IBM Software Group

Leveraging the Mainframe – Audit and Compliance Management

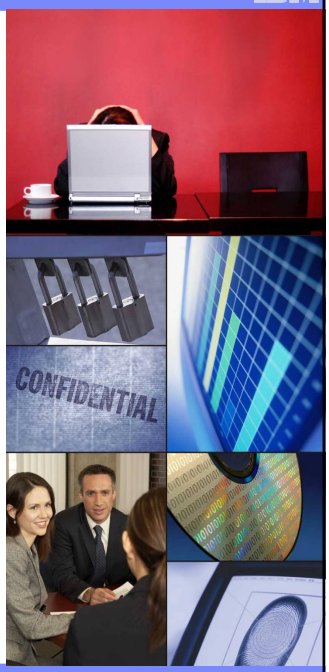
Glinda Cummings, CISSP, Worldwide Product Manager, zSecure

Tivoli. software

IT security challenges

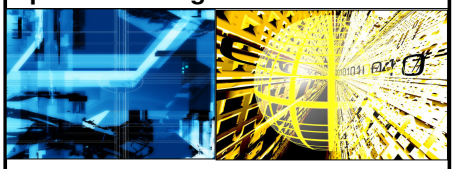
Need to maintain business innovation and growth in the face of risks, while decreasing operational costs

- Increasing *complexity* of security issues in today's environment
- *Compliance* with regulations and audit requirements is difficult
- *Managing change by limiting* and *tracking access* to sensitive or private information and assets
- Establishing a *trusted relationship* with customers and partners
- Protecting against *security incursions* and *risks to confidential information*
- Security issues are hurting the *bottom line!*



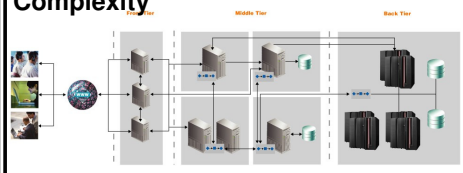
Market dynamics are creating new IT challenges

Speed of Change



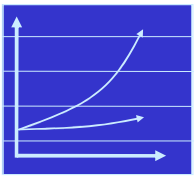
Fast-changing external forces and unpredictable workload make it difficult to meet service levels.

Complexity



Most organizations manage large and complex IT environments with many user types to support business processes.

Cost



Infrastructure costs have been outpaced by spending on management and administration.

Compliance

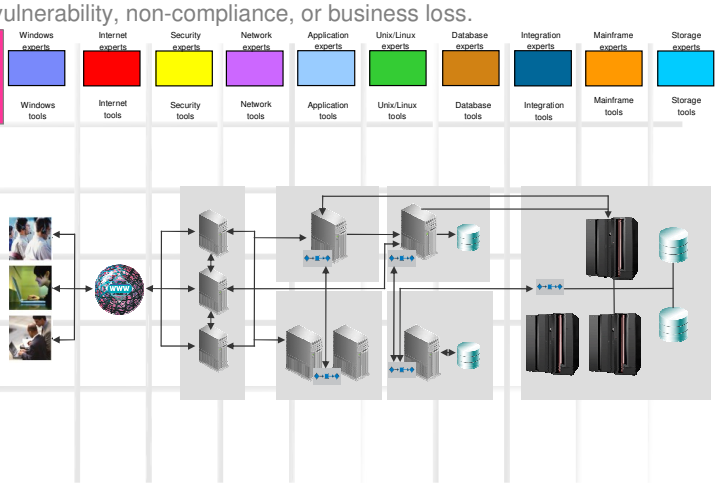
The changing global regulatory and business environment requires security, identity, access and ongoing audit capabilities.

IT Security Management is Complex

The unpredictability of security-related events and workloads, leads to increased likelihood of error, vulnerability, non-compliance, or business loss.

Today's Process view of IT Security Management

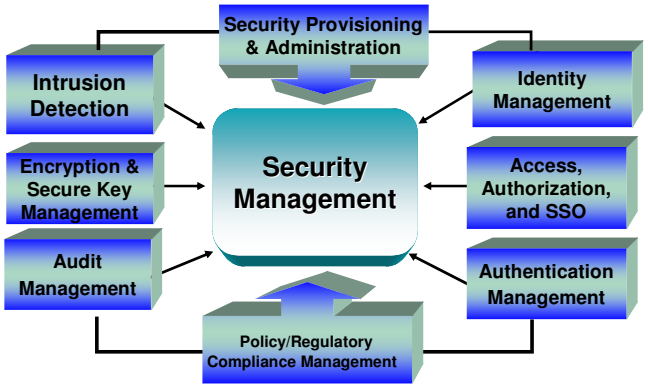
- Security Configuration
- Vulnerability Management
- Security Patch Management
- Access Management
- Privacy Management
- Identity Management
- Security Event Management
- Incident Management
- Threat Management
- Policy Compliance
- Regulatory Compliance
- Business Risk Management



Your Conflict: Regulation versus Reality

Regulation	Reality
▪ Change management – Clearly defined process with approval and reporting – Ability to identify changes ▪ Security management – Separation of duties – Identification of exposures and mis-configurations – Clear audit trail and accountability ▪ Data security – Data confidentiality and integrity – Prevent improper access to financial, medical or personal data – Monitor access to data by technician, administrator, outsiders	▪ Separation of duty impractical with small teams ▪ Highly authorized ids necessary for final go-to technician ▪ Mainframe installations often rely on “system special” and “uid(0)” ▪ Red-tape bypassed for high-impact problem resolution ▪ Manual monitoring impractical due to volume of data ▪ Human mistakes cause service outages ▪ Cleanup projects are long running and expensive

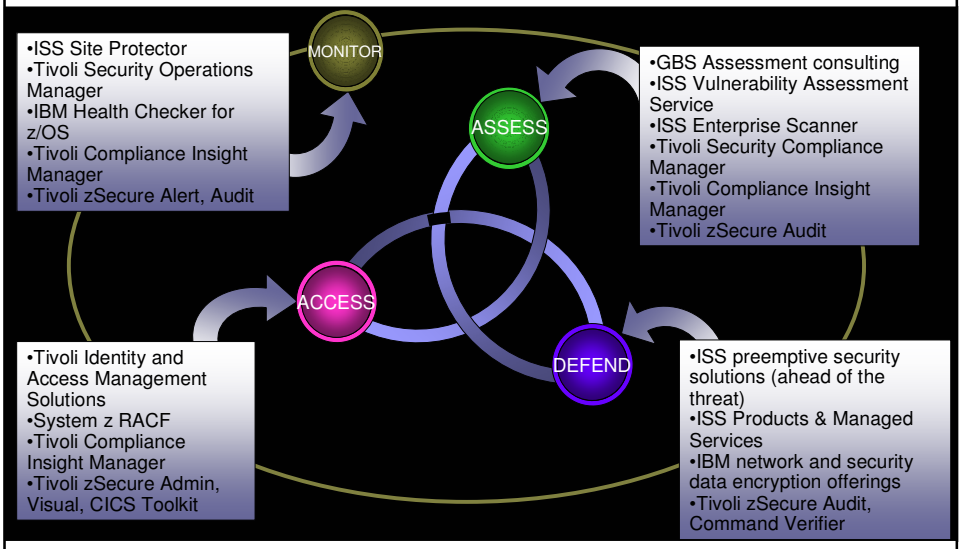
What Makes Up End-to-End Security Management



Five Common areas of concentration

- Authentication
  - Determine who or what is talking to us
- Authorization
  - Allow the right people or entities to do the right things
- Administration
  - Set up and configure things within the IT infrastructure
- Audit
  - Make sure settings are as expected, and help identify what needs to be addressed
- Encryption
  - Protect information from misuse or access by paths other than those intended (and protected). Also detect whether information has been inadvertently modified

IBM's security management vision and strategy:
Preemptive, comprehensive security and compliance offerings



System z Security Considerations

- IBM's goal:
  - Establish the mainframe as the hub for enterprise security management
  - Maintain leadership position in Service Management software market
- Pain Points
  - Customers face the growing complexity of IT environments, the rising costs of managing IT, and the increasing number of compliance initiatives & requirements
    - Must manage security risks, address burgeoning compliance requirements, and support their core business, all with limited resources
  - Customers need a highly secure business environment that complies with standards, providing the right levels of capacity, integration, and cost efficiency
- Customer Requirements
  - System integrity, reliability, availability, scale and performance
  - Simplify the complexity of their infrastructure, with security controls
    - Integration with applications including CICS, IMS, and DB2
  - Make System z & z/OS easier to deploy, administer, and service
    - Currency with latest versions of z/OS and RACF
  - Ability to manage and monitor user activity across the enterprise
    - Need for integrated audit and security event reporting
    - Provide linkage to enterprise-wide identity and access management
  - Ability to demonstrate compliance to key industry regulations and corporate requirements

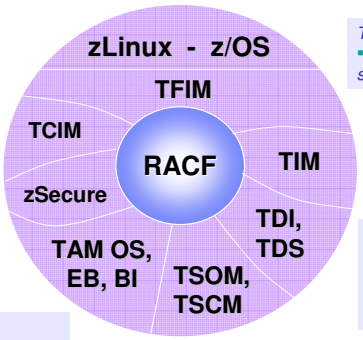
Enterprise Security with System z and Tivoli

- Powerful security for simplified risk management
  - Building on its leadership in IT security, IBM System z is advancing its network and data encryption solutions, strengthening its role in end-to-end security across the enterprise and providing new tools to help address the growing compliance requirements, enabling your business with simplified risk management and governance
  - Customers are leveraging the availability, scale and performance of the IBM System z mainframe to provide a centralized hub for enterprise security on z/OS with Tivoli offerings
- Tivoli zSecure suite and Compliance Insight Manager provide:
  - Integrated mainframe administration and audit and compliance monitoring
  - Distributed log management, access monitoring and compliance reporting
- Additionally, the relational value of Tivoli identity management provides:
  - Identity lifecycle management (user self-care, enrollment and provisioning)
  - Identity control (access and privacy control, single sign-on and auditing)
  - Identity federation (sharing user authentication and attribute information between trusted Web services applications)
  - Identity foundation (directory and workflow)
  - … to effectively manage internal users as well as an increasing number of customers and partners through the Internet

System z Security Offering

- IBM offers the total solution for the enterprise security hub
  - Most secure and resilient hardware platform: System z, reliable, available, and scalable
  - Integrated security features in z/OS, including digital certificates and PKI
  - Most reliable security server: RACF
  - Most comprehensive mainframe security administration & audit: Tivoli zSecure suite
  - Only solution that combines mainframe data into a comprehensive enterprise security dashboard for audit and compliance management: Tivoli Compliance Insight Manager
  - Extensive identity and access management solutions in Tivoli portfolio – including Tivoli Identity Management for z and Tivoli Federated Identity Management for z

Tivoli Security Product Portfolio for System z



Tivoli Compliance Insight Manager
- *Distributed log management, access monitoring and compliance reporting*

Tivoli Federated Identity Manager
- *Cross-domain security for web services and credential transform*

Tivoli Identity Manager
- *Enterprise user provisioning and user management*

Tivoli zSecure suite
- *Integrated mainframe audit and compliance monitoring and security administration*

Tivoli Directory Integrator
- *Data synchronization*

Tivoli Directory Server
- *LDAP infrastructure*

Tivoli Access Manager
- *Authentication, authorization, web and enterprise SSO*
- *TAM OS on Linux for System z*
- *TAM EB on Linux for System z*
- *TAM BI for WebSphere MQ for z/OS*

Tivoli Security Operations Manager
- *Consolidate / correlate security alerts / events*

Tivoli Security Compliance Manager
- *Vulnerability and compliance assessment*

New Capabilities for IBM Security & Privacy

- **Tivoli Compliance Insight Manager**
  - IBM Tivoli branded Consul InSight Security Manager with new functionality, released in July 2007
  - Roll-your-own compliance modules thru wizard for advanced report definition
  - Flexible automated report distribution
  - Advanced toolkit for adding new log collectors, parsers, and normalization
  - Integrates with Tivoli Identity Manager & Tivoli Access Manager for event collection and reporting
  - Agentless iSeries event collection and reporting

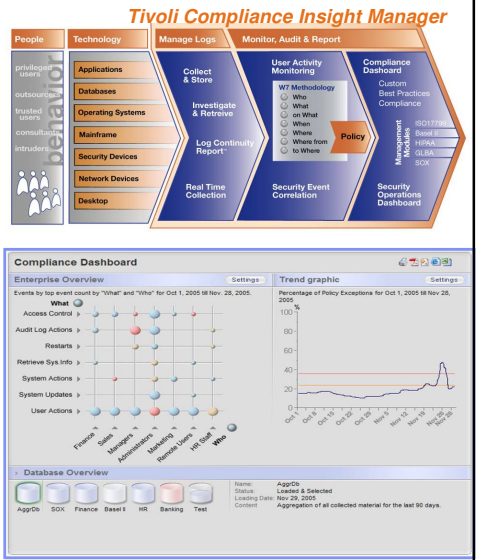
- **Tivoli zSecure suite**
  - IBM Tivoli branded Consul zSecure Suite: new product and module names released in July 2007
  - Fingerprinting and modification detection of z/OS sequential datasets
  - Support for new DB2 V9 audit events
  - XML based reporting enhancements and documentation
  - New component released in Sept 2007: zSecure Manager for RACF z/VM

Assessing and Monitoring Compliance: Tivoli Compliance Insight Manager

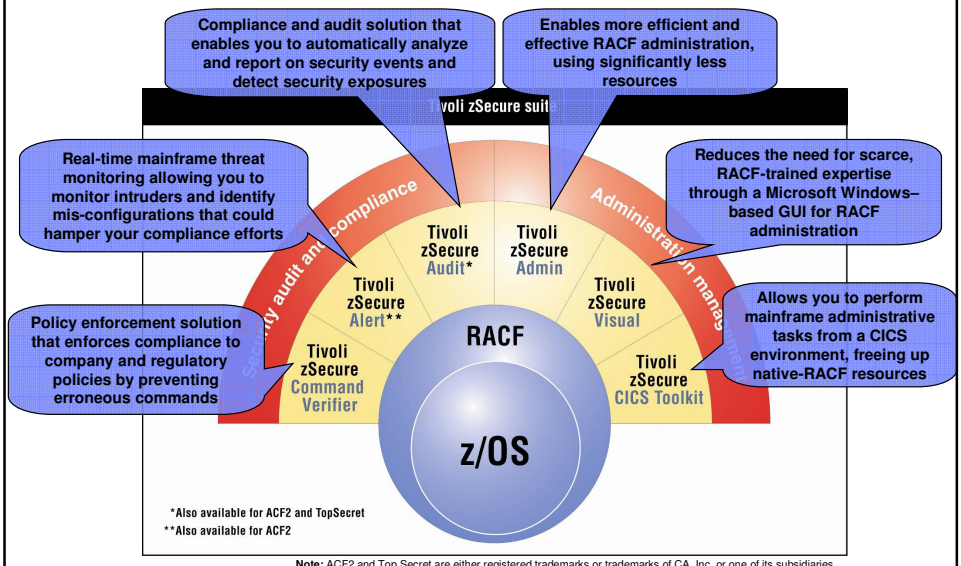
Tivoli Compliance Insight Manager provides an enterprise security compliance dashboard with in-depth privileged user monitoring capabilities, all powered by a comprehensive log and audit trail collection capability

Key Features

- Compliance management modules and regulation-specific reports
- Unique ability to monitor user behavior, including PUMA (Privileged User Monitoring and Audit) reporting
- Broadest, most complete log and audit trail capture capability
- W7 log normalization translates your logs into business terms
- Easy ability to compare behavior to regulatory and company policies – auditors no longer need RACF expertise to monitor activities
- Enabler event source integrates the OS and mainframe database events into TCIM's enterprise compliance dashboard



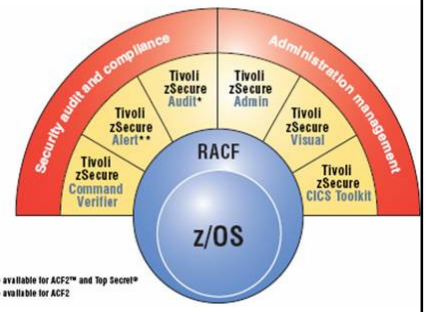
Introducing the IBM Tivoli zSecure Suite



Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Tivoli zSecure Suite

The Tivoli zSecure suite adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit, alert and monitoring capabilities for Resource Access Control Facility



Key Features

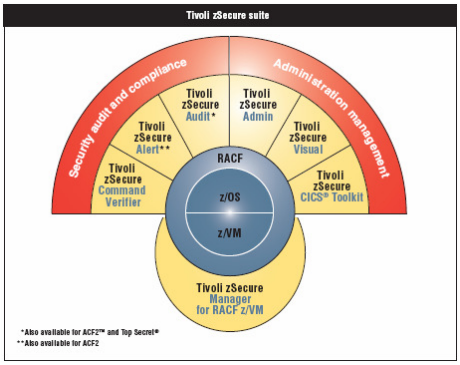
- The zSecure suite improves the efficiency of mainframe administration and enhances the ability for the mainframe to be the hub of enterprise security.
- Administration and provisioning:
  - zSecure Admin enhances user management
  - zSecure Visual offers a Microsoft® Windows® GUI
  - zSecure CICS Toolkit for simplified CICS security management
- Audit, monitoring and compliance:
  - zSecure Audit provides event detection, analysis & reporting and system integrity audit & analysis
  - zSecure Alert provides intrusion detection and alerting
  - zSecure Command Verifier offers automated security monitoring

Benefits Summary

- Administration and provisioning:
  - Reduce administration time, effort and cost
  - Reduce training time needed for new administrators
- Audit, monitoring and compliance:
  - Helps to pass audits more easily
  - Can improve security posture
  - Save time and costs through improved security and incident handling
  - Can increase operational effectiveness

Tivoli zSecure Manager for RACF z/VM

The Tivoli zSecure Manager for RACF z/VM adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit capabilities for the z/VM RACF feature



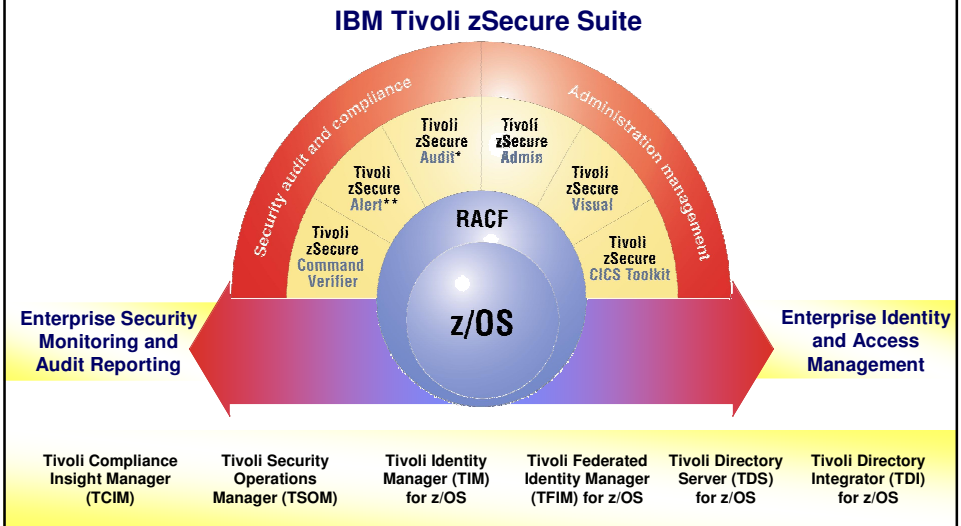
Key Features

- Enhances user management and provisioning for the VM environment
- Automates complex, time-consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF command syntax
- Extends auditing capability by reading the RACF database, analyzing SMF records generated by RACF z/VM, and providing user privileges from both RACF and the VM directory
- Supports ease of management and auditing of the Linux guests if they use RACF for authentication while running in the VM environment
- Allows users to generate and view customized audit reports with flexible schedule and event selections

Benefits Summary

- Improves the functionality of the mainframe's security system while helping reduce administration time, effort and cost
- Save time and costs through improved security and incident handling
- Helps to pass audits more easily

A cornerstone for Tivoli's z/OS Security Strategy



* Also available for ACF2 and Top Secret
** Also available for ACF2

Policy Based Identity Management with Tivoli Identity Manager on z/OS

Provision users across the enterprise

Value of Tivoli Identity Manager

- Automated, policy-based identity management
- Provides workflow for automating the approval process
- Allows for self service enrollment and password management
- Keeps an audit of user management operations
- Reports on out-of-policy changes

Identity information and management are mission-critical

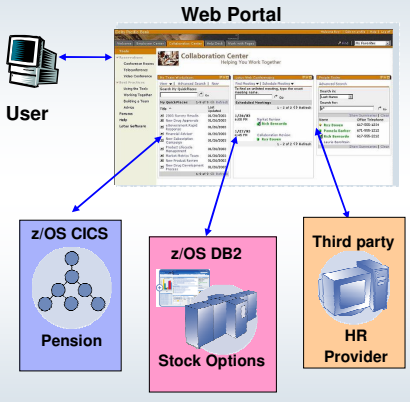
Advantages of TIM on z/OS

- Highly available and resilient
- Highly secure
- Scalable
- Integrates with z/OS RACF identity management

A single hub for provisioning users

Tivoli Federated Identity Manager for z/OS

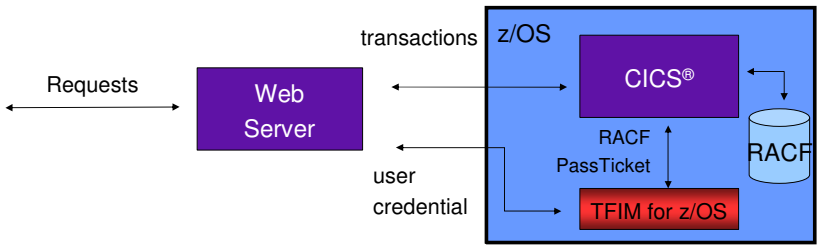
- **Security integration for web services that use z/OS CICS or other z/OS subsystems**
- **Protect z/OS-hosted web services using z/OS security services**
- **Preserve identity of the requesting user for access control and audits**
- **Use z/OS auditing to assist regulatory compliance**
- **Improve integration and simplify the user experience**



Flow Auditable Identities to Mainframe using RACF PassTickets

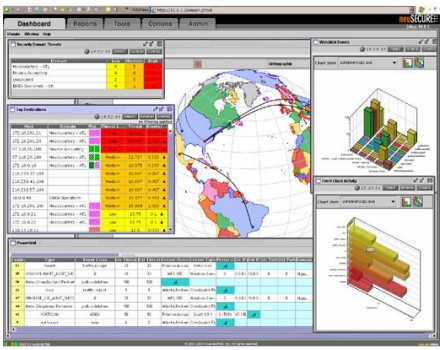
With Tivoli Federated Identity Manager (TFIM) for z/OS

- Link user identities between mainframe and distributed applications and address the compliance and audit requirements
  - Deliver pluggable authentication processing across heterogeneous environment
  - Preserves identity at granularity of original requesting user
  - Uses z/OS auditing to improve regulatory compliance



Tivoli Security Operations Manager

- Advanced security information management (SIM) software platform and appliances designed to improve the effectiveness, efficiency, and visibility of enterprise security operations.
- Unifies policy management, incident handling, and risk mitigation functions of security operations across an enterprise though
  - Log/event aggregation, normalization, archiving and reporting
  - Support for regulatory compliance reporting (Sarbanes Oxley, GLBA, HIPAA, FISMA, Basil II)
  - Comprehensive incident recognition and management
  - Proactive Policy monitoring and enforcement



Case study: Shipping company

- Situation:
  - Customers are stock listed
  - Must keep financial data confidential to prevent insider trading
  - Shipping manifest indicates production volumes
    - Production volumes may be extrapolated to financial data
    - Need to prevent access to shipping databases and reports
- Best Solution Available?:
  - Need to restrict access to reports about shipping volumes
    - Storage admin and sysprogs reading business datasets
    - Security admins granting themselves authority
    - Data security administrators granting improper access
  - Access reduction for privileged users
    - Impractical due to technical limitations
    - If you remove my ability to …. I cannot commit to ….

zSecure Solution

- Real-time alert as mitigating control – zSecure Alert
  - Reduce need to implement separation of access
    sysprogs keep their "must be able to read/change anything" status
  - No need for political battle or costly re-orgs
  - Quick install, instant visibility

Case study: Diversified Manufacturer

- Situation:
  - Decentralized and partitioned
  - Departments with their own applications, responsibility and security administrators
  - Administrators must be limited to very specific actions
    - Only within their own department
    - Prevent cross-department authorities
- Best Solution Available?:
  - Solution (?): implement GROUP SPECIAL, GROUP AUDITOR
    - Impractical when profile ownership is not clearly specified in RACF
    - Does not prevent Permit or Connect outside of department

zSecure Solution

- RACF command screening – zSecure Command Verifier
  - Each security change verified against granular policy
    Using masks for classes and profiles
    Appropriate defaults added, mistakes flagged down
- Audit reports for the departmental auditors – zSecure Audit
  - Identifying inappropriate access and changes within department
  - Identifying logon and activity of privileged users

Case study: SOX reports

- Sarbanes Oxley requirements
  - Monitor changes to operating system and security
  - Monitor activities of privileged users
  - Monitor irregular logons
  - Verify operating system parameters against baselines
  - Verify users with specific (high) application authority
- Best Solution Available?:
  - Costly daily verification
  - Manual creation of queries and reports
  - Difficulty in baselining versus current state

zSecure Solution

- zSecure Suite Audit, Admin and Visual
  - The current definitions are assumed to be "approved"
    - Show changes compared to "yesterday"
    - Inappropriate changes have to be identified within 1 day
    - They will not show up in the report tomorrow
  - The baselines are known
    - Show parameters that are in conflict
    - Approved changes must be reflected in the baseline
    - Inappropriate changes will show up until they have been addressed

Mainframe as a Security Hub

- z/OS is known for running mission-critical workloads for your Enterprise
- Ensuring your applications run and run securely is a business requirement
- z/OS offers highly available, secure, and scalable database hosting
- z/OS has well-honed security processing with very granular permissions capabilities
- z/OS offers superb auditing of operations performed
- control of user/group definitions in multiple registries, including RACF, from z/OS, is now available
- services-based security capabilities, hosted on z/OS, are now available
- Using a combination of Linux for System z and z/OS systems, the mainframe can host the security functions for the Enterprise

IBM – uniquely able to address security

- ✔on all of your computing systems
- ✔across security disciplines
- ✔using a combination of offerings available today
- ✔with active research and innovation in security
- ✔on the platforms you use

Considerations

- So ask yourself:
  - Would you like to do a better job of managing security from a business perspective?
  - How are you proving regulatory compliance today? Is it meeting your needs?
  - Do you need to report/monitor/assess on compliance to regulatory mandates?
  - Do you need to enhance the audit/reporting/admin capabilities of your current security system?
  - Are your security initiatives disjointed?
  - Think back to Marc's presentation on Common Problems of compliance that Gartner reported – do they fit your organization?

Security Summary

- IBM has System z security offerings currently that address the need for compliance, audit and administration for the mainframe, along with access and identity management for the enterprise hub
- System z security management solution includes Tivoli zSecure suite & Tivoli Compliance Insight Manager, IBM Tivoli Identity Manager, IBM Tivoli Federated Identity Manager, and/or IBM Tivoli Access Manager, plus TSOM, TDI