What to Expect from an Enterprise-Wide Mainframe Security Audit

David Hayes
Government Accountability Office
Stu Henderson
The Henderson Group

ABSTRACT

- When Your Auditors Are Experienced System Programmers, You Might Wonder What to Expect

- In This Session, David and Stu Show You Three Levels of Mainframe Audit, and What to Expect for Each

WHY HAVE AUDITS ANYHOW?

Auditors by definition, evaluate the adequacy of controls for some purpose. Controls are mechanisms to support an organization's objectives such as:

- Reliable financial and performance reporting (and decision making)
- Compliance with laws and regulations
- Protection of assets (including information)

WHY HAVE IT AUDITS ANYHOW?

- **Information system audits provide support for auditors addressing the issues just described**

- **An information system control is not significant unless it relates to the support of some accepted control objective. This filter can help you to brush aside audit findings that are not relevant.**

- **Understanding the audit's objectives (which should drive the scope of the review) and how one audit relates to the other audits will help you to get more out of the audit - with less hassle.**

AUDIT OBJECTIVES

- **Information systems controls are usually a component of the internal control environment for business processes subject to audit.**

- **Information needed about computer-supported internal controls often involve applications.**

- **Information systems auditors need to develop adequate understandings of *BOTH* the business processes and the supporting information systems in order to assess risk and determine the appropriate scope of systems review needed.**

AGENDA

- Introduction
- Phase 1, Understanding the Image-Level Controls (Single MVS Image)
- Phase 2, Stretching Cross-Image
- Phase 3, Stretching to the Web (and APPN)
- Summary and Call to Action

Introduction / Situation

- Today's z/OS systems are not isolated. They share with other images, often in other data centers. They share with other platforms over multiple networks.

- This adds sophistication to control configurations, increases the probability of undetected risks, and makes audits more interesting (and strains the capacity of many auditors).

Introduction / Today's Emphasis

- A z/OS audit approach inclusive of relevant systems and control environments
- Expectations for the data center
- A description of the data and information auditors will need
- Preparing for a sophisticated audit
- How data centers can obtain useful results from audits

Introduction

- **z/OS Controls Have Three Major Components:**
  - **OS Security (Control Over Supervisor State…)**
  - **Security Software (RACF, ACF2, or TopSecret)**
  - **Connection Security, Which Involves Networks, Shared Devices, and Sysplexes**

Introduction

- Until Recently, a z/OS Controls Audit Might Look at OS Security and the Security Software.

- With the Advances in Technology and Connectedness, This is No Longer Adequate

Introduction

- We’ll Show You a More Comprehensive Approach in Three Phases:

1. The Typical Audit Territory You’re Familiar With Already – With a More Comprehensive Scope That Recognizes Current Technologies and System Operations
2. Connections Involving Other Images
3. Connections Stretching to the Internet and to APPN

Phase 1, Basic Image-Level Controls

- **To Evaluate Controls on Just One Image, Auditors Will Likely Ask for (Using RACF as an Example):**
  - **SETR LIST, DSMON**
  - **Dataset Rules for System Datasets**
  - **Resource Rules for: DASDVOL, FACILITY, JESSPOOL…**
  - **Policy, Procedure, Evidence of Review of SMF Reports**

Phase 1, Basic Image-Level Controls

- Control File for Tape Management Software
- PARMLIBs & Automated Console Ops
- PROCLIB Concatenation – inventory of PROCs
- Change Control Procedures – including dynamic OS configurations
- Critical Production Dataset Identification & Controls
- Software Products & Control Mechanisms
- Identification of JCL and Batch Environment / Scheduler Controls
- Security Software Policy, Standards, Procedures
- Sniffer Program or LAN Security Study

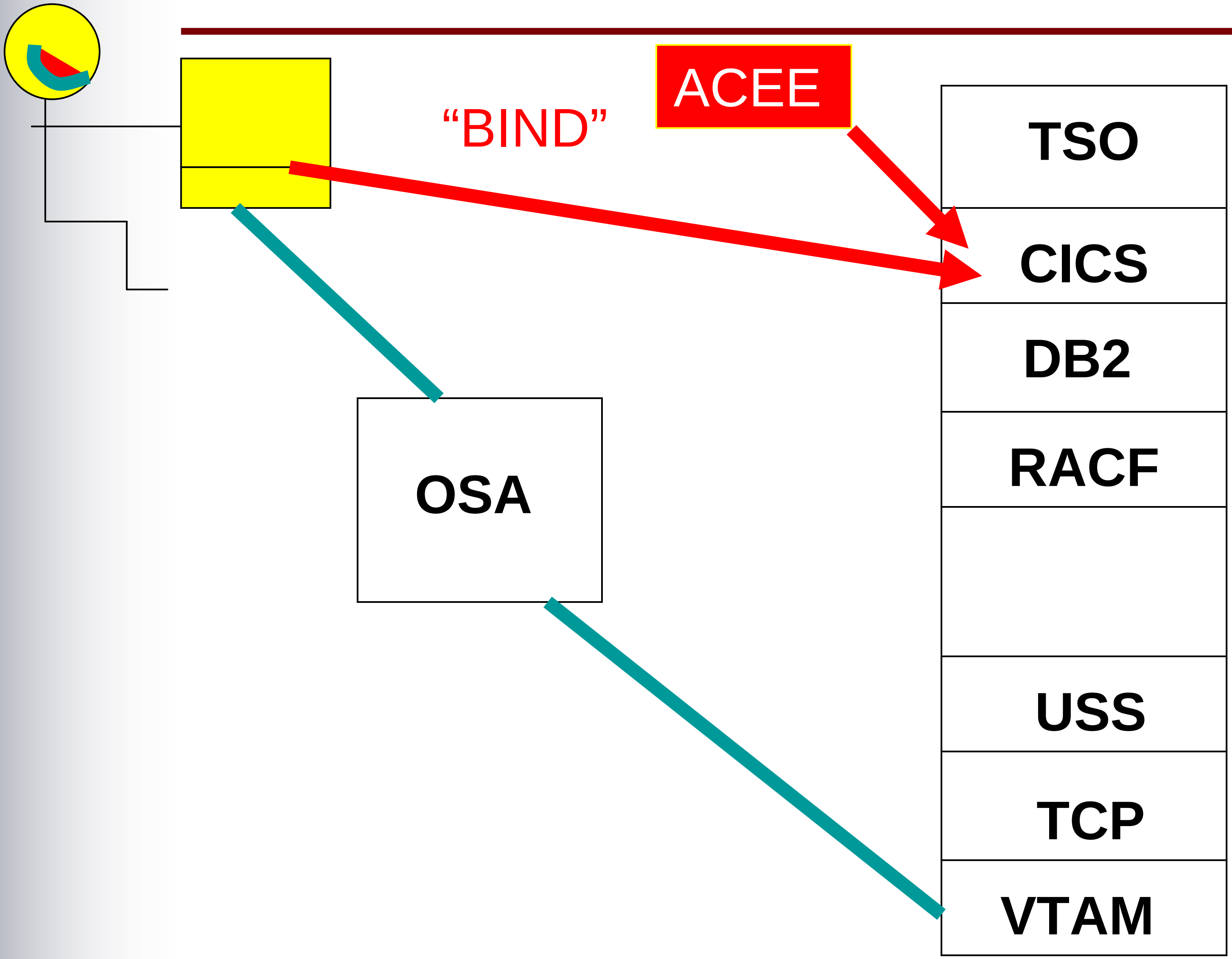
Phase 1, Basic Image-Level Controls

- Analysis
  - BATCHALLRACF, PROTECTALL,
  - What Resource Classes are Active and What the Rules Are
  - Parmlib Members (DEVSUPxx)

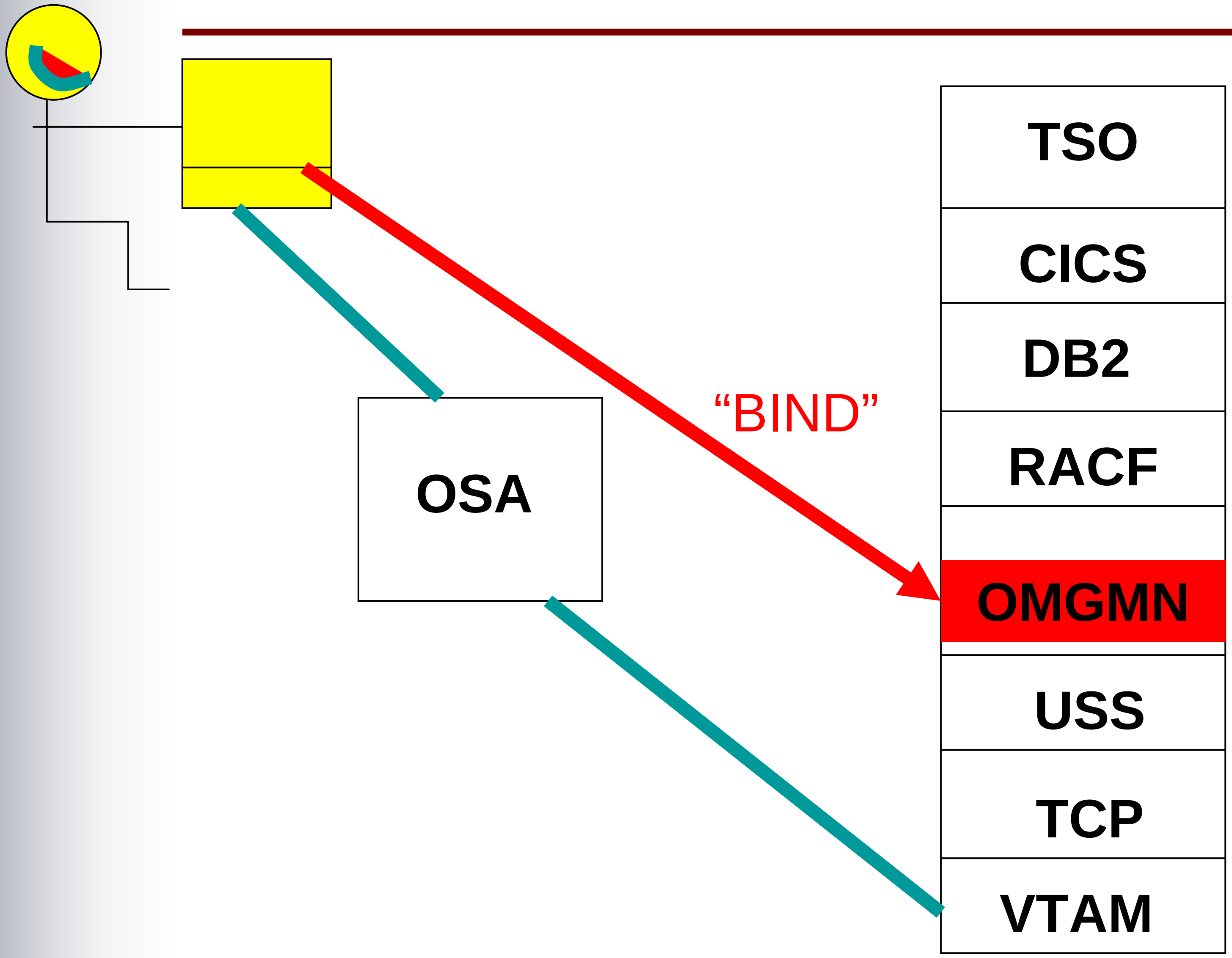
Phase 1, Basic Image-Level Controls

- Are All Paths Into the System Controlled by the Security Software (Applids, NJE/RJE, Batch, TSO, etc)?
- Are All Datasets Properly Protected?
- Are All Essential Resources Properly Protected?

How Your Terminal Connects to the Mainframe



What If an APPLID Uses Hardcoded Passwords?



Three Ways to Get to the “Starting Position”

1. **Walk Up to a Terminal**

2. **Dial-In (Use War Dialer to Learn Phone Number of Modem)**

3. **Telnet**

Phase 1, Basic Image-Level Controls

- Is the Integrity of the Operating System Intact (IBM’s Integrity Statement, Vendor Integrity Statements, Digital Signatures on Programs)?

Phase 1, Basic Image-Level Controls

- **Analysis**
  - **Controls Over Authorized Programs (Backdoors like User SVCs and APF programs)**
  - **How Users Are Identified. Could a sniffer program on Windows learn mainframe userids and passwords?**
  - **How Datasets and Resources Are Protected**

Phase 1, Basic Image-Level Controls

“***The Essence of Control is Comparison to a Standard***”

Phase 2, Stretching Cross-Image

Auditors are required by standards to "understand the entity" – in a z/OS processor complex, this means putting individual system controls into a valid risk-based context. This includes:

- **Understanding of how customization is applied and managed across the enterprise**
- **Evaluating how different environments/users are isolated**
- **Learning how baselines are developed, maintained and monitored**
- **Determining how COOP is designed**

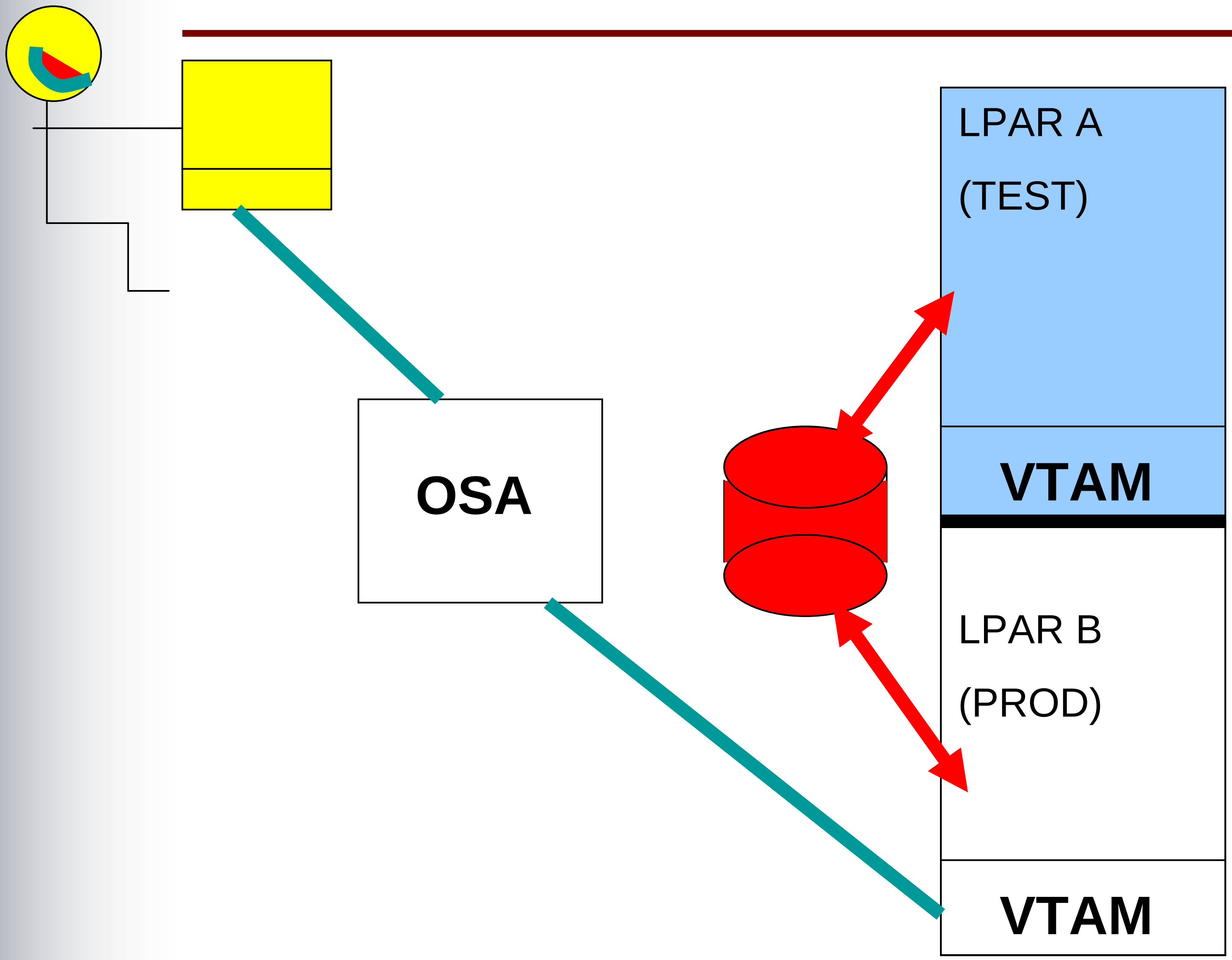
Phase 2, Stretching Cross-Image

- HCD
- Hardware Definitions: Consoles, OSAs, DASD, Especially Shared Devices
- SMP/E
- Cross-Image Customization Strategies

Phase 2, Stretching Cross-Image

- NJE, RJE
- Shared JES Spools
- Sysplexes
- GDS (Geographically Dispersed Sysplex)

Shared DASD Has AP File of Checks to Print

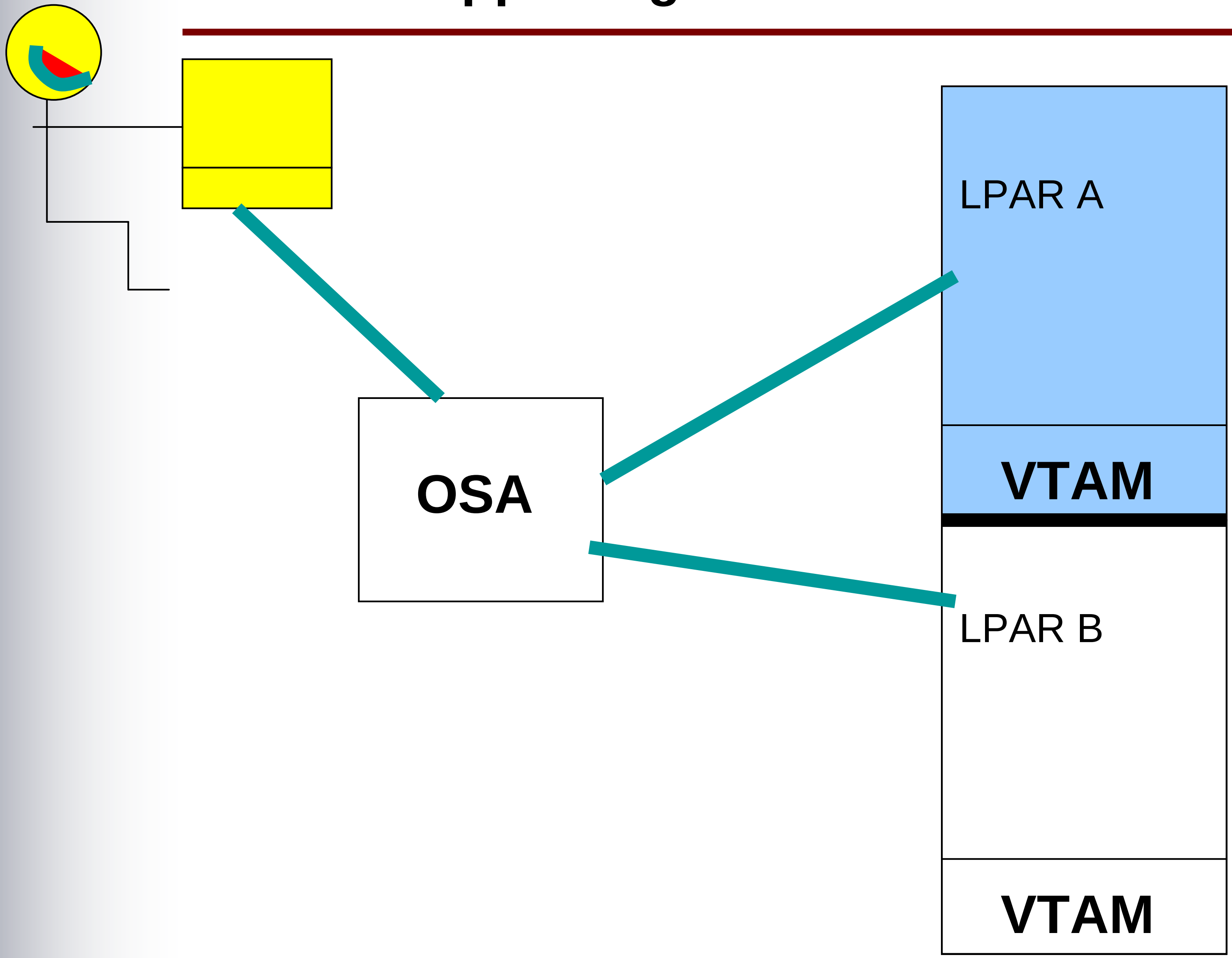


Phase 2, Stretching Cross-Image

An Exposure You May Need to Address, Recently Identified and Researched at GAO.

- **LPAR to LPAR communications when OSA adapters are shared can result in IP traffic routed between networks that are thought to be isolated**

An OSA CHPID Assignment Common to Two LPARs Supporting Isolated Networks



Phase 2, Stretching Cross-Image

LPAR to LPAR IP Routing Details:

- **OSA running in QDIO (Queued Direct I/O) mode**
- **QDIO needs a VTAM Transport Resource List (TRL) major node to be defined and active**
- **The CHPID assigned to an OSA is shared between LPARs**
- **OSA Address Table (OAT) automatically connects LPARs (including forwarding of IP packets between IP stacks defined on the z/System)**
- **IP packets can route internally between IP stacks on the z that have no routing defined otherwise**

Phase 3, the Web (and APPN)

The auditor is frequently asked for information about system controls that relate to applications. In many environments, this requires understanding controls that function within and around the z/Systems:

- Identification of critical controls outside of the mainframe
- Location of application control functions and their relationship/effect/reliance on mainframe-based controls

Phase 3, the Web (and APPN)

- IP Addresses and Ports
- Control Files for TCP/IP and His Daemons
- TCP/IP Address and Port Control
- APPN and SNI

Phase 3, the Web (and APPN)

- Policy Agent (Firewall-Like Functions, Free with TCP/IP)
- TSO NETSTAT
- SERVAUTH SAF Calls
- Control Files Can Determine How Users Are Identified (/etc/httpd.conf)

Phase 3, the Web (and APPN)

- VTAM tightly controls who can do what, until he goes cross-network with APPN or SNI.

- Then he becomes more open-ended, like TCP/IP

Phase 3, the Web (and APPN)

- Enterprise Extender is still SNA, just tunneled through UDP. Firewalls and encryption don't provide protection against SNA attacks.

- If your SNA network talks to a business partner's network (APPN or SNI), then you may be exposed to the networks your business partner connects to, and the ones they connect to, and so on.

Phase 3, the Web (and APPN)

- SNA is not going away any time soon.

- If you don’t know whether the VTAM options which can protect against this are active, an audit can help you understand.

Summary and Call to Action

- **What the Auditor Will Be Expecting From You**
  - **Data center personnel and management that are able to demonstrate an enterprise-wide understanding of operations and controls**

Summary and Call to Action

- **What You Can Do to Prepare for Such an Audit**
  - **Be able to communicate how the data center is operated, how services are provided to customers and how management verifies that control objectives are being achieved on an on-going basis**

Summary and Call to Action

- **How You Can Get the Most Out of Such an Audit**
  - **Do not hesitate to challenge audit conclusions that are technically invalid or incomplete**
  - **Assuming that anything positive can result from an audit… One result can be positive reinforcement for management that investments in baseline activities, monitoring, compliance and configuration management are cost-effective.**

Summary and Call to Action

- You can let an audit happen to you, or you can work with the auditor to get the most benefit out of it.

- Understanding how IT audits relate to the other audits will help you to assist your auditor to your advantage.

Summary and Call to Action

- **For More Information**
  - **On OSA Configurations:** IBM Redbook: ”*OSA Express Implementation Guide*” (SG24-5948-05)
  - **On APPN Risks:** www.net-q.com
  - **On GAO & FISCAM:** www.gao.gov

Summary and Call to Action

- To Contact Us:
  - David Hayes, GAO Applied Research and Methods, hayesd@gao.gov
  - Stu Henderson, the Henderson Group, stu@stuhenderson.com
- Thanks for Your Kind Attention