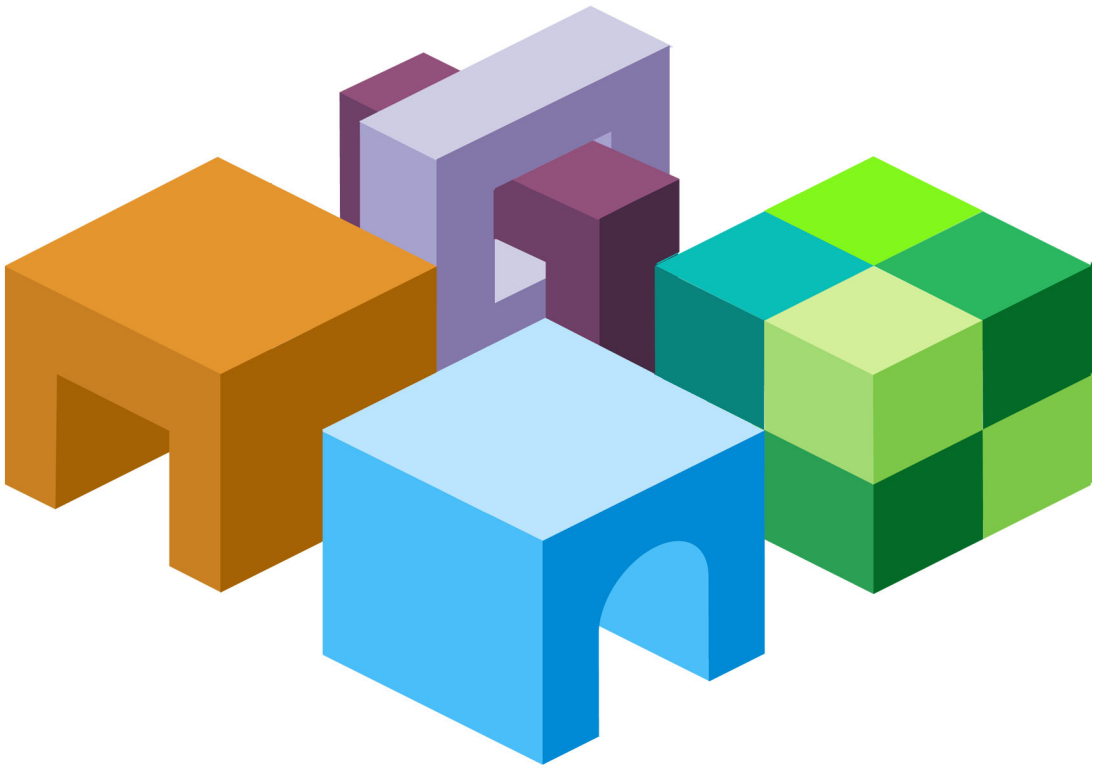

HYPERION® REPORTING AND ANALYSIS MIGRATION UTILITY

RELEASE 11.1.1

MIGRATION PLANNING GUIDELINES

ORACLE®
ENTERPRISE PERFORMANCE MANAGEMENT SYSTEM

Reporting and Analysis Migration Utility Migration Planning Guidelines, 11.1.1

Authors: EPM Information Development Team

Contents

1 Migration Overview

In This Chapter

Overview of Reporting and Analysis

Oracle's Hyperion Reporting and Analysis is a modular business intelligence platform providing management reporting, query and analysis capabilities for a wide variety of data sources in a single coordinated environment.

A single zero-footprint thin client provides the user with access to the following content:

- Oracle Hyperion Financial Reporting, Fusion Edition —Scheduled or on-demand highly formatted financial and operational reporting from almost any data source including Hyperion Planning and Hyperion Financial Management.
- Oracle's Hyperion® Interactive Reporting—Ad hoc relational query, self-service reporting and dashboards against any ODBC data source.
- Oracle's Hyperion® SQR® Production Reporting—High volume enterprise-wide production reporting.
- Oracle's Hyperion® Web Analysis—Interactive ad hoc analysis, presentation, and reporting of multidimensional data.

Reporting and Analysis, which includes Analytic Services, is part of a comprehensive Business Performance Management (BPM) system that integrates this business intelligence platform with Hyperion financial applications and Hyperion Performance Scorecard.

Migrating to Reporting and Analysis

Migration involves migrating information from the source system to Oracle's Hyperion® Shared Services and the Reporting and Analysis Repository.

Customers who want to take advantage of the new and upgraded features in Reporting and Analysis must migrate from their current Brio Portal, Brio Intelligence, BrioOne, Hyperion Performance Suite 8, Hyperion Analyzer, or Hyperion Reports implementation.

A migration involves hosting both currently deployed components and Reporting and Analysis software in a new implementation environment. The migration to Reporting and Analysis warrants careful analysis of your current product deployment.

The migration process, which is outlined in this document, emphasizes tasks that identify new requirements and infrastructure as a part of any new Reporting and Analysis solution. Migrating to Reporting and Analysis involves collecting essential project information, identifying or producing pertinent documentation, and conducting various reviews important to a successful upgrade.

Review the following sections for information on:

- Migration Variables
- Migration Scope
- Reporting and Analysis Migration Utility
- Migration Scenarios
- Migration End Result

Migration Variables

Individual installations vary in size, configuration, security requirements, and business solutions undertaken. Correspondingly, migration to Reporting and Analysis varies from one installation to another. Some aspects of your migration may require manual procedures. The amount of manual migration required depends on your current installation, customizations, and the capabilities that you want to implement in Reporting and Analysis.

Migration Scope

The migration process involves assessing the current product deployment, planning your migration, and running test migrations. It also means preparing a QA release package for the Reporting and Analysis production deployment and incorporating operational procedures to maintain a high level of service.

To migrate successfully to Reporting and Analysis , your organization needs to complete the following activities:

- Document and assess your current environment.
    - List components installed. Include an architectural diagram that shows how the core components and web servers are distributed and the size of the installation.
    - Identify your user load and job processing trends by hours of the day.
    - Describe your users' roles with respect to accessing the system's reports, analyzing data, preparing documents, scheduling reports, and managing users.
    - Perform appropriate infrastructure planning to address capacity and performance-related concerns. For detailed information on capacity planning, refer to the capacity-planning white papers located at http://www.hyperion.com/products/whitepapers. For

further assistance in hardware planning, contact your local Hyperion Consulting Services representative or local partner.

- Identify your authentication (login) and authorization (access rights to content) security requirements so that you can incorporate these into the migration plan.

- Review the capabilities of Reporting and Analysis in conjunction with your requirements and prepare a detailed plan for migration.
- Test and validate the migration.

  It is recommended that you perform and validate migrations on a test server. This provides the smoothest possible migration of your production system with the least impact on your overall business operations.

  In addition, you may decide to run the final migration on your test server rather than on the production system. This can save time and resources, and it enables your current system and the new system to run in parallel until the new Reporting and Analysis server is ready for general use.

Reporting and Analysis Migration Utility

Hyperion is committed to the success of its new and existing customers. As such, Hyperion provides a migration utility to help existing customers migrate to Reporting and Analysis.

The Oracle's Hyperion® Reporting and Analysis Migration Utility is a comprehensive software toolkit available to customers to facilitate their migrations. The Reporting and Analysis Migration Utility takes a specified set of data from supported versions of existing Hyperion products and transfers that data to a working Reporting and Analysis installation. Hyperion offers the Reporting and Analysis Migration Utility at no charge to existing maintenance paying customers. The Reporting and Analysis Migration Utility automates the migration process to a certain extent, but larger and more complex installations or installations with heavy customizations do require manual steps to migrate successfully.

Migration Scenarios

The automation of the migration process depends on the type of product implementation and the number of customizations in your source system. There are six basic scenarios for migrating to Reporting and Analysis, and customizations can change each scenario. Each scenario has a different level of manual steps. These steps are outlined in Chapter 2, "Performing Migration." The number and type of additional manual steps depends on customizations in your source system.

This document provides information on planning and assessing the typical solution requirements. Depending on the complexity of your migration, you may want to include local or Hyperion consulting support.

Review the following sections for information on:

- Migrating from Brio Portal
- Migrating from BrioONE

- Migrating from Brio Intelligence
- Migrating from Hyperion Analyzer
- Migrating from Hyperion Reports
- Migrating from Hyperion Performance Suite 8.x
- Migrating a Customized Environment
- Other Migration Considerations

Migrating from Brio Portal

For Brio Portal customers, migrating to Reporting and Analysis is similar to an upgrade in previous Brio Portal releases except that content is copied from one physical installation to a completely different installation environment.

Because the content is migrated to a new environment, you must complete some pre-migration steps, such as installing Reporting and Analysis, setting up authentication, and configuring hosts in the target environment. See Chapter 2, "Performing Migration" for environment prerequisites and pre-migration steps.

A migration from Brio Portal is the most straightforward migration and requires the fewest manual steps.

Table 1 describes the Brio Portal items that are automatically migrated, the items that you must manually migrate, and the items that are not migrated to Reporting and Analysis.

Table 1 Items Migrated/Not Migrated from Brio Portal

Automatically Migrated	• Folders • SQR jobs • Generic jobs • Documents • Personal pages • Subscriptions • Favorite items • Users • Groups
Manually Migrated	• Custom forms See "Migrating the Test Server" on page 24 for the steps involved in migrating custom forms. Note that SmartForms are migrated as is; however, you must modify them post-migration in order to use them for the target environment. • External authentication of users and groups You do not have to recreate users and groups in the target system. See "Components Requiring Pre-migration Steps" on page 31 for an overview of the steps required to set up external authentication in Reporting and Analysis and to migrate user and group attributes from the source system to the target system.

Not Migrated	• Custom forms • Knowledge Server files Not supported in Reporting and Analysis. • Personal channels Not supported in Reporting and Analysis. • External authentication systems You must set up any external authentication systems in the target environment prior to migration. • WebClient templates The Reporting and Analysis environment uses a combination of JSP and templates. The Reporting and Analysis Migration Utility does not migrate WebClient templates and their customizations.

Migrating from Brio Intelligence

You can use the Oracle's Hyperion® Reporting and Analysis Migration Utility for OnDemand Server (ODS) and Broadcast Server (BCS) migrations. Both components have their own repository database and associated documents. ODS can run as a stand-alone component or as a Portal service. When run as a Portal service, the users, groups, and folders are part of the Portal Repository.

Table 2 describes the Brio Intelligence items that are automatically migrated, the items that you must manually migrate, and the items that are not migrated to Reporting and Analysis.

Table 2 Items Migrated/Not Migrated from Brio Intelligence

	From ODS	From BCS
Automatically Migrated	• Adaptive States • Custom SQL variable limits • Documents • Folders • OCEs • Passthrough for Query Map • Section OCE mapping • User/Group attributes • Users/Groups • Username and password inside OCEs	• Calendars • Directories and printers • Documents • External events • Job cycles • Job intervals • Job parameters • Jobs • Location of output files • OCEs • Section OCE mapping • User/Group attributes • Users/Groups
Manually Migrated	• Content requiring special information such as password-protected documents and BQY documents with detail section reports.	

	From ODS	From BCS
	See "Migrating the Test Server" on page 24 for a description of the steps involved in manually moving Brio Intelligence components to Reporting and Analysis.	
Not Migrated	• Inactive users In Reporting and Analysis, inactivating a user is essentially deleting a user. • Multiple ODS/BCS installations The Migration Utility does not support multiple installations of ODS/BCS as part of a networked environment where users on one host are accessing content located in a directory on another server installation. You must migrate additional installations of ODS and BCS separately. • Automatic distributed refresh (ADR) Reporting and Analysis does not support automatic distributed refresh for BQY jobs. • HTML template customizations	

Migrating from BrioONE

For a BrioONE implementation that has Brio Intelligence with ODS, BCS, or ODS running as a Portal service, you must run the Portal migration first, and then run the Brio Intelligence migration.

For a BrioONE implementation, the migration is similar to a conversion where content from product A is transformed and merged with content in product B. Migrating from BrioONE is essentially the same as migrating from Brio Intelligence and Portal.

Migrating from BrioONE requires more manual steps than a stand-alone migration because you need to decide what to migrate or not migrate and how to handle duplicate content; determine the target folders in the Repository; verify data sources; convert BCS/ODS documents, jobs, and job output to Reporting and Analysis jobs and job output; and so forth. These manual steps are described in "Migrating the Test Server" on page 24.

Migrating from Hyperion Analyzer

Hyperion Analyzer has a repository that contains the users, groups, folders, reports, books and batches. Table 3 describes the Hyperion Analyzer items that are automatically migrated, the items that you must manually migrate, and the items that are not migrated to Reporting and Analysis.

Table 3 Items Migrated/Not Migrated from Hyperion Analyzer

Automatically Migrated	• Folders • Reports

	• User Preferences • Database Connections • Presentations • Folder Shortcut UI • File Permissions • Users • Groups
Manually Migrated	• External authentication of users and groups You do not have to re-create users and groups in the target system. See "Components Requiring Pre-migration Steps" on page 31 for an overview of the steps required to set up external authentication in Reporting and Analysis and to migrate user and group attributes from the source system to the target system.
Not Migrated	• Custom pages or Analyzer API programs Custom pages and Analyzer API programs must be rewritten to reflect the System 9.0 Web Analysis API.

Migrating from Hyperion Reports

Hyperion Reports has a repository that contains the users, groups, folders, reports, books and batches. Table 4 describes the Hyperion Reports items that are automatically migrated, the items that you must manually migrate, and the items that are not migrated to Reporting and Analysis.

Table 4 Items Migrated/Not Migrated from Hyperion Reports

Automatically Migrated	• Folders • Reports • Books • Batches • Templates • Database Connections • SnapShot • Users • Groups
Manually Migrated	• External authentication of users and groups You do not have to re-create users and groups in the target system. See "Components Requiring Pre-migration Steps" on page 31 for an overview of the steps required to set up external authentication in Reporting and Analysis and to migrate user and group attributes from the source system to the target system.
Not Migrated	• Command line programs Command line programs need to be updated for changes in the System 9.0 Web Analysis API. • Batch scheduling Only batches are migrated to the repository.

Migrating from Hyperion Performance Suite 8.x

Table 5 describes the Hyperion Performance Suite items that are automatically migrated, the items that you must manually migrate, and the items that are not migrated to Reporting and Analysis.

Table 5 Items Migrated/Not Migrated from Hyperion Performance Suite

Automatically Migrated	• Folders • SQR jobs • Generic jobs • Documents • Personal pages • Subscriptions • Favorite items • Users • Groups • BQY Documents and Jobs • Custom SQL variable limits • OCEs • Passthrough for Query Map • Section OCE mapping • Calendars • Directories and printers • External events • Job cycles • Job parameters • ACLs
Manually Migrated	N/A
Not Migrated	• Custom forms • External authentication systems You must set up any external authentication systems in the target environment prior to migration. • Inactive users In Reporting and Analysis, inactivating a user is essentially deleting a user. • WebClient Customizations The Reporting and Analysis environment uses a combination of JSP and templates. The Migration Utility does not migrate WebClient templates and their customizations.

Migrating a Customized Environment

You may need to contact a local consulting partner or Hyperion Solutions for support if you want to migrate any of the following customizations:

- Bulk functionality

  For example, bulk load scheduled jobs in a Job Factory, bulk load/edit/delete users and groups, and bulk import/edit report properties.

- Customized security

  For example, two levels of security checking or an API that performs routine synchronization with a security database.

- Altered Brio Intelligence schemas
- Customized web templates

Other Migration Considerations

In addition to understanding the general migration process and reviewing the migration prerequisites, review the following topics for some additional issues to consider before migration.

- Special Symbols in Users and Groups
- Invalid Characters in EPM Workspace
- SmartCuts
- Migrating SAP Database Connections

Special Symbols in Users and Groups

There are certain symbols in a user's first name, a user's last name, a user's login ID, and a group name that are not allowed in Reporting and Analysis. If the Migration Utility encounters any of these symbols, it replaces them with an acceptable symbol. Table 6 shows the symbol in the source system and the symbol it is replaced with in Reporting and Analysis.

Note:

These symbols also apply to roles migrated from the Hyperion Performance Suite 8 source system.

Table 6 Special Symbols

Symbol in Source System	Symbol in Reporting and Analysis
,	_
=	-
+	*
<	[
>	]

Symbol in Source System	Symbol in Reporting and Analysis
(	[
)	]
;	:
\	/
"	`
#	~ **Note:** The '#' symbol is replaced with the '~' symbol only if the '#' symbol is in the first position.

Example

During migration, a user name of `Smith,Alex` is changed to `Smith_Alex`.

Note:

User login IDs and group names are trimmed for space symbols in the first and last positions.

Invalid Characters in EPM Workspace

The following characters are not supported for objects in Oracle Enterprise Performance Management Workspace, Fusion Edition. Rename objects or folders containing these characters before migrating from the source system to the Reporting and Analysis Repository.

Invalid Name Characters

- \
- /
- %
- ?
- +
- <>
- |
- '
- *
- :
- "

Invalid Path Characters

- \

- %
- ?
- +
- <>
- |
- '
- *
- :
- "

SmartCuts

SmartCuts for object names with unsupported characters will not be displayed in EPM Workspace after migration. To ensure that your SmartCuts appear in EPM Workspace, you should update any SmartCuts in your source system to use supported characters.

For information on supported characters for SmartCuts, see "Managing SmartCuts" in the *Hyperion Workspace Administrator's Guide*.

Migrating SAP Database Connections

To migrate SAP database connections, do the following before running the Migration Utility:

- **UNIX**: Copy `SAPLOGON.INI` to the `$HOME` directory, or ensure that the file location is specified in the `$SAPLOGON_INI_FILE` environment variable.
- **Windows**: Copy `SAPLOGON.INI` to the `%WINDIR%` directory, or ensure that file location is specified in the `%SAPLOGON_INI_FILE%` environment variable on the server where SAP is installed.

Note:

The `SAPLOGON_INI_FILE` environment variable should be a directory.

Migration End Result

The final product is a working Reporting and Analysis installation that contains the migrated data (including users, groups, and content) from the existing:

- Brio Portal Repository
- Brio Intelligence Broadcast Server Repository
- Brio Intelligence OnDemand Server Repository
- Brio Intelligence OnDemand Server Repository when running as a Brio Portal service
- Hyperion Analyzer Repository

- Hyperion Reports Repository

2 Performing Migration

In This Chapter

About Performing Migration

Performing migrations on a test server provides the smoothest possible migration of your production system with the least impact on your overall business operations. In addition, you may decide to run the final migration on the test server rather than on the production system. This can save time and resources and enables the current system and the new system to run in parallel until the new Reporting and Analysis server is ready for general use. The best practice for testing and final migration involves qualified personnel working with a dedicated test environment that can be restored to its original state.

The person performing the test and final migrations must be highly familiar with your current products as well as Reporting and Analysis administration tools and processes. In addition to the documentation available with the installation, many courses are available through Hyperion Education Services. Optionally, local consulting partners or Hyperion consulting can help with performing the testing, validation, and final migration process.

Migration Process Checklist

Table 7 provides a brief outline of the tasks involved in migration. The following sections provide more details about each phase.

Table 7 Migration Process Checklist

Migration Steps	Details

❑	**Set up a test server on the target system**	Performing migration on a test server provides the smoothest possible migration of your production system with the least impact on your overall business operations. See "Creating the Test Environment" on page 18 for a detailed description of testing.
❑	**Fulfill prerequisites**	See "Prerequisites for Using the Migration Utility" in the *Migration Guide* for a detailed list.
❑	**Perform manual premigration steps**	Some items are not automatically migrated by the Migration Utility; instead, they require pre-migration or post-migration steps to get transferred to the new system. See "Migrating the Test Server" on page 24 for a list of manually migrated items and how to migrate them.
❑	**Migrate in pre-migration test mode**	Review the log files for any initial problems. Use the findings to adjust your plan as necessary.
❑	**Test the migration**	Take extensive notes about every aspect of the initial test migration. The findings provide a tool for making adjustments to your plan. See "Migrating the Test Server" on page 24 for more details.
❑	**Perform manual post-migration steps**	See "Manual Migration Steps" on page 30 for a list of manually migrated items and how to migrate them.
❑	**Evaluate test results**	Review the log files and the target system content according to your migration plan. Use your findings to adjust your plan if necessary.
❑	**Reset the test server to the original system**	Use the original system copies to restore the test server to its original state. The next round of migration testing uses this "pristine" system to validate your updated migration plan.
❑	**Test the migration again**	When you think your migration plan covers all contingencies, try the migration one more time. Validate the migration. If the migration is not complete, perform the necessary changes and migrate again until the test results are clean.
❑	**Migrate the production server**	When your plan is finished, use it to perform a rapid migration of the production server. You may want to do this during off-peak hours such as evenings or over a weekend.

Note:

The testing phase generally includes what the Migration Utility can migrate automatically. Evaluate what you need to manually migrate during the source system assessment and map solution strategies for those manual tasks. See "Manual Migration Steps" on page 30 for steps on transferring items you must manually migrate. See "Mapping Access Privileges to Reporting and Analysis" on page 32 for a list of automatic and manual steps to allow users proper access Reporting and Analysis content.

Creating the Test Environment

You can set up your test environment on either one or two computers. If you have the resources to set up two systems, follow the environment prerequisites listed in the following section. If you prefer to setup one test box for both source and target environments, ensure that the third-party hardware and software used is compliant with Reporting and Analysis requirements.

The test environment must host both a source system—with Brio Portal, Brio Intelligence, Hyperion Analyzer, or Hyperion Reports installed—and target servers with Reporting and Analysis installed. If necessary, you can perform migration testing using remote session tools.

Review the following sections for information on:

Environment Prerequisites

Review the following sections to assess your source and target system hardware and software against the prerequisites for migration.

Supported Source Environments in the Existing Installation

The Migration Utility supports migration from the following product versions:

- Brio Portal 7.0.5
- BrioONE (Brio Portal 7.0.5 or later and the OnDemand Server 6.6.4 or later)
- Brio Intelligence Server 6.6.4 (OnDemand Server 6.6.4 or later and Broadcast Server 6.6.4 or later)
- Hyperion Analyzer 6.5, 7.0.1, 7.2, 7.2.1
- Hyperion Performance Suite 8.x
- Hyperion Reports 7.0.x or 7.2.x

Note:

The Migration Utility does not support the Macintosh operating system or any customized operating systems.

Supported Target Environments

For migration from a database or platform no longer supported in Reporting and Analysis you must switch to a supported database or platform before running the Migration Utility. See the Reporting and Analysis Support Matrix on the Customer Support site for a list of supported operating systems, databases, Web servers, servlet engines, and browsers.

Note:

If you do not have a supported product release installed in your source environment, you must upgrade to a supported release prior to migration. You can then install Reporting and Analysis

and migrate the installation. If necessary, please contact your local consulting partner or Hyperion for assistance.

Setting Up the Source System

To set up the source test system properly, host the current production system in a test environment. The source test server should mirror the following aspects of the existing system:

- **Server configuration**—Use the same directory structure for the test system, as the one used in the current production system.
- **Data files**—Move all documents to the test environment. Use binary copies where appropriate.

If you have a functional test source system, you can delete all the objects that will not be migrated according to your migration plan from the test environment. This task is optional.

The checklists in the following sections describe the general aspects of creating a source test system. Steps may vary for each implementation. UNIX systems may require the use of binary file transfer. For information on hardware and software requirements, see "Environment Prerequisites" on page 19.

Creating a Source Test System for Brio Portal/Brio Intelligence

Table 8 describes the general aspects of creating a source test system for Brio Portal/Brio Intelligence.

Table 8 Brio Portal/Brio Intelligence Source Test Server Checklist

❑	Install/upgrade the test server operating system for assessment as required. See "Environment Prerequisites" on page 19 for operating system requirements.
❑	Open and save all repository BQYs to Brio Enterprise or Brio Intelligence 6.2.2 or later.
❑	Copy Brio Repository tables from the production database to the test database.
❑	Convert any Detail sections in your BQY documents to Report sections. (Reporting and Analysis does not recognize Detail sections and will not be able to open documents that contain these sections.)
❑	Copy Brio Server INI files and the ODS password (for Windows 6.2.x versions and all UNIX installations) or define the setting, such as printers. Brio Servers (6.5) INI settings are maintained in the Windows registry. You must export the registry entry from the production system and import it into the test server registry.
❑	Install Brio Enterprise or Brio Intelligence 6.2.2 or later on the test server to connect to the test Repository. Modify Repository and server configuration files (for BrioONE and Portal) to use the test server name.
❑	Copy converted files created prior to Brio Enterprise 6.2.2 to the test server. This could take considerable time depending on the size of the ODS and BCS document directories.
❑	Copy OCE files to the test server. Any OCE that is setup to use database drivers not compliant with Reporting and Analysis should be opened, updated, and republished to the Brio Enterprise or Brio Intelligence 6.2.2 or later prior to migration.

❑	Copy customized HTML files to the test server. Requirements for Brio Portal and Brio Intelligence Web interface customizations should be reanalyzed for Reporting and Analysis deployment.
❑	Test logging into the test server with customized Web pages.
❑	Download, copy, and install the Migration Utility. See the *Hyperion Reporting and Analysis Migration Utility Guide* for information on using the Migration Utility.

Creating a Source Test System for Hyperion Analyzer

Table 9 describes the general aspects of creating a source test system for Hyperion Analyzer.

Table 9 Hyperion Analyzer Source Test Server Checklist

❑	Install/upgrade the test server operating system for assessment as required. See "Environment Prerequisites" on page 19 for operating system requirements.
❑	Backup the Hyperion Analyzer Repository.
❑	Copy Hyperion Reports Repository tables from the production database to a test database.
❑	Install the version of Hyperion Analyzer that corresponds to the Production server.
❑	Download, copy, and install the Migration Utility. See the *Hyperion Reporting and Analysis Migration Utility Guide* for information on using the Migration Utility.

Creating a Source Test System for Hyperion Reports

Table 10 describes the general aspects of creating a source test system for Hyperion Reports.

Table 10 Hyperion Reports Source Test Server Checklist

❑	Install/upgrade the test server operating system for assessment as required. See "Environment Prerequisites" on page 19 for operating system requirements.
❑	Backup the Hyperion Reports Repository.
❑	Copy Hyperion Reports Repository tables from the production database to a test database.
❑	Install the version of Hyperion Reports that corresponds to the Production server.
❑	Configure the Hyperion Reports server for the Hyperion Reports Repository.
❑	Connect Hyperion Reports to the Production Repository.
❑	Download, copy, and install the Migration Utility. See the *Hyperion Reporting and Analysis Migration Utility Guide* for information on using the Migration Utility.

Setting Up the Target Test System

After you set up the source test server, you can set up the target test server. You do not need to set up your target system exactly as you have your Reporting and Analysis system implemented and distributed for production use. This is because you can perform final Reporting and Analysis configuration after migration. However, you must have the correct hardware and software as specified in "Environment Prerequisites" on page 19. You can set up the Reporting and Analysis installation directory according to your site's best practice.

While your Reporting and Analysis architecture may match current product deployment infrastructure in size and number of systems, the Reporting and Analysis solutions are configured with server names different from the current production box. It is best to perform this configuration prior to migration. Plan for the appropriate IT resources to create the proper environment with new network DSN settings for the Reporting and Analysis production instance.

The checklists in the following sections describe the general aspects of creating a target test system. Steps may vary for each implementation.

Table 11 describes the general aspects of creating a target test system.

Table 11 Target Test Server Checklist

❑	Set up all supported hardware and software according to the Reporting and Analysis requirements. See """Environment Prerequisites" on page 19 for information on hardware and software requirements for the target system.
❑	Download, copy, and install Reporting and Analysis .
❑	For a Brio Portal migration, configure your hosts (including those that you use as data sources) so that your services are distributed exactly the same way that they are distributed in the source system. See "Setting Up Hosts" on page 22 for more information on proper host configuration.
❑	For a Brio Portal migration, set up your authentication appropriately. See "Setting up Authentication" on page 23 for more information on authentication in the target system.
❑	Download, copy, and install the Migration Utility.
❑	Verify that the performance of your test environment is comparable your production environment and that the appropriate output is produced.
❑	Make a backup of the test server files, directories, and databases after the initial setup. This way, you do not have to reinstall Reporting and Analysis after each test migration.

Setting Up Hosts

When performing a Portal or BrioOne migration, define the mapping for the Source and Target hosts. Using the Migration Utility, map the source host to the target host by entering names of the source and target hosts in the Source-Target Host Mappings screen in the Migration Utility wizard. For example, you must map each source job factory to a target host job factory.

For the BrioOne and Intelligence Server migration, you will be prompted for configuration information for the Target system, including the Target Host, Target Port, Username and Password.

For Reports Migration, you will need the Reports Administrator and the Global Administrator user ID and password.

Setting up Authentication

Setting up authentication involves configuring external authentication for Shared Services. To set up authentication, configure Shared Services with whatever properties are needed to access the external directory services (NTLM, Microsoft AD, or LDAP).

For detailed information on setting up external authentication for Shared Services , see the *Hyperion System 9 Shared Services Installation Guide*.

Validating the Test Environment

Before testing, validate the functionality of the test environment. Table 12 lists the general steps involved in validating the test environment. The table assumes that appropriate high-level planning and system requirements have been fulfilled. For information on environment prerequisites and other migration steps, see "Environment Prerequisites" on page 19 and "Migrating the Test Server" on page 24.

Table 12 Test Environment Validation Checklist

Validation Steps		Details
❑	**Validate source system setup**	To validate the source system setup, run the Migration Utility in the pre-migration test mode. The Migration Utility automatically confirms that all source system settings are properly mapped and that the Repository database is accessible. You can use the log files generated by the Migration Utility for troubleshooting if necessary.
❑	**Validate target system setup**	Bring up the new Reporting and Analysis system at least one time to ensure that the products are installed and configured properly. Use the sample content, which is provided with the Reporting and Analysis installation to validate that the server is functional. Note: Administrators should not log into the target system as a user that is being migrated. Instead, administrators should create a new native user (in the Oracle's Hyperion® Shared Services Console), provision the user with any necessary roles, and log into the system as the new user.
❑	**Validate the source repository**	Before validating the source repository, you may want to delete all objects that will not be migrated. Validating the source repository involves testing the source Repository content for issues such as illegal document and folder names, unsupported document types like ADR managed documents, and so on.

Migrating the Test Server

You can begin migration testing after you set up and validate the test environment and create an initial plan (see "Validating the Test Environment" on page 23). In many cases, the test migration is not much different from the final migration, so you can use the guidelines discussed in this section as a basis for the final migration.

Caution!

Do not publish documents in Reporting and Analysis until you successfully migrate the source system. In addition, do not change the content of the ODS and BCS repositories during migration. Make sure that jobs are not changed, no new documents are registered, and no physical resources (printers or directories), groups, users, or OCEs are added or modified.

Order of Migration

It is recommended that you run the migration in a "staged" process (one type of object at a time). When using the Migration Utility it is possible to migrate all components in one run or to migrate components incrementally; however, you must migrate all components in the order displayed in the Migration Utility. Back up your data after each successful migration instance to ensure easy restoration if you need to repeat the process.

Review the following sections for information on:

- Brio Portal Migration Order
- Brio Intelligence Server Migration Order
- Hyperion Analyzer Migration Order
- Hyperion Reports Migration Order
- Hyperion Performance Suite Migration Order

Brio Portal Migration Order

When you migrate from Brio Portal or BrioONE, follow this sequence:

1. **Brio Portal pre-migration check**—Use the Migration Utility in pre-migration test mode to identify possible migration problems.
2. **Brio Portal migration**—The Migration Utility copies the metadata for the Repository Service and Event Service and maps it into the Reporting and Analysis database schema. Whether or not you choose to migrate the following components all at once or separately, you must migrate them in the order shown:
   - **Users**—Account owners identified by a user ID and user name.
   - **Groups**—Named collections of users.
   - **User Preferences**—User-specific settings.

- **Repository Metadata**—Descriptions of the repository data. For example, the metadata could display the name of the content, permissions, etc.
- **Events**—User subscriptions and notifications of events involving subscriptions, jobs, parameter lists for jobs, and exceptions.
- **Authorization**—Access control information for folders, documents, and resources.
- **Repository Content**—The content of the system, folders, and files. Repository contents is the largest object to migrate.

Brio Intelligence Server Migration Order

When you migrate from Brio Intelligence, follow this sequence:

1. **Brio Intelligence Server pre-migration check**—Use the Migration Utility in pre-migration test mode to identify possible migration problems.
2. **Brio Intelligence Server migration**—Whether or not you choose to migrate the following components all at once or separately, you must migrate them in the order shown:
   - **ODS Objects**

     Users—Account owners identified by a user ID and user name.

     Groups—A named collections of users.

     Folders—Items are organized into folders. Folders are similar to the directories or folders of your operating system, and are arranged in a hierarchical structure. A folder can contain subfolders, items, or both.

     OCE Files—Files that encapsulate and store connection information used to connect Hyperion applications to a database. OCE files specify the database API (ODBC, SQL*Net, etc.), database software, the network address of the database server, and your database user name. Once created, a user can specify the OCE file and database password and logon. An OCE file is required for a Hyperion Intelligence document to use a database, the file extension is .oce.

     BQY Documents—Files created by Hyperion Intelligence and published into the Repository as files or as jobs.

     Row Level Security Data—Data containing row-level security. Row-level security gives users access to only the information they need to make informed decisions. For example, managers need payroll information on their direct reports. Managers do not need to know payroll information for other departments within the organization. When you select this object, the next page in the Migration Utility wizard prompts you to configure the target row level security repository.

   - **BCS Objects**

     Users—Account owners identified by a user ID and user name.

     Groups—A named collection of users.

     Calendars—Calendars used to schedule jobs in the Broadcast Server.

     Events —Events in the Broadcast Server.

Printer Paths—Printer path definitions in the Broadcast Server.

Paths—Path definitions in the BroadCast Server.

OCE Files—Files that encapsulate and store connection information used to connect Hyperion applications to a database. OCE files specify the database API (ODBC, SQL*Net, etc.), database software, the network address of the database server, and your database user name. Once created, a user can specify the OCE file and database password and logon. An OCE file is required for a Hyperion Intelligence document to use a database, the file extension is .oce.

BQY Jobs —Jobs created by Hyperion Intelligence and published into the Repository.

Hyperion Analyzer Migration Order

When you migrate from Hyperion Analyzer, follow this sequence

1. **Hyperion Analyzer pre-migration check**—Use the Migration Utility in pre-migration test mode to identify possible migration problems. The test mode is only available for users and groups. You cannot run a pre-migration test on repository content.
2. **Hyperion Analyzer migration**—The Migration Utility copies the Repository and maps it into the Reporting and Analysis database schema. Whether or not you choose to migrate the following components all at once or separately, you must migrate them in the order shown:
   - **Users and Groups**-—Users are account owners identified by a user ID and user name. Groups incorporate named collections of users.
   - **Repository Content**— The content of the system, namely: folders, files, jobs, URLs, and shortcuts and their metadata (properties). The content resides in the repository, which consists of file in the native file system and metadata for each object in a database in a Relational Database Management System (RDBMS). Repository content is the largest object to migrate.

Hyperion Reports Migration Order

When you migrate from Hyperion Reports, follow this sequence:

1. **Hyperion Reports pre-migration check**—Use the Migration Utility in pre-migration test mode to identify possible migration problems. The test mode is only available for users and groups. You cannot run a pre-migration test on repository content.
2. **Hyperion Reports migration**—The Migration Utility copies the Repository and maps it into the Reporting and Analysis database schema. Whether or not you choose to migrate the following components all at once or separately, you must migrate them in the order shown:
   - **Users**—Account owners identified by a user ID and user name.
   - **Groups**—A named collection of users.
   - **Repository Content**—The content of the system, namely: folders, files, jobs, URLs, and shortcuts, and their metadata (properties). The content resides in the Repository, which consists of files in the native file system and metadata for each object in a database in a

Relational Database Management System (RDBMS). Repository content is the largest object to migrate.

Hyperion Performance Suite Migration Order

When you migrate user provisioning information from Hyperion Performance Suite, follow this sequence:

1. **Hyperion Performance Suite pre-migration check**—Use the Migration Utility in pre-migration test mode to identify possible migration problems.
2. **Hyperion Performance Suite migration**—Whether or not you choose to migrate the following components all at once or separately, you must migrate them in the order shown:
   - **Users Defined Roles**—The roles defined for the users in the Hyperion performance Suite 8.x system.
   - **Users**—Account owners identified by a user ID and user name.
   - **Groups**—Named collections of users.
   - **User Preferences**—User-specific settings (such as an email address).
   - **Repository Metadata**—Descriptions of the repository data. For example, the metadata could display the name of the content, permissions etc.
   - **Repository Files**—The content of the system, folders, and files. Repository content is the largest object to migrate.
   - **Events**—User subscriptions and notifications of events involving subscriptions, jobs, parameter lists for jobs, and exceptions.
   - **Authorization**—Access control information for folders, documents, and resources.

Migration Test Checklist

Table 13 shows the basic steps involved in testing a migration, which may vary for each product implementation.

Table 13 Migration Test Checklist

Migration Test Steps		Details
❑	Migrate in pre-migration test mode	First, run the Migration Utility in pre-migration test mode. When run in pre-migration test mode, the Migration Utility performs all steps necessary to run an automated migration but does not actually move files from the source system to the target system or move data to the Repository tables. Next, review the log files for possible complications. Correct any issues before running the actual migration without having to reset the target environment. For additional information on how to run the Migration Utility in pre-migration test mode, follow the instructions in the *Hyperion Reporting and Analysis Migration Utility Guide* **Note**: Running the Migration Utility in pre-migration test mode does not uncover all issues. Additional errors may arise in the actual migration, so try this process on a test server before initiating it on the production environment. If the test server is to become the

		production Reporting and Analysis instance, then your test migration is your production system. In this case, the migration process is shorter but should have the same emphasis on incremental backups throughout the process.
❑	Evaluate pre-migration test run log files	Evaluate the log files to determine which aspects of the source system need modification before you perform the final pre-migration test run. Modify the source system according to the log messages. See "Using the Migration Log Files " on page 29 for more information.
❑	Migrate the test server	After you get a clean pre-migration test run, perform an actual migration on the test server. Take notes about every aspect of what you encounter during this initial test migration. Also, log the time it takes to complete the automated process.
❑	Validate your test	Analyze the migration log files for important messages, and check all components of the migrated system. Check that all users, groups, files, directories, and properties migrated properly. Check job schedules, OCEs, and e-mail notifications. Run some jobs. Both performance and data validation are important components of validating your test migration. See "Validating the Test Environment" on page 23 for more information on the validation process. Use your findings to adjust your migration plan if necessary.
❑	Reset the test server	Reset the target test server to the original system. Use the backup copies of the original system to restore the test server to its original state. The next round of migration testing uses this "pristine" system to validate the updated migration plan.
❑	Re-test the migration	When you think your migration plan covers all contingencies, try the migration one more time. Make sure that you can perform a complete and successful migration using only the migration plan. Take extensive notes again. If you cannot migrate with total success, use those notes to modify the migration plan further. Keep repeating this test, reset and retest cycle until you get a totally clean migration. During this final test migration, keep track of the time it takes from start to finish, so you can plan the scheduling of the production system migration accordingly. Keep track of all the resources you used as well. Resource tracking should include both computer resources and personnel. You need a complete picture of everything it takes for a smooth migration of the production system.

Note:

While migrating the production system, users need to be locked out of the system until migration and validation are complete.

Evaluating Test Results

After completing the test migration, ensure that all components migrated correctly by checking components in the system and using the migration log files. As a result of the analysis, your team can identify the migrated content and the content that you need to recreate for Reporting and Analysis. Successful testing requires a working knowledge of Reporting and Analysis.

Using the Migration Log Files

The Migration Utility produces log files, which contain error messages, whenever it is run in either pre-migration *test* mode or for the actual migration in *run* mode.

The Migration Utility produces log files for each migration. The log files produced depend on which products you selected in the Migration Utility wizard.

For each product migrated, you select the level of the error messages and the location of the log files in the Migration Utility wizard.

The Migration Utility saves each log produced with a time/date stamp inserted before the `.log` extension. This makes it easy to compare the outcomes of the migrations. For example:

```
migration_0811041139.log
```

Checking the Components Within the System

Confirm that all required components and objects correctly migrate to the Reporting and Analysis test environment. Table 14 includes some post-migration validation tasks:

Table 14 Post-migration Validation Tasks

❑	Verify users and groups in the target system with a particular emphasis on permissions and group membership.
❑	Verify folder structure and documents in the target system with particular emphasis on document location and folder ownership.
❑	Verify OnDemand Server content in the target system with particular emphasis on documents and processing connections.
❑	Verify Broadcast Server content in the target system with particular emphasis on jobs and events.
❑	Verify Job Factories and jobs in the target system with particular emphasis on SQR jobs, databases, and hosts.
❑	Verify that all jobs run according to schedule. Schedule an infrastructure review with Hyperion Consulting Services or your local partner to address performance concerns.
❑	Verify that all jobs produce the appropriate output.

Tip:

You can use the Hyperion Intelligence inventory BQY to determine source system counts for the various items migrated.

Tip:

See Chapter 3, "Validating Migration Results" for an expanded list of migration validation and general post-migration steps.

Migrating the Production Server

After you thoroughly test your migration plan in a test environment, you can perform the final migration either on the same test server or on the production server. Performing the final migration on the test server can often save time and resources and may enable the current system and the new system to run in parallel until the new Reporting and Analysis server is ready for general use.

The final migration should follow the same process as that used for testing. You can use the previous sections of this chapter as a reference for both test and final migration.

Note:

During the final migration process, it is critical that you have a plan for change control or that you do not make any changes until you complete the migration and validation of the production server. Failure to implement a change control process or prevent changes will most likely lead to undesired results.

After you validate the successful migration of content using the Migration Utility, you can perform system configuration and customizations as necessary according to your migration plan.

An example of system configuration is finalizing the production server according to the Reporting and Analysis architecture, which may include deleting obsolete Brio Portal Job Factories (Hosts) and data sources, installing and configuring new Job Service hosts and associated data sources, and editing affected jobs.

Allow a grace period to verify that all jobs are running according to schedule and that components are working properly in the new system. After you set up the Reporting and Analysis server to suit the needs of your organization, users can begin working with the new system.

Manual Migration Steps

Once you meet the migration prerequisites, determine which system components need to be manually migrated. Depending on your current product solution, you may need to perform fewer manual migration steps. The Migration Utility migrates most repository content, including items such as users, groups, and their attributes, documents, folders, OCEs and so on. Because of the complexity of some items, they may require manual migration steps, which are completed either prior to or after you run the Migration Utility. Other components cannot be migrated because Reporting and Analysis does not support them.

Review the following sections for information on:

- Components Requiring Pre-migration Steps
- Components Requiring Post-migration Steps

Note:

You can contact your local consulting support or Hyperion for help with migrating items that are not fully supported by the Migration Utility.

Components Requiring Pre-migration Steps

Table 15 lists the pre-migration steps for components that the Migration Utility does not automatically migrate. After you perform these pre-migration steps, you can use the Migration Utility to automate migration for the remainder of the components.

Table 15 Pre-migration Steps for Items Not Automatically Migrated by the Migration Utility

Components Manually Migrated	Pre-migration Step	Source System
BQY documents with detail section reports	Convert BQY documents with detail section reports (left over from 5.5) into report sections. Then save the documents in Brio Enterprise or Brio Intelligence 6.2.2 or later and delete the detail section.	Intelligence Server
Externally authenticated users and groups	The Migration Utility does not migrate users and groups that were imported into Portal from an external source. As a result, you should set up Shared Services to import users and groups from the same external source you used to import them into Portal. Perform this step prior to Portal migration."	Portal
MAPI email addresses	MAPI email addresses are not supported in Reporting and Analysis. Convert MAPI email addresses to SMTP addresses prior to migration.	Intelligence Server
Password protected documents	Remove password protection to migrate these documents	Intelligence Server
Group and folder names with special characters	There are certain symbols in a user's first name, a user's last name, a user's login ID, and a group name that are not allowed in Reporting and Analysis. If the Migration Utility encounters any of these symbols, it replaces them with an acceptable symbol. See "Special Symbols in Users and Groups" in the *Hyperion Reporting and Analysis Migration Utility Guide*. for information on the symbols are replaced after migration to Reporting and Analysis	
General source system cleanup	You may want to remove source system content that is no longer used or referenced such as: invalid or unused OCEs, expired reports, irrelevant jobs, users no longer with the company, outdated groups, etc.	N/A

Note:

If you configured row-level security (RLS) parameters in your Reporting and Analysis installation prior to migration, the Reporting and Analysis automatically migrates these parameters. After migration, make sure that RLS is enabled in the new system.

Components Requiring Post-migration Steps

Table 16 lists the post-migration steps for migrating components that the Migration Utility does not automatically migrate. See "Validating Hyperion Performance Suite Migration" on page 45 for more information.

Table 16 Post-migration Steps for Items Not Automatically Migrated by the Migration Utility

Components Not Migrated	Post-migration Step	Migration Utility
Alternate metadata OCEs	Alternate metadata OCEs are not migrated. After migration, you must reestablish the link to the alternate metadata OCE.	Intelligence Server
Append Job ID and Report Cycle Name to File Name to Ensure Uniqueness job parameter.	The Append Job ID and Report Cycle Name To File Name to Ensure Uniqueness action parameter is not migrated. You must modify the Append Unique Identifier to Filename parameter in Reporting and Analysis after migration.	Intelligence Server
Locally saved documents	The Migration Utility does not migrate locally saved documents, but the "source" document from which the locally saved document originated is migrated. After migration, if users want to work with locally saved documents online, they must manually enter the URL of the new servlet in the Connection Dialog box. The user must choose Edit on the dialog box and change the server computer name in the URL to that of the new system. For example, the user must replace the bracketed information in the following URL to connect: http://< server machine name>/Brio/dataaccess/browse? By editing the URL, users reestablish the link between the local and the published copy of the document. After a user saves a document with the new URL, the user is no longer prompted to enter the new URL when working with that document online. **Note**: You can allow users to publish their documents to the server by giving them appropriate rights to a personal directory.	Intelligence Server
SmartForms (custom forms)	The custom forms for SQR are now created with JSP (Java Server Page) technology; previous versions were created with HTML. SmartForms must be re-created or edited with JSP to work in Reporting and Analysis.	Portal
Web client customizations	Web client customizations are not migrated. They must be redone after migration.	Intelligence Server

Mapping Access Privileges to Reporting and Analysis

Reporting and Analysis uses roles as a way of granting users and groups access to business functions. For example, the job publisher role grants the privilege to run or publish a job. Before

migrating, make a detailed plan for applying roles and access privileges in the Reporting and Analysis system, based on the Migration Utility generic system for granting roles and access privileges.

Review the following sections for information on:

- Role Mapping
- Access Control Mapping

Role Mapping

To preserve the functions assigned to certain users and groups in the old system, the Migration Utility maps these users and groups to new roles in Reporting and Analysis. In some cases the Migration Utility automatically assign roles at the group or user level, but in other cases you must assign roles as a post-migration step.

See Migrating Roles in the *Hyperion Reporting and Analysis Migration Utility Guide* for information on how legacy roles in the source system are mapped to new roles in Reporting and Analysis.

Access Control Mapping

BQY documents and scheduled jobs in the Brio Intelligence repositories do not have access control like that in Portal and Reporting and Analysis. The Migration Utility uses the guidelines in Table 17 to apply access to migrated components.

Table 17 Access Control on Migrated Components

Server	Components	Access Privilege
ODS	Folders	All ODS groups get View access control on ODS folders. The Content Publisher role gets Modify access on ODS folders. BI_Migrate.ini provides a parameter value that enables you to assign all ODS groups to one default ODS group. If you have many ODS groups, having this "parent" group makes assigning access control privileges on folders much more efficient than having to assign access control privileges to many groups individually.
	OCEs	The owner of ODS OCEs is the Administrator (the user who performs the migration). The Content Publisher role is assigned View access privilege to ODS OCEs.
	Documents	After migration, there is no change in the adaptive states on ODS-registered documents. However, the corresponding access privileges are added. Consider these examples: ● If the Sales Group has View adaptive state in the source system, it has View access to documents and View adaptive state access on jobs in Reporting and Analysis. ● If the Marketing Group has View and Analyze adaptive state in the source system, then it has View access to the document and View and Analyze adaptive state access on jobs in Reporting and Analysis.

Server	Components	Access Privilege
BCS	BCS jobs	In Reporting and Analysis, job owners have full control and Datamodel adaptive state access on their jobs but have no specified control on the job output.
	Job output	Because the publishing user has to specify Group adaptive state access to the job output in the same way as with a BQY document, groups are given various levels of adaptive state access. So if Sales has View and Analyze on the output, then Sales has View access to the output properties and View and Analyze access to the content.
	Job schedules and parameters	The user who scheduled the job is the owner of the job in the new system. In Reporting and Analysis, job owners have full control access and Datamodel adaptive state access on their jobs but have no specified control on the job output.
	OCEs	The owner of OCEs is the Administrator (the user who performs the migration). The Job Publisher role is assigned View access on BCS OCEs
	Physical resources	Groups that have access to directories and printers have View access to those same directories and printers in Reporting and Analysis.
	Calendars and externally triggered time events	The Public group and all custom groups should have access to these calendars and externally triggered events. Administrators already have access, because the Migration Utility assigns the Schedule Manager role to users who belonged previously to the Administrator group. Therefore, administrators have implicit access to all objects in theReporting and Analysis Repository.
HPSu	Deactivated Users/Groups	Deactived users and groups are not migrated to Reporting and Analysis. As a result, you should activate any deactivated users that you want to migrate prior to migration. Users can be manually deactivated after migration using the Shared Services User Management Console.Shared Services does not support the deactivation of groups.

3 Validating Migration Results

In This Chapter

About Validating Migration Results

After you complete the migration, ensure that all components migrated properly. This process includes checking the components in your system and using the log files to validate migration. You may have migrated some or all of the following components:

- Brio Portall 7.0.5
- BrioONE (Brio Portal 7.0.5 or later and the OnDemand Server 6.6.4 or later)
- Brio Intelligence Server 6.6.4 (OnDemand Server 6.6.4 or later and Broadcast Server 6.6.4 or later)
- Hyperion Analyzer 6.5, 7.0.1, 7.2, 7.2.1
- Hyperion Performance Suite 8.x
- Hyperion Reports 7.0.x, or 7.2.x

After you validate the migration, you need to perform post-migration steps to ensure proper functionality of yourReporting and Analysis system. The various components should function with the same level of effectiveness in your new environment as they do in your existing system.

Validating Brio Portal Migration

Use Table 18 as a checklist to confirm that all required Brio Portal components and objects have correctly migrated to the new Reporting and Analysis environment.

Table 18 Portal Migration ChecklistBrio

	Brio Portal Component	Explanation
❑	**Users**	All users and user attributes are migrated to the new environment. See "Mapping Access Privileges to Reporting and Analysis" on page 32 for information on role mapping.
❑	**Groups**	All groups and group attributes are migrated to the new environment. See "Mapping Access Privileges to Reporting and Analysis" on page 32 for information on role mapping.
❑	**Folders**	All the folders defined in the system are migrated to the new environment.
❑	**Documents and links**	Documents and links in the source system are migrated without any issues of access. (See "Mapping Access Privileges to Reporting and Analysis" on page 32.)
❑	**File system for Repository**	The file system for the Repository is migrated.
❑	**Generic job properties**	All available scenarios are migrated. This is job dependent.
❑	**Job runs in Reporting and Analysis**	Migrated jobs run without errors. In cases where the job uses a SmartForm, revert to the default and make sure the job runs with this default HTML form. You must recreate the SmartForm inReporting and Analysis for it to work.
❑	**MIME types**	All MIME types are migrated to the new environment. MIME types associated with each job should also be migrated. Note: If you have one file extension (.txt for example) associated with multiple custom MIME types (A, B, C, and D for example) in the source system, and A is a supported MIME type in Reporting and Analysis, the MIME types migrate as follows: MIME types A, B, C, and D are merged into the supported Reporting and Analysis MIME type. After migration, the custom MIME types seem to have disappeared but they have actually been merged.
❑	**Object property settings and keywords**	Property settings of browsable and nonbrowsable objects are migrated. Keywords for objects in the source system should be migrated.
❑	**Parameter lists**	Parameter lists are migrated as public with the publishing mask (Access Control) set as it is in the source system.
❑	**Portal objects**	These Portal Objects are migrated: ● Broadcast messages ● Preconfigured Portal Pages ● Image bookmarks ● HTML files or job output displayed as Portal Objects ● Exceptions dashboards ● Bookmarks
❑	**Oracle's Hyperion® SQR® Production Reporting jobs**	You can run Production Reporting jobs without any problems using the default parameter form. You must recreate SmartForms in Reporting and Analysis.

❑	**Production Reporting job properties**	All properties are migrated, including: ● General properties: Name, description, owner, expiration (if available), group ● MIME Type, Secure Mode, Rating, Exception, Browse flag, Permissions, Background vs. Foreground, Prompt for database ● Ask properties ● Input properties ● INI file ● Include files ● Output properties: Auto delete, Object time to live, Make output displayable as embedded ● Permissions on job output ● Propagate permissions ● Production Reporting program ● Include files ● Output Formats ● HTML demand paging ● Custom output flags; for example –burst ● Database username/password, command line flags, Run using (data source + Production Reporting version) ● Compile now ● Form -Files required by SmartForm (The form itself must be modified to work in the target environment). ● Advanced options ● Show parameter lists when running job Show save as default
❑	**Subscriptions**	User subscriptions are migrated to the new environment.
❑	**Time events**	Time events are migrated to the new system as public or personal recurring time events.

Note:

After you complete the migration, you must recompile all your Production Reporting jobs. After you recompile the Production Reporting jobs, they should work in the target environment with code changes. Exceptions would include programs that use deprecated Oracle's Hyperion® SQR® Production Reporting commands. Refer to Volume 2 in the *SQR Production Reporting Developer's Guide* for information on deprecated commands.

Validating Access Control on Job Output Runs

The way in which access control on job output is granted varies from Brio Portal v7.x to Reporting and Analysis. In Brio Portal, the group to which access is granted on job output may vary depending on which user runs the job. Because access control on a single job's output can

vary depending on who ran the job in the source system, the way in which the Migration Utility applies access control on job output run in Reporting and Analysis may vary as well.

Use the `jobPublishingMasksCreated.xml` file, located in the same directory as the Migration Utility, to verify that the proper access control is given to job output run in Reporting and Analysis. This XML file lists the access control information for the job output of each job migrated to the new system.

Note:

The syntax of XML (Extensible Markup Language) requires that each element have an opening tag <element tag> and closing tag </element tag>. XML elements are nested to create a hierarchy of elements.

Table 19 defines the tags used in the `jobPublishingMasksCreated.xml`file. Refer to `Sample JobPublishingMasksCreated.xml` following this table to view the format of the `jobPublishingMasksCreated.xml` file.

Table 19 `jobPublishingMasksCreated.xml` **Tag Definitions**

Tag	Definition
<JOBMASKS>	Begins the document. The closing tag </JOBMASKS> appears at the end of the document.
<JOB>	Begins a specific job. The closing tag </JOB> ends each job.
<JOBNAME>	Specifies the job name.
<PATH>	Specifies the location of the job in Browse module.
<JOBPUBLISHINGMASK defined='true/false'>	Specifies whether the administrator defined a publishing mask for this job in the source system. If defined=TRUE, the Migration Utility used the publishing mask specified in the old system. If defined=FALSE, the Migration Utility used the publishing mask of the user who runs the job. In the latter case, an additional list of elements is included for your information: <GROUPREAD> <GROUPWRITE> <GROUPEXECUTE> <WORLDREAD> <WORLDWRITE> <WORLDEXECUTE> These elements can have a value of 1 or 0, where 1 indicates that access is granted and 0 indicates that access is denied. Notice the difference between the two jobs in `Sample JobPublishingMasksCreated.xml`. The second job, job2, has a specified job publishing mask—the element is defined as TRUE, so these extra elements are included.
<JOBPUBLISHING- MASKACCESSORS>	Begins the list of users and groups that can access the job output in Reporting and Analysis. It includes the following sub-elements: <ACCESSOR> and <ROLE>, where

Tag	Definition
	<ACCESSOR> specifies a user or group that has access on the job output in Reporting and Analysis, and <ROLE> specifies the access privilege the preceding accessor has on the job output. In the following example the user ADMINISTRATOR and world group have Modify access privilege on the job output: <PUBLISHINGMASKACCESSORS> <ACCESSOR>ADMINISTRATOR</ACCESSOR> <ROLE>MODIFY</ROLE> <ACCESSOR>world</ACCESSOR <ROLE>MODIFY</ROLE> </PUBLISHINGMASKACCESSORS> Note the first accessor listed, which may be the accessor created from the default group. The Migration Utility chooses the default group of the job owner. However, the group the utility chooses may not match the one to which you want to assign default access in the new system, so modify the access as necessary. In the case of external authentication with externally managed groups, this default group may not exist.
<DATEPUBLISHED>	Specifies the date the job was published.
<FOLDERGROUP>	Specifies the group associated with the permissions of the folder where the job output was published in the source system.
<FOLDERPERMISSIONS>	Begins the list of user and group permissions on the folder that contains the job in the source system. It includes the following sub-elements: <GROUPREAD> <GROUPWRITE> <GROUPEXECUTE> <WORLDREAD> <WORLDWRITE> <WORLDEXECUTE> These elements can have a value of 1 or 0, where 1 indicates that access is granted and 0 indicates that access is denied.
<JOBOWNER>	Indicates the owner of the job.
<JOBACCESSORS>	Begins the list of users and groups that can run the actual job in Reporting and Analysis. It includes the following sub-elements: <ACCESSOR> and <ROLE>, where <ACCESSOR> specifies a user or group that has access on the job in the target system, and <ROLE> specifies the access privilege the preceding accessor has on the job. In the following example the user administrator and the world group have Modify and Run access privilege on the job: <JOBACCESSORS> <ACCESSOR>ADMINISTRATOR</ACCESSOR> <ROLE>MODIFY AND RUN</ROLE> <ACCESSOR>world</ACCESSOR> <ROLE>MODIFY AND RUN</ROLE>

Tag	Definition
	</JOBACCESSORS>
<JOBUUID>	Indicates the UUID of the job. `Sample JobPublishingMasksCreated.xml` includes only two jobs: one job with a specified publishing mask and a second job without a specified publishing mask.

Sample JobPublishingMasksCreated.xml

```
<JOBMASKS>
<JOB>
<JOBNAME>job1</JOBNAME>
<PATH>/genericjobs/</PATH>
<JOBPUBLISHINGMASK defined='false'>
</JOBPUBLISHINGMASK>
      <PUBLISHINGMASKACCESSORS>

          <ACCESSOR>ADMINISTRATOR</ACCESSOR>
          <ROLE>MODIFY</GROUP>
          <ACCESSOR>world</ACCESSOR>
          <ROLE>MODIFY</GROUP>

      </PUBLISHINGMASKACCESSORS>
      <DATEPUBLISHED>2003-01-14 14:29:18.0</DATEPUBLISHED>
      <FOLDERGROUP>ADMINISTRATOR</FOLDERGROUP>

      <FOLDERPERMISSIONS>
          <GROUPREAD>1</GROUPREAD>
          <GROUPWRITE>1</GROUPWRITE>
          <GROUPEXECUTE>1</GROUPEXECUTE>
          <WORLDREAD>1</WORLDREAD>
          <WORLDWRITE>1</WORLDWRITE>
          <WORLDEXECUTE>1</WORLDEXECUTE>

      </FOLDERPERMISSIONS>
      <JOBOWNER>administrator</JOBOWNER>
      <JOBACCESSORS>

       <ACCESSOR>ADMINISTRATOR</ACCESSOR>
         <ROLE>MODIFY AND RUN</ROLE>
         <ACCESSOR>world</ACCESSOR>
         <ROLE>MODIFY AND RUN</ROLE>

      </JOBACCESSORS>

      <JOBUUID>F0RFYLF0ENFHCCFIECDLDRRP_ZhinZr-CRRP_EHINER</JOBUUID>
 </JOB>
<JOB>

      <JOBNAME>job2</JOBNAME>
      <PATH>/SampleContent/Human_Resources/Employees/</PATH>
      <JOBPUBLISHINGMASK defined='true'>

          <GROUPREAD>1</GROUPREAD>
          <GROUPWRITE>1</GROUPWRITE>
```

```
            <GROUPEXECUTE>1</GROUPEXECUTE>
            <WORLDREAD>1</WORLDREAD>
            <WORLDWRITE>1</WORLDWRITE>
            <WORLDEXECUTE>1</WORLDEXECUTE>

        </JOBPUBLISHINGMASK>

        <PUBLISHINGMASKACCESSORS>
            <ACCESSOR>BrioPortal_Demo</ACCESSOR>
            <ROLE>MODIFY</ROLE>
            <ACCESSOR>world</ACCESSOR>
            <ROLE>MODIFY</ROLE>

        </PUBLISHINGMASKACCESSORS>
        <DATEPUBLISHED>2003-01-13 14:54:36.0</DATEPUBLISHED>
        <FOLDERGROUP>BrioPortal_Demo</FOLDERGROUP>
        <FOLDERPERMISSIONS>

            <GROUPREAD>1</GROUPREAD>
            <GROUPWRITE>1</GROUPWRITE>
            <GROUPEXECUTE>1</GROUPEXECUTE>
            <WORLDREAD>1</WORLDREAD>
            <WORLDWRITE>1</WORLDWRITE>
            <WORLDEXECUTE>1</WORLDEXECUTE>

        </FOLDERPERMISSIONS>
        <JOBOWNER>briouser</JOBOWNER>
        <JOBACCESSORS>

           <ACCESSOR>BrioPortal_Demo</ACCESSOR>

           <ROLE>RUN</ROLE>
        </JOBACCESSORS>
        <JOBUUID>MMHREMPID0101</JOBUUID>

 </JOB>
</JOBMASKS>
```

Validating Brio Intelligence Migration

Brio Intelligence has two components, the OnDemand Server and the Broadcast Server. Each component has its own repository database and associated documents. The OnDemand Server can run as a standalone component or as a Brio Portal service. When the OnDemand Server is run as a Brio Portal service, the users, groups, and folders are part of the Brio Portal Repository.

Review the following sections for information on:

- Validating OnDemand Server (ODS) Migration
- Validating Broadcast Server (BCS) Migration

Validating OnDemand Server (ODS) Migration

Use the checklist in Table 20 to confirm that all required OnDemand Server components and objects have correctly migrated to the new Reporting and Analysis environment.

Table 20 OnDemand Server Migration Checklist

ODS Component		Explanation
❑	**Users**	If you migrated ODS as a stand-alone component, users are migrated. If you did not migrate ODS as a stand-alone component (for BrioONE), the Brio Portal migration should have migrated the users. Inactive users and users using external authentication are not migrated. Check that the user attributes of users using external authentication migrated.
❑	**Groups**	If you migrated ODS as a stand-alone component, groups are migrated. If you did not migrate ODS as a stand-alone component (for BrioONE), the Migration Utility should have migrated the groups. Inactive groups are migrated as active groups.
❑	**Group attributes**	Group attributes are migrated. See "Mapping Access Privileges to Reporting and Analysis" on page 32 for assigned group attributes.
❑	**Adaptive States**	Adaptive states for the documents are migrated to the new system.
❑	**Documents**	All BQY documents in the source system are migrated except those using password protection. The Migration Utility does not change OCE settings for BQY job output. BQY documents with mixed passthrough are migrated as two BQY documents, one with Passthrough mode and the other with No Passthrough mode.
❑	**Folders**	If you migrated ODS as a stand-alone component, all folders are moved to the target system. (Categories are called folders in Reporting and Analysis.). If you did not migrate ODS as a stand-alone component (for BrioONE), the Brio Portal migration should have migrated the folders.
❑	**Job output**	Migrated BQY job output registered to ODS is treated as BQY documents in Reporting and Analysis. If multiple outputs are associated with a job, they display in the main browse page as individual BQY documents rather than as job output beneath the related job. You can delete the job output in the form of BQY documents after new job output generates.
❑	**OCEs**	OCE files are migrated to the new system. All processing OCEs should be moved from the ODS repository to the Reporting and Analysis Repository in the OCE category designated in the Migration Utility .
❑	**ODS documents**	BQY documents migrated from the OnDemand Server can be processed with the plug-in.
❑	**Row-level security**	If you migrated row-level security definitions, your tables are populated.
❑	**Section OCE mapping**	Existing ODS queries are still associated with the proper OCEs through the Browse module or Production Reporting Job Publisher.
❑	**User name and password inside OCEs**	The BQY files can connect using their designated OCEs. Attempt a test connection with a BQY file.

Validating Broadcast Server (BCS) Migration

Use the checklist in Table 21 to confirm that all required Broadcast Server components and objects have correctly migrated to the new Reporting and Analysisenvironment.

Table 21 Broadcast Server Migration Checklist

BCS Component		Explanation
❑	**Users**	All active users are migrated. Inactive users are not migrated.
❑	**Groups**	Optionally migrate groups. If groups had a conflict in ODS, a warning should have been generated when running in pre-migration test mode. You should perform an additional pre-migration Test run after you resolve the conflict.
❑	**Group/User attributes**	See "Mapping Access Privileges to Reporting and Analysis" on page 32 for assigned group and user attributes.
❑	**BCS jobs**	Scheduled BCS jobs are migrated without any issues and can be scheduled in the new environment without problems.
❑	**Calendars**	Calendar definitions in BCS are migrated to the new environment.
❑	**Directories and printers**	Directories and printers have the correct paths set up in your operating system. Groups that have access to directories and printers in the source system have view access to those same directories and printers in Reporting and Analysis. **Note**: The version 8 server services need to run using a domain account that has access to migrated output directories and printers.
❑	**External events**	External events are migrated to the new environment.
❑	**Jobs**	Jobs defined in BCS are migrated to the new environment.
❑	**Job cycles**	All cycles associated with a job are migrated.
❑	**Job intervals (three different levels)**	Jobs scheduled to run regularly in the source system map to recurring time events in Reporting and Analysis. Jobs scheduled to run ASAP in the source system do not map to a specified time event in Reporting and Analysis. Jobs scheduled against events in the source system map to externally triggered events in Reporting and Analysis.
❑	**Location of output files**	Output files should be in a directory, printed, or saved to the Repository.
❑	**OCEs**	All processing OCEs are moved from the BCS to the Repository in the OCE category designated in the Migration Utility. All migrated BCS OCEs have _bcs appended to their names. For example, a BCS OCE called Processing OCE in your source system is called Processing OCE_BCS in yourReporting and Analysis system.
❑	**Parameter lists**	Parameter lists are migrated as personal.
❑	**Section OCE mapping**	Scheduled BQY jobs have each query mapped to an OCE.

Validating Hyperion Analyzer Migration

Use the checklist in Table 22 to confirm that all required Hyperion Analyzer components and objects have correctly migrated to the new Reporting and Analysis environment.

Table 22 Hyperion Analyzer Migration Checklist

Analyzer Component		Explanation
❑	**Users**	All active users are migrated. Inactive users are not migrated.
❑	**Groups**	All groups are migrated.
❑	**Group/User attributes**	See "Mapping Access Privileges to Reporting and Analysis" on page 32 for assigned group and user attributes.
❑	**Database Connections**	All database connections are listed and are available to the reports and views.
❑	**Personal Variables**	Personal variables for the users are migrated.
❑	**Reports**	All reports can be run and edited.
❑	**Report Views**	All reports and controls work for Report Views.
❑	**Report Group Templates**	All reports are available to the Report Group. Links and URLs are available in the Report View.

Validating Hyperion Reports Migration

Use the checklist in Table 23 to confirm that all required Hyperion Reports components and objects have correctly migrated to the new Reporting and Analysis environment.

Table 23 Hyperion Reports Migration Checklist

Reports Component		Explanation
❑	**Users**	All active users are migrated. Inactive users are not migrated.
❑	**Groups**	All groups are migrated. If errors arise the group will not migrate. You should perform an additional pre-migration Test run after you resolve the conflict.
❑	**Group/User attributes**	See "Mapping Access Privileges to Reporting and Analysis" on page 32 for assigned group and user attributes.
❑	**Batches**	Can be scheduled and run appear in email, PDF, or the repository.
❑	**Books**	All the reports in the book are migrated and books can be run in either PDF or HTML mode.
❑	**Database Connections**	All database connections are migrated.
❑	**Reports**	Reports can be run in either PDF or HTML mode.
❑	**Reports/Snapshots**	All reports and snapshots are migrated.

❑	**Row/Column Templates**	Row/Column templates are migrated and are added to the correct reports.

Validating Hyperion Performance Suite Migration

Use the checklist in Table 24 to confirm that Hyperion Performance Suite 8.x information has correctly migrated to the new Reporting and Analysis environment.

Table 24 Hyperion Performance Suite Migration Checklist

Hyperion Performance Suite Component		Explanation
❑	**Users**	All active users are migrated. Inactive users are not migrated. (Active users must have their action set to *migrate* in the Migration Utility. See "Setting the Migration Action" in the *Hyperion Reporting and Analysis Migration Utility Guide* for information on how to set the migration action for users.) User properties (first name, last name, description, email address) are correct for users mapped to new native users. Users are provisioned with the correct roles.
❑	**Groups**	All active groups are migrated. Inactive groups are not migrated. (Active groups must have their action set to *migrate* in the Migration Utility. See "Setting the Migration Action" in the *Hyperion Reporting and Analysis Migration Utility Guide* for information on how to set the migration action for groups.) Group descriptions and user/group membership is correct for groups mapped to new native groups. Groups are provisioned with the correct roles.
❑	**User Defined Roles**	User-defined roles must be manually created and manually assigned to users and groups.
❑	**Repository Metadata**	All repository metadata migrated to the new environment.
❑	**Repository Files**	The content of the system, folders, and files migrated to the new environment.
❑	**Events**	User subscriptions, notifications of events involving subscriptions, jobs, parameter lists for jobs, and exceptions migrated to the new environment.
❑	**Authorization**	Access control information for folders, documents, and resources is migrated correctly.

General Post Migration Steps

After you complete the migration, perform the tasks described in Table 25 to ensure proper functionality in your newReporting and Analysis system.

Table 25 Post-migration Checklist

Task	Explanation

❑	**Enable publisher ratings for migrated Brio Portal jobs**	Ratings are migrated, but they cannot be seen unless the Enable publisher ratings parameter is set in the Reporting and Analysis system properties.
❑	**Review access control**	Set access control on users, groups, and other resources according to your migration plan. Make sure to assign the Content Publisher role to any user who needs to view, modify, or publish in Reporting and Analysis. Check that the proper access control is given on job output. Use the `jobPublishingMasksCreated.xml` file produced by the Migration Utility to check that the proper access control is set on job output in the new system. See Example for a sample file.
❑	**Modify the default Insight role**	If you set a default Insight role in the BI_Migrate.ini file during migration, modify the Insight role to reflect the roles you want to give to users and groups in your new system. It is recommended that you apply roles at the group level instead of the user level.
❑	**Set up email for jobs**	If you did not convert MAPI email addresses to SMTP addresses before migrating, you must do so now. MAPI email addresses are not supported in Reporting and Analysis. You may need to set up an email server if you did not do so while installing Reporting and Analysis.
❑	**Set OCE attributes**	Give appropriate access control to users who need to view, modify, and or publish OCEs. See "Mapping Access Privileges to Reporting and Analysis" on page 32 for detail on ownership of migrated OCEs. Because alternate metadata OCEs are not migrated, reestablish the links to alternate metadata OCEs.
❑	**Turn on RLS**	If you migrated Row Level Security (RLS), you must manually turn it on in your new system.

A Sample Migration Project Plan

In This Appendix

Identifying Tasks and Deliverables

Table 26 details the various tasks and identifies deliverables, along with the associated responsibility for a typical migration project. The Target Schedule is an estimate that may change based on information obtained during the initial requirements and analysis phases of the project or during the migration assessment phase as deemed necessary by the Migration Project Team.

Table 26 Sample Migration Project Plan

Project Phase	Milestone Tasks and Deliverables	Responsibility	Target Schedule
Migration Planning	Gain a clear understanding of new features and functionality of Reporting and Analysis; identify and gather resources, information, and material required for aReporting and Analysis migration project; and introduce the project to key stakeholders. Tasks performed include: ● Understand the new features and functionalities of Reporting and Analysis. ● Gather business requirements. ● Review business requirements and confirm project objectives, scope, and schedules. ● Assemble project team, assign roles & responsibilities. ● Identify resource requirements related to consulting services. ● Identify training needs related to Reporting and Analysisand/or the migration process.	Customer 100%	Customer dependent - ongoing

Project Phase	Milestone Tasks and Deliverables	Responsibility	Target Schedule
Migration Assessment and Design	Gather information about the existing environment and future business intelligence needs. Tasks performed include: ● Review of the customers in the existing environment ● Requirements gathering related to customer's future business intelligence needs ● Technical architecture analysis ● Hardware and software requirements ● Production Server inventory – identify content to migrate ● Server load analysis ● Server outage analysis ● Migration project plan ● Identification of customer's training needs ● Deliverables at this point should include: ● Complete existing environment Assessment document ● Complete migration project plan	Customer 50% Local Consulting Resource (1 FTE) 50%	1 – 2 weeks
Migration	Perform migration from the existing environment to the new Reporting and Analysis environment. Tasks performed include: ● Setting up a test environment ● Migrating in pre-migration mode ● Testing the migration ● Evaluating test results ● Resetting the test server to the original system ● Testing the migration again ● Performing the production migration ● Performing the post migration manual steps/customizations	Customer 50% Local Consulting Resource (1 FTE) 50%	2 – 4 weeks
Post Migration Content Development	Develop new content to utilize the new Reporting and Analysis features and functionality. Tasks include: ● Develop dashboards, Intelligence documents, and SQR reports	Customer 50% Local Consulting Resource (1 FTE) 50%	Customer dependent – ongoing

Project Phase	Milestone Tasks and Deliverables	Responsibility	Target Schedule
	• Configure security • Develop content related to thin client		

Identifying Project Staff

Table 27 suggests what to consider as you put together a migration project staff. On the migration staff, include people who meet the following criteria:

Table 27 Project Staff

Staff Position	Description
System administrator	Possesses detailed knowledge of the operating environment and configuration details of existing systems and has authorized access to all relevant systems at your site. Responsible for ensuring that the environment is properly secured and backed up and that adequate restoration procedures are in place when required. Can provide the project team with the appropriate access and security levels
IT specialist	Possesses detailed knowledge of the following IT technology and configuration details of existing systems and has authorized access to all relevant supporting service at your site. • Web server • Database system • Network • Java • Lightweight Directory Access Protocol (LDAP)/ADS
Business analysis	Understands the organization's business requirements and can translate these requirements to a generic solution that can be delivered using IT. Has detailed knowledge of the business operating environment and of the problem to be addressed.
Project manager	Has overall project management responsibility for ensuring the successful use of both internal and Hyperion resources.
Hyperion project specialist	Understands how the ODS, BCS, Intelligence Client, Portal, Reports, Analyzer, and HPSu 8.x documents are used, the business functions they serve, and the customizations that have been implemented.
Database/application specialist	Possesses skills and knowledge of the existing client systems and complimentary products to integrate into the Hyperion implementation. These may be products such as: RDBMS, proprietary client systems, desktop applications, and others.
Consultant support	Provides detailed Hyperion product expertise, domain expertise, and experience associated with multiple previous implementations of the Hyperion product set. Typically works as an integral member of the project team to ensure that Hyperion products are successfully deployed in line with an agreed plan to meet the business needs. If required, the consultant or an associate serves as a business consultant to translate the needs of the client from a business problem to a Hyperion solution based on vertical market and vertical application experience.

Breaking Down the Workload

Table 28 depicts a breakdown of workload for each resource for the major phases of the migration project.

Table 28 Workload Breakdown

Estimated Workloads During the Project	Migration Planning (ongoing)	Migration Assessment (1 to 2 weeks)	Migration (2 to 4 weeks)	On-going Production
Project Manager	50%	50%	25%	0%
IT Specialist	25%	50%	25%	20 - 25%
System Administrator	25%	50%	25%	25%
Business Analyst	25%	25%	50%	25%
Brio/Hyperion Project Specialists	25%	50%	25%	0%
Database Administrator	5%	5%	20%	5%
Consultant	0%	100%	100%	0%

B Limitations

In This Appendix

About Limitations

This appendix discusses functionality that was present in prior versions that has no equivalent method in Reporting and Analysis.

General

Table 29 describes the general limitations as a result of migrating to Reporting and Analysis.

Table 29 General

Limitation	System Affected	Workaround
• **No password migration from native authentication systems** Unlike the previous Migration Utility, passwords will not be migrated for native authentication systems. Instead they will be set to a default or randomly-generated password depending on the configurable setting in the Migration Utility. The password algorithm for Shared Services is not the same as in the prior versions (Reports, Analyzer, HPSU etc.). As a result, the encrypted passwords from the previous version are not readable by the new native authentication system; namely, OpenLDAP.	Native authentication systems in previous versions	Map users to an external provider. **Note**: Deployments that wish to continue with a native authentication system can choose to randomly generate passwords to be stored in a password file. Users must then be notified about the new passwords. A sample program is provided with the Migration Utility that reads the password file and sends out notifications to affected users. Based on the sample, administrators can use any language to create their own program.
• **No administration API for user provisioning**	Hyperion Analyzer, Hyperion Reports, or Hyperion Performance Suite	None at present.

Limitation	System Affected	Workaround
In Reporting and Analysis, APIs are not supported in which users are created in the new User Provisioning module using API calls from the Hyperion Performance Suite SDK. Additionally creation of groups and provisioning of users/groups is not allowed.		

Hyperion Analyzer

Table 30 describes the limitations encountered when migrating Hyperion Analyzer to Reporting and Analysis.

Table 30 Hyperion Analyzer

Limitation	System Affected	Workaround
• **No support for links in EPM Workspace** Similar to UNIX symbolic links. A link is pointer to an object that represents the object based on the link's location in the repository. Links are associated to the object by the objects ID and URL.	Hyperion Analyzer 7.2	None
• **No "batteries included" repository (MySQL)** Prior versions of Hyperion Analyzer were shipped with MySQL for the repository. This is not true for Reporting and Analysis.	Hyperion Analyzer 7.2	None
• **Removal of Granular Roles** Hyperion Analyzer 7.2 had granular roles for POV and PV separately. In Reporting and Analysis, the granular roles are now one role.	Hyperion Analyzer 7.2	None
• **Opening a presentation is different between EPM Workspace and Studio** Opening a "presentation" does not open the first report with direct access to others via Tabs.	Hyperion Analyzer 7.0.1 and 7.2	None
• **Desktop functionality between Analyzer 6/7.x HTML Web Client and EPM Workspace is different** The EPM Workspace desktop display is different from the Hyperion Analyzer Web Client and the Web Analysis Studio.	Hyperion Analyzer 6.x and 7.x	None
• **No tag library (token) or action support to customize Hyperion Analyzer HTML Web Client** There is no longer a tab library or URL actions.	Hyperion Analyzer 6.x and 7.x	None
• **No Web Publish or Batch Utility to save reports as HTML** Web publish saves a report to HTML output and batch utility can do the same for more that one report.	Hyperion Analyzer 6.x and 7.x	None
• **Analyzer Standalone Windows client no longer exists** There is no longer a Windows client.	Hyperion Analyzer 6.x and 7.x	None

Limitation	System Affected	Workaround
• **Startup options and default folder locations different between Studio and EPM Workspace** The startup options that are applied in Web Analysis Studio are no longer applicable to the thin client (EPM Workspace).	Hyperion Analyzer 6.x and 7.x	None
• **No ARU/XML to create or modify users** Customers can no longer create and manage users with an import XML file.	Hyperion Analyzer 6.x and 7.x	None
• **Cannot backup/restore RDBMS repository. Requires file system backup** In past releases you had to backup the RDBMS database in order to backup Analyzer's repository.	Hyperion Analyzer 6.x and 7.x	None
• **Permissions no longer supported** In Hyperion Analyzer 7.x, it was possible to assign users and groups discrete permissions for objects. For example, you could assign the Write permission to a user without assigning the Read permission. In Reporting and Analysis, the permissions are cumulative. For example, the Modify permission includes the View permission. Thus, if a user was assigned just the Write permission for an object in Hyperion Analyzer 7.x, in Reporting and Analysis they user will also be able to view the object. For migrated systems, this is a difference in behavior. In addition, you can no longer bypass intermediate folders to access lower level folders. You must give explicit permission on the intermediate folders to have access to the lower level folders.	Hyperion Analyzer 7.x	None

Hyperion Reports

Table 31 describes the limitations encountered when migrating Hyperion Reports to Reporting and Analysis.

Table 31 Hyperion Reports

Limitation	System Affected	Workaround
• **Cannot copy and paste files (including reports) or folders in the Repository** In previous releases, you could copy and paste reports objects in the Repository, both in the Win32 client and in the Web client (version7.2 and above).	All previous versions of Hyperion Reports	**Reports**: Open a Report in the Win32 client and select **File**, then **Save As**. **Books and Batches**: Open Book or Batch in EPM Workspace and select **File**, then **Save As**.
• **Removal of Win32 Client Repository Maintenance functionality** The following areas of Repository Maintenance functionality no longer appear in the Win32 client:	All previous versions of Hyperion Reports This is a minor impact since most Win32 client functionality, except for Reports design, has moved to the thin client.	Perform Repository maintenance in EPM Workspace instead of in the Win32 client.

Limitation	System Affected	Workaround
❍ **Access Privilege Changes** Accessible in EPM Workspace only. ❍ **Copy, Cut, Paste, Delete, and Duplicate Objects** Accessible in EPM Workspace only, except for "Copy". ❍ **Ability to Create New Folder from File**, then S**ave or File**, then **Open dialog boxes** Accessible in EPM Workspace only.		
● **Removal of Admin menu from the Win32 client** Security maintenance and Hub registration have been removed from the Win32 client.	All previous versions of Hyperion Reports This is a minor impact since most Win32 client functionality, except for Reports design, has moved to the thin client.	Perform Security maintenance in EPM Workspace instead of in the Win32 client.
● **Email addresses configured in Shared Services and not in Preferences** You can still send email links as in the previous releases; however, you must configure the sender's email address in Shared Services and not in Preferences.	All previous versions of Hyperion Reports	Configure the sender's email addresses in Shared Services.
● **Multiple language support for the Repository not included in this release** Currently, Foundation does not provide multi-lingual support, in either the services or the servlets. Locales for each user are not stored, and the browser locale is not used. Currently, Reports supports multiple languages in the database/Repository. In other words, one Report can have a Japanese name and another report can have a Russian name, where both reports can exist in the same folder. This is accomplished by Reports encoding the Report Name (and other info like Description) in UTF-8 format before the object is stored in the database. This requirement is necessary where it is common to have different Reports saved in different languages in the same repository.	All previous versions of Hyperion Reports	None

Hyperion Performance Suite

Table 32 describes the limitations encountered when migrating Hyperion Performance Suite (Brio Intelligence, Brio Portal, and SQR) to Reporting and Analysis.

Table 32 Hyperion Performance Suite (Brio Intelligence, Brio Portal, and SQR)

Limitation	System Affected	Workaround
• **New content indicator discontinued** In previous versions, an icon indicated if a new object had been added to the system. The new user interface does not display an icon to notify users of new content.	Hyperion Performance Suite	Sort using the date and time column.
• **No Migration Utility platform support for HPUX/Linux** There is no platform support for HPUX/Linux.	Hyperion Performance Suite	Run the Migration Utility on a machine using a supported platform (such as Windows or Solaris).
• **Extended Services no longer supported** Extended Services will not function in Reporting and Analysis. In previous versions, this feature allowed partners, services, or customers to extend the capability of servlets and customize them to their environment.	Hyperion Performance Suite	None
• **Reporting and Analysis servlet hardwired to a single GSM** Every Web application deployment will be hardwired to a GSM. Users can no longer select a Web deployment and connect to a GSM of their choice. As a result, test and production deployments will have their own instances of application servers which cannot be used interchangeably.	Hyperion Performance Suite	None
• **Manual provisioning of groups in automatic mode** In previous versions, systems configured for automatic mode did not require manually provisioning of users or groups. In Reporting and Analysis, new groups must be manually provisioned. (You do not need to manually provision users in the group.)	Hyperion Performance Suite	A partial workaround is to provision the World group. All users are members of this group and can login. You must still individually provision groups.
• **No support for reporting usage tracking data by group** In Hyperion Performance Suite, you could create usage tracking reports to track events by named groups. Since group information is no longer part of Reporting and Analysis, the underlying views are no longer valid and will not include group information.	Hyperion Performance Suite	None

Limitation	System Affected	Workaround
• **No driver support of paging for Active Directory and LDAP** There is no longer any driver support for paging Active Directory and LDAP.	Hyperion Performance Suite	None
• **Selective provisioning of users in external groups is not allowed if the users is a member of a provisioned group** Shared Services currently has no functionality for selectively choosing which users to provision (equivalent to Hyperion Performance Suite manual import of users). If a group is provisioned, all users in the group are automatically provisioned.	Hyperion Performance Suite This an issue for migrated systems that are set up in manual mode since more users will have access after migration than before migration.	Provision users individually. Then during migration, map external groups to new native groups.
• **Copy user feature not available** In previous versions of Hyperion Performance Suite, the copy feature allowed administrators to easily create users with same the group and role information. By changing the basic properties like username and password from the copied user, you could create a new user with the same roles and group memberships. Administrators could also edit any of the roles or group information.	Hyperion Performance Suite	None
• **No support for tracking ancestor groups** In User Provisioning, there is no way to determine what groups a given group is a member of.	Hyperion Performance Suite	None
• **Cannot deactivate users, groups, and roles. You can only delete them.** When you deactivate groups and roles, it makes them unavailable for assignment to users, and they are not displayed in the access control screen for assigning permissions. The group and role association for re-activated users is retained.	Hyperion Performance Suite	None
• **Existing Smartforms do not work in Reporting and Analysis** Smartforms are parameter collection forms used by SQR programs. Due to the conversion of the relevant screens from templates to JSPs, the existing Smartforms will not work in the new environment.	Hyperion Performance Suite	Create new Smartforms using the new JSP template.

Limitation	System Affected	Workaround
Note: The Migration Utility removes the association of the Smartform and the SQR program. This ensures the default parameter collection screen is generated when you run the program post migration.		
• **No 508 compliance** Oracle Enterprise Performance Management Workspace, Fusion Edition will not be 508 compliant.	Hyperion Performance Suite	None
• **No option to open content in a new window without "framework"** Reporting and Analysis does not have an option to open content in a new window without "framework."	Hyperion Performance Suite	None
• **No circular group support** Circular references are groups that contain other groups in a cyclical relationship. For example, Group A contains Group B, which contains Group C, which contains Group A. The User Provisioning module does not support circular references in groups. Note: The Migration Utility removes any circular references in the source system before migrating content to Shared Services and the Reporting and Analysis Repository.	Hyperion Performance Suite	Remove circular group references prior to migration.
• **No grouping for job run outputs** Reporting and Analysis does not group job outputs along with the job name. The job outputs appear as separate entries using the fixed text "Output from..." before the job name. In previous versions, every job displayed the most current version of job output directly below the link for the job name. In Reporting and Analysis, when a job has more than one output type (for example, PDF or XML), you must click on the job output to select the output type. Previous versions did not have this additional screen for output selection.	Hyperion Performance Suite	None
• **No support for delegated administration** Delegated administration allows non-administrative users to be granted limited access to administration functionality.	Hyperion Performance Suite	None

Limitation	System Affected	Workaround
Delegated administration is implemented by applying access control on users, groups, and roles so that users with limited administrative capabilities can only access the users, groups, and roles as specified by the Administrator. Reporting and Analysis does not support access control on users, groups and roles.		
● **No database authentication driver support** Reporting and Analysis does not support database security as an external authentication source.	Hyperion Performance Suite	None
● **Cannot specify default user roles** Previous versions of Hyperion Performance Suite allowed an administrator to assign roles to the WORLD group. These roles were then granted to all users who had access to Hyperion Performance Suite. For example, you could set up your system to manually import users, and all users imported would automatically inherit the roles assigned to the WORLD group. In Reporting and Analysis, however, provisioning the WORLD group gives all users access to Reporting and Analysis. As a result, provisioning of the WORLD group may not be desirable.	Hyperion Performance Suite	● Create a group for allReporting and Analysis users. Always add new users to this group and assign them default roles. ● The Migration Utility includes a special group to which all migrated users and groups belong to. This group is assigned the roles assigned to the WORLD group. New users or groups added after migration must be added explicitly to this group, in order for them to be granted these default roles.
● **Cannot change role containment relationships for pre-defined roles** Pervious versions of Hyperion Performance Suite allowed you to modify role containment for pre-defined roles. Changes in role containment relationships are not migrated and cannot be changed after migration.	Hyperion Performance Suite	None
● **User-defined roles not migrated** The Migration Utility does not migrate user-defined roles.	Hyperion Performance Suite	Create user-defined roles in Reporting and Analysis and assign permissions for these roles accordingly.
● **No support for custom authentication drivers** Hyperion Performance Suite provided APIs to create custom authentication drivers. Reporting and Analysis does not provide these APIs.	Hyperion Performance Suite	None

Limitation	System Affected	Workaround
• **No support for NIS drivers** Hyperion Performance Suite supported NIS drivers for external authentication. Reporting and Analysis does not support these drivers.	Hyperion Performance Suite	Use supported external providers or native drivers for OpenLDAP.
• **Primary group no longer retrieved for MSAD users** The Hyperion Performance Suite MSAD Authentication Driver returned a user's primary group. The Oracle's Hyperion® Shared Services driver does not return the primary group. This may affect existing roles and access level.	Hyperion Performance Suite	None

Carry Forward from Hyperion Performance Suite 8.3

Table 33 describes the limitations carried forward from Hyperion Performance Suite 8.3.

Table 33 Carry Forward from Hyperion Performance Suite 8.3

Limitation	System Affected	Workaround
• **Cannot publish password-protected BQY files** You can no longer password protect BQY files.	Brio Intelligence 6.x	Remove password protection before publishing.
• **Cannot have cascading limit values in scheduled jobs** The job limits screen in Hyperion Performance Suite and Reporting and Analysis does not allow users to provide cascading limits even if they are defined in the BQY document. Example: Show cities based on State selected. If limit 1 is State, and you select California, the available choices for limit 2 should be the cities of California such as San Francisco, Los Angeles etc.	Brio Intelligence 6.x	None
• **No job support for MAPI/Exchange as a mail server** The MAPI/Exchange server is not supported for sending emails from the Job Service. Currently, only SMTP/ASMTP servers are supported.	Brio Intelligence 6.x	None
• **Broadcast Server Customized Limit prompts do not appear**	Brio Intelligence 6.x	None

Limitation	System Affected	Workaround
When a filter (limit) is customized, setting the value of the filter as a job parameter does not honor the customizations. For example, if you set a filter to not be ignored, to not include nulls, or to only pick from the values in the database, these restrictions would still be permitted when specifying job parameters.		
● **Cannot create and test OCEs directly on a UNIX server platform** Without a UNIX “fat client”, you cannot create an OCE on a UNIX platform and test connectivity. In Reporting and Analysis , you must create the OCE on a Windows platform, where a connection with the same data source name exists; publish the resulting OCE; and run a job with a UNIX-deployed DAS to verify it works.	Brio Intelligence 6.x	None
● **No equivalent of 6x ODS System Monitor/ Active Users screen to allows shutdown of processes** The OnDemand Server provided a screen to monitor active processes. Portal 7.x had a utility to see the active users in the system. Reporting and Analysis does not provide an equivalent method.	Brio Intelligence 6.x and Brio Portal 7.x	None
● **Web publishing/job scheduling in Oracle's Hyperion Reporting and Analysis not possible from Designer** The Designer client in 6.x allowed scheduling without connecting to the Web. This functionality was lost in the move to Hyperion Performance Suite.	Brio Intelligence 6.x	None
● **Cannot add HTML links in an object’s description field** It used to be possible to add HTML links in the description field using the HTML tags the documents published in the server.	Brio Portal 7.x	None
● **When assigning roles and groups for Insight users, the jump between Intelligence Dynamic Viewer and Intelligence Analyzer is too severe**. This is a result of the inability to assign a default adaptive state to a group.	Brio Intelligence 6.x	None
● **Cannot filter search results by mime type**	Brio Portal 7.x	None

Limitation	System Affected	Workaround
You can no longer use mime types to perform a search.		

Index

U

V

W