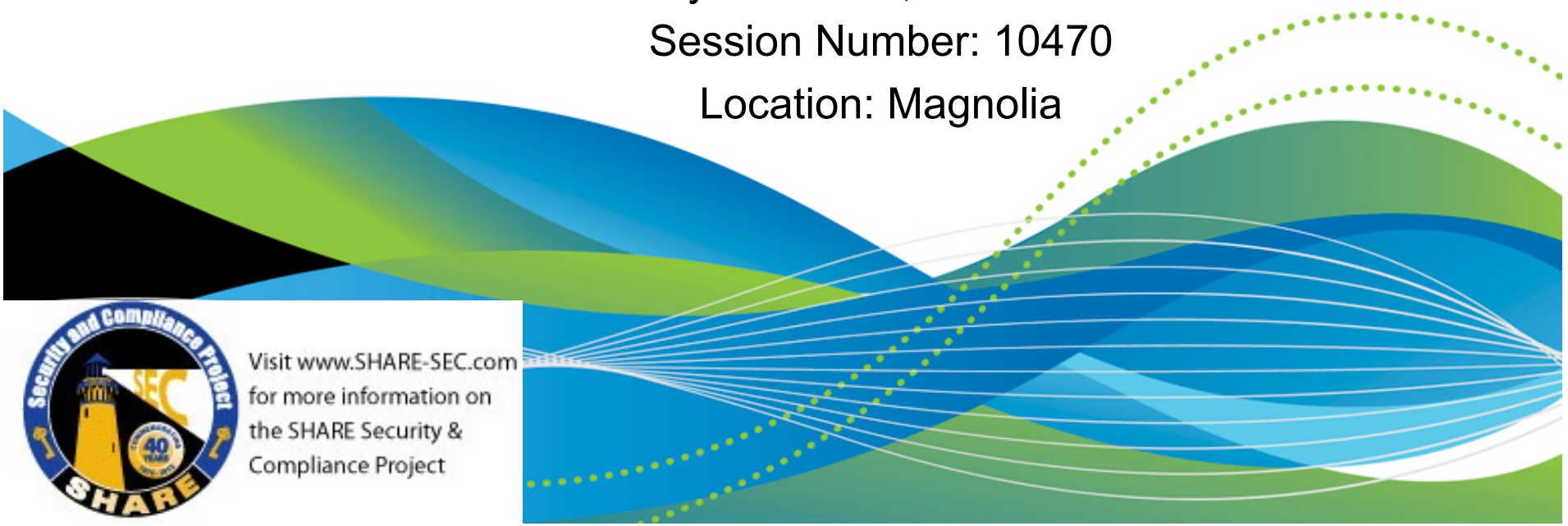
#SHAREorg

SHARE
Technology · Connections · Results

# How to avoid the 10 Most Embarrassing zEnterprise Audit Findings

Paul Robichaux
NewEra Software, Inc.

Tuesday March 13, 2012 – 1:30PM
Session Number: 10470
Location: Magnolia






Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

# Abstract and Speaker


- All information systems and those based on the z/OS operating system must be continuously monitored in an effort to validate their conformity with established standards. Such standards are often times derived from Common Sense, Best Practices, Personal Preference, Operational Policy as well as Industry and/or Governmental Regulation.

- This presentation will provide insight into:

  First, the mission of those charged with the responsibility to enhance, maintain and sustain the operational availability and integrity of the zEnterprise, this within the context of recommended ongoing efforts to reduce the Total Cost of z/Enterprise Ownership (TCO).

  Second, the views of recognized z/OS compliance authorities, each of which contributed to the content of this presentation. A selection of their common audit findings and related remediation strategies will be introduced and result in both a Pre and Post IPL/ESM Check List.

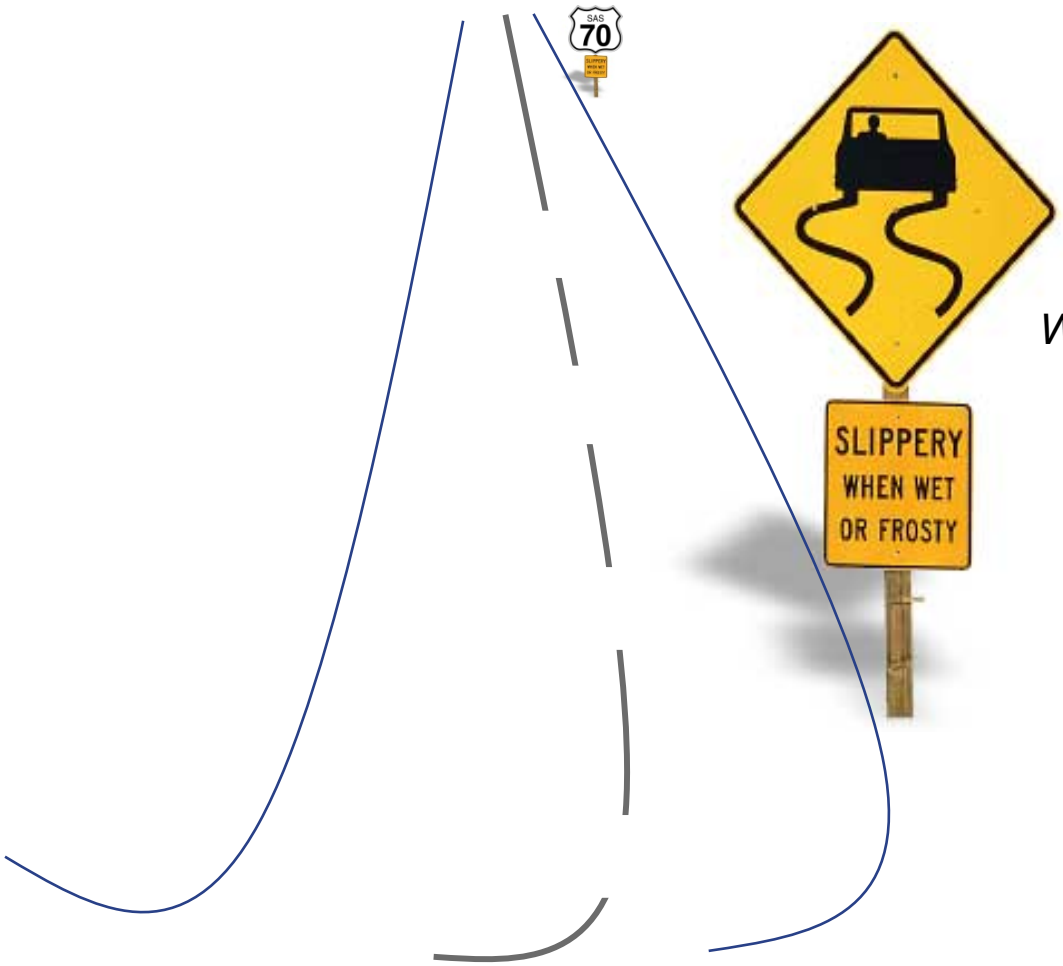
  Third, how to use the IBM Health Checker for z/OS to improve zEnterprise integrity and security and, at the same time, reduce the overall cost of the Mainframe Software Stack (MSS).

- Paul R. Robichaux, CEO, co-founder of NewEra Software, Inc. began his career in large systems 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 to provide software solutions that help users avoid non-compliance, make corrections when needed and in doing so, continuously improve z/OS integrity.

# Our Mission

*Continuous, Sustainable Improvements in z/OS Availability and Compliance.*




*Why is this important?*

"…generally we all want to be technically current, not necessarily at the 'Bleeding-Edge' but close enough to be knowledgeable of release-to-release changes and the impact they will have on our z/OS systems, their operational costs and organizational users."

# Outline – Where We're Going!

1. Our Mission - (1/4)
   - ✓ What is Compliance?
   - ✓ The Need for Shared Values
   - ✓ Critical Success Factors
   - ✓ System Control Points
   - ✓ Organizational Acceptance
   - ✓ Cost of Implementation
   - ✓ Health Checker Overview
   - ✓ Integrity Checks in Action
2. Let's ask the Industry Experts! – (3/4)
   - ✓ Are They Active Enough, Smart Enough?
   - ✓ What does Bad News Look Like?
   - ✓ Who are these Guys?
   - ✓ Distinguish Pre-IPL/ESM from Post-IPL/ESM
   - ✓ Pre-IPL/ESM Details and Recommendations
   - ✓ Post-IPL/ESM Details and Recommendations
   - ✓ Safe Haven Guidelines.
3. Health Checker - Hands-on Lab – *Recommended*

   Session 10601 and Session 10876 or send email to support@newera.com - Send Lab
4. Resources, References and Sessions - *Recommended*
   - ✓ z/Auditing Essentials - Volume 1 - zEnterprise Hardware - An Introduction for Auditors
   - ✓ How Barry Schrager Changed Your World – Believe it!

   Both Edited By Julie-Ann Williams - julie@sysprog.co.uk

# Our Mission

*System Compliance Model – Shared Values:*

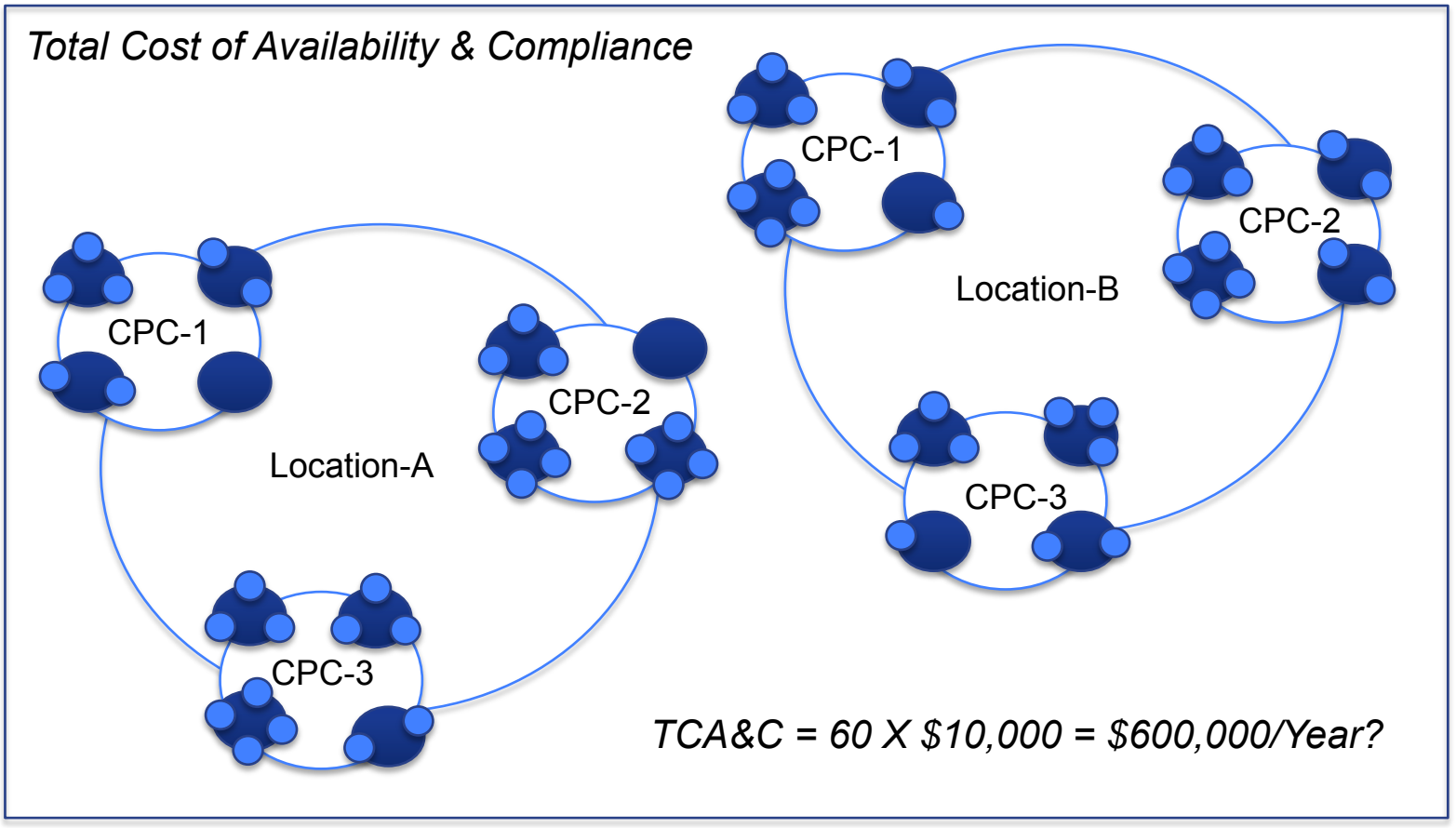
✓ Accept that contemporary Information Systems and the technical professionals that build, maintain and support them must achieve and sustain the highest levels of system integrity.

✓ Recognize that all Information Systems, including those built upon the z/OS operating system must conform to established standards and are subject to independent review for the purpose of compliance verification.

✓ The adoption of a *System Compliance Model* is *The* critical success factor in understanding and improving the effectiveness of the system review process.

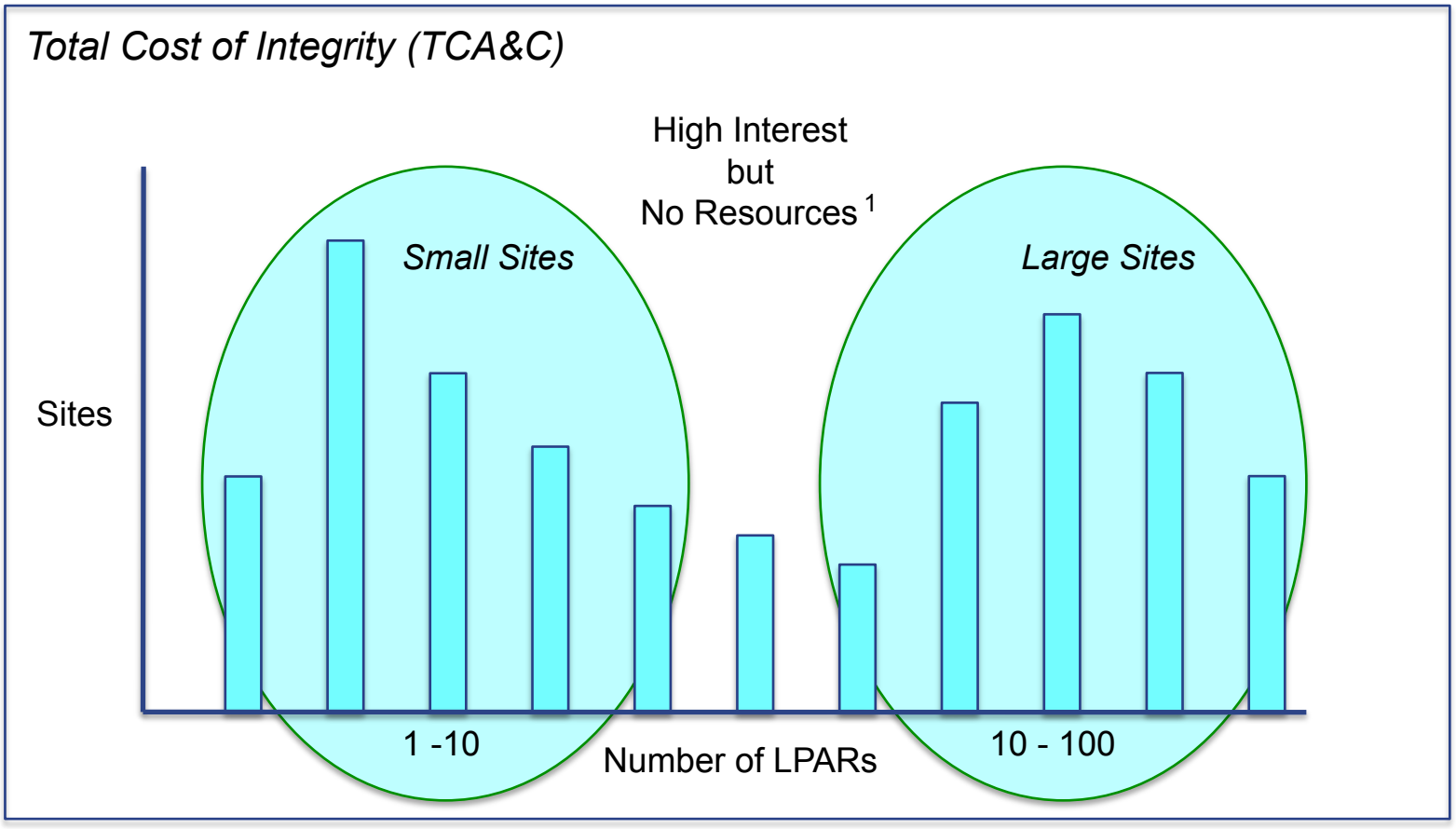
✓ Evangelize the *System Compliance Model to* all *System Stakeholders:* System Users, Management and Compliance Officers as a framework that can efficiently improve, document and demonstrate system compliance.

# Our Mission




Glenn Anderson – MVS Program Keynote – The zEnterprise: A True Game Changer.

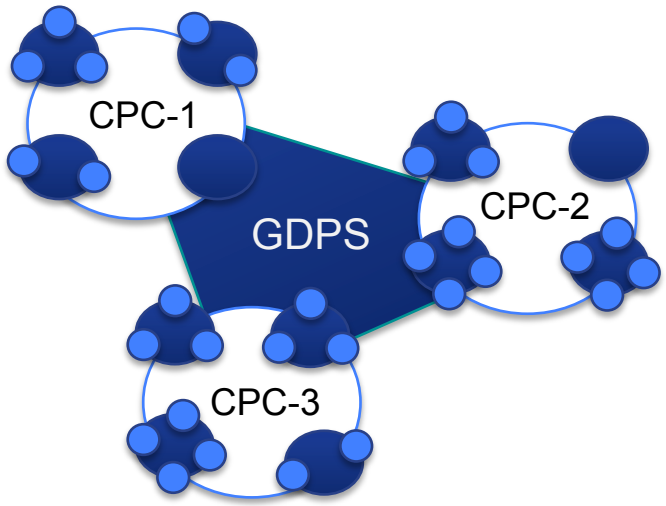
# Our Mission

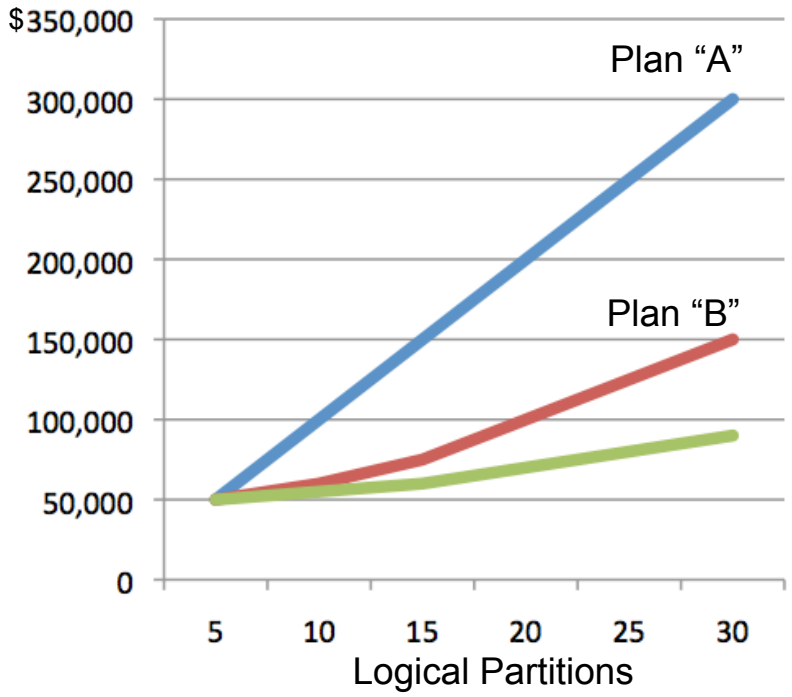



[1] zJournal – zEnterprise Survey – April - May, 2011 – 183 Respondents

# Our Mission

*Total Cost of Integrity (TCA&C) – Cost Strategies*




Glenn Anderson – MVS Program Keynote – Transition IT from a Cost Center to a Value Center.

# Our Mission

*Total Cost of Integrity (TCA&C) – Problem Recognition/*Remediation

| History | Real-time | Future |
|---|---|---|
| ❑ Data Collection<br>❑ Event Filtering<br>❑ Post-Processing<br>❑ Reporting | ❑ Data Collection<br>❑ Discrimination<br>❑ Recognition<br>❑ Notification | ❑ Data Collection<br>❑ Predictive Analytics<br>❑ Recognition<br>❑ Notification |
| Passive | Reactive | Proactive |

Times Arrow

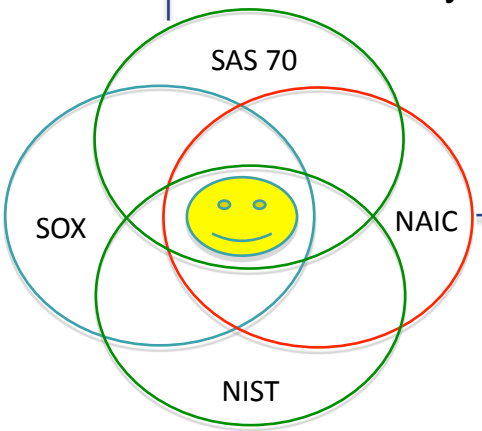
# Our Mission

*System Compliance Model – What is Compliance?*

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

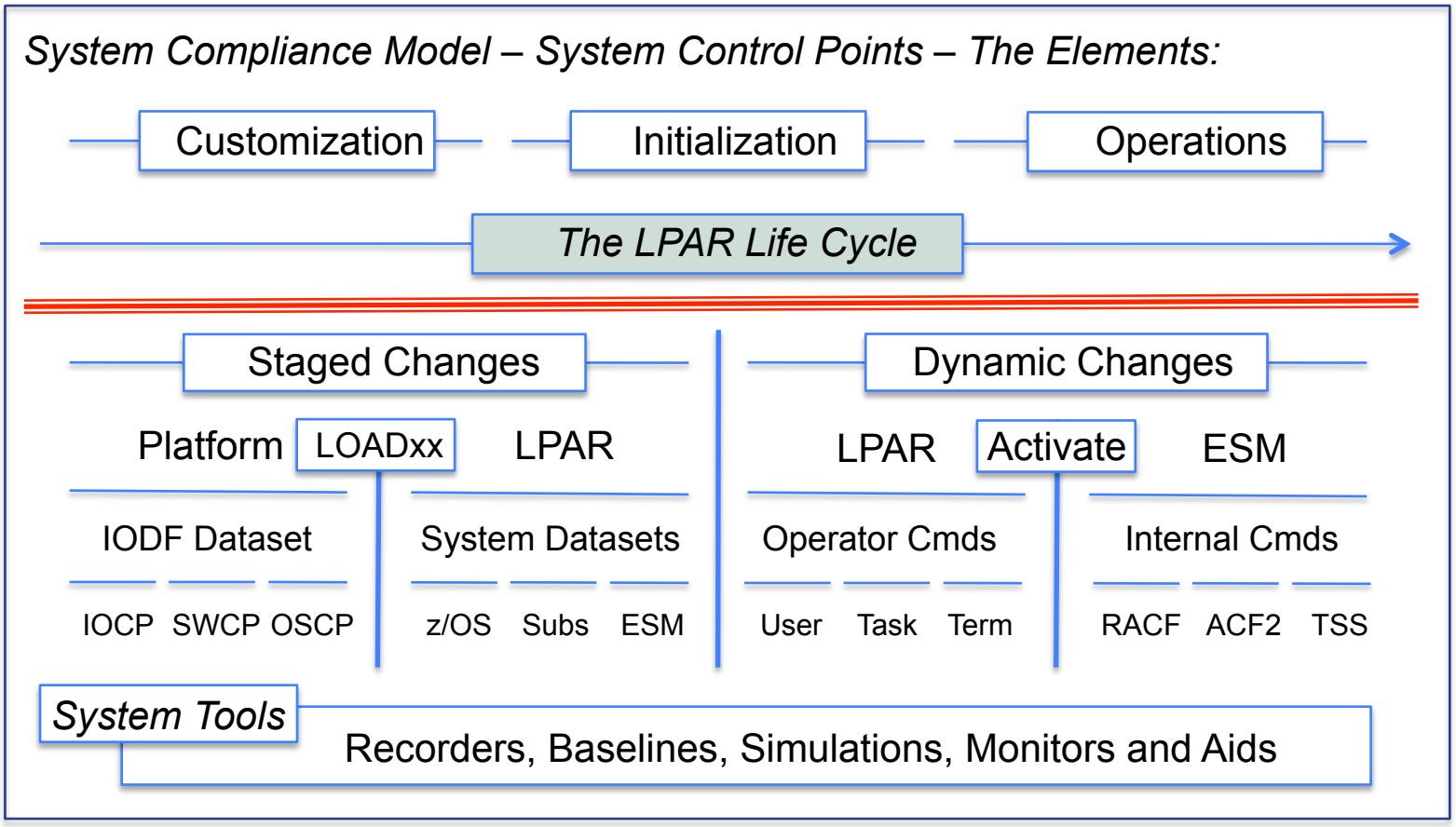
✓ Compliance - describes the goal that corporations or public agencies aspire to in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations.

✓ 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.

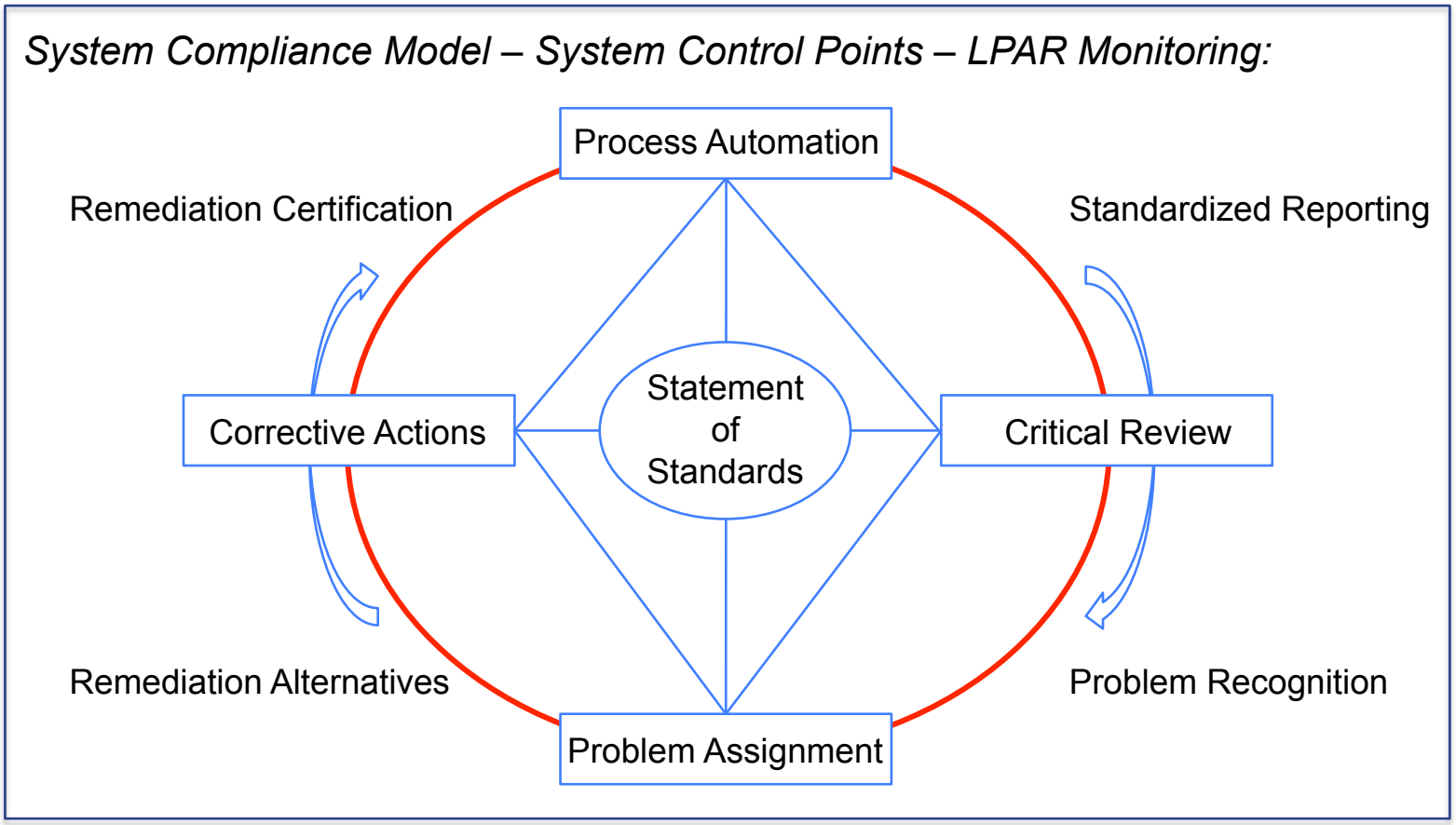



- Common Sense
- Best Practice
- Personal Preference
- Internal Policy
- Industrial
- Governmental

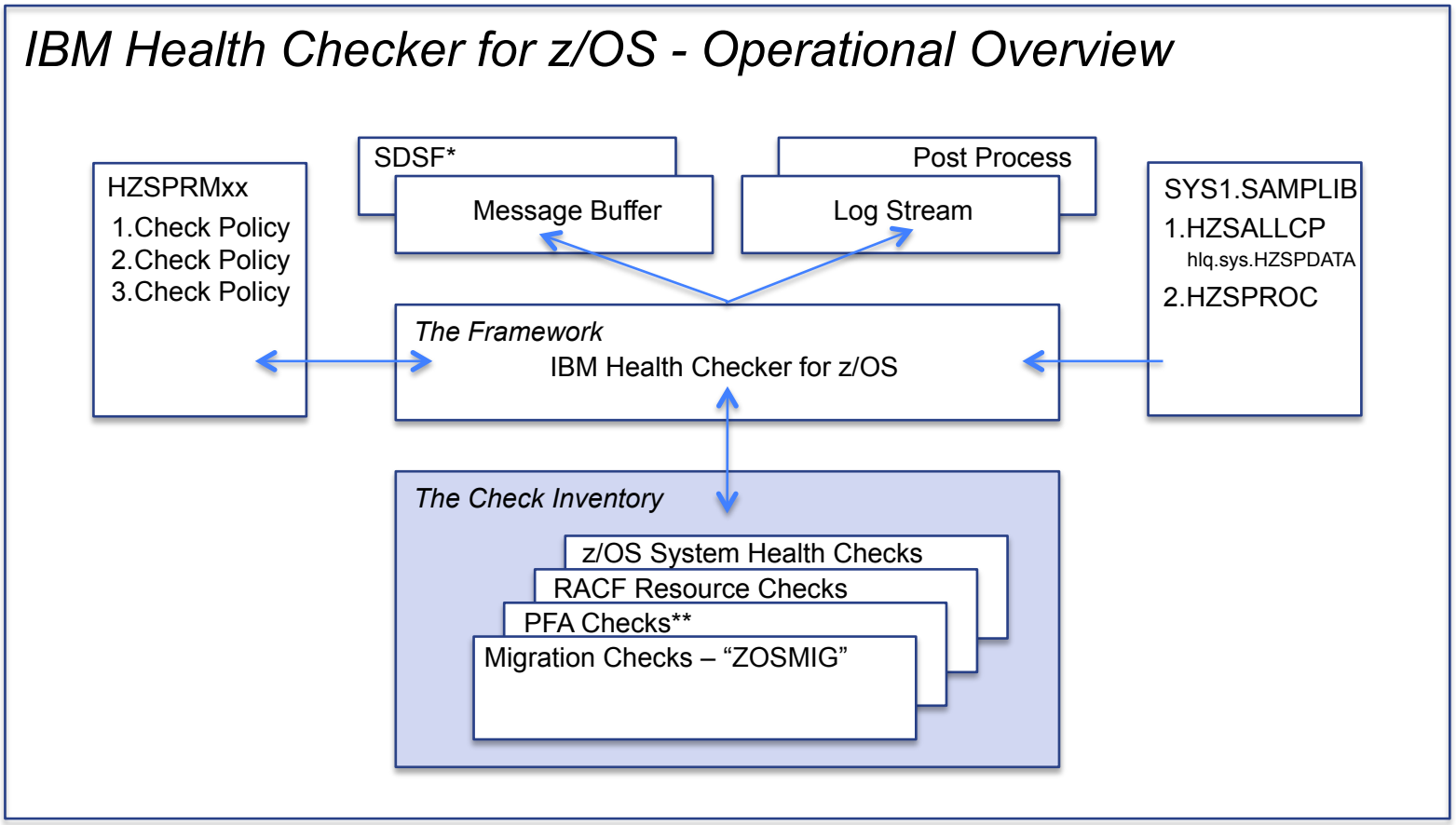
# Our Mission


System Compliance Model – System Control Points – The Elements:
Customization
Initialization
Operations
The LPAR Life Cycle
Staged Changes
Dynamic Changes
Platform
LOADxx
LPAR
LPAR
Activate
ESM
IODF Dataset
System Datasets
Operator Cmds
Internal Cmds
IOCP SWCP OSCP
z/OS Subs ESM
User Task Term
RACF ACF2 TSS
System Tools
Recorders, Baselines, Simulations, Monitors and Aids

# Our Mission

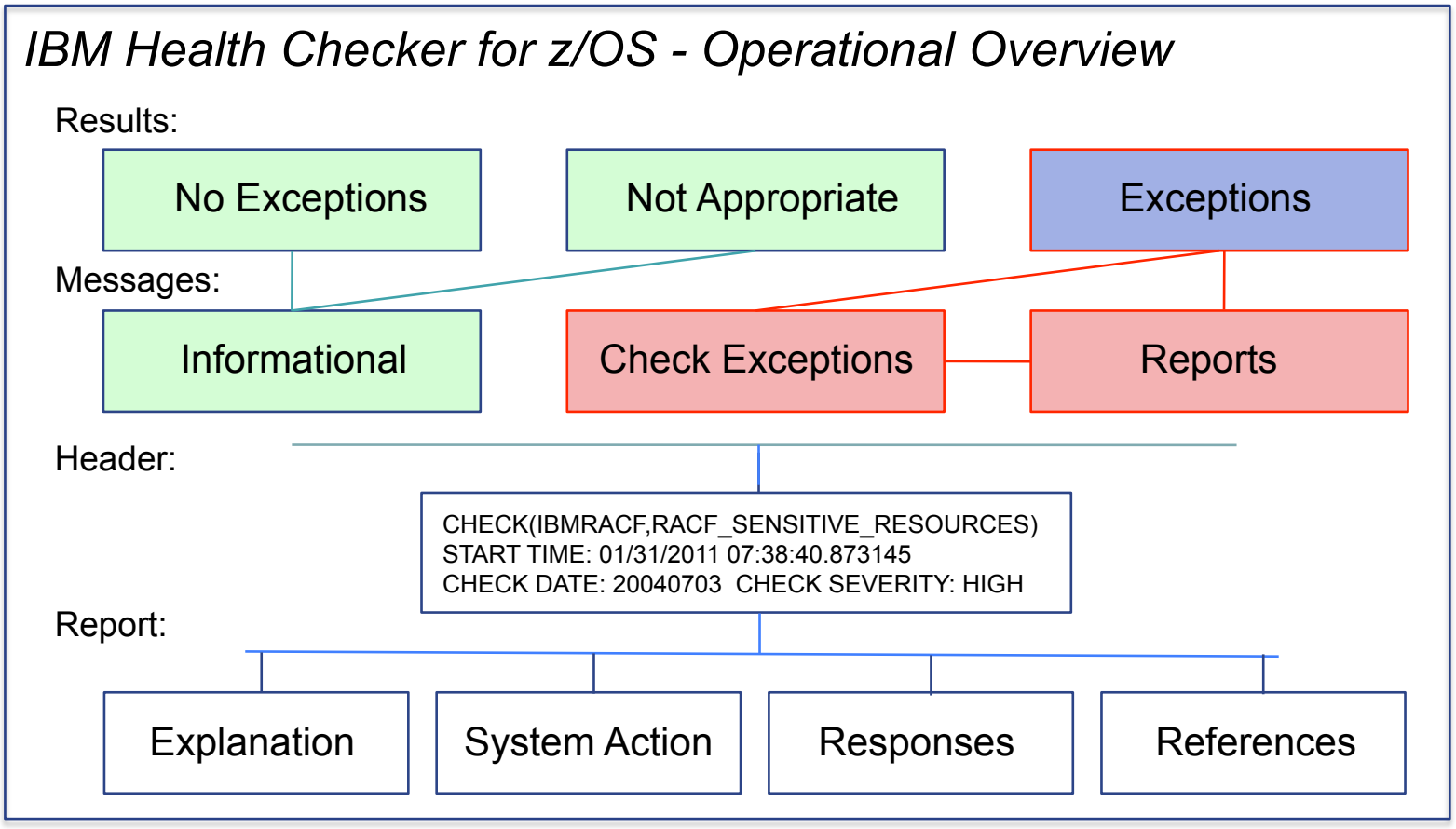

System Compliance Model – System Control Points – LPAR Monitoring:
Process Automation
Remediation Certification
Standardized Reporting
Corrective Actions
Statement of Standards
Critical Review
Remediation Alternatives
Problem Recognition
Problem Assignment

# Ten "*BIG TIME*" Gotchas!




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

# Ten "*BIG TIME*" Gotchas!



# Ten "*BIG TIME*" Gotchas!

*RACF_SENSITIVE_RESOURCE*

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

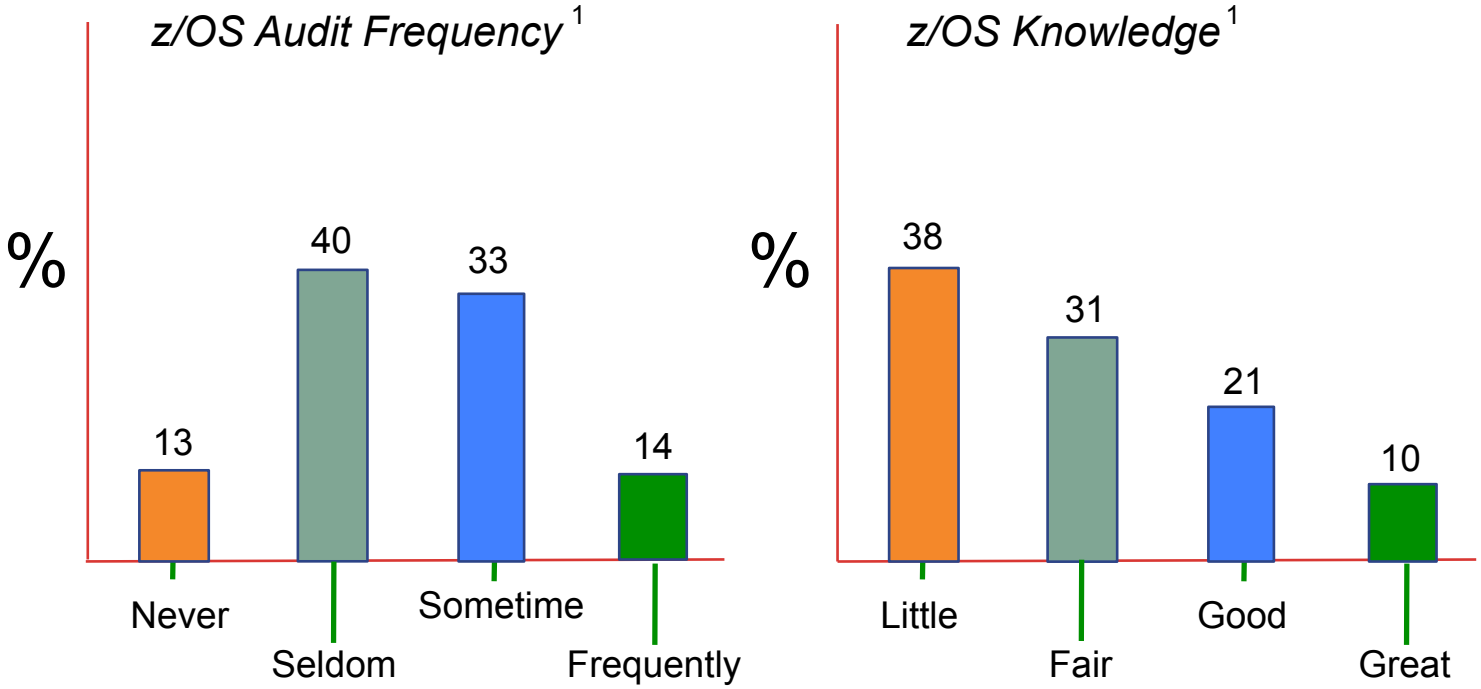
System Action: The check continues processing. There is no effect on the system.

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.

# Ten "*BIG TIME*" Gotchas!

*Who are these Guys? Active Enough, Smart Enough!*



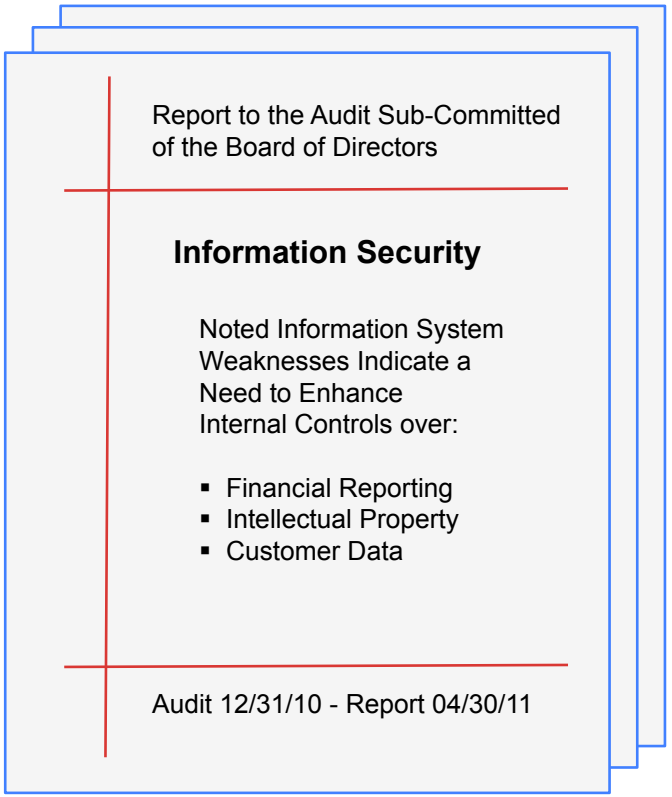

[1] zJournal – zEnterprise Survey – April - May, 2011 – 183 Respondents

# Ten "*BIG TIME*" Gotchas!

## *What Bad News Look Like!*

"...Although progress has been made in correcting previously reported Information Security weaknesses, system control material weaknesses[1] continue to jeopardize the confidentiality, integrity and availability of those formal processes intended to safeguard access to financial, intellectual property and customer data.."

[1] "…A material weakness is a deficiency, or a combination of deficiencies, in internal controls such that there is a reasonable possibility that material misstatement may result…"



# Ten "*BIG TIME*" Gotchas!

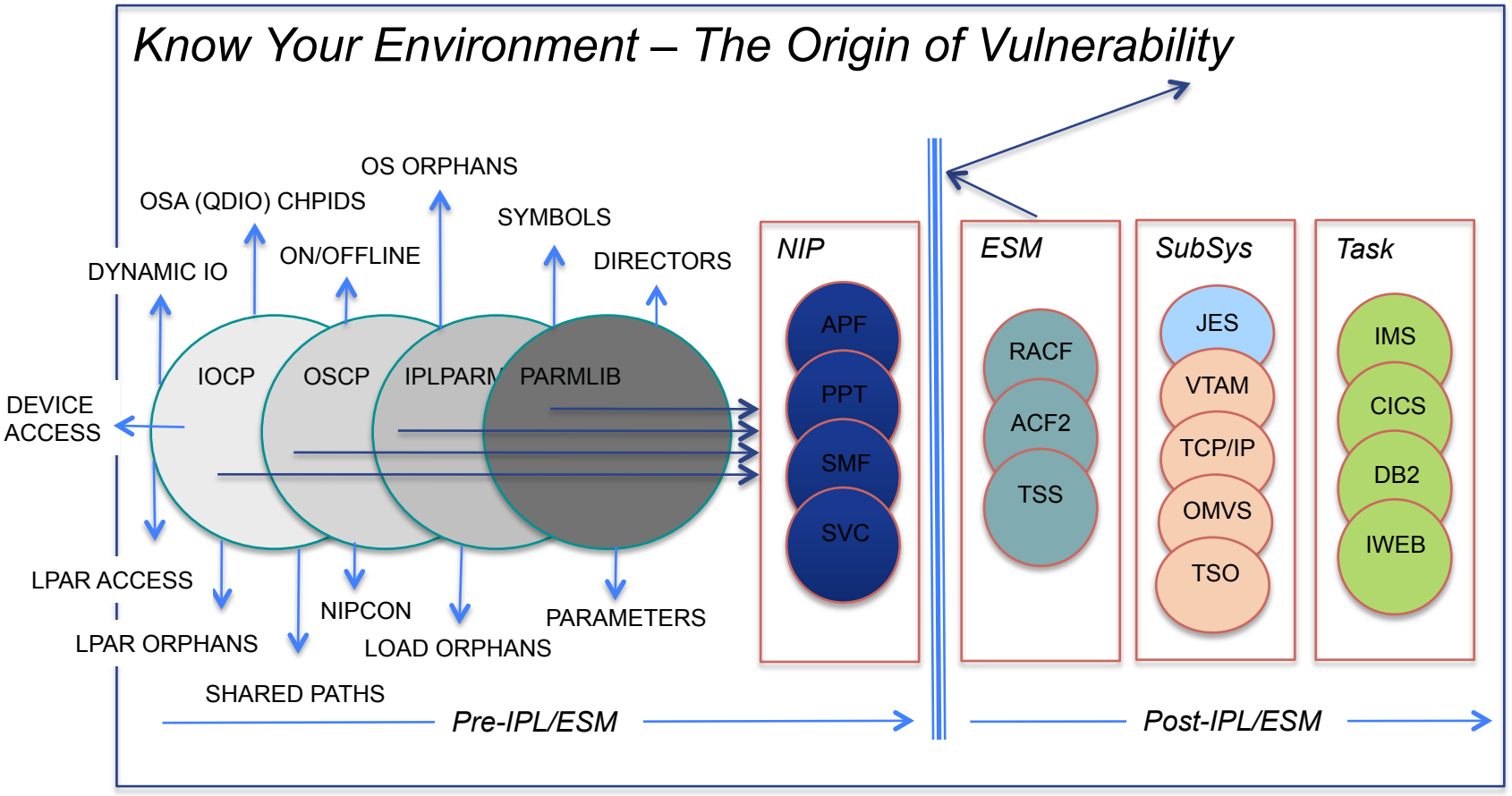
*How to avoid Embarrassing zEnterprise Audit Findings?*

## *Get Ready, Be Prepared!*

Session 10107 - How to Monitor & Assure Your System z Security Status
Presenter - Simon Dodge - Wells Fargo

Session 09221 - Compliance: How to Manage (Lame) Audit Recommendations
Presenter - Brian Cummings – Tata Consultancy Services

# A Look Before and After Initialization



# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List – Post-IPL/ESM*

- ☑ Is the IODF a recognized zEnterprise Control Boundary?
- ☑ Is Shared DASD protected by Shared ESM Rule Sets?
- ☑ Are SMF Log review procedures in place and in use?
- ☑ Do CICS Regions have unique Userids?
- ☑ Are any ESM Dataset Profiles Invalid and/or Missing?
- ☑ Are Access Exception Lists Accurate, Up-to-Date?
- ☑ Do Conflicting Goals result in "No Security"?
- ☑ Are System Vulnerability, Possible Exploits Acknowledged?
- ☑ Are New Compliance Requirements Understood, Implemented?
- ☑ Are Exposures to new Threats Understood, Defended Against?

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 1 of 10*

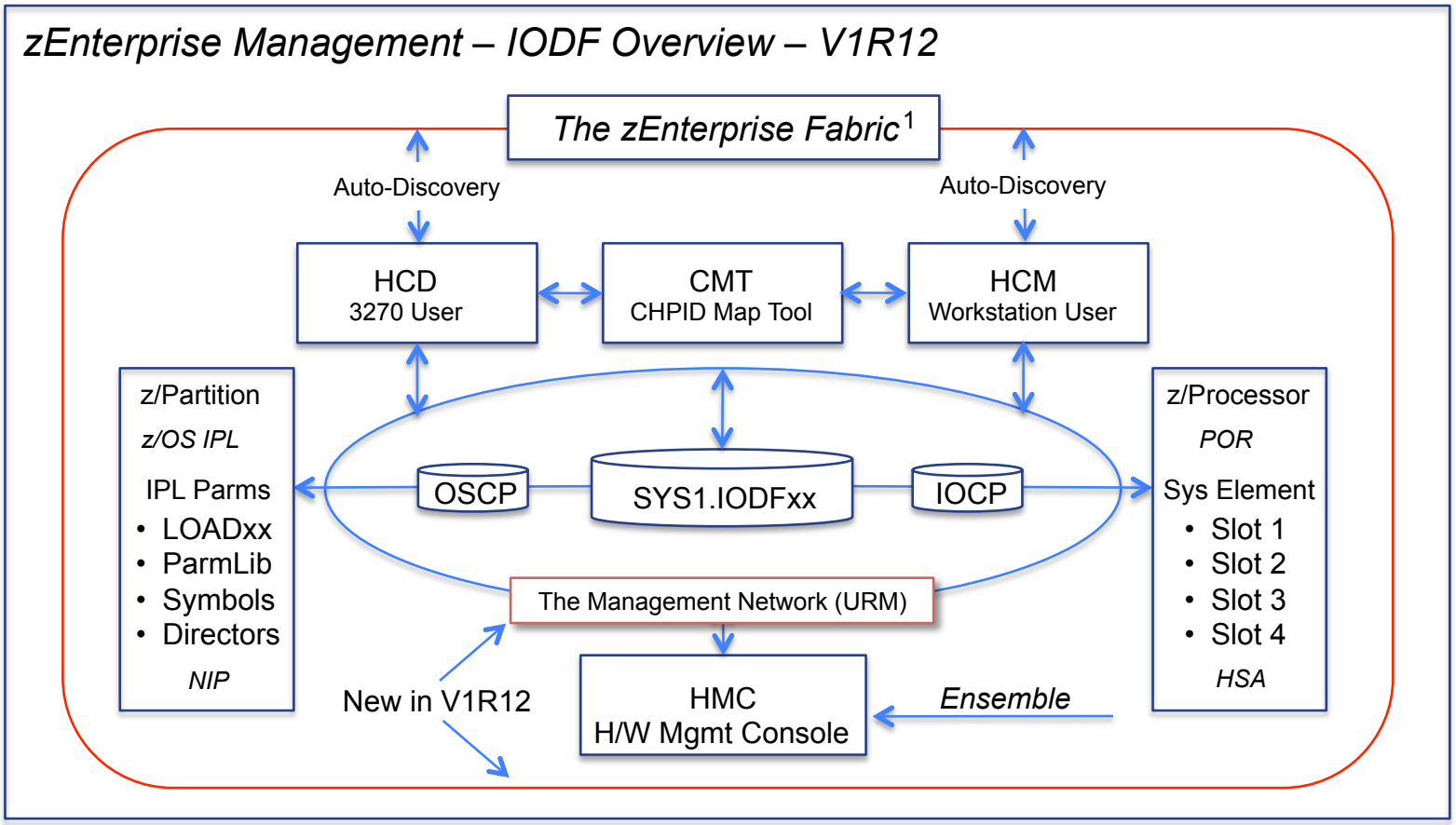
## ☑ Is IODF a Recognized Control Boundary?

It has been noted recently that mismanagement of the IODF Dataset may lead to the very risky sharing of devices with completely different security requirements.

Unfortunately many installations will not acknowledge using the IODF as a boundary control and are now being blistered for their stance and being pressured to view this scenario differently.

An example would be that time when the hardware staff accidentally connected an entire bank of Production DASD to a newly authorized Test LPAR via cloning and in doing so forgot to update the LPAR and DEVICE Candidate List to limit CROSS-LPAR access.

# IODF - the Absolute zControl Point!




[1] The zEnterprise Fabric extends to the edge of the available zInformation System Data Horizon.

# IODF - the Absolute zControl Point!

*zEnterprise Management – IODF Best Practices!*

- ☑ Establish Limits:
  - Access to HCD/HCM
  - NONE/READ/UPDATE Authority to SYS1.IODFxx
  - Access to the Hardware Management Console (HCM)
  - Access to the System Element (SE)
  - Access to the Management Network (URM)
  - Access to LOADxx Members – SYSn.IPLPARM
  - Access to System Parameters – SYS1.PARMLIB
  - Access to NIPS and System Consoles
  - Require “Activity Logging” ON
- ☑ Document and Periodically Review Initialization Process:
  - Power On Reset (POR)
  - Initial z/OS Program Load (IPL)
  - Disaster Recovery/Business Continuity

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 2 of 10*

## ☑ If Shared DASD, Shared ESM Rules?

Shared DASD with two different ESM Rule Sets – if you have multiple LPARs, each with their own ESM Databases and Rule Sets that are sharing sensitive data, the possibility exists that a difference in Access Rules between LPARs will inadvertently open access to everyone on one or the other LPAR. An unintended consequence!

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 3 of 10*

## ☑ SMF Log Review in place and in use?

Large amounts of security logging messages in SMF (tens of thousands per day) caused by access via OPERATIONS (RACF) or NON-CNCL (ACF2), but nobody bothered to look at them.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 4 of 10*

## ☑ Do CICS Regions have unique ID's?

CICS UserId not defined for each CICS Region – The UserId gets a bind to a Region. If there is a region that is permitted to do sensitive transactions, CICS may allow anyone in by using its Default UserId without asking for a RACF UserId and Password.

These are considered the *minimum* Transaction Security elements.

- ❑ System Initialization Table (SIT), i.e. XTRAN=YES|T/Gclass|NO
- ❑ The CICS System Definition File (CSD), i.e. RESSEC(YES)
- ❑ The CICS ESM Class Profiles, i.e. TCICSTRN and GCICSTRN

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 5 of 10*

## ☑ Are ESM Dataset Profiles Invalid/Missing?

- Failure to adequately protect these authorized system datasets libraries will compromise all system applications, all system data and the z/OS system itself. System Datasets Include:
  - APF Libs
  - Linklist Libs
  - RACF Database
  - Parmlib Datasets
  - IPLPARM Datasets
  - IODF Datasets
- A System integrity failure of this nature undermines all business and application controls. In certain cases it renders them worthless.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 6 of 10*

## ☑ Are Exception Lists Accurate, Up-to-Date?

A key component of nearly every regulatory initiative that addresses protection of data is a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user's business function or need to know.

To assure the correct level of access control over different user classes, "Exception Lists" are often used. When these lists are poorly maintained, exposures result and generally more data or resource access is given than is required by an individual or task.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 7 of 10*

## ☑ Do conflicting goals result in "No Security"?

- Switching on classes with a "**" profile (with UACC(READ)) to satisfy an audit requirement has the same impact as switching off security; e.g. OPERCMDS is commonly used this way.
- Not properly implementing new z/OS functions that support the ESM and later finding that, for example, the audit data is no longer protected. Implement SMF Log Streams (as documented so you don't lose audit SMF records at start up).
- Third party products being secured using "internal security" leaves security admin in the hands of the team that installed the product, not the security specialists.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 8 of 10*

## ☑ Are System Vulnerabilities Acknowledged?

- A vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Its three elements are:
  1) Knowledge of a system susceptibility or flaw.
  2) Access to the flaw by an attacker.
  3) Capability to exploit the flaw.
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.[1]
- Example: Program uses MODESET to obtain APF authorization then dynamically elevates security credentials, regardless of the ESM.

[1] From Wikipedia - Vulnerability (computing)

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 9 of 10*

## ☑ Exposures from New Technology?

- LPAR to LPAR communication using QDIO sends IP packets between LPARs sharing an OSA adapter based on the next-hop address in the IP packet header. If the next-hop address has been registered by another IP stack supported by the same OSA adapter (recorded in the OAT), the packet is sent directly from one IP stack to another – the traffic never travels across LANs external to the z/System.
- When these and other conditions exist (which are accepted performance tuning strategies) – the z/System will route IP packets between networks that are not otherwise connected (bypassing firewalls).

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Post-IPL/ESM – 10 of 10*

## ☑ Understanding New Requirements?

- The Defense Information Systems Agency (DISA) has issued a new set of security guidelines. The "Database Security Technical Implementation Guide (STIG)" presents known security configuration items, vulnerabilities, and issues required to be addressed by DOD policy.
- The STIG is provided under the authority of DOD, a requirement that "all information assurance (IA) and IA-enabled IT products incorporated into DOD IS shall be configured in accordance with DOD security configuration guidelines". Implementing the recommendations outlined in the DISA STIG will ensure DOD environments to meet these security requirements and comply with this mandate.

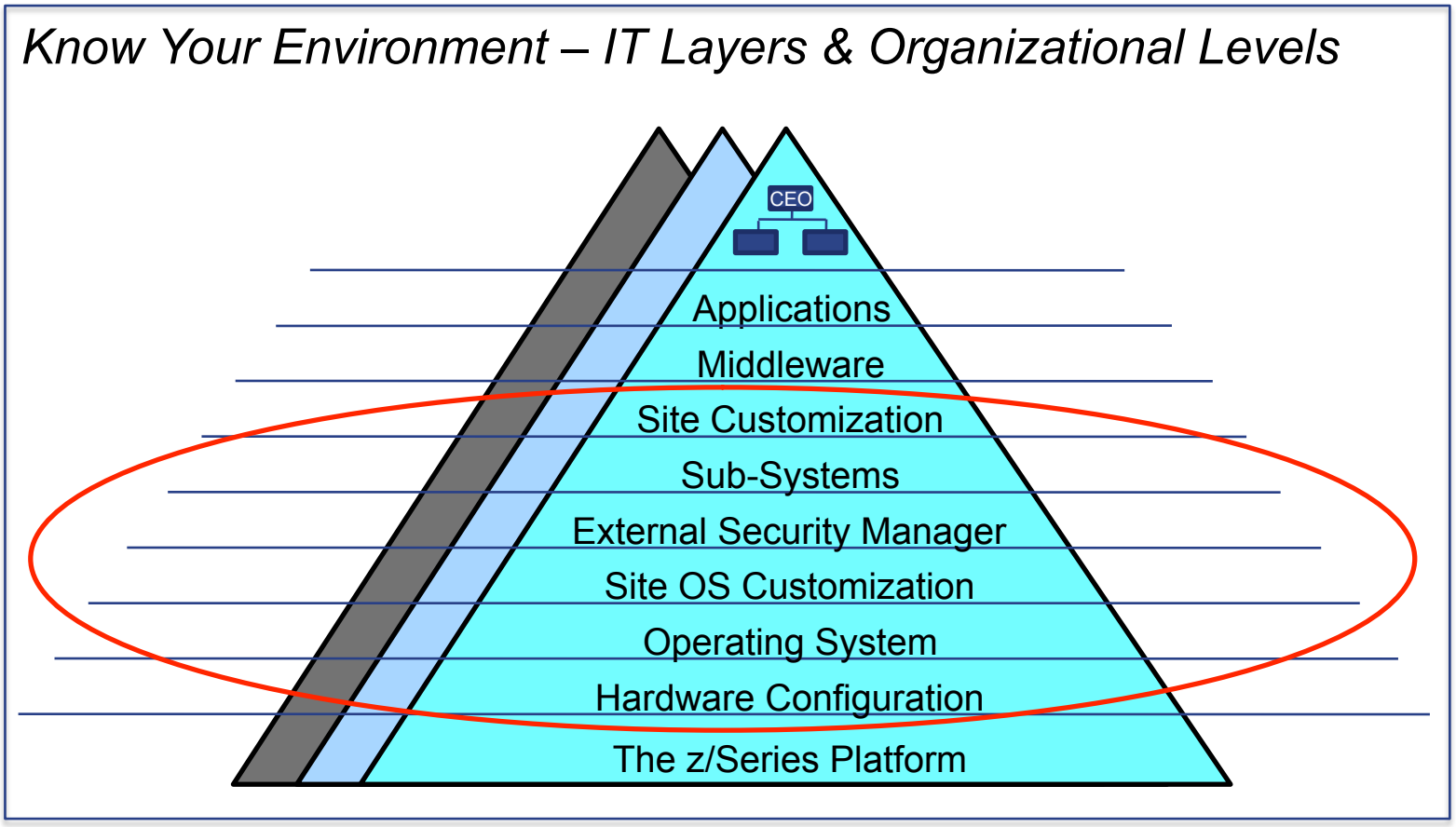
# Ten "*BIG TIME*" Gotchas!

*Know Your Environment – Macro Vs. Micro World View*


*The Whole*

*The Parts*

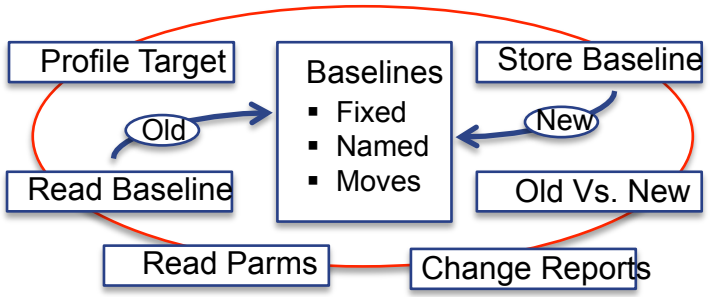
# Ten "*BIG TIME*" Gotchas!



# Ten "*BIG TIME*" Gotchas!

## *Know Your Environment – Baseline the Parts for Little or Nothing!*

### ☑ *The Change Detection Process*




### ☑ *Baseline Types*

- Moving - Update at each Interval
- Fixed - Update with first Interval
- Named - A Specific Named Dataset

### ☑ *Notification*

- On Change Only - YES|NO
- Defined Email Subject
- Defined Recipients List
- Unique for each Detector

### ☑ *The Cycle and Intervals*

Daily — Time of Day + Interval of 1|2|4|6|8|12

Weekly — Time of Day + Interval of MON&|TUE&|WED&|THR&|FRI&|SAT&|SUN

Monthly — Time of Day + Interval of Day in Month 1&|2&|10&|20&|30 or BOM&|EOM

# Ten "*BIG TIME*" Gotchas!

*Know Your Environment – Baseline the Parts – "FREE" Extractors*

| Domain | Extractor | Source |
|---|---|---|
| DB2 Parms | SDSNLOAD(DSNTXAZP) | IBM |
| RACF Policy | DSMON/SETROPTS | IBM |
| ACF2 Policy | ACF2SHOW/ACFRPTSL | CA |
| CSDS Parms | SDFHLOAD(DFHCSDUP) | IBM |
| IODF Dataset | SYS1.LINKLIB(CBDMGHCP) | IBM |
| VOLUME | VOLIST | PUBLIC |
| System SVCs | SVCLOOK | PUBLIC |
| IPL – Date/Time | Rexx | Just Ask |

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM*

- ☑ Is there a Disaster Recovery Plan?
- ☑ Is the ESM secured?
- ☑ Are ESM Defaults still functional?
- ☑ Is the Provisioning System Functional?
- ☑ Are Start-Up Configurations Assured?
- ☑ Is the SMF Logging Configuration Controlled?
- ☑ Are Program Properties Under Control?
- ☑ Are Operator Commands Restricted?
- ☑ Are NIP Consoles Locked Down?
- ☑ Have the ESM Control Boundaries been Identified?

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 1 of 10*

## ☑ Is there a Disaster Recovery Plan?

Without a *TESTED* Disaster Recovery Plan no assurance can be given that the enterprise could, in the even of a disaster, recover as a going concern. Such a finding would directly impact the opinion rendered on the organization's overall financial position.

- How often is the plan updated/revised and then tested?
- How is test data controlled before and after a test?
- Any Walruses in the Gulf?

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 2 of 10*

## ☑ Is the ESM secured?

The External Security Manager (ESM) is an add-on product which provides the basic security framework managed by Security and Risk Officers on the z/OS Platform. Their chief concerns are:

- Who has access to ESM Datasets and Tools? Fewer is better!
- What is the ESM Dataset Profile? UACC "NONE" is better!
- When does the ESM become functional? Sooner is better!
- How are users identified, authenticated and authorized?
- What Classes are Active? Which are Audited? Which are logged?
- How are "Security Events" reported/reviewed/resolved?

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 3 of 10*

## ☑ Are ESM Defaults still functional?

The installation and maintenance of an External Security Manager is the work of a system professional. In doing their important work they follow vendor-specific instructions implementing installation-specific ESM Parameters and Settings.

- Userids needed for ease of installation or migration should be reviewed or removed.
- RACF is distributed granting unlimited rights to IBMUSER. This ID should be REVOKED as soon as possible.
- ACF2's MODE may be set to ALLOW/WARN but should be ABORT.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 4 of 10*

## ☑ Is the Provisioning System Functional?

How are these Control Lists synchronized? What about Bill?

| Employee Roster: | Users/Groups: | Classes/Resources: |
|---|---|---|
| 1. Jerry | 1. Jerry | 1. Jerry |
| 2. Mary | 2. Mary | 2. Mary |
| 3. Sara | 3. Sara | 3. Sara |
| 4. Jim | 4. Bill | 4. Bill |
| 5. Gordon | 5. Gordon | 5. Gordon |
| 6. Bob | 6. Bob | 6. Bob |
| 7. Craig | 7. Craig | 7. Craig |
| 8. Martin | 8. Martin | 8. Martin |

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 5 of 10*

## ☑ Are Start-Up Configurations Assured?

- OPI=YES|N0

If the value is set to 'YES' an operator so prompted may, using Operator Commands, override established IPL values and/or establish new ones. If the value is set to "NO" in the IEASYS00 Member, the operator is not allowed to change values even if another prevailing IEASYS Member attempts to set the value to 'YES".

- WARNUND

Starting in z/OS V1R13 (Rolled back to z/OS V1R11) this IEASYSxx Keyword will suppress operator prompting when an invalid or undefined statement is encountered, instead issuing message IEA660I. Processing IEASYSxx continues uninterrupted.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 6 of 10*

## ☑ Are Operator Commands Restricted?

ParmLib is a predefined collection of z/OS Datasets that contains IBM supplied defaults and site-specific configuration members. Generally, Site specific configurations will prevail over IBM defaults when the system is IPL'ed resulting in a unique z/OS configuration, your very own customized instance of z/OS. But a running configuration may be altered at any time using Operator and Product specific commands.

- SETLOAD may be used to update ParmLib Concatenation.
- SET PROG may alter APF Authorization.
- SETSMF may alter SMF record keeping.

The use of such configuration update commands greatly increases the complexity of maintaining accurate configuration documentation.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 7 of 10*

## ☑ Is SMF Logging Configuration Controlled?

- ACTIVE|NOACTIVE

Defined in the SMFPRM ParmLib Member, the System Management Facility (SMF) controls the interval and record set(s) used by the External Security Managers (ESM) for logging security events.

ACTIVE indicates that SMF logging will be available for logging events as defined in both SMFPRM and the ESM. NOACTIVE indicates that logging is turned off regardless of ESM settings.

SMFPRM may be SET dynamically at any time.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 8 of 10*

## ☑ Are Program Properties Controlled?

Defined in the SCHED ParmLib Member and in the IBM supplied module IEASDPPT, the Program Properties Table (PPT) may determine the final word on whether the use of a named module (program) in an authorized library will or won't be subjected to ESM (RACF, ACF2, TSS) protection.

PASS, the default, indicates that security is in effect, while NOPASS is used to indicate that security protection is not required.

Specific rules affect the protection of JOBLIB and STEPLIB datasets.

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 9 of 10*

## ☑ Are NIP Consoles Locked Down?

The Nucleus Initialization Procedure (NIP) *"BOOTS"* z/OS. During the process, control of the system resides in a special class of Console called a NIP Console. NIP Consoles are defined to z/OS from within the OSCP component found in the IODF Dataset.

Example: `NIPCON DEVNUM=(1040,1140,1020,1120)`

So four NIP Consoles may or may not be active. Only one may be needed. Each z/OS LPAR may be IPL'ed having a unique OSCP. Each OSCP may have it's own unique NIPCON Parm.

Avoid chaining surprises!

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List - Pre-IPL/ESM – 10 of 10*

## ☑ Are the ESM Control Boundaries Identified?

If you have "READ/UPDATE" access to a Dataset, you can UPDATE and SUBMIT any JCL that it might contain. If you attempt to SAVE the update, the EMS will deny it unless you have "UPDATE" authority. If "READ" only just "CANCEL" out the update and no record of the change will be recorded. The System Log will record the SUBMIT.

```
EDIT       IFO.IFOP.CICSTEST.SYSBLACK(CICSJCL) - 01.00     Columns 00001 00072
Command ===> SUBMIT                                          Scroll ===> PAGE
****** ***************************** Top of Data ******************************
000001 //CICSI2PR PROC REG=0M,   REGION SIZE (0M AVOIDS DOS)TCE
000002 // INDEX1='CICSTS32',
000003 // INDEX2='CICSTS32.CICS',
000004 // REGNAM1='I2PR',    REGION NAME FOR MRO
```

# Ten "*BIG TIME*" Gotchas!

*The Top Ten Check List – No Save Haven – The Last Word!*

- ☑ When possible abandon manual processes for automation.
- ☑ Adopt a System Compliance Model, get buy in from others.
- ☑ Establish Specific, Attainable Control Boundaries and Standards.
- ☑ When they don't know, teach them. You just might learn something.
- ☑ Give equal weight to Pre and Post IPL/ESM integrity concerns.
- ☑ Develop culture that attempts to balance compliance and its cost.
- ☑ Remember Compliance must not only "Exist"; it must be "Demonstrable".
- ☑ The ESM alone cannot provide sufficient z/OS compliance.
- ☑ Exercise care when interpreting Audit Findings, limit skepticism. ←
- ☑ Strive to create a Trusted Computing Base on your own terms. ←

# Ten "*BIG TIME*" Gotchas!

*How to avoid Embarrassing zEnterprise Audit Findings?*

## *Get Ready, Be Prepared!*

Session 10107 - How to Monitor & Assure Your System z Security Status
Presenter - Simon Dodge - Wells Fargo

Session 09221 - Compliance: How to Manage (Lame) Audit Recommendations
Presenter - Brian Cummings – Tata Consultancy Services

# Ten "*BIG TIME*" Gotchas!

*Let's Turn to the Experts for Help!*

- Barry Schrager - President, XBridge Systems and Author of CA-ACF2
- Julie-Ann Williams - Sr. Technical Consultant , Millennia Systems Ltd, UK
- Stu Henderson - President, The Henderson Group
- Mark Wilson - Technical Director, RSM Partners Ltd, UK
- Martin Underwood - Lead Consultant , Millennia Systems Ltd, UK.
- David Hayes - Auditor Supervisor, U.S. Government Accountability Office
- Brian Cummings - Managing Partner, TATA Consulting Services

# Outline – Where We're Going!

1. Our Mission - (1/4)
   - ✓ What is Compliance?
   - ✓ The Need for Shared Values
   - ✓ Critical Success Factors
   - ✓ System Control Points
   - ✓ Organizational Acceptance
   - ✓ Cost of Implementation
   - ✓ Health Checker Overview
   - ✓ Integrity Checks in Action
2. Let's ask the Industry Experts! – (3/4)
   - ✓ Are They Active Enough, Smart Enough?
   - ✓ What does Bad News Look Like?
   - ✓ Who are these Guys?
   - ✓ Distinguish Pre-IPL/ESM from Post-IPL/ESM
   - ✓ Pre-IPL/ESM Details and Recommendations
   - ✓ Post-IPL/ESM Details and Recommendations
   - ✓ Safe Haven Guidelines.
3. Health Checker - Hands-on Lab – *Recommended*

   Session 10601 and Session 10876 or send email to support@newera.com - Send Lab
4. Resources, References and Sessions - *Recommended*
   - ✓ z/Auditing Essentials - Volume 1 - zEnterprise Hardware - An Introduction for Auditors
   - ✓ How Barry Schrager Changed Your World – Believe it!

   Both Edited By Julie-Ann Williams - julie@sysprog.co.uk

# Ten "*BIG TIME*" Gotchas!

*Publications:*

- IBM Health Checker for z/OS Users Guide – SA22-7994-11
- MVS Initialization and Tuning Reference – SA22-7592-21
- MVS System Command Reference – SA22-7627-24
- MVS Planning Operations – SA22-7601-12
- 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

# IODF - the Absolute zControl Point!

*IBM Health Checker for z/OS – Getting Started*

- Hands-on Lab - Abstract:

  Getting the IBM Health Checker up and running and customizing the Health Checks for your z/OS systems is easy to do. This self-directed lab will lead you through the process step by step. The lab is intended for those with little or no experience with the Health Checker. Attendees should have knowledge of TSO and JCL.

- Your Instructor:

  Mr. Gordon Daniel, Director of Development
  NewEra Software, Inc.
  gordon@newera.com

- Requesting the Lab:

  Send Email to – support@newera.com
  Subject – Send HC Lab

# IODF - the Absolute zControl Point!

*The Very Latest in Self-Help:*

- ☑ z/Auditing Essentials - Volume 1
  zEnterprise Hardware - An Introduction for Auditors
  Edited By Julie-Ann Williams - julie@sysprog.co.uk

- ☑ Authors:
  - Julie-Ann Williams
  - Craig Warren
  - Martin Underwood
  - Steve Tresadern

- ☑ The Beginning of Data Security - As We Know it Today
  *How Barry Schrager Changed Your World*
  - www.share-sec.com

# That's it folks, all done!

*Session Evaluation* - Session Number - 10470

Paul R. Robichaux
NewEra Software, Inc.
prr@newera.com

- Requesting StepOne:
  Send Email to – support@newera.com
  Subject – Send StepOne
- Requesting HC Lab:
  Send Email to – support@newera.com
  Subject – Send HC Lab
- Requesting White Paper:
  Send Email to – support@newera.com
  Subject – Send White Paper


Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project