*The Modern Mainframe…*
*At the Heart of Your Business*

**End-to-End Security and Compliance**



# Evolving Regulations Point to the Need for More Automated Compliance Reporting

*Regulatory Impact*

| | Secured Data | Workflow | Reporting | Risk Assessment | Encrypted data | Secured Storage Management |
|---|---|---|---|---|---|---|
| **Basel II** | ✓ | ✓ | ✓ | ✓ | ✓ | |
| **HIPAA** | ✓ | ✓ | ✓ | | ✓ | ✓ |
| **Sarbanes-Oxley** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Gramm Leach-Bliley** | ✓ | | ✓ | | | |
| **AML - Patriot Act** | ✓ | | ✓ | | ✓ | |

IBM Service Management Market Needs Study, March 2006

# Service Oriented Finance Security Requirements

**We have a lot of security requirements**

**Service Oriented Finance CIO**

**Your security strategy should include these key elements:**

- Secure platform
- Data privacy
- Compliance and audit
- Manage security across the extended enterprise

**IBM**



# Questions Auditors Might Ask

**Auditor**

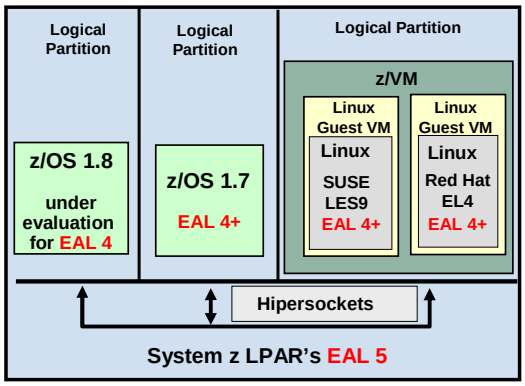
How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the mainframe?

| RACF | Communication server | Multi-level Security | Tape Encryption | SMF Logs | Tivoli Compliance Insight Manager | Tivoli Identity Manager | Tivoli Federated Identity Mgr |
|---|---|---|---|---|---|---|---|

**Secure Platform** ⟷ **Data Privacy** ⟷ **Compliance and Audit** ⟷ **Extended Enterprise**

# Common Criteria Certifications Show System z Platform Security Leads the Industry




- What is Common Criteria?
  - Common Criteria is an accepted standard for evaluating the inherent security of a computing system
  - A higher **EAL** rating is more secure
  - The security requirements in Common Criteria have gained support as "best practices"
  - **IBM System z holds the highest EAL grades in Common Criteria!**
- Crypto Cards rated at FIPS 140-2 level 4



# Security Begins with System z Secure Processing

- Workload Isolation
  - Isolation of users in a separate address space
  - Processing integrity with LPAR separation
  - System programs separated from user programs
- Not Harmed by Malware
  - Viruses cannot be readily introduced
- Communications
  - Internal Hipersocket communications not easily intercepted
- Authorized Program Facility (APF)
  - Executable code can be invoked only by authorized users
  - Cross memory services prevents unauthorized access
- System Integrity Statement
  - IBM accepts responsibility for integrity exposures found by customers

- **System z is a hacker's nightmare!**
- **Allows customers to run multiple workloads on single image**
- **Stops viruses and worms from disrupting operations**

# RACF* – At the Heart of System z Security

- RACF controls authorization and authentication
  - Identifies and authorizes users
  - Controls access to resources
  - Authenticates users through passwords or (PKI) digital certificates
  - Provides auditing and logging
  - Enables central administration of several systems
- RACF structure is enforced automatically
  - System blocks unauthorized attempts
  - You cannot bypass RACF
- RACF is integrated with System z Middleware
  - Transaction monitors, DB2
  - CICS, IMS, WebSphere

**These resources are protected by RACF**

- DB2
- VSAM
- IMS
- CICS
- TSO
- Disk
- Tape
- Print
- JES 2 & 3
- Console
- VTAM
- SDSF
- WebSphere
- MQ
- Programs
- Keys

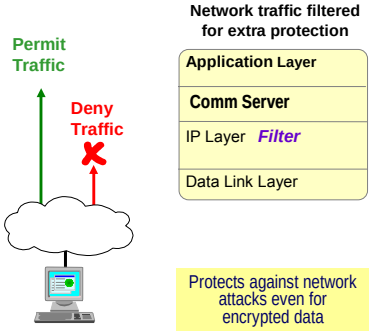
Integrated Security across the platform

*** Resource Access Control Facility**



# Built in Security to Defend Against Network Attacks

- **Intrusion Detection** from Communications Server enables detection of network traffic attacks
- Automatic application of defensive mechanisms
  - Evaluates inbound encrypted data for suspect activity
  - Policy controls connection limits, packet discard
  - Detects anomalies in *real-time*
  - *Avoids overhead* of per packet evaluation against known attacks
- Scan detection and reporting
  - Can map the target of an attempted attack
- Integrates with Tivoli Security Operations Manager



# Questions Auditors Might Ask

Auditor

How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the mainframe?

How do you maintain online data privacy?

How do you know your archival customer data is protected?

RACF | Communication server | Multi-level Security | Tape Encryption | SMF Logs | Tivoli Compliance Insight Manager | Tivoli Identity Manager | Tivoli Federated Identity Mgr

Secure Platform ⟷ Data Privacy ⟷ Compliance and Audit ⟷ Extended Enterprise



# The Foundation of Data Privacy is Encryption

**Free - CP Assist for Cryptographic Function (CPACF)**

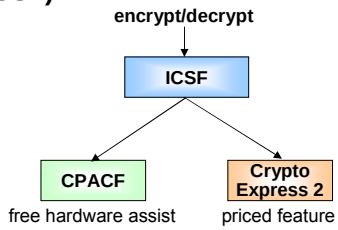
- Each system processor has hardware assist on the chip for cryptography
- CPACF provides cryptographic functions for encryption and decryption of data
  - Used for SSL, VPN, and data storing applications
  - includes DES, T-DES, AES, SHA-1 and SHA-256 hashing

**Priced Feature - Crypto Hardware Processor Card**

- Crypto Express 2 ($38K per card)
- High performance, tamper proof environment for secure key cryptography
- 6000 Secure Socket Layer handshakes per second
- Key is encrypted in hardware and never exposed

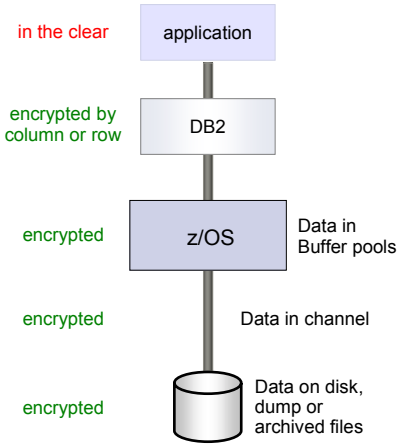
**Integrated Cryptographic Service Facility (ICSF)**

- Provides API's for encryption via CPACF or Crypto Express2
- Routes work to the appropriate crypto processing resource
- Included in z/OS
- Used to administer the cryptographic hardware and keys



# DB2 Encryption Protects Data Privacy in the Database

- Encrypted by DB2
  - Table and Index encryption
  - Image copies encrypted
  - Logs/archives encrypted
  - Data encrypted in buffers
  - Data sent by DRDA
  - Data not exposed!
- DB2 uses encryption to protect the data:
  - Column level encryption
    - Enabled by the application
  - Row level encryption
    - IBM Encryption Tool for DB2
    - Optional feature






# DB2 Multi Level Security

**Goals of Compartmentalized Data**

- Same database used by organizations with a different need to know
- Prevent unauthorized individuals from accessing information at a higher classification than authorized
- Prevent unauthorized declassification of information

**DB2 Multi Level Security**

- Restricts row level access to those with appropriate security clearance
- Mix low and high security data in the same database

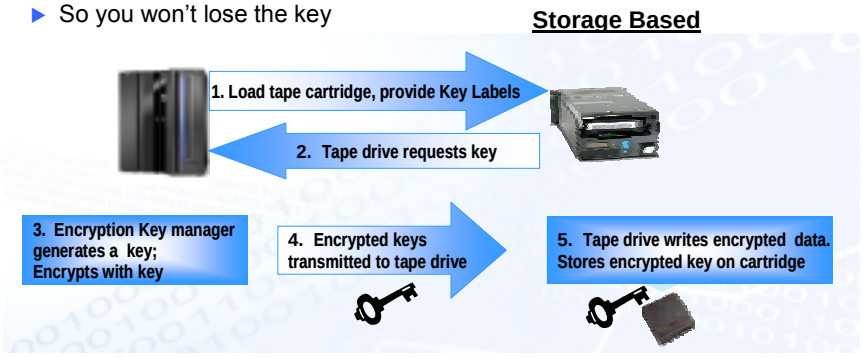

| SECURITY Classification | Revenue | Area | Loss |
|---|---|---|---|
| Executive | 234 | USA | 3% |
| Finance Secret | 198 | Ohio | 13% |
| Executive | 2 | Maine | 29% |
| Finance Confidential | 234 | USA | 11% |
| Finance Secured | 87 | Texas | 14% |
| Finance Secured | 23 | New York | 20% |
| Audit Confidential | 223 | USA | 10% |
| Finance Secured | 45 | Canada | 29% |

*Single image of data is sharable by multiple enterprise departments with different levels of "need to know"*

**With DB2 Multi Level Security data can be consolidated onto a single database, restricting access to only authorized users**

# Optional Ability to Automatically Encrypt All Data on Tape

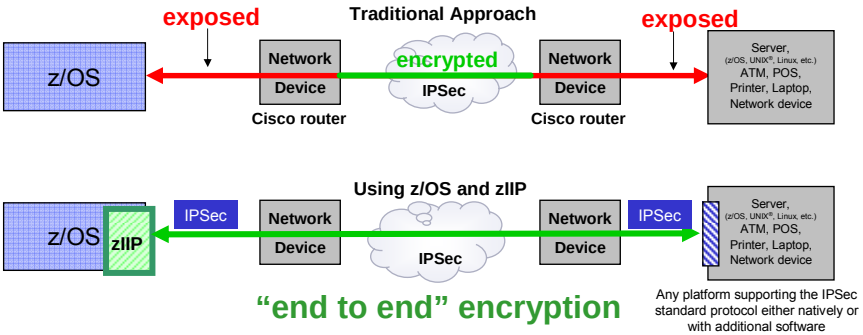
- High performance tape encryption
  - Standard feature on all new TS1120 Tape Drives
  - Cost effectively encrypt all tape data
  - Offload host processing encryption overhead
  - Minimize impact to existing processes and applications
- Leverages System z Key management
  - So you won't lose the key






# Provide End-to-End Encryption at Low Overhead

- The need for *end-to-end* network encryption has become more pervasive due to regulations (e.g. Payment Card Industry requirements)
- Traditional router-based network encryption leaves data exposed
- Data encryption has always been processing intensive
  - System z Communication Server uses crypto express 2 to encrypt network data end-to-end
  - Encryption is now eligible for **zIIP** offload processing – reducing costs



# Questions Auditors Might Ask

Auditor

How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the mainframe?

How do you maintain online data privacy?

How do you know your archival customer data is protected?

What happened leading up to this breach?

Are you reporting consistently across the enterprise?

RACF | Communication server | Multi-level Security | Tape Encryption | SMF Logs | Tivoli Compliance Insight Manager | Tivoli Identity Manager | Tivoli Federated Identity Mgr

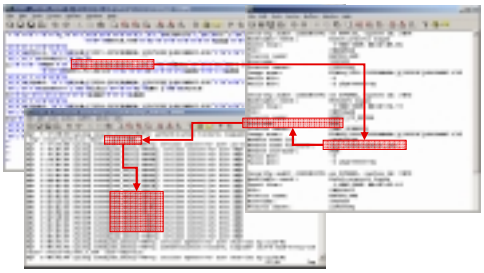
Secure Platform ⟷ Data Privacy ⟷ Compliance and Audit ⟷ Extended Enterprise



# The Foundation of Audit and Compliance is Comprehensive Logging

- System z SMF provides comprehensive logging across the sysplex
  - Consistent record formats help simplify compliance needs
  - Audit records report access to protected resources
- *Log continuity* from Tivoli zSecure Audit validates logs have been maintained
  - Uses the log system event records from multiple sources including System z
  - Examine activities of a specific user

***With distributed systems, customers have to manually piece together logs***



## Tivoli Compliance Insight Manager Strengthens the Compliance Process

- ***Detects*** security violations
- ***Captures*** security audit data from multiple systems
- ***Correlates*** data to identify audit risks
  - who, what, on what, where, when, from where, to where
- ***Analysis engine*** for deep analysis of collected data
  - Determine who was the last person to touch a particular file
- ***Flexible reporting*** related to specific compliance issues
- Checks for ***log continuity*** ensure that log collection is carried out



## DEMO: Tivoli Compliance Insight Manager

**Tivoli Compliance Insight Manager detected that our employee Michael, has been accessing restricted data.**

**How did this happen?**

**Service Oriented Finance Security Officer**

**demo**

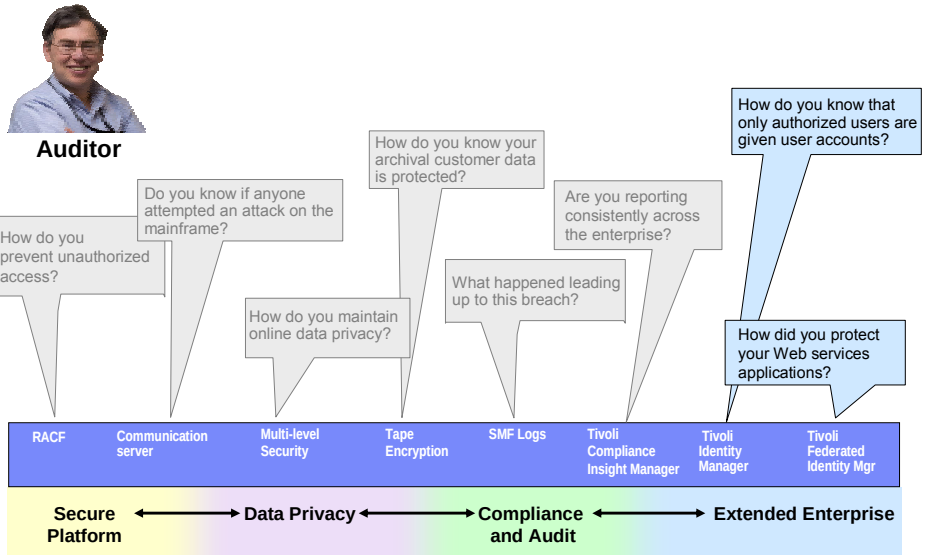
# Other Tivoli zSecure Products Supports System z Auditing and Security Monitoring

Tivoli zSecure tools interoperate to improve auditing and forensic capabilities

- **Tivoli zSecure Audit** is an audit and reporting tool for the mainframe environment
  - Built-in knowledge base identifies exposures
  - Provides real-time alerts based on policy exceptions
- **Tivoli zSecure Alert** provides real-time threat monitoring for z/OS and RACF
  - Can issue alerts when conditions occur
  - Can take action to stop security breaches
- **IBM Tivoli zSecure Command Verifier** prevents erroneous commands, thereby increasing control and decreasing the security risk and clean-up cost
  - Prevent non-compliant RACF commands from executing
  - Reduce security risks due to improper administration
- Flexible **CARLa** (Audit and Reporting Language) language for customized user reporting

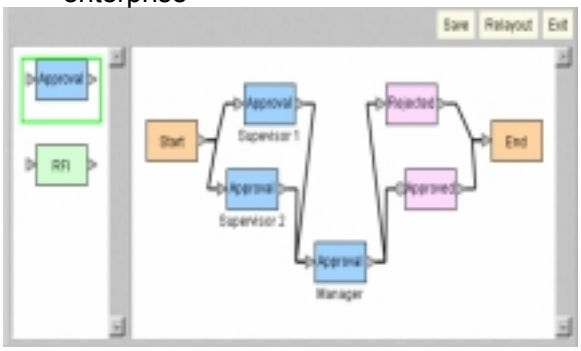


# Questions Auditors Might Ask



# Provision Users with Tivoli Identity Manager for z/OS

- 75-80% of help desk calls are for password reset or other trivial items
- Tivoli Identity Manager can eliminate this problem
- Provides self service password management
- Can provision and delete user accounts across your entire enterprise

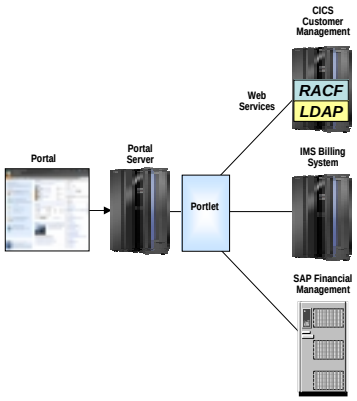



- Provides workflow for automating approval processes
- Searches for out-of-policy changes
- Provides email notification of changes



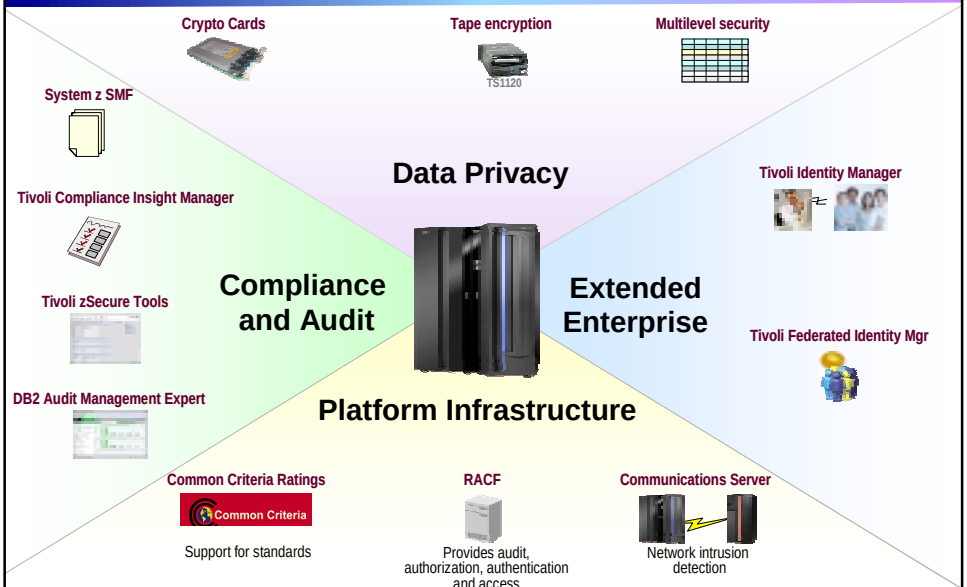
# Single Sign-on: Tivoli Federated Identity Manager

- Propagates the identity of the original requester in a **web services** environment
  - Provides single sign-on for web services
  - Maintains identity of the original user
  - Credentials can be propagated from the portal to RACF for end-to-end security
    - Uses Passtickets issued by RACF
  - Enable trusted transactions between business partners
  - Supports industry standards
    - SAML, Liberty, WS-Federation SSO




***TFIM can provide single sign-on for the Service Oriented Finance Car Loan Solution***

# Strong Security Needs Many Elements






# Service Oriented Finance Requirements Met

So do you feel more secure?

IBM

My operations are now secure with System z

- Secure platform infrastructure!
- Data privacy!
- Compliance and audit!
- Security across the extended enterprise!

Service Oriented Finance CIO