NOTICE: This document contains references to Varian. Please note that Varian, Inc. is now part of Agilent Technologies. For more information, go to **www.agilent.com/chem.**

Agilent Technologies

Varian, Inc.
2700 Mitchell Drive
Walnut Creek, CA 94598-1675/USA

Varian Workstation

Access Control and Audit Trail Software

Setup and Documentation Manual

 Printed in the U.S.A. 03-914942-00:3

Table of Contents

Section 1 - Overview

Software alone cannot provide compliance with the regulations on electronic records and electronic signatures (21 CFR 11). Other documentation is needed. This manual provides much of this documentation. It also provides help in creating documentation that the user must provide.

Manual Outline

This manual is divided into 7 sections:

Section 1 is an overview of the manual. It also provides an outline of what the Access Control and Audit Trail software system administrator should do to get the system running correctly.

Section 2 is a description of the factory validation test plan that was used to validate the Access Control and Audit Trail software. (The detailed test plan is in Appendix 1.) The core workstation software including data handling and instrument control for both chromatography and mass spectrometry has been validated previously.

Section 3 is a description of how to validate the software on-site. This includes a validation program that checks each file for changes from the files that were shipped from Varian Inc. There are also some suggested tests that can be done in the field to perform a limited validation on the product. A “mini” test plan is detailed in Appendix 2.

Section 4 is a description of how the Access Control and Audit Trail software helps the user meet the requirements in 21 CFR 11 regulations. A detailed comparison of the functionality of the software to the individual clauses is given in Appendix 3. This table can be used to demonstrate how this software addresses the regulations.

Section 5 contains material that should be written into Standard Operating Procedures (SOPs). These SOPs should standardize the operation of the Access Control and Audit Trail software, as well as how new users are entered and user information updated.

Section 6 contains course material and certification tests that can be used as a self-learning program which a workstation administrator can take in order to learn how the system functions. This can also be used by a trained Varian service representative to teach users how to act as workstation administrators for the Access Control and Audit Trail software. The certification tests and answers are in Appendix 4.

Section 7 is a step-by-step procedure for getting started with the Access Control and Audit Trail software. This takes the user through the initial configuration of a single or multi-workstation system and the entry of all of the relevant data for workstations, instruments, users, groups, and projects. Appendix 5 contains forms to gather the required information.

How to use the Varian Access Control and Audit Trail Manual Set

The Access Control and Audit Trail software is documented in a two-manual set that contains all of the information that you will need to run and administer this software. This software supports both the Varian Star and MS workstations. If you are not familiar with the operation of the type of workstation that you have, please see the workstation manuals and tutorials on the workstation CDs. You do not need to know how to operate the workstations in order to be a workstation administrator for the Access Control and Audit Trail software.

This manual, the Setup and Documentation manual, should be used as a step-by-step guide for getting started with the use of this software option.

The Access Control and Audit Trail Software Operation manual should be used as a reference manual. It describes what each entry means and what the legal inputs are for each entry. If you are uncertain about an entry while going through this manual, please refer to the Operation manual for more information. In addition to detailed information about individual entries, the Operation manual contains the following information:

1. An explanation of the software itself, how it is organized, and how to use it. This information is used as part of the self-learning course that is contained in this manual for the Access Control and Audit Trail software.

2. Definitions of terms used by these manuals.

3. A brief comparison of the Star and MS workstation software that explains how they are similar, how they are different, and how this relates to the Access Control and Audit Trail software.

Section 2 - Factory Validation of Access Control and Audit Trail Software

We have extensively tested the Access Control and Audit Trail software with the Star and MS workstations. This documentation applies to Version 6.30 and above. We have previously validated the operation and calculations of the core software for both the Star and MS workstations. We have included a copy of the software certificate of validation (see page 83) confirming that this software has been fully evaluated. Results from the actual validation are permanently kept at CSB in Walnut Creek, California, U. S. A. A copy of the test plan that was used to validate this software is in Appendix 1. Note: general terms such as workstation and Varian workstation are used in this manual to refer to both the Star and MS workstations.

Section 3 - On site Validation of Varian workstation software including Access Control and Audit Trail Software

This software can be validated on-site and during its operation. Software validation can be divided into three parts: the validation program, validating operation through a test plan, and long-term validation.

The Varian workstation software has a **validate** program that verifies that the checksum of each executable file of the workstation matches the checksum of what was tested in the factory. Each software version has its own unique list of checksums. These checksums are included in a file installed with the workstation. Once the software is installed and any time afterwards, run the **validate** program to check the software (the Validate Installed Files function is available from the 'About box' in all workstation applications, and from the workstation menu under Program Files).

The workstation software itself has procedures, methods and test files to validate its data handling and calculation algorithms. The algorithms used for all calculations in Star software are detailed in the Regulatory Compliance manual on the Star CD. These should be used if it is necessary to validate the calculation software on-site.

Because the Access Control and Audit Trail option for Varian workstation software does not contain any specific data manipulation calculations, it should not be necessary to validate this software at the customer's site. If the customer feels that it is necessary to do some testing on-site, some of the procedures described in the factory validation test plan can be used. However, all of the tests should not be used, as this would be very time consuming. Appendix 2 has a list of the sections of the factory test plan that might be used to do a shortened file validation procedure.

Section 4 – Varian Workstations and 21 CFR 11 Regulations

To make it easier to document that the Access Control and Audit Trail software provides the tools for meeting the requirements outlined in 21 CFR 11, a table that compares the regulations with the capabilities of the software is provided in Appendix 3.

Section 5 - Sample Standard Operating Procedures (SOPs)

The Varian Access Control and Audit Trail software alone cannot meet the FDA requirements for compliance with 21 CFR 11. Laboratory SOPs are needed to insure that the software is used properly. These SOPs fall into two categories: policies and operational procedures. The policies and procedures listed below are those that we suggest should be covered by SOPs. Other SOPs can be written to cover other parts of the software.

Policies

The Access Control and Audit Trail software requires that certain policies be set for compliance with 21 CFR 11 regulations. These policies should be documented in one or more laboratory SOPs so that software functionality is consistent even when different individuals act as administrators. The policies that should be set in SOPs are listed below with explanations.

SOP Policies	**Explanation**
Enable Login Dialog Timeout	This is not required by the regulations. If you do not check the box, the login will stay on the screen until someone makes an entry or presses “Cancel”. This is a matter of preference.
Disable Accounts After Password Tries	This is required by the regulations, so it should be checked.
Password: Retries	This is required by the regulation, but the number of retries is not stated. This should be set to a reasonable number so that, if someone has two or three passwords for different systems, they will not disable their login if they enter the wrong one. Somewhere between 3 and 6 is a good value.
Password: Minimum Length	It is good practice to set a large enough minimum length that someone cannot find out another person’s password by trial and error. However, do not set it so high that users have a hard time figuring out a password that is both long enough and that they can remember. Practically, between 6 and 10 is a good range for this.
Password: Minimum Numeric Characters	This entry is to prevent users from just using their own name as a password. Your own name is too easy for someone to guess. By adding some numbers to the password, it will be harder to guess someone’s password. Practically, 1 to 3 is a good range for this.

SOP Policies	Explanation
Password: Default Expiration (Days)	The regulations require that passwords be protected from aging. Each user must change their password periodically. There is no mention as to how long. 90 days should be a minimum as it would be difficult to keep track of passwords that changed more often than that. 365 days should be a maximum as changing passwords at least once per year would be good. **Note:** this is only a default setting. Individuals could get an individual length for their password expiration by changing the setting on the Users entry page. In general, it is best that each person's password expiration is kept the same.
Application Timeout	The regulations state that the system should prevent someone else from performing activities under another person's login. Without an application timeout, one person could leave the workstation and someone else could use his or her login. Choosing a good application timeout requires an understanding of how the laboratory works. If the workstation is basically used by one person all of the time and they spend a lot of time setting up automated runs etc., then a long timeout such as 600 seconds might be appropriate. If many people use the instrumentation, then a shorter timeout such as 120 seconds would be more appropriate. This application timeout will apply to every workstation on a networked system, so it should be chosen carefully.
Audit Log Warning	A policy should be set as to how often to archive the system log and the security server audit log. The security audit log for the administration software will grow larger initially when the system is first installed. Later it will grow only when individual entries in the security database are changed or when Alarms occur. A size limitation would be best for the security audit log. Once it gets too big (e.g. >1 Mbyte), it should be archived. The system log will grow quickly as work is done in the lab. A time limit for this log would be best. The system log is automatically archived when it reaches its limit, either in time or size.
Archive Folder	The archive folder is the location of the security audit log. If the system is networked, this should be on the workstation that contains the security database.
User Information	The regulations say that each individual using the system must be clearly identified. The best way to do this is to enter some amount of user information beyond the user's name. This user information could include their company identification number, department name or number, job title or role, or other information. The information that is required should be put into an SOP.
The Global Project	Rights on the global project should be carefully assigned, because those rights apply to all projects, all workstations and all instruments. If a user has the right to run samples on the global project, they can do this on any workstation and any instrument in the system. In general, it is good policy to assign rights on a project basis. Only the activities of acting as a system administrator, system maintenance or unlocking private locks must be assigned on the global project.

Procedures

Besides policies, procedures should be set for the lab in order to comply with the regulations. Some of the procedures that are needed are listed below.

Entering a New User

When the system is first installed, and periodically as individuals come to work in the lab, the system administrator will have to add people to the system. The regulation states that the administrator cannot know both the user's login name and password. However, because each person must be clearly identified, the administrator will have to know the user's login name. Therefore, their password must be unknown to the administrator.

There are two ways to do this. One is to create a user name and a standard password. This will always be the same initial password. The user will then be told to go to a workstation, login with their new login name and password, and then change their password. This should be done immediately. This would be good for the initial configuration of the system.

Alternatively, if the new user were present while the administrator was entering them into the security database, they could enter their own password on the Users information page. This is more efficient when new people are being added to an existing system.

Changing the Default Password

When you first log on to the administration software, a default login (Admin) and password (Chrom) are used. That login name cannot be deleted from the system. It is always there as a protection in case the administrator is locked out of the system. However, the default password should not be left as-is because the system will not be secure. The password for the default login should be changed after the first administrator is logged in and has a password. This can be changed to anything that follows the password rules. The password should be written down and secured in a safe location so that, if it has to be used, it is available.

Open Dialog Boxes

If dialog boxes are open when you log out, it is possible for someone else to add or modify the information. You should set a lab SOP that states to close all open dialog boxes.

Section 6 – Access Control and Audit Trail Software Training Materials

Learning about the Varian workstation software before operating it will make operation for the first-time user much easier. If a user is familiar with the operation of Star 5.x software, then the current version will be easy to operate as very little has changed in the core software. You can review the information about what has changed in product release notes and in the Access Control and Audit Trail software Operation manual. If a user has never worked with the Varian workstation software before, then the tutorials on the workstation CDs will be very helpful in getting to know the system. The current MS workstation software has changed more significantly from its previous 5.x versions. If your system will include MS workstations, it is recommended that you familiarize yourself with the new software.

The most significant changes to the operation of the workstation software when it is used with the Access Control and Audit Trail Software are contained in the Security Administration program. For the users of the workstation, these changes are minimal. Their main interaction with the new software will be logging in, working with the method and data file embedded versions, and dealing with private locks. In order to learn to work with these features, they should review the following sections in the Operation manual:

1. Method File Audit Trail
2. Data File Audit Trail
3. Controlling Access to the Workstation Software

Anyone who will act as an administrator of the Access Control and Audit Trail software will need more comprehensive training. Among other things, a workstation administrator will have to learn how to create and modify the security database, how to archive audit logs, how to create new users, groups, workstations, projects and reasons, and how to clear alerts.

In order to gain this understanding, the workstation administrator should take a course either from a Varian representative trained in the software or through the self-learning course listed below. The self-learning course focuses on reading the Operation manual and taking tests on the material. It culminates in the initial preparation for configuring the system for operation and then logging on for the first time. A course from a Varian representative will follow the same approach. The advantage of taking the course from a Varian representative is that the user will have the opportunity to ask questions about the material.

Note: The self-learning course requires that someone other than the person taking the course administer and grade the tests. Because the tests are multiple choice and the answers are given in Appendix 6, the person administering the course does not have to be knowledgeable about the product.

Self - Learning Course

The self-learning course is designed to prepare the system administrator to set up a Varian workstation system with Access Control and Audit Trail software. The course consists of reading assignments and multiple-choice tests. The procedure to take the course is as follows:

1. Make copies of all the tests in Appendix 6 so that the originals are available for subsequent training courses.
2. Read the assigned sections of the manual.
3. Take the test listed in Appendix 4 for that section.

4. Have someone else grade the test using the answer key in Appendix 4.
5. If you got at least 12 of 15 correct (80%), the person grading the test should report which questions you got wrong and what the correct answers were.
6. If you got less the 12 correct (less than 80%), review the material and retake the test. The person administering the course should not report which answers were wrong.
7. Once you have gotten 80% or more correct on any test, go to the next section.
8. Once you have passed a lesson, fill out the score on the form in Appendix 6.
9. When you are done with all of the sections, go to section 7 in this manual and begin setting up your workstation or workstation network. Going through this self-learning course is step 1 of the getting started procedure.

Lesson and test#	**Reading sections**
1	Operation Manual Introduction Software System Description Overview Of Varian Access Control And Audit Trail Software Security Administration Software Overview Of The Security Administration Software The Security Administration Software Policy/Sessions Page
2	Operation Manual Security Administration Software Users Page Groups Page Workstations Page Instruments Page Projects/Reasons Pages Rights Checks Page
3	Operation Manual Workstation Software Comparison Of Star And MS Workstation Software File Security Overview Of Logs Method File Audit Trail Data File Audit Trail Security Server Audit Log System Log Message Log Controlling Access To The Workstation Software
4	Setup And Documentation Manual Section 1 Through Section 5

Section 7 - Getting Started

After the Varian workstation and Access Control and Audit Trail software is installed on one or more PCs, it is necessary to decide how the system will be configured and to set up the security server and database. The following is a step-by-step procedure for doing this. If you follow these steps, the system will operate as you want it to.

There is a series of forms in Appendix 5 to help you organize the information needed to set up the Security Administration program and security database. One type of form will be printouts of actual screens that have been enlarged and modified so that you can hand enter information directly into them. When you enter the information into the system, you can read it directly from the form. An example of this is shown in the figure below:

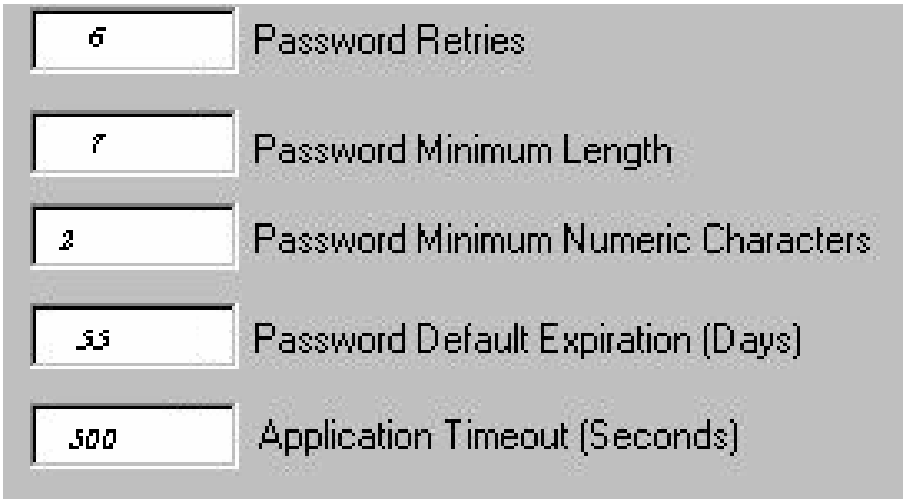


Figure 1 Example of Entering Information into a Screen Form

Another type of form is a table form. This type of form is used when it is necessary to make multiple entries into a section of the software. There are several examples of these in the Appendix.

DO NOT WRITE DIRECTLY ON THE ORIGINAL FORMS. MAKE ENOUGH COPIES OF THESE FORMS SO THAT YOU CAN ENTER ALL OF THE INFORMATION INITIALLY NEEDED FOR THE SYSTEM.

Steps 2 through 11 are decisions that you will want to make BEFORE you enter anything in the security administration software and security database on the workstation. Steps 12 to 25 are the steps that you will take to enter the data that you have created. The order of deciding on the data is different than the order that you will use to enter it into the security server.

Step 1: Take the “Access Control and Audit Trail Software” course. This can either be from the Varian customer support representative who installs your system or through the self-teaching course described in section 7 of this manual. Take all of the tests and have them graded. If you answer at least 80% of the questions correctly, you will be ready to configure the system.

Part 1: Deciding What Entries to Make in the Security Database

Step 2: There are several decisions that you will want to make before you start setting up the security database. The first is most important. If there is only 1 workstation that will be using this software, you will configure the security server, the security database, and the security audit log to be located on that PC. Do this on the Workstations page (Form A) by checking the button for standalone operation.

If you want several workstations to share the same security server, security database and security log, then you will configure one workstation for standalone operation and the other workstations to use a security server by checking the radio button “Use a security server” (Form A). Any workstation can be used as the security server (the workstation configured for standalone operation) as long as it is always powered on and running. The security server does not need to be on a network server although it can be. Once you have configured the workstation that will be used for standalone operation, all of the other workstations should refer to the workstation either by its IP address or by its name on the network.

If you are using a security server on the network, you must make the entries for the initial configuration and setup from this workstation. (After you have done that, you can change the configuration and information in the security database from any other workstation.)

Step 3: You will want to decide on the entries that you will make before you begin configuring the security database. In this way, you can minimize the amount of work necessary to set up the system initially. All of the entries that you make now can be changed later. Some of the entries should be controlled by SOPs for your lab, which are listed in section 5 of this manual “Sample Standard Operating Procedures”. Please review the first section of these SOPs concerning lab policies, in this manual. You can make these entries on Form B. For detailed information about what each Policy entry means, please refer to the Policy page entries of the Operation manual.

Step 4: Once you have set the policies for use of the workstations, you should decide on the workstations, instruments, projects, users and groups that you want to enter initially into the security data base. Workstations and the instruments associated with them should be decided upon first. These are the actual workstations that will acquire information from the security database. They should be given a name to help distinguish them in the laboratory. When samples are run, the name given to the workstation will be permanently attached to the data. Enter all of the workstations that you plan to have configured on this security database on Form C (Workstation and Instrument entry form).

Once you have decided on workstations, you should decide on the names of the individual instruments that will be attached to the workstations. If the workstations are created from the server, 4 default instrument names will be created automatically for each workstation, regardless of whether it is a single- or multi- instrument workstation, or how many instruments actually exist on it. If the workstations are created at the individual PCs, the administration software will detect whether that PC has single- or multi-instrument software, and it will create either 1 or 4 default instrument names respectively. In either case, when you go to the individual workstations, you should delete any “excess” instruments from them.

The names of the instruments will be appended to any data generated on these instruments. The default names, workstation name_1,2,3, or 4, can be used without further modification. However, individual names may help identify the individual instruments in the lab. The instrument names can be entered on the same form as the workstation names.

Step 5: Next you should decide on the projects that will be used in your laboratory. Projects are the way that the security server associates individual users and groups of users with instruments. You create a list of these on the Projects page. You can enter these project names on Form D.

Step 6: After creating the projects, you should associate them with the instruments that you have decided on. One instrument can be associated with any number of projects and any number of instruments can be associated with one project. This is also done on Form D.

Step 7: Once you have created projects, you should add Reasons that are appropriate for your laboratory. You can do this on the Projects/Reasons page. There are preset reasons built into the security server. You can keep these or you can delete them and enter any reasons that you want. A worksheet for the reasons is located in Form E.

Step 8: The next step is to create identities for the individual users who will be using the system. These individual identities will be entered in the Users page. Use Form F as a worksheet for the individual user entries.

Step 9: Once you have created individual users, decide if there are several users that should have the same rights. If you group users together, it can be easier to manage their rights. Use Form G to create groups and add users to them.

Step 10: At this point, you should decide on the rights that individual users and groups of users should receive. Keep in mind that rights are related to users through projects. A user has a particular set of rights for a particular project. If you want a user to have the same rights on all projects, you should assign the rights on the global project. Use Form H to designate the rights for individual users and for groups.

Step 11: Finally, you should decide on a new password for the default login (admin). You should write this down and save it in a secure place. If, for some reason, everyone with administrator rights is deleted from or temporarily disabled on the security server, you will need to log on with the admin login.

Part 2: Entering Information into the Security Database through the Security Administration Software

Once you have completed all of the steps for the initial entry of information into the security database, you are ready to begin entering information. The first to do is log in and create yourself as an administrator user. You then will log out and log back in with your own identity. In this way, the audit trail for the administration software will correctly identify who made the changes to the security database.

Step 12: You should go to the workstation that will be used to hold the security database and log onto the security administration software using the default login name (admin) and the default password (chrom).

Step 13: Go to the Users page and create yourself as a user, enter your password twice, your full name, and give yourself administrator rights. Save this new user and enter an appropriate reason. Close the security administration software.

Step 14: On the workstation, log in using your own identification and password. The first thing you should do is to add any reasons that you had decided to add, especially if you want to use a particular reason while you are initially building the security database. Go to the Reasons page and add the Reasons you added on Form E.

Step 15: On the same page as the Reasons, create the projects that you had previously entered on Form D. You will have to enter a reason for each project.

Step 16: Go to the Workstations page. Since this is the standalone workstation, you will only need to set the location of the workstation security file and the workstation log file. Those were entered on Form A.

Step 17: On the Workstations page, identify by name the workstations that will be on the system. If this is a single-PC system, then there will only be one workstation to identify. If there is more than one PC using the security database, enter the workstation names from Form C.

Step 18: Once you have entered all of the workstations, select the name of the workstation that you are working on and “Apply ID” to it. This will uniquely identify this workstation. Later, you will identify the other workstations in a similar manner.

Step 19: Move to the Instruments page and identify by name the instruments on each of the workstations that you have created. When you created the workstations, default names were created for all of the instruments. If you wish to accept them, then you need do nothing. If you want to change some of them based on the information that you entered into Form C, then do so here.

Step 20: After entering the names of all of the instruments, you will need to associate those instruments with individual projects. Remember that they are automatically associated with the global project. Enter the instrument and project associations that you previously created on Form D.

Step 21: Go to the Policy page and enter the information here that you entered on Form B.

Step 22: Now go to the Users page and begin to enter the individual users as you have created them on Form F. Depending on what SOPs you have set for entering individuals, you may want to enter all of the individuals now and give the users preset passwords that they can change later. Or you may want to have each of the individuals come to you and enter their passwords when you create their identities. After an individual has been created and their information has been entered, you can enter their rights as you set them on Form H.

Step 23: If you have decided to create groups, go to the Groups page and create the groups that you wish to have based on your entries on form G. Then associate the individuals you want in each group, with that group. Once you have done that, give each group the rights on each project that you have previously entered on Form H.

Step 24: Once you have done all of this, you can exit the security server software. If you are only using one workstation, you are finished. If you are using multiple workstations on a network, you will need to go to each of those workstations individually and identify the security server that they will be using. To do this, you will log in to the security administration software on the individual PC using the preset login and password. You will then go to the Workstations Page and select the “Use security server” radio button. Then enter the IP address or the NAME OF THE SECURITY SERVER ON THE NETWORK. This is not necessarily the name that you gave the security server when you created its name in the security server software. It is the name it has on the network. This information can be obtained from the Network Administrator. When you have entered this name, log out of the security server software.

Step 25: Now log in to the workstation on the same PC using your own name and password. If it is not successful, the workstation could not find the security server. See your network administrator for help in making sure that this workstation has access to the workstation that you have designated as the security server. Once you have logged in, go to the Workstations page. On the bottom of the page, select the name that you wish to assign to this workstation. Once you have done that, click on apply ID. An identification number should be applied. Once you have done this for all workstations associated with this security server, you are done with the initial system configuration and ready to run the workstation software.

Appendix 1 – Factory Validation Plan

VARIAN CHROMATOGRAPHY SYSTEMS BUSINESS
LC RESEARCH

M E M O R A N D U M

TO: Distribution
FROM: Gary Burce

DATE: November 28, 2001
MEMO NO.:
SUBJECT: 21 CFR 11 test plan

Overview
Software testing for Star 6.0 will focus on the sections of the code that have changed from Star 5.52. Most of the changes are in the area of access control and audit trails. The actual testing is divided into three parts, user entry testing, operational testing and reliability testing.

In user entry testing, all of the possible entries the can be made to the software will be tested. Most of them will be in the Security Administration section of the software. A wide range of entries will be tested with a focus on the boundary conditions. Where entries interact, their interaction will be tested. (For example, if the security server requires that 10 characters be present in all password, the system will be checked to make sure that no newly entered passwords can contain less than 10 characters.) The persistence of all entries will be tested.

In operational testing, the newly added functions of the Star version 6.0 will be tested. This will include checking to see that access control is working properly, that audit trails are correctly created and that changes to files are correct while the content of previous versions are preserved. This will also involve testing the ancillary functions such as the version comparing software and the audit trail display and archiving software.

In reliability testing, Star 6.0 with the security and access control operating will be tested with all of the other modules running in automation to prove the reliability.

Star 6.0 will be tested and supported using Windows 2000 and Windows NT service pack 6. If possible, minimal testing will be done with Windows NT service pack 4 and Windows 98 although Windows 98 will not support security. Operation with Windows XP will not be tested at this time.

Adobe Acrobat 5.0 will be run at the same time as Star 6.0 in all systems used for testing to simulate how customers will do electronic signatures. Acrobat 4.0 will not be tested.

Documentation and Software Release Procedure

The following procedure will be used with this test plan document:

1. Part, or all of the test plan, will be performed on each release of the software before the final release of software.
2. The part of the test plan used will depend on the individual features available in the software and what has been previously tested.
3. All defects, change requests, comments and observations about the software will be entered into the Tracker database for 21 CFR 11.
4. The change control board will evaluate each entry into Tracker for its seriousness and assign it a P1, P2, or P3 status with P1 meaning “must fix before shipment”, P2 meaning “desirable to fix but not required” and P3 meaning “under consideration for changing in future versions of the software”.
5. When a release candidate is created, all previously found defects listed in Tracker as P1 will be rechecked whether they have been previously listed as repaired or not. In addition, everything in this test plan will be checked on the release candidate. A release candidate will be approved only when all of the test plan is complete and all of the P1 defects have been cleared.
6. When testing a release candidate, all of the entries in this test plan will be signed off and dated by the evaluator, either electronically or manually. A copy of this final test plan is stored in the product documentation for at least 5 years after product obsolescence per CSB procedure.
7. When a release candidate is approved, all P2 issues deemed important by the change control board will be discussed in the release notes.
8. The basic functions of the workstation software that have not changed from the previous version will not be explicitly checked. They will be tested to some extent while running the reliability testing as described below. The core Star and MS workstation software is tested separately from this test plan.

Glossary for the test plan:

NA	Not applicable for this test
Pass	The system should do the required task
Fail	The system should not allow you to do the required task

User Entry Testing

Scope and Purpose

In the user entry testing section, the evaluation will test all of the user entries for the following:

1. Check all inputs to make sure that all valid inputs can be made.
2. Check all inputs to make sure that all invalid inputs are rejected.
3. Check all inputs to make sure that when inputs are made, they are effective.
4. Check all inputs to make sure that they are persistent.
5. Check all inputs to make sure that they cannot be duplicated.

The administration security server is the major change that has extensive user inputs. The user inputs associated with this software will be checked as a separate part of the test plan. All of the other new features have minimal user input changes. These will be checked as part of the operational testing.

Administration Security Server – Policy/Sessions Page

Entry	Range of values	Input tests	Pass Date Name	Function tests	Pass Date Name
Enable Login Dialog Timeout	Yes/No	Check and Uncheck.		Check to see if the login timeout actually works.	
Disable Accounts After "Password Retries" Is Exceeded	Yes/No	Check and Uncheck.		Uncheck box, log in incorrectly set number of times consecutively and unconsecutively.	
Password Retries	1 to 99	Enter valid and invalid numbers.		Uncheck box, log in incorrectly set number of times consecutively and unconsecutively.	
Password Minimum Length	0 to 20	Enter valid and invalid numbers.		Enter valid numbers and test on next page for control of password length.	
Password Minimum Numeric Characters	0 to 20	Enter valid and invalid numbers.		Enter valid numbers and test on next page for control of password length.	
Password Default Expiration (Days)	0 and 1 to 999	Enter valid and invalid numbers.		Enter valid numbers, save changes, change date on computer, make sure password change is prompted x days in advance.	
Application Timeout (Seconds)	0 and 1 – 999	Enter valid and invalid entries.		Make sure that the workstation application timeout at the appropriate time.	
User Information Titles	31 characters	Enter more than 16 characters.		Check boxes on next page for proper prompts.	
Include In Signatures	(Check)	Check and Uncheck.	NA	NA	NA
Security Audit Log Warning Type – Size	On/Off	Click on and off and make sure entries are grayed out.		Make sure audit log is controlled by size.	
Size	1 – 9999 Kbytes	Enter valid and invalid numbers.		Make sure that the warning comes up at the proper size.	
Security Audit Log Warning Type - Date	On/Off	Click on and off and make sure entries are grayed out.		Make sure that the date is used for a warning.	
Number Of Days	1 - 999	Enter valid and invalid numbers.		Make sure that the warning comes up at the proper date.	
Next Archive Number	NA	Make sure that the entry is correct.		NA	NA

Entry	Range of values	Input tests	Pass Date Name	Function tests	Pass Date Name
Archive Folder	Any path and folder up to 260 characters	Make sure that only valid folders are accepted.		Make sure that the archive is really stored in the designated folder.	
Browse For Archive Folder	Click	NA	NA	Make sure you can look for archive folders everywhere.	
Run Audit Maintenance	(Press)	NA	NA	Make sure that the audit maintenance utility is displayed.	
System Log Maintenance -Size	On/Off	NA	NA	Make sure that the system log is archived when its size limit is reached.	
System Log Maintenance – Size Limit	1 to 2550 K Bytes	Make sure only valid numbers are entered.		Make sure that the size limits are applied from the actual size.	
System Log Maintenance - Date	On/Off	NA		Make sure that the date is used for logging the system log.	
System Log Maintenance – Days	1 to 255	Make sure only valid numbers can be entered.		Make sure that the system is backed up on the appropriate day.	
Modify Policy	(Press)	NA	NA	Check accepting and rejecting modifications and see if the policies change.	

Make sure that the Policies page entries are not discarded when the application is exited. **Pass**

Evaluator _____ Date_____

Software version_____

Administration Security Server - Users Page Entries

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Select A User From List	Click on user in list	Click on user.		Check to see the user data appears.	
User Name	1 to 15 characters	Enter more than 16 characters.		Log in with name.	
Password	1-20	Enter previously set values.		Log in with password.	
Repeat Password	1-20	Enter previously set values and different entries.		NA	
Full Name	0 to 18 characters	Enter more than 19 characters.		NA	NA
Last Password Changed Date	Date and time	NA	NA	Check to see this is correct.	
UID	Large number	NA	NA	Make sure number is created and stays with user.	
Password Expiration (Days)	0 and 1 to 999	Enter valid and invalid numbers.		Change dates to make sure account expires in those days. Change dates to make sure that a prompt appears 5 days before the expiration date.	
Current Password Failure Count	0 to 99	Enter valid and invalid numbers.		Make sure that the password count is incremented correctly and that it can be reset from the page.	
Account Enabled	(check)	Check and Uncheck.		Make sure software cannot be accessed when account is disabled.	
Create	(Press)	NA	NA	Make user new user created. Make sure existing users are not affected.	
Modify	(Press)	NA	NA	Make sure existing user is modified and new values are saved.	
Remove	(Press)	NA	NA	Make sure existing user is removed and cannot log in.	
Test Login	(Press)	NA	NA	Make sure any of the logins can be tested.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Information tab					
Specific Information	0 - 31 characters	Enter variety of values with some greater than 31 characters.		Make sure inputs stay with user.	
Other Information	0 - 127 characters	Enter variety of values with some greater than 127 characters.		Make sure inputs stay with user.	
Rights Tab					
Select Project	Project names	Make sure all projects can be accessed.		Make sure rights entered stay with project.	
System					
Workstation Administrator	(Check)	NA	NA	Make sure user can access security server and perform all actions on it.	
Perform System Maintenance	(Check)	NA	NA	Make sure user can upgrade software and save archives.	
Unlock Private Locks	(Check)	NA	NA	Make sure user can unlock private locks but not get into the application.	
Data and Results					
View Data And Results - Chrom	(Check)	Use chrom data handling files and applications if installed.	NA	Make sure that user can display data but not change data. Check in Interactive Graphics, Std and Custom Chrom Report applications, PolyView, and Method Builder (import method).	
Recalculate Data And Save Results - Chrom	(Check)	Use chrom data handling files and applications if installed.	NA	Make sure that user can display and change data but cannot do batch recalculation. Check in Interactive Graphics and PolyView.	
Perform Batch Recalc And Save Results - Chrom	(Check)	Use chrom data handling files and applications if installed.	NA	Make sure user can do all recalculations. Check in System Control.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
View Data And Results - MS	(Check)	Use MS data handling files and applications if installed.	NA	Make sure that user can display data but not change data. Check in MS Data Review, Std and Custom MS Report applications, Method Builder, and MakeMS and BatchSMS.	
Recalculate Data And Save Results - MS	(Check)	Use MS data handling files and applications if installed.	NA	Make sure that user can display and change data but cannot do batch recalculation. Check in MS Data Review normal processing and manual recalculations screens, and MakeSMS and BatchSMS.	
Perform Batch Recalc And Save Results - MS	(Check)	Use MS data handling files and applications if installed.	NA	Make sure user can do all recalculations. Check in System Control and MS Data Review normal processing.	
Methods					
View Methods - Chrom	(Check)	Use chrom data handling files and applications if installed.	NA	Make sure that user can see a method but not modify it. Check in Method Builder, System Control, and Interactive Graphics.	
Modify Methods - Chrom	(Check)	Use chrom data handling files and applications if installed.	NA	Make sure that user can change method and either save it as the same name or to a different name. Check in Method Builder.	
View Methods - MS	(Check)	Use MS data handling files and applications if installed.	NA	Make sure that user can see a method but not modify it. Check in Method Builder, System Control, MS Data Review manual recalculations screens, Active Compound Set Editor.	
Modify Methods - MS	(Check)	Use MS data handling files and applications if installed.	NA	Make sure that user can change method and either save it as the same name or to a different name. Check in Method Builder and MS Data Review manual recalculations screens.	
Delete Methods	(Check)	NA	NA	In Method Builder, check that the Delete Section function offers the option to Delete the whole method when all sections are selected for deletion, if and only if this right is present.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
MS Instrument				Check that this Rights Category is present only for an MS Workstation	
Autotune an MS	(Check)	NA	NA	Check that Autotune can be performed in MS drivers in System Control if and only if this right is present.	
Manually Tune an MS	(Check)	NA	NA	Check that Manual Tuning functions can be performed in MS Drivers in System Control if and only if this right is present. Check that clicking on the various elements of the MS in the 1200 status window only brings up tuning windows if this right is present.	
Execute a 1200MS Macro	(Check)	NA	NA	Check that the fields used to execute macros are accessible in the 1200 Control Window in System Control if and only if this right is enabled.	
Edit a 1200MS Macro	(Check)	NA	NA	Check that the PML editor can only be used to edit files if this right is enabled.	
Instrument					
View Instrument Status	(Check)	NA	NA	Make sure user can see instrument status but not make a run.	
Run Without Standards	(Check)	NA	NA	Make sure user can run samples but not do “C” type runs.	
Run With Standards	(Check)	NA	NA	Make sure user can do all types of runs.	
Change and Configure Instruments	(Check)	NA	NA	Make sure the ability to reconfigure the instruments, (including changing instrument ID) is based on whether or not this right is present.	
Add/Apply Rights	Click	NA	NA	Make sure rights have been changed.	
Remove Rights	Click	NA	NA	Make sure that all rights are removed for the current user for the current project.	
Clear All	Click	NA	NA	Make sure this command unchecks all the rights in the table.	
Set All	Click	NA	NA	Make sure this command checks all the rights in table.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Print User Report	Click	NA	NA	For each user in the database make sure the User Report is printed and accurately represents the rights given to each user in the various projects.	

Make sure that the Users page entries are not discarded when the application is exited. **Pass**

Evaluator _____ Date_____

Software version_____

Groups Page Entries

Entry	Range of Values	Input test	Pass Date Name	Function test	Pass Date Name
Group Name	1 to 15 characters	Type in valid and invalid names.		Make sure all groups can be accessed.	
Groups	All created groups	Make sure all groups in the list can be selected.		NA	NA
Group ID	NA	Make sure that number is present for each group.	NA	NA	NA
User List	All created users	Make sure all users can be selected for as many groups as desired.		NA	NA
Members	All created users	Make sure all members can be selected.		Make sure that all members of a group have the group rights.	
Add Member	(Click)	Make sure selected user is added.		NA	NA
Remove Member	(Click)	Make sure selected user is removed.		NA	NA
Create	(Click)	Make sure that new group is created.		Make sure that rights now apply to group members.	
Modify	(Click)	Make sure that list of members of modified group is modified.		Make sure that the added or removed users have the appropriate rights.	
Remove	(Click)	Make sure that the group is removed.		Make sure that users no longer have rights associated with that group.	

Groups Page Rights Entries

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Select Project	Project names	Make sure all projects can be accessed.		Make sure rights entered stay with project.	
System					
Workstation Administrator	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Perform System Maintenance	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Unlock Private Locks	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Data And Results					
View Data And Results	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Recalc Data And Save Results	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Perform Batch Recalc And Save Results	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Methods					
View Methods	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Modify Methods	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Delete Methods	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
MS Instruments				Check that this Rights Category is present only for an MS Workstation	
Autotune an MS	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Manually Tune an MS	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Execute a 1200 Macro	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Edit a 1200 Macro	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Instruments					
Change And Configure Instruments	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Run Without Standards	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Run With Standards	(Check)	NA	NA	Make sure user has appropriate rights in rights check software.	
Clear All	Click	NA	NA	Make sure no rights are displayed.	

Entry	Range of Values	Input Test	Pass Date Name	Function test	Pass Date Name
Remove Rights	Click	NA	NA	Make sure that all checked rights are removed.	
Add/Apply Rights	Click	Na	NA	Make sure rights have been changed.	

Make sure that the Groups page entries are not discarded when the application is exited. **Pass**

Evaluator _____ Date_____

Software version_____

Workstations Page Entries

Entry	Range	Input Test	Pass Date Name	Function test	Pass Date Name
Use a standalone system workstation	(Check)	Check to see that proper inputs become available.		Run the system from the standalone database.	
Browse Security File	NA	Check to see that you can see security files.		Check to see that you can use different security files.	
Use A Security Server	(Check)	Check to see the proper entries are available.		(This function is evaluated later)	NA
Workstation Name	1 to 15 characters	Create valid and invalid workstation names.		NA	NA
Workstations	NA	NA	NA	Make sure all workstations created are listed here.	
Apply ID		NA	NA	Make sure that all workstations have unique IDs.	
Create WS	(Click)	NA	NA	Make sure that you can access the new workstation.	
Modify WS	(Click)	NA	NA	Make sure that the workstation name and ID have changed.	
Remove WS	(Click)	NA	NA	Make sure that the workstation has been removed.	

Make sure that the Workstations page entries are not discarded when the application is exited. **Pass**

Evaluator _____ Date_____

Software version_____

Instruments Page Entries

Entry	Range	Input Test	Pass Date Name	Function Test	Pass Name Date
Instruments	NA	NA	NA	Make sure all instruments are listed.	
Instrument Name	1 to 15 characters	Make sure that preset names are created for each workstation. Enter valid and invalid names. Make sure that same name cannot apply to two different instruments.		Make sure that the Instrument name is read on the appropriate instrument.	
Workstation	Select from list	Select any of the workstations that are displayed.		Make sure that the actual instrument is correctly identified at the workstation.	
Instrument Number	1 to 4	Select all four entries.		Make sure that two instruments on the same workstation cannot have the same number.	
Create	Click	NA	NA	Make sure that you can access new instrument.	
Modify	Click	NA	NA	Make sure that instrument number has changed.	
Remove	Click	NA	NA	Make sure that the instrument is no longer present.	
Projects	NA	Make sure that all of the projects are displayed and can be selected for an instrument.			
Projects Allowed Access	NA	NA	NA	Make sure that rights assigned to a project are applicable to that instrument.	
Add Project	Click	Make sure project is added to the list.		NA	NA
Remove Project	Click	Make sure project is removed form the list.		NA	NA

Make sure that the Instruments page entries are not discarded when the application is exited. **Pass**

Make sure that single-instrument workstations are handled correctly. **Pass**

Evaluator _____ Date_____

Software version_____

Projects/Reasons Page Entries

Entry	Range of Values	Input test	Pass Date Name	Function test	Pass Date Name
Project Name	1 to 15 characters	Input valid and invalid project names.		Make sure all projects can be selected in the Projects lists on other pages: Users, Groups, Instruments, and Rights Checks.	
Project ID	NA	Make sure all projects have different project numbers and that the Global project has a 0.		Make sure that the project ID is correct in all user/instrument associations.	
Data Directory	Any existing directory 0 – 511 characters	Make sure this is the directory that System Control defaults to for storing data. It should be able to be changed at the user's discretion.		(Checked in other applications)	NA
Browse	Click	NA	NA	Make sure that the button allows the detection of all directories.	
Create	Click	NA	NA	Make sure that new projects are added to list.	
Modify	Click	NA	NA	Make sure that new data directory is associated with the new directory.	
Remove	Click	NA	NA	Make sure that the project has been removed from all user/instrument associations, and Projects lists on other pages.	
Reasons	1 to 78 characters	Check that all characters can be entered.		Check that all reasons are displayed in operation.	

Make sure that the Projects page entries are not discarded when the application is exited. **Pass**

Evaluator _____ Date_____

Software version_____

Rights Checks Page Entries

Entry	Range of Values	Input test	Pass Date Name	Function test	Pass Date Name
User / Project / Instrument	Click to select user from list	Make sure all users are listed here.		Once a user is selected, a list of projects is displayed.	
User / **Project** / Instrument	Click to select project from list	Make sure all projects the user is associated with are displayed		Once a user is selected, a list of instruments is displayed.	NA
User / Project / **Instrument**	Click to select Instrument from list	Make sure all instruments associated with the project are listed here.		Once an instrument is selected, a list of rights is displayed.	NA
Start Over	Click	NA	NA	Restarts the selection process, displaying a list of users.	
Rights	Click on a Right to Trace it.	Make sure Enabled/Disabled state of each right is correct for the current User / Project / Instrument combination.	NA	Make sure Trace information is displayed at the bottom of the window for the selected right.	

Make sure that the Rights page entries are not discarded when the application is exited. **Pass**

Make sure that the Rights for any individual are correct and can be printed. **Pass**

Evaluator _____ Date_____

Software version_____

Operational testing

Scope and Purpose

Operational testing will be done to make sure that newly added features of the system operate as they are described in the product definition, the regulations, the test plan and the operator's manual. It is the job of the evaluator to make sure that the manual matches the actual operation.

Operational testing will be done on both Windows NT, 2000, and XP. The most recent versions of these operating systems should be used. There are no requirements for the system to have instruments attached to it during this testing.

Rights Tests

Scope and Purpose

The user input testing will check whether the administration security server can input the information properly and display it. Operational testing will focus on making sure that the rights assigned to a user apply to the user and that the user cannot get more rights than are assigned.

The following will be tested:

1. Check to see that whatever rights are assigned to a user, they control his access to the system.
2. Check to make sure that all actions requiring reasons will prompt the user for reasons and record reasons accurately.
3. Check to make sure that the user cannot obtain more rights than they are entitled to.
4. The assignments of rights will be checked with the security server configured locally and with it configured on the network.

The operation will be checked while someone is changing rights on the security server.

Rights Test	**Expected Result**	**Pass Date Name**
Method Builder		
Without any method rights		
Try to log into Method Builder	Fail	
Click on the method button on an instrument in System Control	Fail	
Double clock on a method through explorer	Fail	
Select a method from the tool bar	Fail	
Try other ways to get into the Method Builder	Fail	
Chrom Data Handling Only		
Try to get into the Method Builder from Interactive Graphics	Fail	
MS Data Handling Only		
Try to get into the Method Builder from MS Data Review normal processing screen	Fail	
Try to get into the Method Builder from MS Data Review manual recalculations screens	Fail	
With only the rights to view a method		
Log into Method Builder and view any method and any version of a method	Pass	
Try to change a method	Fail	
Chrom Data Handling Only		
Try other approaches to change a method (Interactive Graphics, etc.)	Fail	
MS Data Handling Only		
Try other approaches to change a method. (MS Data Review manual recalculations screens, etc.)	Fail	
With the right to modify a method		
Create new versions of a method	Pass	
Create 20 internal versions of a method and make sure that you can access any of them	Pass	
Create 20 internal versions of a method and make sure that you can run any of them	Pass	
Modify a method and save it as another name	Pass	
Import a method from a data file and save it	Pass	

Modify a method and try to save it as a method that already exists	Fail	
Modify a method that is password protected and try to save it. (without the password)	Fail	
Modify a method that is password protected and try to save it as a different name	Pass	
Modify a method that is password protected and save it as the same using the password	Pass	
With the right to Delete a Method		
In Method Builder, if you request to delete all sections of a method, you are offered the option delete the file	Pass	
No -> File is not deleted	Pass	
Yes -> File is deleted	Pass	
Without the right to Delete a Method		
The above option is not available when deleting all sections of a method.		
MS Data Handling Only		
Import a Compound list and save the method	Pass	
Select a data file to view, calculate Target Ion Ratios from it, and perform local Target Compound integrations	Pass	
Modify a method in MS Data Review manual recalculations and save it	Pass	

Evaluator _____ Date_____

Software version_____

Perform the following tests on data files for chromatography data handling:

Rights Test	**Expected Result**	**Pass Date Name**
Interactive Graphics		
Without any data and results rights		
Try to log into Interactive Graphics	Fail	
Double click on a .RUN file through explorer	Fail	
Select a .RUN file from the Star tool bar	Fail	
Try other ways to get into the Interactive Graphics	Fail	
Try to access Report	Fail	
Try to open a custom report, PolyView, Star Finder and Aurora	Fail	
With the right to view data only		
Log into Reports and display data – also print the report	Pass	
Log into Interactive Graphics and display a chromatogram (several of them)	Pass	
Log into Interactive Graphics and try to recalculate and save a chromatogram	Fail	
Log into custom report writer and view a custom report	Pass	
Log into batch reprocessing and try to recalculate a group of .RUN files	Fail	
Log into System Control and try to recalculate data through a sequence	Fail	
With the rights to recalculate and save results but not to do batch reprocessing		
Log into Interactive Graphics and try to recalculate results	Pass	
Log into Interactive Graphics, display several chromatograms and try to recalculate all of them	Pass	
Log into Report and Custom Report writer and view a chromatogram.	Pass	
Log into PolyView, Aurora, and Star Finder	Pass	
Log into batch printing and try to recalculate a group of .RUN files	Fail	
Log into System Control and try to recalculate data through a sequence	Fail	
With the rights to batch recalculate data.		
Log into Interactive Graphics, Report and Custom report write and do everything	Pass	
Log into Batch reprocessing and reprocess a group of files	Pass	
Log into System Control and batch recalculate data	Pass	

Evaluator _____ Date_____

Software version_____

Perform the following tests on data files for MS data handling:

Rights Test	**Expected Result**	**Pass Date Name**
MS Data Review and related applications		
Without any data and results rights		
Try to log into MS Data Review	Fail	
Double click on a .SMS file through explorer	Fail	
Select a .SMS file from the Star tool bar	Fail	
Try other ways to get into the MS Data Review	Fail	
Try to access Standard MS Report	Fail	
Try to open a Custom MS Report	Fail	
Log into Method Builder, and try to select and view a chromatogram, calculate Target Ion Ratios, and integrate Target Compounds	Fail	
Log into Method Builder, and import a data file method	Pass	
With the right to view data only		
Log into MS Data Review and display a chromatogram (several of them)	Pass	
Log into MS Data Review and recalculate and save the active chromatogram.	Fail	
Log into MS Data Review, do manual recalcs, and try to save them	Fail	
Log into MS Data Review and try to reprocess a recalc list	Fail	
Log into System Control and try to recalculate data through a sequence	Fail	
Log into Std MS Reports and display data – also print the report	Pass	
Log into Custom MS Reports and view a custom report	Pass	
Log into batch printing and print a group of .SMS files	Pass	
Log into Method Builder, and select and view a chromatogram, calculate Target Ion Ratios, and integrate Target Compounds	Pass	
With the rights to recalculate and save results but not to do batch reprocessing		
Log into MS Data Review and try to recalculate and save the active chromatogram	Pass	
Log into MS Data Review, do manual recalculations, and save them	Pass	
Log into MS Data Review and try to reprocess a recalc list	Fail	
Log into System Control and try to recalculate data through a sequence	Fail	
Log into Std and Custom MS Reports and do everything	Pass	
With the rights to batch recalculate data.		
Log into MS Data Review, Std MS Reports and Custom MS Reports, and do everything.	Pass	
Log into System Control and batch recalculate data.	Pass	

Evaluator _____ Date_____

Software version_____

Rights Test	Expected Result	Pass Date Name
System Control		
Without any System Control rights		
Try to log into System Control	Fail	
Try to change from the System Control configuration screen that has been locked to one of the instruments.	Fail	
Try to change from an instrument screen that has been private locked to another instrument	Fail	
With the right to view instrument status		
Log into System Control and try to view instruments	Pass	
Log into System Control and try to change instrument configuration	Fail	
Log into System Control and try to run the instrument	Fail	
With the right to run samples without standards		
Log on and run a single sample (Run all run types except a C type)	Pass	
Log on and run a sample list with all run types except a C type	Pass	
Log on and run a sequence with several different sample lists with all run types except a C type	Pass	
Log on and try to run a single sample with a C type	Fail	
Log on and try to run a sample list with one or more samples – not the first sample- as a C type Should run but not run as a C type	Fail	
Log on and try to run a sample list with all non-C type samples and then suspend automation and add C type runs to the sample list C type should be converted to A type	Fail	
Log on and try to run a sequence with the first sample list having C type samples. Should run but not run a C type run	Fail	
Log on and try to run a sequence with one of the sample lists having a C type run Should run but convert C to A	Fail	
Log on and run a sequence, suspend automation and add a sample list that has a C type run Should convert C to A type.	Fail	
With the right to run samples with standards		
Log on and run a single injection with a C type run	Pass	
Log on and run a sample list with a C type runs	Pass	
Log on and run a sequence with one or more sample lists having C type runs	Pass	
With the right to change instrument configuration and ID.		
With the right to change instrument configuration and ID, try to change the instrument configurations	Pass	
Without the right to change instrument configuration and ID, try to change them	Fail	

Evaluator _____ Date_____

Software version_____

Rights Test	Expected Result	Pass Date Name
System rights		
Without system administrator rights		
Try to log on to the system administration program	Fail	
With system administrator rights		
Run system administration	Pass	
With rights to unlock private lock		
Try to unlock private lock when you have the right to the application	Pass	
Try to unlock private lock when you do not have the right to the application	Pass	

Evaluator _____ Date_____

Software version_____

Perform the following tests on MS Workstation Only

Rights Test	**Expected Result**	**Pass Date Name**
MS Instrument (Check in System Control)		
Without the right to autotune an MS		
Try to perform Autotune for the 2000 MS	Fail	
Try to perform Autotune for the 1200 MS	Fail	
With the right to autotune an MS		
Try to perform Autotune for the 2000 MS	Pass	
Try to perform Autotune for the 1200 MS	Pass	
Without the right to manually Tune an MS		
Try to change the trap multiplier offset for the 2000 MS	Fail	
Click on the picture of the Detector in the 1200 MS Status Display	Nothing	
With the right to manually tune an MS		
Try to change the trap multiplier offset for the 2000 MS	Pass	
Click on the picture of the Detector in the 1200 MS Status Display, then change the detector voltage	Pass	
Right to execute 1200 Macros		
Without this right, try to enter the macro command **?2+2** in the 'Ctrl' field at the bottom of the 1200 control window. Repeat for the 'Proc' field.	Fail	
Repeat with this right enabled. The 'Out' field should display 4		
Without the right to edit 1200 Macros		
Execute Tools->PML Editor command from the 1200 Control Window.	Pass	
Open a PML, try to modify it	Fail	
With the right to edit 1200 Macros		
Modify and save a PML	Pass	

Evaluator _____ Date_____

Software version_____

Administration Security Audit Log

Scope and Purpose

The administration security audit log records all of the actions that an administrator makes using the administration security server software. It also records any alerts such as the repeated failure of a login or the powering down of the PC where the security database is located. These tests will check the following:

1. Check to see that all entries and modifications made to the security database are correctly logged.
2. Check to see that alarm conditions are properly logged and that an administrator is informed when an alarm occurs.
3. Check to see that the information in the security server can be printed out correctly.
4. Check to see that the log can be archived and that a new log is automatically created in the correct manner.

Run this test on the security server both on the network and on the local PC

Administration Security Audit Log Tests	**Expected Result**	**Pass Date Name**
Log accuracy		
Enter a variety of actions in the administration security software, carefully recording (on paper) what you have done Make sure that the log accurately reflects what was done (Attach printout of log and written or typed list)	Pass	
Open a second session and repeat the process Make sure that the new entries are correct.	Pass	
Alarm conditions		
Create alarm conditions and make sure that they are accurately recorded in the log	Pass	
Make sure that the alarms can be cleared from the log maintenance screen	Pass	
Printing the log		
Print the log and make sure that the printout is correct	Pass	
Archiving the log		
Archive the security audit log. Make sure the old log can be read back and that it has the proper starting and ending entries (See Operation manual for these.)	Pass	
After archiving, open the newly created log and make sure that the first entries are correct	Pass	

Evaluator _____ Date_____

Software version_____

Accessing the Security Server from Multiple Workstations

Scope and Propose

When the security server is located on a network, it can be accessed from a variety of workstations. Access from these individual workstations is necessary to configure each workstation in the security server database. Also, administrators can log on from anywhere in the system both for the purpose of modifying the security server database and operating the workstations. This section tests this multi-workstation operation. The evaluation will test network security database operation for the following:

1. Check to see that multiple workstations can be configured on a network server.

2. Check to see that administrators can access the security database from different workstations.

3. Check to see that administrators can work on the same database at the same time safely.

4. Check to see that alarms will be displayed to any administrator who logs onto the network no matter where the alert was generated.

Accessing the Security Database From Multiple Workstations	**Expected Result**	**Pass Date Name**
Configuring multiple PCs		
Configure 5 different PCs on a network and make sure that they keep their proper identity The PCs should be a mixture of MS workstations and Star single- and multiple- instrument workstations	Pass	
Run some operations on each to make sure that the rights assigned to a project can properly conveyed to each PC	Pass	
Accessing the security data base		
Log on as an administrator from each of the 5 PCs and make changes to the security database Check from another PC that they are correct.	Pass	
Log on as an administrator while someone else is already logged on as an administrator Try to make changes in the security database.	Pass	
Accessing alarms from different PCs.		
Create an alarm on one workstation, log in to another workstation as an administrator (in a regular application) and make sure that you are informed about the alarm	Pass	
Create an alarm on one workstation while an administrator is already logged on and see if they are informed of the alarm	Pass	

Evaluator _____ Date_____

Software version_____

System Log and Message Logs

Scope and Purpose

When the system is running, all significant actions on a workstation in the system are logged in two places, the system log and the message log. A message log is associated with each instrument in System Control. When samples are run either individually or as part of automation, a message log is created. This message log (which is present in all of the workstation software versions) contains all of the information about what was done to the samples (methods used, instrument errors etc.). In earlier workstation versions, the message log was overwritten as soon as a new run or sequence of runs was begun. Now, the message log will be permanent. In addition, the message log is coupled with the system log.

The system log is a log that reflects what was done on the entire workstation. This includes things like who logged into which application and when, what they did in that application and when they logged out. A system log is automatically generated on each workstation when the Access Control and Tracking Software is first started. It is continually maintained with no intervention from the user. Message logs are referenced and stored with the system log. After either the size of the system log or the number of days that the system log is active exceeds the limits, it is automatically archived and a new one is created. The last entry in the old system log and the first entry in the new system log will refer to each other, thus maintaining the continuity of the audit. During the evaluation, the following will be tested:

1. Check that the appropriate entries are put into the system log.
2. Check that the appropriate message logs are referenced in the system log.
3. Check that the message log cannot be overwritten.
4. Check that the system log can be archived and a new one started in an appropriate fashion.
5. Check that the system log can be displayed correctly.

System and Message Log Test	**Expected Result**	**Pass Date Name**
Saving information in the system log		
After doing a detailed set of operations, make sure that the system log reflects all of these actions	Pass	
After running 2 or more automation sequences using different login identities, and some manual operations using a third login identity, make sure that all activities are stored in the message log correctly	Pass	
Make sure that the correct message logs are referenced in the system log	Pass	
Preserving the message log		
Make sure that the message logs are not over written when a new automation is started	Pass	
Make sure that a new message log is started when a new automation is started	Pass	
Displaying and archiving the system log		
Make sure that the active system log can be displayed	Pass	
Make sure that the message log can be accessed from the system log and from the log viewer	Pass	
Make sure that when the system log is automatically archived, a new one is created and the appropriate messages put as the last entry of the old and the first entry of the new one	Pass	
Make sure that an archived system log can be displayed and searched	Pass	

Evaluator _____ Date_____

Software version_____

Method Editing

Scope and purpose

The ability to have internal versions of a method has been added to the workstation software. These internal versions allow changes to be made to a method without completely obscuring the original method. The evaluation will test the accuracy and readability of the versioning system by doing the following:

1. Check to see that changes to a method are kept in the newest version of the method.
2. Check to see the older versions of the method can be accessed and run.
3. Check to make sure that the compare software automatically highlights the method changes.
4. Check to make sure that a method can be saved to a new name and have the correct version saved with no other versions present.
5. Check to make sure that the password protection for a method functions correctly.

Method Versioning Test	**Expected Result**	**Pass Date Name**
Internal method versioning		
Build a method and then modify it 10 times. Make sure that all of the versions are correct	Pass	
Run an older version of a method	Pass	
When running an older version of a method, check to see that the proper entries are made in the run log	Pass	
Check to see that when a method is saved to another name, only the current version is saved	Pass	
Try to save a method with the name of a method that already exists	Fail	
Try to save a method that is password protected with a different name	Pass	
Try to save a method that is password protected as the same name when you have the password	Pass	
Make sure that a request for reasons is always asked for when modifying a method and that you must enter a reason or you cannot save the changes	Pass	
Make sure you can exit Method Builder without saving changes and that the method is not changed	Pass	

Evaluator _____ Date_____

Software version_____

Data File Versioning

Scope and purpose

Recalculation of results can be done in several different ways. When results are recalculated, the previous results must be available for review and print, and a reason for the new results calculation must be present. During the evaluation, the following will be checked:

1. Check to see that the changes to the data file are properly recorded.
2. Check to see that the previous version is still readable.
3. Check to see that the software can save a large number of versions.
4. Check to see that you cannot save results without giving a reason for making the changes.
5. Check to see that you can abandon making changes without any changes being made.

Chromatography Data Handling

Result File Versioning Test	**Expected Result**	**Pass Date Name**
Interactive graphics		
Make 10 recalculations and make sure that the changes are properly made in the data file	Pass	
Make sure the previous 9 versions can be read and printed	Pass	
Make sure that you must enter a reason for a change	Pass	
Make sure that you can abandon changes and they are not stored in the data file	Pass	
Display 7 files in Interactive Graphics, recalculate all and make sure that the reason entered is stored in all of the files	Pass	
Standard reports		
Make sure the previous versions can be read and printed	Pass	
Batch reprocessing		
Batch reprocess 10 data files and make sure that they all are changed correctly	Pass	
Make sure that the same reason is put into all of the data files	Pass	
System control		
Batch reprocess 10 data files and make sure that they all are changed correctly	Pass	
Make sure that the same reason is put in all of the data files	Pass	

Evaluator _____ Date_____

Software version_____

MS Data Handling

Result File Versioning Test	Expected Result	Pass Date Name
MS Data Review – normal processing, active data file		
Make 10 recalculations of the active data file and make sure that the changes are properly made in the data file	Pass	
Make sure the previous 9 versions can be read and printed	Pass	
Make sure that you must enter a reason for a change	Pass	
MS Data Review – normal processing, recalc list		
Reprocess a recalc list that contains 10 data files and make sure that they all are changed correctly	Pass	
Make sure that the same reason is put into all of the data files	Pass	
System control		
Batch reprocess 10 data files and make sure that they all are changed correctly	Pass	
Make sure that the same reason is put in all of the data files	Pass	
MS Data Review – manual recalculations		
Make 10 recalculations of the active data file and make sure that the changes are properly made in the data file 1 recalculation is defined as leaving the manual recalculations screens after 1 or more manual recalculations have been performed	Pass	
Make sure the previous 9 versions can be read and printed	Pass	
Make sure that you must enter a reason for a change	Pass	
While doing manual recalculations, make sure that combinations of the following actions are done: a) In the Target Compound screen, re-integrate some compounds after dragging peak events, some after editing the method, and leave some untouched b) In the Unknown Peaks screen, do successive re-integrations after dragging peak events and editing the method When changes are saved upon exiting the manual recalculations screens, make sure that only the last re-integrations done on each peak are saved	Pass	
Make sure that you can abandon changes when leaving the manual recalculations screens and they are not stored in the data file	Pass	
Standard MS reports		
Make sure the previous versions can be read and printed regardless of how they were generated	Pass	

Evaluator _____ Date_____

Software version_____

1200 Macro Versioning

Scope and purpose

The Macros specific to the 1200 instrument now contain an audit trail like the data files and methods. During the evaluation, the following will be checked:

1. Check to see that the changes to the PML file are properly recorded.
2. Check to see that the previous version is still readable.
3. Check to see that the software can save a large number of versions.
4. Check to see that you cannot save results without giving a reason for making the changes.
5. Check to see that you can abandon making changes without any changes being made.

PML Versioning Test ***To be done from an account with the right to modify PMLs***	**Expected Result**	**Pass Date Name**
Open the Editor from Tools->PML Editor… in the 1200 Control Window	Pass	
Create a New PML containing **"Line1";cr;** and save it with rev info	Pass	
Add lines **"Line2";cr;** through **"Line10";cr;** saving it each time with revision info	Pass	
Print the PML and verify that its contents are correct	Pass	
Print the PML Version Info and verify that the revisions are properly documented	Pass	
Exercise the **Open Version** command and check that you can retrieve an older version of the PML	Pass	
Check that you are prompted to save changes if you attempt to exit without changes	Pass	
Check that electing to not save changes preserves the currently saved file.	Pass	

Evaluator _____ Date_____

Software version_____

System Control

Scope and Purpose

The Rights check part of the test plan (above) tests most of the individual and group rights. However, System Control has a number of specific interactions that should be specifically tested. This part of the evaluation will test the following:

1. Check to make sure that rights are apportioned to each instrument correctly when multiple instruments are being run at the same time.

2. Check to make sure that changes made to an instrument's run parameters in System Control are NOT entered into the method.

3. Check to make sure that a user cannot significantly alter the operation of an instrument.

Detailed System Control Rights Interaction Test	**Expected Result**	**Pass Date Name**
Multi Instrument operation		
Log onto one instrument, perform some operations for which you have the rights, then go to another instruments and perform some operations for which you do not have the rights	Fail	
Mixed use operation		
Create a sequence on one instrument that contains injections and recalculations when you do not have the rights to recalculate data. Should skip the recalc when it gets to that point	Fail	
In MS workstations, invoke the MakeMS and Activate (compound table set) utilities as Autolink entries in the sample/recalc lists Also specify the following Sample Types in the lists: Print Calib after a calibration block, and Print Summary at the end	Pass	

Evaluator _____ Date_____

Software version_____

Private and Public Locks

Scope and Purpose

The Varian workstations can accommodate several different operations on one workstation at the same time. Although only 1 person at a time can be logged into a workstation, they can start automated actions and then log out. This allows another individual to log in and perform tasks while the original tasks are continuing. When one person is logged in and they have started a process, they can make sure that no one else can interact with that operation. This is called a private lock. When an operation is private locked, only the person who has locked it and someone authorized to open private locks can open it. When a private lock is opened it becomes a public lock. A public lock can be opened by anyone with the rights to that application. Also, when someone leaves the workstation unattended, the system will automatically public lock. During the evaluation, the following will be checked:

1. Check to see that a public lock is created when an application times out.
2. Check to see that a private lock can be created by the user.
3. Check to see that the private lock status monitor correctly reflects that locked state.
4. Check to see whether a private lock can be opened only by someone who has the right to open private locks.
5. Check to see that someone who can open a private lock cannot access the applications unless they have the rights to use that application.

Private Lock Test	**Expected Result**	**Pass Date Name**
Creating a private lock		
Make sure that a user can private lock the system using the lower tool bar icon	Pass	
In multi-instrument workstations, make sure that each of the instruments in System Control can be private locked and unlocked independently	Pass	
Make sure that if a user tries to log into another application, the system acts like a public lock (must have a login).	Pass	
Timeouts		
Make sure that all applications create a public lock when they time out	Pass	
Make sure that anyone can open the public lock (if they have rights on that application) that was created by a timeout	Pass	
Opening a private lock		
Make sure that the logged in user can open their own private lock	Pass	
Make sure that someone with the right to open private locks can open a private lock but must log in to the application to access it	Pass	
Display of lock information		
Make sure that the lower tool bar icon displays the correct information about the locks	Pass	
Make sure that creating and opening private locks are recorded in the security audit log	Pass	
Make sure that a lock is displayed in each part of System Control when it is locked	Pass	

Evaluator _____ Date_____

Software version_____

Electronic Signatures

Electronic Signatures Test	Expected Result	Pass Date Name
With Adobe Acrobat installed		
Make sure that all print commands can print to distiller	Pass	
Make sure that automated print commands can print to distiller	Pass	

Evaluator _____ Date_____

Software version_____

Required Reasons

Scope and Purpose

Whenever a change is made to a data file, method file, administration file or for many other activities, the change requires a prompt for a reason.

Required Reasons Test	**Expected Result**	**Pass Date Name**
Completeness		
Make sure that all actions that change a method or a data file prompt the user for a reason	Pass	
Make sure that all actions that change the security database prompt the user for a reason	Pass	

Evaluator _____ Date_____

Software version_____

Other Workstation Applications

Scope and Purpose

Chromatography Data Handling

Chromatography Workstation applications such as PolyView, Aurora, Star Report Writer and Star Finder are all controlled by Access Control and Audit Trail software. These applications deal with .RUN files. You need the rights to view data to access them. Whatever file structure (reduced file data with or without raw data) you have created as part a method is not checked, because the method will identify what was done. If you are running 21 CFR 11 software, the ability to manually delete the raw data while keeping only the channel data will be eliminated. Either the raw data will stay in the file or it will go to a backup file. The evaluation will check the following:

1. Check access to other applications using the appropriate rights.

2. Check operation of PolyView using appropriate rights including being logged into the project through which the data was generated.

3. Make sure that the raw data is always saved at least in a backup file.

Note: there are no limitations on the access to Aurora because results cannot be viewed or modified through Aurora.

PolyView Test	**Expected Result**	**Pass Date Name**
PolyView access and operation		
Make sure that you can access PolyView only if you can view data	Fail	
Make sure that you can calculate results only if you have the right to modify results	Fail	
Make sure that if you log on using the global project and you have right to modify data, you can recalculate any file	Pass	
Saving raw data		
Make sure that when you create channel data from PolyView, you must save the raw data either in the file itself or as a backup	Pass	

Evaluator _____ Date_____

Software version_____

MS Data Handling

The following MS workstation applications that deal with .SMS files are all controlled by the Access Control and Audit Trail software. The MS Custom Reports applications that can be optionally installed generate reports from the results that are stored in the data files. They customize the content and format of the reports as appropriate for the target markets, but they do not modify or regenerate the stored results. The MakeMS, MakeSMS, and BatchSMS convert data files between the current .SMS format and the previous .MS format, which is not supported by the AC&AT software. The Active Compound Set Editor and Activate applications maintain and invoke sets that specify which compounds in the method Compound Table are active, i.e., will be processed when the method is executed. The evaluation will check the following:

1. Check access to the applications using the appropriate rights.
2. Check operation of the applications using appropriate rights, including being logged into the project through which the data was generated.

Note: There are no limits to invoking these applications in System Control. This is covered by the ability to access System Control and run Samples or do Batch Reprocessing.

Other MS Applications Tests	**Expected Result**	**Pass Date Name**
Custom MS Reports access and operation		
Make sure that you can access these applications from the workstation applications Toolbar only if you can View Data	Fail	
Make sure that you can perform any operations in these applications once they are accessed	Pass	
MakeMS access and operation		
Make sure that you can access it from the command line and convert 1 or more .SMS files to .MS only if you can View Data	Fail	
Make sure that you can invoke it in System Control as an Autolink entry in the sample/recalc list	Pass	
MakeSMS access and operation		
Make sure that you can access it from the command line and convert 1 or more .MS files to .SMS only if you can Recalc Data	Fail	
BatchSMS access and operation		
Make sure that you can access it from the workstation applications Toolbar only if you can Recalc Data	Fail	
Make sure that you can convert one or more files between .MS and .SMS once BatchSMS is accessed	Pass	
Active Compound Set Editor access and operation		
Make sure that you can access it from the workstation applications Toolbar and open one or more methods only if you can View Methods	Fail	
Make sure that you can perform any operations (create, modify, and delete active compound sets for the method, and apply the current settings to the method) once the active set editor has been accessed	Pass	
Activate access and operation		
Make sure that you can invoke it in System Control as an Autolink entry in the sample/recalc list.	Pass	

Evaluator _____ Date_____

Software version_____

Reliability Testing

Scope and purpose

Reliability testing is done to make sure that the system will run for a long period of time in a fully loaded configuration. The system is tested with many different types of instruments attached. It is tested with different software operating systems. The system will be run in automation with interactions with the system on a periodic basis. The system should not fail for at least 3 days of fully loaded operation for it to pass.

Configuration to run

Four instruments with AutoSamplers attached to the system. Periodic interactions with the system through running recalculation in Interactive Graphics, using Adobe Acrobat to sign files, building new methods and modifying old methods, printing reports, starting a stopping automation, and running the security server.

Operating systems

Windows NT, 2000, XP. Use the most recent versions of these operating systems.

Evaluator _____ Date_____

Software version_____

Appendix 2 – Suggested on Site Validation Procedures for Varian Access Control and Audit Trail Software

The most important aspects of the Varian Access Control and Audit Trail software are its ability to limit access to workstation applications based on the rights given to a user, and its ability to produce accurate audit trails and versions of data files and method files. The table below lists the functions that should be tested and the parts of the test plan listed in Appendix 1 that could be used as a template for on-site validation. The Comments column suggests ways to limit the testing of each function. **Note:** You must have administrator privileges on this system to perform these tests.

Function to test	**Section of test plan to use**	**Comments**
Does the assignment of rights to an individual correctly limit their access to the software functionality	Rights tests	Use only one way to access an application. Do not try all different ways to access an application.
Does the software that creates versions of methods work correctly	Method editing	Check all
Does the software which creates versions of data files work correctly	data file versioning	Check all, for the data file types that are supported by the workstations on the system.
Security Audit Log Functions	As an administrator, after configuring the system for the first time, check the Security Audit Log to make sure that the entries you made are reflected in the log	
System Log Functions	After performing the tests on methods and data files, check the System Log to make sure that the entries appropriate to your testing were entered	

Appendix 3 – Comparison of Varian workstations with Access Control and Audit Trail (AC&AT) software to 21 CFR 11 regulations

Section	Regulation	Varian workstation functions
11.1 (a)	The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.	NA
11.1 (b)	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug and Cosmetic Act and the Public health Service act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	All records created by the workstation are subject to the security system and the audit trail system. Some of them such as the .RUN and .SMS (data) and .MTH (method) files have their own audit trails built in. Others, such as .SMP (sample lists) and .SEQ (sequences) are documented in the external security audit log and workstation system log files.
11.1 (c)	Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 10, 1997.	Electronic signatures generated in 3rd-party software such as Adobe Acrobat can be used to generate signatures.
11.1 (d)	Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with sec 11.2, unless paper records are specifically required.	NA
11.1 (e)	Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	Documentation on operation, validation and compliance is available with every workstation software package. In addition, details of the development of this software may be reviewed at CSB.
11.2 (a)	For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	All files and records in the Varian system can be maintained in a secure manner. They can have electronic signatures attached to them where appropriate through software such as Adobe Acrobat. There will always be a complete record of who used or generated these files and when they were generated and used.

Section	Regulation	Varian workstation functions
11.2 (b)	For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part provided that: 1. The requirements of this part are met; and 2. The document or parts of a document to be submitted have been identified in public docket etc.	NA
11.3(a)	The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.	NA
11.3(b)	The following definitions of terms also apply to this part.	NA
11.3(b1)	The Act means the Federal Food, Drug, and Cosmetic Act (secs 201-903 (21 U. S .C. 321-393))	NA
11.3(b2)	The Agency means the Food and Drug Administration	NA
11.3(b3)	Biometric means a method of verifying an individual's identity based on measurement of the individual's physical features (s) or repeatable actions (s) where those features and/or actions are both unique to the individual and measurable.	The AC&AT software does not support Biometric identification at this time.
11.3(b4)	Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	In most laboratories, the AC&AT system will be considered a closed system.
11.3(b5)	Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.	The workstations uses Adobe Acrobat for digital signatures.
11.3(b6)	Electronic record means any combination of test, graphics, data audio, pictorial or other information representation in digital form, which is created, modified, maintained, archived, retrieved or distributed by a computer system.	Everything in the AC&AT system that is created as a permanent record by the workstation software is covered by the security, user identification, and audit trail features.
11.3(b7)	Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	Adobe Acrobat meets all requirements for electronic signatures.
11.3(b8)	Handwritten signature means the scripted name or legal mark of an individual and executed or adopted with the present intention to authenticate writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is	NA

Section	Regulation	Varian workstation functions
	preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.	
11.3(b9)	Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	The AC&AT system will usually not be considered an open system. This, however, will be dependent on the individual company organization. Compliance with open system requirements will be SOP issues.
11.10	Controls for closed systems. Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	NA
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Results of testing at Varian as well as test procedures to challenge the system are provided as part of the standard package. Each of the security and audit trail features of the system can be tested at the customer's site. Any file that has been changed either has an internal audit trail that can be reviewed for who has changed it and what the change was, or it will be part of an external audit trail. The individual who changed the file and the date of the change is clearly identified. This can be correlated with the security audit log to establish that the individual had authority to make the change. The system will not allow any individuals to make changes who have not been authorized to make those kinds of changes.
	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	All permanent Varian system files can be read on the display and printed on paper through the software itself. They can also be converted into standard formats such as Adobe Acrobat format for reading and printing by universally available software. All audit trails can be viewed and printed. When there is an internal audit trail, each version of the file can be printed individually.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Methods and data files that were created by all earlier versions of Star WS software since its introduction in 1988 can be converted to the current file formats. Similarly, methods and data files that were created by all previous Windows-based versions of MS WS software since its introduction in 1998 can be converted to the current file formats. Previously generated results are not compatible with the current data file

Section	Regulation	Varian workstation functions
		format, and are deleted. Data files that were created by the earlier DOS-based MS software also can be converted to the current format with conversion utility programs that are part of the MS workstation software. The file format conversions happen automatically when the file is opened. The Access Control and Audit Trail software will add protection and will create and maintain an audit trail on the new files. It will also note that the older versions of the files were not created under a protected system. Use of Window NT, 2000, or XP operating systems will limit who is able to move and delete files through the operating system itself.
11.10(d)	Limiting system access to authorized individuals.	The operating system must be Windows NT, 2000, or XP to assure that access to the files through Explorer is controlled. The AC&AT software has a secure login and password system that allows the assignment of selected rights to create, maintain and change files. In addition, these rights can be assigned on a per project/per instrument basis. By using the security server on a network, individual rights to access instruments can apply to all instruments and workstations.
11.10(e)	Use of secure computer generated time stamped audit trails to independently record the date and time of operator entries and actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Data files (.RUN or .SMS) have a built-in audit trail which record the person making the change, the date the change was made, and the nature of the change. The old results and the newly calculated results are both stored in the data file as two different versions. An unlimited number of versions can be created if multiple recalculations are done. The user is prompted to enter a free form reason for the change. Company SOP determines the type of entry that is acceptable for a reason for the change. The data is accessible for as long as the files are accessible. In a similar manner, a method file (so long as it keeps the same name) has a built-in audit trail. A Message Log is created whenever data files are created through the System Control application. This message log records all relevant information about how the data was created, when it was created, and who created it. This log is permanently stored in the archive directory and referenced in the system log. A System Log and a Security Audit Log are continuously created. These record what has happened on the system or in the security database, who performed the actions and when they were done. These are permanent files that are continuously maintained. When they are archived, a new log is immediately created.

Section	Regulation	Varian workstation functions
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Whenever there is a requirement that a sequential set of steps occur, the workstation software performs those steps automatically in the proper sequence.
11.10(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input and output device, alter a record or perform the operation at hand.	Rights are assigned to individuals and groups. These rights can be based on projects or they can be global. They can be specific to instruments. The ability to private and public lock the system is present. In this way, an individual can lock the system and prevent anyone else from intervening in the actions that he/she is performing. A timeout is present for all actions. If no active input from the user has been received for a period of time set in the application timeout entry, the system will automatically public lock to prevent any unauthorized usage. Each creation of a user on the system automatically generates a unique random representation associated with that user. This representation cannot be duplicated even if the same user with all of the same information is created a second time or on a different instrument. When a request for authentication of the user is needed, this representation is used as one of the bases for assessment. The administration function produces an audit trail so that each creation of a system user is completely documented.
11.10(h)	Use of a device (e.g., terminal) checks to determine, as appropriate, the validity of the source of the data input or operational instruction.	The AC&AT system identifies instruments and makes them part of the authentication system. All other devices must be authenticated through the operating system.
11.10(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks.	Documentation on education, training and experience of all Varian employees is preserved at Varian Inc. as part of our ISO 9000 certification. All projects document who is participating in the project. Varian provides tutorials for self-learning of workstation software. Varian provides a training course for administrators and users of the AC&AT and workstation software.
11.10(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	NA – company SOPs
11.10(k)	Use of appropriate controls over system documentation including 1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2. Revision and change control procedures to maintain an audit trail that documents time	Operation manuals are distributed on the workstation software CD. The customer should exercise control over these. The only directly accessible documentation about the system is in system help. Installation of software revisions and updates are logged in the security audit log. Only someone

Section	Regulation	Varian workstation functions
	sequenced development and modification of systems documentation.	with system maintenance rights can perform these actions. These actions may also be limited by the operating system settings.
11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure that authenticity, integrity, and, as appropriate, the confidentiality of electronic records form the point of their creation to the point of their receipt. Such procedures and controls include those identified in Sec 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	NA – All capabilities that relate to closed systems also relate to open systems. The customer must write standard SOPs to account for the mixed use of the system.
11.50	Signature manifestations.	NA
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 1. The printed name of the signer, the date and time when the signature was executed, and 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Done through Adobe Acrobat.
11.50(b)	The items identified in paragraphs a1, a2 and a3 of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)	Done through Adobe Acrobat.
11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Done through Adobe Acrobat.
11.100	General requirements	NA
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Done through Adobe Acrobat.
11.100(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	NA – Related to company SOPs
11.100(c)	Persons using electronic signatures shall, prior to or at the time of such use, verify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding	NA – Related to company SOPs

Section	Regulation	Varian workstation functions
	equivalent of traditional handwritten signatures.	
11.100(c1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations, (HFC-100), 5600 Fisher Lane, Rockville Md. 20857	NA – Related to Company SOPs
11.100(c2)	Personnel using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	NA – Related to company SOPs
11.200	Electronic signature components and controls.	NA
11.200(a)	Electronic signatures that are not based upon biometrics shall *meet the following requirements*	At present there is no provision for Biometric identification of individuals in the AC&AT software. Therefore, the following is not applicable.
11.200(a1)	Employ at least two distinct identification components such as an identification code and password	Done through Adobe Acrobat.
11.200(a1i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components: subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Done through Adobe Acrobat.
11.200(a1ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Done through Adobe Acrobat.
11.200(a2)	Be used only by their genuine owners; and	Done through Adobe Acrobat.
11.200(a3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration by two or more individuals.	Done through Adobe Acrobat.
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	NA
11.300	Controls for identification code/passwords Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	NA

Section	Regulation	Varian workstation functions
11.300(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Done through Adobe Acrobat.
11.300(b)	Ensuring that identification code and password issuances are periodically check, recalled, or revised (e.g. to cover such events as password aging)	Done through Adobe Acrobat.
11.300(c)	Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	NA
11.300(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and as appropriate, to organizational management.	Done through Adobe Acrobat.
11.300(e)	Initial and periodic testing of devices, such as token or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	NA

Appendix 4 – Tests for the Administrator Course for Varian Access Control and Audit Trail Software

This Appendix contains four tests, the answer key, and a sheet for recording the results of the tests for the self-learning course described in Section 6. These tests are also used for the course taught by Varian representatives. Do not write on the material in this section. Copy the tests and a sheet for recording the results of the testing, so that someone else may take the course. The material includes a certificate that should be filled out by the student and the test administrator.

Test for lesson 1

1) What is an implied right?
   a) This is something so basic that everyone is allowed to do it
   b) This is a simple right, like viewing a method that you can do because you have a more all encompassing right like the ability to modify a method
   c) This is a right that you have in the global project
   d) None of the above
2) What is a global project?
   a) A project that is available to everyone
   b) A project that is associated with all instruments
   c) A project that is used only by administrators
   d) None of the above
3) Who can open a private lock?
   a) The person who activated the lock
   b) Any person authorized to use the applications that was locked
   c) Any person authorized to convert a private lock to a public lock
   d) All of the above
   e) A & C
   f) A & B
4) Who can open a public lock?
   a) The person who activated the lock
   b) Any person authorized to use the applications that was locked
   c) Any person authorized to convert a private lock to a public lock.
   d) All of the above
   e) A & C
   f) A & B
5) Does the administrator for the Access Control and Audit Trail software also have to be an administrator for the operating system?
   a) Yes
   b) No
6) What is the default password for logging into the administration software?
   a) Admin
   b) Password
   c) Chrom
   d) (blank)
7) On the Policy page, what is the purpose of the User information titles?
   a) Help remind the administrator what information should be entered for every user
   b) Create the field name on the Users identification page
   c) In a future release of the software, designate what information is printed with an electronic signature
   d) All of the above

8) If the minimum password length is 4 and the minimum number of numeric characters is 5, which of the following is true?
   a) A password with 4 numbers will be accepted
   b) The screen will generate an error when you try to save the new policy
   c) A password with 5 number will be accepted
   d) All of the above
9) Which of the following entries will be rejected by the software on the comments screen for a reason?
   a) (two spaces)
   b) (Enter)
   c) I don't know
   d) None of the above
10) What does the application timeout setting do?
   a) Sets the time that an application will be active without user input before it is private locked and requires another login
   b) Sets the time that an application will be active with or without user input before the application will be private locked and require another login
   c) Sets the time that an application will be active without user input before it is public locked and requires another login
   d) All of the above
11) How does this version of workstation software address electronic signatures?
   a) The capability to add signatures to documents is built into the software
   b) We recommend using Adobe Acrobat
   c) We recommend using Microsoft Word
12) Can an instrument be assigned to two projects?
   a) Yes
   b) No
13) On the Policy page, you can set a reminder to archive the security audit log when it exceeds a certain size. What are the units of that size?
   a) Mbytes
   b) K Bytes
   c) Bytes
   d) Entries
14) What is the maximum time limit for the application timeout?
   a) 120 seconds
   b) 999 seconds
   c) 5 minutes
15) Can the system be set so that applications never time out?
   a) Yes
   b) No

Test for lesson 2

1) Which of the following actions does the right to do system maintenance NOT automatically let you do?
   a) Add or update software in the workstation
   b) Add or update users in the administration software
   c) Fix a file whose audit trail has been corrupted
   d) None of the above
2) If you had five workstations attached to the same network and you wanted to have them all share the same security database, how many of them would you set to standalone operation?
   a) 5
   b) 1
   c) 0
   d) 2
3) When you apply an ID to a workstation that is part of a network, which workstation do you have to make this input from?
   a) The workstation with the security database on its local drive
   b) The workstation that needs to have the ID applied to it
   c) Any workstation
4) How many projects can be associated with one instrument?
   a) 1
   b) 4 at most
   c) Any number
5) What is the effect of associating a project with a data directory?
   a) When you log in with that project, you will ONLY be able to store raw data files in that directory
   b) When you log in with that project, you will ONLY be able to store raw data files in that directory and any subdirectories.
   c) When you log in with that project, you will be prompted to store raw data files in that directory but you will be able to select any directory for actual storage.
6) How many reasons can be entered into the list of reasons?
   a) 10
   b) An unlimited number
   c) 100
   d) 10 times the number of projects entered
7) How soon before a password expires will the system start to remind the user to change their password?
   a) 1 day
   b) 2 days
   c) 5 days
   d) 7 days

8) What page do you use to modify an individual users password expiration time from the system password expiration time?
    a) Policy page
    b) Users page
    c) Groups page
    d) None of the above. All users must have the same password expiration time
9) If a user has the right to run with standards, do they also have the right to run without standards?
    a) Yes
    b) No
10) Can you enter the instrument ID number?
    a) Yes
    b) No
11) Can you enter the instrument name?
    a) Yes
    b) No
12) On the instruments page, which of the following are directly associated with an instrument?
    a) Projects
    b) Users
    c) Groups
    d) Workstations
    e) A and D
    f) B and C
    g) All of the above
13) Can a user be assigned rights on both the global project and other projects?
    a) Yes
    b) No
14) When you are asked for a reason for an entry, can you enter both a preset reason and a free form reason?
    a) Yes
    b) No
15) When you are going to change entries in the security database, do you have to be physically logged into the workstation that has the security database on it?
    a) Yes
    b) No

Test for Lesson 3

1) Which of the following are the files that contain internal versions?
   a) Method file
   b) Sequence file
   c) Sample list file
   d) Data file
   e) All of the above
   f) A and D
   g) A, C and D
2) How can you protect a method from being modified while allowing a new method to be created from that method?
   a) Do not give anyone but yourself the right to modify methods
   b) Password protect existing methods
   c) Do not give anyone but yourself the right to view methods
3) What entry in a method is directly above the Version information in the method section tree display?
   a) Method name
   b) Pump parameters
   c) Method notes
4) Does the “Save As” function create a new version in the method?
   a) Yes
   b) No
5) Where can you select the version of the calculated results that you want to view, in either Interactive Graphics or MS Data Review?
   a) When you first open a data file
   b) On the “File” pull down menu
   c) On the “View” pull down menu
   d) A and C
6) Is a version of the results stored every time that you move a baseline?
   a) Yes
   b) No
7) Is a version of the results stored every time that you do a recalculation?
   a) Yes
   b) No
8) When are you asked for a reason for the change in data processing when you are doing manual recalculations?
   a) When you do the recalculation
   b) When you more the baselines
   c) When you exit Interactive Graphics, or the manual recalculations screens in MS Data Review

9) What are some of the functions that make it possible to tell when an archived System Log has been destroyed or moved to another location?
   a) System logs are no longer sequentially numbered
   b) The time of the last entry in one log does not correspond to the time of the first entry in next log
   c) The person who archived the system log is not the person who created the new system log
   d) All of the above
10) What is the maximum number of versions that can be added to a method?
   a) 10
   b) 25
   c) Unlimited
   d) 99
11) Which of the following actions will NOT be entered into the system log
   a) Creating a new version of a method file
   b) Staring an automated run
   c) Changing the configuration of the instruments
   d) Private locking an instrument in System Control
12) Can you run and collect data using an older version of a method?
   a) Yes
   b) No
13) Can you add versions to a method that was created with an older version of workstation software?
   a) Yes
   b) No
14) How do you know by looking at the System Control screen that an instrument is private locked?
   a) The words “private lock” are displayed in the instrument screen on the configuration screen
   b) A picture of a lock is displayed in the instrument screen on the configuration screen
   c) There is no display until you try to access the instrument itself
15) When the System Log is archived, do you have to create a new log file?
   a) Yes
   b) No, the software automatically creates a new log file

Test for Lesson 4

1) If you are not familiar with the Star or MS workstation, where do you find information about it basic operation?
   a) On the Workstation CD
   b) In the Access Control and Audit Trail software Operation manual
   c) On the Varian Inc. website
   d) All of the above
2) What software validation tool has been shipped with previous Varian Star and MS workstation software versions?
   a) Test plan for testing the workstation software in the customer's lab
   b) Results of our testing the workstation software at CSB
   c) Validate program that compares checksums for workstation files against a standard
   d) All of the above
3) When an administrator adds a user to the system, when should the user enter their password?
   a) The first time that they use the system
   b) When they are specified to do in the laboratory SOP
   c) Immediately after the administrator enters their login name
4) What is the suggested range for the minimum length of a password?
   a) 6 to 10 characters
   b) Anything above 6 characters
   c) An even number of characters
   d) Twice the minimum number of numeric characters
5) If you change the password for the default login name, admin, why must you remember it?
   a) It is the only way for a service person to access the administration software
   b) It is the only way for a service person to update the software
   c) It is the only access to the system if all of the accounts of all of the workstation administrators have been disabled
   d) You will only be able to change the default password by logging in through the default login.
6) What is the first thing that we advise administrators who are new to this software, to do when they are first setting up the software?
   a) Read the manual
   b) Take a training course form the local Varian service person
   c) Take the self-teaching course
   d) Any and all of the above
7) When using a network of workstations sharing the same security database, why do you want to initially make all of the entries on the standalone workstation?
   a) It is easier to do this
   b) The standalone workstation will usually not be in the laboratory
   c) The standalone workstation automatically has the security server database created on it.
   d) The standalone workstation will usually be in a secure location
8) What other information will you enter on the entry form in the Appendix of this manual, when you enter the workstations?
   a) Reasons
   b) Instruments
   c) Users
   d) Users and Groups

9) Can you delete the preset reasons?
   a) Yes
   b) No
10) Where do you associate workstations with projects?
   a) Form D
   b) The Workstations page of the Administration software
   c) The Projects page of the software
   d) Nowhere - you do not directly associate workstations with projects, you only associate instruments with projects
11) When you log into the Administration software for the first time and create your own login name and password, why should you immediately validate the entry and close the software
   a) The location of the security database will be set
   b) So that you can log in as yourself, creating the proper identification in the audit trail
   c) To make sure that the audit trail file is initially created correctly
   d) All of the above
12) What are the advantages of having a new user enter their password immediately after the administrator has created their login name?
   a) There is never a time when a user login name has a password that is known to the administrator
   b) The user will be able to ask the administrator questions about what the best password would be
   c) The identity of the user is confirmed by the administrator
   d) A and B
   e) A and C
   f) B and C
   g) All of the above
13) Why should policies, such as how many incorrect logins will be needed to cause an account to be disabled, be part of the lab SOP?
   a) So that the administrator can justify what they enter to the users
   b) So that the administrator knows exactly what to enter in each column
   c) So the there is consistency in the lab between different administrators
14) Why is this manual in a ring binder rather than spiral bound?
   a) To make the material seem more impressive when a regulator examines the material
   b) To make sure that it stands up on the bookshelf easily
   c) To make it easy to copy the forms in the back
15) Why do you add projects to the system before you add users?
   a) When you give a user rights, you give them rights on a project and those projects must have been built previous to doing this
   b) Adding projects is less complex than adding users so you can get some practice in working with the software before adding users
   c) The Projects page is the first screen displayed when the administration software is accessed

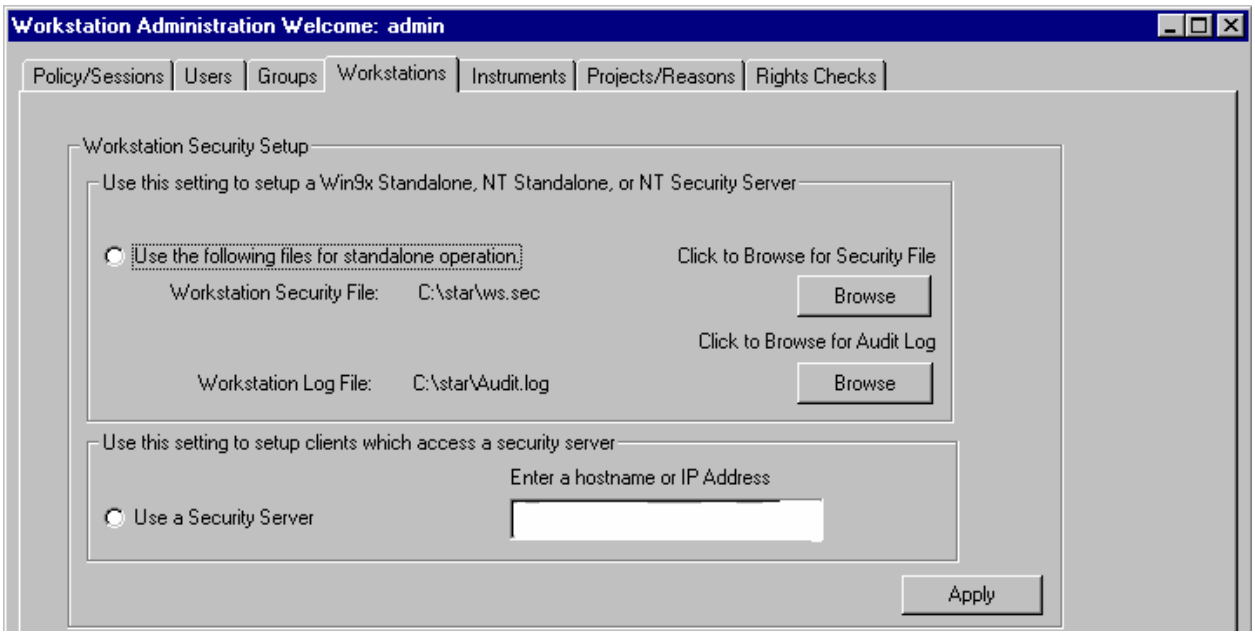
Answers for Tests 1 through 4

Test # / Question #	1	2	3	4
1	B	B	F	A
2	B	B	B	C
3	E	B	C	B
4	F	C	B	A
5	B	C	B	C
6	C	B	B	D
7	D	C	B	C
8	C	B	C	B
9	D	A	D	A
10	C	B	C	D
11	B	A	A	B
12	A	E	A	E
13	B	A	A	C
14	B	A	B	C
15	A	B	B	A

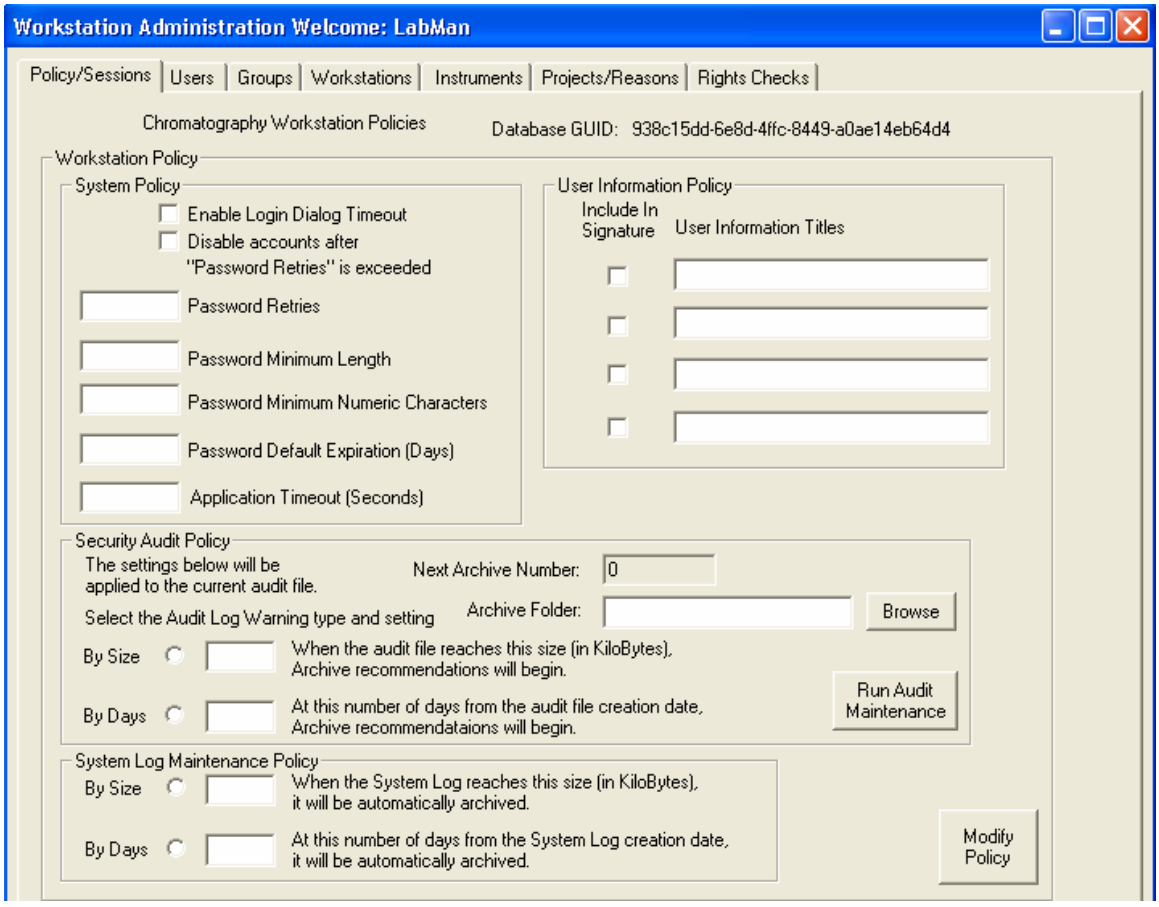
Appendix 5 - Forms for Getting Started to Set-up Security Administration Software

The forms in this section should be used in conjunction with the individual steps in section 7 – Getting Started. These forms allow the user to enter information that will then be put into the security administration software. It is easier to decide on what will be entered before you begin making entries than to do it while you are making the entries. This will allow you to consider the overall plan for the system configuration.

Form A – Selecting the Local Workstation for Standalone or Network Operation.



Form B – Entering Policies Using the Policy Page



Form C – Workstation and Instrument Entry Form

Workstation operating locally and containing the security database and log.

Workstation name	
Instrument 1 name	
Instrument 2 name	
Instrument 3 name	
Instrument 4 name	

Workstations using the security server on the above workstation.

Workstation name			
Instrument 1 name			
Instrument 2 name			
Instrument 3 name			
Instrument 4 name			

Workstation name			
Instrument 1 name			
Instrument 2 name			
Instrument 3 name			
Instrument 4 name			

Workstation name			
Instrument 1 name			
Instrument 2 name			
Instrument 3 name			
Instrument 4 name			

Workstation name			
Instrument 1 name			
Instrument 2 name			
Instrument 3 name			
Instrument 4 name			

Note: Default instrument names are automatically created when a workstation is created. The default names are of the form (Workstation name)_1 to (Workstation name)_4. If you wish to keep the default name, enter **default** in the spaces above.

Note: If all of your workstations are going to operate off of their own security database and server, you can use the network entries on this form to enter their names.

Form D – Project Entry and Instrument Association Form

Enter the project along the top row and the Instruments below each project.

Project Instrument				

Projects Instruments				

Projects Instruments				

Form E – Reason Entry Form

The first 10 reasons are reasons preset in the Security Administration software. These may be deleted if desired.

Incorrect baseline assignment
Incorrect peak assignment
Initial system setup
Methods development
Method validation
New instrumentation added to the system
New project
New user added to organization
User assignment changed
User left organization

Form F – Individual user information Entry Form

Enter the user information titles that you entered on Form B in the Policy page in rows 1 – 4, and then enter the appropriate information for each user.

User login name			
Use full name			
Individual password expiration date			
1			
2			
3			
4			

User login name			
Use full name			
Individual password expiration date			
1			
2			
3			
4			

User login name			
Use full name			
Individual password expiration date			
1			
2			
3			
4			

Form G – User Groups

Use this to group individual users (created using Form F).

Group **Users**			

Group **Users**			

Group **Users**			

Form H – User or Groups/Project Rights Entry Form

Note: Rights granted in the Global project will apply to all projects with which a user is associated.

User or Group				
Project				
System				
Administrator				
System maintenance				
Unlock private locks				
Data and Results				
View data				
Recalc data				
Batch recalc				
Sign/Approve				
Methods				
View				
Modify				
Delete				
MS Instrument				
AutoTune an MS				
Manually Tune an MS				
Exec. 1200MS Macros				
Edit 1200MS Macros				
Instrument				
View Status				
Configure				
Run without standards				
Run with standards				

Software Certificate of Compliance

Varian Chromatography Systems certifies that its Star and Saturn workstation software products are defined, designed, tested and manufactured according to its Quality System procedures. Our Quality System has received ISO 9001 certification number FM21797.

Software development follows the life cycle approach. Market and scientific research leads to a formal Product Definition. The Product Definition is used to produce System Functional Requirements and Software Requirement Specifications documents. The Software Requirement Specifications are then used to design the software. The software is tested against the Product Definition and the Software Requirement Specifications.

Each product has a formal written Test Plan. The Test Plan identifies specific tests to be performed and the acceptable results that must be achieved. The Test Plan verifies that the software performs as defined in the Product Definition, including all algorithms and computations. All or portions of the Test Plan are executed at various points in the development process to determine the product's compliance with the Requirements documents. The entire Test Plan is always executed on the final software version. All significant deviations from the Product Definition that are found in the final software version are either corrected or are documented in the Release Notes supplied with the product. The Test Plan and the test results for the final software version released as the product are maintained in the Quality Documentation archived for each product.

Varian Chromatography Systems will make its software documentation for Star and Saturn workstations available for inspection at its Walnut Creek facility as required by government regulations.

This Software Certificate of Compliance is not a warranty nor is it intended to be in lieu of any government-mandated testing requirements applicable to specific customer uses of equipment or software. Warranties on Varian software products are expressly in lieu of and exclude all other expressed or implied warranties, including but not limited to warranties of merchantability and of fitness for a particular purpose, use or application, and all other obligations or liabilities on the part of Varian, unless such other warranties, obligations or liabilities are expressly agreed to in writing by Varian.