MANEWS Issue Number 17

# the Mainframe Audit News

**Table of Contents**

1. What is CICS?
2 How to Audit CICS: Appplication Audits
3 CICS Application Audits: Icing the Cake
4. Q and A
5. Seminar Information and Miscellanea; z/OS Glossary; About the Mainframe Audit News: How to Subscribe/Unsubscribe

## 1) What is CICS?

**CICS** (IBM's Customer Information Control System) is transaction management software. This means that it supports requests from terminals for transactions, and then executes the programs which perform the functions of those transactions. The request is in the form of a transaction identifier or **tranID**.

CICS restricts what a user can do to a limited number of pre-defined transactions. For example, one transaction might be named **INQ3** (inquiry number 3). It might permit a user to type in a customer number and then have the customer's name and address displayed on the terminal screen. A user of CICS is limited to executing only the predefined transactions which exist on his copy of CICS, and to which he is permitted by the security software. An **application** (such as Payroll or Order Entry) will consist of a collection of transactions which perform application specific functions.

Whenever a CICS user types in the name of a transaction he wants to execute, CICS can call the security software first, asking "Should I let this user do this transaction?" Last issue we discussed a security audit of the CICS **infrastructure**. This issue we cover how to perform a security **audit of a given application** running under CICS.

==========
==========

## 2) How to Audit CICS: Application Audits

Planning, Scoping, and Data Gathering

As you plan and scope your first CICS application audit, you will want to select one important, production application. Get a list of all its transactions and the security rules controlling who can execute them. For each transaction, get a one or two sentence description of what it does. This will be available in the documentation for the application, and from the CICS system programmer.

Find out the name of the **region** (copy of the CICS program) where the application executes and learn the security software rules controlling who can access that region. Get a copy of the SIT, that is the file containing all the options, including security options, for the region. Refer to the infrastructure audit (as described in our last issue) to determine how well the security infrastructure provides a secure foundation for the application

Your data gathering steps might include:

a) Get list of tranIDs and what each one does

b) Get the security software rules protecting them

c) Verify the security infrastructure

a) List the TransIDs and what they do

For example, a CICS order entry system might have several transactions defined, including:

| TranID | What It Does |
|---|---|
| **OE01** | Display information about a specified customer |
| **OE02** | Display a customer's credit history |
| **OE03** | Enter an order for a customer |
| **OE04** | Cancel an order for a customer |
| **OE05** | Edit information about a specified customer |
| **OE06** | Display sales totals for the entire department for the day. |

b) How Do I Get the Security Software Rules for My Application's Transactions?

Assume that you know for example that the transactions for this application all have names beginning **OE**, and that no other transactions use this naming standard. You want to list the security software rules for all transactions that begin **OE**. You can issue the rule-listing commands yourself or have data center staff issue them for you. It might be best to have the commands issued in batch, so that you have a file of the output which you can process and keep in your working papers. There will be several methods for listing these rules. Here are some of the standard ones, assuming that the security software will be one of: RACF, ACF2, or TopSecret:

*To list the rules for transactions in **RACF***, using the standard SAF class names of TCICSTRN and GCICSTRN:

Use the **SEARCH** command to learn the names of rules whose names start with a given prefix, say **OE** for Order Entry:

```
SEARCH CLASS(TCICSTRN) MASK(OE)

RL TCICSTRN * ALL RESGROUP      and
RL GCICSTRN  xxx ALL
```

(In RACF, TCICSTRN and GCICSTRN are the standard resource class names for CICS transactions. Non-standard names may be in use in any given region.)

*To list them with **ACF2***, using the type **CKC** (which ACF2 mosgt often uses for CICS transactions), issue:

```
ACF
SET RESOURCE(CKC)
DECOMP LIKE(OE-)
END
```

(In ACF2, CKC is the standard resource type for CICS transactions. Non-standard types may be in use in some installations.)

*To list these transaction rules in **Top Secret***, issue:

```
TSS WHOHAS OTRAN(OE-)
```

(In TopSecret, OTRAN [Online Transactions] is the standard resource class for CICS transactions. It is almost always used for online transactions.)

c) Infrastructure Review:

Your infrastructure audit will tell you whether or not your application audit can rely on these assumptions:

- Every signon request to the region is processed by the security software.
- Every transaction request to the region is processed by the security software.
- Security administration for userids, passwords, CICS regions, CICS transactions, and other CICS resources can be relied upon to let only authorized users have access.
- Any resources for this application which need protection (beyond transactions definitions) have been identified, have been defined to the security software, and are protected by means of CICS calling the security software.

Analysis

You want to see who is permitted to execute which transactions within the application, and then to see whether they SHOULD be permitted to those transactions. Interpreting the security software rules is beyond the scope of this article, but is not difficult to learn. Verify your understanding of the facts by asking the security administrator "My analysis of the rules indicates that these people can do these transactions. Could you tell me. Does this look right to you? Have I missed anything? Is there any other way that someone could be permitted to do these transactions?"

Take careful notes during this interview, and thank the administrator for helping you confirm your facts.

Some people may try to tell you that some user should be allowed to execute a given transaction because "he needs it to do his job" or "it's appropriate to his job definition". These are subjective opinions and do not constitute a standard against which you can validate the security rules.

A useable standard to evaluate the security rules will consist of written approvals signed by the business owner of the application, that is, by the person who best understands the associated business risk, and the person responsible for the data. You might want to check as well whether these written approvals include input from the Compliance or Legal departments indicating which if any of these transactions are subject to regulations such as Sarbanes-Oxley or PCI (Payment Card Industry) rules.

If such written approvals do not exist, you may conclude that the application is not auditible because management has not provided a standard against which the security rules can be evaluated. In this case, you might pursue the matter further by interviewing the owner of the application and the Compliance or Legal departments. You might also present in your audit report a simple summary of the security rules, such as "Only staff in the Order Entry department are permitted to execute these transactions." OR "Order Entry staff are permitted to execute these transactions, as are eleven application programmers, three system programmers, and five computer operators." State the facts and allow readers to draw their own conclusions, since your opinion is not objective.

==========

**3) CICS Application Audits: Icing the Cake**

When you have completed the steps described above, you will be in a position to help the financial auditors answer questions such as:

- Can we rely on the numbers?
- Are we protecting the organization's assets?
- Are we in compliance with all laws and regulation?

To give them even more value, you can help them to address financial separation of duties (**SOD**). (For separation of duties relating to security administration, we talk about functions such as APPROVE, EXECUTE, and REVIEW.) The financial duties or functions to consider for SOD might include: INITIATE (a financial action), APPROVE, EXECUTE, RECORD, REVIEW. You would not want one person to be

able to initiate a request to cut a check, then approve his own request, and so on. So consider making a matrix, or an Excel spreadsheet with the application's CICS transaction down the left side, and with userids across the top. Review the description of what each transaction does to determine which financial function does it represent (INITIATE, APPROVE, etc). Label the transactions on the left hand side with **I** for INITIATE, **A** for APPROVE, and so on.

Now below each userid, mark which transactions that user is permitted to execute. Do this by labeling the intersection of the userid and the transaction id with **I**, or **A**, or whatever symbol you use for that transaction's function.

Once the matrix is filled out, you can eyeball it to see if anyone is able to perform more than one of the functions. If so, this may represent a violation of separation of duties, which you would want to review with the financial auditors. They will be interested in what you have to show them.

Of course, if one CICS transaction includes all the functions (INITIATE, APPROVE, etc), that would be of interest as well.

==========
==========

**3) Q and A**

**Q:** What is happening with the ldap backend databases on z/OS?

**A:** First a little background: **ldap** (*lightweight directory access protocol*) is a set of rules for accessing information in a directory of users. It works on all types of computers and is a universally accepted standard. The user definitions in the directory (database) can be used to prove who a user is, and to maintain other information about users.

An ldap server (program) on one computer can communicate, and share user definitions with, other ldap servers on other types of computer.

On Windows, the Active Directory is an ldap database. With z/OS and MVS, IBM gives us an ldap database for free.

On z/OS, the ldap server can pass userids and signons to the security software (RACF, ACF2, or TopSecret) to verify someone's identity (as part of signon, for example). In some cases, the ldap server can perform administration for the security software, for example resetting passwords.

You can see that this may make it possible to integrate all the different UNIX, Windows, and mainframe security, while coordinating it all with the mainframe security software. This can give us single signon with no additional software, using universally accepted standards.

With ldap on z/OS, there are several different ways the database that stores all the information can be configured, along with a new method that combines the others. The standard types of database, or back-end, are:

- **SDBM** uses the security software database as a store (the only one of the three that can do security software administration)
- **TDBM** uses a DB2 database as a store
- **GDBM** uses a DB2 database to maintain a change log

These can be used separately or together. The new approach (which IBM considers to be the way to go) uses yet another back-end named **TDS** (Tivoli Directory Server). TDS can use any or all of the three backends described above.

While there is much more to cover about ldap on z/OS (some planned for future issues), you should be aware of this much, since it will affect your audits. We will likely be seeing much more of ldap, since it helps us to simplify security administration across platforms. This will be more important when we start using IBM's new blade server, which we was described in the last issue. See the IBM manual on Identity Propagation (Section 5B below) to see where this is all going.

## 5) Seminar Information and Miscellanea (Useful Articles, Proverb, Interesting Products)

### 5A) >>>>Seminar Information

**Henderson Group seminars are available for in-house as well as public sessions.**

The Henderson Group offers these "How to Audit..." courses :

- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (November 7-10, 2011 in Clearwater, FL and May 1-4, 2012 in Raleigh, NC)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 11-13, 2012 in Bethesda, MD), a logical follow-on to the previous course

To learn more about them, please go to

**http://www.stuhenderson.com/XAUDTTXT.HTM**

**5B) >>>>Useful Information**

**Three Useful Links:**

**1.** IBM has a new Redbook out in draft form describing how to link security on mainframes to that on distributed systems like Windows and UNIX. To get a free PDF copy of "***End to End Security - z/OS Identity Propagation"***, click on

www.redbooks.ibm.com/redpieces/abstracts/sg247850.html?Open

or go to www.redbooks.ibm.com and enter the following order number in the SEARCH box: ***SG24-7850-00***

**2.** **IBM z/OS glossary:**
http://publib.boulder.ibm.com/infocenter/zos/basics/topic/com.ibm.zglossary.doc/zglossary.pdf

**3.** **To download any or all of the z/OS IBM manuals in pdf format for free:** www.ibm.com/servers/eserver/zseries/zos/bkserv/

**5C) >>>>This Issue's Proverb of the Day**

***"The identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the top-down approach used to identify likely sources of misstatement and the controls to test, as well as to assess risk and allocate audit effort."***

*— SSAE No. 15 (Statement on Standards for Attestation Engagements No. 15 from the AICPA), Paragraph .51*

**5D) >>>>Interesting Products**

While we generally do not recommend or overly criticize software products, we think you will find the following new product of interest:

**DataSniff from Xbridge** is a tool to find sensitive data on your mainframe, so you know what you need to protect. Protecting sensitive data is easy once you know where it is. Finding it is the hard part. DataSniff from Xbridge has just the tool you need to locate sensitive data throughout your z/OS system.. For more info:

Xbridge Systems, Inc., Theresa T. Tama, Regional Sales Manager,
(703) 447-1391, theresa@xbridgesystems.com

.

**5E) >>>>About the Mainframe Audit News; How to Subscribe/Unsubscribe**

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**, **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 **httpd daemon** software which connects a mainframe to the Internet. (Note, we will expand each of these acronyms and explain how the software works over past and future issues.)

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.

To Subscribe, Unsubscribe, or Request Back Issues

Send an email to: **stu@stuhenderson.com** with the subject field set to: MA News and in the body of the email: SUBSCRIBE or UNSUBSCRIBE or BACK ISSUES: 1, 2