# z/OS Audit Essentials

## Using the IBM Health Checker for z/OS to improve Compliance and Security Integrity

Paul R. Robichaux
NewEra Software, Inc.

4:30 – 5:30 pm, Monday, August 2, 2010
Hynes Convention Center – Room 111

# Abstract and Speaker


- To verify actual integrity levels, all information systems, including those based on the z/OS operating system should be continuously monitored in an effort to validate their conformity with established standards. Such standards are derived from: Common Sense, Best Practices, Operation Policy, Industry and/or Governmental Regulation.

- The IBM Health Checker for z/OS offers a substantial number of z/OS System and Security Checks that can be used within its Framework to constantly monitor for and report on conditions that would result in a deviation from standards and diminished system integrity at the LPAR level.

- This session will provide an operational overview of the IBM Health Checker for z/OS and call out processes from the currently available inventory of Checks that can be used to maintain high levels of automated vigilance over established system and security standards.

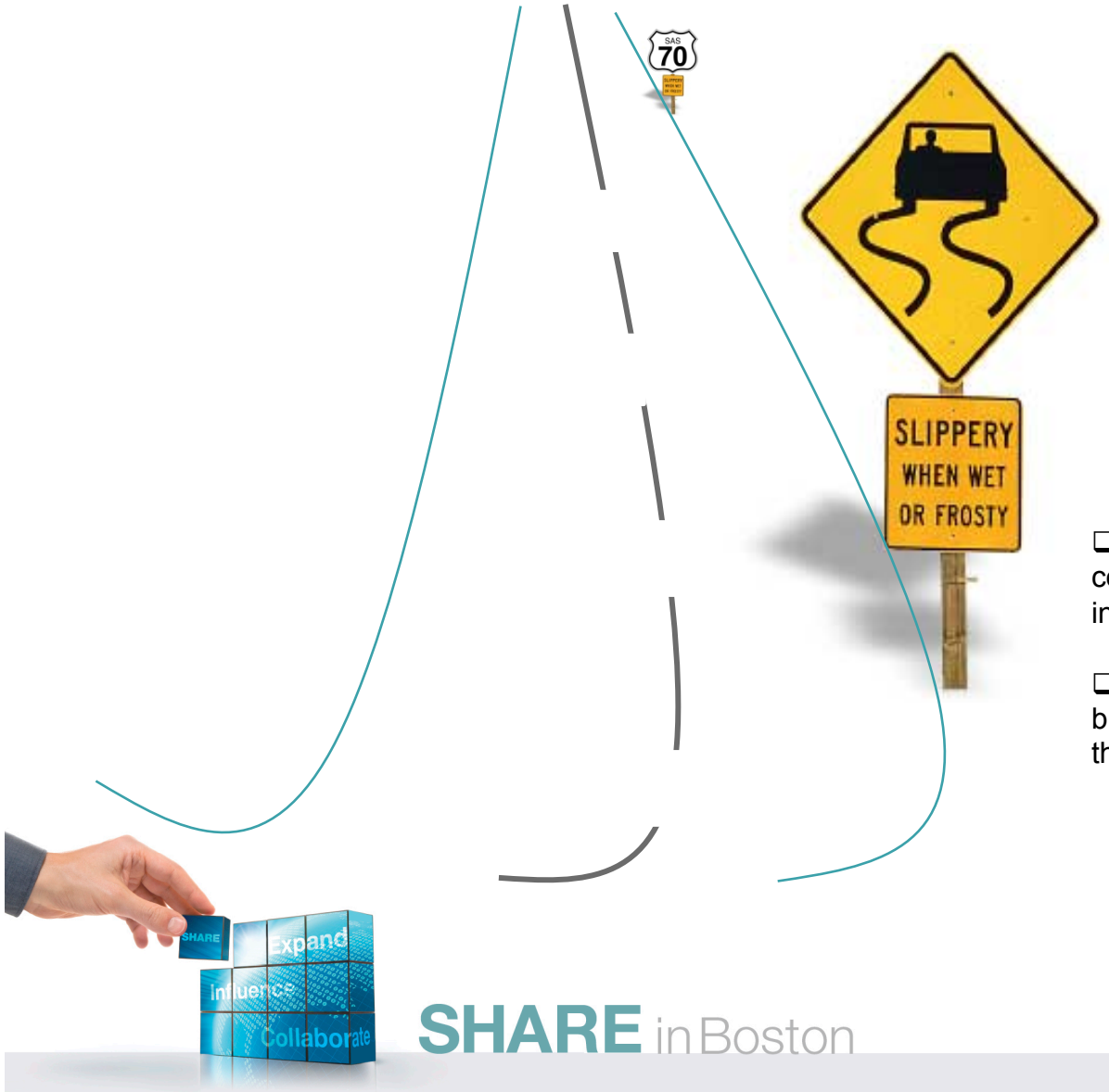
- Paul R. Robichaux, CEO, co-founder of NewEra Software, Inc. began his career in large system computing as an operator and programmer of IBM 407s and 402s. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.

- The corporate mission of NewEra Software is provide software solutions that help their users avoid non-compliance, make corrections when needed and in doing so, continuously improve z/OS integrity and compliance.

# Presentation Outline

1. Our Mission
2. Applicable Terminology
3. Model of System Integrity
4. The IBM Health Checker for z/OS
5. Level-One Integrity Audit
6. Resources and References
7. Dedication

# Our Mission – Why it's important!




- "The road to complete and sustained z/OS compliance runs through verifiable system integrity."
- "System integrity failures can undermine all business and application controls, rendering them worthless."

*Brian Cummings*, TATA Consulting

# Our Mission – The Resulting Imperative!

✓ The Imperative - Accept that contemporary Information Systems and the technical professionals that build, maintain and support them must achieve and sustain the highest levels of integrity.

✓ The Imperative - Recognize that all Information Systems, including those built upon the z/OS operating system, are subject to independent review.

✓ The Imperative - Document a *Model of System Integrity Controls* in an effort to improve the efficiency and ROI of the system review process.

✓ The Imperative - Evangelize the *System Integrity Model to* all *System Stakeholders:* Customers, Management and Auditors as a framework that can efficiently document and demonstrate system compliance.

✓ The Imperative - Consider using The IBM Health Checker for z/OS as the system monitor and focal point of a viable z/OS *System Integrity Model*.

# Applicable Terminology - Compliance

✓ Compliance - the act of adhering to, and demonstrating adherence to, a standard or regulation.

✓ Compliance - describes the goal that corporations or public agencies aspire to in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations.

✓ Compliance - operational transparency that results in organizations adopting the use of consolidated and harmonized sets of compliance controls in order to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity.

- Common Sense
- Best Practice
- Personal Preference
- Internal Policy
- Industrial
- Governmental

# Applicable Terminology - Transparency

✓ Transparency - as used in organizational management and in a social context more generally, transparency implies openness, communication, and accountability.

✓ Transparency - a metaphorical extension meaning a "transparent" object that one can see through.

✓ Transparency - procedures and processes that include open meetings, financial disclosure statements, freedom of information legislation, budgetary review, audits, etc.

- Process Automation
- Periodic Reporting
- Critical Reviews
- Problem Identification
- Research Assignment
- Resolution Review

# Applicable Terminology - Remediation

- ✓ Remediation - An action or series of actions taken to remedy a situation.
- ✓ Remediation - authorized corrective action taken as a result of Process, Critical and/or Resolution Review.
- ✓ Remediation - Intended to correct or improve a discovered deficiency or problem thus returning the environment to a state of compliance with an accepted practice or mandated standard.

- Preventive Controls
- Detective Controls

# Applicable Terminology - Preventive

✓ Preventive - controls that serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company.

✓ Preventive - an action or series of actions that prohibits or mitigates the possibility of an event or series of events.

- RACF - IBM
- ACF2 - CA
- Top Secret - CA

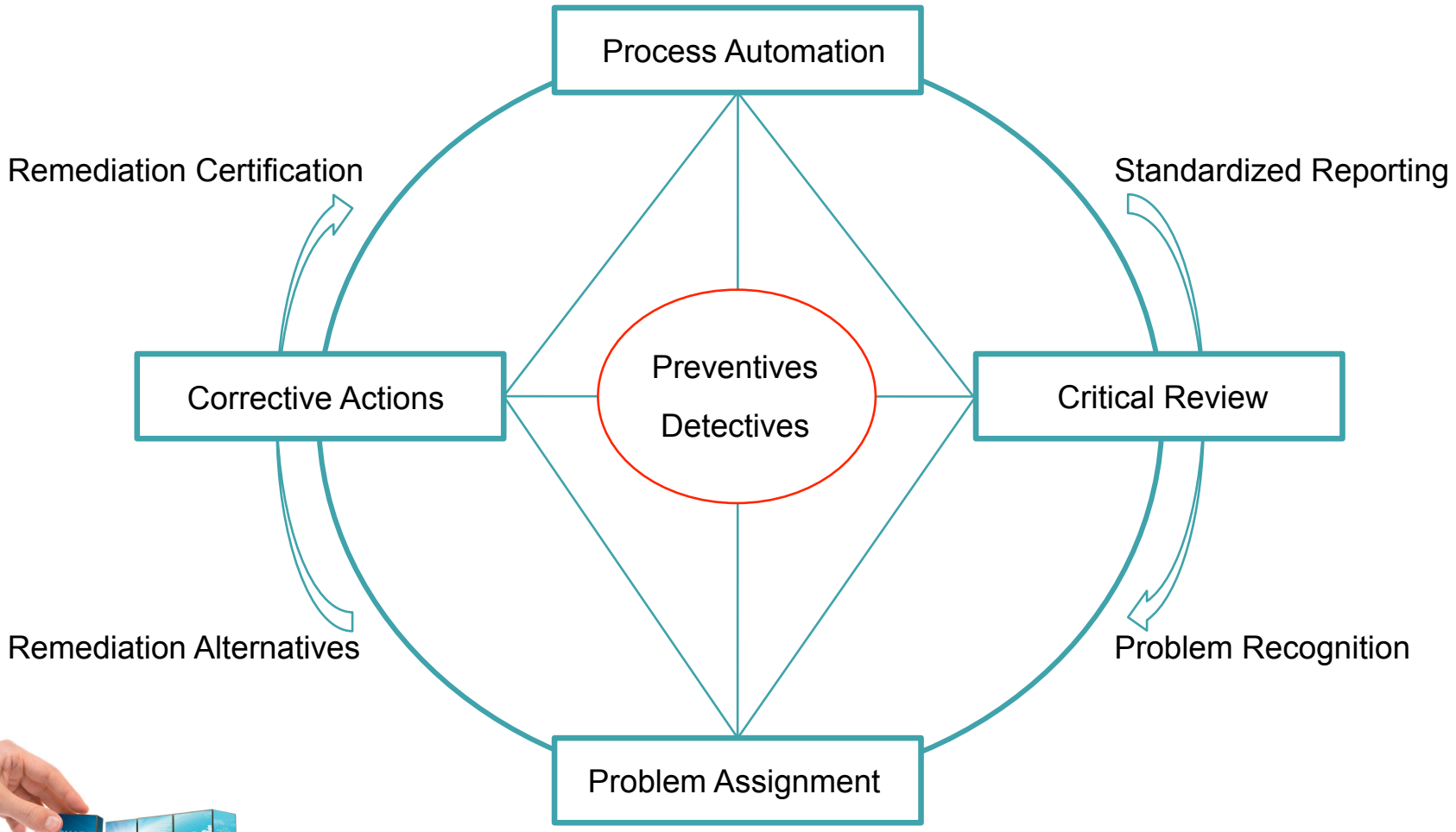
# Applicable Terminology - Detective

✓ Detective – sometimes called *Compensating Controls* - any control that performs a *monitoring activity* can be defined as a Detective Control. Continuing the example of accounting rules, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional control is required to ensure that financial results adhere to established reporting requirements.

✓ Detective - does not prevent action or access but instead detects, records and reports such events. They enhance the integrity of the environment by complementing its existing preventive controls.

- The IBM Health Checker for z/OS - IBM
- The Image Control Environment - NewEra Software
- eventAction - Action Software International
- InCompliance - Vanguard Integrity Professionals
- CA Compliance Manager for z/OS - Computer Associates

# Model of System Integrity - Overview




# Model of System Integrity - Robustness

*10 z/10 Processor with 115 LPAR Targets*

```
------ SYS2.IODF4C - 2013-05-28 16:16:27 - LPARS:115 ------

-------------Processors------------- -----------Logical Partitions----------
-Unit- -Modl- --Serial-- cm -ProcId- -Total- -LCSS0- -LCSS1- -LCSS2- -LCSS3-
------ ------ --Number-- -- -------- cm Numb cm Numb cm Numb cm Numb cm Numb
__2097 ___E26 02DBE22097 .. CPUNORTH .. ___7 .. ___4 .. ___0 .. ___3 .. ___0
__2097 ___E26 02DBD22097 .. CPUSOUTH .. ___6 .. ___3 .. ___0 .. ___3 .. ___0
__2097 ___E56 015BD42097 .. CPUEAST_ .. __16 .. ___3 .. ___0 .. ___0 .. __13
__2097 ___E56 0CDA512097 .. CPUWEST_ .. __18 .. ___2 .. ___0 .. ___6 .. __10
__2097 ___E56 0CDA412097 .. CPUGREEN .. __13 .. ___1 .. ___0 .. ___0 .. __12
__2097 ___E26 0000002097 .. CPUBLACK .. ___4 .. ___2 .. ___0 .. ___2 .. ___0
------ ------ ---------- -- -------- -- ---- -- ---- -- ---- -- ---- -- ----
__2097 ___E56 015BE42097 .. CPUBLUE_ .. ___8 .. ___7 .. ___0 .. ___1 .. ___0
__2097 ___E56 03D4222097 .. CPURED__ .. __14 .. __11 .. ___0 .. ___3 .. ___0
__2097 ___E56 03D4022097 .. CPUBROWN .. __22 .. __14 .. ___8 .. ___0 .. ___0
__2097 ___E56 03D3E22097 .. CPULAST_ .. ___7 .. ___2 .. ___5 .. ___0 .. ___0
_______ _______ __________ .. ________ .. ____ .. ____ .. ____ .. ____ .. ____
_______ _______ __________ .. ________ .. ____ .. ____ .. ____ .. ____ .. ____

          Working directly with Targets found in an IOCP Extract
```

# Model of System Integrity – System Criteria

| Attribute | Characteristics | IBM/HC |
|---|---|---|
| ✓ Automatic | System Controlled Automated Process | |
| ✓ Standards | Site, Industry and Regulatory | |
| ✓ Actionable | Findings Lead to Actions | |
| ✓ Flexible | Site Customization | |
| ✓ Extensible | Local and 3rd Party Support | |
| ✓ Transparent | Multiple Methods for Sharing Findings | |
| ✓ Robust | Multi-System, Multi-LPAR Support | |
| ✓ Efficient | Demonstrable ROI | |


Evaluation: IBM Health Checker for z/OS as a System Integrity Monitor

# About the IBM Health Checker for z/OS

IBM Health Checker for z/OS provides a foundation to help simplify and automate the identification of potential configuration problems before they impact system availability *and integrity*. It compares active values and configuration settings to those suggested by IBM *and others*. The IBM Health Checker for z/OS consists of:

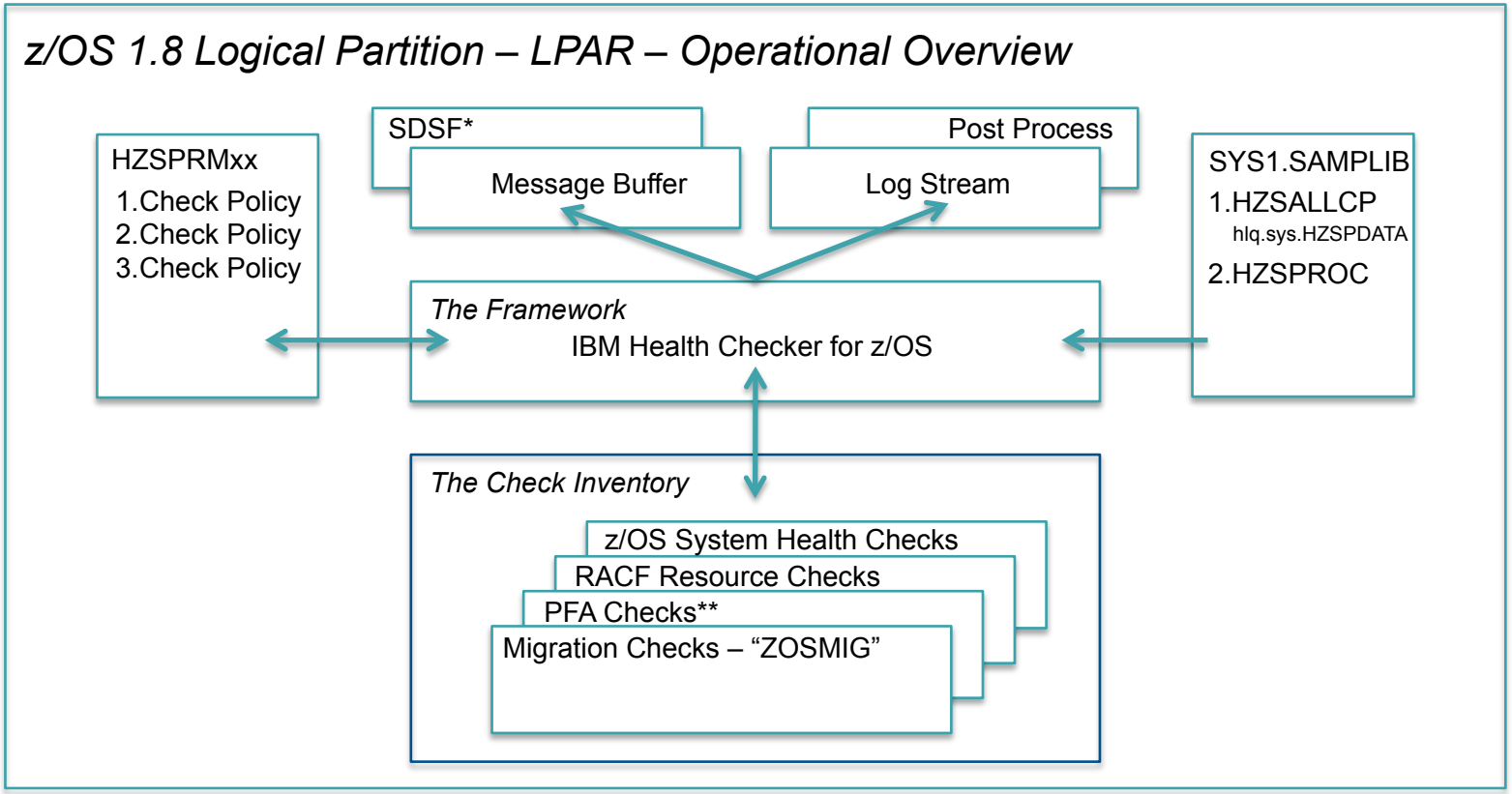
- A framework to manage functions such as check registration, messaging, scheduling, command processing, logging, and reporting.

- An Inventory of Checks, which evaluate settings and definitions specific to products, elements, or components. Checks are provided separately and are independent of the framework. The framework supports checks written by IBM, independent software vendors, and users.

The IBM Health Checker for z/OS is a component of the z/OS Operating System.

http://publibz.boulder.ibm.com/epubs/pdf/e0z2l140.pdf

# About the IBM Health Checker for z/OS




* Or an equivalent (CA SYSVIEW) or HC HZSPRINT Service or HC MODIFY DISPLAY Command
** PFA = Predictive Failure Analysis

# About the IBM Health Checker for z/OS

*Real-Time Check Status - IBM SDSF Display*

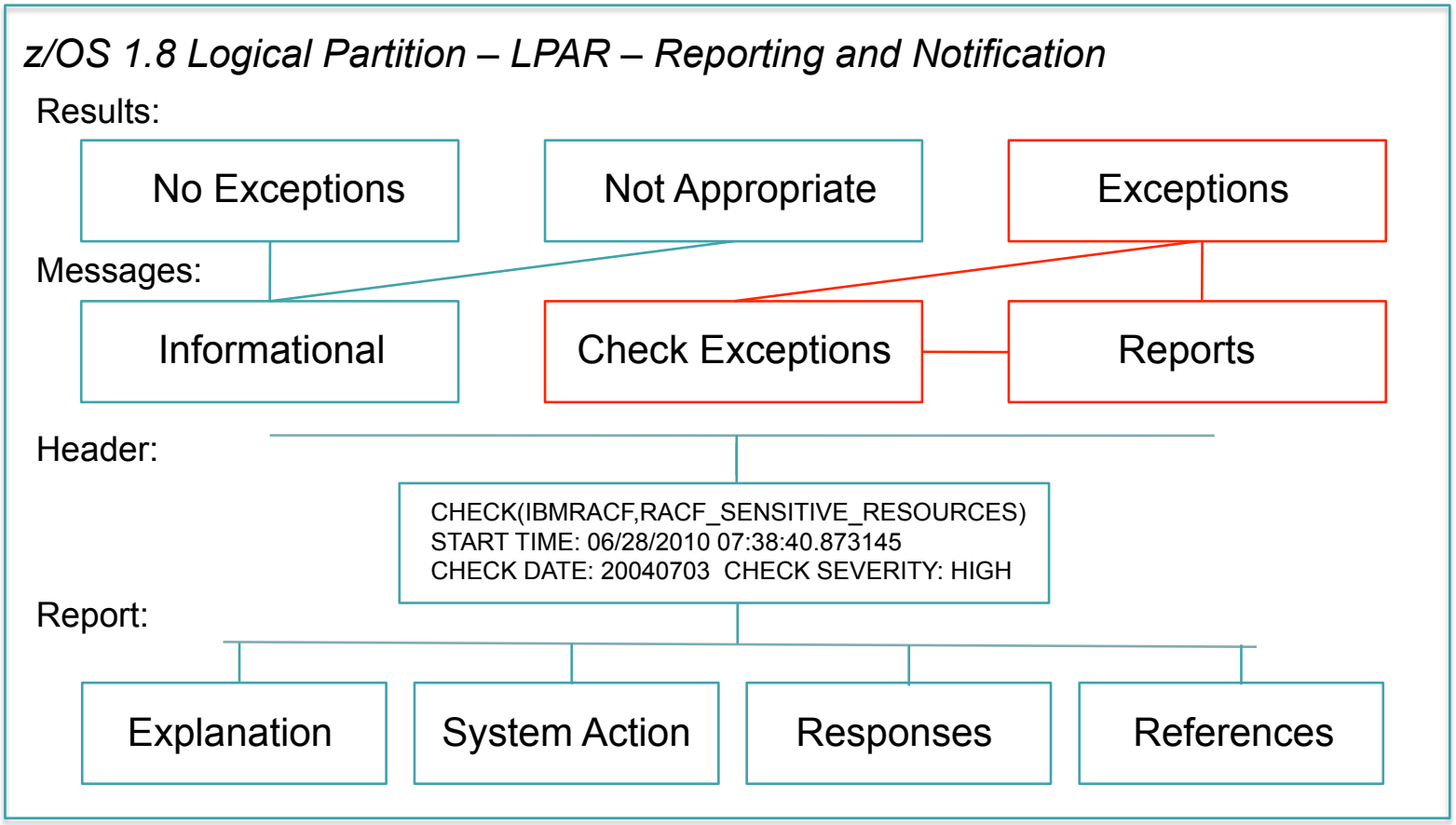
```
  Display  Filter  View  Print  Options  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  SOW1                        LINE 42-58 (113)
COMMAND INPUT ===> _                                      SCROLL ===> PAGE
NP    NAME                          CheckOwner      State              Status
      IXGLOGR_STRUCTUREFULL         IBMIXGLOGR      ACTIVE(ENABLED)    SUCCES
      NEZ_JES2_INSPECTION           NEWERA          ACTIVE(ENABLED)    EXCEPT
      NEZ_JES3_INSPECTION           NEWERA          ACTIVE(DISABLED)   ENV N/
      NEZ_OPSYS_INSPECTION          NEWERA          ACTIVE(ENABLED)    EXCEPT
      PDSE_SMSPDSE1                 IBMPDSE         ACTIVE(ENABLED)    EXCEPT
      RACF_FACILITY_ACTIVE          IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_GRS_RNL                  IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_IBMUSER_REVOKED          IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_OPERCMDS_ACTIVE          IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_SENSITIVE_RESOURCES      IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_TAPEVOL_ACTIVE           IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_TEMPDSN_ACTIVE           IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_TSOAUTH_ACTIVE           IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_UNIXPRIV_ACTIVE          IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RRS_ARCHIVECFSTRUCTURE        IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_DUROFFLOADSIZE            IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_MUROFFLOADSIZE            IBMRRS          ACTIVE(DISABLED)   ENV N/
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=IFIND     F6=BOOK
 F7=UP        F8=DOWN      F9=SWAP      F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

# About the IBM Health Checker for z/OS

*Real-Time Check Status – CA SYSVIEW Display*

```
SYSVIEW 12.5 CA31 ------------- Health Checker -------------- 03/19/10 16:04:23
Command ====>                                                 Scroll *===> PAGE
GSVX005I Beginning of data -------------------- Lvl 1 Row 1-12/434 Col 1-79/633
Formats DEFAULT NEXT2RUN OWNER STATUS
Options CNFM NOXSYS ACT INACT NODEL ENAB DISAB BYNAME
Policy  *NONE*            LogStr  *NONE*                      TaskId  HCHECK
Owner   CA=               Check   =
--------------------------------------------------------------------------------
Cmd Name                                  UState   SState   Status          Global
    ALLOC_VRFY_EOV_X37_SVCS_STATUS        ACTIVE   ENABLED  SUCCESSFUL
    ALLOC_VRFY_PLSOPT10_SNA_X37_SVCE      ACTIVE   ENABLED  SUCCESSFUL
    ALLOC_VRFY_PLSOPT94_USE_STUB          ACTIVE   ENABLED  SUCCESSFUL
    ALLOC_VRFY_PLSZSEC_EOV_X37_SVCE       ACTIVE   ENABLED  EXCEPTION-MEDIUM
    CCS_ENF_SCREEN_VALIDITY               ACTIVE   ENABLED  SUCCESSFUL
    DB2_IDB2_AGNT_DBUG_DF3G@PTX66IDC      ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_AGNT_DBUG_DF3G@PTX77IDC      ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_AGNT_DBUG_D91A@PTX66IDC      ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_AGNT_DBUG_D91A@PTX77IDC      ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_DATASHR_DF3G@PTX66IDC        ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_DATASHR_DF3G@PTX77IDC        ACTIVE   ENABLED  EXCEPTION-LOW
    DB2_IDB2_DATASHR_D91A@PTX66IDC        ACTIVE   ENABLED  SUCCESSFUL
--------------------------------------------------------------------------------
1=HELP 2=RECALL 3=RETURN 5=FIND 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT 12=RECALL
14=SPLIT
```

# About the IBM Health Checker for z/OS




# About the IBM Health Checker for z/OS

*Real-Time Check Status - SDSF Display - RACF_SENSITIVE_RESOURCE*

Explanation: The RACF security configuration check has found one or more potential errors with the system protection mechanisms.

System Action: The check continues processing. There is no effect on the system.

Operator Response: Report this problem to the system security administrator and the system auditor.

System Programmer Response: Examine the report that was produced by the RACF check. Any data set which has an "E" in the "S" (Status) column has excessive authority allowed to the data set. That authority may come from a universal access (UACC) or ID(*) access list entry which is too permissive, or if the profile is in WARNING mode. If there is no profile, then PROTECTALL(FAIL) is not in effect. Any data set which has a "V" in the "S" (Status) field is not on the indicated volume. Remove these data sets from the list or allocate the data sets on the volume.

# About the IBM Health Checker for z/OS

*Real-Time Check Status - SDSF Display - RACF_SENSITIVE_RESOURCE*

Problem Determination: See the RACF System Programmer's Guide and the RACF Auditor's Guide for information on the proper controls for your system.

Source:
RACF System Programmer's Guide
RACF Auditor's Guide

Reference Documentation:
RACF System Programmer's Guide
RACF Auditor's Guide

Automation: None.

Check Reason: Sensitive resources should be protected.

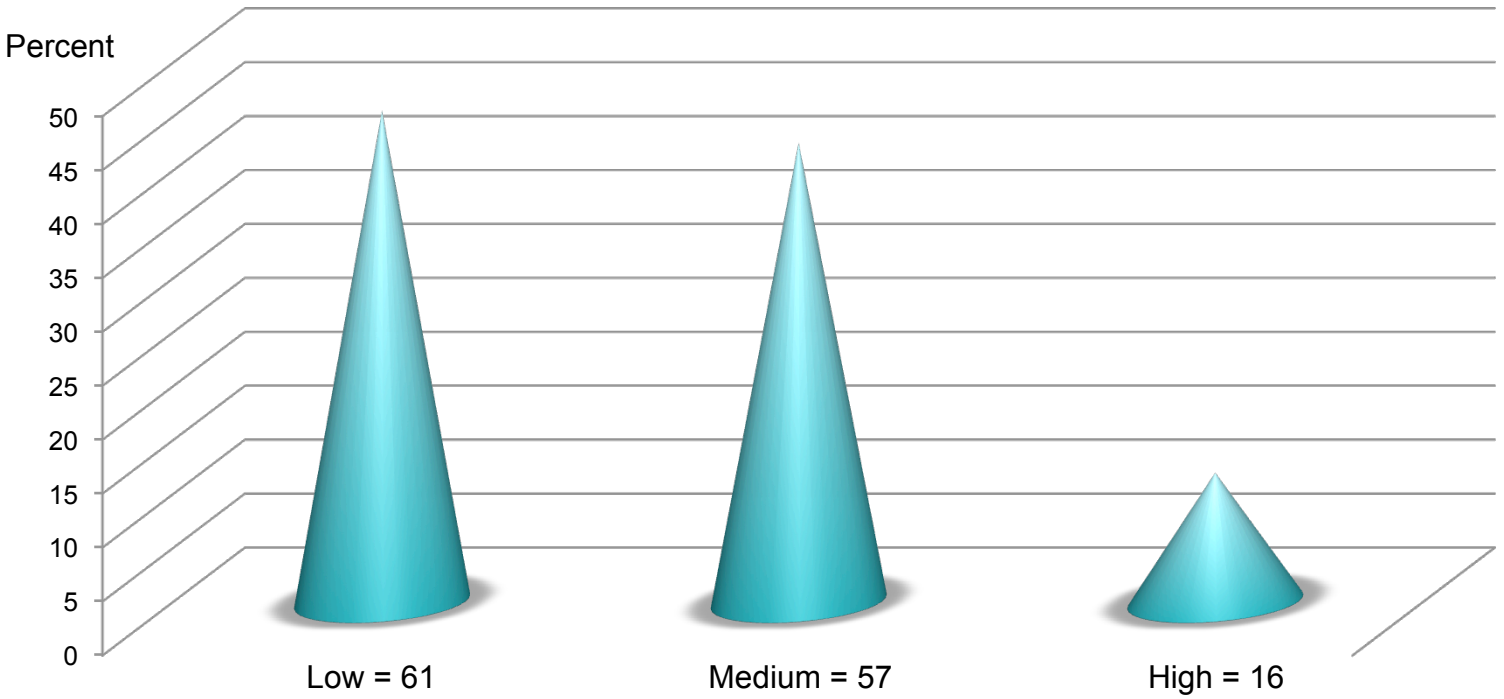
# About the IBM Health Checker for z/OS

*Real-Time Status - Operator Console Display*

```
  13.11.45 STC01629  IFO0375I IPLCHECK INITIALIZATION COMPLETE FOR
   STC=IPLCHECK.
 *13.12.27 STC01533 *HZS0003E CHECK(NEWERA,NEZ_JES2_INSPECTION):
 *NEZH051E The NEZ_JES2_INSPECTION check has found one or
 *more potential errors in IPL integrity on this system.
 *13.12.27 STC01533 *HZS0003E CHECK(NEWERA,NEZ_OPSYS_INSPECTION):
 *NEZH051E The NEZ_OPSYS_INSPECTION check has found one or
 *more potential errors in IPL integrity on this system.
- 13.13.21 TSU01619  IEF450I CCHIN1 SPFPROCE SPFPROCE - ABEND=S622 U0000
-  REASON=00000000
- 13.13.21 TSU01619  IEF377I CCHIN1 SPFPROCE SPFPROCE
-         CCHIN1.SPFLOG2.LIST NOT CATLGD 2
- 13.13.21 TSU01619  $HASP395 CCHIN1   ENDED
```

# About the IBM Health Checker for z/OS

Default Check Severity as a Percentage of all Checks – ( ALL 150 ) - ( MIG 16 ) = 134




# About the IBM Health Checker for z/OS

*High Severity Checks*

- CNZ_EMCS_INACTIVE_CONSOLES
- CSV_LNKLST_NEWEXTENTS
- RACF_SENSITIVE_RESOURCES
- RACF_GRS_RNL
- RRS_Storage_Num_LOGBlks
- RRS_Storage_Num_MSFBlks
- RRS_Storage_ServerRequest
- RRS_Storage_NumTransBlks
- HSM_CDSB_DASD_BACKUP
- RTM_IEAVTRML
- VSAMRLS_DIAG_CONTENTION
- VSAMRLS_SINGLE_POINT_FAILURE
- VSM_CSA_CHANGE
- VSM_CSA_THRESHOLD
- XCF_CDS_SEPARATION
- XCF_CDS_SPOF

# Policy PARMLIB Member - HZSPRMxx

*Check Policy – Updating Individual Checks –* `INACTIVE/DELETE` *- Options*

- ✓ Inactive

```
ADDREPLACE POLICY STMT(INACT1) UPDATE
       CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE)
       DATE(20100628) INACTIVE
       REASON('INACTIVATE ASM LOCAL SLOT CHECK')
```

- ✓ Delete

System Programmer Response: If it is intended that the system broadcast data set be used for user mail then no action is required. Consider using a check policy in HZSPRMxx to DELETE this check:

```
ADDREP POLICY STMT(DEL1) DELETE CHECK(IBMTSOE,TSOE_USERLOGS)
```

# Policy PARMLIB Member - HZSPRMxx

*Check Policy – Updating Individual Checks -* `UPDATE,filters` *- Options*

```
[,ACTIVE|INACTIVE]
[,ADDCAT=(cat1,...,cat16)]
[,DATE={date | (date,NOCHECK)}]
[,DEBUG={OFF|ON}]
[,VERBOSE={NO|YES}]
[,DESCCODE=(desccode1,...,desccoden)]
[,INTERVAL={ONETIME|hhh:mm}]
[,EXCEPTINTERVAL={SYSTEM|HALF|hhh:mm}]
[,PARM=parameter,REASON=reason,DATE={date | (date,NOCHECK)}]
[,REASON=reason]
[,REPCAT=(cat1[,cat2[,...,cat16]])]
[,REMCAT=(cat1[,cat2[,...,cat16]])]
[,ROUTCODE=(routcode1,...,routcoden)]
[,SEVERITY={HIGH|MEDIUM|LOW|NONE}]
[,WTOTYPE={CRITICAL|EVENTUAL|INFORMATIONAL|HARDCOPY|NONE}]
[,REXXTIMELIMIT=timelimit]
```

# LEVEL-ONE Integrity Audit - Check List

| Audit Activity | Note | Status |
|---|---|---|
| ✓ Review and Agree on an Integrity Model | Ok | Done |
| ✓ Identify all z/Platforms | 10 | Done |
| ✓ Identify all z/OS LPARS by z/Platform | 115 | Done |
| ✓ Isolate LPARS of Audit Interest | 25 | |
| ❑ Determine if HZSPROC Active on Interest LPAR | | |
| ❑ Isolate Health Checks of Audit Interest | | |
| ❑ Review HZSPARMxx Policy Statements | | |
| ❑ Agree Policy to Audit Requirements | | |
| ❑ Review Check Status by LPAR | | |
| ❑ Reconcile Non-Standard Findings | | |

# LEVEL-ONE Integrity Audit - Reconciliation

| Check Name | Default | Interest |
|---|---|---|
| RACF_SENSITIVE_RESOURCES | High | High |
| RACF_GRS_RNL | High | High |
| RACF_ICHAUTAB_NONLPA | Medium | High |
| RACF_classname_ACTIVE | Medium | High |
| RACF_IBMUSER_REVOKED | Medium | High |
| CNZ_CONSOLE_ROUTECODE_11 | Low | Medium |
| CSV_APF_EXITS | Low | Medium |
| CSV_LNKLST_SPACE | Low | Medium |
| USS_PARMLIB | Low | Medium |
| XCF_CDS_SEPARATION | Low | Medium |

classname: FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV - Interest: Audit Interest

# LEVEL-ONE Integrity Audit - Score Card

| Check Name | High | Finding | Score |
|---|---|---|---|
| RACF_SENSITIVE_RESOURCES | High | | |
| RACF_GRS_RNL | High | | |
| RACF_ICHAUTAB_NONLPA | High | | |
| RACF_classname_ACTIVE | High | | |
| RACF_IBMUSER_REVOKED | High | | |
| CNZ_CONSOLE_ROUTECODE_11 | Medium | | |
| CSV_APF_EXITS | Medium | | |
| CSV_LNKLST_SPACE | Medium | | |
| USS_PARMLIB | Medium | | |
| XCF_CDS_SEPARATION | Medium | | |

classname: FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV - Interest: Audit Interest

# LEVEL-ONE Integrity Audit - Interactive

*Real-Time Status - Operator Console Display – Check No Longer Valid*

```
  Display  Filter  View  Print  Options  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  SOW1                      CHECK NO LONGER VALID
COMMAND INPUT ===>                                      SCROLL ===> PAGE
NP    NAME                              CheckOwner      State              Status
      PDSE_SMSPDSE1                     IBMPDSE         ACTIVE(ENABLED)    EXCEPT
      RACF_FACILITY_ACTIVE              IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_GRS_RNL                      IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_IBMUSER_REVOKED              IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_OPERCMDS_ACTIVE              IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_SENSITIVE_RESOURCES          IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_TAPEVOL_ACTIVE               IBMRACF         ACTIVE(ENABLED)    EXCEPT
S     RACF_TEMPDSN_ACTIVE               IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RACF_TSOAUTH_ACTIVE               IBMRACF         ACTIVE(ENABLED)    SUCCES
      RACF_UNIXPRIV_ACTIVE              IBMRACF         ACTIVE(ENABLED)    EXCEPT
      RRS_ARCHIVECFSTRUCTURE            IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_DUROFFLOADSIZE                IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_MUROFFLOADSIZE                IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_RMDATALOGDUPLEXMODE           IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_RMDOFFLOADSIZE                IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_RSTOFFLOADSIZE                IBMRRS          ACTIVE(DISABLED)   ENV N/
      RRS_STORAGE_NUMLARGELOGBLKS       IBMRRS          INACTIVE(ENABLED)  INACTI
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=IFIND     F6=BOOK
 F7=UP        F8=DOWN      F9=SWAP      F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display - RACF_SENSITIVE_RESOURCES*

Verifies the protection of each resource by examining the UACC, WARNING status, and the ID(*). If there is no profile protecting a data set, then if NOPROTECTALL or PROTECTALL(WARN) is in effect, the check flags the data set as an exception.

Optionally, specify a user ID to the check which, if specified, is used to perform a RACF authorization check for the next higher access authority after the highest expected general access authority.

- APF Dataset Report
- RACF Dataset Report
- PARMLIB Dataset Report
- Current Link List Dataset Report
- System Rexx Dataset Report
- Sensitive General Resources Report

```
S Resource Name                              Class    UACC Warn ID*  User
- ------------------------------------------ -------- ---- ---- ---- ----
```

- ICHAUTAB Report

```
S Module   REQUEST=VERIFY REQUEST=LIST Location
- -------- -------------- ------------ --------
```

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display - RACF_GRS_RNL*

During its normal course of processing, RACF performs numerous serialization requests using the Global Resource Serialization (GRS) RESERVE, ENQ, and DEQ services. These serialization requests allow RACF to ensure that changes to the RACF database and RACF control blocks are done in a consistent manner, maintaining the integrity of RACF data.

CHECK(IBMRACF,RACF_GRS_RNL)
START TIME: 06/30/2010 07:37:21.871542
CHECK DATE: 20040703  CHECK SEVERITY: HIGH

RACF_GRS_RNL Report

```
S Major    Minor                Type  QName    Rname              Type
- -------- -------------------- ----- -------- ----------------- ----
```

IRRH203I No RACF ENQ names were found in the GRS Resource Name List.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display - RACF_ICHAUTAB_NONLPA*

Examines the RACF Authorized Caller Table (ICHAUTAB) and reports if there are any non-LPA entries in it.

The output format is similar to the report format for the ICHAUTAB Report in RACF_SENSITIVE_RESOURCES, with the exception that LPA-resident modules are not listed.

ICHAUTAB Report

```
S Module   REQUEST= REQUEST= Location
           VERIFY   LIST
- -------- -------- -------- --------
```

IRRH239I There are no ICHAUTAB programs on this system.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display - RACF_classname_ACTIVE*

Examines the status of any of the following single RACF general resource class:

*classname=*

- UNIXPRIV
- FACILITY
- TAPEVOL
- TEMPDSN
- TSOAUTH
- OPERCMDS

IRRH229E The class TAPEVOL is not active.

Explanation: The class is not active. IBM recommends that the security administrator at your installation activate this class and define in it the profiles to properly protect your system.

System Action: The check continues processing. There is no effect on the system.

Operator Response: Report this problem to the system security administrator and the system auditor.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – RACF_IBMUSER_REVOKED*

Examines the RACF Profile Database to determine if the user ID, IBMUSER is still active.

IRRH225E The user ID IBMUSER is not revoked.

Explanation: The user ID IBMUSER has not been revoked. IBM recommends revoking IBMUSER.

System Action: The check continues processing. There is no effect on the system.

Operator Response: Report this problem to the system security administrator and the system auditor.

System Programmer Response: Revoke IBMUSER.

Problem Determination: See the RACF Auditor's Guide and the RACF Systems Programmer's Guide.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – CNZ_CONSOLE_ROUTECODE_11*

```
Console    Console       Active
Type       Name         System
SYSCONS    HWCI        S0W1
SMCS       PRR1        (Inactive)
SMCS       PAT1        (Inactive)
SMCS       GHB1        (Inactive)
SMCS       MFZ1        (Inactive)
MCS        S0W103E1    (Inactive)
MCS        S0W10FFF    (Inactive)
```

CNZHF0005I One or more consoles are configured to receive messages intended only for programmers.

Explanation: One or more consoles are configured to receive messages with routing code 11. Messages issued with routing code 11 are intended to be sent to the programmer, not the operator console.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – CSV_APF_EXITS*

CSVH0955I A problem was found with each APF list entry displayed.

```
VOLUME  DSNAME                                  ERROR
VTMVSC  ANF.SANFLOAD                            DS not found
VTMVAB  CEE.SCEERUN                             Volume not found
```

Explanation:  CSVH0955I has been placed in the message buffer to describe the APF list entry error and condition that caused the exception.

A potential system integrity risk exists when a data set cannot be allocated using the criteria specified in the system APF list. If this data set were created it would be considered APF-authorized.

The error is one of the following conditions:

DS is alias

The data set name is an alias of another data set.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – CSV_LNKLST_SPACE*

Explanation: CSVH0979I has been placed in the message buffer for each LNKLST LNKLST set. It lists all data sets with secondary space defined.

IBM suggests that partitioned data sets (PDS's) in the LNKLST be allocated with only primary extents, for two reasons.

First, a PDS allocated with only primary space defined has only one extent. This makes it easier to stay within the 255-extent limit for an active LNKLST concatenation without having to reallocate data sets with fewer initial extents.

Second, if a PDS will be updated while in the LNKLST set, it can be extended if it has been allocated using secondary space. This can cause members to be placed in extents that did not exist when the LNKLST concatenation was activated. An attempt to access a member in a new extent causes the requesting program to abend.

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – USS_PARMLIB*

CHECK(IBMUSS,USS_PARMLIB)
START TIME: 06/30/2010 13:14:18.100041
CHECK DATE: 20060112  CHECK SEVERITY: LOW

BPXH003I z/OS UNIX System Services was initialized using:

OMVS=(OM,FS,SV,MS,61,65,VN)

where each 2-character item is a BPXPRMxx suffix.

BPXH039I No differences were found between the system settings and the settings in the BPXPRMxx parmlib members.

END TIME: 06/30/2010 13:14:19.908682  STATUS: SUCCESSFUL

# LEVEL-ONE Integrity Audit

*Real-Time Check Status - SDSF Display – XCF_CDS_SEPARATION*

IXCH0907I Describes couple data set configurations.

```
CDS Type      = The type of couple data set, ex. "CFRM" or "SYSPLEX"
Use           = PRI or ALT to indicate primary or alternate
Volser        = The volume serial on which the couple data set resides.
Unit          = The device number associated with the volume
Data Set Name = The couple data set name.

CDS Type Use Volser Unit Data Set Name
-------- --- ------ ---- ----------------------------------------
SYSPLEX  PRI Z14AUX 3102 SYS1.XCF.CDS03.JDC2
         ALT Z14MAN 310B SYS1.XCF.CDS04.JDC2
CFRM     PRI Z14AUX 3102 SYS1.XOH.PRMCFRM.JDC2
         ALT Z14AUX 3102 SYS1.XOH.ALTCFRM.JDC2
```

The check found that the primary CDS for types that should be separated reside on the same volume:

```
CDS Type    Volser    Data Set Name
--------    ------    ----------------------------------------
SYSPLEX     Z14AUX    SYS1.XCF.CDS03.JDC2
CFRM        Z14AUX    SYS1.XOH.PRMCFRM.JDC2
```

# LEVEL-ONE Integrity Audit - Score Card

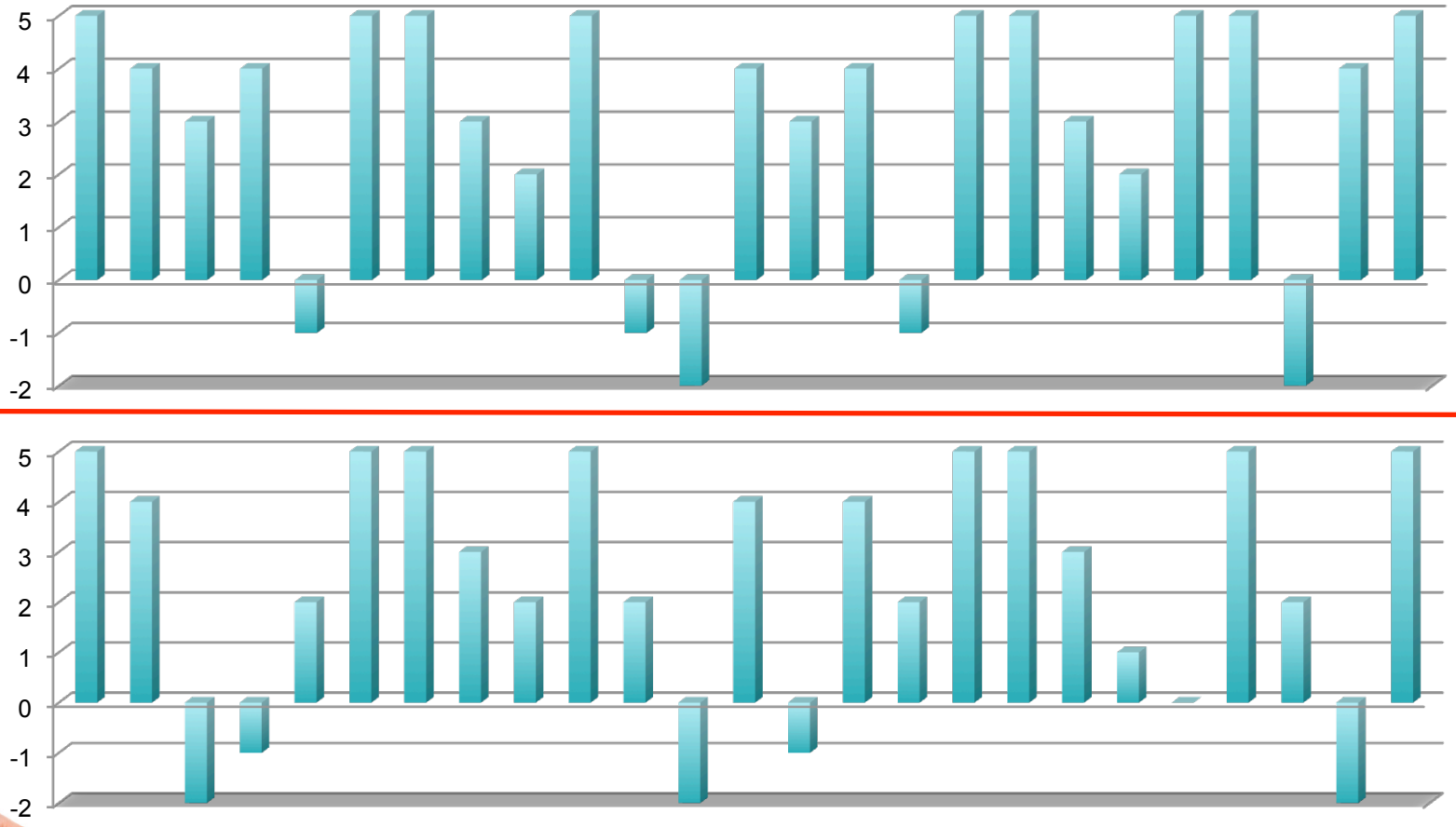
| Check Name | High | Finding | Score |
|---|---|---|---|
| RACF_SENSITIVE_RESOURCES | High | Exception | |
| RACF_GRS_RNL | High | None | |
| RACF_ICHAUTAB_NONLPA | High | NOP | |
| RACF_classname_ACTIVE | High | Success | |
| RACF_IBMUSER_REVOKED | High | Success | |
| CNZ_CONSOLE_ROUTECODE_11 | Medium | Exception | |
| CSV_APF_EXITS | Medium | Exception | |
| CSV_LNKLST_SPACE | Medium | Exception | |
| USS_PARMLIB | Medium | Success | |
| XCF_CDS_SEPARATION | Medium | Exception | |

classname: FACILITY, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV - Interest: Audit Interest

# LEVEL-ONE Integrity Audit - Check List

| Audit Activity | Note | Status |
|---|---|---|
| ✓ Review and Agree on an Integrity Model | Ok | Done |
| ✓ Identify all z/Platforms | 10 | Done |
| ✓ Identify all z/OS LPARS by z/Platform | 115 | Done |
| ✓ Isolate LPARS of Audit Interest | 25 | Done |
| ✓ Determine if HZSPROC Active on Interest LPAR | 20 | Done |
| ✓ Isolate Health Checks of Audit Interest | 10 | Done |
| ✓ Review HZSPARMxx Policy Statements | Ok | Done |
| ✓ Agree Policy to Audit Requirements | Ok | Done |
| ❑ Review Check Status by LPAR | | |
| ❑ Reconcile Non-Standard Findings | | |

# LEVEL-ONE Integrity Audit - Sample




*Audit Finding Profiles within Scope by LPAR*

# LEVEL-ONE Integrity Audit – Batch

*Check Status - Batch - Summary*

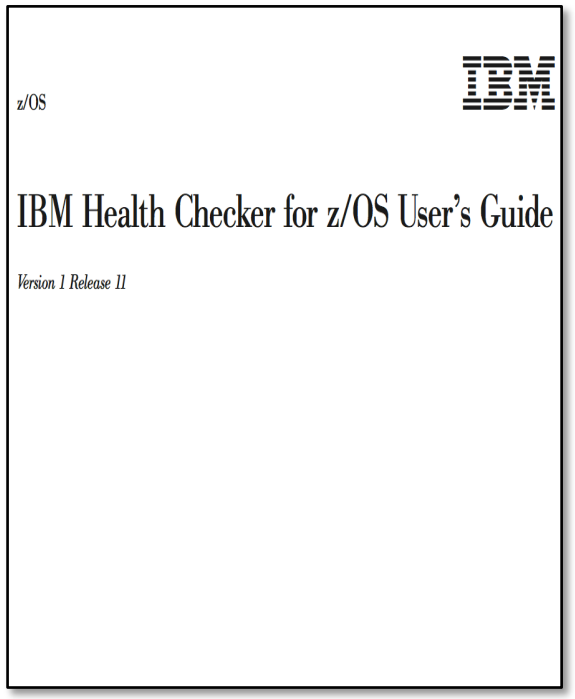
| Entry | Date | Time | State | Owners | Check Name |
|---|---|---|---|---|---|
| 001 045 | 06/30/10 | 15:42:45 | EXC HIG | IBMRACF | RACF_SENSITIVE_RESOURCES |
| 002 095 | 06/30/10 | 16:37:43 | EXC HIG | IBMXCF | XCF_CDS_SEPARATION |
| 003 101 | 06/30/10 | 16:22:49 | EXC HIG | NEWERA | NEZ_JES2_INSPECTION |
| 004 102 | 06/30/10 | 16:22:49 | EXC HIG | NEWERA | NEZ_OPSYS_INSPECTION |
| 001 004 | 06/27/10 | 15:37:21 | EXC MED | IBMASM | ASM_PAGE_ADD |
| 002 017 | 06/30/10 | 16:37:43 | EXC MED | IBMCNZ | CNZ_SYSCONS_PD_MODE |
| 003 038 | 06/30/10 | 16:25:52 | EXC MED | IBMRACF | RACF_TEMPDSN_ACTIVE |
| 004 040 | 06/30/10 | 15:37:21 | EXC MED | IBMRACF | RACF_UNIXPRIV_ACTIVE |
| 005 041 | 06/30/10 | 15:37:21 | EXC MED | IBMRACF | RACF_TAPEVOL_ACTIVE |
| 006 044 | 06/30/10 | 15:37:21 | EXC MED | IBMRACF | RACF_IBMUSER_REVOKED |
| 007 092 | 06/30/10 | 15:37:21 | EXC MED | IBMXCF | XCF_TCLASS_CLASSLEN |
| 008 097 | 06/30/10 | 15:37:21 | EXC MED | IBMXCF | XCF_SFM_ACTIVE |
| 001 012 | 06/27/10 | 15:37:24 | EXC LOW | IBMCS | CSVTAM_VIT_DSPSIZE |
| 002 013 | 06/27/10 | 15:37:24 | EXC LOW | IBMCS | CSVTAM_VIT_OPT_PSSSMS |

# Site Support – Write your own Check!

*Write your own RACF resource checks!*

You can create your own RACF installation-defined resource checks to see if your resources have the security characteristics you want. Do the following for each check you wish to create:

1 - Define a RACF profile containing a list of the resources you want your RACF installation-defined resource check to look at, along with the maximum allowable general user access you want for each resource…




# 3rd Party Vendor Support - CA

## CA ACF2 – health checker integration

**Health check routine**

- ✓ Determine Expiring Digital Certificates
- ✓ Determine use of SAFDEFs with NOAPFCHK
- ✓ Determine if the CA ACF2 AUTO Start feature is in use (CAISEC00)

Leveraging the power of the z/OS Health Checker for your Security implementation

**Benefit**

- ✓ Reduce likelihood of failed production jobs due to expired certificate
- ✓ Reduce risk of user bypassing APF checking on RACROUTE calls
- ✓ Enables CA ACF2 to start early and ensures other Address Spaces that start during IPL will have correct level of security

caWorld'10 2 May 16-20, 2010 

# 3rd Party Vendor Support - CA

*Available Checks:*

CA Security Products now integrated with the IBM Health Checker for z/OS through the CA Health Checker Common Service.

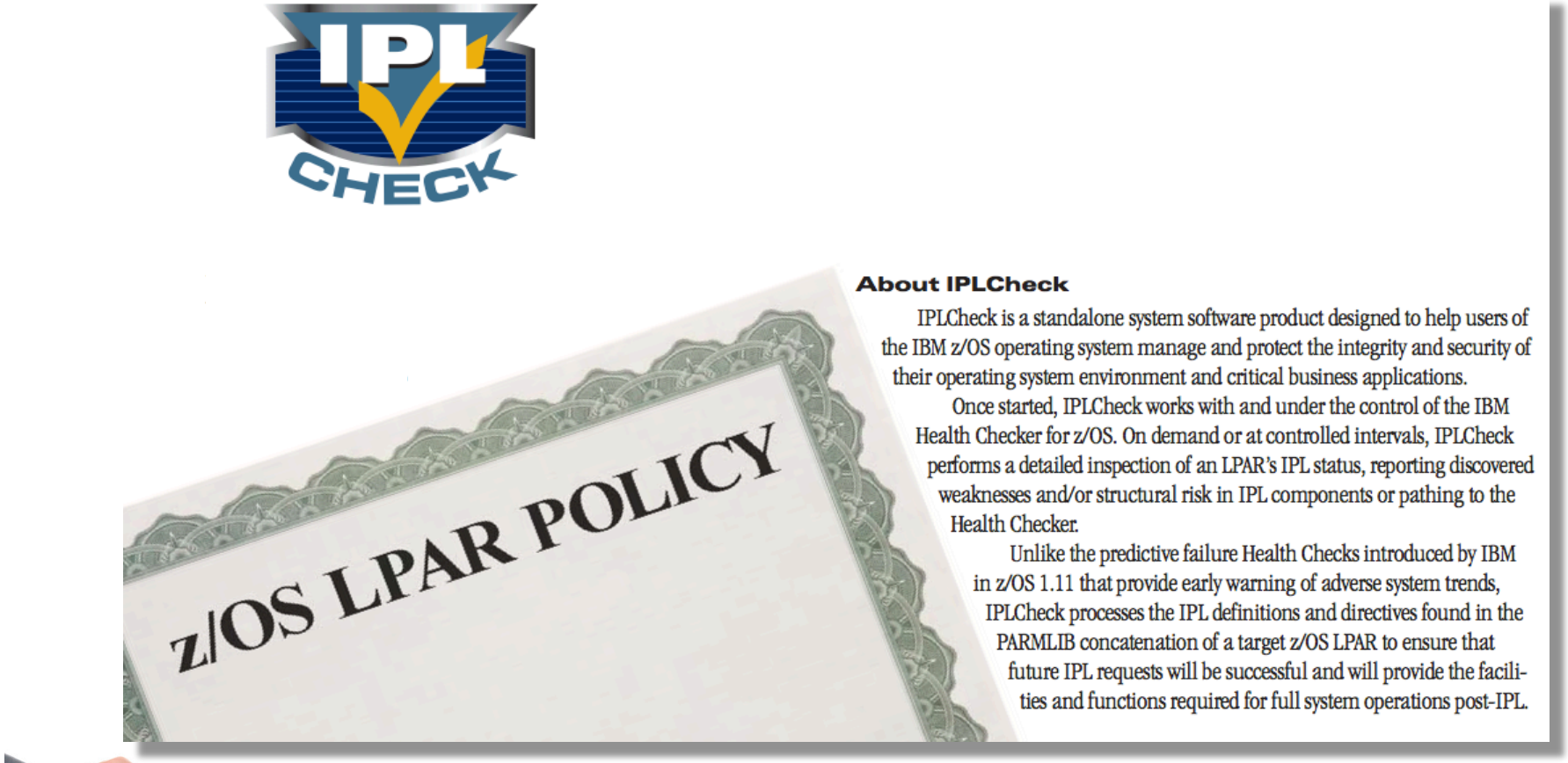
ACF2 Checks Include:

- ACF2_CHECK_JES2_EXITS - Validates all the CA ACF2 JES2 exits are in place and enabled.
- ACF2_CHECK_EXITS - Validates all CA ACF2 security exit points.
- ACF2_CHECK_DATABASES - Validates that no connected MVS master or user catalogs exist on the same volumes as the CA ACF2 databases.
- ACF2_CHECK - Expiring ACF2 Digital Certificates.

Top Secret Checks Include:

- TSS_CHECK - Reports conflicts with the placement of the CA Top Secret Audit Tracking File and the Security File.
- TSS_CHECK - Reports if CACHE and SECCACHE features are enabled.
- TSS_CHECK - Expiring Top Secret Digital Certificates.

# 3rd Party Vendor Support - NewEra




# 3rd Party Vendor Support - NewEra

*Available Checks:*

NewEra Integrity Products now integrated with the IBM Health Checker for z/OS through the NEZ_CHECK Interface.

Configuration Integrity Checks Include:

- NEZ_OPSYS_INSPECTION - Validates z/OS configuration definitions.
- NEZ_JES2_INSPECTION - Validates JES2 configuration definitions.
- NEZ_JES3_INSPECTION - Validates JES3 configuration definitions.
- NEZ_VTAM_INSPECTION - Validates VTAM configuration definitions.
- NEZ_TCPIP_INSPECTION - Validates TCP/IP configuration definitions.
- NEZ_CICS_INSPECTION - Validates CICS SIT configuration definitions.
- NEZ_OPSYS_CHANGES - Reports dynamic z/OS configuration changes.

# Model of System Integrity – System Criteria

| Attribute | Characteristics | IBM/HC |
|---|---|---|
| ✓ Automatic | System Controlled Automated Process | Good |
| ✓ Standards | Site, Industry and Regulatory | Good |
| ✓ Actionable | Findings Lead to Actions | Excellent |
| ✓ Flexible | Site Customization | Good |
| ✓ Extensible | Local and 3rd Party Support | Good |
| ✓ Transparent | Multiple Methods for Sharing Findings | Good |
| ✓ Robust | Multi-System, Multi-LPAR Support | Somewhat |
| ✓ Efficient | Demonstrable ROI | Excellent |


Evaluation: IBM Health Checker for z/OS as a System Integrity Monitor

# Resources

- Brian Cummings - Tata Consultancy Services - brian.cummings@tcs.com
- Stu Henderson - The Henderson Group - stu@stuhenderson.com
- Reg Harbeck - CA, Inc. - Reg@ca.com
- Julie-Ann Williams - millennia ltd - julie@sysprog.co.uk
- Craig Warren - millennia ltd - craig@sysprog.co.uk
- Martin Underwood - millennia ltd - martin@sysprog.co.uk
- Barry Schrager - Vanguard Professionals - barry.schrager@go2vanguard.com
- Mike Cairns - IBM Tivoli Asia Pacific - mike.cairns@au1.ibm.com
- Dinesh Dattani - z/OS Consultant - dinesh123@rogers.com
- David Hayes - U.S. Government Accountability Office - hayesd@gao.gov
- Mark Wilson - RSM Partners - markw@rsmpartners.com

# References



- IBM Health Checker for z/OS Users Guide – SA22-7994-09
- MVS Initialization and Tuning Reference – SA22-7592-17
- MVS System Command Reference – SA22-7627-18
- MVS Planning Operations – SA22-7601-09
- CICS Audit Essentials – Julie-Ann Williams, Mike Cairns, Craig Warren and Martin Underwood
- CICS Best Practices – Julie-Ann Williams, Craig Warren and Martin Underwood
- Mainframe Audit News – Stu Henderson, The Henderson Group
- Information Security – NIST Publication 800-53 – February 2009
- NAIC Model Audit Rules & Implementation – Deloitte
- AUDIT.NET
- z/OS Audit Essentials, Volume 1 of 2 – Julie-Ann Williams, Editor


# Dedication

In Memory of

Denise Fitzpatrick

SHARE volunteer from 3/1/2000