MANEWS 01

==
==

M A News
Mainframe Audit News
October, 2001
Issue Number 01

Table of Contents

IN THIS ISSUE

(YOU CAN USE the Find function of your email or Acrobat software to jump directly to a given section. For example, to jump directly to the Great Websites section, you would Find on "7)" or on "Great Websites".)

===
===

1) Introducing the Mainframe Audit News

This is the first edition of the Mainframe Audit News, a vehicle for sharing information about auditing IBM mainframe computers. By "mainframe computers", we mean large, powerful, IBM computers, located in a data center that provides the management controls to provide effective information processing. (These management controls include: physical security such as locked doors, environmental sensors such as fire detection equipment, automated backups of critical data, business resumption plans, problem management processes, and others.)

We will not concentrate on these management controls, since they are properly part of a data center audit. Rather we will concentrate on the computer itself and the software running on it. In most cases that software will include the MVS operating system.

We intend to explain the MVS operating system, as well as other system software associated with it. (MVS stands for Multiple Virtual System, a name which no one ever uses.)

Our audience consists of information technology (IT) auditors, as well as financial auditors who want to learn something about IT auditing.

We will make a point of expanding acronyms clearly. We will always try to explain in simple terms what each piece of software does, and how to audit it. We will make a special point of giving practical advice in dealing with system programmers who may not welcome the audit. We will also give suggestions on the overall conduct of the audit.

Further, we will share information about web sites of interest to the mainframe auditor. We will provide a tech support hotline for the mainframe auditor to get quick answers to technical questions, and share some answers in our Q&A (Question and Answer) column.

About the Mainframe Auditors' Newsletter (MA News)

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily MVS, OS/390, z/OS, and the system software associated with them). This software includes: CICS, DB2, JES, VTAM, MQSeries, TSO, USS (UNIX System Services), TCP/IP, and others. It also includes the Websphere server software which connects a mainframe to the Internet. (Note, we will expand each of these acronyms and explain how the software works over the course of the next several issues.)

We expect to have a new issue at least every three months.

We will never include attachments to the email.

The MA News is meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM.

We will not make the list of subscribers available to anyone else for any reason.

Topics will include:

? How the Hardware Controls Work

? How the "BackDoors" to the Hardware Controls Work

? How to Scope and Plan a Mainframe Audit

? Different Types of Mainframe Audit

? What Data to Collect, How to Collect It, How to Interpret It

? What All Those Acronyms Mean, Including MVS, CICS, TSO, and z/OS

? What the Different Software Packages Do, How They Work, and How to Audit Them

? How to Deal with Mainframe System Programmers

? How to Make Practical Audit Recommendations

? Common and Not-So-Common Mainframe Audit Findings

? How to Make Your Audit Findings Sail Through the Closing Meeting Easily

? A Question and Answer Column

To Sign Up for the Mainframe Auditors' Newsletter, see section 9) below.

2) Why Mainframe Audits Matter

While many people have claimed that the "mainframe is dead", it is actually thriving. The reasons for this include both:

2A) Capability and
2B) Changes within IBM.

2A) >>>> Capability

The mainframe has always been hard to kill, since no other commonly available platform can support extremely large files (for example, the customer master file of a Fortune 500 company, or the files of a large government agency).

No other commonly available platform can process the number of transactions that a mainframe does. When the VP of Marketing reads about e-commerce and asks the CIO to support it, the CIO will say "Yes, we can.". He or she quickly realizes that the mainframe is often the only computer available with the power to hold the master files and to process the large volume of orders hoped for.

2B) >>>> Changes Within IBM

IBM has changed its attitude in the last decade or so, turning away from IBM-only standards to industry-wide standards. This has resulted in the UNIX operating system being available on the mainframe, under the control of MVS. (UNIX under MVS goes by two names: OMVS and USS.)

This has also resulted in support for ways to connect the mainframe to other platforms, including: TCP/IP, MQ Series, DCE (Distributed Computing Environment), and the Websphere Internet Server.

[TCP/IP, or Transmission Control Protocol/Internet Protocol, is the communications standard for two computers to exchange information. It is used by UNIX and by the Internet. MQ Series is software which makes it very easy for a program on one computer to exchange information with a second program which is executing on a different brand of computer. DCE, or Distributed Computing Environment, is an industry-wide set of standards for programs on different brands of computer to work together. Websphere makes it possible to connect the mainframe to the Internet, which raises a new set of control issues for the data security officer and for the auditor.]

DCE is of special interest because it is supported by Novell Directory Services (from Novell), by Windows 2000 with Active Directory (from Microsoft), and by all five of IBM's strategic platforms, including the mainframe. DCE can provide the foundation for single-signon and for centralized security administration.

All these changes in IBM make it possible, perhaps inevitable, that the mainframe become "just another node on the network", connected to the Internet, and also to internal networks. While some internal audit departments have concentrated on smaller, less-powerful computers, many are now discovering that the majority of essential computing power, and the majority of the critical applications still execute on the mainframe. The Internet connection makes it yet more important that annual audit planning consider the place of the mainframe.

3) What's the Difference Among MVS, OS/390, and z/OS?

MVS (Multiple Virtual System) is an operating system which is part of the software package called OS/390. Recently, IBM has started offering z/OS, a successor to OS/390 based on improved hardware and software technology. Like OS/390, z/OS includes the MVS operating system.

We next explain these concepts in these sub-sections:

3A) What is an operating system?
3B) What is OS/390?
3C) How is z/OS different?

3A) >>>>What is an operating system?

An operating system is the software that controls all the other software and all the hardware on a computer. Examples include: Windows, UNIX, OS/400, MVS, and VM. The operating system is the program which starts executing as soon as the computer starts running. The operating system selects other programs and allows them to execute.

When other programs need to use hardware resources (for example, to read from a disk drive, to allocate memory, or to know the current date), they make requests of the operating system. The operating system satisifies these requests by dealing directly with the hardware, but only after verifying that they are appropriate. For example, when a program requests access to a file on a disk drive, the operating system allows the access only after verifying that the file belongs to that program.

The operating system prevents other programs from dealing directly with the hardware. (We'll describe how in a future issue.) If you are picturing a kindergarten (with the operating system as the teacher and the other programs as the children), you have a good idea of what an operating system is.

If one child tries to take another child's candy, the operating system stops it. If there is only one stuffed animal, the operating system makes the children share it politely. When children ask to have their milk heated, the operating system doesn't let the children use the stove. It deals directly with the stove for them.

The concept of an operating system is important to auditors, since it is the place where all the controls are centralized. If the kindergarten teacher were neglectful and let some child use the stove directly, we would be concerned. If there were a breakdown in the controls MVS uses to prevent a program from using hardware resources directly, we would be similarly concerned. In auditing MVS, we examine these controls and the way that they are managed to ensure that they work effectively.

3B) >>>>What is OS/390?

IBM used to sell each of the software products needed to support the MVS operating system as separate products. This was expensive and complicated. It also led to conflicts when a data center has one version of one software product, but didn't have the corresponding version of some other software product.

As part of the shift in attitude at IBM described above, IBM re-packaged MVS and a large number of other software products into a package called OS/390. This simplified ordering, maintenance, and administration. It improved software quality, while reducing the need for system progammers. At the same time, IBM lowered hardware and software prices. They also added several software products to OS/390 that made it easy to connect MVS to other computers in a network. IBM's mainframe sales increased significantly after the introduction of OS/390.

3C) >>>>How is z/OS different?

In 2001, IBM introduced significant new hardware technology for all its computer platforms (the mainframe, the personal computer, the AS/400 mid-range, and the RISC/6000 UNIX computers). To take advantage of the hardware, IBM upgraded the software. The result was greatly improved reliability, with greatly increased ability to connect over a network.

On the mainframe, this new software is called z/OS. (The "z" stands for zero downtime, and IBM means it. z/OS computers should experience no more than a few minutes downtime [that is, time when the computer isn't available] per year).

In addition to improved availability and connectivity, z/OS supports "64-bit addressing". This hardware improvement increases the maximum amount of memory that can be used. The increase is from 2 gigabytes (about two trillion) to to 16 exabytes (about sixteen trillion, trillion). This makes it possible to process much larger amounts of data at a time.

z/OS includes the MVS operating system. In the first release of z/OS, all of the software works essentially the same as it did in the last release of OS/390. The transition should not require re-training for users, application programmers, nor auditors.

4) What's the Difference Between TSO and CICS?

TSO (Time Sharing Option) and CICS (Customer Information Control System) are both programs which let users at terminals use the computer. They differ in what they allow the users to do.

TSO is often thought of as a programmer's workbench. It allows the terminal user to browse files, to edit them, and to execute programs.

CICS in contrast allows the terminal user to do only a limited number of functions, each of which is defined as a specific transaction. Each transaction corresponds to a specific program, which is often written by the organization's application programming group.

For example, if you wanted to let the sales clerks in the order entry department type in a customer number at a terminal and get back the customer's name and address, this would likely be a CICS transaction. The transaction might be named INQ3 (for inquiry 3), and might be carried out by a program named INQ3PGM. Sales clerks would be permitted to use CICS, and to execute the transaction INQ3. They would not be able to browse the customer master file, to compile programs, or to execute other programs.

The application programmer who develops the program INQ3PGM would likely use TSO to develop the program: editing it, compiling it, linkediting it (steps necessary to prepare the program for execution), and testing it. Once the program is developed under TSO, the finished product would be transferred to CICS, where it would be made available to the sales clerks at their terminals.

Their are often several copies of the CICS program executing, each of which is called a "region". One might be for marketing transactions, another for finance transactions, another for inventory transactions. Yet another region might be reserved for the applications programmer to test out a new version of the transaction.

For an auditor, it is important to collect basic information about CICS: how many regions exist, what each is for, and what transactions are defined in each region. This will be critical for scoping the audit.

You don't want to say "Next week, I'm going to audit CICS." and then discover that there are literally hundreds of CICS regions. Your scoping statement should say something like "This audit addresses security on the production marketing CICS region. It is restricted to the order entry transactions there and the controls over who can execute them."

For TSO, the auditor will can safely assume that there is only one copy of TSO executing on each MVS system. TSO does not have "transactions", however there are TSO commands which perform certain functions, such as editing, compiling, and executing a program.

TSO is unlike CICS, which has a controlled set of transactions, and automatic control over who can execute which ones. TSO instead relies more on the security software to control who can use TSO in the first place, and who can read and write specific datasets with it. (Examples of security software are: RACF, ACF2, and TopSecret, which we will address in a future issue.)

So while CICS and TSO are similar in allowing users at terminals to access the computer, their different structure means differing audit approaches for: scoping, data-gathering, and analysis.

5) Question and Answer Column

Since this is our first issue, we have not yet received any question. This gives us the freedom to make up our own questions and answers, a freedom we will continue to abuse if we don't hear from our readers.

Our first question is from an editor and system programmer in Bethesda, MD:

Q) Is an auditor likely to give the most value to his or her organizaton by auditing the mainframe or by auditing other platforms?

A) Neither, although every platform should be considered in planning and budgeting the audits for the upcoming year. The most value an IT auditor can give the organization is by addressing the key areas we are about to describe. They all result from the increasing interconnection among platforms, and the lack of communication among different departments and technical specialists. We will address mainframe aspects of these areas in future issues.
These key areas are:

>Coordinating the assignment of UNIX uids and gids across the organization and across all platforms (including the mainframe) to avoid conflicting assignment. (A uid is a number which identifes a user; a gid is a number which identifies a group of users.) If one person is assigned the uid 5027 for example on one UNIX platform, and a different person is assigned the same uid on a different platform, there will likely be extra future confusion and work when applications are ported (carried) to a different platform. This is

easily avoided with organization-wide standards. Such standards are not likely to be developed unless someone helps all the UNIX administrators to communicate and work together.

>Coordinating firewall configuration and policy across the organization. (A firewall is a computer (and software) which protects a TCP/IP network by controlling which messages are permitted to flow in and out of each computer.) It is common for an organization to have more than one firewall, each implemented in a different fashion by a different department. The mainframe computer comes with a firewall program which should considered as part of an organization-wide approach to firewall configuration.

>Coordinating use of digital certificates and IP addresses across the organization. (A digital certificate is a message telling you someone' public encryption key, an essential part of network security and e-commerce. An IP address is a number (made of of four octets separated by dots, for example: 198.181.31.5) which identifies a computer over an IP or Internet Protocol network.) Mainframe security software products support digital certificates (and IP addressing). Their use on the mainframe should be coordinated with that on other platforms.

>Protecting mainframes connected to the Internet. While mainframes have better Internet security tools than most other platforms, these tools are often not implemented completely and effectively. Many experts consider it just a matter of time before the Internet hackers learn enough about mainframes to try hacking them over the Internet. An effective audit can help an organization to protect the mainframe before this happens.

6) The Program Properties Table

The Program Properties Table, or PPT, is one of several ways the system programmer can "open a back door" to the MVS operating system, by giving a program privileges which let it bypass security. Any MVS security audit should address the PPT to ensure that every entry is appropriate and authorized. One problem facing the auditor is how to determine which entries are appropriate and authorized. This article will first describe how the PPT can open back doors; then describe the initial entries in the table provided by IBM, and then describe how to evaluate any additional entries.

3A) >>>>How the PPT Can Open Back Doors

Each entry in the PPT describes one program, and assigns that program certain attributes or privileges. The two attributes of concern in an MVS security audit are called "Bypass Password" and "Privileged Protect Key".

The Bypass Password attribute indicates that the indicated program can bypass dataset security with RACF or TopSecret security software (but not with the ACF2 security software).

The Protect Key specifies a number from zero to fifteen which controls what memory the program can update. Most non-privileged programs execute with a protect key of eight. Protect key values of zero through seven are considered "privileged" and permit the program to obtain all the privileges of the MVS operating system itself. Once a program has the privileges of the operating system, it can bypass all the security of the system. It can read, change, delete, and create any data on the system. It can execute any instruction on the system. It can prevent logging of what it does.

(Note: if you are working on a system with the RACF security software, RACF provides a report of every program in the PPT which has either of these two attributes (Bypass Password and Privileged Protect Key). This may be found in the Program Properties Table sub-report of the DSMON (Data Security Monitor) report. On systems with the TopSecret security software, a similar report is available. Several software tools for auditors, such as CA-Examine, also report on the PPT. The other way to learn what programs in the PPT have these two attributes is to examine the PPT itself. Parts of the PPT are kept in two places, one a member of the dataset SYS1.LINKLIB named IEFSDPPT. The other place is the SCHEDxx members of the dataset SYS1.PARMLIB.)

3B) >>>>Inital PPT Entries Provided by IBM

Below is a list of the programs to be found in the original PPT which have either "Bypass Password" or a privileged Protect Key (that is, one from zero through seven), as specified by IBM. Any additional entries with these privileges should be formally documented as described below.

```
ProgramName Description
-------- ------------------------------------
AHLGTF GTF
AKPCSIEP ISP
ANFFIEP IP Printway
APSPPIEP PSF
ASBSCHIN APPC/MVS Scheduler
ASBSCHWL APPC/MVS Message Log Writer
ATBINITM APPC/MVS
ATBSDFMU APPC/MVS SDFM
AVFMNBLD AVM
BPXINIT OMVS
CBRIIAS OTIS
CBROAM OAM
CNLSSDT MVS Message Service
COFMINIT VLF
COFMISDO DLF
CQSINIT0 IMS CQS
CSVLLCRE LLA
CSVVFRCE Virtual Fetch
DFSMVRC0 IMS Control Program
DSNUTILB DB2 Batch
DSNYASCP DB2
DXRRLM00 IMS Manager
EPWINIT FFST
EZAPPFS NPF
EZBTCPIP TCP/IP
GDEICASB DFP/DFM
GDEISASB DFP/DFM
GDEISBOT DFP/DFM
HASJES20 JES2
HHLGTF GTF
IASXWR00 External Writer
IATCNDTK JES3
IATINTK JES3
IATINTKF JES3 FSS
IDAVSJST SMSVSAM
IEAVTDSV Dumping Services
IEDQTCAM TCAM
IEEMB860 Master
IEEVMNT2 Mount Command
IEFIIC Initiator
IFASMF SMF
IGDSSI01 SMS
IGG0CLX0 CAS
```

IHLGTF GTF
IKTCAS00 TCAS
IOSVROUT IOS
IRRSSM00 RACF
ISFHCTL SDSF
ISTINM01 VTAM
ITTTRCWR CTRACE Writer
IWMINJST WLM
IXCINJST XCF
IXGBLF00 System Logger
IXGBLF01 System Logger
IXZIX00 JES Common Coupling
MVPTNF TNF
MVPXVMCF VMCF
SNALINK SNALINK

(This list is extracted from the IBM manual: MVS Initialization and Tuning Reference, available online from the websites listed below.)

3C) >>>>How to Evaluate PPT Entries For an MVS Audit

Ask these questions:

>Is each entry necessary? For example, a JES2 installation would not need the program for JES3, nor a JES3 installaiton the program for JES2. An installation which uses ACF2 or TopSecret security software would not need the program RACF.

>Do we have assurance that each entry can be trusted? For example, the IBM-supplied programs may be trusted, since they are covered by the integrity statement IBM gives us for the trustworthiness of the MVS operating system. Other entries might be trusted because we have comparable integrity statements from the vendor, or because our systems programming group has conducted a formal assessment of the code and considered it trustworthy. (Note: "formal" here means "in writing", and therefore capable of being reviewed by others.)

> Does the system programming group have control of the PPT entries for programs with these two attributes? That is, do they have a list of what entries other than the IBM-supplied entries SHOULD be in the PPT? If not, then there is no standard to compare to, and it is impossible to determine

whether the entries in the list are appropriate.
Before writing the audit findings and recommendations, recognize these issues related to the associated risk:

>The programs listed in the PPT have the privileges described above only if they are located in certain program libraries called "APF-authorized" libraries. (APF stands for "Authorized Program Facility", a very silly name. We will discuss APF authorization in a future issue.) If anyone, or even any system programmer can update these libraries (thus replacing one of these programs with a rogue version), the risk is greater. If there is a formal change control process, and the security software prevents anyone from updating these libraries without going through the change control process, then there is less risk. (And you might want to audit the effectiveness of the change control process.)

>Just because an entry isn't necessary (for example, the entry for JES3 in a JES2 installation), doesn't mean that there is a serious problem. It does suggest that the PPT hasn't been managed as well as it might. If however for example, there is a program with the name of the JES3 program in an APF-authorized library of a JES2 installation, then you might worry about what that program really does. But most audits don't (and should not) provide time to make such evaluations. An unnecessary entry becomes more significant to the audit if APF-authorized libraries can be updated by without going through a change control/quality assurance process.

>You probably do not have the time (nor knowledge nor inclination?) to evaluate each PPT entry in detail. Your audit should be addressing the issue of whether the management controls are effectively in place to ensure that the entries are all appropriate. The audit emphasis should be on these management controls (such as change control management and system software quality assurance) rather than on some individual entry that might seem out of line.

>The real question is do we (and does the system programming group) have a reliable means of knowing that only appropriate programs are listed in the PPT. This means: do we have a standard against which to compare the actual entries.

==
==

7) Great Websites for Mainframe Auditors

This issue we offer websites that provide glossaries or explanations of MVS acronyms, as well as other information useful to auditors. We do not endorse (nor disparage) any of their products, nor the quality of their websites, since we have not had an opportunity to evaluate them. However, we find them interesting, and hope you will too.

? http://www.planetmvs.com for Planet MVS

? http://mainframes.com for more mainframe info

? http://www.north-ridge.com/tnd420/TND0219a.htm for a glossary

? http://www-1.ibm.com/ibm/history/reference/glossary_m.html for an IBM glossary

? http://www.auridian.com/glossary/ for another glossary

? http://whatis.techtarget.com/ for yet another glossary

? http://www.stuhenderson.com/ for basic IT audit info sources

----

The following links are to IBM sites with glossaries or with access to IBM manuals online:

? http://www.ibm.com/servers/eserver/zseries/zos/bkserv/ for z/OS info

? http://www.ibm.com/servers/s390/os390/bkserv/ for OS/390 info

? http://www.ibm.com/servers/s390/os390/bkserv/redbooks.html for redbooks

? http://www.ibm.com/networking/nsg/nsgmain.htm"> for a glossary

==
==

8) Tell Us What You Think

We'd love to hear from you, in particular on these topics:

>What do you like/not like about the MANEWS?

>What websites do you know that you want to share with other auditors?

>What topics and/or columns would you like to see in future issues?

>What software tools do you use and like for MVS audits? Examples are: CA/Examine, ICU from Janus, and the MVS audit tool from Consul. What other products do you use? What do you like about them? (We do not intend to conduct a complete critique of such products. However we would like to make a complete list available to everyone, along with your comments on the features you like best.)

Please email your comments to stu@stuhenderson.com. Thanks.
===
===

9) How to Subscribe/Unsubscribe

This section shows you how to:

9A) Subscribe,
9B) Unsubscribe,
9C) Request back issues,
9D) Take advantage of our free technical support for mainframe auditors.

9A) >>>>To Subscribe to the Mainframe Auditors' Newsletter (MA News)

Send an email to: stu@stuhenderson.com

with the subject field set to: MA News

and in the body of the email just this word: SUBSCRIBE

9B) >>>>To Unsubscribe from the Mainframe Auditors' Newsletter (MA News)

Send an email to: stu@stuhenderson.com

with the subject field set to: MA News

and in the body of the email just this word: UNSUBSCRIBE

9C) >>>>To Request Back Issues of the Mainframe Auditors' Newsletter (MA News)

Send an email to: stu@stuhenderson.com

with the subject field set to: MA News

and in the body of the email just this phrase

(for example to request issues 1 and 2): Back Issues: 1, 2

9D) >>>>To Get Questions Answered from the Mainframe Auditors' Newsletter (MA News)

Send an email to: stu@stuhenderson.com

with the subject field set to: MA News

and in the body of the email the word: Question: (followed by
your question, and tell us whether you want your name included or not if we decide to publish your question and answer)

Whether we print your question and answer or not, we will try to email you back an answer to your question within five business days. If you need a faster answer, please phone your question to (301) 229-7187, leaving the question on the machine. Please repeat your phone number slowly and clearly.

11) Feature Article: SYS1.PARMLIB Developments Auditors Need to Know

(Note this article made our first issue so big that it has been moved to Issue Number 02, which will be published shortly after this issue.)

Stu Henderson, (301) 229-7187, stu@stuhenderson.com, www.stuhenderson.com