HP OpenView Select Audit

For the Windows®, HP-UX®, and Linux® Operating Systems

Software Version: 1.01

Sarbanes-Oxley Model Guide

Document Release Date: November 2006
Software Release Date: November 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

HP OpenView Select Audit includes the following software developed by third parties:

- ANTLR Copyright 2005 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- Install Anywhere, Copyright 2004 Zero G Software, Inc.
- Jasper Decisions Copyright 2000-2006 JasperSoft Corporation.
- JavaScript Tree, Copyright 2002-2003 Geir Landro.
- Legion of the Bouncy Castle developed by Bouncy Castle.
- log4J from the Apache Software Foundation.
- OpenAdaptor from the Software Conservancy.
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

HP OpenView Select Audit is part of HP's business service Identity Management Suite. Select Audit provides reporting, monitoring, and alerting capabilities to facilitate risk assessment and breach response processes. It outputs data to multiple destinations including databases and files.

Select Audit uses models to manage the compliance management lifecycle. The models capture the relationship between controls and how the controls are analyzed for effectiveness. They also analyze and interpret events and provide a dashboard report that indicates the current state of the controls. This guide contains a description of the Select Audit Sarbanes-Oxley model.

Audience

This guide is intended for administrators who are responsible for maintaining and updating the Select Audit Sarbanes-Oxley model. This guide assumes a working knowledge of:

- Audit concepts and requirements
- The audit life cycle and regulatory compliance requirements
- The reporting requirements of your company's operational and audit policies

The Select Audit Documentation Set

This manual refers to the following Select Audit documents. These documents are installed with Select Audit and are available in the `<install_path>/docs` folder where `<install_path>` represents the path where Select Audit is installed.

- *HP OpenView Select Audit 1.01 Administration Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`administration_guide.pdf`).
- *HP OpenView Select Audit 1.01 Installation Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP OpenView Select Audit 1.01 User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`user_guide.pdf`).
- *HP OpenView Select Audit 1.01 Sarbanes-Oxley Model Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`sb_model_guide.pdf`)
- *HP OpenView Select Audit 1.01 Concepts Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Center User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_center_guide.pdf`)

- *HP OpenView Select Audit 1.01 Report Designer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_design_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Developer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_devel_guide.pdf`)

Online help is available with the Audit Portal.

Chapter Summary

This guide includes the chapters listed in Table 1.

See the *HP OpenView Select Audit 1.01 Release Notes* (`relnotes.pdf`) on the Select Audit installation CD for known installation issues at the time of this release.

Table 1 Guide Overview

Chapter	Description
Chapter 2, About the Sarbanes-Oxley Model	This chapter provides background information about control modelling as related to the Select Audit Sarbanes-Oxley (COBIT) model.
Chapter 3, Report Model Structure	This chapter describes the Sarbanes-Oxley (COBIT) model structure and its nodes.
Chapter 4, Sarbanes-Oxley (COBIT) Model Thresholds	This chapter describes the model's thresholds.
Chapter 5, The Model Loader	This chapter describes the model loader in the Audit Portal.
Appendix A, Database Links	This appendix lists the database links for the model nodes.

2 About the Sarbanes-Oxley Model

This chapter provides background information for the Select Audit Sarbabes-Oxley model. It contains the following sections:

Compliance Requirements

Compliance is about managing and controlling risks. Control objectives are used to establish controls to mitigate those risks. Compliance regulations such as the Sarbanes-Oxley Act (SOX) require organizations to demonstrate they have appropriate and adequate controls over financial processes, and any IT systems that support these processes.

From an IT perspective, these controls are concerned with identity management processes that manage access to financial applications. They are also concerned with ensuring that security monitoring and incident management processes are in place to prevent intruders from gaining access to the financial systems. Organizations are required to demonstrate that the controls are working.

The compliance reports ensure that the controls are correctly operated and risks are mitigated effectively. The control framework provides the basis for the model, which drives automated reporting.

The Sarbanes-Oxley model uses metrics, which act as indicators to show that controls are effective and operating correctly. The metrics are related to the events to demonstrate the appropriate and correct operation of the controls.

Modelling the Control Framework

The modelling framework can capture a state top-down, from the risks to the relevant controls, or bottom-up, from the controls and relating them to the risks.

The model concentrates on key controls, minimizing the number of key risk metrics that have to be gathered. It relies heavily on process-based analysis and metrics which measure an activity or procedure that is part of an internal control. Key Performance Indicators (KPIs) are included in the model to measure the effect of the control activity on the data and to detect occurrences of errors.

The model captures the relationships between perceived risks and IT controls. Business functions and processes are captured at a high level. Each business process and process task is captured as a node in a graph. Links are used to relate concepts. Each process contains tasks representing the major stages within each process.

Risks and risk indicators are captured. Risk indicators are metrics derived from the overall business area. They are given an indicator to show that the processes are running effectively. Risk indicators are linked to a business area or business process. Risks are related to a business process task.

The model is further defined with control objectives that mitigate the risks and controls that implement the control objectives. Each of these form a node within the control model graph. Control objectives are linked to risks and controls are linked to control objectives.

The control model represents a set of relationships between business risks and controls. Within each area, you can express rules to define how the elements relate. You can express the importance of different risks. You can define acceptable values for risk metrics by defining a threshold or defining a fuzzy set that defines the goodness of the metric values.

Modelling the Controls

The controls are linked to tests and KPIs. Tests are a set of conditions that should be maintained. KPIs are metrics that indicate the effectiveness of the control. The control contains a description of how the sets of tests and KPIs relate to produce the assessment of how the control is functioning.

The modelling framework contains a library of components that are used to describe the tests in detail, including the ability to describe a process that must be used to initiate change. Other tests include the ability to compare data sets and to check on segregation of duty or authorization. The model can be used to check an expected state or desired state against the actual state.

Sources of IT events are modelled. Events from a system are represented as a set of fields, where one field is the event time. Events can be considered as single events or as a set of events within a time-frame. The event fields can be mapped into a form expected by the component library, allowing the events to be filtered and selected based on field values.

Reporting

A graph built from library components describes the different concepts within the model. The components form the graph nodes which are linked to data sources. Each node in the graph is tagged with the type it represents within the control framework.

The graph is used to analyze the event data and generate reports. Each component generates results relating to the events that violate the description within the model. These results then act as events and form nodes further up the graph.

The analysis results are presented in an assurance report. At the top level, the different areas are shown with a status indicator, showing how well the risks are being mitigated. The report can be navigated down through the report structure for further detail. The lower levels provide details of issues.

Sarbanes-Oxley (COBIT) Model

The Sarbanes-Oxley (COBIT) model demonstrates the level of compliance to defined control objectives for system components. You can view reports that show the status of the components, the trend of the level of compliance and the history of the status.

Model Reports

The Dashboard folder, under the Models folder in the Report Center Library contains reports generated by the Sarbanes-Oxley (COBIT) model.

Figure 1 Sarbanes-Oxley (COBIT) Model Reports Folder

The Sarbanes-Oxley (COBIT) reports are categorized in the **Sarbanes-Oxley (COBIT)** subfolder. This folder contains the following four subcategories:

- Access Management
- Administration
- Change Controls
- User Management

You can drill down through the subfolders to view sub-levels of data. The reports are scheduled to generated at 2:00 am, based on the machine time, and then every 24 hours.

The report data is represented in a tree structure and shows the results of the analysis of the model node fact data.

Model Report Structure

The model reports show the status, trend and status history of a metric. An example of a model report is shown in Figure 2.

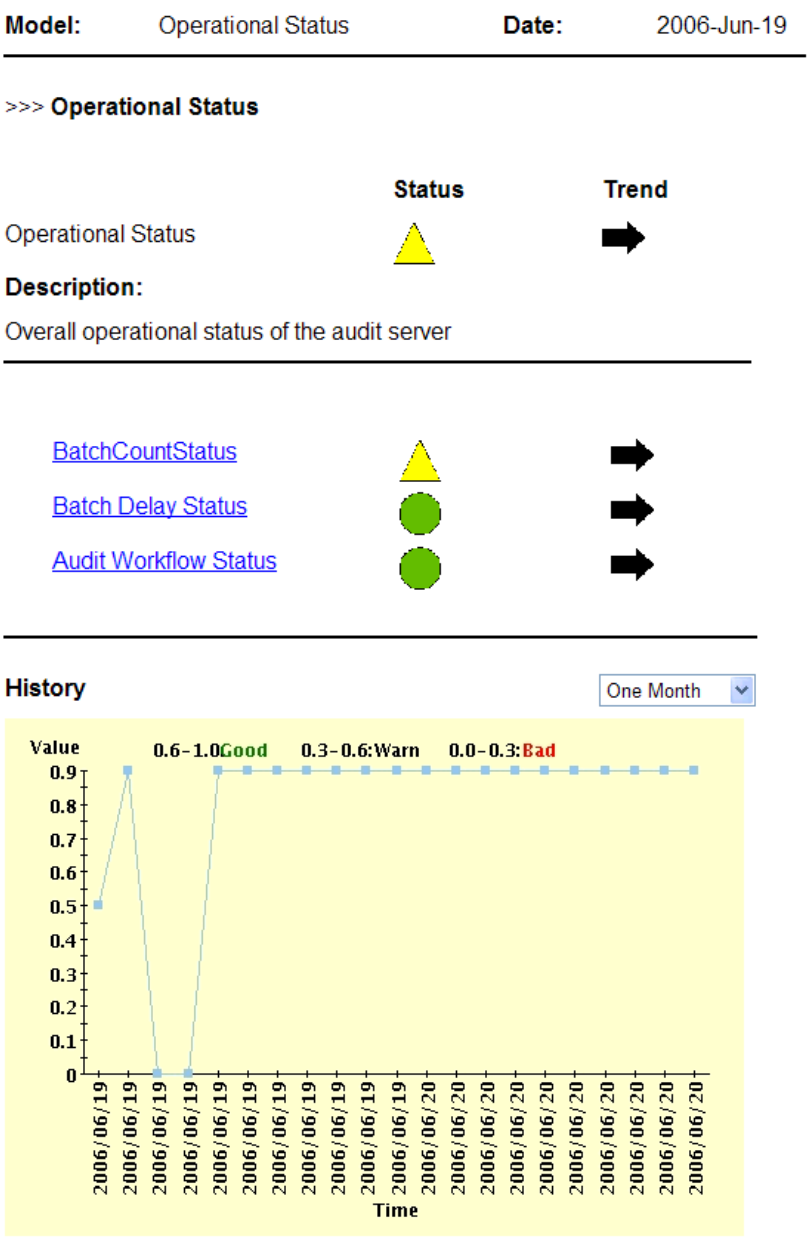

Figure 2 Sample Model Report

The level of the current report is shown at the top of the report, along with the model name and the date the report was generated. The body of the report is divided into two sections. The top section of the report shows the metric being represented, its status and the trend. Status of the level of compliance with the defined control objectives is shown by a status indicator:


compliance level is good


compliance level is adequate


compliance level is poor

The status is calculated from the child nodes and is determined by the lowest level of any child node. For example, if a child node is red, the top-level status will be red, even if all other child nodes are green.

The trend of the level of compliance is shown by arrows:

 improving level of compliance

 compliance level staying the same

 declining level of compliance

The child nodes are listed under the report metric. You can click the child node name to drill down to reports for those nodes. Some child node reports do not have show a status or trend, as shown in Figure 3.

Model: Operational Status **Date:** 2006-Jun-20

>>> Operational Status / BatchCountStatus / **Batches Done**

	Status	**Trend**
Batches Done		

Description:

Number of batches successfully processed

stats

parameter	**value**
count	13522

Figure 3 Model Report Without Status

These reports show low-level data elements that compute the model data using data directly from the database. The output and parameters of the element are listed in the Stats table.

History status

The bottom section of the model report shows the status history. The status history is recorded each time the model runs. The graph maps status values over a period of time. The X axis shows the time period which is set using the drop-down list at the top of the graph. The following time periods are available:

- One Month
- Three Months
- Half Year
- One Year

The Y axis represents a scale of "goodness" between 0 and 1, where 0 is red and 1 is green for that particular node.

Deleting Model Reports

You can delete model reports using the Report Center. If you want to delete model reports, you must delete all the reports at each level. Deleting an upper-level report does not automatically delete related reports at a lower level.

When you delete a model from the Audit Server, the reports generated by that model are not deleted.

Changing the Model Report Execution Time

To change the report execution schedule for the Sarbanes-Oxley (COBIT) model, you need to edit an XML file in the `auditserver.ear` file.

For UNIX

1. Go to the `dist` directory of the Audit Server installation.

   ```
   cd /opt/OV/SelectAudit/auditserver/dist
   ```

2. Create a temporary working directory and go into that directory.

   ```
   mkdir temp
   cd temp
   ```

3. Extract the `ear` file into this directory.

   ```
   /opt/bea/jdk142_08/bin/jar -xvf ../auditserver.ear
   ```

4. Go to the `lib` directory.

   ```
   cd APP-INF/lib
   ```

5. Extract the contents of the `auditservercommon.jar` file.

   ```
   /opt/bea/jdk142_08/bin/jar -xvf auditservercommon.jar
   ```

6. Change to the `analysis` directory.

   ```
   cd com/hp/ov/selectaudit/auditserver/common/analysis
   ```

7. Edit the `scheduler.xml` file and change the `CronExpression` (using the usual crontab format) to whatever you like:

   ```
   <bean id="SOXtimerTask"
   class="org.springframework.scheduling.quartz.CronTriggerBean">^M
         <property name="jobDetail" ref="SOXModel"/>^M
                  <!-- run every morning at 2 AM -->^M
         <property name="cronExpression" value="0 0 2 * * ?"/>^M
   </bean>^M
   ```

8. Change to the `lib` directory.

   ```
   cd /opt/OV/SelectAudit/auditserver/dist/temp/APP-INF/lib
   ```

9 Create a new `auditservercommon.jar` file.

```
/opt/bea/jdk142_08/bin/jar -cvf auditservercommon.jar com
```

10 Remove the `com` directory tree.

11 Create a new `ear` file.

```
cd /opt/OV/SelectAudit/auditserver/dist/temp
/opt/bea/jdk142_08/bin/jar -cvf ../auditserver.ear *
```

12 Remove the working `temp` directory.

For Windows

1 Go to the `dist` directory of the Audit Server installation.

```
cd C:\Program Files\HP OpenView\SelectAudit\auditserver\dist
```

2 Create a temporary working directory and go into that directory.

```
mkdir temp
cd temp
```

3 Extract the `ear` file into this directory.

```
C:\bea\jdk142_08\bin\jar -xvf ..\auditserver.ear
```

4 Go to the `lib` directory.

```
cd APP-INF\lib
```

5 Extract the contents of the `auditservercommon.jar` file.

```
C:\bea\jdk142_08\bin\jar -xvf auditservercommon.jar
```

6 Change to the `analysis` directory.

```
cd com\hp\ov\selectaudit\auditserver\common\analysis
```

7 Edit the `scheduler.xml` file and change the `CronExpression` (using the usual crontab format) to whatever you like:

```
<bean id="SOXtimerTask"
class="org.springframework.scheduling.quartz.CronTriggerBean">^M
      <property name="jobDetail" ref="SOXModel"/>^M
                <!-- run every morning at 2 AM -->^M
      <property name="cronExpression" value="0 0 2 * * ?"/>^M
</bean>^M
```

8 Change to the `lib` directory.

```
cd C:\Program Files\HP
OpenView\SelectAudit\auditserver\dist\temp\APP-INF\lib
```

9 Create a new `auditservercommon.jar` file.

```
C:\bea\jdk142_08\bin\jar -cvf auditservercommon.jar com
```

10 Remove the `com` directory tree.

11 Create a new `ear` file.

```
cd C:\Program Files\HP OpenView\SelectAudit\auditserver\dist\temp
C:\bea\jdk142_08\bin\jar -cvf ..\auditserver.ear *
```

12 Remove the working `temp` directory.

3 Report Model Structure

The Sarbanes-Oxley (COBIT) model is an identity management model that supports the COBIT control objective DS5 *Delivery and Support Ensuring Systems Security*. DS5 deals with security and identity management. The aim of DS 5 is to “safeguard information against unauthorized use, disclosure or modification, damage or loss enabled by “logical access controls which ensure that access to systems data and programs is restricted to authorized users”.

This chapter contains the following sections:

Overall Structure

The Sarbanes-Oxley (COBIT) model has status indicators that are based on various risk metrics. The status indicators indicate whether there are issues in the way that the identity management framework is being controlled. The risk metrics may relate to the failure to properly execute controls or indicate that the controls are ineffective.

The model covers four areas of identity management:

- Access Management
- User Management
- Change Control
- Administration

Access Management is concerned with ensuring that there are policies in place to guarantee that the application roles and access rights are effectively managed. It aims to reduce risks associated with users not having appropriate access rights.

User Management is concerned with procedures that ensure that users accounts are appropriately managed.

Change Control is concerned with how the identity systems are maintained to ensure that risks are not increased by the maintenance or reconfiguration operations, as well as procedures to keep authentication and access mechanisms in place. Metrics provide indications that the levels of change are appropriate.

Administration relates to both Access Management and User Management. It is concerned with how control objectives are maintained and looks at the actions of those maintaining the controls.

Access Management

Access Management relates to the COBIT control DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights, and DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place.

Access Management has three sub-groups:

- **Access Management Status** looks at the resources that are being accessed. This branch looks into the resources being managed within the Select Access (SA) system.
- **Resource Entitlement Management** looks at the entitlements that are deployed through Select Identity (SI). These are based on changes to the user/service assignments but reflect system changes.
- **User Service Management** looks at the how users are mapped into the Select Identity Service model.

Access Management Status

The Access Management Status section helps support COBIT control objectives DS 5-6 *User Control of User Accounts* which involves users reviewing their activity, and DS 5-10 *Violation and Security Activity Reports* which involves reviewing security logs.

The Access Management area looks at how access patterns over the resource set are protected by Select Access. This status indicator has four areas where detailed metrics are generated:

- Unprotected Resources
- Frequent Access Users
- Unusual Deny Patterns
- Unknown User Access Patterns

Metrics generated at this level are not fed into the overall status of the model, but are displayed as potential warnings and lists of things that should be reviewed.

Unprotected Resources

Unprotected Resources supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

Unprotected Resources are those where access has been gained by users who have not been authenticated. At the first level, the unprotected resource list provides a list of statistics based on how many times different unprotected resources have been accessed. Drilling down one level gives a list of unprotected resources and the number of times each has been accessed. Such a list should be reviewed for high value resources.

Frequent Access Users

The Frequent Access Users section supports COBIT Control Objective DS 5-6 *User Control of User Accounts* which requires users to review their activity.

This section looks for individuals with particularly high access patterns. The initial report contains access statistics based on looking at users and the number of times they (successfully) access the resource set. The first page has a set of statistics showing the average (mean) resource accesses per user, the (sum) total resource accesses, the total minimum and maximum accesses by each user and the (sample) standard deviation over the set. There is also a list of those with high access patterns (high is defined as mean + 2* standard deviation). The list shows a user name along with the size of the deviation (access count -mean)/standard deviation. Its magnitude gives an idea of who is accessing most resources.

This list can be reviewed periodically to check that this activity is normal for the user's job. Drilling down one level, the report lists all users making accesses during the report period and the number of accesses they have made.

Unusual Deny Patterns

Unusual Deny Patterns relates to DS 5-6 *User Control of User Accounts* which is concerned with having reviews of user accounts, and DS 5-10 *Violation and Security Activity Reports* which involves reviewing security logs.

Unusual Deny Patterns look for users who have been denied access to resources a large number of times. This area of the report is mainly concerned with looking for security violations.

The first node contains a list of statistics regarding the number of denies per user. It also has a list of users with an unusual number of denies. The limit is based on a multiple of the standard deviation above the mean value of 2.56. Drilling down further provides a complete list of users with Unknown User Access Patterns.

Unknown User Access Patterns

Unknown User Access Patterns supports "need to have" rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights. It also relates to DS 5-6 *User Control of User Accounts* which is concerned with having reviews of user accounts.

The Unknown User Access Patterns section looks at resources that unknown users are trying to access. The list shows those resources that have unusual numbers of access attempts from unknown users. This uses a threshold of 2.5 * standard deviation. High values may indicate that there has been a switch in the access control policy regarding a particular resource or it may indicate that there are external links into a resource. This list should be reviewed.

Resource Entitlement Management

Resource Entitlement Management supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

Resource entitlements are treated in a very similar way to the user to service mappings. The resource entitlement profiles are the entitlements themselves, based on the resource name and the rights being added or removed. They examine the number of users given new entitlements, the number of entitlements being removed and the number of unapproved resource entitlement changes.

Status Indicators

The status indicator is based on three values:

- The total number of resource entitlements given
- The total number of resource entitlement changes without approval
- The total number of resource entitlements removed

There are expected levels of turnover within an organization and thresholds are set to note numbers outside of this which could indicate compliance issues. These thresholds reflect the size of the user set controlled by SI, along with the turnovers within the organization.

Resource Entitlement Allocations

Resource Entitlement Allocations supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

The Resource Entitlement Allocations part of the model shows statistics collected from looking at the number of users added to a given entitlement profile (resource, role list). Drilling down shows lists of the entitlements profiles with the number of users added.

Unapproved Resource Entitlements

Unapproved Resource Entitlements supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

This section looks at the number of unapproved allocations of resource entitlements from within the SI system. As with the user to service mappings, this figure reflects the number of resource allocations where there is no record of an authorization.

Resource Entitlement Removals

Resource Entitlement Removals supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

As with Resource Entitlement Allocations, Resource Entitlement Removals gives statistics around entitlement profiles and then allows you to drill down to see the profiles being removed along with the number of occurrences.

User Service Management

User Service Management supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

User Service Management relates to how users gain access to applications through the Select Identity (SI) service model. This section only looks at user being allocated to or removed from services within Select Identity. The service, the context variable and value used to determine the role within the service are examined. Depending on the SI workflow, the service allocation events can be associated with authorization events. User service management is split into three sections:

- Service Allocations
- Service Removals
- Unapproved Service Operations

Status Indicators

The status indicator from this system is based on three values:

- The total number of service allocations
- The total number of service removals
- The number of unapproved service operations

The first two values represent the number of operations involving managing user accesses to services. These numbers should correspond to the turnover level of an organization. The threshold values should be configured according to the organization’s size and the reporting period. If values are too high or too low, this may indicate that there is a lack of control over the management of users’ rights.

The third value should be zero. All changes leading to the rights of users being changed should have approval records.

Service Allocations

Service Allocations supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

Service Allocations are looked at in terms of the service, the context variable and value used when allocating the user. The first level of service allocations shows a set of statistics on the number of users added to each service/context profile. The statistics include the total number of user to service allocations, the number of service profiles, and the average (mean) number of allocations to each profile. Drill downs list the different service profiles along with the number of users allocated to each.

Service Removals

Service Removals supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

Service Removals are handled in much the same way as Service Allocations. Service profiles are based on the service name and context variable. The statistics allow the user to dig down further to see the number of users allocated to given service profiles.

Unapproved Service Operations

Unapproved Service Operations supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

This section is a count of all the user to service operations that cannot be associated with an approval event. This reflects on risks that users “need-to-have” rights have not been correctly considered.

User Management

User Management relates to DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights. It also relates to DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms.

The User Management section looks at how user profiles are managed. This category is split into three sections:

- Users
- Rights
- Passwords

User management covers the requirements for formal procedures for establishing and maintaining user accounts and rights, and maintaining authorization mechanisms.

Users

The Users section relates to DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights.

The Users area is split into three areas. The first is concerned with authentication mechanisms linked to the users within Select Access. The second and third are concerned with how user accounts are created and deleted in Select Access and Select Identity.

Authentication Management

Authentication Management relates to control objective DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place. Metrics here provide indications that the levels of change are appropriate.

This section looks at how authentication methods are managed under three areas:

- **Authentication Method Change Patterns** looks for patterns of fluctuation on the authentication mechanisms used. This is the only value used in the status indicators, where thresholds are based on looking for sequences of methods being added and removed.
- **Authentication Method Removals** lists and counts the authentication methods removed from the system.

- **Authentication Method Adds** looks and lists authentication methods added into the system. A count of the methods is given.

Select Access User Management

Select Access User Management relates to DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights.

This area looks at the number of users added and removed from the Select Access system and applies thresholds to these numbers that reflect the expected turnover in the system. These thresholds are set to expect a level of change (static systems could imply account sharing).

Select Identity User Management

Select Identity User Management is broken into four sections, each of which has a status indicator. The metrics provide an indication of how well the user management process is running within an organization and are indicative of well-run controls.

SI User Adds looks at users added into the system. There are three categories of user:

- *User Add Request Approvals* counts the number of newly-authorized users and checks that no names are authorized twice. A list of all authorized users is produced.
- *User Add Request Rejections* counts the number of rejected authorizations and lists the user name and the number of times each name is rejected.
- *User Add Request Modifications* is based on the number of modified requests and the names for the modified accounts are listed.

Status Indicators

The status indicator for this category is based on:

- Duplicate name add approvals
- Number of user add approvals
- Number of user add approvals rejected
- Number of user add approvals modified

SI User Modifications looks at user profiles being modified within the SI system. It looks at authorizations (approvals) for user profile modifications that are either accepted, rejected or approved.

Status Indicators

The status indicator for this category is based on:

- Maximum number of modifications for a user
- Total number of user modifications
- Total number of modified modification requests
- Total number of modification requests rejected

SI User Terminations looks at accepted, modified and rejected requests.

Status Indicators

The status indicator for this category is based on:

- Total number of user terminations
- Number users with modified termination requests
- Total number of terminate requests rejected

SI User Management Problems looks at how the requests are treated and where there are problems in fulfilling user provisioning requests. For each of the add, modify and terminate actions, there is a list of users and a count of the number of failures. Statistics are generated over these lists.

Status Indicators

The status indicator for this category is based on:

- Total number of failures to add users
- Total number of failures to modify users
- Total number of failures to remove users

Rights

The Rights section relates to DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights, and DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights.

This section looks at how user rights are managed within Select Access. It has two main sections. SA Matrix Management links users or groups to the resources they are allowed to access. SA Group Management reflects how users in groups are treated and their implied rights.

SA Matrix Management

SA Matrix Management supports “need to have” rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights.

SA Matix Management looks at risk in terms of the stability of the SA Access Control matrix. Too much change is viewed as indicating potential risk. It looks at matrix changes that restrict permissions, those that increase permissions and rules introduced into the matrix.

“Deny” Matrix Changes looks at the number of Allows changed to Inherits or Denies, Inherits changed to Denies and Rules removed to be replaced by a Deny. The first two are simple counts where rules are effectively removed. The rules are listed with the number of removals of each rule.

The status indicator is based on a looking at the number of changes for each count (including total number of Rule removals). It is a measure of stability.

“Allow” Matrix Changes are changes that increase users permissions. It looks at counts of different changes that increase (or potentially increase) users’ rights. There are three counts (Deny to Allow, Inherit to Allow and Deny to Inherit) along with a list of rules that are switched to allow.

The status indicator is based on the number of changes for each count (including total number of rule to allow changes). It is a measure of stability (instability implies potential risk).

Rule Inclusion Details lists rules included in the matrix, along with the number of inclusions for each rule. Statistics are collected for these numbers.

Status Indicators

The status indicators for the overall SA Matrix Management are formed from the individual status indicators for the permission removals and permissive matrix changes along with the number of rule inclusions.

SA Group Management

SA Group Management supports "need to have" rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights, and DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights.

The SA Group Management area looks at both SA groups and dynamic groups. The model deals with two aspects. It first looks at the number of groups added and deleted. Next, it looks at changes to the group definitions.

Group Adds/Removals looks at counts for the number of groups added, dynamic groups added, groups removed and dynamic groups removed. The status indicator is formed from all these counts. The thresholds are based on the assumption that the group structure is relatively stable and too much turnover is an indication of risk.

Group Change Management looks at how group memberships are managed. Within this grouping there are three sections.

Users Added to Groups lists groups that have had users added and how many users are added in each case. Statistics for this list are also given.

Users Removed from Groups lists groups that have had users removed and how many for each group. Statistics for this list are given.

Dynamic Group Filter Changes looks at changes to the dynamic groups and looks at the number of changes for each dynamic group.

Status Indicators

Status indicators for SA Group Management are based on the maximum number of changes for each group. This can be viewed as an indication that one group has unusual activity and therefore indicates potential risk.

Passwords

The Passwords section relates to DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place.

Passwords also relates to COBIT Control Objective DS 5-6 *User Control of User Accounts* which requires users to review their activity.

This section looks at various metrics from SI concerning user account passwords, password expiry and resets. Metrics are indicative of the risks associated with bad password management. The Passwords section includes one subsection, SI Password Management, which in turn, looks at four categories:

SI Password Management

SI Password Management has four sub-categories:

- **Password Expire Notification Count** counts the number of password expiry notifications sent out to users.
- **Passwords Expired Count** counts the number of passwords that are expired, giving an indication that users are not taking password changing seriously and implying risk.
- **Administrative Password Resets** looks at the work load of administrators who are resetting passwords. It lists administrators who have reset passwords along with the number of passwords reset. It looks at the spread of the workload amongst administrators with the assumption that there are risks associated with one administrator resetting all passwords.
- **User Password Resets** looks at the number of times users have had passwords reset. It produces a list of those with unusual (> 2.56* std + mean) numbers of password resets as an indication of those users who may not be managing accounts well or those only using them occasionally. Drilling down you can view lists of all users whose passwords are reset and how many times.

Status Indicators

The status indicators are based on:

- the standard deviation over the count of administrative password resets
- the number of passwords expired
- the maximum number of changes per user

Change Control

Change Control relates to control objective DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place. Metrics here provide indications that the levels of change are appropriate.

Metrics in this area also are indicative of well-run change control processes with respect to the identity management rights management systems. These come under the AI 6 *Manage Changes* category. The metrics are indicative of the approach as a whole rather that any individual section.

This section looks at change control within the identity management system, that is metrics suggesting that the technology-based controls are maintained and running.

This category covers three areas:

- the coverage of the identity management system. The metrics indicate risks associated with changes to reduce the coverage of identity management systems.

- changes to the audit configuration and the risks associated with the failure to gain adequate information.
- changes to the identity management system itself, for example, changes to ensure the system's security is maintained.

Control Coverage

Control Coverage relates to control objective DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place. Metrics here provide indications that the levels of change are appropriate.

It also supports "need to have" rights as referred to in DS 5-3 *Security of Online Access to Data* which is concerned with reducing risks associated with users not having appropriate access rights, and DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights.

Control Coverage looks at the configuration of aspects of the identity management system that reflect the number of services, applications and resources that are controlled, or rules or workflows that help in the control. Coverage metrics indicate that there is a risk where there is a high volume of change. This suggests that the identity management system is not stable.

Rule Change Management

Rule Change Management looks at how the Select Access rules are managed. This section of the model has three pieces:

- a count of rules added
- a count of rules removed
- a list rules changed, along with the number of changes

The maximum number of changes to a rule is an indicator that the rule change control process is failing.

Status Indicators

Status indicators are based on:

- the number of rules added
- the number of rule removed
- the number of rules changed
- the maximum number of changes made to a rule

SA Resource Management

SA Resource Management looks at a number of metrics associated with resources are managed within Select Access. The metrics assess the resources, resource folders and resource services.

Resource Management looks at the number of resources added and deleted. It has a status indicator based on these counts.

Resource Folder Management lists the resource folders added and removed, with a count of each. The status indicators are based on the total numbers of folders added and removed. It also has with a check that resource folders are not being added multiple times which would indicate issues with the change control processes.

Resource Service Management acts in the same way as Resource Folder Management.

SI Service Management

SI Service Management looks at how services are managed within Select Identity. It looks at services being added, modified and deleted. The additions and deletions are counted. A list is created of services that have been modified, along with the number of times each has been modified. There is also a list of services that have been modified an unusual number of times:

- **Service Additions** lists and counts the number of services added.
- **Service Changes** lists and counts the number of services changed.
- **Service Removals** lists and counts the number of services removed.
- **Service-Context Link Changes** lists and counts the number of modifications of the links between a service and its contexts.
- **Service-Role Link Changes** lists and counts the number of link role modifications made for each service.
- **Service View Changes** lists and counts the number of service view modifications that have been made for each service.

Status Indicators

The status indicator is based on the number of service additions, removals and modifications.

SI Service Element Management

This section of the model looks at how service roles, views and contexts are managed within SI. For each of these, the number of adds, modifications and deletes are counted. The status indicator is formed from a combination of all these counts.

SI Workflow Management

SI Workflow Management looks at the operations that add, remove and delete workflows. Too much activity indicates a lack of control over how the identity management system is managed. In this case, the metrics indicate the risk that workflows may not cover the stages necessary for compliance.

The metrics cover three area:

- **Workflow Removals** counts the number of workflows deleted.
- **Workflow Creations** counts the number of workflows created.
- **Workflow Changes** lists and counts the number of modifications on each workflow.

Status Indicators

The status indicator is formed from the number of workflows created, deleted and the maximum modifications for a given workflow.

SI Resource Management

SI Resource Management looks at how the set of resources within the SI system are managed. It looks at resources added, modified and deleted. There is a count of resources created and resources deleted, along with a list of modified resources with a count of the number of times each has been modified.

Status Indicators

The status indicators are based on the number of resources added and deleted. There is also a check on the maximum number of changes applied to any resource. This would indicate a risk in change control.

Identity System

Identity System relates to control objective DS 5-2 *Identification, Authorisation and Access* that requires that logical access is restricted by the implementation of appropriate identification, authentication and access mechanisms. This control objective also requires procedures to keep authentication and access mechanisms in place. Metrics here provide indications that the levels of change are appropriate.

Under the Identity System section, there are metrics reporting on system changes. There is a single node that looks at the SA System Changes.

SA System Changes

This node has four categories relating to the configuration of the Select Access system:

- **Select Access Audit Config Changes** counts the number of changes to the log file configurations.
- **SSL Disabled in New Components** counts new components where SSL flag is set to false.
- **New User Sources** counts the number of new sources for user data.
- **Policy Signature Disabled** counts the number of times that the policy signature flag is disabled.

Status Indicators

The status indicators are based on a combination of the counts. The thresholds allow some log file changes and new user sources but start to warn as policy signatures or log SSL links are disabled.

Administration

The Administration section of the report looks at the management of administrators and administrator actions. These reflect significant internal risks to an enterprise. The metrics act as indicators of risk. Controls for administrator actions fall under a range of the major COBIT control objectives but they are gathered in this section to give a consistent view of administrator actions.

The Administrator area of the report is split into two sections. Administration Management looks at administrator management. Administrator Activity looks at a particular administrator's logins and actions.

Administration Management

Administration Management relates to DS 5-4 *User Account Management* which requires formal procedures for establishing and maintaining user accounts and rights, and is especially aimed at administrators who have critical access.

Administration Management is split into two sections. The first section looks at Select Access administrator delegations. The second looks at Select Identity administration management.

SA Delegation Management

This area of the model looks at delegation within the SA system. There are three situations examined and each situation has the changes listed:

- the delegation of administrative access rights
- the removal of delegated access rights
- the delegated rights change from what was inherited

Status Indicators

The status indicators are based on the total number of each of these changes. As such, the status indicator denotes abnormal delegation activity which may indicate risk.

SI Administration Management

SI Administration Management looks at how Select Identity administrator roles are managed. It assesses creations, modifications and deletions.

Status Indicators

The status indicators are based on the number of roles created and the maximum changes to any given role.

Administrator Activity

Administrator Activity, which looks at logins, relates to COBIT DS 4-2 *IT Continuity Plan Strategy and Philosophy* that requires that the IT Continuity Plan is in line with the overall Business Continuity Plan to ensure consistency and that the IT Continuity Plan takes into account the IT long-range and short-range plans to ensure consistency.

It also relates to DS 4-6 *Testing the IT Continuity Plan* which requires the IT Continuity Plan is assessed for its adequacy on a regular basis or upon major changes to the business or IT infrastructure. Administrators review this data to help them keep control of their accounts.

Administrator Activity has one node: Administrator Logins.

Administrator Logins

There are two main areas under the Administrator Logins section of the model. Senior Security Administrator Activity looks at the Senior Security Administrator activity and Delegated Administrator Logins looks at Delegated Administrator logins.

Status Indicators

The status indicators are based on the number of login failures and the number of hosts the logged on from.

Senior Security Administrator Activity

This section looks at administrator logins and login failures. For both of these, the number of login attempts from each host is listed.

Delegated Administrator Logins

Delegated Administrator login activity is indicated in the same manner as for Senior Security Administrators.

4 Sarbanes-Oxley (COBIT) Model Thresholds

This chapter describes the model thresholds for the Sarbanes-Oxley (COBIT) model. It contains the following sections:

All metric information is computed from audit logs for the time period specified for the report (one month, by default). The values measured from the system are passed through a function, which maps the input to a number between 0 and 1. The number determines the compliance level of the status indicator for the node. For example a node may indicate that:

- 0 – 0.2 shows as red
- 0.2 – 0.8 shows as yellow
- 0.8 – 1 shows as green

The graph presented on the bottom of a node report page will show the historical trend of the compliance level, and will also present the specific ranges for red, yellow and green levels for that node.

Access Management

Access Management Status

The following nodes do not feed into overall status indicators and therefore do not have thresholds:

- Unprotected Resources
- Frequent Access Users
- Unusual Deny Patterns
- Unknown User Access Patterns

Resource Entitlement Management

Table 2 Resource Entitlement Management Thresholds

Node	Description	Default Threshold Limit
Resource Entitlement Allocations	specifies the total number of users being given entitlements on resources	120 users
Unapproved Resource Entitlements	specifies the total number users having resource allocations added or removed where there is no approval record	10 users
Resource Entitlement Removals	specifies the total number of users having resource allocations removed	120 users

User Service Management

Table 3 User Service Management Thresholds

Node	Description	Default Threshold Limit
Service Allocations	specifies the total number of users allocated to services	50 users allocated per service
Service Removals	specifies the total number of users removed from services	100 users removed per service
Unapproved Service Operations	specifies the total number of user to service operations (i.e. adds and removes) where there is no approval record This depends on the SI workflows being used. A workflow can be set to provision users with no approval step. In such a case, there will be lots of unapproved users. There needs to be an approval stage for SOX-critical applications.	50 unapproved service operations

User Management

Users

Table 4 User Thresholds

Node	Description	Default Threshold Limit
Authentication Management		
Authentication Method Change Patterns	looks for sequences of authentication methods being added and then removed or removed and added etc.	4 sequences
Authentication Method Removals	specifies the total number of authentication methods removed	5 methods
Authentication Method Adds	specifies the total number of authentication methods added	5 methods
Select Access User Management		
Users Added	specifies the total number of users added	30 users added
Users Removed	specifies the total number of users removed	30 users removed
Select Identity User Management		
SI User Adds		
User Add Request Approvals	looks at the total number of new users being approved Note: Approved refers to those that are directly approved and those that are approved after modification.	30 total new users approved
User Add Request Rejections	specifies the total number of new user request that are rejected	20 rejected new user requests
User Add Request Modifications	specifies the total number of new user requests that are modified before approval	10 new user request modifications

Table 4 User Thresholds (cont'd)

Node	Description	Default Threshold Limit
SI User Modifications		
Approved User Profile Updates	total number of approved modification requests	30 modification requests approved
Modified User Profile Updates	looks at the number of modification requests per user and applies a threshold to the maximum (i.e. warning if any user has more that 15 modifications before approval)	20 modification requests per user
Denied User Profile Updates	looks at the total number of modification requests denied	20 modification requests denied
SI User Terminations		
Approved User Removals	looks at the total number of users where there are termination approvals (i.e. approved or approved after modification)	30 users
Modified User Removals	looks at the total number of modified termination approval requests	30 users
Denied User Removals	looks at the total number of termination requests that are turned down	30 users
SI User Management Problems		
User Change Failures	looks at the total number of failures in modifying users Note: A failure is where the operation fails or where it only partially succeeds.	20 user modification failures
User Removal Failures	looks at the total number of failures in terminating users Note: A failure is where the operation fails or where it only partially succeeds.	10 user terminate failures
User Add Failures	looks at the total number of failures in adding users Note: A failure is where the operation fails or where it only partially succeeds.	10 user add failures

Rights

Table 5 Rights Thresholds

Node	Description	Default Threshold Limit
SA Matrix Management		
"Deny" Matrix Changes		
Dynamic Rule Changes	looks at Rule to Denys. Rule to Deny: specifies the total number of Rules changed to a Deny	15 changes
Inherit to Deny	specifies the total number of Inherits changed to Deny	15 changes
Allow to Inherit or Deny	specifies the total number of Allows changed to Inherits or Denys	15 changes
"Allow" Matrix Changes		
Deny to Allow	specifies the total number of Denies changed to Allows	15 changes
Inherit to Allow	specifies the total number of Inherits changed to Allows	15 changes
Deny to Inherit	specifies the total number of Denys to Inherits	15 changes
Dynamic Rule Changes	looks at Rule to Allows. Rule to Allow: specifies the total number of Rules changed to an Allow	15 changes
Rule Inclusion Details		
Rule Inclusion List	looks at the total number of rules included in the access control matrix	15 rules
SA Group Management		
Groups Adds/Removals		
Dynamic Groups Added	specifies the total number of dynamic groups/ groups added	5 dynamic groups/groups
Dynamic Groups Removed	specifies the total number of dynamic groups removed	5 dynamic groups
Groups Added	specifies the total number of groups added	5 groups
Groups Removed	specifies the total number of groups removed	3 groups
Group Change Management		

Table 5 Rights Thresholds

Node	Description	Default Threshold Limit
Users Added to Groups	looks at the maximum number of users added to any group	10 group changes
Users Removed from Groups	looks at the maximum number of users removed from any group	10 group changes
Dynamic Group Filter Changes	looks at the maximum number of group filter changes	10 group changes

Passwords

Table 6 Password Thresholds

Node	Description	Default Threshold Limit
SI Password Management		
Password Expire Notification Counts	specifies the total number of expiry notifications sent	25 notifications
Password Expired Count	specifies the total number of expired passwords	25 passwords
Administrative Password Resets	looks at the number of passwords reset by each administrator It looks at standard deviation or spread over this data. The threshold is detecting extreme spread.	5 administrator resets
User Password Resets	looks at the maximum number of password resets for a given user, i.e. if any user has more than 2 resets during the report period then it starts to show a “warning” status	5 resets

Change Control

Control Coverage

Table 7 Control Coverage Thresholds

Node	Description	Default Threshold Limit
Rule Change Management		
Rules Added	specifies the total number of access rules added	15 added access rules
Rules Removed	specifies the total number of access rules removed	15 access rules removed
Rules Changed	looks at the number of changes for each rule. The node then looks at the total number of rule changes and the maximum number of changes for a rule.	10 total changes 5 changes to a rule

Table 7 Control Coverage Thresholds (cont'd)

Node	Description	Default Threshold Limit
SA Resource Management		
Resource Management	specifies the total number of resources added and the total number of resources removed Note: No resources change is deemed to be a concern as some periodic change is expected indicating some review and control of resources is in place.	40 resources
Resource Folder Management	looks at the number of adds and deletes for each folder name. The rules then look at the maximum number of adds and deletes for a given folder and the total number of folder adds and deletes.	total 4 folder adds or deletes 10 adds or deletes for a folder
Resource Service Management	looks at the number adds and deletes for given resource service Status indicators are formed from metrics of the total number of adds and deletes, and the maximum number of adds and deletes for a service.	total of 10 adds or deletes maximum of 4 adds or deletes for a resource service
SI Service Management		
Service Additions	looks at the total number of services added to the SI system	10 services added
Service Changes	looks at the total number of services that have been modified	30 modified services
Service Removals	looks at the total number of services removed from the SI system	15 services deleted
Service-Context Link Changes	lists and counts the number of modifications of the links between a service and its contexts	20 modifications
Service-Role Link Changes	lists and counts the number of role link modifications made for each service	20 modifications
Service View Changes	lists and counts the number of service view modifications that have been made for each service	20 modifications
SI Service Element Management		
Service View Add Count	looks at total number of service views added	20 service view adds
Service View Removal Count	looks at total number of service views deleted	20 service view deletes

Table 7 Control Coverage Thresholds (cont'd)

Node	Description	Default Threshold Limit
Service View Change Count	specifies the number of service views modified	30 modifications to service views
Service Role Add Count	looks at total number of service roles added	20 service role adds
Service Role Change Count	specifies the number of service roles modified	30 modifications to service roles
Service Role Removal Count	looks at total number of service roles deleted	20 service role deletes
Service Context Add Count	looks at total number of service contexts added	20 service context adds
Service Context Change Count	specifies the number of service contexts modified	30 modifications to service contexts
Service Context Removal Count	looks at total number of service contexts deleted	20 service context deletes
SI Workflow Management		
Workflow Removals	specifies the total number of workflows deleted	8 workflow deletions
Workflow Creations	specifies the total number of workflows added	5 workflows added
Workflow Changes	looks at the number of modifications made for each workflow and applies the threshold on the maximum number of modifications for any given workflow	5 workflow modifications
SI Resource Management		
Resource Removals	specifies the total number of resources deleted	5 resources removed
Resource Creations	specifies the total number of resources added	5 resources created
Resource Changes	specifies the total number of resources modified	5 resources modified

Identity System

Table 8 Identity System Thresholds

Node	Description	Default Threshold Limit
Select Access Audit Config Changes	specifies the total number of log file changes on the SA system	10 file changes
SSL Disabled in New Components	specifies the total number of new components that do not communicate with the other SA components using SSL	4 components
New User Sources	specifies the number of new user sources added into the SA system	4 user sources
Policy Signature Disabled	specifies the total number of policy signature disabled events within the SA system	4 disabled events

Administration

Administration Management

Table 9 Administration Management Thresholds

Node	Description	Default Threshold Limit
SA Delegation Management		
Delegated Rights Added	specifies the total number of administrator rights delegated	5 administrator rights
Delegated Rights Removed	specifies the total number of administrator access rights removed	5 administrator rights
Inherited Rights Changes	specifies the total number of rights changed from Inherit (i.e. to Allow or Deny)	5 administrator rights

Table 9 Administration Management Thresholds (cont'd)

Node	Description	Default Threshold Limit
SI Administration Management		
Admin Role Removal Count	specifies the total number of administrator roles removed	5 roles removed
Admin Role Creation Count	specifies the total number of administrator roles created	5 roles created
Admin Role Changes	looks at the number of modifications for each administrator role with the rule applying a threshold on the maximum changes for a rule, i.e. are there any administrator roles with more than 2 modifications	5 roles modified

Administrator Activity

Table 10 Administrator Activity Thresholds

Node	Description	Default Threshold Limit
Administrator Logins		
Senior Security Administrator Activity		
Successful Logins	looks at the total number of successful logins for the Senior Security Administrator	12 logins
Login Failures	specifies the total number of login failures for the Senior Security Administrator	10 failed logins
Delegated Administrator Logins		
Successful Logins	looks at the total number of successful logins for the Delegated Administrator	12 logins
Login Failures	specifies the total number of login failures for the Delegated Administrator	20 login failures

5 The Model Loader

HP Openview Select Audit includes the ability to load different types of models into the audit modeller. This chapter describes the Select Audit Model Loader. It contains the following sections:

Model Loader Features

The Model Loader enables users to load and remove models as necessary. The audit modeller has the ability to run multiple models on the same server.

The modeller is a compliance tool that allows users to view reports based on predefined thresholds. These thresholds are set based on compliance criteria such as, if a user enters a wrong password more than a threshold of three times, raise an alert and indicate a compliance “warning” status based on a specific time period.

There are two types of models. The Operations model is run four times a day to capture and analyze normal operations data. Compliance models are run once and generate reports based on compliance specifications. The Operations model is included with the Audit Server upon installation. The compliance models are optional add ons. Compliance models for different policies and regulations will be made available periodically.

The model definition is contained within a directory generated as random numbers, under the `models` directory created by the Audit Server installer, for example, `<config dir>/models/1027774882/*`.

Model Tree Definition

The main file in the Model Tree is `complete.xml`. This file contains the root nodes for the model. Subsequent tree nodes can be defined either in predefined node `xml` files, for example, `SAGroups.xml` to define a Select Access group, or they can be defined inside the `complete.xml` as one complete file. The `complete.xml` file begins with a root tag `<Package>` with the ID and name as attributes.

Model Database/Report Definitions

The `DBdesc_saudv2.xml` file defines the views that are used. This file is referenced in the `TRDefault` properties file as the `DBFile` key. This directory includes the SQL file that generates the views, as well as the model graphics definition file for report generation on every tree node defined in the Model Tree Definition. For example, if there was a `SAGroups.xml` tree node defined, a graphics file with the same name must be defined in the

reports definition directory. The `Label` tag name that is defined in the `xml` file is the name that is used to create a report directory in Jasper under the main Reports directory in the Report Library.

Model Properties File

The `TRDefault` properties file contains values for how the model interacts with the database and the report generation process. It contains the linkage between the model graphics, the reports and the model database.

Loading Compliance Models

The models are loaded into Select Audit using the Audit Portal. Refer to the *HP OpenView Select Audit 1.01 Administration Guide* for more information.

Loading the Model in the Audit Portal

The Model Loader in the Audit Portal has two screens:

- the Model Loader screen
- the loaded model Configuration screen

Model Loader Screen

The **Model Loader** screen is used to upload the model file. The Model Loader:

- checks that the model file is a `zip` file. The loader checks for a `.zip` ending and makes sure the file is a real `zip` file.
- checks that the `zip` file contains the `complete.xml` file and that it is a valid `xml` file. The `xml` file must contain the root tag `<Package>` with the attribute name.

The name of the model is retrieved from the name attribute in the `<Package>` root tag. If there is any error in the loading process, an error message is displayed. The model is extracted from its `zip` format and copied to the Select Audit setup configuration directory. A new directory that is generated as random numbers, for example, `<config dir>/models/1027774882/*`, is created in the `models` directory created by the Audit Server installer.

Ensure the user who starts the WebLogic server has read/write access for the configuration directory, otherwise an error is generated.

If you attempt to load a model with a name that is already stored in the database, you will be prompted to update the model. If you update the existing model, the Model Loader removes the existing model (both the files and the database entries) and copies the new model in as a new entry.

After the model is loaded successfully, the left-hand tree view is refreshed with the newly-loaded model. The previously-generated model reports are not deleted on update.

Loaded Model Configuration Screen

The left-hand tree view displays the name of the loaded models with links to a configuration screen for each model as shown in Figure 4.

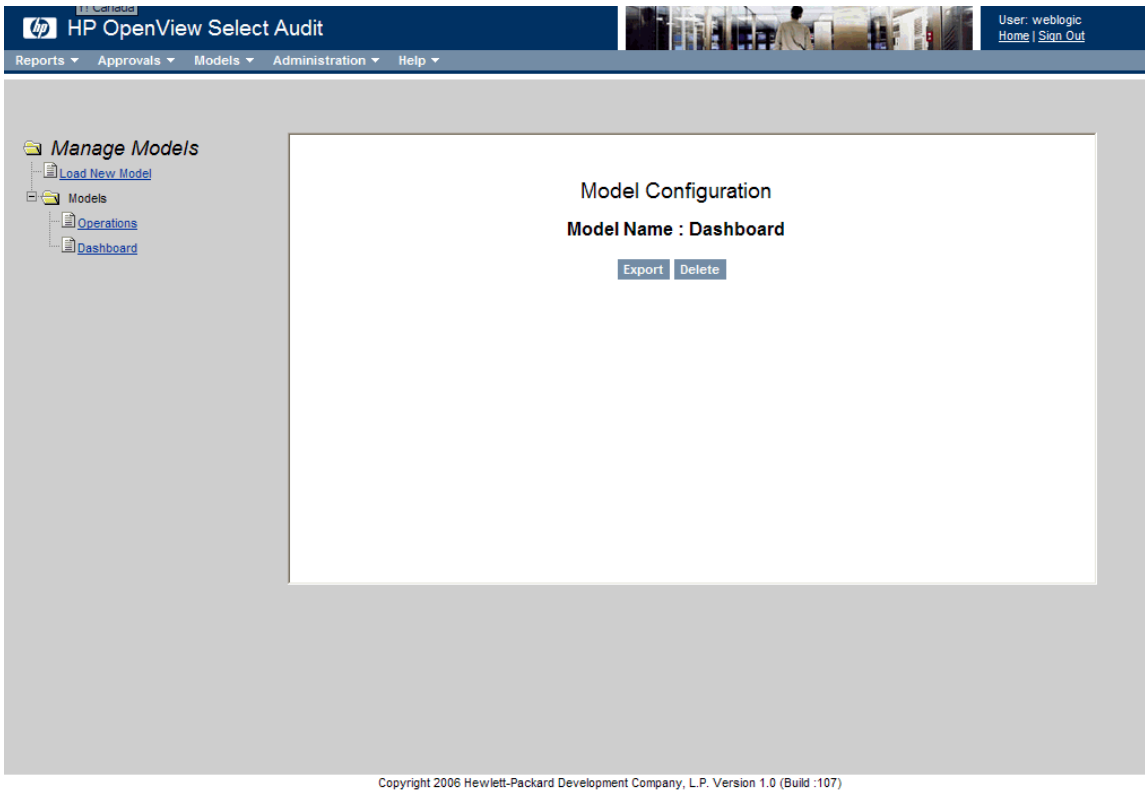

Figure 4 Compliance Model Configuration Screen

The compliance model **Configuration** screens have two buttons:

- The **Export** button zips up the model directory and downloads the `zip` file to the client browser machine.
- The **Delete** button deletes the model from the model directory and all the files in the directory.

Model File

The model file consists of a `zip` file (usually named `model.zip`) that includes the properties file `TRDefault`. The loaded model must contain the file `complete.xml`.

A Database Links

This appendix outlines the database links for the nodes in the Sarbanes-Oxley (COBIT) model.

Access Management

Access Management Status

Unprotected Resources	Looks at view SASEventView where `EVENTID=39` and `SAUser` had the value 'Unknown User'. Queries groups by and counts `SAResource`. Results are written into the RES_OPENRES table where statistics are collected over the Amount column.
Frequent Access Users	Looks at view SASEventView where `EVENTID=40` (access denied) and `SAUser` had the value 'Unknown User'. Queries groups by and counts `SAResource`. Results are written into the RES_UNKNOWNDENY table where statistics are collected over the Amount column. A further results table RES_DENYUNUSUALRES of those unusual values is written.
Unusual Deny Patterns	Access Patterns looks at view SASEventView where `EVENTID=40` (access denied) and queries groups by and counts `SAUser`. Results are written into the RES_DENYPATTERN table where statistics are collected over the Amount column. A further results table RES_DENYUNUSUAL of those unusual values is written. Access Patterns looks at view SASEventView where `EVENTID=39` (access allowed) and queries groups by and counts `SAUser`. Results are written into the RES_ACCESSPATTERN table where statistics are collected over the Amount column. A further results table RES_UNUSUALACCESSORS of those unusual values is written.

Resource Entitlement Management

Resource Entitlement Allocations	Looks at SIUserAttrView and groups by ATTRNAME and new, where ATTRNAME like '%ENTITLEMENTS' and AUDITTYPE=1, 17, 11, 19, 34, 2, 8, 52 (those operations that can lead to entitlement adds). Results written to table RES_SIRESATTRALLOC2.
Unapproved Resource Entitlements	Looks at SIUserAttrb where ATTRNAME like '%ENTITLEMENTS' and AUDITTYPE= 1, 17, 29, 2, 3, 3, 8 to find all entitlement operations and then looks in SIUsrView to remove the approved entitlement changes (where AUDITSUBTYPE=1, AUDITTYPE= 1, 17, 29, 2, 3, 30, 8) by matching against the requestId. Results written to table RES_NONAPPROVEDRESALLOCS.
Resource Entitlement Removals	Looks at SIUserAttrView and groups by ATTRNAME and old, where ATTRNAME like '%ENTITLEMENTS' and AUDITTYPE= 2, 3, 13, 15, 19, 33, 53 (those operations that can lead to entitlement removals). Results written to table RES_SIRESUSRDELALLOC.

User Service Management

Service Allocations	Looks at SIUserMembershipView and looks for AUDITTYPES 1, 2, 8, 11, 19, 34, 52 with a membership operation 1, grouping and counting by the columns membershipname, ctxvarname and contextvarvalue. Results are written into RES_SISERVALLOCMEMB where statistics are computed.
Service Removals	Looks at SIUserMembershipView and looks for AUDITTYPES 3, 15, 13, 19, 33, 53 with a membership operation 1, grouping and counting by the columns membershipname, ctxvarname and contextvarvalue. Results are written into RES_SISERVREMMEMB where statistics are computed.
Unapproved Service Operations	Looks in SIUSERMembershipView and finds those requestIDs where there is not an approval record in SIUserView. For AUDITTYPE= 1, 2, 3, 8, 11, 13, 15, 19, 33, 34, 52, 53, and AUDITSUBTYPE 1 in SIUSRVIEW.

User Management

Users

Authentication Management	Authentication Method Change Patterns looks for sequences of add and removal of the same resource. Authentication Method Removals looks at SAComponentView. Where `EVENTID=26`. Results collated to RES_AUTHADD table where statistics are generated on the SUM column. Authentication Method Adds looks at SAComponentView. Where `EVENTID=25`. Results collated to RES_AUTHADD table where statistics are generated on the SUM column.
Select Access User Management	Users Added Count and Users Deleted Count look at SASEventView with counting the number of `EVENTID=1` and removed counting `EVENTID=2`.
Select Identity User Management	All look at the SIUserView. SI User Adds User Add Request Approvals groups by and counts the username, where `AUDITTYPE-1`, `STATUS=5` or `6` (approve or modify) and `AUDITSUBTYPE=1` (approval). Results are written into RES_USRADD, where statistics are calculated over the Amount column. User Add Request Rejections groups by and counts the username, where `AUDITTYPE-1`, `STATUS=7` (rejected) and `AUDITSUBTYPE=1` (approval). Results are written into RES_SIUSERADDREJECT, where statistics are calculated over the Amount column. User Add Request Modifications groups by and counts the username, where `AUDITTYPE-1`, `STATUS=6` (modified) and `AUDITSUBTYPE=1` (approval). Results are written into RES_SIUSERADDMODIFY, where statistics are calculated over the Amount column. SI User Modifications As the three above but where `AUDITTYPE=2` (modify). • Modify results table RES_SIUSRMOD • Modified modification results table RES_SIUSRMODMOD • Denied modification results table RES_SIUSRMODDENY SI User Terminations As the three above but where `AUDITTYPE=13` (terminate) • Terminate results table RES_SIDELAUTH • Modified terminate requests RES_SIUSRDELMOD • Denied terminate requests RES_SIUSRDELUNAUTH

	SI User Management Problems User Change Failures as above but where `AUDITTYPE=2` and results table RES_SIUSRMODFAIL. User Removal Failures as above but where `AUDITTYPE=13` and results table RES_SIUSRTERMFAIL. User Add Failures counts and groups by UserName where `AUDITTYPE=1` and `STATUS=3` or `4` (Failure or partial success), (with no subtype to look at issues with all phases). Results written into SIRES_USRADDFAIL, where statistics are calculated over the Amount column.

Rights

SA Matrix Management	All look at SA Matrix View. "Deny" Matrix Changes collects `newValue` where it's a rule name and counts occurrences of each and then calculates list of statistics across these counts. "Allow" Matrix Changes • *Deny To Allow* counts `OldValue=deny`, `newValue=allow`. This view just has matrix events. Could check this by joining with AUDITEVENT table via ID foreign keys and had `ComponentEVENTID=31`. • *Inherit To Allow* counts `OldValue='inherit'`, `newValue='allow'`. • *Rule To Allow* looks for old values that are not in the set (allow, inherit, allow, deny, disabled, enabled) and are assumed to be rule names. Counts the number of changes for each rule name `(count(oldValue) … group by oldValue)` and calculates list of statistics across these counts. • *Deny to Inherit* counts `OldValue='deny'`, `newValue='inherit'`.
SA Group Management	Group Adds/Removals looks at SASEventView where `EVENTID=4` for groups added, `5` for groups deleted, `7` for dynamic groups added and `8` for dynamic groups deleted. Group Change Management • *Users Added to Groups / Users Removed from Groups* looks at the SAAttributeView, groups and counts the column EntryName with `EVENTID=6` for Users Add to/Remove from group where column type is add or remove respectively and `Name` is 'uniqueMember'. Results are written to RES_USERADDTOGROUP, RES_USERDELFROMGRP, with statistics being gathered over the Amount column and used in status indicator construction. • *Dynamic Group Filter Changes* `EVENTID=9` and `NAME=nxSearchFilter`. Results are written into RES_GROUPFILTERCHANGE with statistics being gathered over the Amount column and used in status indicator construction.

Passwords

SI Password Management	This looks into the view SITargetView. Password Expire Notification Count counts where `AUDITTYPE=18`. Password Expired Count counts where `AUDITTYPE=24`. Administrative Password Resets groups and counts according to `AdminName` where `AUDITTYPE=6`. Results written into RES_SIPWADMIN, and statistics generated over the Amount column. User Password Resets groups and counts with `TargetName (user)` where `AUDITTYPE=6`. Results written into RES_SIPWUSR where statistics are generated with unusual user resets being added into RES_SIPWUSRUNUSUAL.

Change Control

Control Coverage

Rule Change Management	Rule Added Count looks at SASEventView counts where EVENTID=28. Rule Removal Count looks at SASEventView counts where EVENTID=29. Rules Changes looks at SARuleView where results are grouped and counted by ACCESSRULENAME where TYPE=new, EVENTID=30. Counts are written into RES_RULECHANGES where statistics are generated.
SA Resource Management	Resource Management looks at the SAAttributeView where EVENTID=10 for add and 11 for delete. Resource Folder Management looks at SASEventView collects SAResource (i.e. counts and groups by this) where add is EVENTID=19 and delete is EVENTID=20. Results are saved to table RES_RESFOLDERCREATED, RES_RESFOLDERDELETED and then have statistics calculated over the Count column. Resource Service Management looks at SASEventView collects SAResource (i.e. counts and groups by this) where add is EVENTID=22 and delete is EVENTID=23. Results are saved to table RES_RESSSEVICEADD, RES_RESSERVICEDEL and then have statistics calculated over the Count column.
SI Service Management	Service Additions looks at SITargetView and groups by and counts TargetName, where AUDITTYPE=2000 and TARGETTYPE=6. Results are stored in RES_SISRVADD where they are then counted for use in status indicators. Service Changes looks at SITargetView and groups by and counts TargetName, where AUDITTYPE=2002 and TARGETTYPE=6. Results are stored in RES_SISRVMOD where they are then counted for use in status indicators. Service Removals looks at SITargetView and groups by and counts TargetName, where AUDITTYPE=2001 and TARGETTYPE=6. Results are stored in RES_SISRVREM where they are then counted for use in status indicators. Service-Context Link Changes as above but SIType=7 and results are stored in RES_SISRVCNXLINK. Service-Role Link Changes looks at SIServiceChangeView groups by and counts column serviceName where AUDITTYPE=2002, SIType=8. Service View Changes as above but SIType=9 and results are stored in RES_SISRVVIEWLINK.

SI Service Element Management	All look at SITargetView. Service View • Service View Add Count looks at `AUDITTYPE=2006`. • Service View Removal Count looks at `AUDITTYPE=2007`. • Service View Change Count looks at `AUDITTYPE=2008`. Service Role • Service Role Add Count looks at `AUDITTYPE=2009`. • Service Role Change Count looks at `AUDITTYPE=2015`. • Service Role Removal Count looks at `AUDITTYPE=2010`. Service Context Link • Service Context Add Count looks at `AUDITTYPE=2011`. • Service Context Change Count looks at `AUDITTYPE=2013`. • Service Context Removal Count looks at `AUDITTYPE=2012`.
SI Workflow Management	All look at SITargetView. • Workflow Removals counts events where `AUDITTYPE=5001`. • Workflow Creations counts events where `AUDITTYPE=5000`. • Workflow Changes groups by and counts `TargetName` (workflow name) where `AUDITTYPE=5002`. Results written into RES_SIWORKFLOWMOD where statistics are calculated for the number of changes to each workflow.
SI Resource Management	Looks at SITargetView. • Counts Resources Created where `AUDITTYPE=3000` • Counts Resources Created where `AUDITTYPE=3001` Groups and counts `TargetName` (resource name) where `AUDITTYPE=3002`. Results are written into RES_SIRESMOD which then has statistics calculated over it and these are used in constructing status indicators.

Identity System

Select Access Audit Config Changes	Looks at SASEventView count of `EVENTID=32`.
SSL Disabled in New Components	Looks at SACompChangeView and new like `'%serverUseSLL%false%serverUseSSL'`.
New User Sources	Looks at SASEventView count of `EVENTID=47`.

Policy Signature Disabled	Looks at SASEventView count of `EVENTID=85` where message includes ‘policy signature disabled’ in SQL message like `'%policy signature disabled%'`.

Administration

Administration Management

SA Delegation Management	All look at SASEView where `EVENTID= 34` (add), `35` (delete), `36` uninherited and `SAResource` is 'Administrator Access'. Results are grouped and counted by the SAUser column and written to the tables listed below where statistics are generated and used in status indicators. • Delegation of administrator access rights RESDELADMIN • Removal of delegated administrator access rights (RESUNDELADMIN) • Delegated rights changing from inherit (RES_IHHERITEDDELADMIN)
SI Administration Management	All look at SITargetView. • Admin Role Removal Count counts `AUDITTYPE =10001` • Admin Role Creation Count counts at `AUDITTYPE=10000` • Admin Role Changes groups and counts according to `TargetName` (the role name) where `AUDITTYPE=10002`. Collated into the table RES_SIADMINROLEMOD and statistics are calculated over the Amount column.

Administrator Activity

Administrator Logins	All look at SASEVENTVIEW. Senior Security Administrator Activity • Login (`EVENTID=50`, `Administrator='Senior Security Administrator'` these messages are grouped counted by Host with results into RES_SECADMINLOGIN where statistics are collected over the results set. • Login failure (`EVENTID=52`, rest as above) Results are stored in RES_SECADMINLOGINFAILURE. Delegated Administrator Logins • Login (`EVENTID=56` these messages are grouped counted by Host with results into RES_DELADMINLOGIN where statistics are collected over the results set. • Login failure (`EVENTID=58`, rest as above) Results are stored in RES_DELADMINLOGINFAILURE.

Index