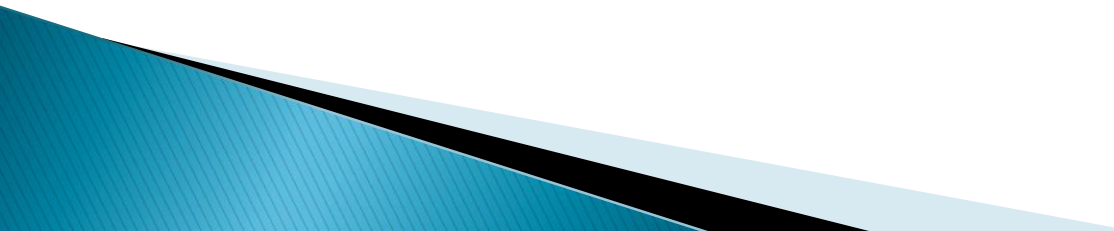


Auditing z/OS

Joe Castillo
MUFG Union Bank
IT Infrastructure Audit

Outline

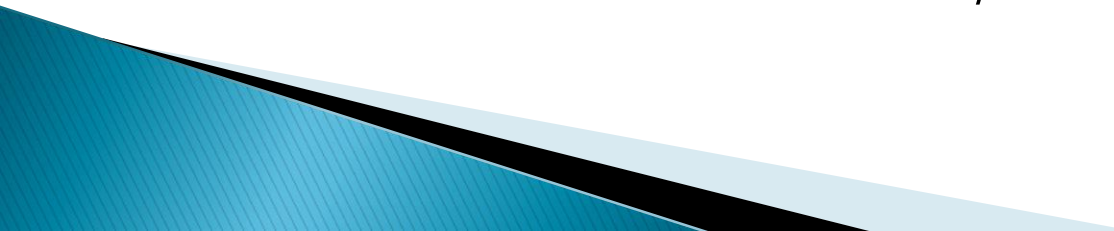
- ▶ Introduction
 - ▶ Why audit mainframe z/OS?
 - ▶ What is Audit?
 - ▶ IT Audit Basic rules
 - ▶ Resources and skills
 - ▶ Gathering Information
 - ▶ Planning the z/OS Audit
 - ▶ Simplified z/OS audit work program
 - ▶ Wrapping up
- 

Introduction

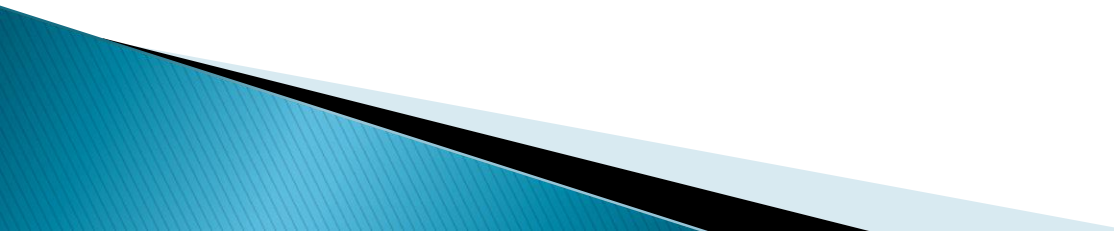
- ▶ 20 years IT audit
- ▶ 10 years various IT positions
- ▶ Starting back in 1979
- ▶ CISA, CTGA certified
- ▶ Banking industry
- ▶ Decline in experience, knowledge



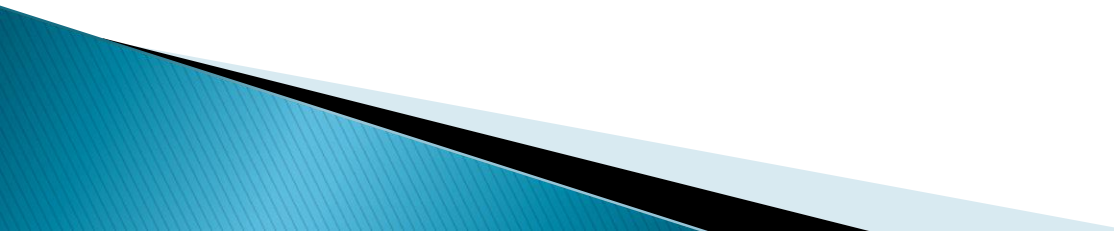
Intended Audience

- ▶ IT Auditors who want to learn how to audit IBM z/OS, especially those doing it for the first time
 - ▶ System Programmers who want to have a better understanding of what IT auditors do in their audits
 - ▶ Those users and technicians interested in risks and controls in z/OS
- 

Why audit mainframe z/OS?

- ▶ Introduced 50 years ago (1964) System 360
 - ▶ Key industries (banking, financial, retail, government, airlines, academia)
 - ▶ Most popular mainframe platform
 - ▶ Secure, reliable, supported, integrity
 - ▶ High volume transaction (max = 52,000 transactions per second)
 - ▶ Mature, proven technology
 - ▶ Core system for major organizations
 - ▶ High risk entity
- 

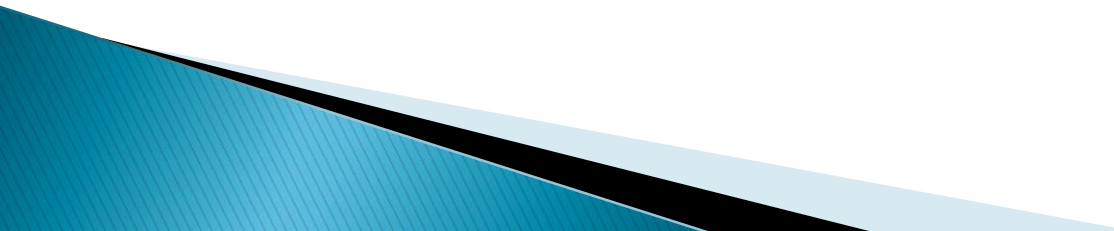
What is Audit?

- ▶ Internal Auditing is an *independent and objective* assurance and advisory activity designed to add value and improve an organization's operations. It helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
- 

What is IT Infrastructure Audit?

- ▶ Auditing of the computing infrastructure
 - Operating system (z/OS, Windows, UNIX, Tandem, etc,)
 - Data Centers
 - Network Controls
 - Technical Operations
 - Processes:
 - Change Management
 - Problem Management
 - Asset Management
 - Disaster Recovery
 - Many more areas but not business applications

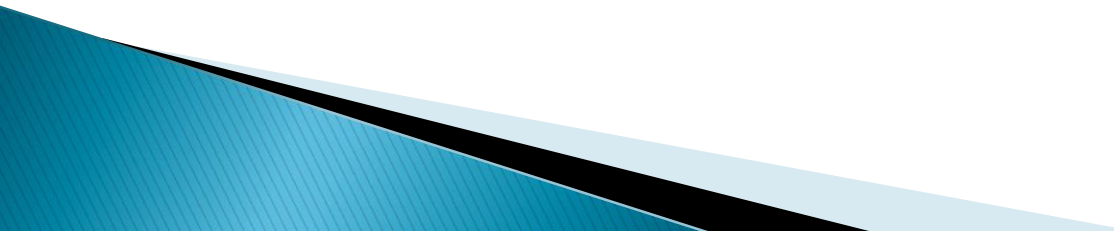
IT Audit Basic Rules

- ▶ 1 – Understand the architecture, know the controls*
 - ▶ 2 – Compare to a standard*
 - ▶ 3 – Know the risks*
 - ▶ 4 – Identify control parameter files*
 - ▶ 5 – Scope appropriately*
 - ▶ 6 – Know the root cause*
 - ▶ 7 – Understand the processes*
- 

Common reaction when your boss asks you to audit z/OS for the first time



You have options.....

- ▶ Option 1 – But I don't have the skills and knowledge. Give it to someone else. (Not recommended)
 - ▶ Option 2 – Accept the challenge. Learn the basics of Auditing z/OS. Will be able to add a marketable skill to your resume. (Recommended)
 - ▶ Option 3 – Outsource the assignment. (Not recommended – you will not gain the knowledge and skills)
- 

Resources

▶ Audit Software

- Vanguard Administrator/Analyzer
- CA Auditor (formerly Examiner)
- CAAT tools like ACL
- Write your own tools

▶ Books

- ISACA Audit and Control on MVS/zOS
- Mainframe Security
- CA Top Secret Auditor Guide
- IBM Redbooks

▶ Audit work programs

- ISACA
- AuditNet

More resources ...

- ▶ Training
 - Stu Henderson Consulting Group
- ▶ Conferences
 - Technologies
 - Not many Auditing z/OS sessions




What Skills Do You Need?

Audit skills?	Yes
System Programmer Skills?	Probably not
TSO?	Recommended
ISPF?	Highly recommended
Job Control Language (JCL)?	Recommended
Assembler?	Probably not
COBOL?	Probably not
RACF/TSS/ACF2?	Highly recommended
CAAT	Recommended

- ▶ Can always request information and work with Tech Support and Information security staff to obtain
- ▶ Preferred method is to audit through the computer, not around it

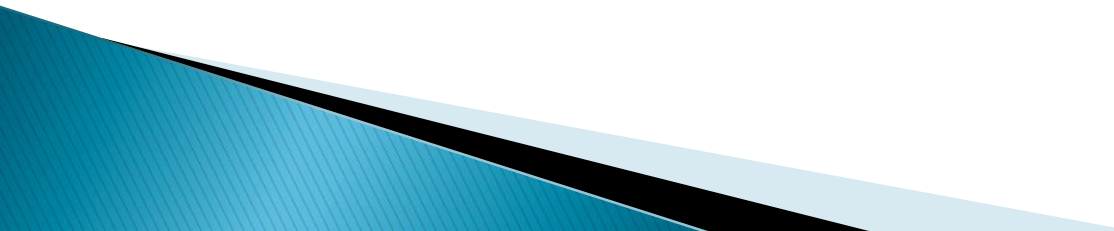
Gathering information

- ▶ Technical Operations organization
 - ▶ Identify staff
 - ▶ Obtain network diagram
 - ▶ Identify mainframe environment (LPARS, naming conventions)
 - ▶ Current IBM z/OS version
 - ▶ Security Software package (RACF, ACF2, Top Secret)
 - ▶ Useful system reports (DSMON, SETROPTS, TSS AUDIT REPORT)
- 

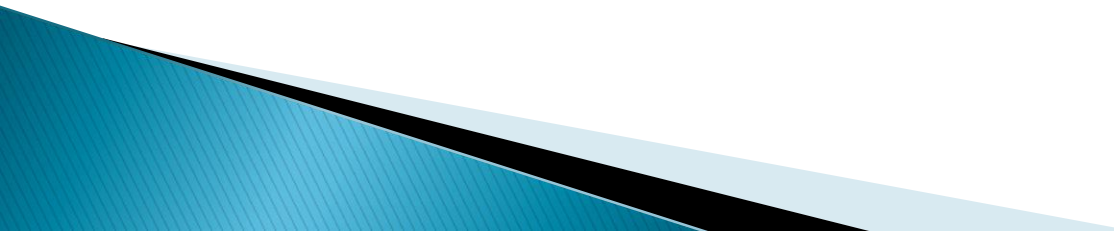
IBM Support Lifecycle

<input type="checkbox"/> z/OS	2.1.x	E	5650-zOS	30 Sep 2013	
<input type="checkbox"/> z/OS**	1.13.x	S	5694-A01	30 Sep 2011	30 Sep 2016
<input type="checkbox"/> z/OS**	1.12.x	S	5694-A01	24 Sep 2010	30 Sep 2014
<input type="checkbox"/> z/OS	1.11.x	S	5694-A01	25 Sep 2009	30 Sep 2012
<input type="checkbox"/> z/OS**	1.10.x	S	5694-A01	26 Sep 2008	30 Sep 2011
<input type="checkbox"/> z/OS	1.9.x	S	5694-A01	28 Sep 2007	30 Sep 2010
<input type="checkbox"/> z/OS	1.8.x	S	5694-A01	29 Sep 2006	30 Sep 2009
<input type="checkbox"/> z/OS	1.7.x	S	5694-A01	30 Sep 2005	30 Sep 2008
<input type="checkbox"/> z/OS	1.6.x	S	5694-A01	24 Sep 2004	30 Sep 2007
<input type="checkbox"/> z/OS	1.5.x	S	5694-A01	26 Mar 2004	31 Mar 2007
<input type="checkbox"/> z/OS	1.4.x	S	5694-A01	27 Sep 2002	31 Mar 2007
<input type="checkbox"/> z/OS	1.3.x	S	5694-A01	29 Mar 2002	31 Mar 2005
<input type="checkbox"/> z/OS	1.2.x	S	5694-A01	26 Oct 2001	31 Oct 2004
<input type="checkbox"/> z/OS	1.1.x	S	5694-A01	30 Mar 2001	31 Mar 2004

Identify General Controls

- ▶ Change Management
 - ▶ User provisioning process
 - ▶ Audit trails
 - ▶ Logs and monitoring
 - ▶ Segregation of duties
 - ▶ Disaster Recovery
 - ▶ Problem Management
- 

Policy, Standards and Procedures

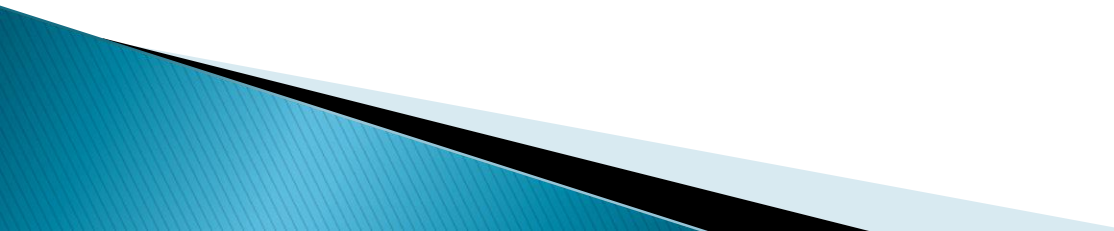
- ▶ Organization–Wide*
 - ▶ Mainframe Technical Standards*
 - ▶ MSRs*
 - ▶ Baseline Configurations*
 - ▶ COBIT5
 - ▶ FFIEC
 - ▶ COSO
 - ▶ *These are the standards which are compared
 - ▶ Root cause of many control deficiencies
- 

Planning the Audit

- ▶ Perform a risk assessment before and after

Areas:	Area:	Ref	Impact	Likelihood	Total
Hardware Controls	Supervisory VS Problem State		4	3	7
	Protect Keys	12	4	3	7
	Address Space		4	1	5
	System Authorization Facility (SAF)		4	1	5
MVS Backdoors	User Supervisor Controls (SVC)		4	4	8
	APF authorization	8, 17	5	3	8
	TSO/APF authorized	7	4	3	7
	I/O appendages		5	2	7
	Functional Subsystem (FSS)		0	0	0
	Exits		4	3	7
	Protect Key Zero (APF & PPT)	3	4	1	5
	Advanced backdoors (DIAG & CSVAPF)	13, 17	4	3	7
	SYS1.PARMLIB (incl PPT)	16	5	3	8
	Key (significant) datasets		3	3	6
MVS Security	Parmlib settings	14	4	4	8
	APF authorized datasets	7	4	4	8
	Security (TSS) Rules		4	4	8
MVS Control Objectives	Unauthorized modifications	20	3	4	7

Scope

- ▶ What you will look at
 - ▶ What timeframe you are reviewing
 - ▶ High risk vs General Controls
 - ▶ Number of hours
 - 400 minimum
 - 1200 max
 - ▶ Cycle audit, focused or targeted
- 

Ready



Set.....

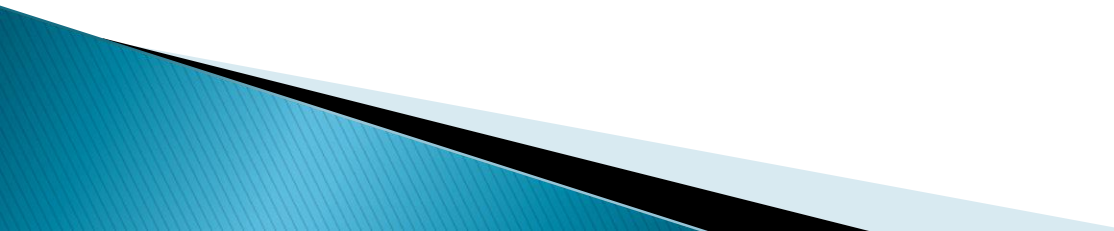
Go

The Basic Plan for Auditing z/OS

- ▶ Four basic questions:
 - 1 – What is it? (Audit Rule #1)
 - 2 – What are the Risks? (Audit Rule #3)
 - 3 – What are the Controls (Audit Rule #1)
 - 4 – What is the Audit test plan (Audit Rule #2)

- ▶ Test Plan sections:
 - ▶ Security
 - ▶ Logs and monitoring
 - ▶ General Controls
 - ▶ Compared to a standard

The Four Primary Audit Areas

- ▶ High Risk areas:
 - SYS1.PARMLIB
 - APF PROGRAMS&LIBRARIES
 - SVC PROGRAMS
 - STARTED TASKS
- 

Step 1 – SYS1.PARMLIB

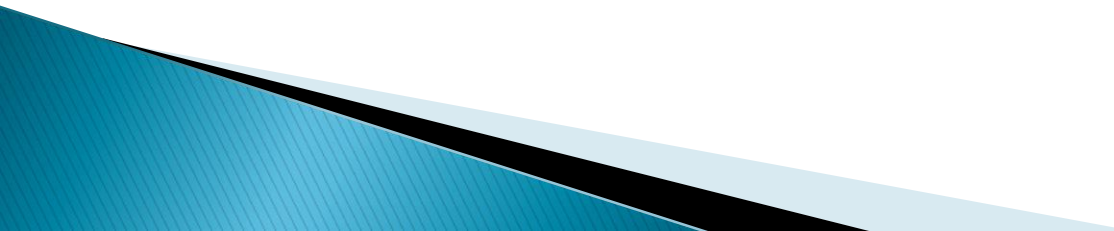


SYS1.PARMLIB

▶ What is it?

- System parameter libraries contain specification (parameters) that are used during an initial program load (IPL) of the mainframe.
- SYS1.PARMLIB is the dataset where the system programmer specifies almost all of the options for MVS including security options and backdoors.
- Review to determine what backdoors have been opened on the system. Will compare list of backdoor with authorized backdoors. (A backdoor is a way to gain access to a privileged feature)

SYS1.PARMLIB.....

- ▶ What are the risks?
 - If these parameters are modified incorrectly, the system may not be able to come up the next time its IPL'd.
 - Even if it starts it may not start properly and might cause service disruptions and partial system failures.
 - Company may experience system 'down-times' which may cause some financial losses.
- 

SYS1.PARMLIB

- ▶ What are the controls?
 - Access controls to restrict UPDATE or higher access
 - Restrictions on userids which can read file contents
 - Change management
 - Baseline configuration settings

SYS1.PARMLIB.....

- ▶ What is the test plan?
 - Match recent SYSx.PARMLIB changes to approved change records
 - Match current parmlib settings to a standard or baseline setting
 - Match current authorization and access level settings with a standard
 - Place the risk on the business client
 - Always have a standard to compare to
 - Determine the risk maturity level.

Step 2 – APF Programs and Libraries



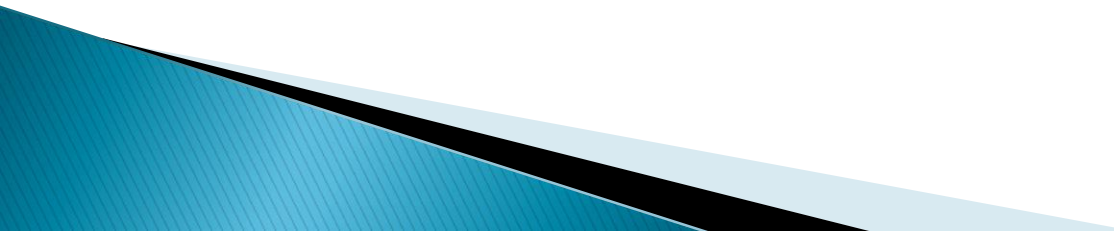
APF PROGRAMS AND LIBRARIES

▶ What is it?

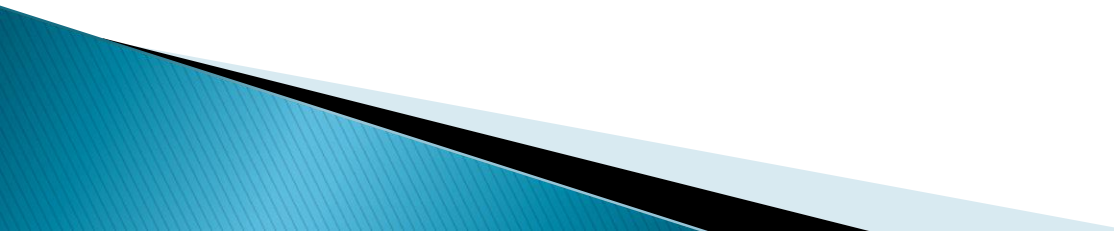
- a) The **Authorized Program Facility (APF)** is used to allow the installation to identify system or user *programs* that can use sensitive system functions. To maintain system security and integrity, a *program* must be authorized by the APF before it can access restricted functions, such as *supervisor calls (SVC) or SVC paths*.
- b) **APF** allows the system to identify which programs can execute privileged functions. **These functions are usually critical since many of them can bypass security and/or integrity checking.**
 - APF authorization is defined through SYS1.PARMLIB settings or by using some operator commands.
 - APF-authorized libraries usually correspond to subsystems and products that require that certain modules can execute privileged instructions in order to work properly.
 - APF programs reside in APF libraries

APF PROGRAMS & LIBRARIES....

▶ What are the Risks?

- Exposure of sensitive system libraries and their contents to unauthorized activities could compromise the integrity of the IBM z/OS operating system
 - Exposure of “backdoors” through compromised, unused or obsolete members, resources or settings.
 - Ability to bypass security and/or integrity checking
- 

APF PROGRAMS & LIBRARIES....

- What are the controls?
 - Access controls over the ability to update APF libraries
 - Access control over the ability to execute APF authorized programs
 - Access controls over the ability to modify APF program code
 - Access controls over the ability to update SYS1.PARMLIB
- 

APF PROGRAMS & LIBRARIES....

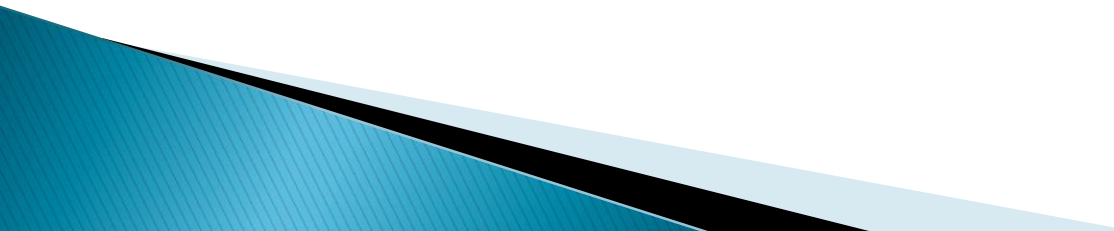
▶ What is the test plan?

- Review SYS1.PARMLIB members which contain APF library and program listings:
 - PROGxx, IEAAPFxx, SCHEDxx, other members
 - Automatic APF libraries: SYS1.LINKLIB, SYS1.SVCLIB, SYS1.LPALIB, SYS1.NUCLEUS
 - RACF DSMON AND CA TSSAUDIT reports list APF libs
- Review and determine:
 - If there are any duplicate and obsolete libraries
 - If the same program name exists on different libraries and volumes
- Review access controls to each library
- Determine if access is supported by a standard
- Identify APF load modules – AC(1)

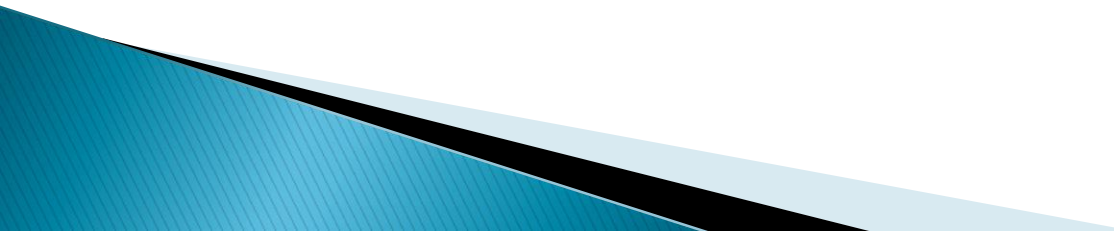
Step 3 – SUPERVISOR CALLS



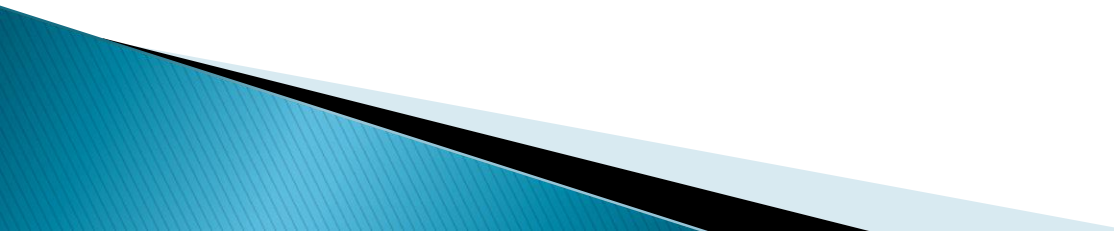
SUPERVISOR CALLS

- ▶ What is it?
 - ▶ **Supervisor calls (SVC)** is a processor instruction that directs the processor to pass control of the computer to the operating system's supervisor program.
 - ▶ Most SVCs are requests for a specific operating system service from an application program or another part of the operating system. Supervisor calls may run with protect key zero and supervisor state.
 - ▶ Access and authorization controls are necessary in order to prevent unauthorized SVCs from executing without limitations.
- 

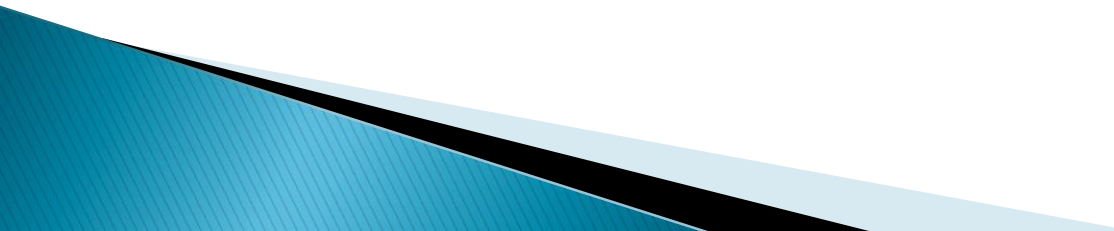
SUPERVISOR CALLS...

- ▶ What are the Risks?
 - Restricted SVCs are not available to all programs, execute sensitive supervisory or security related function within the operating system and execute from APF libraries. Failure to control these SVCs may compromise the integrity of the system
 - Unrestricted SVCs are available to all programs and execute either within or outside an APF library. Failure to control code modifications to these SVCs may cause significant damage each time executed.
- 

SUPERVISOR CALLS...

- ▶ What are the Controls?
 - Ensure Change Management controls are used for SVCs
 - Ensure an inventory of SVCs is maintained
 - Control access to APF libraries
 - Control access to the SVCTABLE
 - Control access to SVC program code
- 

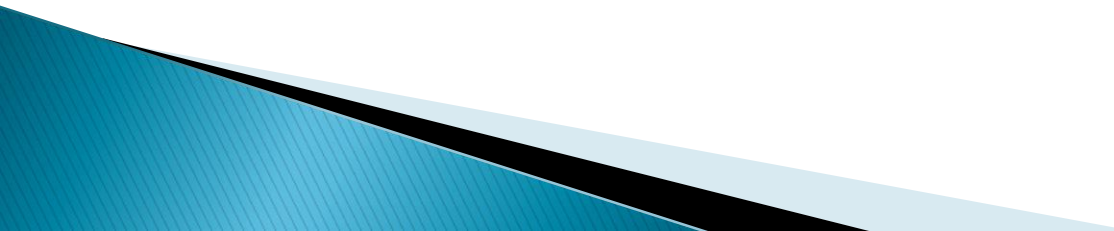
SUPERVISOR CALLS.....

- ▶ What is the Test Plan?
 - Identify restricted and unrestricted SVCs, determine how each is being controlled
 - Identify SVCs with a protect key zero and supervisor state, controls should be defined as these can run with full and unrestricted access to kernel level system services
 - Review access controls to APF libraries and SVC code.
 - Identify standards associated with SVC and compare control settings
- 

Step 4 – STARTED TASKS

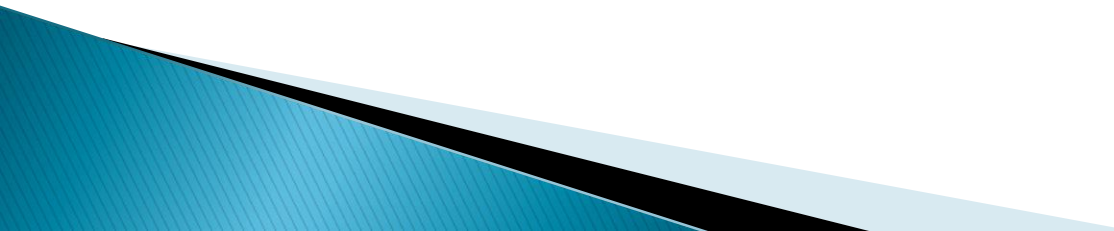


STARTED TASKS

- ▶ What is it?
 - ▶ **Started tasks (STC)** are initiated by a computer operator's submission of a 'START' command rather than initiation by a job and then executed in an address space, which is unattended. The started job can then execute another job. Started tasks are generally used for critical applications.
- 

STARTED TASKS.....

▶ What are the Risks?

- Started tasks which can execute automatically and execute other jobs may be running with unlimited access in the environment and potentially promote fraudulent activity and compromise the integrity of the z/OS operating system environment.
 - Vendor supplied STCs may have an unknown and undefined risk
 - STCs may be established with privileges to bypass security
- 

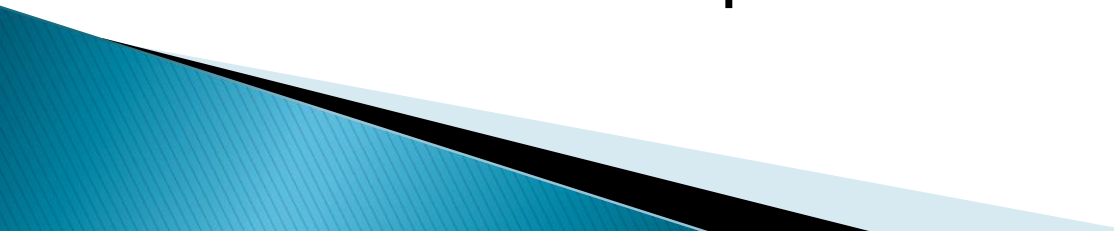
STARTED TASK...

- ▶ What are the Controls?
 - Maintain an inventory of all STCs and their use
 - Control attributes and privileges assigned to each STCs
 - Restrict UPDATE or higher access to sensitive libraries, including APF libraries
 - Control authorization levels assigned to STC's
 - Ensure standards exist for the control of STCs

STARTED TASKS...

- ▶ What is the Test Plan?
 - Review and compare standards associated with STCs
 - Validate STCs are being inventoried and are active
 - Identify all STCs with access to APF and system libraries to determine if the access is warranted and compare to a standard
 - Validate that STCs are not running with privileged attributes which can bypass security (NORESCHK, NOSUBCHK, NOVOLCHK, NODSNCHK) and that a standard supports its usage
 -

IN SUMMARY

- ▶ There are many other areas to audit in z/OS but keep your scope narrow
 - ▶ If the four areas mentioned have control deficiencies, then you'll have problems in other areas
 - ▶ If the four areas are satisfactory, then you have some confidence in z/OS that adequate controls are in place
- 

CONCLUSIONS....

- ▶ We talked about:
 - Audit, IT Infrastructure Audit and its mission
 - z/OS Audit Skills, resources, experience
 - Planning your z/OS Audit
 - Four significant areas to test:
 - SYS1.PARMLIB
 - APF programs and libraries
 - Supervisor Calls (SVCs)
 - Started Tasks (STCs)
 - Definitions, risks, controls and test plans

THANK YOU

► Any Questions?

