** A Partial list of manual security compliance processes that we have seen implemented at several of our clients. These are all processes that were replaced and automated using the Policy Minder software.

1. Detecting changes in system values
2. Documenting the system value settings that support or implement the organization's security policy as well as the risk acceptance statements for the system values that couldn't be set to "best practices" or an auditor's preferred setting.
3. Discovering inactive profiles
4. Setting inactive profiles to Status *DISABLED (or changing the password to *NONE or …)
5. Removing (deleting) inactive profiles from the system
6. Discovering new profiles with a special authority, such as *ALLOBJ (seven special authorities – need to report on each)
7. Discovering new members of powerful group profiles such as QSECOFR
8. Looking for profiles with default passwords
9. Making sure users in a particular group or user class are configured correctly (with the right group profile, special authorities, accounting code, initial program/menu, limited capability setting, etc.)
10. Looking for new profiles that have been set to password expiration interval of *NOMAX (meaning that the system will never force a password change)
11. Looking for profiles that are not set to be limited capability profiles
12. Monitoring the security settings on specific files (such as the files containing HIPAA or cardholder data)
13. Monitoring the security settings on specific programs (such as the de-crypt routines that decrypt credit card numbers)
14. Looking for newly created libraries (to take better control of what's happening on the system as well as to ensure that legitimate new libraries are added to the back-up routine and the HA strategy/software)
15. Monitoring the security configuration of a directory containing private information (such as the file that is sent to ADP for payroll processing)
16. Monitoring the authorities to authorization lists securing critical files
17. Monitoring the list of file shares assigned to directories and libraries
18. Looking for new programs that adopt a powerful profile such as QSECOFR or other profiles with *ALLOBJ special authority
19. Monitoring the authority and ownership of source files
20. Monitoring the authority settings of specific commands such as PWRDWNSYS and CRTUSRPRF
21. Detect any change to a specific set of user profiles or to any user profile. For example, detecting a change to a user's group assignment, initial menu, accounting code, job description, etc.

While we understand that some of these processes, when accomplished manually, may take far less than 1.5 hours per week, per system, there are several (6,8,9,10,11,12) that would take more than 1.5 hours per week per system on an average system. Please keep in mind that every system is different in terms of the numbers of libraries, files, profiles, directories etc., which would have to be accounted for in each unique situation, when considering the time required for a manual process. After much discussion we came to the conclusion that 1.5 hours per system, per week, for each compliance process, on average, was most likely legitimate.