GUIDING AUDITORS TO NAVIGATE THE WORLD OF MAINFRAME SECURITY

"Oh no, the auditors are coming. They don't understand the mainframe, I'm going to have to explain to them again what RACF is." Does this sound familiar? Yet there's nothing to fear: the audit is our friend.

Having worked within an Internal Audit team, I know first-hand what it's like to be an auditor and the valuable work they do. One thing that struck me was the diverse nature of the job. Each year an audit plan is set that is agreed by the audit committee. This plan sets out what entities (e.g. projects, platforms, applications, business initiatives) will be audited. From an auditor's perspective, such a plan could see you being involved with auditing different technologies, processes and so on.

Therein lies one of the main problems: how can you expect someone to retain deep technical knowledge of a platform with such a diverse workload?

The reality is that we should be helping our friends in audit to better understand the control issues on the mainframe, which in turn present risks to the businesses we serve. I have always viewed auditors to be our best friends: they are not an enemy, this is a partnership. Whether you work in Security or Audit, we share a common goal: to help reduce risk.

What you should also realize is that the final report from either an internal or external audit is powerful. It receives attention at board level and is cascaded down the management chain. This is why I enjoyed being on the receiving end of an audit, because I'd happily point out audit concerns that I knew the auditor wouldn't find. Those concerns would typically make it into the auditor's final report and then management was obliged to do something about them.

However, what if you are the auditor, or you are on the receiving end of an audit, and the audit team does not have sufficient knowledge of the mainframe and its various sub systems? The big issue is that weaknesses in controls that present significant risks may go unreported. Suppose you're working in mainframe security and you know about some of these issues but you fail to tell the auditor? If you have a breach because someone exploited a control weakness, how will you explain yourself during an investigation? Ethics comes into play too.

Auditors often need a helping hand to navigate around the mainframe. Remember, their job is to test the effectiveness of controls and report their findings. They will probably have a check list of controls they need to test as part of the audit, but are those tests fit for purpose and do they go far enough?

Here are five tips for people conducting audits, and five tips if you're on the receiving end.

You are an auditor:

- If you are routinely conducting audits that involve the mainframe, it is worth getting some formal technical training. For example, attend a course designed for Auditing the Mainframe. Also attend events with groups such as GSE and SHARE as these provide a wealth of information.
- Ask the auditee if they have a mainframe security product installed that can generate reports, or perform scans of z/OS, RACF, major sub systems to identify exposures and vulnerabilities.
- Use sources such as NIST and ISACA for checklists on testing mainframe controls; the mainframe security audit product will probably have some of these tests built in.
- If you don't have much knowledge of the mainframe, be honest with the auditee and ask them for guidance and to provide whatever information they can on known weaknesses. If you pretend to know what you are talking about, the mainframer will spot you a mile off.
- Consider supplementing your audit with outside help to bring in the skills and knowledge you need. This could be support from a vendor, an external consultant or perhaps bring in an employee on secondment from the IT Department.

You are the auditee:

- Never hide anything from the auditor: if you know the auditor is not skilled enough to find exposures you know about, as a security person you have a duty to report it. Think ethics and remember that auditors and security folk share a common goal: to help reduce risk.
- Explain the backdoors. Often, auditors are testing controls around financial applications but if there is a backdoor (e.g. 5,000 users have update access to APF libraries), the auditor needs to know that the front door locks can be circumvented.
- Show the auditor the mainframe security tools at your disposal to highlight exposures. There will usually be issues that you want to get fixed, which will be of significant interest from a risk perspective.
- Do what you can to translate some of the technical jargon. For example, an auditor might not understand what an APF authorized library is, so explain they are part of the operating system, contain software programs that need to operate in a highly privileged state and, in the wrong hands, can be used to circumvent controls.
- It may be unlikely but if a manager has told you not to tell the auditor anything but you know of weaknesses that increase risk, consider using your employer's "speak up" procedure. Think

ethics.

In conclusion, do not be afraid of the auditors. And auditors, please do not be afraid of the mainframe and the people that run it.

This is a partnership. Security people build and maintain controls, auditors identify and report weaknesses in those controls. Together, you are helping to improve controls and reduce risk. Support one another, share knowledge, get those issues into the report so they get the attention they need from executive and senior management. Remember, for security to be successfully implemented, it requires top down management support.