**MANEWS 13**

# the Mainframe Audit News

January, 2010 Issue Number 13

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

**Table of Contents**


1) How to Conduct a Mainframe Application Security Audit
2) How to Make Financial Auditors Love You
3) All the Paths Into the System?
4) Seminar Information and Miscellanea
5) About the Mainframe Audit News: How to Subscribe/Unsubscribe


**This issue of the MAN continues describes how to conduct a rapid, effective mainframe application security audit.**

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

## 1) How to Conduct a Mainframe Application Security Audit

The trick to performing an efficient application security audit is to determine and obtain the information you need BEFORE THE AUDIT begins. We assume that you know something about the application being audited. We also assume that the application does not connect to the Internet or intranet, in which case our approach would have to be expanded beyond the scope of this article. Here's what to do:

**Basic Data Gathering**: Find out if the security software is RACF, ACF2, or TopSecret. Find out the naming standard for production datasets. (It might say for example, that *all production datasets have names beginning **PROD.**, and that the second qualifier identifies the application*. So for the **XYZ** application, all datasets might have names beginning ***PROD.XYZ.*** . Once you know the naming standard, request copies of the dataset rules for that application from the security software (RACF, ACF2, or TopSecret).

So you might ask (BEFORE the audit begins), "please get me the dataset rules in RACF for all datasets whose names begin ***PROD.XYZ***.".

If the application is online (has transactions entered at a terminal), find out what middleware is supporting the online component. It will often be CICS or IMS. Find

out the naming standard for online transactions (something like "*All Accounts Payable transactions have names beginning AP, such as AP01, AP02, etc*.". Request copies of the resource rules from RACF, ACF2, or TopSecret for the transactions for your application. These will tell you who is permitted to execute those transactions. Request information on any internal security rules the application software might use. (This would be security rules separate from RACF, ACF2, or TopSecret, sometimes necessary for applications with large numbers of security rules for individual screens and fields.)

Further if the application is online, learn the name of the security software rule that controls who can sign onto that application's middleware. For CICS or IMS, this will often be the name of the CICS or IMS "region" that is the specific copy of the middleware. You might learn for example that the name of the CICS region for production general ledger is "**PRODCICS**". Of course, get a copy of the security software rule. In RACF, this might be an rule named **PRODCICS** in the **APPL** resource class. In ACF2, it might be the **SOURCE** rule for **PRODCICS**. In TopSecret, it might be the **FACILITY** rule named **PRODCICS**. These rules will tell you who is permitted to sign onto the application. Verify that the application does use the security software to verify userids and passwords (as opposed to hard-coded lists of userid and passwords, which would likely lead to an audit finding.)

Even further, if the application is online, request a list of all the transactions with a description of what each one does.

Whether online or batch, there may be a formal risk assessment of the application, its datasets, and its transactions. Some regulations (and sound management practice) require this. Get a copy of the risk assessment if it exists. Determine whether any applicable regulations require it and exactly what they require. Find out if the security administrator has a copy of the risk assessment.

Learn all users of the computer who have privileges that permit them to access any dataset, regardless of the security software rules. For RACF, this will be the users with the **OPERATIONS** attribute. For ACF2, this will be users with **NON-CNCL** or **SECURITY**. For TopSecret, this will be users with **NODSNCHK**.

Learn also (still before the audit actually starts, or at least within 15 minutes of the start) who is the Owner of the application, that is the business unit manager who is responsible for approving access permissions to the application. For example, the head of the Payroll Department might be the Owner of the Payroll application. She is the person who best understands the associated business risks. Get copies of the **signed approvals**, and the **annual re-certification** of the approvals if they exist.

The written approvals and annual re-certification of them will be the **standard you use to evaluate the rules** in the security software. If the written approvals don't exist, or if the Owner isn't formally identified, you might conclude that the application is not auditable, on the grounds that the organization has not defined what "correct" is. In this case, you should inquire if there is any other document that could be used as a standard against which to evaluate the security software rules.

So, now before the audit starts, you have: descriptions of datasets and transactions, security software rules protecting them and controlling access to the application itself, written approvals signed by the Owner, and a copy of the risk assessment, if any.

Set your control objectives, perhaps basing them on the financial audit control objectives and the risk assessment. Develop tests using the information you have collected to address each control objective.

If one control objective is to evaluate the adequacy of control over the ability to read confidential or sensitive information in the Payroll datasets, then your tests might include comparing the security software rules to the written approvals. You will likely conclude that controls are adequate if you can establish a logic chain like this:

> The Owner of the application is identified and made responsible for approvals and may reasonably be considered to understand the associated business risks.
> The security administrator has written approvals signed by the Owner.
> The written approvals seem reasonable in the light of the formal risk assessment.
> The security software rules match the written approvals.
> The number of users with privileges that let them access the data regardless of the security software rules is reasonably small. (If necessary, review the list of such users with the Owner and ask her opinion.)

If any of these links is missing or weak, this will likely lead you to an audit finding. Be sure you describe the finding in terms of actual business or operational risk. Relate it to financial control objectives.

Note that these steps do not rely on opinions, subjective evaluation of "appropriate", nor "consistent with job definitions", all of which could be argued pointlessly until the end of time.

Be sure to review your findings and recommendations in draft form with IT staff. Ask them specifically if there are any compensating controls you may have missed, and whether they believe that your facts are correct. Ask their advice on any needed improvements and give them credit where appropriate.

Note: You may already be required to follow a specific audit methodology. You should have no problem fitting the efficient approach outlined here into your methodology. If there is a problem, ask yourself whether the methodology could be improved by incorporating some of the steps described here.

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

## 2) How to Make the Financial Auditors Love You

Some IT staff have complained that they see no purpose to whatever it is that the IS auditors do, but it takes a lot of their time and energy. To counter this, you can always base your IS audit on the financial audit. Here are some quick steps you can take right now:

a) Ask yourself whether you can quickly list the control objectives for the financial audit, and whether the rest of your team can. If yes, pat yourself on the back. If not, ask the financial auditors to tell you. Ask them also what they expect from the IS audit. If they don't know, describe what you can do for them, and ask them if they are interested. If they are, deliver on it.

b) Show the financial auditors this list of steps and ask them how they feel about them.

c) Map your audit's control objectives to the financial audit's control objectives. If you aren't sure what they are, they likely include these familiar concepts:

Reliability of the numbers (financial, inventory, sales, other)
Protection of assets (including information assets and information processing assets)
Going concern
Compliance with laws and regulations

e) Review your last IS audit report by asking these questions: Do the control objectives match to the financial control objectives? How many of your findings and recommendations are clearly related to the financial control objectives?

f) Review your last audit of the Disaster Recovery Plan or Business Resumption Plan. Did it clearly state whether or not the state of readiness of the data center supports the

concept that the organization is a going concern? Can the financial auditors rely on your audit to address this concept?

g) At the end of your next IS audit, ask the financial auditors if they found your report useful.

h) If IT staff questions your audit, you can state that what you are doing is in response to the financial audit. You can also demonstrate how each of your audit steps relates to the objectives of the financial audit.

:
==========
==========

**3) All the Paths Into the System?**

In earlier issues, we showed that all of mainframe security consists of two parts: the **Trusted Computing Base** (which relies on hardware controls), and the **Q1Q2 mechanisms**. The Q1Q2 mechanism answers the two questions: who is this user? and can he do **x**? This mechanism will always be one of three software packages: RACF, ACF2, or TopSecret.

To address Q1 ("***Who is this user and can he use this system***?") in your audit, you need to determine whether all paths into the system rely on the Q1Q2 mechanism to verify users' identities. (If not, for example, if some software allows users to log on at a terminal using userids and passwords from a hard-coded list, this will almost certainly lead to an audit finding. The risk is that a user terminated for dishonesty for example might have his RACF userid revoked, but still be able to access the system by means of the hard-coded userids and passwords.)

Your audit might inquire whether there is a policy requiring every path into the system to use RACF, ACF2, or TopSecret. Whether or not there is such a policy, you might investigate whether every path is SAF-controlled. To do this, you have to understand all the possible paths into the system. This article describes the paths for you, both batch and online.

Every piece of work (every program in the system) is either **foreground** or **background**. Foreground means **online**, that is, it is connected to a terminal Background means that it is either **batch** or a **started task**, and is not connected to a terminal. (A batch job consists of programs which execute in the background and their dataset definitions. The language used to specify which programs and which datasets

is called **JCL**, or Job Control Language. A started task or started procedure also is defined with JCL. However, it is initiated by means of an operator START command.)

So to summarize, here are the paths into the system. You will need to ensure that your security software controls access through every one of them. To do this you will need to review various settings in the security software, (For example, in RACF the BATCHALLRACF switch listed in the SETR LIST report requires every batch job to have a RACF userid.) We will cover these settings in future issues.

Background Paths (Supported by the JES software)

The **Internal Reader** (for example, the TSO SUBMIT command and the job scheduling software)
**Started Tasks** (initiated by the operator START command at the console or from within a program)
**NJE** (Network Job Entry) and **RJE (**Remote Job Entry) which let other computers submit batch jobs, printouts, and operator commands over SNA and TCP/IP connections. Ask the JES system programmer for a list of these connections and a description of what they connect to.

Online Paths (Supported by the VTAM software)

**TSO** (Time Sharing Option, this is the programmers' workbench)
**USS** (UNIX System Services, this is real UNIX running under MVS on the mainframe)
**CICS** (Customer Information Control System, transaction management software)
**IMS** (Information Management System, database and transaction management software)
**TCP/IP** (real TCP/IP, often connecting the mainframe to the Internet, supports FTP, httpd, and other daemons)
**All Other Applids** (which can be identified from the control file called SYS1.VTAMLST)

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

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

### 4A) >>>>Seminar Information

---

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

How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (May 4-7, 2010 in Raleigh, NC and November 16-19, 2010 in Clearwater, FL)

How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 12-14, 2010 in Bethesda, MD), a logical follow-on to the previous course

(NEW) **Effective FISCAM Audits of Mainframes with z/OS and MVS** (dates and locations to be announced)

To learn more about them, please go to

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

### 4B) >>>>Useful Articles

---

**How to Secure Mainframe FTP** is described in an article at http://zjournal.tcipubs.com/issues/zJ.Dec-Jan08.pdf in the **zJournal**.

**FISCAM** (Federal Information System Controls Audit Manual) documents the approach to be used for IS audits of Federal agencies of the US government: www.gao.gov.new.items/d09232g.pdf

**21 RACF Tips** RACF is of course the security software for mainframe computers (it competes with ACF2 and TopSecret.) The handout from a recent ISACA presentation **"21 Things You Didn't Used to Know About RACF**" is available at:

www.stuhenderson.com/XARTSTXT.HTM

If you are involved in RACF audits, you should take a look. If you're involved in ACF2 or TopSecret audits, then you should look too, since the concepts apply (with different buzzwords) to those software tools as well.

**Tape Security**

To learn more about why tape security requires special efforts, you might want to read this article titled "**Full Tape Security from Security Software and Tape Management Software**": www.stuhenderson.com/TAPESEC1.PDF

**4C) >>>>This Issue's Proverb of the Day**

"*Scope creep? We don't have time to worry about that now*!"

"*Control objectives? We'll make them up when we have to write the report!*"

**4D) >>>>Interesting Products**

While we seldom recommend products, we think the following software product is worth your taking a look to make your own evaluation.

**EKC** has a new product named "**ESSF**" which provides archiving and selective backup of profiles in the RACF database. Profiles may be recovered from the ESSF Dbase, or ANY valid RACF dataset on DASD available on the LPAR where the product executes. Upon Recovery/Restore of USER or GROUP profiles all the appropriate connections to/from groups/users will be automatically (re)set as required. For more info, contact EKC at www.ekcinc.com.

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

## 5) 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, 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 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 for 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 the phrase you want: SUBSCRIBE or UNSUBSCRIBE or BACK ISSUES: 1, 2

---