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

M A News
Mainframe Audit News
February, 2008
Issue Number 09

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

Table of Contents and Introduction to the Mainframe Audit News

1. Introducing the Mainframe Audit News
2. Some Comments About Auditors
3. About the Mainframe Audit News: How to Subscribe/Unsubscribe
4. Seminar Information

1) Introducing the Mainframe Audit News

This is the ninth edition of the Mainframe Audit News, a vehicle for sharing information about auditing IBM mainframe computers. For more information on this newsletter, including how to subscribe or un-subscribe, please see section 3.

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

2) Some Comments About Auditors

We repeat here a slightly edited version of a recent article in the **RACF User News**. (RACF is one of three possible security software packages on the mainframe, the others being ACF2 and TopSecret. For back issues or a free subscription, please go to www.stuhenderson.com). The article was based on an online discussion of "how to deal with auditors".

The technical points are not important for our purpose here. You may ignore them. (If your installation uses ACF2 or TopSecret, those packages have similar, nearly identical technical points, which are still not important for use here.) Rather, the difference between an auditor taking a single item off a checklist and turning it into a complete audit finding and recommendation, as opposed to a "control objective" approach is critical. It is critical both to making our audits more effective, and to

maintaining relations with auditees. (If you are conducting a mainframe audit, the technical points below may also be of use to you.) Here is the article:

"Occasionally, an auditor will take a single point such as "Mixed case passwords are not used. You should require them." and turn that into the entire audit finding/recommendation. This misses two important issues, which are worth raising:

A) Is there some standard that says whether mixed case passwords are required, either a law/regulation or a company standard? If not, then the auditor is just expressing his opinion. It should be treated as that, just one person's opinion, unless the auditor demonstrates why this is important (which leads us to the second issue:)

B) What is the **control objective**, that is the purpose of even looking at the use of mixed case passwords? If the auditor cannot relate the finding to a reasonable control objective, then the auditor has likely failed to show the relevance of the finding. Suppose however that the auditor has stated as a control objective: "Ensure that no unauthorized user can access the computer system." Then, the comment on use of mixed case passwords is just one component of the evaluation of controls. The auditor should also be considering several other findings, such as:

1. What is the minimum password length, and what characters are allowed?

2. How many invalid passwords does it take to revoke a userid?

3. Are the PROTECTED and RESTRICTED user attributes used?

4. Are all paths into the system controlled by RACF (including NJE, RJE, batch jobs, FTP, USS, and every applid)? If a program (applid) has its own hard-coded list of userids and passwords, then for that path into the system, the use of mixed-case passwords in RACF is irrelevant.)

5. Who has read access to ANY copy of the RACF database? (Including tapes, copies sent off site, full pack dumps of disk packs, users with the OPERATIONS attribute, started tasks marked TRUSTED, and others) Anyone who can read the RACF database or its backup could run a password cracker program against it and learn everyone's password. By requiring mixed case passwords, you might make it harder to guess a password, but if it takes 10 hours instead of 3 hours for the cracker program to run, this may not be important.

6. Does the Help Desk reliably verify a caller's identity before resetting a password?

7. Are user's well-trained in how to make passwords "easy to remember, but difficult to guess"?

8. Are pass phrases used? (Or will they be used, once software such as TSO and CICS are able to support them?)

9. What are settings for other password rules, such as password interval, password history, and automatic revoke after x days of inactivity?

All of these points (and several others we don't have room for) contribute to any conclusion as to how well an installation prevents unauthorized users from accessing the system. **Auditing** is defined as "evaluation of the adequacy of controls to achieve some purpose". A c**ontrol** is defined as the "comparison to a standard to achieve some purpose". So if an auditor addresses all these points (each of which can be a comparison to a standard), in order to evaluate how well a specific control objective is achieved, then the auditor is adding value. If an auditor just takes one of these points out of context, and doesn't relate it to a specific objective, then the audit will be less useful.

Unless your installation is clearly in violation of some law/regulation/company policy, an auditor's recommendation can be stated as a practical suggestion, for example:

> *In the light of all the (previously described) controls and the importance of the data on this system, the risk of someone guessing someone else's password seems higher than necessary. To reduce this risk, you should consider tightening the controls (for example by requiring mixed case passwords and by reducing the password interval from 150 to 30 days)*. "

In the light of the above article, you might want to ask yourself at the start and at the end of each audit you conduct, which of the two audit approaches you have followed, and whether you are happy with the result.

3) 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 the next several 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

---

4) >>>>Seminar Information

This issue we describe two seminars for mainframe auditors:

- How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2 and MQ Series Security** (May 5-8, 2008 in Raleigh, NC and November 17-20, 2008 in Clearwater, FL)

- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (May 20-22, 2008 in Bethesda, MD)

To learn more about them, please go to

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