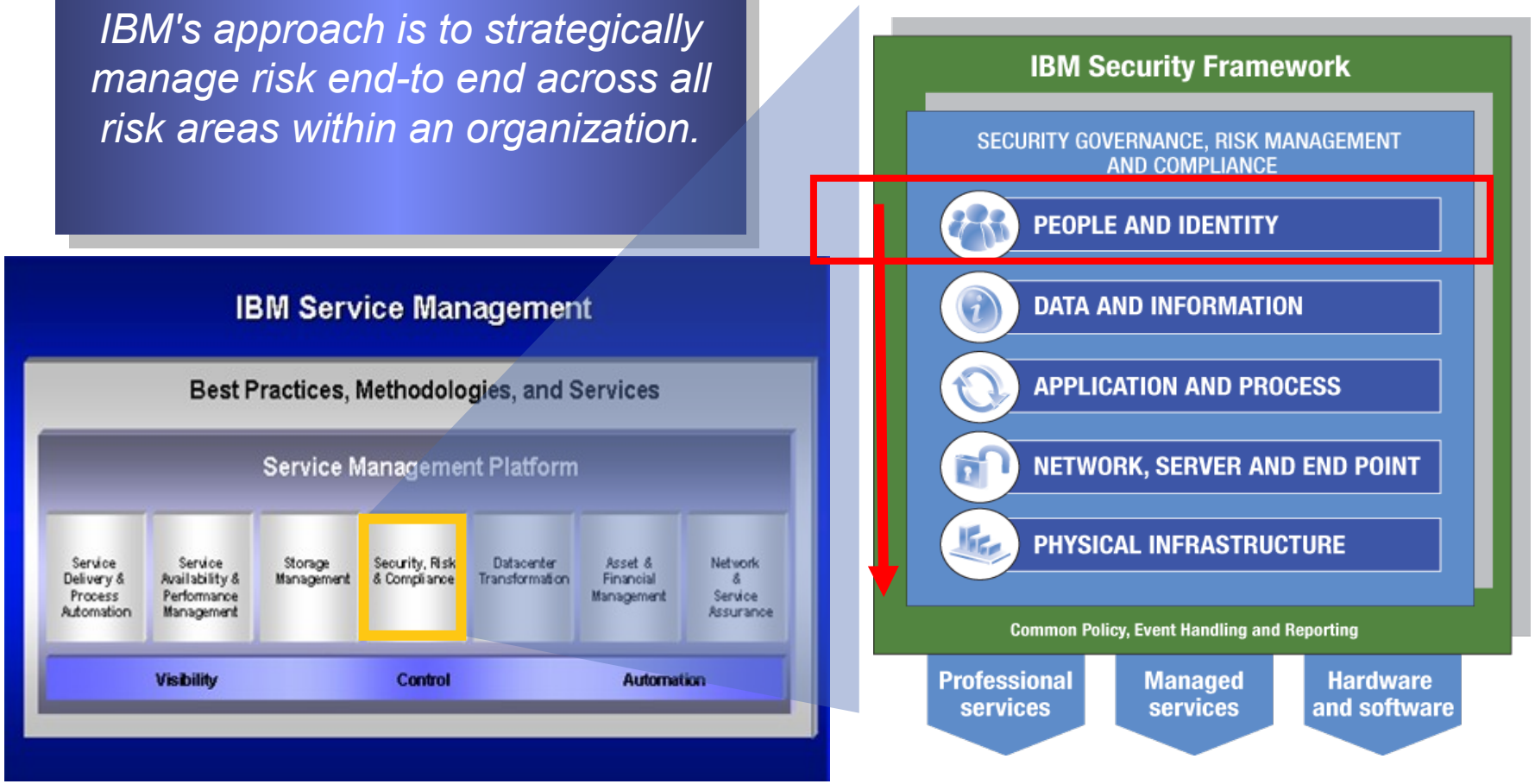
Nick Briers, IBM Tivoli Software

Agenda

- What is a privileged identity
- What are the management challenges for privileged identities
- Putting it all together with Tivoli Solutions to manage privileged identities
- IBM Services offerings and real user example
- Summary

IBM delivers a new approach to Security Management

IBM's approach is to strategically manage risk end-to end across all risk areas within an organization.



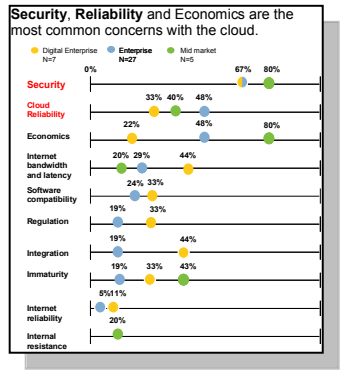
Building a smarter planet requires ***Secure*** Dynamic Infrastructure

Dynamic Infrastructure:

- The convergence of business and IT infrastructure into one dynamic infrastructure enables new breakthrough service opportunities.
- IBM's leadership in helping clients harness emerging capabilities, like cloud computing, provides a foundation for innovation.

Security remains a 'must have':

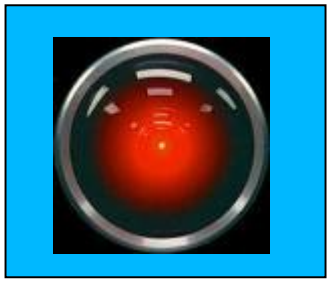
- Top of mind requirement for Cloud and DI
- Reduce Cost: reduces help desk and OPEX
- Manage Risk: persistent threats and compliance
- Improve Service: enable secure collaboration



What is a ‘privileged identity’?

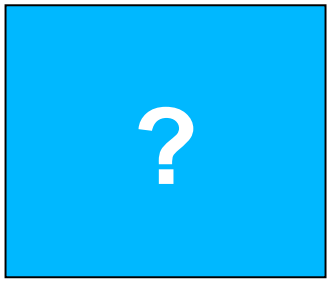
- Someone with IT permissions to:
  - Access highly sensitive data
  - Change critical IT systems
  - Conduct high value transactions
  - Cover their tracks in the audit trail
- As viewed by Analysts:
  - Forrester: PUPM (Privileged User and Password Management)
  - Burton: “The seedy underbelly” – PAM (Privileged Account Management)
- Who is a privileged user?

IT Administrators



System Accounts

Business Executives



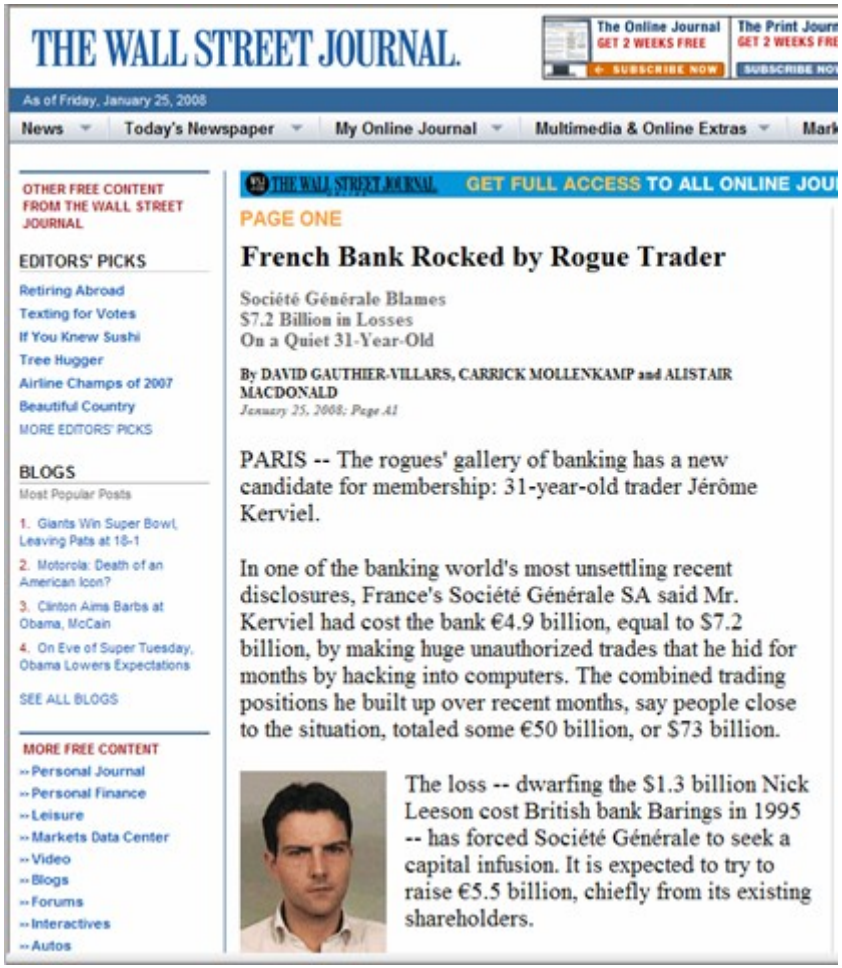
Other?

What damage can be done by privileged identities?

- Establish new user definitions
  - to perform work as a userid which is un-noticed by identity management policy enforcement
- Change other user's capabilities
  - inadvertent escalation of privilege to other users
  - create other privileged users
  - deny access to services required by a user
- Access sensitive information
  - copy, modify, or destroy
- Change audit logs
  - remove or modify file-based audit logs
  - modify audit log records
- Privileged identities may, by their intent, “own” a system

Who cares about privileged identities?

Malicious insiders care…



THE WALL STREET JOURNAL.

The Online Journal GET 2 WEEKS FREE SUBSCRIBE NOW | The Print Journ GET 2 WEEKS FRE SUBSCRIBE NO

As of Friday, January 25, 2008

News | Today's Newspaper | My Online Journal | Multimedia & Online Extras | Mark

OTHER FREE CONTENT FROM THE WALL STREET JOURNAL

EDITORS' PICKS

Retiring Abroad
Texting for Votes
If You Knew Sushi
Tree Hugger
Airline Champs of 2007
Beautiful Country
MORE EDITORS' PICKS

BLOGS

Most Popular Posts

1. Giants Win Super Bowl, Leaving Pats at 18-1
2. Motorola: Death of an American Icon?
3. Clinton Aims Barbs at Obama, McCain
4. On Eve of Super Tuesday, Obama Lowers Expectations

SEE ALL BLOGS

MORE FREE CONTENT

- Personal Journal
- Personal Finance
- Leisure
- Markets Data Center
- Video
- Blogs
- Forums
- Interactives
- Autos

THE WALL STREET JOURNAL. GET FULL ACCESS TO ALL ONLINE JOU

PAGE ONE

French Bank Rocked by Rogue Trader

Société Générale Blames
$7.2 Billion in Losses
On a Quiet 31-Year-Old

By DAVID GAUTHIER-VILLARS, CARRICK MOLLENKAMP and ALISTAIR MACDONALD
January 25, 2008; Page A1

PARIS -- The rogues' gallery of banking has a new candidate for membership: 31-year-old trader Jérôme Kerviel.

In one of the banking world's most unsettling recent disclosures, France's Société Générale SA said Mr. Kerviel had cost the bank €4.9 billion, equal to $7.2 billion, by making huge unauthorized trades that he hid for months by hacking into computers. The combined trading positions he built up over recent months, say people close to the situation, totaled some €50 billion, or $73 billion.

The loss -- dwarfing the $1.3 billion Nick Leeson cost British bank Barings in 1995 -- has forced Société Générale to seek a capital infusion. It is expected to try to raise €5.5 billion, chiefly from its existing shareholders.

The problem:

- 3 of the Top 10 Threats to Enterprise Security are insider related:
  - Employee error
  - Data stolen by partner/employee
  - Insider Sabotage
- Insider driven fraud costs US enterprises over $600 Billion annually

Who cares about privileged users?

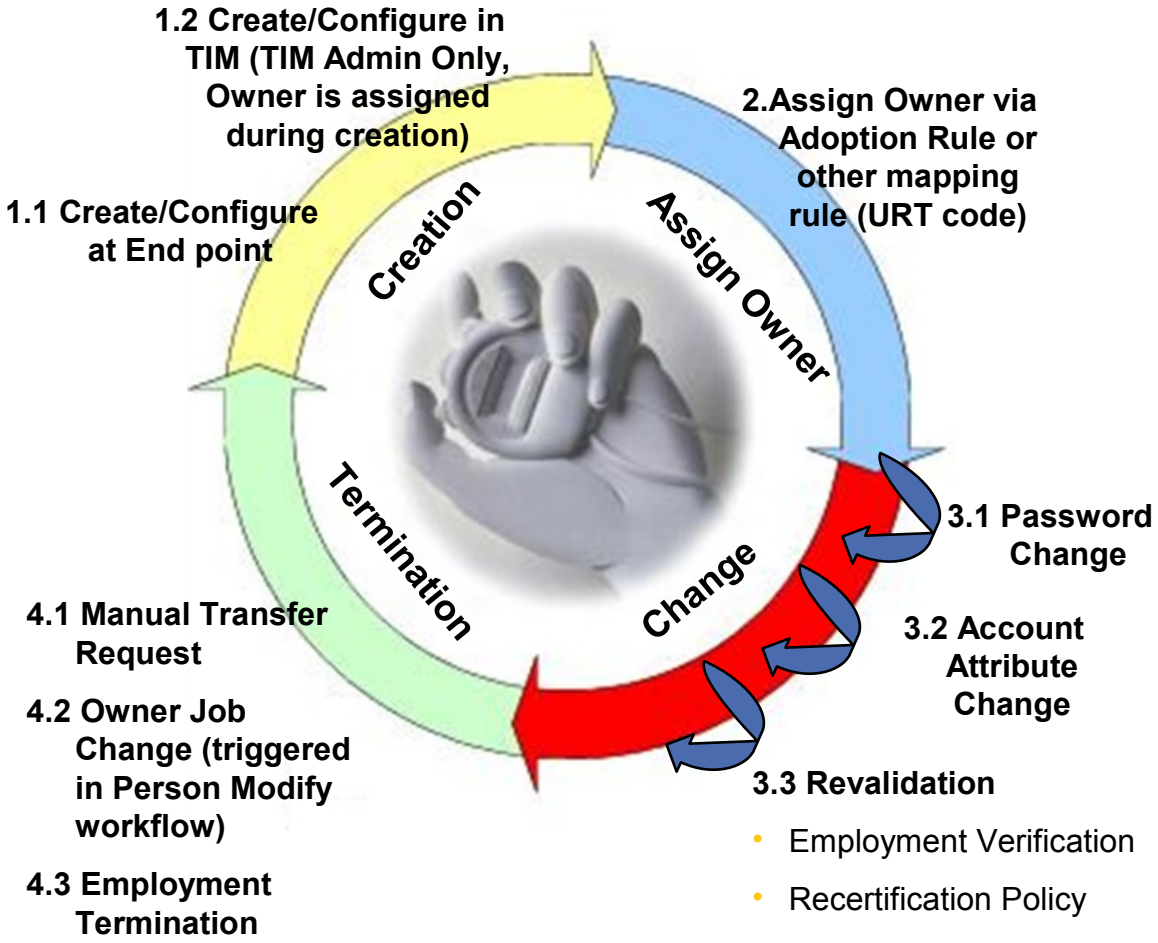
Your auditors care…

Regulatory Compliance Initiative	Relation to Privileged Account Controls
Payment Card Industry (PCI) Data Security Standard (DSS)	• Protect stored cardholder data (#3) • Develop and maintain secure systems and applications (#6) • Restrict access to cardholder data by business need-to-know (#7) ***Insufficient internal controls over privileged accounts negatively impact an organization's capability to meet these requirements***
California Senate Bill 1386 (now California Civil Code 1798)	• SC 1386 requires organizations that lose private information of California residents to report loss to affected individuals ***Unauthorized users of privileged accounts can bypass system controls to access private information without the organization knowing about it***
Sarbanes-Oxley Act (SOX) Section 404	• Requires corporate management to take responsibility for establishing and maintaining adequate internal control structure and procedures for financial reporting • Requires management to assess and report effectiveness of the internal control structure and procedures for financial reporting ***Insufficient internal controls over privileged accounts can have a negative impact on an organization's ability to meet these requirements***

Source: The Burton Group

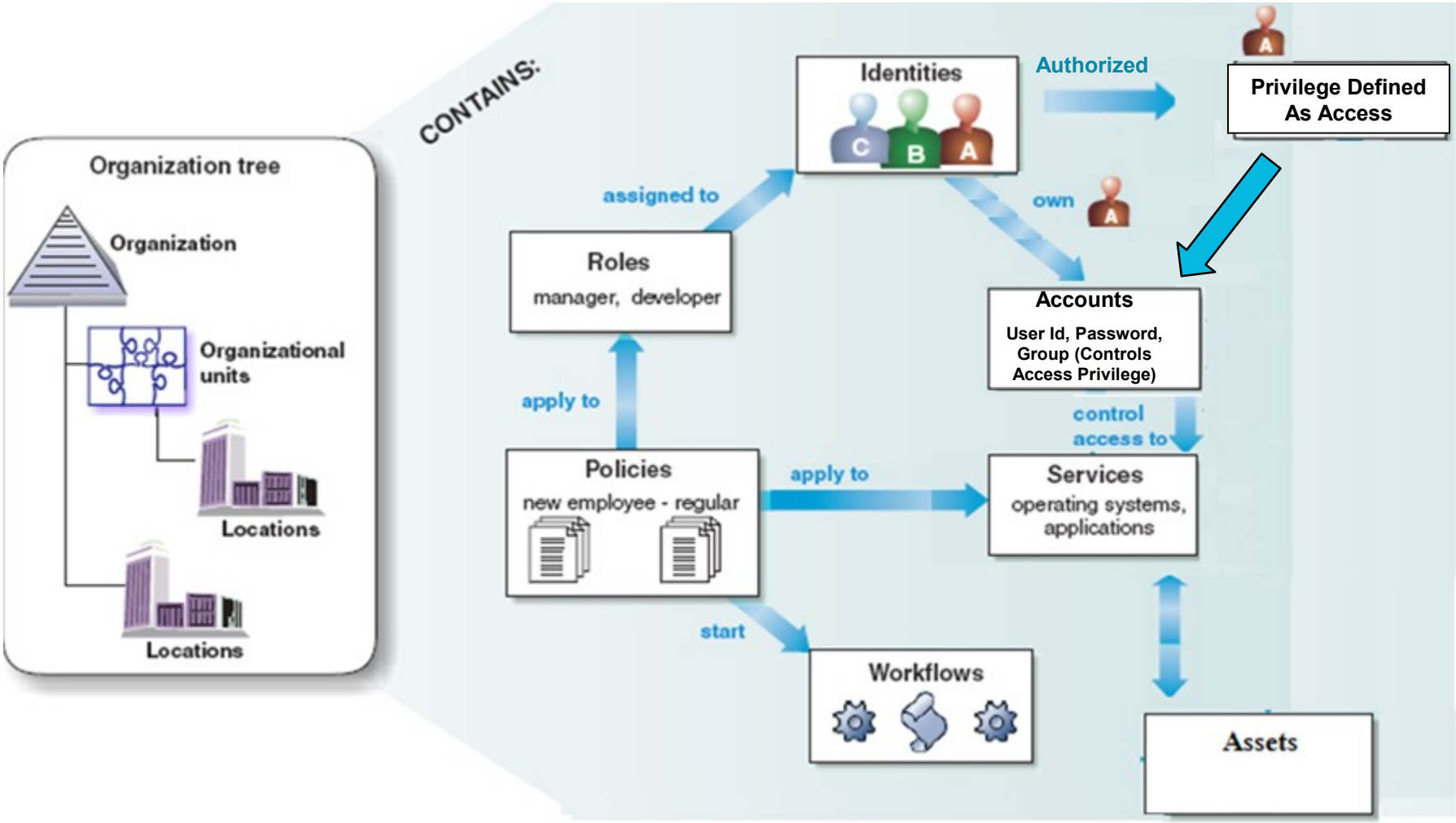
Identity and Access Assurance manages privileged identity risk with a complete, closed loop process

Shared Privileged ID Account Lifecycle Management in Tivoli Identity Manager (TIM)



- Privileged ID accounts in TIM are flagged and can be enabled for sharing.
- Specific Access Control is required for Privileged ID via TIM ACI
- Specific Lifecycle workflows are required for lifecycle change events of shared ID (Create/Modify/PasswordChange/Suspend/Delete)
- Password Change needs to support privilege sharing

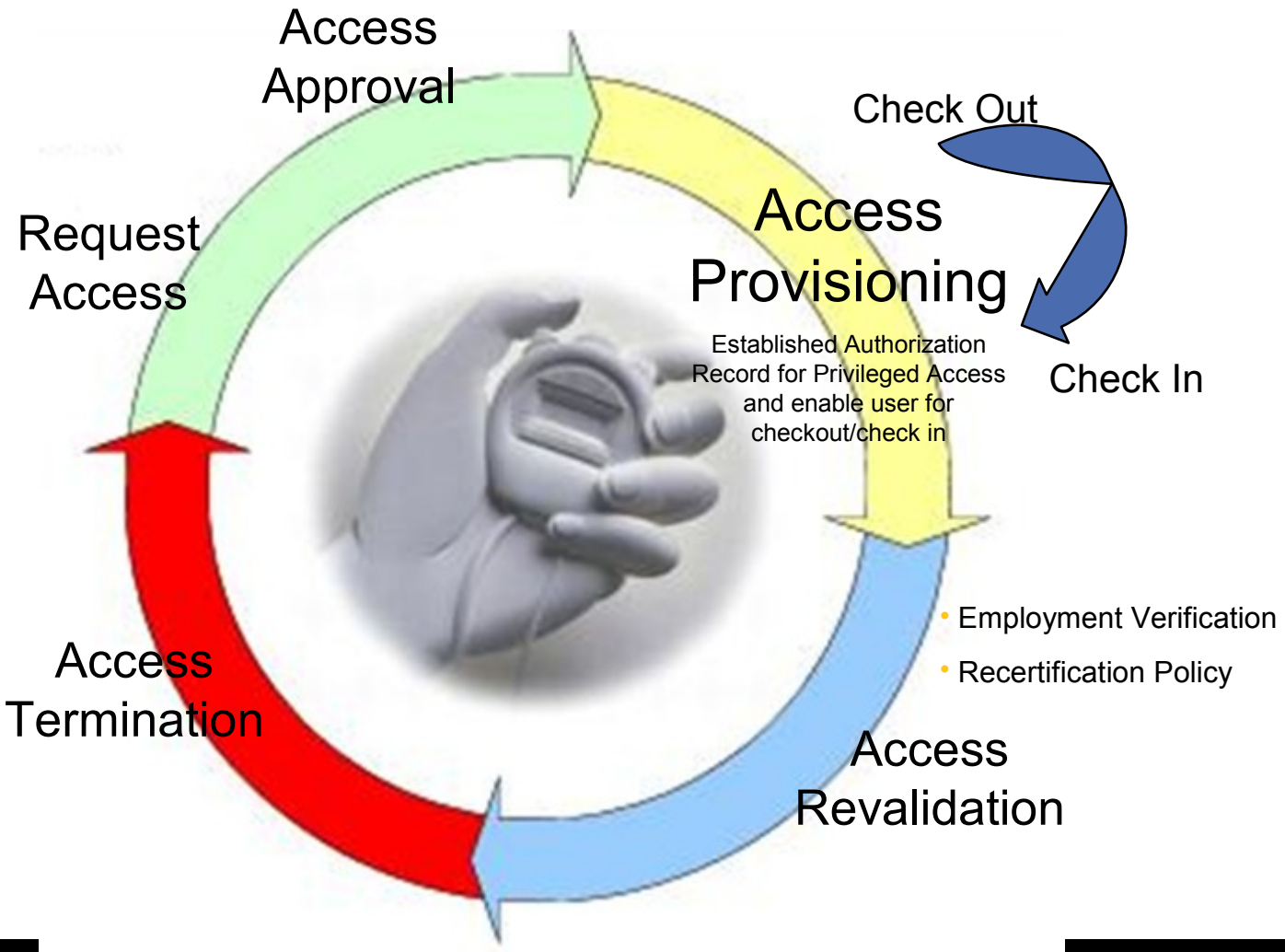
Privilege Identity Management with TIM 5.0 only



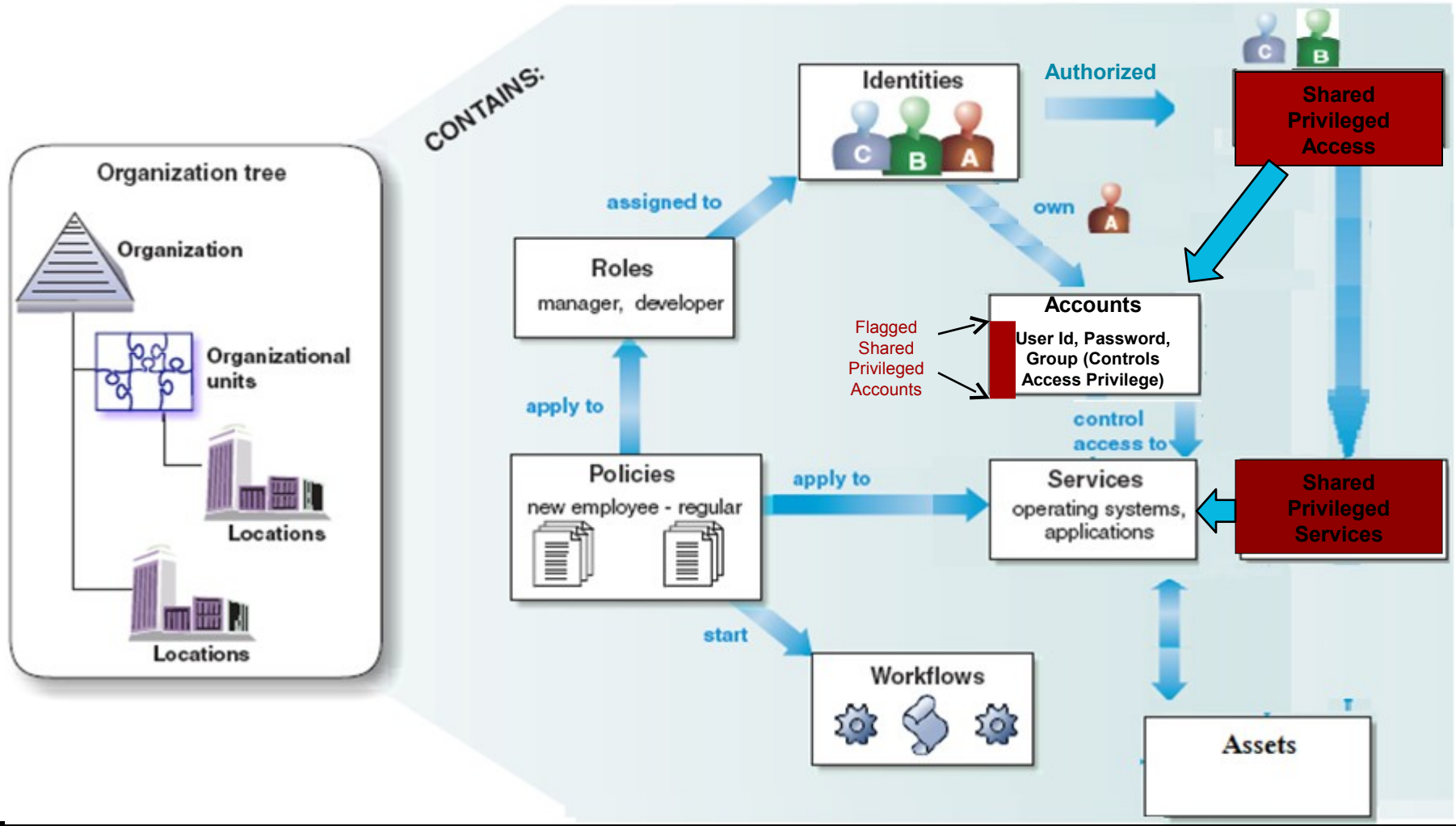
Challenges with ‘business as usual’ approach

- Privileged identities are shared
- No audit trail – Joe signed on to work station but administrator signed on to SAP for example
- Difficult to manage good practices
  - For example changing passwords frequently requires all sharers to be informed

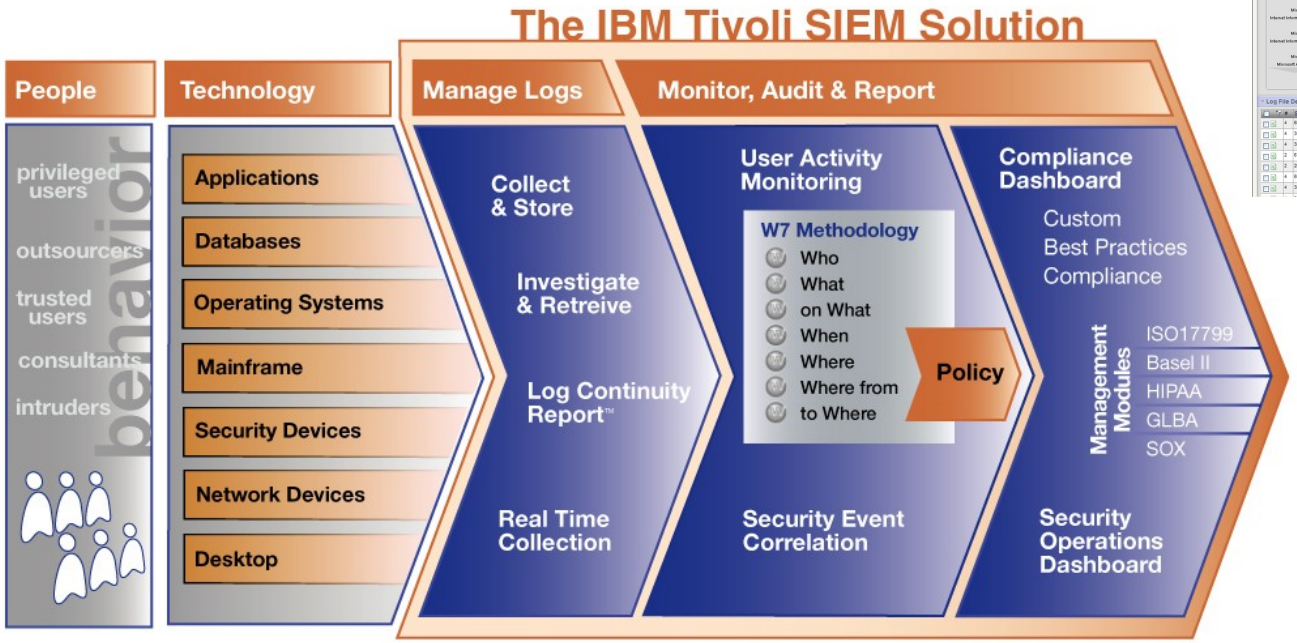
Shared privileged identities require additional controls

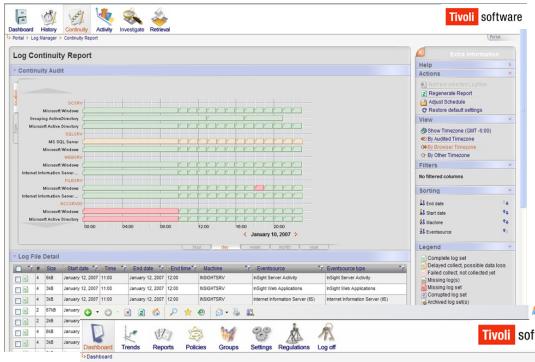


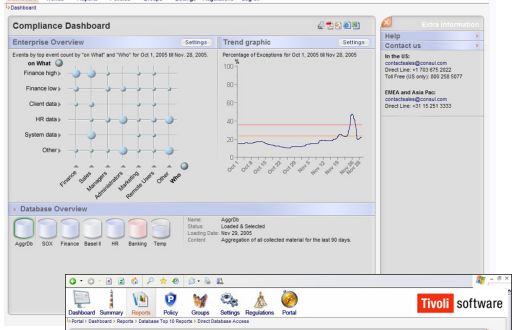
Shared privilege identity management – Integration of ID Management and Single Sign-on solution

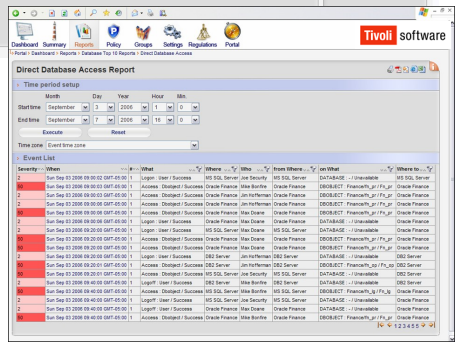


Compare activity of privileged identities against ‘white list’ policies and regulations

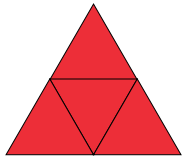








Putting it all together -Privileged Identity Management Solutions

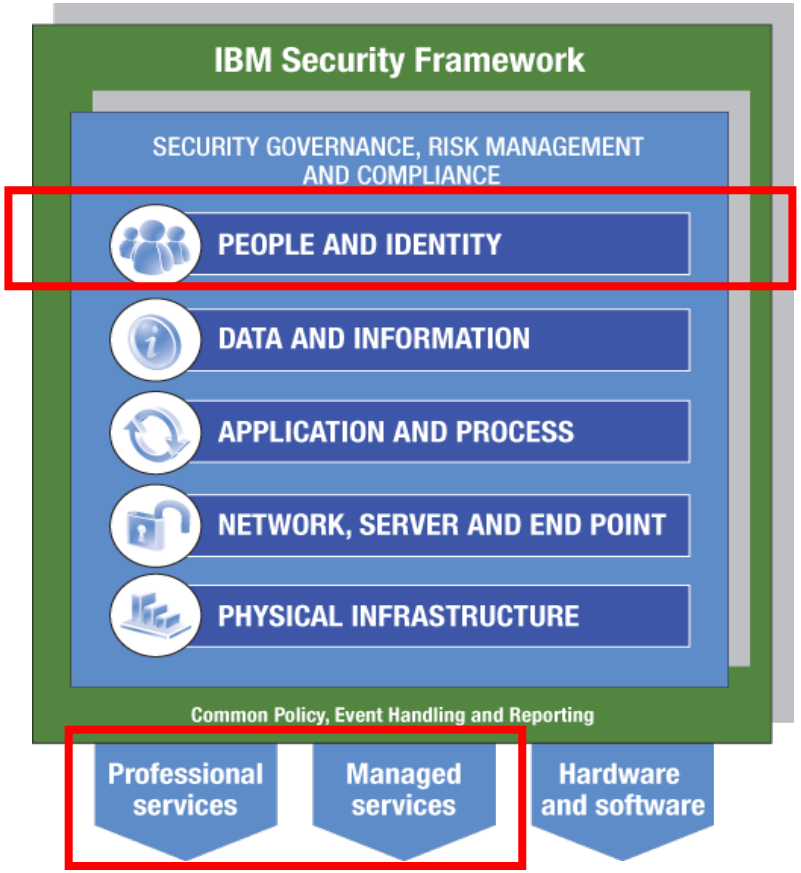


- Leverage your IAM infrastructure (*Tivoli Identity Manager*)
  - Approval workflows to enforce least privileges and business need-to-know
  - Ensure password management/ regular password changes
  - Centralized ID management and password management and password store improves overall control and security
- Exploit your SSO infrastructure (*Tivoli Access Manager for Enterprise Single Sign-On*)
  - Utilize check-in/ check-out (see upcoming example)
  - Single sign-on of all privileged IDs with strong authentication option
- Control access to OS infrastructure (*Tivoli Access Manager for OS*)
  - Limit the rights of privileged users by restricting and auditing 'root'
- Leverage your SIM infrastructure (*Tivoli Compliance Insight Manager*)
  - Audit real user access
  - Audit privileged identity access
  - Correlate and report

Agenda

- What is a privileged identity
- What are the management challenges for privileged identities
- Putting it all together with Tivoli Solutions to manage privileged identities
- IBM Services offerings and real user example
- Summary

Our managed services provide a complete solution for management of privileged IDs and users



- IBM Internet Security Systems (ISS) provides managed and professional Services for Tivoli Security products
  - Designed to help you realize the full benefits from your investment in Tivoli software
- Our managed services offerings include:
  - Managed provisioning
  - Managed authentication
  - Managed user monitoring
- Together these services can help you:
  - Control authorizations to privileged accounts on critical resources
  - Manage authentication of privileged users
  - Monitor privileged user activities

How we helped a customer struggling with privileged ID management

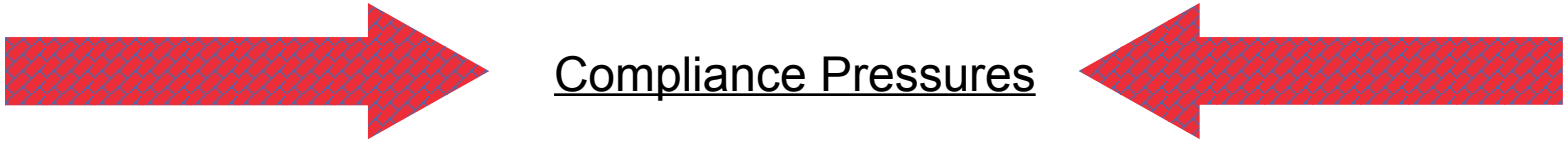
Customer Overview

- Retail industry customer with over 4,000 stores nationwide

Requirements

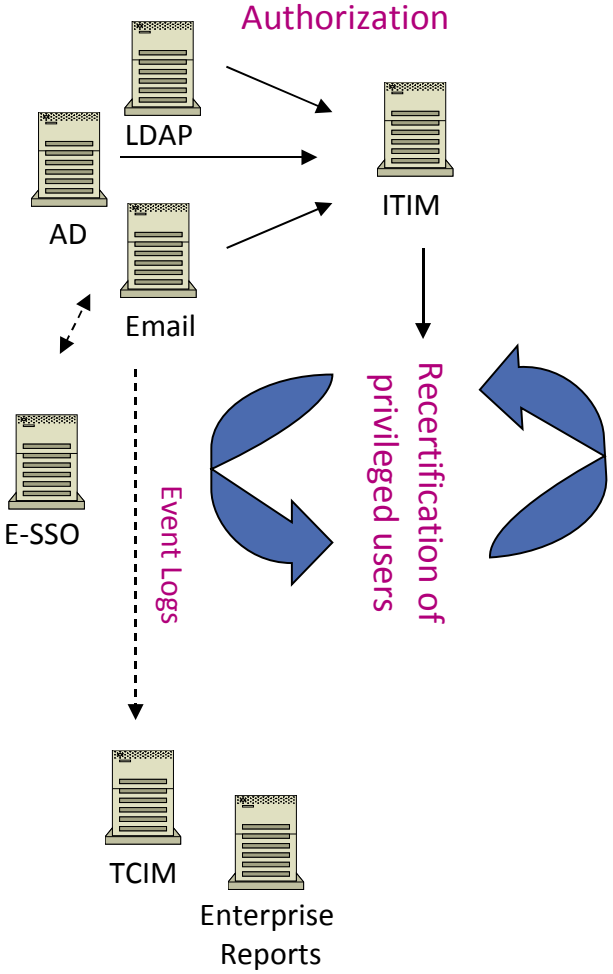
- Minimize number of distinct privileged user accounts
- Ensure all privileged accounts have proper authorizations
- Monitor activities of authorized privileged users … without impacting availability and performance
- Enable system operator to securely check out privileged ID for emergency or temporary access

Compliance pressures had made these requirements all the more urgent



- Privileged accounts needed to have proper authorizations and have evidence to show this
- Termination of privileged access should be timely
- Accountability needs to be maintained, even with shared user or service accounts
- Privileged user activities must be monitored and recognizable

Through use of three Tivoli products and services assets, we were able to meet our pilot requirements



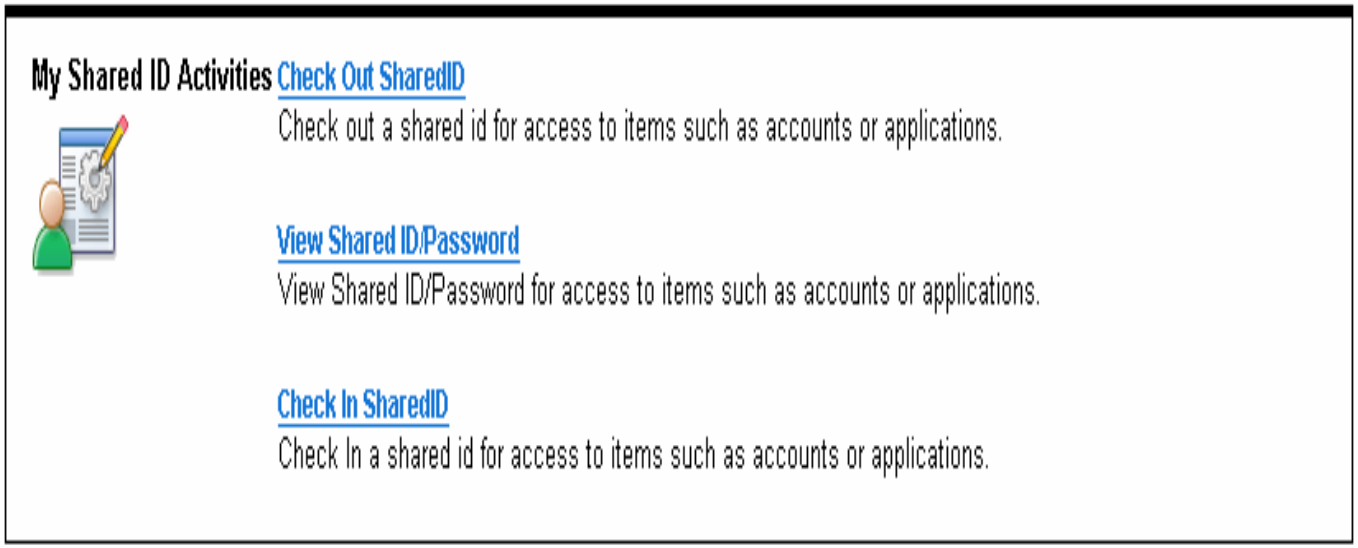
1
- Enforce authorization processes before entitlements are given and capture unauthorized privileged accounts based on group membership
- Flag the privileged users and their accounts as privileged

2
- Periodically recertify account authorizations through a consistent work flow.
- Disable accounts that are not recertified within a defined timeframe.
- Measure percentage complete for privileged certifications as part of a compliance program

3
- Monitor activities such as:
  - Creation of user accounts
  - Deletion of log files
  - Access to files defined as sensitive
  - Addition of privileges to accounts or groups

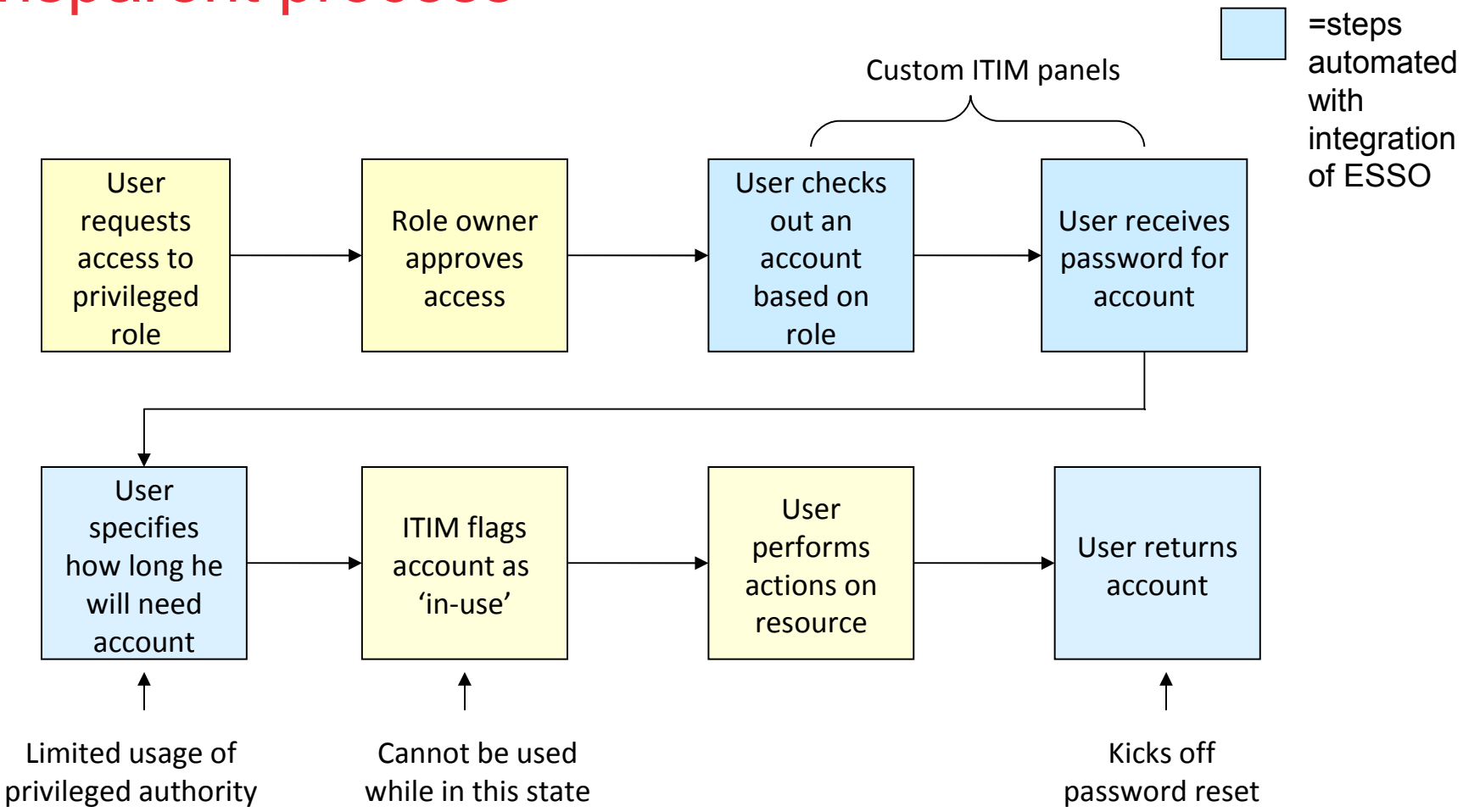
4
- Provide centralized authentication

Tivoli Identity Manager 5.0 along with IBM assets helped limit access to privileged/shared accounts



- Extension to Tivoli Identity Manager self-service user interface
- Supports check in/out of shared IDs and viewing of shared ID/password

Integration of TAM ESSO enables a streamlined, transparent process



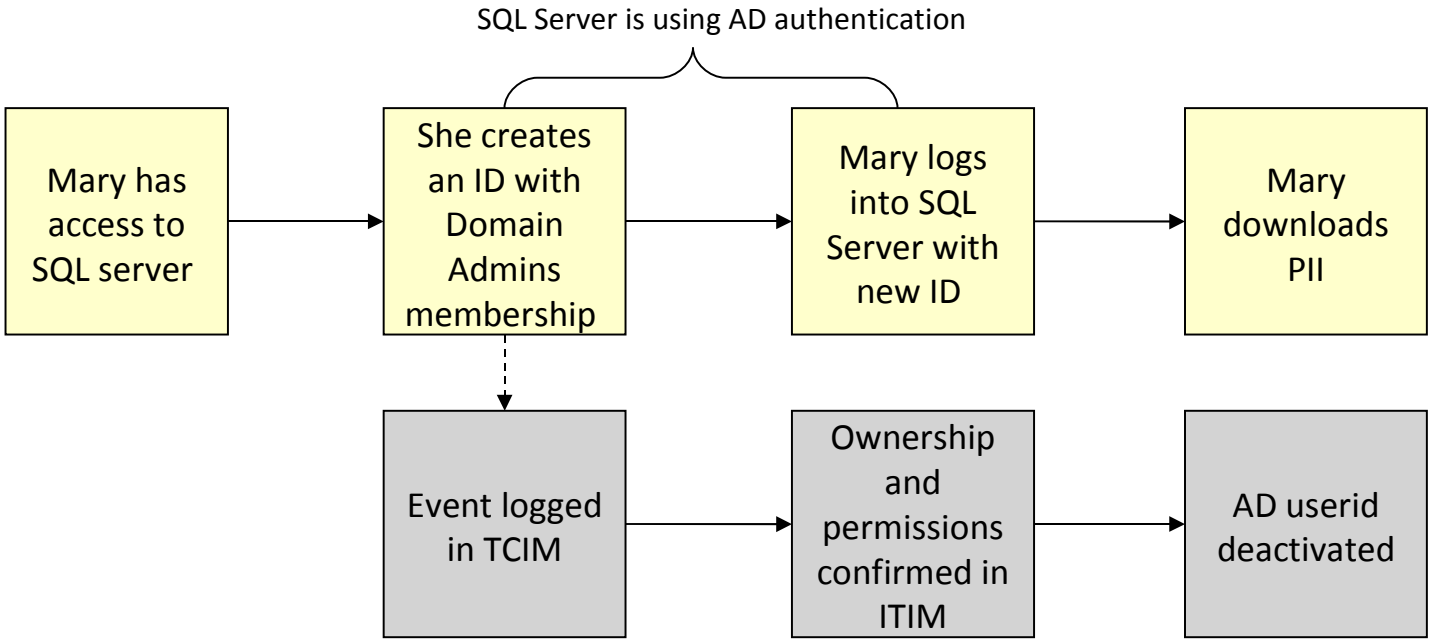
TCIM enabled advanced functionality to check user behavior through defined use cases

Analysis engines (iView) allowed reporting and alerting on both potential and objective compliance gaps such as:

- **Creation of user IDs** – bypassing provisioning system
- **Addition of privileges to IDs or groups** – bypassing provisioning and authorization workflow
- **Deletion of IDs** – removing accountability
- **Allowing direct root access** – violating technical standard
- **Clearing or editing log files** – removing accountability; potential change management violation
- **Adding someone as admin** – bypassing provisioning and authorization workflow
- **Access to file / dataset defined as sensitive –** potential regulatory or PII issue
- **Multiple and/or sequential changes to user ID ownership –** odd user behavior
- **Multiple and/or sequential changing of passwords** – off user behavior

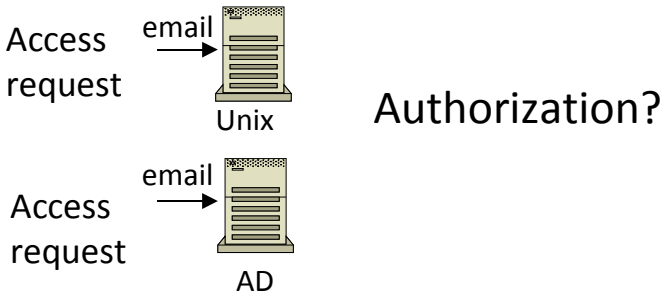
Deploying and running the TCIM components as a managed service eliminated need to find trained staff and allowed for increased consistency and reduced total cost of ownership

ITIM and TCIM were used to recognize and react to privileged misuse of IT resources



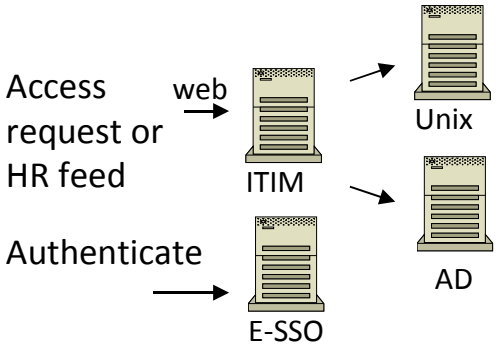
Incorporation of ITIM and E-SSO greatly improved security and compliance

Old Model …



- Access requests provided often via email with no approval chain of evidence
- Hard to differentiate privileged needs versus general user
- One account per system per user

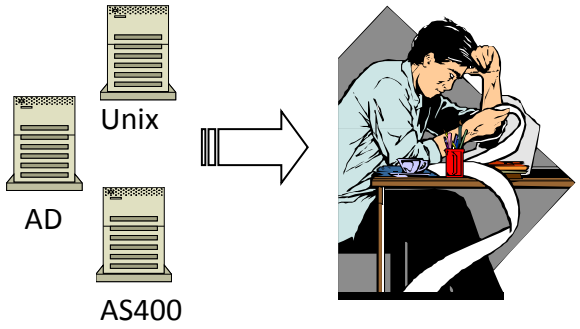
New Model …



- Authorizations for privileged access centrally governed with chain of evidence in transaction tables
- Check-in and check-out functionality to minimize need for individual accounts (less is more)
- Ease of use with single sign-on

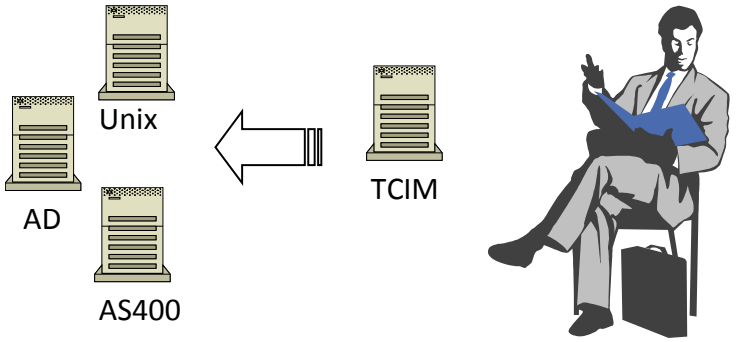
Through the deployment and support of TCIM, privileged monitoring greatly matured

Old Model …



- Volumes of data with no aggregation
- Required expertise on each log type for interpretation
- Prioritization of events extremely difficult
- No reporting functionality
- Not forensically sound (e.g., chain of custody, handling)

New Model …



- Mapping of all heterogeneous log data onto a common naming convention (W7)
- Original log files preserved and data analysis performed outside original
- Ability to create policies to automatically filter and prioritize

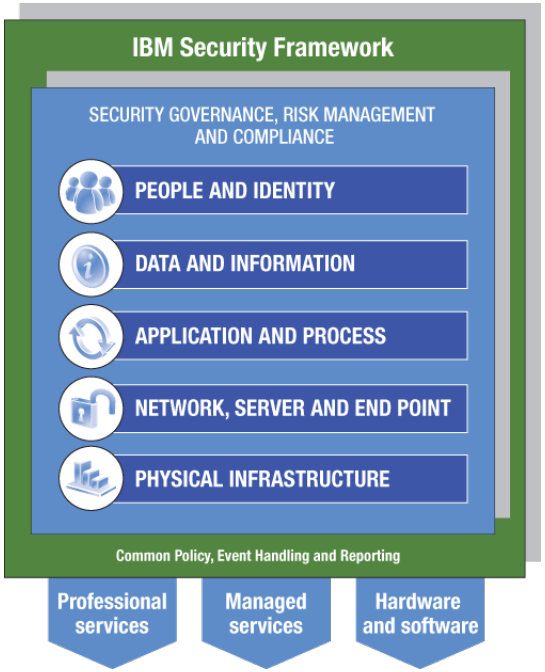
IBM's unmatched security investment and worldwide skills deliver innovation and end to end solutions for our customers

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

IBM Launches $1.5 Billion Security Initiative
The program is designed to recalibrate a customer's compliance and security offerings across IBM's five domains of information technology security.

By Thomas Claburn, InformationWeek
Nov. 1, 2007

IBM on Thursday announced a major security initiative encompassing products, services, and research to help businesses manage risk and keep information safe. To support the initiative, IBM said it plans to spend $1.5 billion on security-related projects in 2008. ...



- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 200+ security customer references and 50+ published case studies
- 40+ years of proven success securing the zSeries environment

Questions?

Additional Information

Define Security Requirements and Policies

- Goal: Mitigate Risk to the organization
- Solution:
  - Seek to eliminate the usage of singly all-powerful userids
  - Spread the capabilities for administration across a set of roles
  - Require user-specific login and interaction with all systems, a user may take on several roles
  - Require and enforce separation of duties between roles
  - Define policies for exception handling, including human approval processes for emergency user of all-powerful userids
  - Require strong authentication for privileged users

Enroll Users and Provide Self Service

- Goal: Enable administration within defined policies
- Solution:
  - Enforce a set of checks and balances in identity administration
  - Employ an approval process for users to act in sensitive roles and capabilities
  - Ensure that “service” userids are never used for interactive use
  - Verify that ALL users defined on systems are accounted for!
  - Have a “emergency” procedure for exceptional situations and recovery processing

Automate Access Rights Provisioning

- Goal: Eliminate manual and ad-hoc administration of access control settings
- Solution:
  - Create a roles-based access control model
  - Reduce access control administration and increase role membership administration
  - Employ the fine-grained access control enforcement capabilities of the systems and applications which privileged users use
  - Utilize tools including TAMOS, 'setuid' programs, and similar capabilities for systems administration tasks

Control User Access to Resources

- Goal: Guarantee that the right accounts are used for the right tasks
- Solution:
  - Centralize authentication and credential transform services
  - Require user-specific credentials be used as deep as possible in the computing environment
  - Ensure that various system-level user/account defintions are not usable in interactive modes (e.g. NOLOGIN settings)

Monitor User Activity

- Goal: Validate that no un-expected behavior occurs … and when it does you know when, where, and by whom
- Solution:
  - Actively monitor and report on user capabilities and role relationships
  - Monitor systems and activities of all users which may act in sensitive roles
  - Ensure separation of duties between monitoring and operations
  - Remind privileged users of the infrastructure in place
  - Correlate user and privileged identity

Account Administration

- Privileged users can often define and/or update other user definitions.
  - Seek to extinguish such capabilities except in emergency situations
  - Employ a process for approving the definition or modification of sensitive userids
- Privileged userids are often defined for emergency administrative use
  - Require human approval for emergency usage
  - Monitor any actions performed by privileged userids and actively review the reports
  - Require reset of the account upon completion of the task/situation
- Service IDs
  - Password changes for service IDs must often be coordinated with application server configuration changes
  - Employ a process for accomplishing this – do not simply mark these userids as having non-expiring passwords
  - Ensure that these userids cannot be used for interactive use

Account Authentication

- Privileged user accounts are often used for direct interaction with the system or device for emergency purposes
  - Utilize a set of defined roles and granular access control checking and 'sudo' or command verifier applications to enforce a separation of duties
  - Consider requiring stronger authentication for users which are allowed to perform administrative tasks in interactive mode
- Privileged user accounts that are used for “service IDs” or for systems management functions are often also used for interactive administration on the system
  - Utilize all means to constrain the capabilities of “service IDs”
  - Ensure that “service IDs” cannot be used for user interactive work (e.g. NOLOGIN)

Account Authorization

- Even privileged users often have access control settings which can be used to limit their behavior
  - Utilize granular access control rules and separate roles to limit the scope of capabilities of individual users
  - On Unix systems employ tools such as 'sudo' to limit users' behavior
  - Seek to establish a complete set of 'sudo' rules and granular access controls based on role such that permissions updates are rarely required
    - Employ a process which includes human oversight for any access control rule changes
  - Allow users to perform operations based on the roles they are allowed to act in rather than granting the user explicit permissions to sensitive operations
- Some systems allow for a distinct separation of duties to be employed
  - In RACF, a userid should not have both “SPECIAL” and “AUDITOR”.
  - Verify that expected separation of duties is maintained and that user definitions are set up as expected per the policies defined

Account Auditing

- Privileged users often have access (read and write) to any logs of what operations they (or others) may perform.
  - Utilize granular access controls to protect logs from modification
  - Eliminate usage of all-powerful userids except for emergency situations and only after human approval at the time of use
- Passive logging of operations performed by privileged users is often used as a means of being able to do forensic analysis.
  - Log successful and unsuccessful operations of privileged users
  - Protect and gather the logs
  - Review reports on the activities of privileged users – look for anomolies

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

Bu sunum 28 Mayıs 2009 tarihinde Swiss Otel'de yapılan Tivoli Pulse 2009 toplantısı için hazırlanmıştır.

http://www.ibm.com/software/tr

http://www.ibm.com/software/tr/tivoli