

Compliance Manager Report Pack

Software Version 1.0

HP OpenView Performance Insight

User Guide

March 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

© Copyright 2006 Hewlett-Packard Development Company, L.P.

Trademark Notices

OpenView is a U.S. registered trademark of Hewlett-Packard Development Company, L.P.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Windows® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Product Bundles and Part Numbers

The Compliance Manager solution is available with OVPI or without OVPI. Bundle **T3294-88001** is for customers who already have OVPI. This bundle includes:

- Compliance Manager Report Pack
- Compliance Manager Portlet
- CM Service Desk Datapipe
- CM OVIS Datapipe
- Internet Services Report Pack 2.0
- Internet Services Report Pack 1.0_to_2.0 Upgrade
- Right-to-use license

Bundle **T3293-88001** adds OVPI to the items listed above. Purchase of the Compliance Manager Media Kit, part number **T3295AA**, is mandatory regardless which product bundled is acquired. The media kit includes four CDs for OVPI and one CD for Compliance Manager.

Installation and configuration services are available. The cost of installation and configuration services are not included in the price of either bundle.

Support

Please visit the HP OpenView web site at:

<http://www.managementsoftware.hp.com/>

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can use the support site to:

- Search for documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Discuss issues 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

<https://managementsoftware.hp.com/passport-registration.html>

Contents

- 1 **Overview** 3
 - The Compliance Manager Solution 3
 - Sarbanes-Oxley and Corporate Accountability 4
 - Data Model Elements 5
 - Reports and Process Control Areas 5
 - Threshold Violations: Color-Coding and Numeric Totals 7
 - Periodic Maintenance 7
 - Upcoming Enhancements 8
 - Sources for Additional Information 9
- 2 **Installing the CM Report Pack** 11
 - Guidelines for a Smooth Installation 11
 - Contents of the Compliance Manager CD 11
 - Hardware and Software Requirements 12
 - Installing the CM Report Pack 14
 - Finding Forms and Reports 15
 - Finding New Views of the Object Model 16
 - Finding Change Forms 17
 - Finding Reports 18
 - Using the Web Interface 19
 - Uninstalling Compliance Manager 20
- 3 **Creating a Data Model** 21
 - Planning Your Data Model 21
 - Using Forms to Create a Data Model 23
 - Setting Thresholds 30
 - Planning Ahead for Downtime 32
 - Maintaining the Data Model 34
- 4 **Historical Status Reports** 37
- 5 **Component Group Reports** 43
 - Component Group Changes 43
 - Component Group Availability 46
 - Component Group Incidents 50
- 6 **Admin Reports** 57
 - Administration and Deletion 57
 - Configuration and Logging 59

Table Structures and Sizes	60
7 Installing the Compliance Manager Portlet.....	63
BEA WebLogic 8.1	63
Apache Pluto	65
The build.xml File.....	65
The build.properties File	69
Installing the Portlet	69
Apache Jetspeed 2	71
Glossary.....	73
Index.....	77

1 Overview

You used to hear people talk about *managing* information technology. Today you are more likely to hear people talk about *governing* information technology. While managing information technology is about finding ways to maintain optimal performance, governing information technology is about accountability. If you want to govern information technology, you need a system in place that provides answers to the following questions:

- Do I have controls in place?
- Can I claim that my controls are working?
- Do my operations have an acceptable risk profile?
- Do I have a deficiency, or a likely trouble spot?
- Where are my problems historically?
- Can I isolate the information systems responsible for financial reporting?
- Can I review compliance on a quarterly basis?

The new emphasis on governance is a response to new laws and regulations, emerging standards, and advances in technology. The laws and regulations stress corporate accountability, the emerging standards promote adoption of a new framework for information technology, and advances in technology are making it possible to automate and centralize processes that used to be manual and de-centralized. The laws, the standards, and the technology have *internal controls* as a common theme. If you want to comply with the rules, you need to be accountable, and if you want to be accountable, you need internal controls. If you have internal controls, it follows that you need a system that raises the visibility of controls and makes it clear to all interested parties that the controls are working.

The Compliance Manager Solution

HP OpenView Compliance Manager collects data from other applications, processes the data it collected from other applications, and displays the results in reports that raise the visibility of controls and highlight areas where deficiencies are occurring. Compliance Manager operates by applying a data model to the information technology in your environment. Once the components in your environment are mapped to the model, Compliance Manager can collect data about the components in your environment and roll up data from the component level to the process level. Rolling up data produces a top-down view of compliance that serves two purposes. It provides summary information for the people who are only interested in summary information, and it allows the people who care about the supporting detail to trace deficiencies from the high-level business process to an application, from an application to a component group, and from a component group to a specific component.

Compliance Manager automates IT governance. As a reporting solution for corporate executives and auditors, Compliance Manager provides proof that internal controls are in place and that they are accomplishing what they were designed to accomplish. Compliance

Manager is actually multiple pieces of software. The main software pieces are the report pack, the database connectors (datapipes), and the portlet. Here is a brief description of what the main pieces of software do:

- The report pack configures OVPI to process collected data. The package itself contains templates for reports, processing directives for OVPI, forms for creating a data model, forms for modifying the data model, and forms for setting thresholds.
- Each datapipe configures OVPI to collect data. The datapipe itself contains processing directives for OVPI, a form for assigning data structures to components in your data model, and a linkage report.
- The portlet is an interface to OVPI, designed to be contained within a portal and restricted in terms of layout and behavior. The portlet uses screen-scrape technology to render reports for display in compatible information portals. The portlet displays the executive-level reports only and displays status using symbols and colors.

The first release of Compliance Manager collects data from two OpenView applications, Internet Services (OVIS) and Service Desk. OVIS supplies availability data, while Service Desk supplies change data and incident data. Upcoming releases of Compliance Manager will expand the scope of IT governance. You will be able to add new control areas for Service Desk (configuration, release, and information security), new datapipes for OpenView applications, and new datapipes for 3rd-party applications.

IT governance is being shaped by federal regulations and emerging standards. Before we look closer at the Compliance Manager data model, and the reports, let's briefly review the impact of Sarbanes-Oxley.

Sarbanes-Oxley and Corporate Accountability

When a series of high-profile accounting scandals and business failures caused the investing public to suffer serious losses, the United States Congress did what it could to repair the situation by passing laws aimed at improving the credibility of financial statements. The purpose of the Sarbanes-Oxley Act of 2002 is to strengthen corporate accountability by forcing publicly-traded corporations to adhere to new reporting requirements. The new requirements compel corporate executives to take these actions:

- Establish and maintain adequate internal controls over financial reporting
- In the annual report to shareholders, include a section that assesses the effectiveness of internal controls
- Certify the accuracy of financial statements
- If there is a material change to the company's financial condition, divulge this information to the public as soon as possible

Sarbanes-Oxley also created the Public Company Accounting Oversight Board (PCAOB) and authorized it to craft tougher accounting standards. The PCAOB has expectations. It expects auditors to be independent and it expects the reports that auditors issue to be informative and accurate. To encourage compliance with these expectations, the PCAOB can inspect accounting firms and publicly-owned companies. Inspections are likely to take place when the PCAOB believes that the public would benefit from additional information about a developing situation. The following situations can cause the PCAOB to begin an inspection:

- Two companies merge
- One company acquires another company

- A company announces that it has changed auditors
- A company announces that earnings will be restated

Soon after it was created, the PCAOB began discussing the criteria that should be used for determining whether a company's internal controls are compliant with SOX. Following discussions that took place in 2003 and early 2004, the PCAOB issued Auditing Standard No. 2. The portions of this standard that deal with information technology direct companies to design internal controls in accordance with a recognized framework (COSO, for example), and to recognize the influence of information technology (IT) on internal controls.

Auditing Standard No. 2 advises companies to pay particular attention to the role that technology plays in the collection and processing of financial information. It points out that the accuracy and integrity of information can be undermined by information technology if the technology itself is not adequately controlled.

Data Model Elements

Compliance Manager cannot operate unless the components in your environment have been mapped to a process-oriented, hierarchical data model. Once the mapping step is complete and thresholds are set, Compliance Manager will collect data about the components in your environment, detect threshold breaches, and display status information. In top-down order, these are the five building blocks that make up the data model:

- Business Process
- Application
- Application Instance
- Component Group
- Component

Each block is supported by the block underneath. For example, one application, or possibly several applications, support each business process, and each application will be supported by at least one application instance or possibly several application instances. Similarly, each application instance is supported by one or more component groups, and each component group is supported by one or more components.

You will need to analyze your infrastructure and produce an inventory that aligns with the data model. Once that step is done, you are ready to install the Compliance Manager Report Pack. As soon as you have access to the create forms and the threshold forms, you can create your own data model and set thresholds. When the data model is finished, you can install datapipes and integrate source data with Compliance Manager. For details about integrating source data with Compliance Manager, refer to the user guide for the datapipe.

Reports and Process Control Areas

Compliance Manager collects data directly from Service Desk 4.5. There are actually two independent datapipes, bundled as one package. One datapipe collects change data and the other datapipe collects incident data. The collections from Service Desk 4.5 take place once a day. Compliance Manager does not collect availability data directly from OVIS. Compliance

Manager collects OVIS data from the Internet Services Datapipe. The Internet Services Datapipe collects data from OVIS every 15 minutes, and the collection from the Internet Services Datapipe takes place once a day.

The first data collection will take place at night, so even though everything is installed and your data modelling chores are finished, you will not see data in reports until the day after the first collection. On that first day following the first collection, you will see some data in every report, even though every report is designed to show data in monthly amounts. Any column that holds a month's worth of data will also hold less than a month's worth of data, so until the first calendar month is over, you will be looking at month-to-date data.

Compliance Manager offers reports for users and reports for the administrator. These are the reports for users:

- Business Process Status
- Business Process Status: Month-to-Date
- Application Status
- Application Status: Month-to-Date
- Application Instance Status
- Component Group Incidents
- Component Group Changes
- Component Group Availability
- Component Availability
- Incident KCI Source Data
- Incident KRI Source Data

These are the reports for the administrator:

- Administration and Deletion
- Configuration and Logging
- Table Structures and Sizes

The data in the reports for users comes from three process control areas:

- Availability management (OVIS)
- Incident management (Service Desk)
- Change management (Service Desk)

Each process control area contains multiple metrics, and each metric is classified as either a Key Risk Indicator (KRI) or a Key Control Indicator (KCI). The tables below list all the metrics in each process control area and indicate whether each metric is a risk indicator or a control indicator. A control indicator is more crucial than a risk indicator.

Process Control Area: Availability Management

Metric	Type of Indicator
Measured Unavailability	KRI
Planned Unavailability	KRI
Unplanned Unavailability	KCI

Process Control Area: Incident Management

Metric	Type of Indicator
Total Major Incidents	KRI
Percent Incidents over Deadline	KRI
Total Incidents	KRI
Average Duration Major Incidents	KCI
Percent Major Incidents over Deadline	KCI

Process Control Area: Change Management

Metric	Type of Indicator
Total Changes	KRI
Total Emergency Changes	KRI
Total Open Changes	KRI
Total Detected Changes No Ticket	KCI

Threshold Violations: Color-Coding and Numeric Totals

You are responsible for setting thresholds for every component group. If the value for a metric is below the threshold for the month, the status is green, indicating compliance. If the value for a metric exceeds the threshold, the status changes from green to either orange or red. Risk indicator violations are orange; control indicator violations are red.

Use the following forms, available in the **Object-Specific Tasks** pane of the Management Console, to set thresholds:

- Configure Availability Thresholds
- Configure Change Thresholds
- Configure Incident Thresholds

Some reports display the number of thresholds violations recorded for the month and some provide color-coding but no totals. Violation totals do not appear in these higher-level reports:

- Business Process Status
- Application Status

If you need the number, use the Application Instance Status Report, or any of the component group overview reports.

Periodic Maintenance

Since applications and components can come and go, you need to be able to make periodic changes to the data model. You have two forms for that purpose, Business Process Deletion and Application Deletion. Use the Business Process Deletion form to eliminate an entire business process and all its associated applications. Use the Application Deletion form to:

- Delete an application and everything associated with it
- Delete one or more application instances underneath an application
- Delete one or more component groups underneath an application instance

When you delete an item using a form, the item will disappear from reports immediately. As explained in [Chapter 3, Creating a Data Model](#), you can let the data for the item age out naturally, or you can run a nightly process to remove the data as soon as possible.

Upcoming Enhancements

The following table provides details about version history.

Version	Release Date	Features/Enhancements
1.0	March 2006	Initial release: <ul style="list-style-type: none"> • Requires OVPI 5.1 SP2 • 9 user reports • 3 admin reports • 1 launch point report • Thresholds sub-package • Create forms for the data model • Change forms for thresholds • Change form for BP/APP assignment • Demo package

Expect the following enhancements in future releases:

- Extended collections, with extended aggregations, for existing control areas:
 - Change Management
 - Availability Management
- New control areas related to Service Desk:
 - Configuration Management
 - Release Management
 - Information Security Management
- Additional datapipes for OpenView applications:
 - Service Desk 5.0
 - Configuration Management (App Manager, Patch Manager)
 - Select Identity
- Additional datapipes for third-party applications
- Cross-launching to additional reports (for example, reports in System Resources)
- Trending analysis in historical status reports and month-to-date reports

Sources for Additional Information

This user guide includes screen captures taken from the demo package. The demo package contains samples of every report in the report pack. If you have access to the demo package and you want to know what fully-populated reports look like, install the demo package. Like real reports, demo reports are interactive. Unlike real reports, demo reports are static.

The following release notes and user guides are related to Compliance Manager:

Release Notes: Compliance Manager

- *Compliance Manager CD Release Notes, December 2005*
- *Compliance Manager Report Pack 1.0 Release Notes, December 2005*
- *Compliance Manager OVIS Datapipe 1.0 and 1.1 Release Notes, February 2006*
- *Compliance Manager Service Desk Datapipe 1.0 Release Notes, December 2005*

Release Notes: OVPI

- *OVPI 5.1 Service Pack 2 Release Notes, 31 August 2005*

Release Notes: Other OpenView Applications

- *Internet Services Report Pack 2.0 Release Notes, October 2005*
- *Thresholds Module 5.0 Release Notes, June 2005*

User Guides: Compliance Manager

- *Compliance Manager OVIS Datapipe 1.0 User Guide, March 2006*
- *Compliance Manager Service Desk Datapipe 1.0 User Guide, March 2006*

User Guides: Other OpenView Applications

- *Internet Services Report Pack 2.0 User Guide, October 2005*
- *Service Desk Reporting Solution User Guide, May 2006*
- *Thresholds Module 5.0 User Guide, December 2005*

If you want to download manuals for any OpenView application, including manuals for the reporting solutions that run on OVPI, go to this site:

<http://www.managementsoftware.hp.com>

Select **Support** > **Product Manuals** to reach the **Product Manuals Search** page. The user guides for OVPI are listed under **Performance Insight**. The user guides for report packs and datapipes are listed under **Performance Insight Reporting Solutions**.

The manuals listed under **Performance Insight Reporting Solutions** indicate the month and year the manual was published. If a manual is revised and reposted, the date on the title page will change. Since we post revised manuals on a regular basis, we recommend searching this site for updates before using any of the manuals that were copied to the Docs directory on the Compliance Manager CD.

2 Installing the CM Report Pack

This chapter covers the following topics:

- Guidelines for a smooth installation
- Contents of the Compliance Manager CD
- Hardware and software requirements
- Using Package Manager to install Compliance Manager 1.0
- Finding forms and reports
- Bringing up the web interface
- Uninstalling the Compliance Manager Report Pack

Guidelines for a Smooth Installation

The Compliance Manager 1.0 CD includes a package extraction program. When you insert the Compliance Manager 1.0 CD in the CD-ROM drive, the package extraction program starts automatically. Once you make your selections, the install script extracts every package on the CD to the Packages directory on your system. When the extract finishes, the install script launches Performance Insight and starts Package Manager.

Once Package Manager is running, you are free to install any prerequisite package that is not already installed. When all of the prerequisites are in place, your only remaining task is to install two packages, ComplianceManager and ComplianceManager_Thresholds. Before using Package Manager to install any package, be familiar with the contents of the Compliance Manager CD and understand the hardware and software requirements.

Contents of the Compliance Manager CD

The Compliance Manager CD includes the Compliance Manager Report Pack and many other packages. The following table provides a list of the directories inside each package.

Package	Directories
Compliance Manager	ComplianceManager.ap ComplianceManager_Demo.ap ComplianceManager_Thresholds.ap Docs
CM OVIS Datapipe	CM_OVIS_Datapipe.ap Docs

Package	Directories
CM Service Desk Datapipe	CM_SvcDsk_Datapipe.ap ServiceDesk_Integration Docs
Thresholds	Thresholds.ap Docs
Internet Services Report Pack	Internet_Services.ap Internet_Services_Demo.ap UPGRADE_Internet_Services_to_20.ap Docs
Internet Services Datapipe	Internet_Services_Datapipe.ap
Common Property Tables	CommonPropertyTables.ap UPGRADE_CommonPropertyTables_to_35.ap Docs
Compliance Manager Portlet	Portlet_WAR/itcompliance.war

The Docs directory contains user guides and release notes. Before using any document in any Docs directory, check for updates on the web (**OpenView Support > Product Manuals > Product Manuals Search**). Most of the documents in the Docs directory are dated September 2005. If you find a document on the web that is more current, use that document instead.

Hardware and Software Requirements

Minimum Hardware Requirements

- 2 GHz Pentium IV CPU or equivalent powered UNIX system
- 2 GB RAM (swap file size must be physical RAM)
- 12 GB drive free space + swap file size space

Supported Operating Systems

- Microsoft Windows 2000 SP4
- Windows 2003 SP1
- HP-UX 11.1
- Solaris 8/9

Oracle Requirements

- Oracle 9.2.0.5 with patch, or
- Oracle 9.2.0.6

OVPI Requirements

- Service Pack 2 for OVPI 5.1
- Common Property Tables 3.5
- Thresholds Module 5.0

Service Pack 2 for OVPI 5.1

Service Pack 2 was released September 2005. Service Pack 2 corrects several defects in OVPI 5.1, adds Oracle 9.2.0.6 support, and adds support for pivot tables, also known as cross-tabs. Since Compliance Manager uses pivot tables, installing Service Pack 2 is mandatory. You can download Service Pack 2 from:

http://support.openview.hp.com/cpe/ovpi/patch_ovpi.jsp

For details about cross-tabs and other new features, refer to *Release Notes for OVPI 5.1 Service Pack 2*, dated 31 August 2005.

Common Property Tables

You have two ways to meet the requirement for Common Property Tables:

- Upgrade to Common Property Tables 3.5 from an earlier release
- Install Common Property Tables 3.5 for the first time

If no version of Common Property Tables is currently installed, Package Manager will install Common Property Tables for you, automatically. If you need to upgrade, installing the upgrade package is easy. Just be sure to upgrade Common Property Tables first, before doing anything else, and do not install other packages when you do this. If you need help with the upgrade, refer to the *Common Property Tables 3.5 User Guide*.

Thresholds Module

There is a thresholds sub-package that comes with Compliance Manager 1.0. The file name is:

ComplianceManager_Thresholds.ap

Installing ComplianceManager_Thresholds.ap is mandatory. When you install it, Package Manager will install a similar-sounding prerequisite package—the Thresholds Module—for you, but only if the Thresholds Module is not already installed. If you are currently running an earlier version of the Thresholds Module, you should upgrade to the latest version. Do this upgrade after upgrading Common Property Tables.

OVIS Integration Requirements

- Internet Services Report Pack 2.0
- Internet Services Datapipe 1.0
- Compliance Manager HP OpenView Internet Services (OVIS) Datapipe 1.0

If you are currently running version 1.0 of the Internet Services Report Pack, you can upgrade to version 2.0 by installing UPGRADE_Internet_Services_to_20.ap. If you are new to OVPI and you are not running any version of the Internet Services Report Pack, install version 2.0. For details about the Internet Services Report Pack, including data collection, report descriptions, installation, and the procedure for adding an OVIS system as a supported database, refer to the *Internet Services Report Pack 2.0 User Guide*.

The CM OVIS Datapipe collects availability data from tables maintained by the Internet Services Datapipe. For details about the CM OVIS Datapipe, including details about the OVIS Data Model Assignment form, refer to the *CM OVIS Datapipe 1.0 User Guide*.

Service Desk Integration Requirements

- Service Desk 4.5 with SP 14, or later; with the following configuration restrictions:
 - No more than four service levels (less than four is okay)
 - No more than three configuration item levels (less than three is okay)
 - Must recognize major incidents as well as non-major incidents
- Compliance Manager Service Desk Datapipe 1.0

The Compliance Manager Service Desk Datapipe collects data from Service Desk 4.5. For details, including package installation and CM/SD data integration, refer to the *CM Service Desk Datapipe 1.0 User Guide*.

CM Portlet Host Requirements

The CM portlet is compatible with the following host systems:

- BEA WebLogic 8.1
- Apache Pluto
- Apache Jetspeed 2

Installing the CM Report Pack

Follow these steps to extract packages from the Compliance Manager CD and install the Compliance Manager Report Pack:

- 1 Log in to the system. On UNIX systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.
Windows NT: Select **Settings > Control Panel > Administrative Tools > Services**
UNIX: As root, do one of the following:
HP-UX: `sh /sbin/ovpi_timer stop`
Sun: `sh /etc/init.d/ovpi_timer stop`
- 3 Insert the Compliance Manager CD in the CD-ROM drive and follow the instructions for extracting packages from the CD to the Packages directory on your system. On Windows, the instructions appear in a Main Menu that opens automatically. On UNIX, log in as root, mount the CD (if the CD does not mount automatically), navigate to the top level of the CD directory, and run the `./setup` command.
- 4 When the extract finishes, the install script launches Performance Insight and starts Package Manager. The Package Manager welcome window opens.
- 5 Click **Next**. The Package Location window opens.
- 6 Click **Install**. Approve the default destination directory or browse to the correct directory.
- 7 Click **Next**. The Report Deployment window opens. Type your username and password.

- 8 Click **Next**. The Package Selection window opens. Click the check boxes for:
 - ComplianceManager*
 - ComplianceManager_Thresholds*
 - ComplianceManager_Demo*
- 9 Click **Next**. The Type Discovery window opens. Disable the default.
- 10 Click **Next**. The Selection Summary window opens.
- 11 Click **Install**. The Installation Progress window opens and the install begins. When the install finishes, a package installation complete message appears.
- 12 Click **Done**.
- 13 Restart OVPI Timer.

Windows NT: Select **Settings > Control Panel > Administrative Tools > Services**

UNIX: As root, do one of the following:

HP-UX: **sh /sbin/ovpi_timer start**

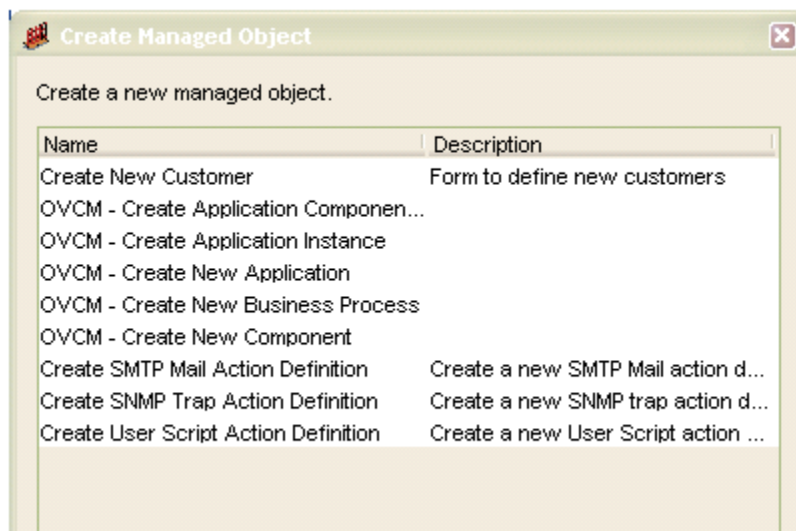
Sun: **sh /etc/init.d/ovpi_timer start**

The Compliance Manager Report Pack is now installed on OVPI. Your next step is to create a data model using the forms in the Create Managed Object window. Once the data model is finished, and your thresholds are set, you can install datapipes. Although installing a datapipe is easy, we recommend that you consult the user guide for the datapipe. The user guide contains information about mapping source data to the data model.

Finding Forms and Reports

Installing Compliance Manager 1.0 deploys several “create” forms, several change forms, and numerous reports. Until you create your data model, install datapipes, and use forms that come with each datapipe to assign incoming source data to the data model, change forms will have no data in them and reports will be empty. Although empty forms and empty reports are not very fascinating, eventually you will need to know where these items are located.

To access the create forms, start the Management Console, open the Object/Property Management frame, and select **File > New**. The Create Managed Object window opens.



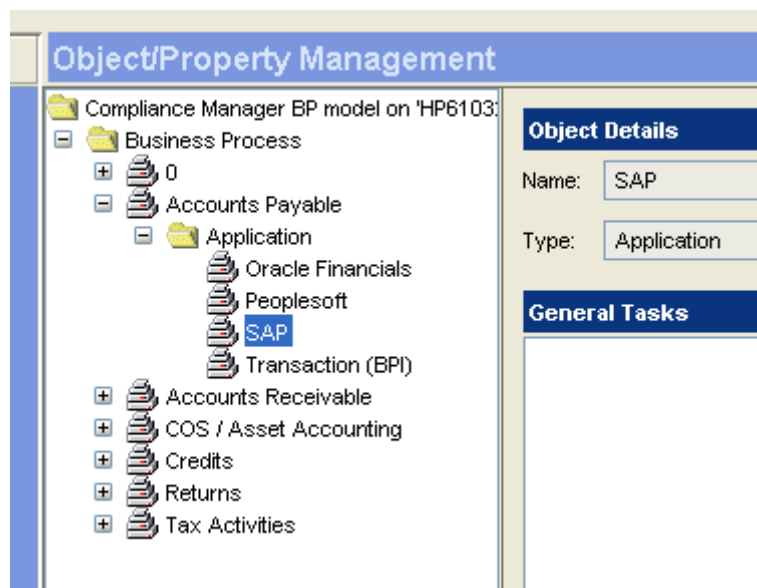
The create forms let you create new objects. A business process, an application, an application instance, a component group, and a component are all objects. Once you create the new object, OVPI adds the object to the object model. Assuming you completed the data model planning activity discussed in [Chapter 3, Creating a Data Model](#), you can start using the create forms immediately.

Finding New Views of the Object Model

Creating new objects adds new objects to the OVPI object model. Creating new objects also creates new views of the OVPI object model. The new views are Business Process and Application. To select either view, start the Management Console, open the Object/Property Management frame, and select **View > Change View**. The Business Process view is the higher-level view. It shows two types of objects:

- Business processes
- Applications

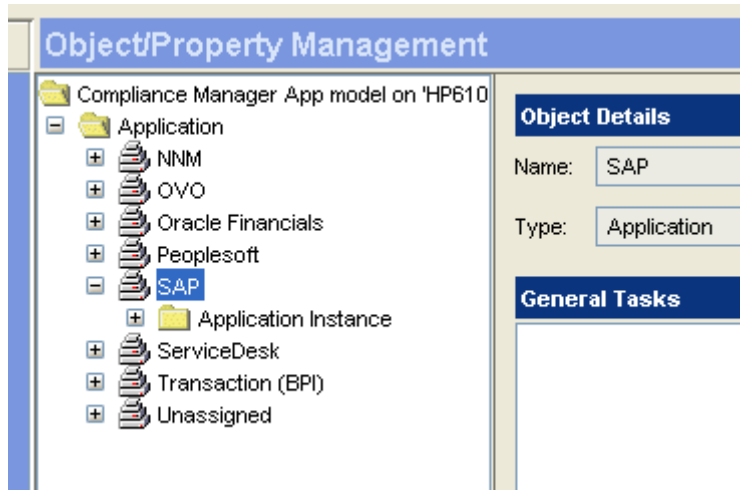
The next screen shot shows an example of the object model's Business Process view. You can see a list of business processes underneath the Business Process folder. To display a list of the applications that support a business process, expand the business process directory (Accounts Payable), then expand the Application folder.



The Application view shows the following objects:

- Application
- Application instance
- Component group
- Component

The next screen shot shows an example of the Application view. You can navigate from an application (SAP) to the Application Instance folder, and from an application instance to the Component Group folder. From a component group you can navigate to individual components.



Finding Change Forms

Change forms appear in two places:

- Management Console > Objects > Object/Property Management > General Tasks
- Management Console > Objects > Object/Property Management > Object Specific Tasks

Change forms make it easy to configure thresholds, delete applications, assign business processes to applications, modify the business process/application relationship, and perform administrative tasks. Change forms are object-specific. If you are highlighting an application instance, the change form will pre-select that instance of the application in the drop-down menus. Change forms appear or disappear depending on where you are in the object model. The following table provides a list of the forms available at each level in the object model.

Object Model Level	Forms You Can Access
Business Process	OVCM Logging and Data Maintenance OVCM Planned Downtime Manual Entry Application Deletion Application Relationships
Application	OVCM Logging and Data Maintenance OVCM Planned Downtime Manual Entry Add Notes Application Deletion Application Relationships Configure Availability Threshold Configure Incident Threshold Configure Change Threshold

Object Model Level	Forms You Can Access
Application Instance	OVCM Logging and Data Maintenance OVCM Planned Downtime Manual Entry Add Notes Configure Availability Threshold Configure Incident Threshold Configure Change Threshold
Component Group	OVCM Logging and Data Maintenance OVCM Planned Downtime Manual Entry Add Notes Configure Availability Threshold Configure Incident Threshold Configure Change Threshold
Component	OVCM Logging and Data Maintenance OVCM Planned Downtime Manual Entry

Finding Reports

If the OVPI client applications are installed on your system, you can use any of the following applications to open reports:

- Report Viewer
- Report Builder
- Management Console

If you have the Management Console, reports are listed under Object Specific Reports, and any report you open is automatically constrained by your location in the object model. If you intend to view reports on the web, use your web browser to reach the Web Access Server. Once you log in, you will see the following folders:

- Admin
- Historical
- Month-to-date
- Integration

Reports in these folders are not constrained. In the Historical folder you will find every report except the two month-to-date reports. For more information about the three historical status reports and the month-to-date reports, see Chapter 4. For more information about the component group overview reports, see Chapter 5. For more information about the admin reports, see Chapter 6. The Integration folder contains one or more datapipe-specific linkage reports. For details about any linkage report, refer to the user guide for the datapipe.

Using the Web Interface

Follow these steps to access the web interface:

1 Browse to your OVPI server. The **Log On** window opens.

2 Select **Log On**.

Type the username and password you created when OVPI was installed, or the username and password assigned to you by the administrator. The OVPI default user name is *trendadm* and the recommended password, for simplicity, is *trendadm*.

3 The OVPI Home Page opens. The **History** section contains a list of the last 10 reports you looked at. Ten is a default value that can be changed. The **Favorites** section contains links you selected earlier. In the top-right menu, select **Catalog**.

4 In the left pane, expand **System**.

5 Expand **Launch Point**.

6 Select **Compliance Manager - Launch Point**. The Launch Point page opens.

The screenshot displays the HP OpenView Performance Insight web interface. At the top, there is a navigation bar with the HP logo on the left and a user profile section on the right showing 'Profile | Log off trendadm'. Below the profile are several menu items: Home, Catalog, Preferences, Administration, Schedule, and Help. The main content area is divided into two panes. The left pane shows a tree view of the system structure, with 'System' expanded to show 'Launch Point', which is further expanded to show 'Compliance Manager - Launch Point'. The right pane displays the 'Compliance Manager Launch Point' page. This page has a title 'Compliance Manager Launch Point' and a sub-header 'Launch Point'. Below this, there is a large yellow box containing text about the Compliance Manager package, its purpose, and how it monitors IT process areas. To the right of this text is a vertical list of report categories: Business Processes, Applications, Application Instances, Instance Component Groups, and Administrative Reports. At the bottom of the page, there is a 'Back to Top' link and a small icon.

7 Open reports by clicking the data model elements to the right or by expanding the report directories on the left.

The OVIS_Integration folder will not be part of the directory structure until the CM OVIS Datapipe is installed; likewise, the ServiceDesk_Integration folder will not be part of the directory structure until the CM Service Desk Datapipe is installed.

Uninstalling Compliance Manager

Uninstalling Compliance Manager automatically uninstalls any datapipe used by Compliance Manager. Uninstalling Compliance Manager also uninstalls ComplianceManager_Thresholds. Uninstalling Compliance Manager has no impact on the following packages:

- Common Property Tables
- Thresholds Module
- Internet Services Report Pack

Follow these steps to uninstall Compliance Manager:

- 1 Log in to the system. On UNIX systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.

Windows NT: Select **Settings > Control Panel > Administrative Tools > Services**

UNIX: As root, do one of the following:

HP-UX: **sh /sbin/ovpi_timer stop**

Sun: **sh /etc/init.d/ovpi_timer stop**

- 3 From the Management Console, start Package Manager. The Package Manager welcome window opens.
- 4 Follow the on-screen directions for package removal; when prompted, select Compliance Manager 1.0. When the uninstall is complete, a package removal complete message appears.
- 5 Click **Done**.
- 6 Restart OVPI Timer.

Windows NT: Select **Settings > Control Panel > Administrative Tools > Services**

UNIX: As root, do one of the following:

HP-UX: **sh /sbin/ovpi_timer start**

Sun: **sh /etc/init.d/ovpi_timer start**

The Compliance Manager Report Pack is now uninstalled.

3 Creating a Data Model

The chapter covers the following topics:

- Planning your data model
- Creating your data model
- Setting thresholds
- Planning ahead for downtime
- Periodic maintenance

Planning Your Data Model

Compliance Manager is an aggregator of information. It retrieves data from multiple sources, merges data from multiple sources, and uses merged data to create a combined view of an IT infrastructure. The view that Compliance Manager produces adheres to a particular data model or template. This template consists of two high-level elements and a set of lower-level elements. The high-level elements are:

- Business processes
- Enterprise-wide applications that support each business process

An enterprise-wide application contains these lower-level elements:

- Specific instances of that application
- Groups of components that make up the instance
- Components that make up the group

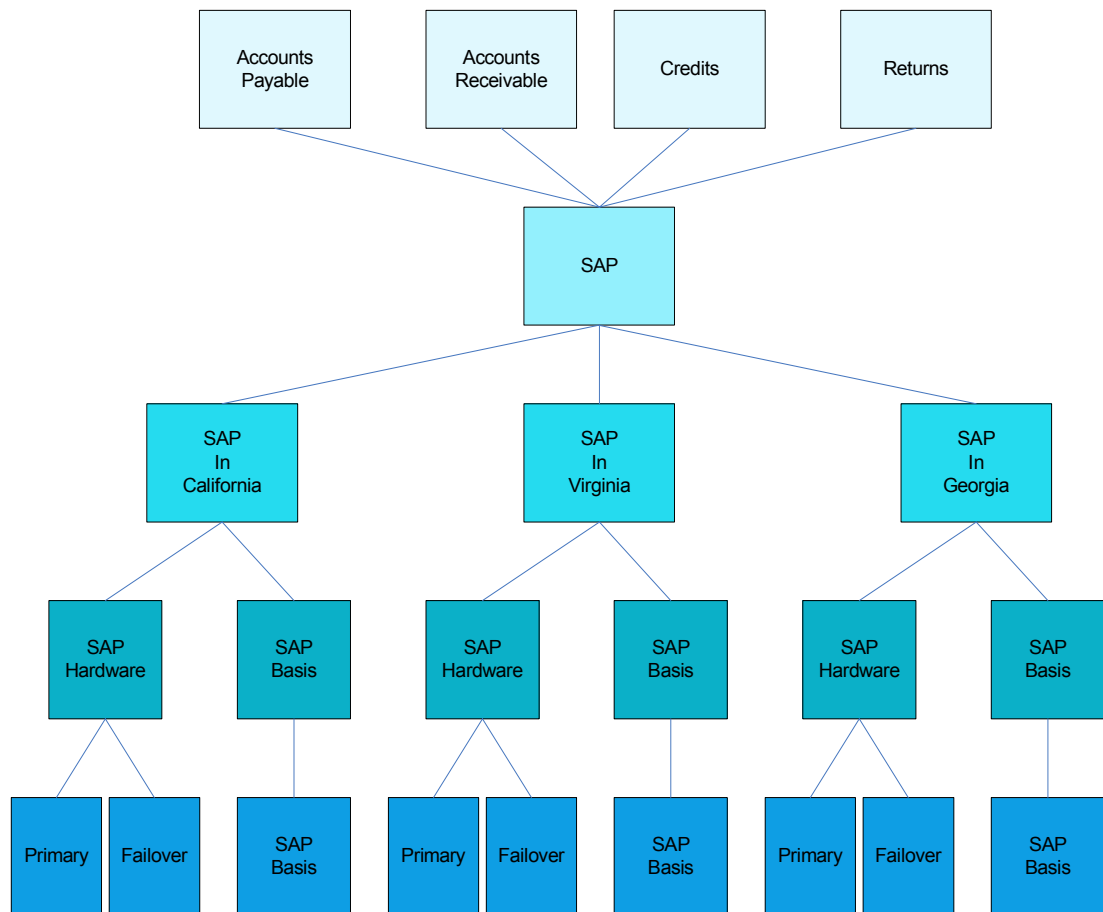
Compliance Manager cannot create a combined view of your IT infrastructure until you do two things—generate a view of your business that aligns with this data model, and create the structure that Compliance Manager needs to aggregate information. Here is an example of an environment that accommodates the data model:

- Your company is a large national manufacturer of computer hardware. Your business processes such as Accounts Payable, Accounts Receivable, Credits and Returns rely on several applications and one of those applications is SAP.
- You use multi-platform SAP installations in three different states to control your order entry and provisioning.
- OpenView Internet Services tracks application availability using a SAP-specific probe. OpenView Internet Services also tracks the availability of the hardware platforms the SAP instances run on using ICMP ping tests.
- Changes to your SAP applications, including changes to hardware and networking components are handled with the help of Service Desk. Service Desk is also tracking incidents logged with the help desk.

If we interpret this sample environment using the Compliance Manager data model, the environment would look like this:

Level	Structure	Content
1	Business Processes	Accounts Payable Accounts Receivable Credits Returns
2	Application Supporting all 4 BPs	SAP
3	Application Instances	SAP in Virginia SAP in California SAP in Georgia
4	Component Groups per Instance	SAP Basis (multiple) SAP Hardware (multiple)
5	Components	SAP Basis (multiple) Primary (multiple) Failover (multiple)

Here are the same results in diagram form:



Using Forms to Create a Data Model

As explained in the previous chapter, all of the create forms are listed in the Create Managed Object window. To open it, start the Management Console and click the Objects icon. Then select **File > New**. The Create Managed Object window opens. Use the create forms in this sequence:

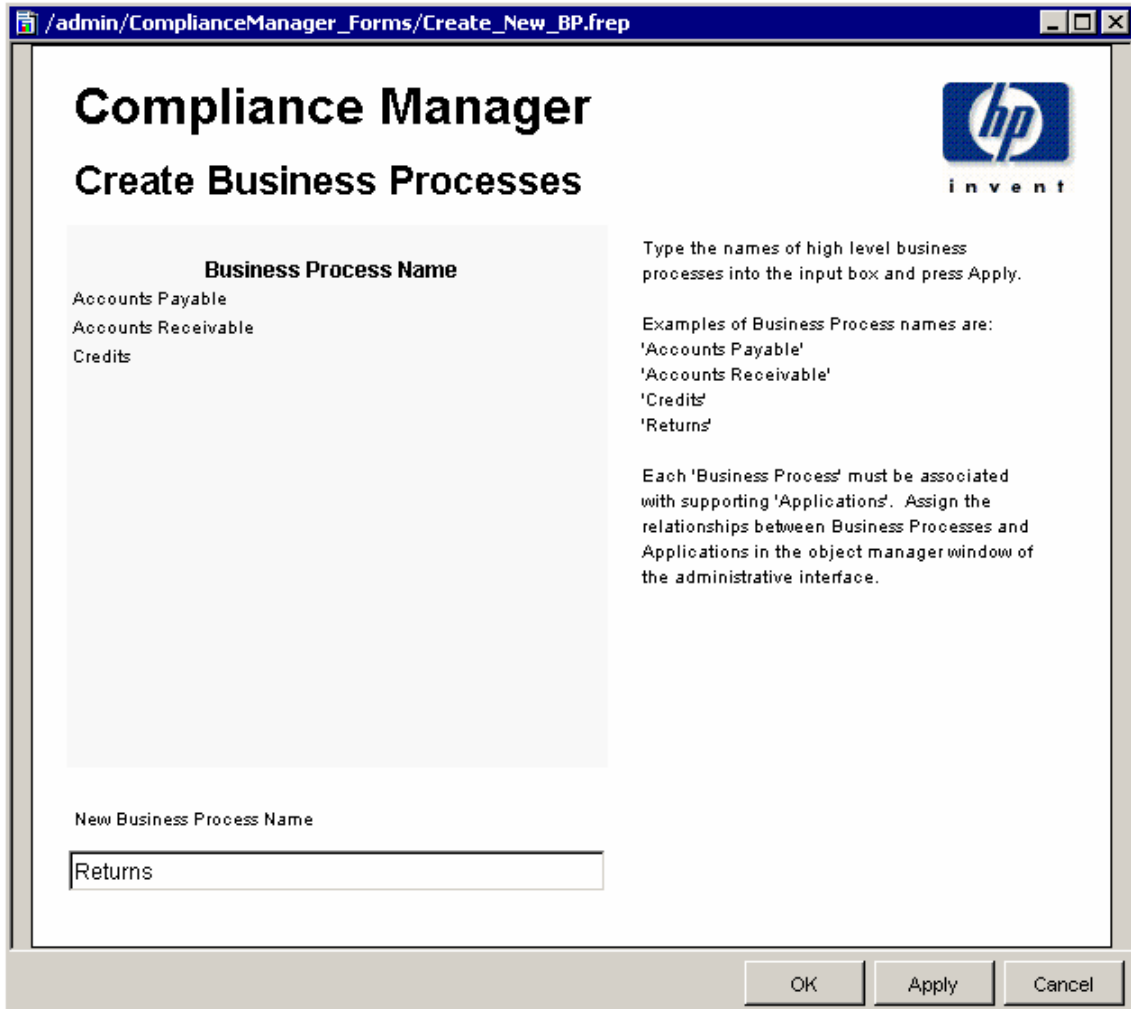
- 1 Create Business Process
- 2 Create Applications
- 3 Assign Business Processes to Applications (a task, not a create form)
- 4 Create Application Instances
- 5 Create Component Groups
- 6 Create Components

When you are working with a particular form, create everything at once—that is, create all of your business processes at the same time, create all your applications at the same time, and create all of your applications instances at the same time. When you have multiple instances of an object (for example, multiple instances of Primary, Failover, and SAP Basis) be sure to create multiple instances of the object.


The relationship between a business process and supporting applications is not built into the Create Application form. To establish that relationship, use item 3, Assign Business Processes to Applications. This form is actually an object-specific task, not a create form, and you will find it under **Object Specific Tasks**. The best time to assign business processes to applications is right after you finish creating business processes and applications.

When you finish assigning business processes to applications, move on to Step 4. Once you are at step 4, the hierarchy is built into the form, so having to open another form to define a relationship is not necessary.

There are no conventions to follow regarding what you can name an object. You may use special characters and spaces.



Compliance Manager
Create Supporting Applications



Existing Applications

Type the names of enterprise wide applications or application services into the input box and press Apply.

Each 'Application' supports one or more high level 'Business Processes' above it. It will also have multiple 'Instances' and each Instance may have groups of components.

Collected data relating to an Application will not be reflected in the Business Process reports until you assign the relationship between the two. Make that assignment using forms in the 'Object Manager' window of the administrative interface.

New Application Name

OK Apply Cancel

Compliance Manager

Application Relationships



Each Business Process is associated with one or more Applications. You can use this form to change the associations between Business Processes and Applications. Changes applied here will change how the status of each Business Process is affected by the underlying Applications. All changes are recorded in the logging report.

Search by Business Process Search by Support Search by Application

Business Process	Support	Application
Accounts Payable	Is Supported By	Oracle Financials
Accounts Payable	Is Supported By	Peoplesoft
Accounts Payable	Is Supported By	SAP
Accounts Payable	Is Supported By	Transaction (BPI)
Accounts Receivable	Is Supported By	Oracle Financials
Accounts Receivable	Is Supported By	Peoplesoft
Accounts Receivable	Is Supported By	SAP
Accounts Receivable	Is Supported By	Transaction (BPI)
COS / Asset Accounting	Is Supported By	Oracle Financials
COS / Asset Accounting	Is Supported By	Peoplesoft
COS / Asset Accounting	Is Supported By	Transaction (BPI)
Credits	Is Supported By	SAP
Credits	Is Supported By	Transaction (BPI)
Returns	Is Supported By	Oracle Financials
Returns	Is Supported By	SAP
Tax Activities	Is Supported By	Peoplesoft
Tax Activities	Is Supported By	SAP
Tax Activities	Is Supported By	Transaction (BPI)


Is Supported By

OK Apply Cancel

/admin/ComplianceManager_Forms/Create_New_Application_Instance.frep

Compliance Manager

Create Application Instances



Select an Application

SAP

Application Instances

SAP in California
SAP in Virginia

An 'Application Instance' is a specific instance of a company wide Application. Each Instance must have one or more groups of components.

Select an Application - use the other create forms if you don't have the Application that you need. Now type the name of an Instance into the input box and press Apply.

Examples of application instances would be:
'Primary Oracle Warehouse'
'Failover Oracle Warehouse'
'SAP for Internal Audit Dept'
'SAP for Payroll Dept'

New Application Instance Name


SAP in Georgia

OK Apply Cancel

/admin/ComplianceManager_Forms/Create_New_App_Inst_Comp_Grp.frep

Compliance Manager

Create Component Groups



Select an Application

SAP

Select an instance of the application

SAP in California

An 'Application Instance Component Group' is a name given to any group of elements which makes up an application instance - hardware or software. Each 'Group' belongs to one and only one Application Instance

Select an Application and an Instance of that Application - use the other create forms if you don't have the Applications and Instances that you need. Now type the names of component groups into the input box and press Apply.

Examples of application component groups:

- 'App Servers'
- 'Databases'
- 'Workstations'
- 'Data Collectors'

Existing Component Groups

SAP Hardware

Each Component Group can have thresholds for Availability, Changes, Incidents, Security, Configuration and Release Management. Use the forms in the object manager window of the administrative interface to set these threshold values.

New Component Group Name

SAP Basis

OK Apply Cancel

Compliance Manager

Create Components



Select an Application

Oracle Financials

Select an instance of the application

UK Central Server

Select a Component Group

Central App Servers

Existing Components

HTTP Server 1
HTTP Server 2

An 'Application Instance Component' is a name given to any elements which makes up an application instance - hardware or software. Each 'Component' belongs to one and only one Application Instance

Component Group.

Select an Application, an Instance of that Application and a Component Group name - use the other create forms if you don't have the values that you need. Now type the names of components into the input box and press Apply after each.

New Component Group Name

OK

Apply

Cancel

Setting Thresholds


As soon as the data model is defined, you can set thresholds. Threshold forms are object-oriented forms and like all object-oriented forms, you cannot see them or use them from the web interface. They are visible from the Management Console only. To open the threshold forms, start the Management Console and the select **View > Change View > Application**. You will see the threshold forms under **Object Specific Tasks**.

Thresholds values are not inherited. You cannot set the threshold at the Application Instance level and then let those value be inherited by the component groups. You must set thresholds for each component group under each Application Instance. The thresholds you set are allowed to vary from component group to component group.

The **mirrored** option applies to the availability form only and rarely will this option be enabled. If you want to monitor redundant components separately, enable this option. If this option is enabled, consider the impact on data aggregation and information flow.

Compliance Manager

'Availability' Settings



Choose an Application

NNM
▼

Choose an Application Instance

East
▼

Modify the settings for an application component group using this form. Use the allowable values to set tolerances for each component group KRI or KCI Availability metric. Increasing the allowable value for a threshold makes it less likely to be breached.

The 'Allowed' values represent the threshold for that metric per month. Metric counters are reset at the beginning of each month.

Managed components (hardware and software entities) can be grouped as to their redundancy capabilities. For example: a web server demon may be mirrored many times over, so the loss of one child process has no effect on availability.

Use the allowable values to set tolerances for each component group. The unit of measurement is seconds (s).

Component Group Name	Mirrored ?	Allowed Measured Unavailability	Allowed Planned Unavailability	Allowed Unplanned Unavailability
East	No	500	500	100

Are the components mirrored ?

No
▼

Allowed Measured Unavailability

500

Allowed Planned Unavailability

500

Allowed Unplanned Unavailability

100

Compliance Manager



'Change' Settings

Choose an Application

Modify the threshold values for an application component group using this form. Use the allowable values to set tolerances for each component group KRI or KCI change metric. Increasing the allowable value for a threshold makes it less likely to be breached.

Choose an Application Instance

The 'Allowed' values represent the threshold for that metric per month. Metric counters are reset at the beginning of each month.

Allowable Monthly Thresholds

Component Group	No. Changes With No Ticket	No. New Changes	No. Open Changes	No. Emergency Changes
All CL05	1	10	20	5

Allowed # Changes with No Ticket

Allowed # New Changes

Allowed # Open Changes

Allowed # Emergency Changes

Compliance Manager



'Incident' Settings

Select an Application

Select an instance of the application

East
North
South
West

Modify the settings for an application component group using this form. Use the allowable values to set tolerances for each component group KRI or KCI Incident metric. Increasing the allowable value for a threshold makes it less likely to be breached.

The 'Allowed' values represent the threshold for that metric per month. Metric counters are reset at the beginning of each month.

Component Group Name	Allowed No. Incidents	Allowed % Incidents Over Deadline	Allowed % Major Incidents Over Deadline	Allowed No. Major Incidents	Allowed Avg Duration Major Incidents (Days)
East	100	10	10	20	1

Allowed No. Incidents

Allowed No. Major Incidents

Allowed % Incidents Over Deadline

Allowed Average Duration Major Incidents

Allowed % Major Incidents Over Deadline

Planning Ahead for Downtime

The Planned Down Time metric is not collected automatically. But because it is used in various calculations, it must be entered manually. Follow these steps to enter planned downtime manually:

- 1 From the Management Console select **Objects**.
- 2 Under **General Tasks** double-click **OVCM – Planned Down Time Manual Entry**.
- 3 Filter the component groups by application and application instance
- 4 Select the desired component group.
- 5 Select the desired component.

- 6 Select the desired future date. Planned down-time can be entered from 2 to 6 days in advance
- 7 Enter the planned down time in seconds.
- 8 Click **Apply**.

Compliance Manager



Planned Downtime - Manual Entry

Use this form to manually update the 'Planned Downtime' metric for a component. Planned Downtime is one of the Availability KRIs and will be used in conjunction with the 'Allowed Planned Downtime' threshold to calculate if a KRI has been breached. Availability thresholds take account of the 'Mirror' feature where several components can operate in failover mode. Select an Application, Instance, Component Group and Component then update the Planned Downtime for a particular day. The value entered should be in seconds. You can only update Planned Downtime for days in the future on Components which are actively receiving data.

Select an Application

Select an Instance of the Application

Filter by Application

Filter by Instance

Select a Component Group

Application	Instance	Component Group	Allowed Planned Downtime	Is Mirrored
NNM	East	East	500	No
NNM	North	North	500	No
NNM	South	South	500	No
NNM	West	West	500	No
OVD	Europe	Europe	500	No

Select a Component

East

Date

Future Planned Downtime (secs)

Enter Planned Downtime (secs) for the Selected Day

Planned Downtime for the Selected Component

No Data

Maintaining the Data Model

Since applications and components can come and go, you need a method for making periodic changes to the data model. You have two forms for that purpose, Business Process Deletion and Application Deletion. Use the Business Process Deletion form to eliminate an entire business process and all the applications and application instances associated with it. Use the Application Deletion form to:

- Delete an application and everything associated with it
- Delete one or more application instances underneath an application
- Delete one or more component groups underneath an application instance

When you delete an element using one of the forms, the element will disappear from reports immediately. You can let the data for the item age out naturally, or you can run a nightly process to remove the data as soon as possible.

Compliance Manager
Business Processes Deletion

Use this form to mark unnecessary Business Processes for removal. By default, a Business Process will only be removed when all of the data associated with it has been removed from the system. Until then it will remain 'Marked for Deletion'. It is possible to change the deletion method and force the removal of data model elements and their data. The deletion routine runs a nightly basis.

Business Process	Marked for Deletion
Accounts Payable	Yes

Yes - delete it.

OK Apply Cancel

The data aging option is controlled by a setting on the Administration form, shown below on page 36. Your choices are:

- Follow table retention period rules
- Force data removal

The default is to follow table retention period rules.

Compliance Manager

Application Deletion

Use this form to mark unnecessary Applications and their elements for deletion from the CM data model. An Application or its elements will only be deleted when all of the data associated with it has been removed from the system. Until then it will remain 'Marked for Deletion'. Deletions are performed on a recursive basis. Marking any element for deletion will mark all of the associated child elements too and will disable any further data collections for those elements. Subsequently removing the 'Marked for Deletion' flag will have the effect of restarting collections again.

Application	Instance	Component Group	Component	Marked for Deletion	Has Marked for Deletion Children
NNM	-	-	-	No	
NNM	East	-	-	No	
NNM	East	East	-	No	
NNM	East	East	East	No	
NNM	North	-	-	No	
NNM	North	North	-	No	
NNM	North	North	North	No	
NNM	South	-	-	No	
NNM	South	South	-	No	
NNM	South	South	South	No	
NNM	West	-	-	No	
NNM	West	West	-	No	
NNM	West	West	West	No	
OVO	-	-	-	No	
OVO	Europe	-	-	No	
OVO	Europe	Europe	-	No	
OVO	RoW	-	-	No	
OVO	RoW	RoW	-	No	
Oracle Financials	-	-	-	No	
Oracle Financials	UK Central Server	-	-	No	
Oracle Financials	UK Central Server	Central App Servers	-	No	

Compliance Manager

Administration



Use this form to update the configuration settings for Compliance Manager logging and table maintenance. Click the Apply button to save any changes. Click the Cancel button to cancel any changes. Click the OK button to save changes and close the form.

The logging setting is used to determine the number and detail of messages sent to the 'Configuration and Logging Report'.

Selections include

- 0 = High Level only,
- 1 = Normal / Informational
- 2 = All / Debug

Compliance Manager data model elements (Applications, Business Processes etc) can be removed by marking them for deletion. They will normally only be removed when the data associated with them has aged out naturally. You can force the removal of all data associated with a marked for deletion element by setting the 'Deletion Method' to 1 instead of 0.

- 0 = Normal - follow table retention period rules
- 1 = Force data removal

Configuration	Value	Meaning
Logging Level	1	Normal
Deletion Method	0	Allow data to age

Change setting

OK

Apply

Cancel

4 Historical Status Reports

Compliance Manager accommodates a range of needs. It appeals to people who want their confidence levels confirmed as quickly as possible and who have no interest in the supporting details, and it also appeals to people who are interested in tracing a deficient condition to its source. The high-level status reports, along with the month-to-date versions, are designed primarily for the people in the first group. There are five status reports:

- Business Process Status
- Business Process Month-to-Date
- Application Status
- Application Status Month-to-Date
- Application Instance Status

These reports have two panes, top and bottom. The top pane is high-level, the bottom pane is supporting-level. Select a row in the top pane to display supporting-level detail in the bottom pane. When the business process in the top pane is supported by multiple applications, you will see multiple supporting applications in the bottom pane.

A color-coded block in the top pane (BP Status and Application Status) represents a month of data. Green indicates compliance, orange and red indicate non-compliance. When a block is orange, that means that there is an underlying KRI violation somewhere in the combination of components that supports the business process. When a block is red, there is an underlying KCI violation somewhere in the combination of components that supports the business process. If the block is green, there are no underlying violations for that particular month.

If the BP Status report indicates that one supporting application is causing most or all of the threshold breaches, you have these options:

- Close BP Status and open Application Status
- Open BP Month-to-Date (by clicking the BP in the top pane)

Application Status traces deficiencies from the Application to one or sometimes several supporting Application Instances. BP Month-to-Date traces deficiencies from the BP to the Application, and from the Application to one or more Process Areas.

If the Application Status report indicates that one supporting application is causing most or all of the threshold breaches, you have these options:

- Close Application Status and open Application Instance Status
- Open Application Month-to-Date (by clicking the Application in the top pane)

Application Instance Status traces deficiencies from the Application Instance to one or more months and to one or more Process Areas. The Application Month-to-Date traces deficiencies from the Process Area at the Application level to one or more Process Areas at the Application Instance level.

Compliance Manager

Historical Business Process Status

Examine the status of your high level business processes over the previous 12 months. The lower table shows the status of the enterprise wide applications which support the selected business process. Click on a problem business process area to focus on the applications supporting it. Cells are colored red to indicate a KCI breach, orange for a KRI breach and green for normal.

Business Process Status

	Aug 04	Sep 04	Oct 04	Nov 04	Dec 04	Jan 05	Feb 05	Mar 05	Apr 05
Accounts Payable	Red	Red	Green	Green	Green	Green	Green	Orange	Orange
Accounts Receivable	Red	Red	Green	Green	Green	Green	Green	Orange	Orange
CDS / Asset Accounting	Green	Red	Green	Green	Green	Green	Green	Orange	Orange
Credits	Red	Green	Green	Green	Green	Green	Green	Green	Orange
Returns	Red	Red	Green	Green	Green	Green	Green	Orange	Orange
Tax Activities	Red	Green	Green	Green	Green	Green	Green	Green	Green


Supporting Application Status

	Aug 04	Sep 04	Oct 04	Nov 04	Dec 04	Jan 05	Feb 05	Mar 05	Apr 05
Accounts Payable Oracle Financials	Green	Red	Green	Green	Green	Green	Green	Orange	Orange
Accounts Payable SAP	Red	Green	Green	Green	Green	Green	Green	Green	Orange

Compliance Manager

Month To Date - BP Status

Examine the current status of your high level business processes for this month to date. The lower table shows the status of the enterprise wide applications which support the selected business process.

Apr 2005 

Business Process Status

Business Process Name	Month Start	Key Control Status	Key F
Accounts Receivable	Fri, Apr 1 12:00 AM	0	
Accounts Payable	Fri, Apr 1 12:00 AM	0	
Credits	Fri, Apr 1 12:00 AM	0	
Returns	Fri, Apr 1 12:00 AM	0	
COS / Asset Accounting	Fri, Apr 1 12:00 AM	0	
Tax Activities	Fri, Apr 1 12:00 AM	0	

Supporting Application Status

Application Name	Availability	Security	Incident	Change	Release
Oracle Financials	KRI Breach
SAP	KRI Breach	.	.	KRI Breach	.

Compliance Manager

Application Status

Examine the status of your enterprise applications over the previous 12 months. The lower table shows the status of the specific instances which support the selected high level application. Click on an application to drill down to the instances of it.

Cells are colored red to indicate a KCI breach, orange for a KRI breach and green for normal.

Application Status Overview

	Aug 04	Sep 04	Oct 04	Nov 04	Dec 04	Jan 05	Feb 05	Mar 05	Apr 05
Oracle Financials	Green	Red	Green	Green	Green	Green	Green	Orange	Orange
SAP	Red	Green	Green	Green	Green	Green	Green	Green	Orange

Application Instance Status

	Aug 04	Sep 04	Oct 04	Nov 04	Dec 04	Jan 05	Feb 05	Mar 05	Apr 05
Oracle Financials UK Central Server	Green	Green	Green	Green	Green	Green	Green	Orange	Orange
Oracle Financials UK Satellite 1 Server	Green	Green	Green	Green	Green	Green	Green	Orange	Green
Oracle Financials UK Satellite 2 Server	Green	Red	Green	Green	Green	Green	Green	Orange	Orange

Compliance Manager

Month To Date - Application Status

Examine the status of your enterprise applications. The lower table shows the status of specific instances of the high level application. Click on an application to drill down. A list of business processes which rely on the selected application is provided.

Apr 2005

Application Status

Application Name	Month Start	Availability	Security	Incidents	Change	Release
Oracle Financials	01-Apr-2005	KRI Breach
SAP	01-Apr-2005	KRI Breach	.	.	KRI Breach	.

Application Instance Status

Instance Name	Availability	Security	Incident	Change	Release	Config
UK Central Server	KRI Breach
UK Satellite 1 Server
UK Satellite 2 Server	KRI Breach

**Business Pr
supported by thi**
Accounts Receival
Accounts Payable
Returns
COS / Asset Accou

Compliance Manager

Examine the status of your enterprise application instances on a month by month basis, for the previous 12 months.

Historical Application Instance Status

Applications

- Oracle Financials
- NNM
- OVO
- ServiceDesk
- Transaction (BPI)
- SAP
- Peoplesoft

Select an Application from the list. The Instance Status table below provides a historical view of months with high level KCI and KRI breaches colored accordingly. The numbers in the cells of represent the total number of breaches of KCI or KRI.

Red = KCI Breach
 Orange = KRI Breach
 Green = All Clear

The lower metrics table shows a month by month analysis of exactly which process area had the breaches. Click on a cell in the lower table to examine a targeted report for that selected Application Instance.

Application Instance Status

		Aug 04		Sep 04		Oct 04		Nov 04		Dec 04		Jan 05		Feb 05		Mar 05		Apr 05	
		KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI	KCI	KRI
Oracle Financials	UK Central Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Oracle Financials	UK Satellite 1 Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Oracle Financials	UK Satellite 2 Server	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Application Instance Status by Process Area

Time Period	Instance	Availability	Security	Incident	Change	Release
Apr 2005	UK Central Server	Orange	Green	Green	Green	Green
Mar 2005	UK Central Server	Orange	Green	Green	Green	Green
Feb 2005	UK Central Server	Green	Green	Green	Green	Green
Jan 2005	UK Central Server	Green	Green	Green	Green	Green
Dec 2004	UK Central Server	Green	Green	Green	Green	Green
Nov 2004	UK Central Server	Green	Green	Green	Green	Green
Oct 2004	UK Central Server	Green	Green	Green	Green	Green
Sep 2004	UK Central Server	Green	Green	Green	Green	Green
Aug 2004	UK Central Server	Green	Green	Green	Green	Green

5 Component Group Reports

Compliance Manager rolls up data and threshold counts from the lowest level of the data model to the highest level. Rolling up data and threshold counts produces a top-down view of compliance. This top-down view allows you to trace a deficiency showing up in a high-level status report to its source in components at the lowest level of the data model. For example, if the Application Instance Status report is showing deficiencies with a process control area, you can turn to a component group report to inspect that process control area in more detail.

There are three component group reports and three lower-level reports:

- Component Group Changes
- Component Group Availability
 - Lower level: Component Availability
- Component Group Incidents
 - Lower level: Component Group Incidents - KCI Data
 - Lower level: Component Group Incident - KRI Data

Component Group Changes

There are three drop-down lists at the top:

- Select application
- Select application instance
- Select month

Beneath the drop-downs, you can see a list of component groups associated with the selected application instance. For each component group, you have two aggregated values, one for all KCIs for the month, and one for all KRIs for the month.

Selecting a component group updates the rest of the report. Below the selection table, you have a notes section, a list of components, and list of the business processes supported by the component group. The source for notes is the Explanatory Notes form. (See page 42.) The Explanatory Notes form is a **General Tasks** form you can use whenever you need to add details about an event or situation that could impact compliance reporting.

At the bottom of the report there is a table and a graph. The table shows daily KCI data and daily KRI data. The graph contains the same data. The table and the graph make it easy to see when threshold breaches took place.



If you have any questions about which columns in a report are being populated by any one datapipe, refer to the user guide for the datapipe.

Compliance Manager

Component Group Changes

application, and instance of that application, and a time period to examine historical change metrics. Data is collected on a daily basis but thresholds apply to each calendar month. Coloured squares indicate a breach of the threshold.



Select an Application

Oracle Financials

Select a month

Apr 2005

Red = KCI Breach
Orange = KRI Breach

Select an Instance

UK Central Server

Application Instance Component Groups

Component Group Name	Month	# Changes No Tkt (KCI)	Allowed Changes No Tkt	# New Changes (KRI)	Allowed New Changes	# Open Changes (KRI)	Allowed Open Changes	# Emergency Changes (KRI)	Allowed Emergency Changes
Central App Servers	Apr 2005	1	1	10	10	20	20	5	5
Central DB	Apr 2005	1	1	10	10	20	20	5	5
Central Timer	Apr 2005	1	1	10	10	20	20	5	5

Notes:

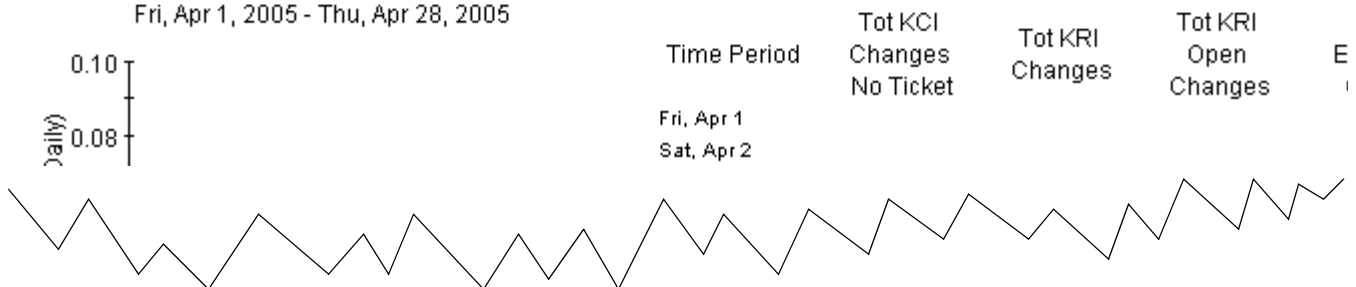
Components within this Group

Application	Instance	Component Group	Component
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2

Business Processes Supported by this Group

Changes - New, Open, Without Ticket and Emergency
Fri, Apr 1, 2005 - Thu, Apr 28, 2005

Daily Change Metrics

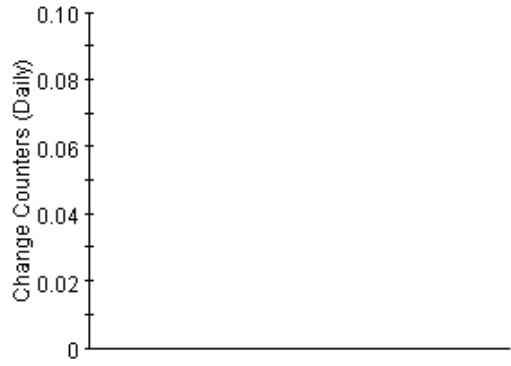




Notes:

Components within this Group				Business Processes Supported by this Component
Application	Instance	Component Group	Component	
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1	
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2	

Changes - New, Open, Without Ticket and Emergency
 Fri, Apr 1, 2005 - Thu, Apr 28, 2005



Daily Change Metrics

Time Period	Tot KCI Changes No Ticket	Tot KRI Changes	Tot KRI Open Changes	Tot KRI Emergency Changes
Fri, Apr 1				
Sat, Apr 2				
Sun, Apr 3				
Mon, Apr 4				
Tue, Apr 5				
Wed, Apr 6				
Thu, Apr 7				
Fri, Apr 8				
Sat, Apr 9				
Sun, Apr 10				
Mon, Apr 11				
Tue, Apr 12				
Wed, Apr 13				
Thu, Apr 14				
Fri, Apr 15				
Sat, Apr 16				

Component Group Availability

There are three drop-down lists at the top:


- Select application
- Select application instance
- Select month

Beneath the drop-downs, you can see a list of component groups associated with the selected application instance. For each component group, you have a value for each KRI and each KCI. Red and orange indicate a threshold violation.

Selecting a component group updates the rest of the report. Below the selection table, you have a notes section, a list of components, and list of the business processes supported by the component group. The components in the list of components are links. Select a link to open Component Availability. Again, the source for the notes is the Explanatory Notes form.

At the bottom of the report is a graph and a table. Both the graph and the table track the same two KCIs and the same KRI. The table and the graph make it easy to see which days during the month were responsible for threshold breaches.

Compliance Manager



Explanatory Notes

Select an Application: Oracle Financials

Select a month: Apr 2005

Select an Instance: UK Central Server

Use this form to insert notes to the monthly Component Group table. This allows you to reference outages or breaches and provide reminders on the surrounding activity for future reference. Select the Application, Instance and Component Group then update the text notes field.

Component Group Name	Availability	Security	Change	Incident	Release	Config
Central App Servers	-	-	-	-	-	-
Central DB	-	-	-	-	-	-
Central Timer	-	-	-	-	-	-

Explanatory Notes for the selected Group

Insert notes below and press Apply.

Compliance Manager

Component Group Availability



Select an Application:

Select a month:

Select an Instance:

Select an application, and instance of that application and a time period to examine historical availability metrics. All metrics are measured in seconds for the month or day. Coloured squares indicate a breach of the threshold.

Red = KCI Breach
Orange = KRI Breach

Mirrored component groups will display the best possible metrics from any one of their components. Unmirrored component groups will display the worst possible metrics from any one of their components.

Application Instance Component Groups

Component Group Name	Month	Mirrored Components	Unplanned Unavail (KCI)	Allowed Unplanned Unavail	Planned Unavail (KRI)	Allowed Planned Unavail	Msr'd Unavailability (KRI)	Allowed Msr'd Unavail
Central App Servers	Apr 2005	No	0	100	7,350	500	300	500
Central DB	Apr 2005	No	0	100	300	500	300	500
Central Timer	Apr 2005	No	0	100	300	500	300	500

Notes:

Components within this Group

Application	Instance	Component Group	Component
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2

Business Processes Supported by the Application

Availability and Outages (Actual, Planned and Unplanned)
Fri, Apr 1, 2005 - Thu, Apr 28, 2005

Per Day
6,000
4,800



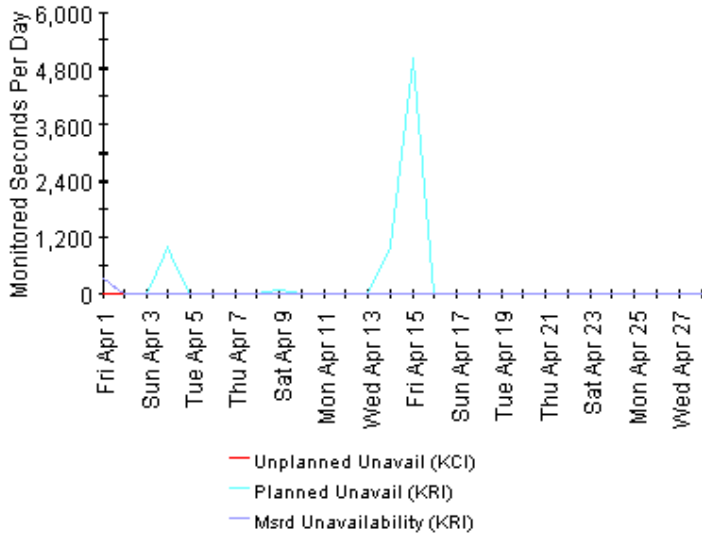
Daily Availability Metrics

Time Period	Unplanned Unavail (s)	Msr'd Unavailability (s)	Planned Unavail (s)
Fri, Apr 1	0	300	300
Sat, Apr 2	0	0	0





Availability and Outages (Actual, Planned and Unplanned)
 Fri, Apr 1, 2005 - Thu, Apr 28, 2005



Daily Availability Metrics

Time Period	Unplanned Unavail (s)	Msrd Unavailability (s)	Planned Unavail (s)
Fri, Apr 1	0	300	3
Sat, Apr 2	0	0	
Sun, Apr 3	0	0	
Mon, Apr 4	0	0	1,0
Tue, Apr 5	0	0	
Wed, Apr 6	0	0	
Thu, Apr 7	0	0	
Fri, Apr 8	0	0	
Sat, Apr 9	0	0	
Sun, Apr 10	0	0	
Mon, Apr 11	0	0	
Tue, Apr 12	0	0	
Wed, Apr 13	0	0	
Thu, Apr 14	0	0	1,0
Fri, Apr 15	0	0	5,0
Sat, Apr 16	0	0	
Sun, Apr 17	0	0	

Compliance Manager

Component Availability

Select an application, and instance of that application and a time period to examine historical availability metrics. All metrics are measured in seconds for the month or day.



Coloured squares indicate a breach of the threshold.

Thresholds are checked against the aggregate values from the beginning of a month. Each month the counters return to zero. Use the daily table at the bottom right to examine individual days throughout the month.

Select an Application

Oracle Financials

Select a month

Apr 2005

Select an Instance

UK Central Server

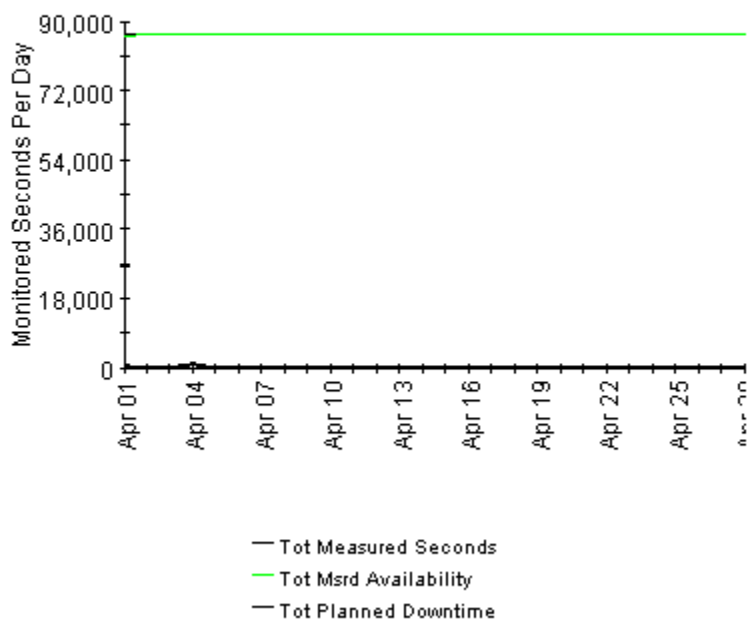
Select a Component Group

Central App Servers

Component Availability Measurements

Component Name	Time Period	Total Measured Seconds	Tot Measured Availability	Tot Planned Downtime
HTTP Server 1	Apr 2005	2,419,200	2,418,900	1,350
HTTP Server 2	Apr 2005	2,419,200	2,414,400	6,300

Availability and Outages (Actual, Planned and Unplanned)
Fri, Apr 1 12:00 AM - Thu, Apr 28 12:00 AM



Daily Availability

Time Period	Tot Measured Seconds	Tot Msrd Availability
01 Apr 2005	86,400	86,100
02 Apr 2005	86,400	86,400
03 Apr 2005	86,400	86,400
04 Apr 2005	86,400	86,400
05 Apr 2005	86,400	86,400
06 Apr 2005	86,400	86,400
07 Apr 2005	86,400	86,400
08 Apr 2005	86,400	86,400
09 Apr 2005	86,400	86,400
10 Apr 2005	86,400	86,400
11 Apr 2005	86,400	86,400
12 Apr 2005	86,400	86,400
13 Apr 2005	86,400	86,400
14 Apr 2005	86,400	86,400
15 Apr 2005	86,400	86,400
16 Apr 2005	86,400	86,400
17 Apr 2005	86,400	86,400
18 Apr 2005	86,400	86,400
19 Apr 2005	86,400	86,400

Component Group Incidents

There are five drop-down lists at the top:

- Select application
- Select application instance
- Select month
- Filter by KRI
- Filter by KCI

The KRI and KCI filters are helpful when you have numerous component groups to choose from. Beneath the drop-downs, you can see a list of component groups associated with the selected application instance. For each component group, you have two color-coded values, one for all KCI incident breaches for the month, and one for all KRI incident breaches for the month.

The column headings, **Incident KRI Breach** and **Incident KCI Breach** are both links. Click **Incident KRI Breach** to Component Group Incidents - KRI Data. Click **Incident KCI Breach** to open Component Group Incident - KCI Data.

Selecting a component group updates the rest of the report. Below the selection table, you have a notes section, a list of components, and list of the business processes supported by the component group. At the bottom of the report you can see values for KRI metrics (totals for the month) and values for KCI metrics (totals for the month). To see daily data, open the KRI Data and KCI Data reports.



If you have any questions about which columns in a report are being populated by any one datapipe, refer to the user guide for the datapipe.

Compliance Manager

Component Group Incidents

Select an application, an instance and a time period to examine historical incident metrics. Coloured squares indicate a breach of the threshold.



View any related notes and the KRI and KCI metrics causing the breach. Cross launch to the detailed source data if required.

Select an Application: Oracle Financials
 Select a month: Apr 2005

Select an Instance: UK Central Server
 Filter by KCI Breach: [Dropdown]
 Filter by KRI Breach: [Dropdown]

Component Group Incident Breaches

App Name	App Instance Name	Component Group Name	Date	Incident KCI Breach	Incident KRI Breach
Oracle Financials	UK Central Server	Central App Servers	Apr 2005	0	0
Oracle Financials	UK Central Server	Central DB	Apr 2005	0	0
Oracle Financials	UK Central Server	Central Timer	Apr 2005	0	0

Notes:

[Empty notes area]

Components within this Group

Application	Instance	Component Group	Component
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2

Business Processes Supported by this Component Group

[Empty business processes area]

KCI Incident Data

Avg KCI Duration Major Incidents	Allowed Avg Dur Major Incidents	Pct KCI Major Incids Over Deadline	Allowed Pct Maj Incid Deadline
0	1	0	10

KRI Incident Data

Total KRI Major Incidents	Allowed Major Incidents	Pct KRI Incidents Over Deadline	Allowed Pct Incidents Over Deadline	Total KRI Incidents	Allowed
	20	0	10		

Compliance Manager

Component Group Incidents - KCI Data

Select an application, instance and a month to examine historical incident metrics. Coloured squares indicate the status of the threshold. Examine the tables of collected data at the combined component group and also at the individual component level.



Select an Application Select a month

Choose an Application Choose a Month

Select an Instance

Choose an Instance Filter by KCI Breach

Component Group Incident Breaches

App Name	App Instance Name	Component Group Name	Date	Incident KCI Breach
Oracle Financials	UK Central Server	Central App Servers	Apr 2005	0
Oracle Financials	UK Central Server	Central DB	Apr 2005	0
Oracle Financials	UK Central Server	Central Timer	Apr 2005	0
Oracle Financials	UK Satellite 1 Server	Sat 1 App Servers	Apr 2005	0
Oracle Financials	UK Satellite 1 Server	Sat 1 DB	Apr 2005	0

Notes:

Average Duration of Major Incidents (KCI)

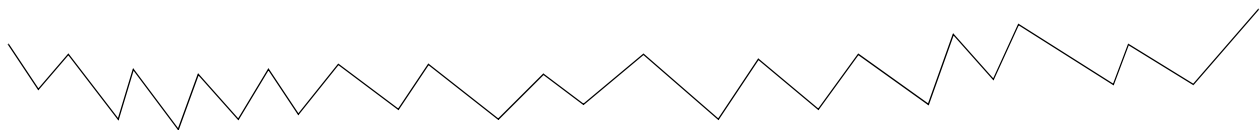
Avg Duration (days)	Allowed Average Duration
0.00	1.00

% Major Incidents Over Deadline (KCI)

Percentage	Allowed Percentage
0.00	10.00

Daily Incident Source Data for KPI Metrics at the Component Group Level

Date	Avg Duration Major Incidents	Tot Closed Major Incidents	Tot Duration Major Incidents	Pct Incidents Over Deadline	Tot Major Incidents Over Deadline
1 Apr 2005	0.00			0.00	
2 Apr 2005	0.00			0.00	
3 Apr 2005	0.00			0.00	
4 Apr 2005	0.00			0.00	
5 Apr 2005	0.00			0.00	
6 Apr 2005	0.00			0.00	
7 Apr 2005	0.00			0.00	





8 Apr 2005	0.00		0.00
9 Apr 2005	0.00		0.00
10 Apr 2005	0.00		0.00
11 Apr 2005	0.00		0.00
12 Apr 2005	0.00		0.00
13 Apr 2005	0.00		0.00
14 Apr 2005	0.00		0.00

Components within this Group

Application	Instance	Component Group	Component
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2

Daily Incident Source Data for KPI Metrics at the Component Level

Date	Tot Closed Major Incidents	Total Duration Major Incidents	Total Major Incidents Over Deadline
1 Apr 2005			
2 Apr 2005			
3 Apr 2005			
4 Apr 2005			
5 Apr 2005			
6 Apr 2005			
7 Apr 2005			
8 Apr 2005			
9 Apr 2005			
10 Apr 2005			
11 Apr 2005			
12 Apr 2005			
13 Apr 2005			
14 Apr 2005			
15 Apr 2005			

Compliance Manager

Component Group Incidents - KRI Data

Select an application, instance and a month to examine historical incident metrics. Coloured squares indicate the status of the threshold. Examine the tables of collected data at the combined component group and also at the individual component level.



Select an Application Select a month

Choose an Application Choose a Month

Select an Instance

Choose an Instance Filter by KRI Breach

Component Group Incident Breaches

App Name	App Instance Name	Component Group Name	Date	Incident KRI Breach
Oracle Financials	UK Central Server	Central App Servers	Apr 2005	0
Oracle Financials	UK Central Server	Central DB	Apr 2005	0
Oracle Financials	UK Central Server	Central Timer	Apr 2005	0
Oracle Financials	UK Satellite 1 Server	Sat 1 App Servers	Apr 2005	0
Oracle Financials	UK Satellite 1 Server	Sat 1 DB	Apr 2005	0

Notes:

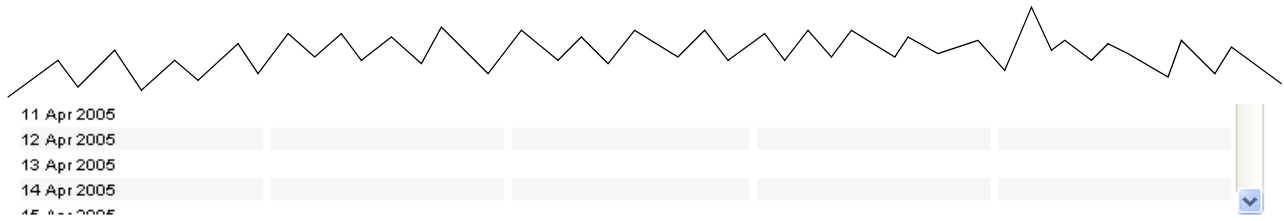
KRI Values for : # Major Incidents, % Incidents Over Deadline, Total # Incidents

# Major Incidents	Allowed # Major Incidents	Pct Incidents Over Deadline	Allowed Pct Incidents Over Deadline	Total # Incidents	Allowed # Incidents
	20	0.00	10.00		100

Daily Incident Source Data for KPI Metrics at the Component Group Level

Date	Tot New Major Incidents	Tot Incidents Over Deadline	Tot Closed Incidents	Tot New Incidents
1 Apr 2005				
2 Apr 2005				
3 Apr 2005				
4 Apr 2005				
5 Apr 2005				
6 Apr 2005				
7 Apr 2005				
8 Apr 2005				
9 Apr 2005				
10 Apr 2005				





Components within this Group

Application	Instance	Component Group	Component
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2

Daily Incident Source Data for KPI Metrics at the Component Level

Date	Tot New Major Incidents	Tot Incidents Over Deadline	Tot Closed Incidents	Tot New Incidents
1 Apr 2005				
2 Apr 2005				
3 Apr 2005				
4 Apr 2005				
5 Apr 2005				
6 Apr 2005				
7 Apr 2005				
8 Apr 2005				
9 Apr 2005				
10 Apr 2005				
11 Apr 2005				
12 Apr 2005				
13 Apr 2005				
14 Apr 2005				
15 Apr 2005				

6 Admin Reports

The following administrative reports will help you diagnose problems and verify that the report pack is operating normally:

- Administration and Deletion (variant web view name: Data Model Administration)
- Configuration and Logging (variant web view name: Data Collection Logging)
- Table Structures and Sizes

If you are using the web interface, you will find the admin reports in the Admin folder. Another way to access the same reports is to open the Launch Point page and select **Administrative Reports**.

Administration and Deletion

The Administration and Deletion report shows the contents of the data model, from the application level to the component level. In addition to showing the contents of the data model, this report indicates whether each item has monthly data and whether each item is marked for deletion. The following table provides a list of scenarios, and the corresponding status (Yes or No) under **Has Monthly Data?** and **Marked for Deletion?**

Scenario	Has Monthly Data?	Marked for Deletion
You created an element; before any data collection took place, you used the Application Deletion form to delete it.	No	Yes
You created an element and collected data; however, infrastructure changes took place, so you used the Application Deletion form to delete the element.	Yes	Yes
An element you created is collecting data.	Yes	No
You created an element; the first nightly collection has not taken place yet.	No	No
You created an element; the first nightly collection has taken place, but for some reason no data was collected.	No	No
You created an element; it was collecting data, but for some reason data collection ceased and existing data has aged out.	No	No

Compliance Manager

Administration and Deletion

Use this report to examine which Applications have collected data and which do not. An item which is 'Marked for Deletion' will be removed when all child components have no data left in the system and have been removed. You can force full data removal by changing the deletion method using the administrative form.



Choose an Application ▼

Choose an Instance ▼

Administrative View of Compliance Manager Data

Application	Instance	Component Group	Component	Has Monthly Data	Marked for Deletion
NNM	-	-	-	●	No
NNM	East	-	-	●	No
NNM	East	East	-	●	No
NNM	East	East	East	●	No
NNM	North	-	-	●	No
NNM	North	North	-	●	No
NNM	North	North	North	●	No
NNM	South	-	-	●	No
NNM	South	South	-	●	No
NNM	South	South	South	●	No
NNM	West	-	-	●	No
NNM	West	West	-	●	No
NNM	West	West	West	●	No
OVD	-	-	-	●	No
OVD	Europe	-	-	●	No
OVD	Europe	Europe	-	●	No
OVD	RoW	-	-	●	No
OVD	RoW	RoW	-	●	No
Oracle Financials	-	-	-	●	No
Oracle Financials	UK Central Server	-	-	●	No
Oracle Financials	UK Central Server	Central App Servers	-	●	No
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 1	●	No
Oracle Financials	UK Central Server	Central App Servers	HTTP Server 2	●	No
Oracle Financials	UK Central Server	Central DB	-	●	No
Oracle Financials	UK Central Server	Central DB	Central DB	●	No
Oracle Financials	UK Central Server	Central Timer	-	●	No
Oracle Financials	UK Central Server	Central Timer	Central Timer	●	No
Oracle Financials	UK Satellite 1 Server	-	-	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 App Servers	-	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 App Servers	HTTP Server 1	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 App Servers	HTTP Server 2	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 DB	-	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 DB	Sat 1 DB	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 Timer	-	●	No
Oracle Financials	UK Satellite 1 Server	Sat 1 Timer	Sat 1 Timer	●	No
Oracle Financials	UK Satellite 2 Server	-	-	●	No

Configuration and Logging

Use this report to view log files related to OVIS and Service Desk integration. The log files contain information about configuration changes. Filter the contents by information source and by date range.

Compliance Manager Configuration and Logging



This report displays configuration information relating to Compliance Manager collections and internet processes. It lists log entries in descending chronological order. Filter the selection by the time the entry was created or by the source of the log entry.

	Configuration Parameter	Meaning
Logging Level		High Level and Errors Only
Deletion Method		Delete when no data

Select log message source Log Time < Month Log Time > Month

Log Entries

Time	Component	Message
Mon, Aug 29 5:00 AM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Sun, Aug 28 5:00 AM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Sat, Aug 27 5:00 AM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Fri, Aug 26 5:01 AM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Thu, Aug 25 5:01 AM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Wed, Aug 24 4:43 PM	CM Pre-pop Daily Rows	Info: Pre-populated the daily table with rows to allow for Planned Downtime allocation
Wed, Aug 24 4:43 PM	ServiceDesk Datapipe	Info: 444 days of stats on Incidents and Changes were mapped in 22 seconds.

The amount of detail in Configuration and Logging is controlled by a setting on the Administration form. See page 60. Your choices are:


- Minimal detail in the log
- Normal detail in the log
- Maximum detail in the log

If you intend to use the Configuration and Logging report for debugging purposes, you want maximum detail in the report. The Administration form also controls the way that data for a deleted item is removed. Your options are:

- Allow data to age-out according to data retention rules
- Remove data as soon as possible

Data retention rules vary from table to table. If you want to remove data as soon as possible, removal is handled by a process that runs once a day, at night.

Compliance Manager Administration



Use this form to update the configuration settings for Compliance Manager logging and table maintenance. Click the Apply button to save any changes. Click the Cancel button to cancel any changes. Click the OK button to save changes and close the form.

The logging setting is used to determine the number and detail of messages sent to the 'Configuration and Logging Report'.
 Selections include
 0 = High Level only,
 1 = Normal / Informational
 2 = All / Debug

Compliance Manager data model elements (Applications, Business Processes etc) can be removed by marking them for deletion. They will normally only be removed when the data associated with them has aged out naturally. You can force the removal of all data associated with a marked for deletion element by setting the 'Deletion Method' to 1 instead of 0.
 0 = Normal - follow table retention period rules
 1 = Force data removal

Configuration	Value	Meaning
Logging Level	1	Normal
Deletion Method	0	Allow data to age

Change setting 1 ▼

Table Structures and Sizes

Use this report to investigate property tables and data tables. For a property table, the report indicates the number of rows and how many elements within the property table have been marked for deletion. Any table that shows a value for number of rows has data in it. Any table showing zero rows, which is obviously incorrect, is color-coded red for easy detection.

For a data table, the report indicates the age of the oldest data and the age of the most recent data. The age information tells you whether or not data is aging out in accordance with your expectations and whether or not data is being collected. If data is being collected and it is not being aged out, the number of rows will increase daily.

Compliance Manager

Table Structures and Sizes

This report highlights the volume and age of data in each of the Compliance Manager table structures. It tells you where the data is stored and how much there is. Note that there is one default row per property (K_>xxx) table, in addition to any user created rows. Use this and the other administrative reports to verify that data is arriving as expected into the system and that aggregations are taking place.



Data is aged out of data tables based upon the 'retention period' defined for that table. You can examine and modify the current settings using the 'Table Manager' application in the Admin UI. Select Data Tables -> Category -> ComplianceManager.

Processes in K_ITC_Business_Process

Total	# Marked for Deletion
7	0

Monthly Business Process Data - SM_ITC_Business_Process

Oldest	Most Recent	Number of Rows
01-JAN-04	01-APR-05	88

Relationships in K_ITC_BP_App_mbr

Total	# Enabled
19	18

Business Processes are created and then associated with applications. The K_ITC_BP_App_mbr table stores these relationships. The user enables or disables the associations using the 'Define BP to App Relationships' form located in the Objects window in the Admin UI.

Applications in K_ITC_Application

Total	# Marked for Deletion
8	0

Monthly Application Data - SM_ITC_Application

Oldest	Most Recent	Number of Rows
01-JAN-04	01-APR-05	28

Instances in K_ITC_Application_Instance

Total	# Marked for Deletion
13	0

Monthly Application Instance Data - SM_ITC_Application_Instance

Oldest	Most Recent	Number of Rows
01-JAN-04	01-APR-05	79

Groups in K_ITC_App_Inst_Comp_Grp

Total	# Marked for Deletion
19	0

Monthly Component Group Data - SM_ITC_App_Inst_Comp_Grp

Oldest	Most Recent	Number of Rows
01-JAN-04	01-APR-05	175

Components in K_ITC_App_Inst_Component

Total	# Marked for Deletion
20	0

Monthly Component Data - SM_ITC_App_Inst_Component

Oldest	Most Recent	Number of Rows
01-JAN-04	01-APR-05	175

Daily Component Data - SD_ITC_App_Inst_Component

Oldest	Most Recent	Number of Rows
16-APR-04	28-APR-05	175

7 Installing the Compliance Manager Portlet

The Compliance Manager portlet is a reusable web component that processes requests and generates dynamic portal content in accordance with the JSR-168 standard. It uses screen-scrape technology to render and display reports in the Compliance Manager Report Pack. The portlet does not render and display every report in the report pack. The portlet renders these executive-level reports only:

- Business Process Status
- Business Process Status: Month-to-Date
- Application Status
- Application Status: Month-to-Date
- Application Instance Status

The interaction between top pane and bottom pane does not change in the portlet; the interaction is no different from the web interface view or Report Viewer. The look is slightly different. In addition to color coding, the portlet provides symbols that supplement color-coding. There is a symbol for compliance that equates to green, a symbol for KRI breach that equates to orange, and a symbol for KCI breach that equates to red.

The portlet is a compressed .war file on the Compliance Manager CD. The directory path is:

```
Portlet_WAR/itcompliance.war
```

A functioning information portal is a prerequisite for the Compliance Manager portlet. You may install the portlet in the following environments:

- BEA WebLogic 8.1
- Apache Pluto
- Apache Jetspeed 2

BEA WebLogic 8.1

Portal components include desktops, books, pages, and portlets. A book, which is usually a set of pages represented by tabs, allows a portal visitor to move from page to page. A page is a container for portlets. A page can also nest a book. To install the Compliance Manager portlet on an existing WebLogic portal application, perform these simple tasks:

- Insert the Compliance Manager CD in the CD-ROM drive
- Start WebLogic and open the portal application
- Import the Compliance Manager portlet from the Compliance Manager CD
- Move the portlet to the portal application
- Drag the Compliance Manager portlet to an existing page

Task 1: Start WebLogic Workshop

Microsoft Windows

Select **Start > Programs > BEA WebLogic Platform 8.1 > WebLogic Workshop**.

UNIX

- 1 Log in to the target UNIX system.
- 2 Go to the workshop directory of the WebLogic Platform installation. For example:

```
cd bea/weblogic81/workshop
```
- 3 Enter the following command:

```
sh Workshop.sh
```

Task 2: Start WebLogic Server and open the portal application

- 1 Select **Tools > WebLogic Server > Start WebLogic Server**.
- 2 When the server has started, select **Portal > Portal Administration**.
- 3 When the WebLogic Administration Portal login page opens, log in.
- 4 Open the portal application by selecting **File > Open > Application from Workshop**.
- 5 Navigate the application directory and select the parent portal you want to open.
- 6 Click **Open**.
- 7 If the application folders are not displaying in WebLogic Workshop, select **View > Application**.

Task 3: Import the .war file from the Compliance Manager CD

- 1 Right-click the application project files folder in the portal application directory.
- 2 Select **Import**. The Import Files window opens.
- 3 Navigate to the itcompliance.war file on the Compliance Manager CD.
- 4 Select the itcompliance.war file and click **Import**.
- 5 Move the Compliance Manager portlet from the list of imported portal web projects to the portal application.

Task 4: Add the Compliance Manager portlet to an existing page.

- 1 In the **Portal Resources** tree, select the page you want to add the portal to.
- 2 In the **Manage Page Contents** editor in the Editor pane, click **All Portlets** to display the list of portlets.
- 3 Click **Add to Page** next to the Compliance Manager portlet. The Compliance Manager portlet appears in the **Portlets in Page** list to the right of the list of all portlets.
- 4 Click the **Position Page Contents** tab.
- 5 Select **Using Drag & Drop** if this button is not already selected.
- 6 Drag and drop the Compliance Manager portlet to the desired location on the page.
- 7 Select the **Lock Placeholder** box to prevent users from rearranging the portlet.
- 8 Click **Save Changes**.
- 9 To verify your changes:
 - a Select the Desktop associated with the book

- b** Select the Desktop Properties associated with the page
- c** Click **View Desktop**.

Apache Pluto

Apache Ant is a common build utility used by most Apache software packages. Apache Ant uses a `build.xml` file and a `build.properties` file to deploy the Compliance Manager portlet to Apache Pluto.

The `build.xml` File

The `build.xml` file is specific to Pluto, but anyone can use it.

```
<!--
```

```
Ant build file for deploying individual portlets to the binary distribution
(which includes Tomcat 5) of Pluto ver 1.0.1. Release Candidate.
```

```
This script depends on setting the CATALINA_HOME to the full
path to where the pluto-1.0.1 binary distribution is installed.
```

```
Run this build inputing the path to the war file (including file name)
when prompted by the input task or using the full command line:
ant -Dfull.war.path=<path_to_war_file>. Alternatively,
you can set the full.war.path property in build.properties.
```

```
Use Ant version 1.6+ to run this build.
```

```
Here's how to call this script inside of your portlet application Ant build:
```

```
<target name="deploy-pluto" description="Deploy portlet application to
Pluto" depends="war">
  <ant dir="${env.CATALINA_HOME}/portlet-deploy" inheritall="false">
    <property name="full.war.path" value="${basedir}/${war.name}"/>
  </ant>
</target>
```

```
Setting the full.war.path property inside this ant task causes the input task
to be
```

```
skipped inside of the get-war-path target of this file.
```

```
author: Craig Doremus (craig-at-maine.com)
```

```
-->
```

```

<project default="deploy" name="portlet-deploy" basedir=". ">

<property environment="env" description="To pick up environmental variables"/
>

<property file="build.properties" description="Properties file"/>
<property name="this.dir" value="portlet-deploy" description="Current
directory"/>

<property name="pluto-context" value="pluto" description="Web context name
for pluto webapp"/>

<property name="lib.dir" value="lib" description="Holds libraries used for
deployment"/>

<path description="Deployent classpath" id="deploy.classpath">
<pathelement location="${env.CATALINA_HOME}/webapps/${pluto-context}/WEB-INF/
classes"/>

<fileset dir="${lib.dir}">
<include name="*.*/>
</fileset>

<fileset dir="${env.CATALINA_HOME}/shared/lib">
<!-- <include name="pluto-1.0.1.jar"/> -->
<include name="pluto-*.jar"/>
<include name="portlet-api-1.0.jar"/>
</fileset>
</path>

<target name="init">
<fail unless="env.CATALINA_HOME"
message="CATALINA_HOME must be set to the Tomcat installation home directory"/
>

<property name="tomcat.home" value="${env.CATALINA_HOME}"/>
<echo>

Pluto version 1.0.1 deployment build

This script deploys a portlet application packaged
in a war file with a proper web.xml and portlet.xml file.

Pluto installation home: ${tomcat.home}

</echo>

<mkdir dir="${lib.dir}" description="Creates dir for libraries, if it is not
present"/>

```

```

<!--
Check if dependencies are available.
-->
  <condition property="noget">
    <and>
<available filepath="{lib.dir}" file="castor-0.9.5.jar" />
<available filepath="{lib.dir}" file="regexp-1.3-dev.jar" />
<available filepath="{lib.dir}" file="servletapi-2.3.jar" />
<available filepath="{lib.dir}" file="xerces-2.4.0.jar" />
<available filepath="{lib.dir}" file="xml-apis-2.0.2.jar" />
    </and>
  </condition>

</target>

<target name="get-war-path" depends="init,get-deps">
<input
message="Enter the full path to the portlet war file (including file name):"
addproperty="full.war.path"/>

</target>

<target name="deploy-portlet-war" depends="get-war-path">
<!-- Check that the file that is the value of full.war.path exists -->
<condition property="path.set" value="true">
  <and>
<isset property="full.war.path"/>
    <not>
      <equals arg1="{full.war.path}" arg2="" trim="true"/>
    </not>
    <available file="{full.war.path}"/>
  </and>
</condition>
<fail message="The property full.war.path has not been set or the war file
does not exist."
unless="path.set"/>

```

```

<echo message="File to be deployed: ${full.war.path}"/>
<!-- Run the deploy class -->
<java classname="org.apache.pluto.portalImpl.Deploy" fork="yes">
  <classpath>
    <path refid="deploy.classpath"/>
  </classpath>
  <arg value="${tomcat.home}/webapps" />
  <arg value="pluto" />
  <arg value="${full.war.path}" />
  <arg value="${basedir}" />
</java>
</target>

<target name="deploy" depends="deploy-portlet-war">
<echo>
Deployment done!
If this is the first time you have done the deployment,
please make sure you edit portletentityregistry.xml and
pageregistry.xml in ${tomcat.home}/webapps/pluto/WEB-INF/data
to register your portlet with Pluto and add it to
the page layout.
</echo>
</target>

<target name="get-deps" unless="noget">
  <get dest="${lib.dir}/castor-0.9.5.jar" usetimestamp="true"
ignoreerrors="false" src="http://www.ibiblio.org/maven/castor/jars/
castor-0.9.5.jar">
  </get>
  <get dest="${lib.dir}/regexp-1.3-dev.jar" usetimestamp="true"
ignoreerrors="false" src="http://www.ibiblio.org/maven/regexp/jars/
regexp-1.3-dev.jar">
  </get>
  <get dest="${lib.dir}/servletapi-2.3.jar" usetimestamp="true"
ignoreerrors="false" src="http://www.ibiblio.org/maven/servletapi/jars/
servletapi-2.3.jar">
  </get>
  <get dest="${lib.dir}/xerces-2.4.0.jar" usetimestamp="true"
ignoreerrors="false" src="http://www.ibiblio.org/maven/xerces/jars/
xerces-2.4.0.jar">
  </get>

```



```
        <get dest="{lib.dir}/xml-apis-2.0.2.jar" useimestamp="true"
ignoreerrors="false" src="http://www.ibiblio.org/maven/xml-apis/jars/
xml-apis-2.0.2.jar">
    </get>
</target>
```

The build.properties File

The build.properties file must be modified, but the only change you have to make is to supply the correct path to the .war file.

```
#build.properties
#Use this file to override any properties in build.xml or
#set new properties.

#Full path to the war file to be deployed (including file name)
#Uncomment to set the property instead of using the input task
#in the get-war-path target
full.war.path=C:\\Inetpub\\itcomplianceportlet\\itcompliance.war
```

Installing the Portlet

Follow these steps to install the portlet on Apache Pluto:

- 1 Shut down Apache Pluto.
- 2 Open a command prompt.
- 3 Navigate to the directory that contains the build files and the .war file.
- 4 Type the following command: **ant deploy**
- 5 Modify the following files:
 - <PLUTO_HOME>\webapps\pluto\WEB-INF\data\pageregistry.xml
 - <PLUTO_HOME>\webapps\pluto\WEB-INF\data\portletentityregistry.xml
 - <PLUTO_HOME>\webapps\pluto\WEB-INF\data\portletcontexts.txt

- Modify the pageregistry.xml file as follows:

```
<fragment name="compliancereports" type="page">
  <navigation>
    <title>IT Compliance Reports</title>
    <description>Displays the OVPI IT Compliance Reports</description>
  </navigation>
  <fragment name="row" type="row">
    <fragment name="col1" type="column">
      <fragment name="p1" type="portlet">
```

```

        <property name="portlet" value="5.1"/>
    </fragment>
</fragment>
</fragment>
</fragment>

```

b Modify the portletentityregistry.xml file as follows:

```

<application id="5">
    <definition-id>itcompliance</definition-id>
    <portlet id="1">
        <definition-id>itcompliance.complianceportlet</definition-id>
        <preferences>
            <pref-name>password</pref-name>
            <pref-value>kangag00!</pref-value>
            <read-only>>false</read-only>
        </preferences>
        <preferences>
            <pref-name>locale</pref-name>
            <pref-value>en</pref-value>
            <read-only>>false</read-only>
        </preferences>
        <preferences>
            <pref-name>helpdocs</pref-name>
            <pref-value>http://cm.hp-now.com:7001/compliancemanager2/appmanager/help/
index.html</pref-value>
            <read-only>>false</read-only>
        </preferences>
        <preferences>
            <pref-name>ovpiurl</pref-name>
            <pref-value>http://156.152.46.28:80/reports/webview?rn=/system/0_Launch_Point/
Launch_Point_ITC.rep</pref-value>
            <read-only>>false</read-only>
        </preferences>
        <preferences>
            <pref-name>username</pref-name>
            <pref-value>trendadm</pref-value>
            <read-only>>false</read-only>
        </preferences>
    </portlet>

```

</application>

- c** Add the new context to the portletcontexts.txt file by adding a new line and your context name: /itcompliance
- 6** Restart Apache Pluto.

Apache Jetspeed 2

Apache Jetspeed 2 has an auto-deployment directory. Follow these steps to install the portlet:

- 1** Copy the itcompliance.war file to this directory:
`<JETSPEED_HOME>\webapps\jetspeed\WEB-INF\deploy`
Within about 10 seconds Apache Jetspeed 2 will deploy the .war file.
- 2** Access the default portal and login as admin/admin.
- 3** Change your admin password.
- 4** Get into edit mode by clicking the pencil icon.
- 5** In edit mode, add the Compliance Manager portlet.
- 6** In edit mode, remove any unwanted portlets.

Glossary

Aggregation

The process of taking compliance or violation data and combining it with other compliance or violation data so it can be presented at higher levels of information reporting.

BS15000 Standard

A standard based on the ITIL framework, issued by the British Standards Institution, that provides implementation guidelines for IT service management.

COBIT

Control Objectives for Information and Related Technology is an open standard published by the Information Technology Governance Institute (ITGI).

Condition

The factor that initiates, stops, or changes one or more events. Comparing a KCI or KRI metric to a threshold is a condition.

Continuous Control Monitoring

The ongoing measurement of the environment to assess the effectiveness of controls so significant deficiencies and emerging material risks are exposed and so advance knowledge is provided of when issues threaten compliance.

Control

A condition that is monitored so violations can be reported. In Compliance Manager a control would be a metric that is monitored for threshold breaches.

Datapipe

The software configured data interface between applications or data stores. In Compliance Manager datapipes allow daily access to data collected by other applications.

Data Table

A table in the database where data is stored.

Database Connector

A connection to a specific database instance by OVCM. With OVCM licensing a quantity is specified with the software license and, if more database connectors are required, additional licenses will need to be purchased.

Governance

Is managing your business to meet both internal and external objectives by defining key processes within your business so objective controls can be established, measured, and managed.

Internal Control

A process designed to provide reasonable assurance regarding effectiveness of operations, reliability of financial reporting, or compliance with regulations or laws.

ICMB

ITIL Certification Management Board.

ITIL

Information Technology Infrastructure Library (ITIL) is a series of book that specify best practices for managing IT infrastructure processes and changes. The series was revised in 2000 and will be revised again in 2006. The titles in the series are:

- Software Asset Management
- Service Support
- Service Delivery
- Planning to Implement Service Management
- ICT Infrastructure Management
- Application Management
- Security Management
- The Business Perspective

JSR-168

Java Specification Request #168 is a Java portlet definition that provides standards for API's to allow information transfer between applications, specifically the areas of aggregation, personalization, presentation, and security. The report presentation interface for Compliance Manager complies with JSR-168. See: <http://www.jcp.org/en/jsr/detail?id=168>

Key Control Indicator (KCI)

A metric with a threshold defined such that a breach of the threshold indicates the presence of a significant deficiency within the IT Environment.

Key Process Indicator (KPI)

A general compliance industry term for a metric with a threshold defined such that a breach of the threshold indicates a violation of processes established for the IT environment. HP internal audit felt they needed to segment their process adherence data to provide more detailed high-level information for managers and auditors. Compliance Manager uses KCIs and KRIs to provide this segmentation and to better align with collected data.

Key Risk Indicator (KRI)

A metric with a threshold defined such that a breach of the threshold indicates emerging material risk within the IT environment for a significant deficiency or a material weakness.

Material Information (financial or other)

Information is material if it impacts the reported result. Compliance Manager monitors IT infrastructure data and compares the compiled data to thresholds that define the level at which the data, in aggregate with other data, could (at some predetermined acceptable risk level) become material to reported results governed by the compliance initiative.

Material Risk

The likelihood that the data being analyzed would impact the reported results governed by the compliance initiative.

Material Weakness

When processes or controls are operating so poorly as to allow material information to go undetected and/or unreported.

Materially Significant

When some measured data becomes significant, in aggregate with other data, to some reported result.

OGC

Office of Government Commerce.

Portlet

A reusable web component, usually managed by a container, which processes requests and generates dynamic portal content.

Process Area (a.k.a. Key Control Area or Metric Area)

The property table level where KCI and KRI metric data is compared to thresholds to indicate process compliance or violation for a specific application instance.

Process Control Area

A broad set of metrics that are managed by a specific set of processes such that common controls can be established. In OVCM version 1.0 the out-of-the-box defined process control areas are; availability management, change management, and incident management.

Property Table

A table in OVPI that defines the structure and content attributes of one or more OVPI data tables.

Reasonable Assurance

A statement, hopefully backed by supporting data, that it is likely that reported information is presented accurately.

Risk Management

An assessment of the likelihood that processes and controls are adequate to ensure that material information is detected and reported.

Sarbanes-Oxley (SOX)

An act passed by the United States Congress in 2002 in response to accounting scandals and business failures. The implementation of this act has resulted in the need to monitor and report on the IT infrastructure that supports financial systems.

Significant Deficiency

A condition in which the information presented (as governed by the compliance initiative) is deemed to be sufficiently likely to be unreliable.

Index

A

Administration and Deletion Report, 57
Administration form, 59
Apache Ant, 65
Apache Jetspeed 2, 71
Apache Pluto, 65
Application Deletion, 34
Application Instance Status, 37
Application Status, 37
Application Status Month-to-Date, 37

B

BEA Weblogic, 63
build.properties file, 69
Business Process Deletion, 34
Business Process Month-to-Date, 37
Business Process Status, 37

C

CM_OVIS_Datapipe.ap, 11
CM_SvcDsk_Datapipe.ap, 12
ComplianceManager_Demo.ap, 11
ComplianceManager_Thresholds.ap, 11
Component Availability, 43
Component Group Availability, 43
Component Group Changes, 43
Component Group Incident - KRI Data, 43
Component Group Incidents, 43
Component Group Incidents - KCI Data, 43
Configuration and Logging Report, 59

D

data aging options, 34
data retention rules, 59
demo package, 9

E

Explanatory Notes form, 43

I

Internet_Services.ap, 12
Internet_Services_Datapipe.ap, 12
Internet_Services_Demo.ap, 12
itcompliance.war, 63, 64, 69, 71

K

Key Control Indicator (KCI), 6
Key Risk Indicator (KRI), 6

L

Launch Point, 19

M

Manage Page Contents editor, 64

P

pageregistry.xml, 69
Planned Down Time Manual Entry, 32
Portal Resources tree, 64
portletcontexts.txt, 69, 71
portletentityregistry.xml, 69
process control areas, 6
Product Manuals Search (web page), 9
Public Company Accounting Oversight Board (PCAOB), 4

S

Sarbanes-Oxley Act of 2002, 4
ServiceDesk_Integration, 12

T

Table Structures and Sizes Report, 60

Thresholds.ap, 12

U

UPGRADE_CommonPropertyTables_to_35.ap, 12

UPGRADE_Internet_Services_to_20.ap, 12

W

web access server (web interface), 19

web interface, 19