The Basics of Security with RACF in z/OS

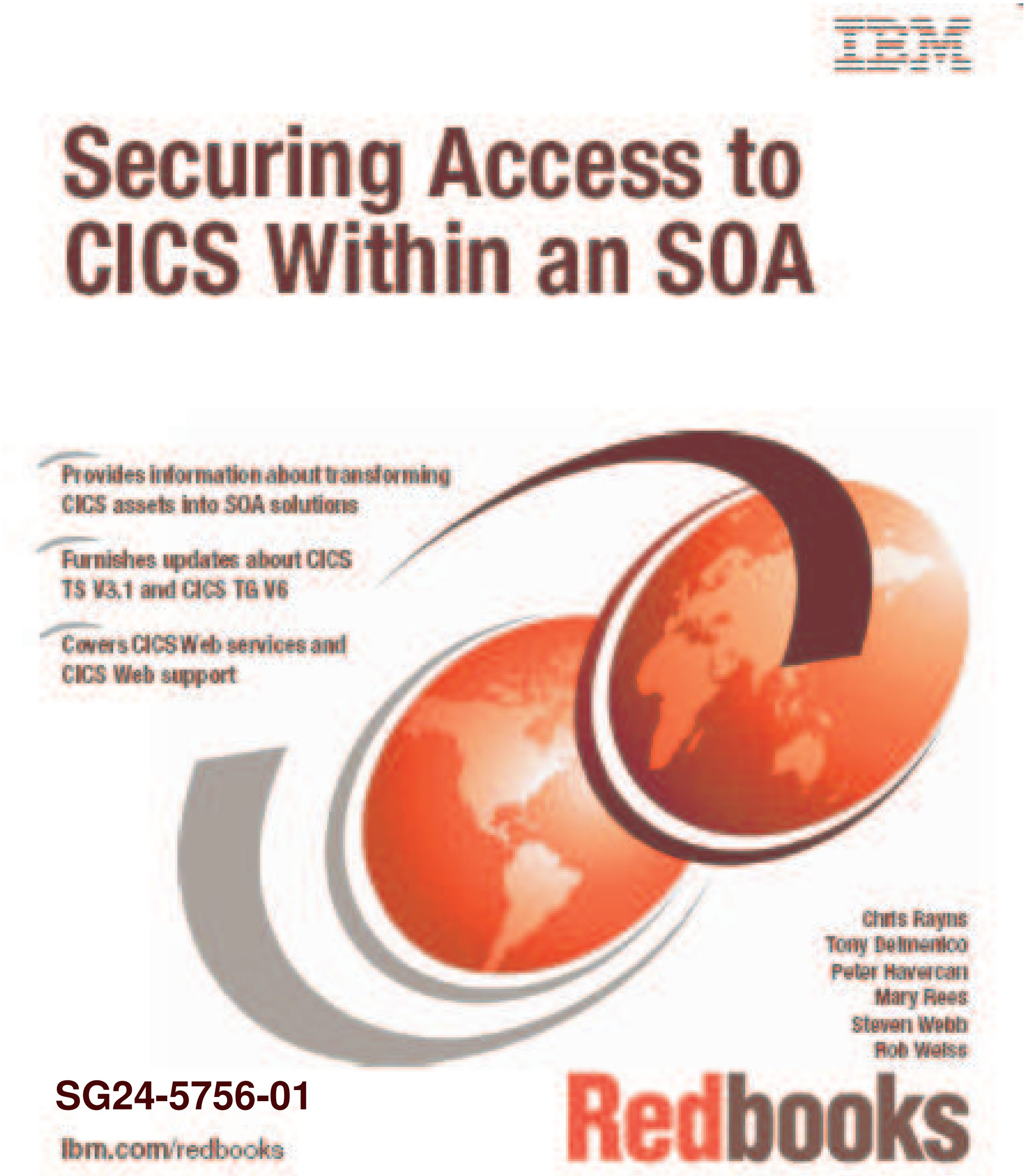
Session RAB1

Rob Weiss Rob_Weiss@us.ibm.com

z/Security and Privacy Consultant

I’m a member of the WWISCP.

And, I’ve been in IBM for over 30 years.



IBM

Securing Access to CICS Within an SOA

Provides information about transforming CICS assets into SOA solutions

Furnishes updates about CICS TS V3.1 and CICS TG V6

Covers CICS Web services and CICS Web support

Chris Rayns
Tony Delmenico
Peter Havercan
Mary Rees
Steven Webb
Rob Weiss

SG24-5756-01

ibm.com/redbooks

Redbooks

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

CICS*
DB2*
DB2 Universal Database
IBM*
IBM logo*
S/390*
LINUX
z/LINUX
z/VM

System z
System z9
Tivoli*
WebSphere*
z/OS*
zSeries*
RACF
z/OS Security Server

Thanks to Barbara Sannerud, of IBM SWG who's materials provided the basis for much of the material included in this presentation.

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

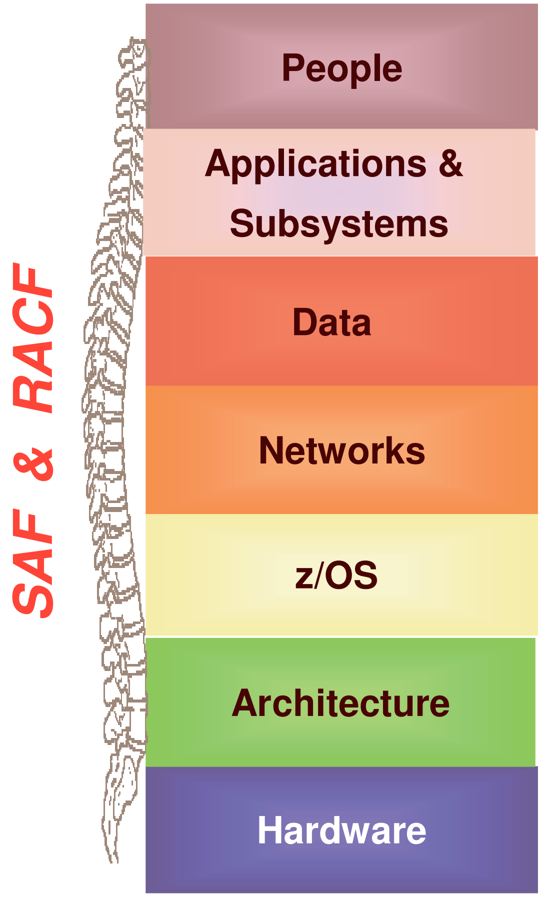
Initial Considerations for this document

- This document does not pander to FUD or "Fear, Uncertainty, and Doubt." The concerns expressed are those of numerous product experts, security experts, privacy experts, and performance experts within IBM.

- Critical RACF Best Practices that will improve RACF performance and that of other notable subsystems.
  - **Observation: HLQs should uniquely represent projects, applications, Users, Organizational Structures and further identify the files as Production, Test, Development, etc. Plus, any divisional, geographical or other considerations.**

The Backbone of Security: RACF

RACF and z/OS SAF provide security throughout the stack



- Offers **administrative** tools, reporting, auditing
- Provides remote **administration**
- Works with LDAP to **authenticate** users
- **Access** control to all classes of resources for applications and middleware
- Provides **auditing** without modifying applications
- Integrates into the **operating system**
- Provides Enterprise Identity Management
- Supports **cryptographic** services
- Supports digital certificates

Proven security, integrated throughout the stack.

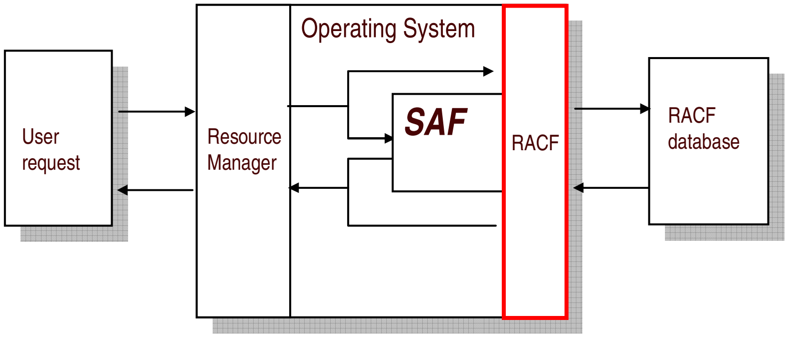
RACF - Consistent Security Policy

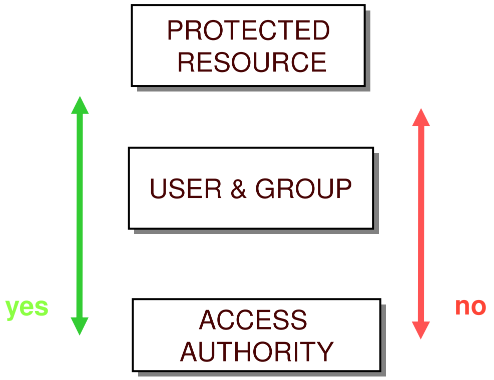
- A single security solution to control access to z/OS Security Server and other system resources
- RACF protects resource access, authorizes users, and logs unauthorized access
- RACF gives you the ability to identify and authenticate users
- Provides flexible access - centralized or decentralized profile controls
- Supports these functions (user identification, access control, and auditing) without modifying applications
- Helps enforce *segregation of duties* by allowing the administrator to change access rules but not change auditing controls
- Reliable, consistent security addressing required security needs

RACF and z/OS provide consistent security for multiple resources, end to end throughout their lifecycle.

A Proven Approach to Protecting Resources

- RACF acts as a layer in the operating system that verifies user identities and grants requests to resources
- RACF can protect a multitude of network and application resources
- RACF can authorize when a user can access resources
- RACF provides global access checking. Customers can establish system-wide authorization levels
- RRSF allows a security administrator to manage remote RACF databases such as in the case of a disaster recovery center
- RACF allows for Pass Tickets, one-time non-reusable passwords alternatives for applications that span platforms





SAF- A Common Base for Resource Control

- SAF (system authorization facility) is a part of z/OS that directs control to RACF when receiving requests from a resource manager
- Resource managing components invoke SAF for access control or authorization checking
- The SAF router is a system service- *part* of the operating system
- SAF provides consolidation and co-location for multiple security services
- SAF simplifies security and removes the overhead of security for multiple systems software products
- It enables the use of common controls across products and systems
- The SAF router, the main element of SAF, can also work with 3rd party security tools

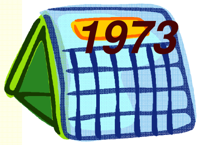
SAF interface is extensible, simplifies security and is part of operating system.

IBM's Unique Integrity Statement

MVS Integrity Statement

- IBM will **accept all APARs* that describe exposures to the System Integrity of MVS** or that describe problems where the installation of the indicated release of any of the programs listed below **introduces an exposure** to MVS System Integrity, as defined below
- A lapse to integrity would allow unauthorized users to circumvent protection mechanisms
- In z/OS unauthorized problem programs cannot
  - circumvent or disable store or fetch protection
  - access an OS password-protected or RACF-protected resource
  - obtain control in an authorized state supervisor state (protect key <8) or Authorized Program Facility (APF) authorized

Since…



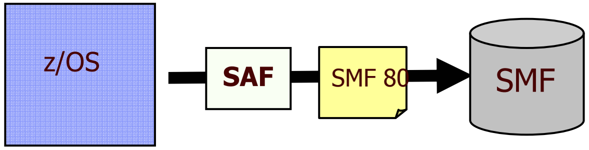
***authorized program analysis report (APAR).** A request for correction of a problem caused by a defect in a current program release.

IBM commits to providing system integrity-can other vendors claim the same?

Auditing Needs

- RACF records system events, enabling monitoring of users and their activities; reports on attempts to perform unauthorized actions
- RACF cuts SMF records for post processing and provides a Report Writer, XML interfaces for reporting
- The report describes attempts to access RACF-protected resources by user ID, of successful access, or security violations
- Common approach avoids auditing integration and compliance challenges posed by inconsistent distributed systems logging
- IBM has built auditing capabilities into all its subsystems which cut records which can be used for audit purposes

RACF enables consistent auditing - critical for compliance needs.



On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks. **That's about one every 2.3 seconds.**

"Defending Data: a Never-Ending Vigil"
Todd Spangler quoting Dan Lohrman, Chief Security Officer for the State of Michigan Baseline, 2004

Provide improved consistent auditing and reporting critical for today's compliance needs

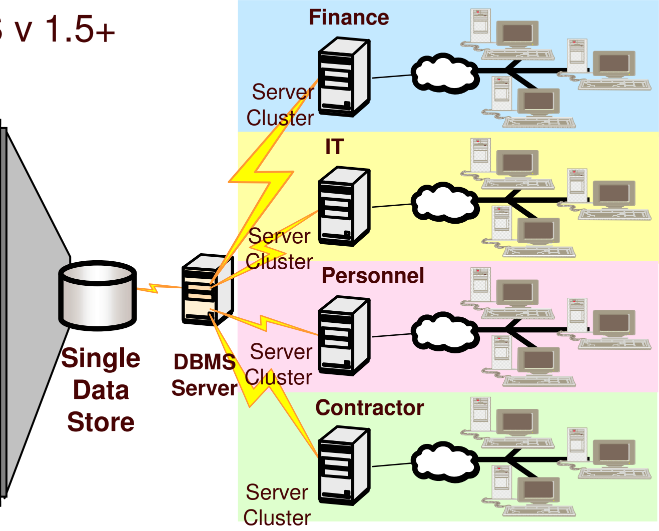
Multi Level Security Access (MLS)

Definition: The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization

- MLS represents a mechanism to classify data based on both hierarchical security levels combined with a non-hierarchical security categories
- A single secured repository features different sensitivity attributes accessible by users with varying clearance levels
- Eliminates need for duplicate IT infrastructures, silos, redundant software
- Implemented through RACF with DB2 UDB for z/OS v8 and z/OS v 1.5+
- DB2 also supports row level encryption

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

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
IT	87	USA	14%
Contractor	23	UK	20%
IT	223	USA	10%
Contractor	45	Canada	29%



MLS Leverages z/OS to Simplify Security

- MLS is integrated with z/OS leveraging the value of virtualization
- Eliminates need for redundant, isolated infrastructures to achieve security
- No more difficult to maintain custom SQL views
- One consolidated DB2 database with security provided by DB2 leveraging RACF security -share resources with mixed security levels in one image
- MLS provides additional functions as well:
  - The system does reuse a storage object until purged.
  - The system labels hardcopy with security information.
  - The system creates audit records around security events
  - Can mask names of data sets, files and directories from users without proper access
  - Prohibits user declassification (Write-Down) of data except with explicit authorization to do so

MLS reduces risk and helps with compliance

DB2 UDB for z/OS v8+ Security

Improved security

- Quality of end to end security
  - Row level security
  - Leverages RACF and zSeries security
  - MLS
- Common Criteria
- Auditing capabilities
- Encryption
- Rolling maintenance & upgrades
- Trusted Database roles vNext
- Trusted context vNext

- Gartner published an advisory on its Web site just days after Oracle's latest quarterly patch cycle, which included a total of 103 fixes with 37 flaws in Oracle database products.
- "the range and seriousness of the vulnerabilities patched in this update cause us great concern..."

Date: 23 January 2006

DB2 UDB value is one of availability and integrated security, not one featuring rapid repair and a commodity server approach

Security: CICS

- CICS security managed by security profiles defined in RACF
- CICS users authenticated by RACF
- Users can be authenticated by userid and passwords or through SSL certificates
- CICS also provides transaction security
- Transactional integrity
- Resource security applies to CICS resources used by a CICS transaction
- System programming commands protected
- Thread-safe mode:
  - Isolates user transaction storage from other user-key transactions
- Violations logged to SMF

CICS handles over 30 billion transactions/day!

Middleware uses RACF to protect transactions and other defined resources

Integrated IMS Security

- IMS transactions and resources also protected by RACF
- Data is protected at the row level for DB2 and the segment level for IMS.
- IBM Data Encryption for IMS and DB2 Databases
- IMS Transaction authorization works with RACF:
  - IMS post version 1.9 will use RACF instead of the Security Maintenance utility (SMU)
  - At *control region* initialization, RACF builds profiles for transactions to be checked against user's privilege
  - At *transaction authorization time,* RACF compare transaction profiles in storage against the user access privilege to return authorized or unauthorized indication
  - IMS offers a protected view of data through the combined Program Specification Block (PSB) and Program Control Block (PCB)

RACF provides:

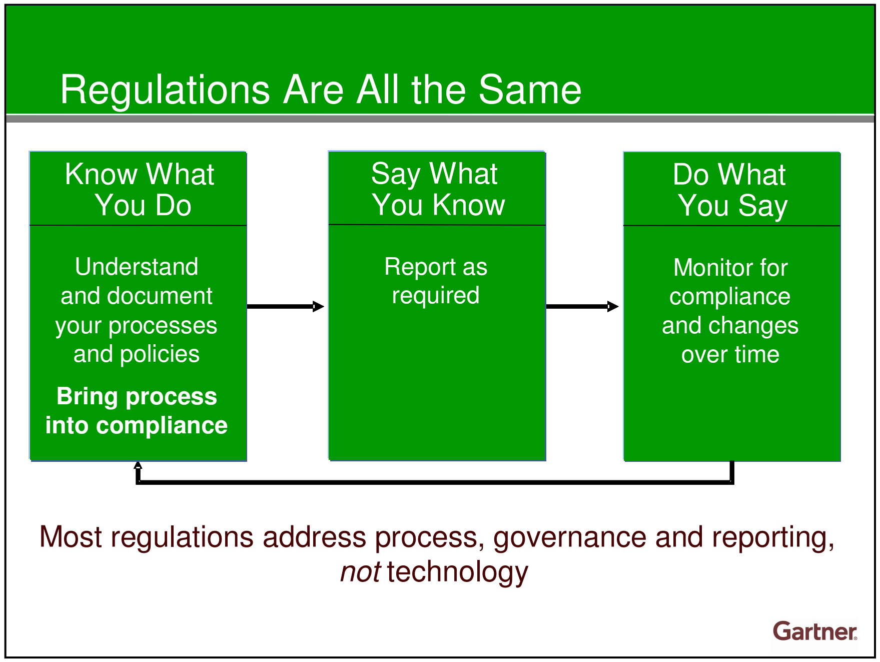
. IMS user verification
. IMS trans. authorization
. Authorization to IMS
  control region resources

Over 50B transactions per day run through IIMS

IMS customers have run over 3000 days without an outage

IMS benefits from transaction security through RACF

Pillar 3: Addressing Regulatory Compliance



Regulations Are All the Same

Know What You Do

Understand and document your processes and policies

Bring process into compliance

Say What You Know

Report as required

Do What You Say

Monitor for compliance and changes over time

Most regulations address process, governance and reporting, *not* technology

Gartner

- "IT Security is like **spinach** — A nutrient necessary for well-being, but which few enjoy. However, the advent of **compliance** offers a rare opportunity for businesses to improve both **security** and the benefits derived from it.
- IBM in general, and the **System z9 in particular,** deserve credit for delivering superior security over the long term and for adapting to **business compliance** with new **security solutions that continue to stand out from the competition."**

Infrastructure Associates 15 November 2005 "IBM Mainframe Encryption: Upgrading the Gold Standard for Security." Wayne Kernochan

> *"Sixty-one percent of companies will increase spending on security technologies to support compliance with SOX"*
>
> *Forrester, " IT Execs Wake Up To Sarbanes-Oxley Compliance", 05/23/04*

Reducing Operational Risk

- Basel II is a wake up call for banks and financial institutions to improve information security and risk mgt.
- Protection of privacy and confidentiality very important to multiple industries
- Manage security and integrity of financial data for financial reporting
- Maintain operational resiliency
- Maximize availability
- Improve security controls in applications and IT
- Reduce people, process and technology risk

REGULATIONS

• Basel II -proposes methods for banks to calculate capital provisions needed against credit, commercial, & operational risk- the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events.

• Sarbanes-Oxley - Strengthen financial reporting, internal controls **(security),** transparency

• HIPAA - **Secure** medical records & usage

• Patriot Act - Prevent **fraudulent** use of the financial system to support illegal activities

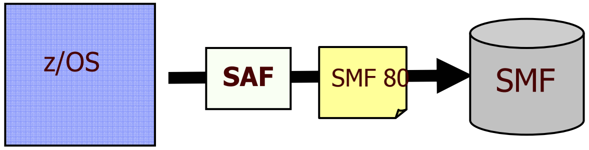
• Gramm-Leach-Bliley Act - Protection of personally identifiable financial information **(confidentiality)**

• SB 1386 mandates the disclosure of **security breaches** where private information of has been compromised

Auditing Needs

- RACF records system events, enabling monitoring of users and their activities; reports on attempts to perform unauthorized actions
- RACF cuts SMF records for post processing and provides a Report Writer, XML interfaces for reporting
- The report describes attempts to access RACF-protected resources by user ID, of successful access, or security violations
- Common approach avoids auditing integration and compliance challenges posed by inconsistent distributed systems logging
- IBM has built auditing capabilities into all its subsystems which cut records which can be used for audit purposes

RACF enables consistent auditing - critical for compliance needs.



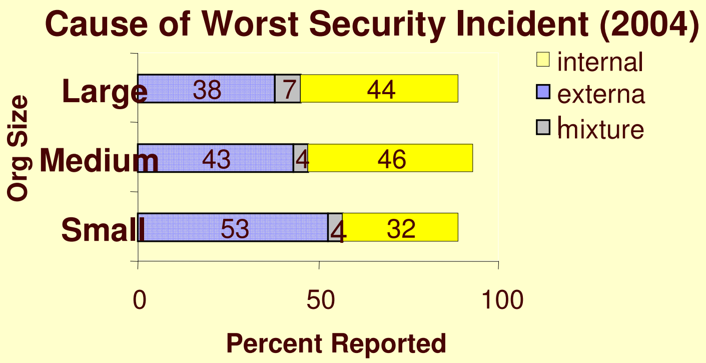
On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks. **That's about one every 2.3 seconds.**

"Defending Data: a Never-Ending Vigil"
Todd Spangler quoting Dan Lohrman, Chief Security Officer for the State of Michigan Baseline, 2004

Provide improved consistent auditing and reporting critical for today's compliance needs

Integrated Health Checker - For Integrity

- Identifies potential configuration problems over an IPL
- Health checker consists of:
  - A framework to manage scheduling, processing, reporting of health checks
  - Checking mechanism that evaluates software settings
  - Extensible solution - authored by IBM, ISVs, or users.
- RACF supplies checks for use by the IBM Health Checker for z/OS
  - Checks that RACF is protecting z/OS **providing additional protection**!
  - Checks APF libraries & RACF data sets
- Interim checking between releases
- Integrated into z/OS 1.7



2004 PwC ISBS UK based study

The percent incidents due to internal causes accounted for a significant percentage of all security breaches.

Helps avoid potential security problems resulting from introduction of invalid systems software

Things are going to speed up! Hold onto your hats!!!

The Eye Chart

- **The Spreadsheet used in this presentation is not included here because of size and lack of readability. Arrangements have been made for you to get a working copy of the actual spreadsheet.**

- **Because of time limitations, these items will briefly reviewed.**

- **The questions are mapped to ISO-17799-1.**

Didn't get the media with the spreadsheet?

- **From your work e-mail, send me an e-mail with "REQUEST VIP RAB1" in the subject line.**
- **In the text of the note, please, include the name and location (city) of your corporate work location.**
- **I will not send to Yahoo, Gmail, Hotmail, MSN, or the like.**
- **Personally, I'd like to know your job assignment as a SECADM, SYSPROG, or whatever.**
- **You will find my e-mail address is on the cover page for this session.**

Didn’t get the media with the spreadsheet?

- **The spreadsheet is provided without warranty of any kind, expressed or implied.**
- **It is ONLY a sample and has not been reviewed by the IBM Corporation for the accuracy, usability, suitability for any purpose or any other review of the materials provided.**
- **Requests for change of any kind will neither be accepted nor acknowledged. It is WYSIWYG. YMMV. You are on your own.**

- **Can I make that any clearer?**