Mainframe Infosec Compliance: What is It and How Does It Benefit Me?

Stu Henderson
The Henderson Group
5702 Newington Road
Bethesda, MD 20816
(301) 229-7187
www.stuhenderson.com

Abstract:

Many organizations have not been able to demonstrate that they have effective compliance management. In this session Stu Henderson describes what compliance management is, the factors determining its success or failure, and what you can do to benefit from an effective compliance management. His recommendations address relevant changes in technology, regulation, and tools, as well as organizational and procedural issues. Stu's recommendations are based on over a decade of observing real-life mainframe security practices, and the factors blocking their effectiveness. Whether you are a CISO, mainframe auditor, or the person responsible for regulatory compliance, you all face the challenge of providing effective compliance management. In this article, you will learn useful steps you can take to improve the quality of your compliance and your ability to demonstrate it to your peers.

What is Compliance Management?

We make policy and standards to protect ourselves, and we manage our compliance to them in order to know how well we are following them. For computer security, these policies serve to protect our information and information processing capability. Given the ongoing publicity about various computer breaches, one might conclude that for many organizations either that the policies are inadequate or that the data centers are not in compliance with them.

To have effective compliance management, you need both effective policies and standards, and effective means to manage compliance to them. This paper will show you how to address both for mainframe information security

Effective compliance means going beyond just checking the boxes off a checklist. It means using policies and compliance management to provide effective security and to be able to demonstrate it to others.

The application economy requires a unified security approach that covers whole business exposed.

Policy versus Standards

Policy is higher level, while standards are more detailed. Policy involves assignment of responsibility and authority and provides for the creation of the detailed standards to provide effective security.

What Does a Good Policy Look Like

To illustrate with a counter-example, consider an auditor's recommendation that "the security administrator should review the violations report every day.". It is not clear why he or she should do this. The administrator does not have the authority to do anything about any violation. We don't know who is responsible should there be a security breach. We may be missing important things that are happening. ("Doesn't the violations report tell us when the security is working?") We may be missing out on trends that are occurring gradually over time. There is no standard of what a "good" or "acceptable" or "improper" violation looks like.

An effective policy might state that:

- In order to prevent unauthorized salary changes and to protect employees' confidential data, no one is allowed to access the Payroll datasets without the written authority of the Payroll manager
- The security administrator has the authority and responsibility to implement rules that permit access to Payroll data only to users approved by the Payroll manager
- The security administrator is responsible for monitoring improper access attempts against the Payroll data and reporting them both to the Payroll manager and to the supervisor of the violator
- The auditor is responsible for reviewing the security software rules to verify that they match the written approvals from the Payroll manager.

This clarifies the purpose, states who is responsible for what, grants authority to carry out the functions, ensures that the access approval decision is made by the right manager, and specifies what a violation is,

Common Problems With Policies

Often policies don't address every area of information security or remain at a high level without providing sufficiently detailed standards and baselines.

Often, no one is clearly responsible for various information security decisions, with the result that they don't get made, or get made for convenience without input from those who best understand the associated risk.

Often tools meant to report on compliance do not address all relevant topics, or produce such a large volume of data that reporting becomes meaningless.

Often, we don't know what it is that we don't know, so it doesn't get addressed in the policy.

How to Make Better Policies and Standards

Get input from your Legal and Compliance Departments. They should be able to provide you with descriptions of all relevant laws and regulations. Refer to the laws and regulations in your policy.

Ideally you can convince these departments to review the contents of every dataset in your shop to determine which ones might contain sensitive data. If they don't give you this support, you may want an automated tool. Such tools can scan all your datasets (and perhaps even parts of disk drives where data still resides after the dataset is erased), looking for data that fits the patterns of social security numbers, credit card numbers, and so on. This can help you identify data that needs additional security and regulatory protection [Carla, a screen shot here?].

Use the STIGs ("***Security Technical Information Guides***", please see links at end of this article). These are developed by the Federal government, with a separate document for each type of computer. They provide detailed suggestions for things to consider when setting security standards. You may not agree with everything in them. However, reading what they cover will help you to be sure that you are addressing every area you need to in your policy and standards.

Do the same with government developed guides such as NIST Special Publication 800-53 "***Security and Privacy Controls for Federal Information Systems and Organizations***". (Please see links at end of this article.) Use this as a guide for policy completeness.

List every configuration file for every software package on your systems. (This includes the parmlibs for MVS.) List every option and privilege in the security software, as well as every resource class. Make sure that your policy makes someone responsible for deciding which of these to use and how. Make sure that these decisions are documented.

This document is often called a "baseline", since it details the basic settings for that software in your installation. This is a useful to give to auditors, so they take less of your time asking detailed questions. It also is useful if you have staff turnover. Even if the one person who is familiar with the software should retire, you at least have documentation of how and why its options were set.

Finally, the task of documenting baselines is an excellent way to groom new staff just out of college. This work will help them to become familiar with the various software options, and to develop good working relations with key system programmers.

Review the list of areas you may not be familiar with (provided below under "What We Don't Know That We Don't Know") to see if you need to consider any of them in your policy.

Make sure that your policy and standards are all based on information from all the appropriate sources. Decisions such as the granting of security privileges, activation of encryption, and use of security software features should not be made by system programmers alone.

Basic Requirements for Effective InfoSec Policy and Standards

Breadth (Does it cover all the areas it needs to cover?)

- Are all the standard areas covered?
- What areas do we not know that we need to know?

Depth (Is compliance measureable?)

- Someone responsible?
- Sufficient detail to determine whether standards are being met?
- Effective tools to enforce and to monitor?
- Based on knowledgeable sources?

Why Automate

We all know that on the mainframe, the volume of data describing all security related events would be too great for anyone to manage manually. As we develop the different data sources, processing, and types of output for compliance management, it will be clear that automated tools will be necessary. The complexity of mainframe technology (from Supervisor State to digital certificates to tape labels to http and ftp daemons to DB2 and beyond) adds to the difficulty of having it all addressed manually.

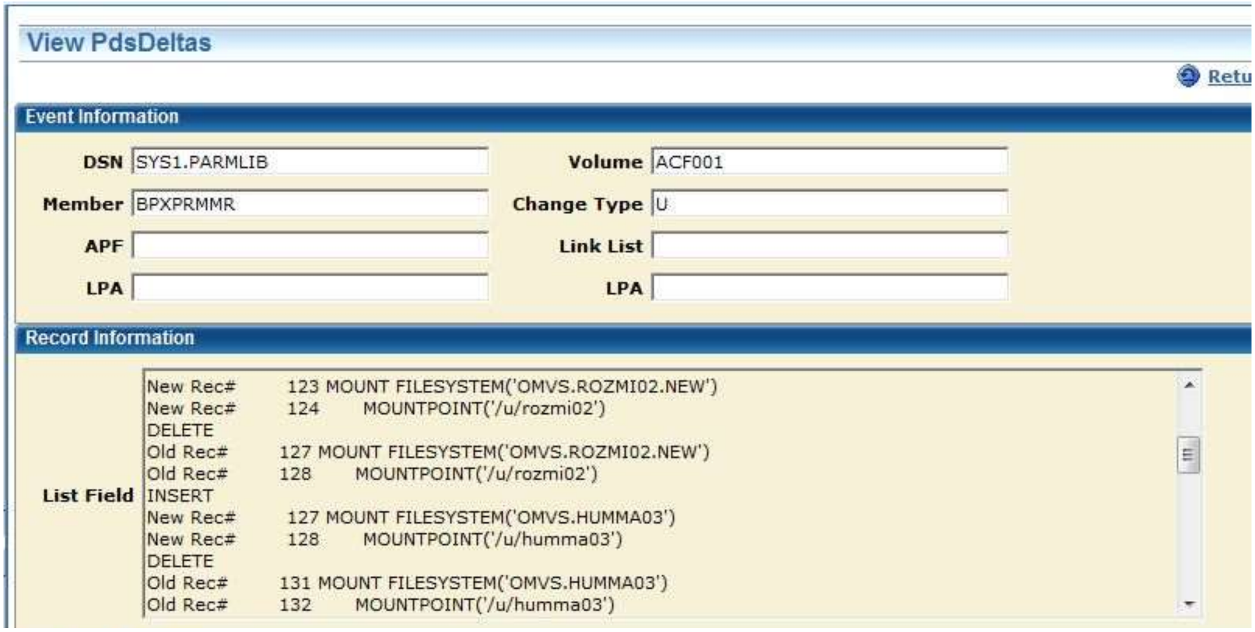
The Process

Compliance, by definition, implies comparison to some standard. Effective compliance management will ensure that the standards are clear, meaningful, and capable of measurement. For example, to say the users should be granted certain powerful privileges in the security software "based upon their job definitions" is not clear. Saying that "only system programmers and other appropriate personnel" should have the privileges would not be meaningful, nor capable of measurement. A more effective standard might be "No user is to have this privilege without the written approval of the CIO.". This is clear and meaningful, and measureable. It has the added benefits of flexibility and independent approval.

To automate compliance management, both the standard and the actual reality have to readily computer-readable.

This data all needs to be processed in a variety of ways: listings, warnings, trend analysis, exception reporting, "top ten" lists, comparison to standards, dataset access versus member level access, and more.

Imagine for example a compliance management process that identifies only that "Sam the system programmer updated SYS1.PARMLIB". Now compare this to "Sam the system programmer updated the PROG25 member of SYS1.PARMLIB, along with before and after images of the member and the fact that there was no change ticket authorizing a change to that member.



View PdsDeltas

Event Information

DSN	SYS1.PARMLIB	Volume	ACF001
Member	BPXPRMMR	Change Type	U
APF		Link List	
LPA		LPA	

Record Information

List Field

```
New Rec#     123 MOUNT FILESYSTEM('OMVS.ROZMI02.NEW')
New Rec#     124       MOUNTPOINT('/u/rozmi02')
DELETE
Old Rec#    127 MOUNT FILESYSTEM('OMVS.ROZMI02.NEW')
Old Rec#    128       MOUNTPOINT('/u/rozmi02')
INSERT
New Rec#     127 MOUNT FILESYSTEM('OMVS.HUMMA03')
New Rec#     128       MOUNTPOINT('/u/humma03')
DELETE
Old Rec#    131 MOUNT FILESYSTEM('OMVS.HUMMA03')
Old Rec#    132       MOUNTPOINT('/u/humma03')
```

Example of screen shot illustrating view of changes

(We have illustrated compliance management functions with examples from **CA Chorus for Security and Compliance Management**). Thanks to **CA Technologies** for providing the sample screenshots.).

To illustrate the creative possibilities for compliance management processing consider a further example. Imagine a compliance management tool that notified you of a ten-fold increase in the volume of data being downloaded from your mainframe via FTP. (At least one well publicized breach might have been cut off had IT management been aware of this fact.)

In short, the processing provided by automated tools has to be very flexible in evaluating a large number of actual events against numerous standards and trends.

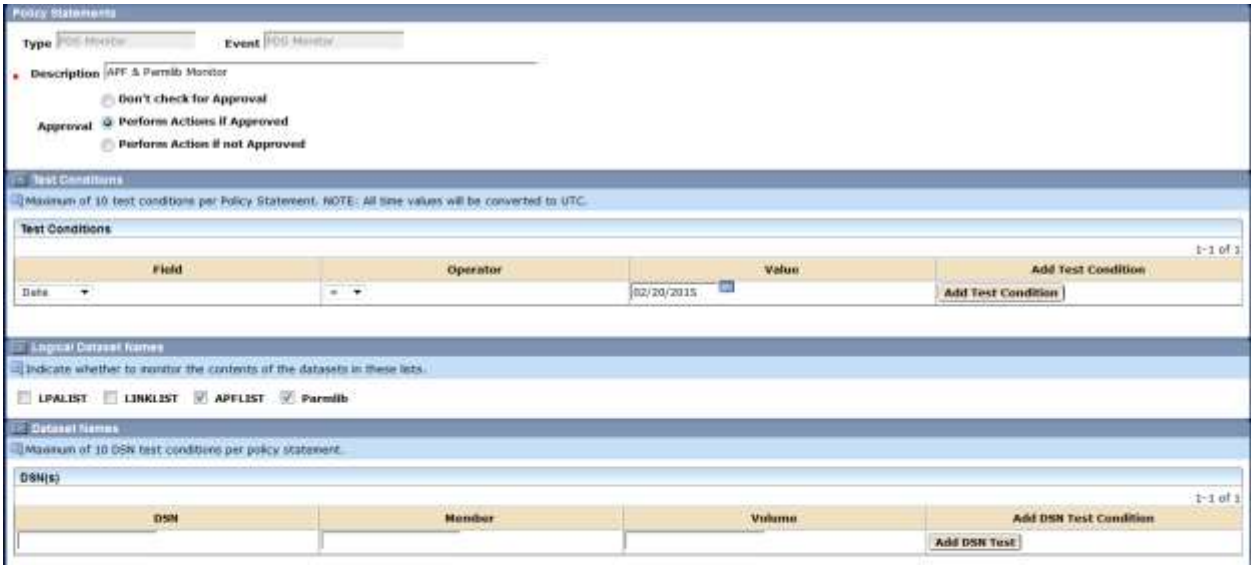
The Inputs

Inputs include both descriptions of real events and descriptions of the standards they are to be compared to. On mainframe computers, the records describing events come from a large number of sources and in great volume. Sources include both logs and event monitors. The logs include: SMF data, the SYSLOG dataset, CICS logs, network logs, DB2 logs, USS logs, TCP/IP logs, logs for TCP/IP daemons, and others.

Event monitors include any software that causes some event to be triggered whenever specified events occur. These include ENF (Event Notification Facility), software which intercepts operator console messages. They also include software tools designed to monitor compliance with policies by intercepting important events such as the opening of key datasets.

Now that mainframes are commonly connected to UNIX and Windows computers using TCP/IP, compliance management tools will need to be able to process inputs from those platforms as well.

Inputs involving standards can be more difficult to automate. For example, a necessary and common standard is that no one should be allowed to update key datasets such as APF datasets and parmlibs. The list of APF datasets and parmlibs can change from day to day,   Some automated compliance tools require that the list of "datasets to be monitored" is updated manually whenever there is a change. Other tools allow you to specify "monitor all APFs and parmlibs". The tool then automatically updates the list of "datasets to be monitored" whenever needed.



Policy Statements

Type PDS Monitor Event PDS Monitor

* Description APF & Parmlib Monitor

Approval
○ Don't check for Approval
● Perform Actions if Approved
○ Perform Action if not Approved

Test Conditions

Maximum of 10 test conditions per Policy Statement. NOTE: All time values will be converted to UTC.

Test Conditions

1-1 of 1

Field	Operator	Value	Add Test Condition
Date ▾	= ▾	02/20/2015	Add Test Condition

Logical Dataset Names

Indicate whether to monitor the contents of the datasets in these lists.

☐ LPALIST ☐ LINKLIST ☑ APFLIST ☑ Parmlib

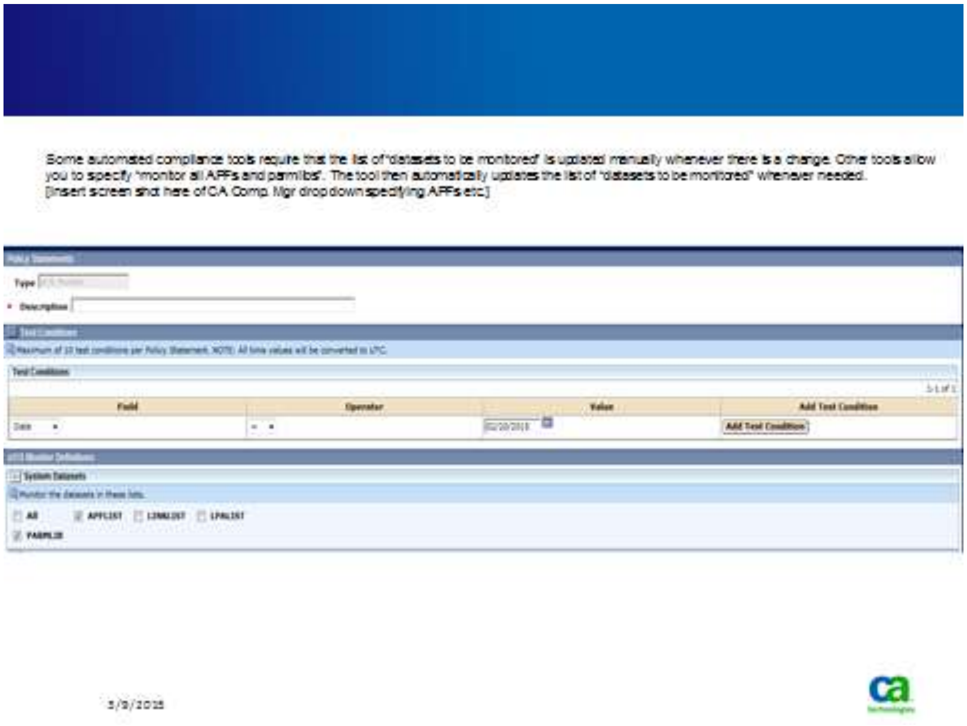
Dataset Names

Maximum of 10 DSN test conditions per policy statement.

DSN(s)

1-1 of 1

DSN	Member	Volume	Add DSN Test Condition
			Add DSN Test



Some automated compliance tools require that the list of "datasets to be monitored" is updated manually whenever there is a change. Other tools allow you to specify "monitor all APFs and parmlibs". The tool then automatically updates the list of "datasets to be monitored" whenever needed.
[insert screen shot here of CA Comp Mgr drop down specifying APFs etc.]

Policy Statements

Type

* Description

Test Conditions

Maximum of 10 test conditions per Policy Statement. NOTE: All time values will be converted to UTC.

Test Conditions

1-1 of 1

Field	Operator	Value	Add Test Condition
Date ▾	= ▾	02/20/2015	Add Test Condition

System Datasets

Monitor the datasets in these lists.

☐ All ☑ APFLIST ☐ LINKLIST ☐ LPALIST
☑ PARMLIB

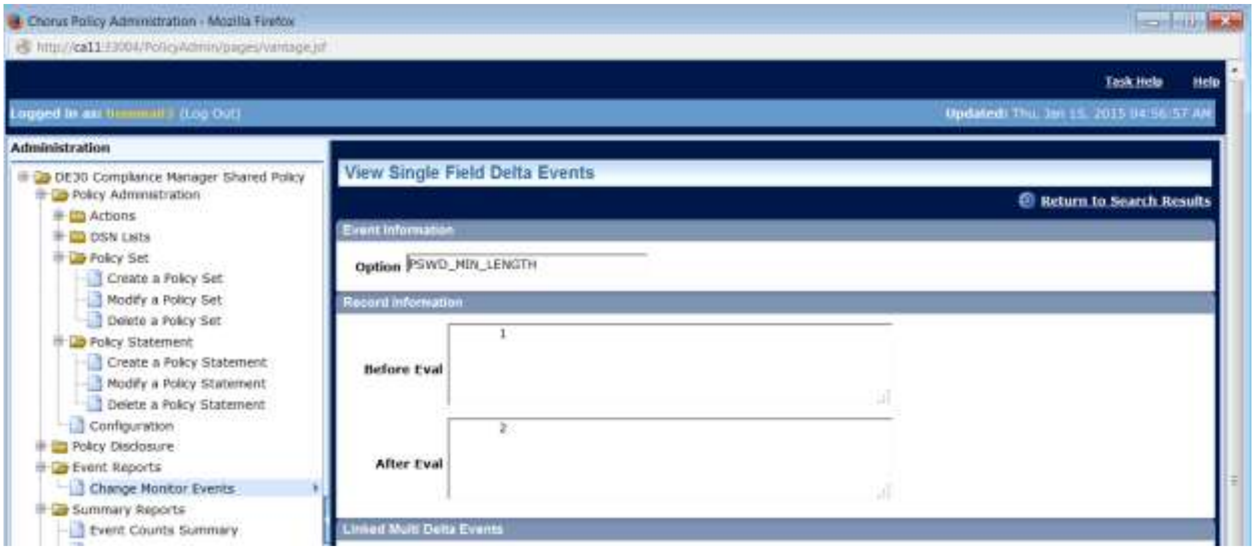
3/9/2015

Screen shots showing automated selection of APF datasets

To make the standards effective, you will want tools that can easily maintain the specifications in computer-readable format. You want to automate this specification as much as possible, covering all the major areas of mainframe security. These areas include both system security (MVS, JES, IODF specifications for LPARs, sysplexes and shared DASD) and the ESM (External Security Manager such as CA ACF2, IBM's RACF, and CA TopSecret). For other security related options specified in configuration files (such as configuration files for TCP/IP, its daemons, and the Policy Agent firewall software), you will want tools that make the standard specification as easy as possible.

The Outputs

For some events, you will want immediate notification, such as the raising of alarms by means of texting, emails, and phone calls. For other events, you will want the fact to be recorded and compared to some standard on a daily basis. For yet other events, you'll want to be able to conduct different types of analysis, including trend analysis over time and correlation of one type of event and another.

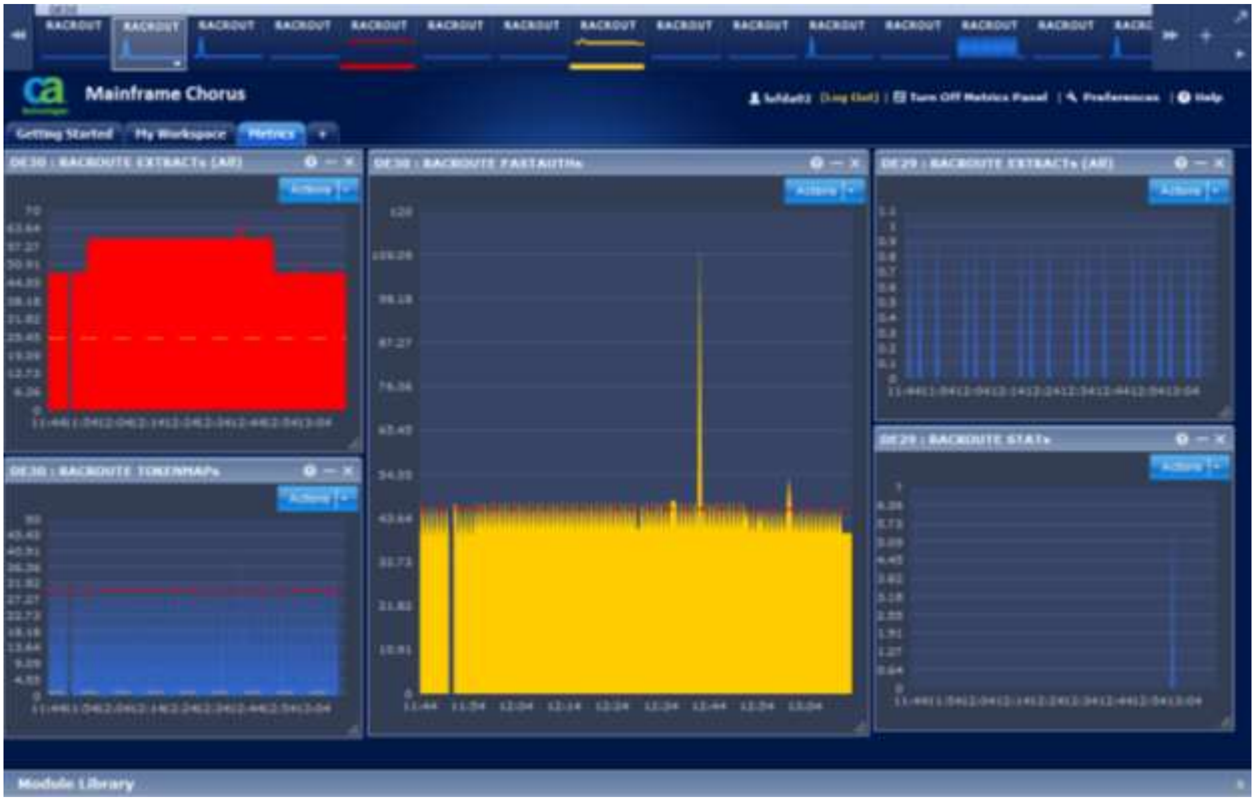


Option PSWD_MIN_LENGTH

Before Eval 1

After Eval 2

Screen shot showing capture of single event



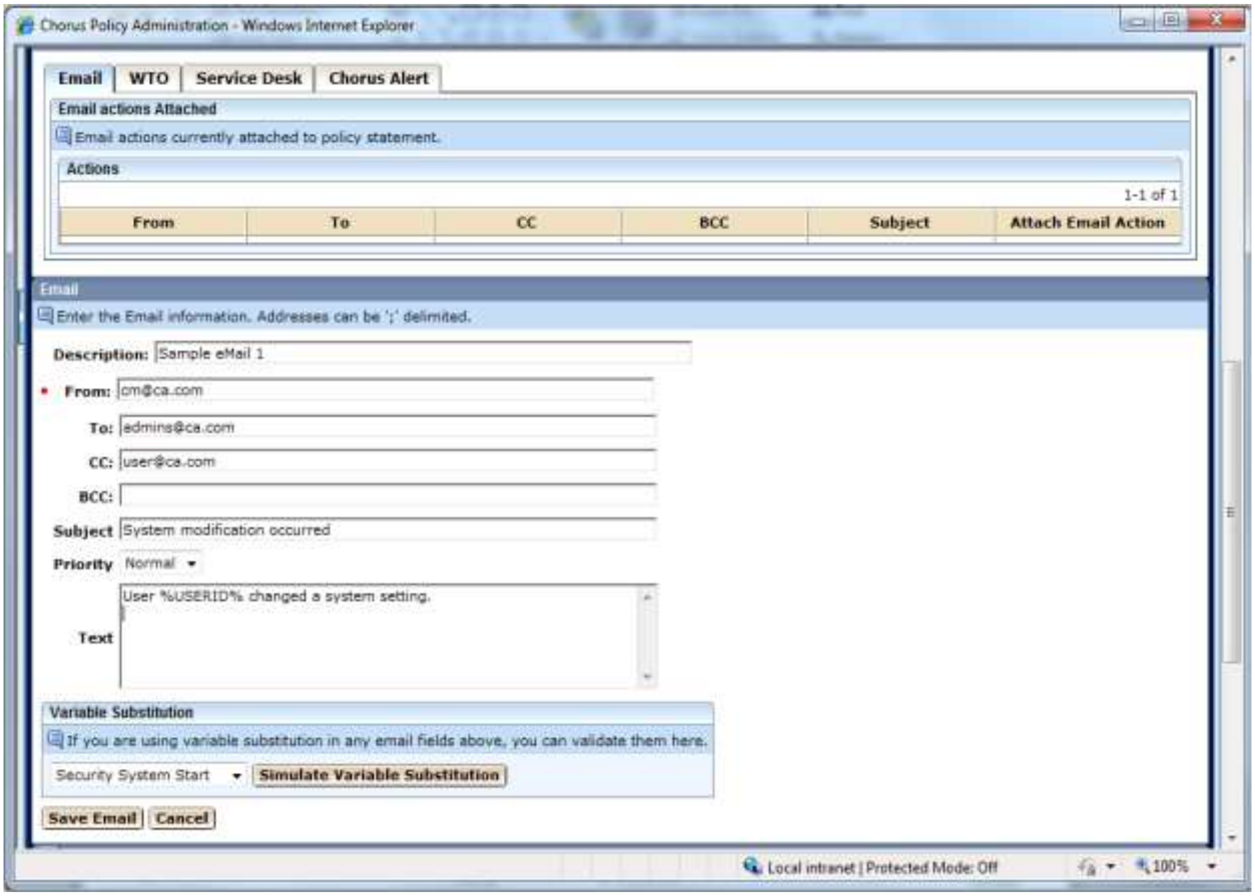
Screen shot showing time-based analysis

Characteristics of an Effective Automated Tool

An effective tool for compliance management will be able to handle large volumes of data from all the standard mainframe sources. It will also support inputs from UNIX and Windows computers, and be capable of supporting inputs from other sources (such as smart phones for example) in the future.

It will support a variety of input sources for standard specifications, with controls to prevent changes by anyone other than those authorized in the policy.

It will provide dataset and member level monitoring, with change control, including before and after images of changes.


Chorus Policy Administration - Windows Internet Explorer
Email
WTO
Service Desk
Chorus Alert
Simulate Variable Substitution
Save Email
Cancel
Local intranet | Protected Mode: Off
100%

Email actions Attached

Email actions currently attached to policy statement.

Actions

1-1 of 1

From	To	CC	BCC	Subject	Attach Email Action

Email

Enter the Email information. Addresses can be ';' delimited.

Description: Sample eMail 1
* From: cm@ca.com
To: admins@ca.com
CC: user@ca.com
BCC:
Subject System modification occurred
Priority Normal
Text User %USERID% changed a system setting.

Variable Substitution

If you are using variable substitution in any email fields above, you can validate them here.

Security System Start

Screen shot showing possible actions to be taken

Implementation Issues for an Automated Tool

Beyond the standard issues for any software tool (such as performance tuning, resource consumption, and response time), compliance management tools will need to provide both completeness and flexibility. For example, here are some new and some not so new technology changes which affect security exposures, and which are often not addressed by automated tools:

- Connections to networks beyond our partner networks with APPN and Enterprise Extender
- Residual data on disk
- Residual data on tape
- Use of tape management software to supplement security software
- Dynamic changes to authorized dataset lists
- Connections between the mainframe and distributed computers
- Policy Agent firewall software for TCP/IP
- Personal Identification Information (PII) in dataseets

- Digital certificates and PKI (Public Key Infrastructure)
- Shared DASD between LPARs with separate security software databases
- Databases mirrored over a sysplex with separate security software databases
- Data in the "cloud"
- Mainframe to Internet connections, including FTP, http, DB2, CICS, MQ Series, and TN3270

(Ask your system programmers to help you sort through these topics and to become aware of new ones.)

No single tool will likely be able to address all of these issues. But you will want to be aware of them, and to address them at least in your policies.

Benefits

Effective compliance management for mainframe security will of course result in better protection against security breaches. It provides other benefits as well. It can reduce audit costs by providing a framework which collects and presents data easily for auditors to process. Security administrators will be more productive, since their efforts will be focused on more useful activities.

Compliance management can help relieve staff shortages in two ways. First it can automate and simplify basic tasks. (Remember the poor security administrator reviewing the violations report manually?) Because compliance requires formal specification of standards, new hires who are not familiar with mainframes will find it easier to become acclimated and productive.

Recommendations

Improve the policies. Make them comprehensive. Use them as the basis for developing specific standards and baselines. Use them to make the right people responsible and accountable. A measure of effective policy-making is that it results in a set of standards that addresses every area which is relevant to information security.

Improve the tools. Make them comprehensive. Have them provide minimal output reporting against all of the standards resulting from the policies.

Learn what it is you don't know. There are two ways to ensure complete coverage:

- Look at the areas the STIGs etc. cover and consider whether each is relevant

- List every software package with a configuration file and every option for each. (You don't have to do it all at once but get projects under way to include every security software option, privilege, and resource class as well as the components for system security.)

Make the documentation of standards easy and extensible with someone responsible for each piece.

Apply the same change control to system software as to application software

Involve all the right parties in deciding what the standards should be. Very often this will include the Legal department and the owner of the application, each of whom may need to get involved more than casually.

We have shown why effective compliance management for mainframe security requires both effective policy and automated tools. Without effective policy, compliance management becomes meaningless. We have described what to expect of automated tools, what characteristics to look for, and the benefits the tools should provide you.

A good automated tool will facilitate information security management by simplifying processing of vast amounts of data in the light of the policies. It will also prepare you well for information security audits. Given the publicity and attention being given to computer security breaches, and the continued importance of the mainframe to our global economy, your installation needs an effective compliance management function. If you don't make it happen, then who will?

For Further Information:

- Links to STIGs for various platforms

  http://web.nvd.nist.gov/view/ncp/repository

- Link to Special Publication 800-53 and related

  http://csrc.nist.gov/publications/PubsSPs.html#800-53

- Article **Stu Henderson's Clear Explanation of Effective z/OS Security Auditing** a proven security audit program for mainframes with z/OS and MVS (http://www.stuhenderson.com/MVSAUDL.pdf)
- **CA Technologies Manuals (available at support.ca.com)**
- **Information Security Newsletters:** http://www.stuhenderson.com/Newsletters-Archive.html

About the Author: Stu Henderson is an experienced system programmer, auditor, trainer, and consultant, specializing in information security. He is editor of the ***RACF User News*** and the online ***Mainframe Audit News***. He teaches seminars nationwide, both public sessions and in-house. His website www.stuhenderson.com contains a wealth of articles and useful links.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

While every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.