Sterling Integrator®

Pre-Upgrade Analysis

Version 5.1

Sterling Commerce

An IBM Company

Contents

Pre-Upgrade Analysis Overview

Upgrade Risk Factor Review

This chapter provides information on how to conduct your pre-upgrade risk factor analysis prior to upgrading your system from 3.x, 4.x, or 5.0 to Sterling Integrator 5.1. By completing the analysis, you should be able to complete your upgrade within your allotted maintenance window and have fewer areas to troubleshoot upon completion.

If you do not review and address the risk factors identified in this documentation:

- Your system may not function properly
- Your system may function in a sub-optimal manner
- You could potentially lose or corrupt data

Prerequisite Knowledge for an Upgrade

Before you begin the upgrade, you should be knowledgeable on the following topics and documents:

- Application servers
- Database structure in general
- Operating Systems in general
- UNIX Operating System
- VI or another text editor

Before you begin the upgrade, you should be come familiar with the following documents:

- System Requirements
- Preupgrade Analysis Guide
- Upgrade Guide
- Release Notes

Assumptions for Upgrades

The procedures represented in this document are accurate as of the publication date. The document is intended to be used by system administrators and software installation personnel who have previously installed and administered the Sterling Integrator application.

Pre-Upgrade Analysis Checklist

5.1 Upgrade Risk Factor Analysis Checklist

Use this check list to keep track of the risk factors you need to review prior to upgrading to 5.1.

Check after completed	Upgrade Risk Factors Analysis Checklist	Risk Detection Completed	Recommendation Applied/Notes
	Archiving: System has file system archive exports		
	Business process: Hard coded environment-specific configurations		
	Business process: Environment-specific deployment		
	Business process: Customer modifications to out-of-box business processes		
	Business process: Schema changes		
	Business process: Sub-process service calls vulnerable to infinite loops		
	Business process: Meta data service		
	Business process: Lax XPath syntax		
	Business process: Unsupported BPML parameters		
	Business process: Unsupported Xpath statements		
	Database Schema: Identified tables, views, triggers, indexes, constraints or store procedure that are not part of the core product		
	Document Envelope: Deprecated envelope parameters		
	Document Envelope: Required envelope parameters are not used		
	Document Envelope: Generate from Data Option		
	External Programs: Custom archiving		
	Map: User Exits		
	Map: Non-existent pools in JDBC maps		

Check after completed	Upgrade Risk Factors Analysis Checklist	Risk Detection Completed	Recommendation Applied/Notes
	Map: Inbound Map code list look up		
	Performance and Tuning: Performance tuning have been applied to the property files		
	Properties Files: Customer specific properties files		
	Properties Files: Deprecated property files are being used		
	Properties Files: enveloping.properties files has been updated to invoke a customized envelop business process		
	Properties Files: environment-specific properties file settings		
	Properties Files: Non-performance related properties in the properties files have been updated.		
	Scripts: Start up scripts have been modified.		
	Service and Adapter: Customer services or adapters		
	Service and Adapter: Customer modifications to out of the box Service Configurations		
	Service and Adapter: Environment specific adapter configurations		
	Trading Partner: PGP Profiles		
	Upgrade Roll-back: You do not have a copy of the file system or database which has been proven to restore reliably.		
	XSLT Adapter: Lax XPath Syntax		
	3rd Party Libraries: Unaccounted for 3rd party Library dependencies		

Upgrade Risk Factors

Archiving Risk Factors

Archiving risk factors are related to any archive or purge configurations or usages which cause problems when deployed to the upgraded system.

Archiving Risk Factors	**The system has file system archive exports**
Description	You have run the file system backups. Archive exports created by one version of the system are not restorable on other versions.
Detection Method	For each instance, • Determine if you are archiving business processes in your current instances by checking the archive directory location specified in the Archive Manager for files. • If the file exists, the files can not be restored in the upgraded instance.
Recommendation	Always leave an instance of the old version online for error research purposes. Disable all schedules and all listening server adapters in the old version (with the exception of the admin HTTP server adapter).

Business Process Risk Factors

Business Process risk factors are coding practices or check-in configurations which cause problems when deployed to the upgraded system.

Business Process Risk Factor	**Hard coded environment-specific configurations**
Description	Business Processes contain hard coded values which are only applicable to a specific instance (for example, test, production, or development). An example of a hard coded value could be a directory path which exists in a test environment, but not the production environment.

Detection Method	Search the Business Process BPML for Windows or UNIX Path strings.
Recommendation	Migrate references to directory paths into customer specific properties file and call that properties file from the business process.

Business Process Risk Factor	**Environment-specific deployment**
Description	The Business Processes deployed in each system are not identical. An example is a Business Process which is in development or test, but has not been moved to production.
Detection Method	• Create a list of all of the Business Processes in all of the instances. • Create a list of all instances for each Business process. • For each Business Process in the list, query the list for that Business Process for each instance.
Recommendation	Ensure that each environment's configurations are migrated like for like. For example, production moved to production and test moved to test.

Business Process Risk Factor	**Customer modifications to out-of-box Business Processes**
Description	The out-of-box Business Processes have been modified and no longer match what is shipped with the product software.
Detection Method	Identify out-of-box Business Processes being used in your implementation by doing one of the following: • Compare the active version of the Business Process to the Business Process of the same name in the installed_data directory which represents the out-of-box version. • Compare the active version of the Business Process to an earlier out-of-box version of the Business Process by accessing the Business Process through the Business Process Manager.
Recommendation	Compare the out-of-box Business Processes from your original system version to the out-of-box Business Process for 5.1. If they are the same, the modifications can be put back by changing the default Business Process version to the last version. The upgrade process does not delete the original modified version but it will no longer be the default version after the upgrade. If the out-of-box Business Process has changed, then the new Business Process and old Business Process will need to be compared to identify the differences. If the modifications are still applicable, you will need to integrate them into the new out-of-box Business Process or copy and rename the out-of-box Business Process and make the changes to the copy of the out-of-box Business Process and make any other changes necessary to use the copy.

Business Process Risk Factor	**Schema changes**
Description	Business Processes (through Lightweight JDBC Adapters or JDBC maps) access system tables which have been changed in higher versions.
Detection Method	• Find all of the SQL statements in your Business Processes, maps, Lightweight JDBC adapter configurations that access system tables. • Compare the SQL statements and the table schema from the original and target environments to determine if any modifications are necessary.

Recommendation	Never change system tables. Sterling Commerce strongly recommends not to access system tables in your SQL statements.

Business Process Risk Factor	**Sub-process service calls vulnerable to infinite loops**
Description	The implementation of invoke sub-process service causes an infinite loop.
Detection Method	In the Business Processes, find invoke sub-process services. Review to see if the Assign to and From * occurs sequentially before WFD_NAME.
Recommendation	Do one of the following: • In the Graphic Modeler (GPM) modify the Invoke Sub-Process call to Assign Process Data First, then Messages. • From the BPML, change the Invoke Sub-Process call to Assign Process Data First, then Messages and from BPML, make sure the WFD_NAME assign occurs sequentially after the Assign to and From * or delete the Assign to and From *.

Business Process Risk Factor	**Business Process meta data service**
Description	Business Processes which use BPMeta data may have to be updated if the service is not creating it's output under /ProcessData/BPDATA. For example, the tags used to generate /ProcessData/CURRENT_WF_WFD_ID and /ProcessData/WFD_412_V.3_NAME are now generated as /ProcessData/BPDATA/PARENT. In the 3.x generation of the product, this service was used to retrieve the actual BPID and the MetaData service was used to retrieve the name of the process.
Detection Method	Identify the Business Processes that use the BPMetadata service. Check the format of the tags in ProcessData to see if the BPDATA tag is not being used.
Recommendation	Change assigns in Business Process steps and sub-processes which are down stream of the BPMetaData service to account for the new output format of the service.

Business Process Risk Factor	**Lax XPath syntax**
Description	The Business Processes use less restrictive syntax than is allowable in higher versions of the Xalan parser (2.5.0).
Detection Method	In your Business Processes, search for references to attributes which include the text() node (/someLocation/@someAttribute/text()).
Recommendation	Change XPath syntax to use the string function (string(/someLocation/@someAttribute)).

Business Process Risk Factor	**Unsupported BPML parameters**
Description	Some service configurations, when scheduled, produce BPML which is intended to be consumed by a User Interface wizard before being executed by the SI engine. Specifically, the AS2FileSystemAdapter, when scheduled manually or when directly imported into SI generates the

	schedule_AS2FileSystemAdapterCollect Business Process. This Business Process contains replacement tokens in it which the Wizard would have otherwise processed. If those replacement tokens are in the BPML when it executes, they generate errors which do not get reported in the Current Processes. These errors can not terminated via the TroubleShooter. The following two risks have been identified: • An auto-generated Business Process is present in the XML export • An instance of the AS2FileSystemAdapter is present in the XML export BPML generated from older versions of the AS2 Wizard contain values in the from attribute which are not valid BPML in higher versions <assign to=max-files-to-collect from='&maxCollect;' append=true/>.
Detection Method	• Review each Business Process, for each assign node, and determine if the From attribute contains & and ; • Review each Business Process to account for all of the assigns where this occurs
Recommendation	• Do not import the BPML, do not import the AS2FileSystemAdapter instance. • Re-run the AS2 Wizard on the new system (the wizard will auto-generate these assets). • Replace the bad parameter with <assign to=max-files-to-collect from='-1' append="true">.

Business Process Risk Factor	**Unsupported XPath statements**
Description	The system now uses Xalan 2.5.0 to provide XPath and XSLT support. The Xalan 2.5.0 implementation of the XPath specification is more restrictive than the version of Xalan that was used by earlier releases. Some invalid XPath statements return values in 2.2 but return a different result in 4.3. Specifically, XPath statements that applied the text() predicate to attribute nodes conduct differently.
Detection Method	Use the native system tool: • ForWindows: cd \install_dir\install\upgrade ver3_1_0\misc\xpathReport.cmd • For UNIX: cd install_dir\upgrade ver3_1_0\misc\xpathReport.sh
Recommendation	For each instance of bad XPath found, manually analyze and correct the XPath statements.

Database Schema Risk Factors

Database Schema risk factors are related to any table, view, stored procedure, index, or other objects which cause problems when deployed to the upgraded system.

Database Schema Risk Factor	**Identified tables, views, triggers, indexes, constraints or stored procedures that are not part of core product**

Description	Your implementation makes use of custom tables, views, triggers, indexes, constraints or stored procedures.
Risk Detection	For each instance: • Look for new triggers, indexes, tables, views, constraints or stored procedures . • Consult your technical personnel and DBA and review your design documentation, BPML, and database schema to determine if any new triggers, indexes, tables, views or constraints have been added to the schema. Use the following files located under the installation directory as a guide to help you spot new or altered database assets. These files are for the creation of the tables, indexes and sequences: EFrame_TableChanges.sql, EFrame_IndexAdds.sql and EFrame_Sequence.sql.
Recommendation	The upgrade process should retain the custom assets since it runs against the original database. However, you should review all custom database assets after the conversion to ensure they are still present and functioning properly. You will also need to review any BPML, maps or code that use these assets and regression test them thoroughly. If any modifications were done that affect base tables, it is imperative that the tables be reviewed for changes between the versions. It is strongly discouraged to add new assets to the schema or to alter the schema in any way. In some cases for performance reasons, it is ok to add indexes to the schema. If you have added new tables to the schema, you should move them to a new schema. A new JDBC pool will need to be added and any services, adapters or maps that use the custom table will need to be updated.

Document Envelope Risk Factors

Document Envelope risk factors are practices relating the configuration of the system EDI Envelope Definitions which cause problems when deployed to the upgraded system.

Document Envelope Risk Factor	**Deprecated envelope parameters**
Description	Envelope parameters in previous versions are no longer present in new version.
Detection Method	Generate a list of envelope parameters which are deprecated.
Recommendation	Contact Professional Services about the Envelope conversion tool.

Document Envelope Risk Factor	**Required envelope parameters are not used**
Description	Envelope parameters required in new version are not present in previous version.
Detection Method	Generate a list of envelope parameters which are mandatory in 4.2, but not mandatory or not present in 3.x.
Recommendation	Contact Professional Services about the Envelope conversion tool.

Document Envelope Risk Factor	**Generate from Data option**
Description	If you used Generic Envelopes in which the map is determined using the Generate from Data option, the new values are automatically checked off. For example, qualifier codes, since the map names did not also include Qualf codes.
Detection Method	Not applicable

Recommendation	Qualifier codes in envelopes need to be unchecked for Inbound and outbound ST Envelopes.

External Programs Risk Factors

External Programs risk factors are related to any in-house or 3rd party command-line tools which cause problems when deployed to the upgraded system.

External Programs Schema Risk Factor	**Custom archiving**
Description	During an upgrade, the implementation relies on external programs or scripts which are not accounted for in the asset catalog.
Detection Method	For each system instance, for each Service Configuration: • Search for CommandLine and CLA2 adapters (by parentDefName), if a command line is in the service configuration, search through the list of external programs to see if it is in the list of external programs. • If external program not found in ListOfExternalPrograms, record the name of service configuration and name of program. For each instance: • Create a list of CLA and CLA2 adapter instances. For each adapter instance in that list, for each business process, search through the Participant nodes for instances of CommandLine and CLA2 adapters (by list of CLA and CLA2 configurations), if a command line is in the service configuration, record the name and location of the command and the Business Process name where it is called from.
Recommendation	• Find the missing external program and account for it in the location the system expects it to be. • Change the service configuration or Business Process to use the renamed program.

Map Risk Factors

Map risk factors are coding and configuration practices which cause problems when deployed to the upgraded system.

Map Risk Factor	**User Exits**
Description	Java code may use retired classes. User Exits may require JAR to be deployed. Note: This risk was resolved in 5.0 patch 3.
Detection Method	To find declarations: • For each map (MLX format), for each node in `//ExplicitRule`, if the text value of ExplicitRule contains the string object or x0Dx0Aobject then record the name of the field (ExplicitRule../Field/@Name) and the name of the map (ExplicitRule/PreSessionRule) To find instancing:

	• When invoking native Java classes, julianDate = new ("jDateConv");
Recommendation	Ensure that the JAR file containing the component referenced in the extended rule is re-deployed to the upgraded system using install3rdParty.

Map Risk Factor	**Non-existent pools in JDBC maps**
Description	You have a database pool referenced in a map which is not configured in the new version.
Detection Method	For each map (MLX format), for each node in //ODBCSyntax, for each /DataSources/DataSource use the /DSN child node. Review the jdbc.properties and jdbc_customer.properties files, look for a pool name that matches the /DSN. If one does not exist, record the map name and the value of /DSN. XPath to detect Database: /Mapper/node()/ODBCSyntax XPath to detect pool name: /Mapper/node()/ODBCSyntax/DataSources/DataSource/DSN Note: DB-to-DB maps may have two. The pool could be defined in either the jdbc.properties or jdbc_customer.properties /customerPropertiesFiles/customerPropertiesFile [@name="jdbc.properties"]/property[@name="<DSN>.url"] /customerPropertiesFiles/customerPropertiesFile [@name="jdbc_customer.properties"]/property[@name="<DSN>.url"] Example: /customerPropertiesFiles/customerPropertiesFile [@name="jdbc.properties"]/property[@name="mysqlPool.url"]
Recommendation	Do one of the following: • Create a new jdbc pool in jdbc_customer.properties • Save the map as MLX format and manually change the name of the datasource to an existing JDBC pool name. Save the map. • Ensure that all JDBC pools defined in the original SI installation are installed in the upgraded SI installation. See the 5.1 Upgrade Guide for details.

Map Risk Factor	**Inbound Map code list look ups**
Description	The Standard Rule of Code List changed in 4.2 such that it no longer works on the output side of a map.

Detection Method	For each system, for each map (MLX format), for each node in //UseSelect if @ TableName contains Code List and that node is part of the OUTPUT, then record the name of the map and the name of the element that contains the code list.
	XPath = /Mapper/OUTPUT/node()/*//UseSelect
	XPath = /Mapper/OUTPUT/node()/*//UseSelect[contains(TableName/text(),'Code List')]

Recommendation	Code List calls must be re-implemented on the input side of the map. This may involve creating temporary elements.

Performance and Tuning Risk Factors

Performance and tuning risk factors are related to any product performance tuning configurations which cause problems when deployed to the upgraded system.

Performance and Tuning Risk Factor	**Performance tunings have been applied to the properties files**
Description	Performance tunings have been moved to different properties files in the later versions of the software.
Detection Method	Review the list of properties file changes to determine which changes were targeted for performance.
Recommendation	Retune the upgraded system, rather than migrate the tuning parameters.

Properties File Upgrade Risk Factors

Properties Files risk factors are related to any properties files (/properties/*.properties) which cause problems when deployed to the upgraded system.

Properties File Risk Factor	**Customer specific properties files**
Description	You created new properties files.
Detection Method	For each instance: • Review each file in the properties directory. Generally, custom properties files are prefixed with a company specific identifier to distinguish them from base properties files. • Identify the file of the same name from InstalledData (baseline). If one is not found, record the name of the properties file.
Recommendation	Move customer specific properties file to the new instance.

Properties File Risk Factor	**Deprecated properties files are being used**
Description	You have customizations in properties files which must be migrated to other properties files in the new version.
Detection Method	Search for pool_customer.properties in the properties directory.
Recommendation	Reimplement customizations into jdbc_customer.properties.

Properties File Risk Factor	**enveloping.properties file has been updated to invoke a customized deenvelope/ envelope Business Processes**
Description	You made edits to the system properties file for enveloping.
Detection Method	Compare the file enveloping.properties located under the \install_dir\install\properties directory to the same file located in the \install_dir\install\installed_data directory.

	Review any differences to see if they are changes you applied. It is especially important to check to see if you have modified the file and replaced any of the following lines with a call to a custom Business Process:
	
	`enveloping.X12=X12EnvelopeUnified`
	`enveloping.EDIFACT=EDIFACTEnvelopeUnified`
	`enveloping.CII=CIIEnvelope`
	`enveloping.TRADACOMS=TRADACOMSEnvelope`
	`enveloping.ACH=ACHEnvelope`
	`enveloping.VDA=VDAEnvelope`
	`enveloping.SWIFT=SWIFTEnvelope`
	`enveloping.RND=RNDEnvelope`
	`enveloping.CHIPS=CHIPSEnvelope`
	`enveloping.FEDWIRE=FedwireEnvelope`
	
	There are other properties in this file you may have manually changed which should also be recorded.

Recommendation	Move any customizations you have made to the customer_overrides.properties file.

Properties File Risk Factor	**Environment-specific properties file settings**
Description	Properties files contain one or more parameter values which are specific to an instance. Example of this is an email address for the administrator of the test system versus an email address for the administrator of the production system.
Detection Method	For each instance: • For each customer properties file, for each property, lookup the value in installedData properties. • If values do not match, record the name of the customer properties file, the name and value of the property, and the InstalledData value.
Recommendation	The properties file values need to be migrated from like system to like system. For example, from old Production to new Production. All customer specific changes to system properties files should be moved into the customer_overrides.properties file. Any custom properties files should be migrated between like environments (Development to Development).

Properties File Risk Factor	**Non-performance related properties in the system properties files have been updated**
Description	Core properties files have been changed from out of the box settings.
Detection Method	For each instance: • For each properties file, for each property, lookup the value in installedData properties. • If values do not match, record the name of the properties file, the name and value of the property, and the InstalledData value.

Recommendation	Define all of your specific overrides in the customer_overrides.properties file.

Scripts Upgrade Risk Factors

Scripts risk factors are related to any changes to the product scripts which cause problems when deployed to the upgraded system.

Scripts Risk Factor	**System start up scripts have been modified**
Description	The scripts that system relies on for start up or shut down were modified.
Detection Method	For each instance, for each script in the bin directory (.cmd or .sh), compare to same script in instance's InstalledData.
Recommendation	• Analyze functionality of script changes. • If desired, migrate the modifications to the new versions of the scripts.

Service and Adapter Upgrade Risk Factors

Services and Adapters risk factors practices relating the configuration of or use of Services which cause problems when deployed to the upgraded system.

Service and Adapter Risk Factor	**Custom services or adapters**
Description	Custom services or adapters are deployed.
Detection Method	For each instance: • In most cases, your technical team will know if you have defined any custom services or adapters. • For each instance, look through the XML Export file of customer services. For each service, using the parentdefname, look for a match in the installedData list of services. If no match is found, record the name of the service from the Customer Services.
Recommendation	The custom service must be installed and tested in 4.2. The install bundle needs to be provided to the implementation team, along with any 3rd party libraries.

Service and Adapter Risk Factor	**Customer modifications to out of the box Service Configurations**
Description	The service or adapter configuration which shipped with the system has been modified by the customer.
Detection Method	For each instance: • Review the configuration, review the Customer Export service configurations for a match. • When a match is found, for each parameter in the installedData, find the parameter in the Customer XML. Compare the two. If they do not match, record the name of the service and the name of the parameter.

Recommendation	These service configurations must be specifically imported.

Service and Adapter Risk Factor	**Environment specific adapter configurations**
Description	This risk applies only if you have several instances. The adapter configuration is named, for example, Production or Test and contains a parameter value which allows the adapter to only access its target resource when deployed on a particular environment. An example of this is a Command Line Adapter which refers to a program deployed only on the production server.
Detection Method	For each instance: • For each service configuration in the ServiceConfigs, search through each instance's business processes looking for use of that service configuration name. When one is found, record the system name, and the business process name. • Review the output. When an occurrence of a service configuration is present in one of the systems' Business Processes, but not in all the other systems' Business Processes by that name, record the name of the Business Process and the name of the system where it occurs.
Recommendation	Do one of the following: • Abstract the system dependency by implementing a systemName parameter in a properties file which supports a choice in the BPML. This allows a single BPML code base to be shared across instances. • Abstract the system dependency by implementing a systemName parameter in a properties file, the include a system-specific property name with the name of the Service Configuration. Pass that looked up value to the Dynamic Service Invoker service. • Create purpose-specific adapter configurations which all have the same name, but are parameterized for different systems. In this case, some service configurations will be system-specific. • Implement a Service Group and disable the individual system specific Services that do not apply to the instance.

Trading Partner Upgrade Risk Factors

Trading Partner Profile risk factors are practices relating the configuration of the system Trading Partner Definitions which cause problems when deployed to the upgraded system.

Trading Partner Risk Factor	**PGP Profiles**
Description	PGP executables must be accessible from new instance and directory paths updated in the PGP adapter configurations if necessary.
Detection Method	Determine if you are using PGP.
Recommendation	Ensure PGP executables are accessible on new instance and directory paths updated in the PGP adapter configurations as necessary.

Upgrade Roll-back Upgrade Risk Factors

Upgrade roll-back risk factors are related to any roll-back procedures, resource, or other factors which cause problems when deployed to the upgraded system.

Upgrade Roll-back Risk Factor	You do not have a backup of the file system or database which has been proven to restore reliably.
Description	• You do not have a backup of system and the database from which a restore can be achieved. • You has a backup, but has not verified to completeness and restorability of the backup.
Detection Method	Not applicable
Recommendation	A backup and restore and regression test rehearsal is planned and executed.

XSLT Upgrade Risk Factors

XSLT risk factors are coding practices which cause problems when deployed to the upgraded system.

XSLT Risk Factor	**Lax XPath syntax**
Description	The business processes use less restrictive syntax than is allowable in higher versions of the Xalan parser (2.5.0).
Detection Method	In your business processes, search for references to attributes which include the text() node (/someLocation/@someAttribute/text()).
Recommendation	Change XPath syntax to use the string function (string(/someLocation/@someAttribute)).

3rd Party Libraries Upgrade Risk Factors

3rd Party Library Risk Factors are related to any JAR or WAR files which cause problems when deployed to the upgraded system.

3rd Party Libraries Risk Factor	**Unaccounted for 3rd Party Library dependencies**
Description	The services or adapters used in the implementation rely on 3rd party libraries which are either not accounted for in the asset catalog or which must be upgraded for the new version of the system.
Detection Method	For each instance, • Review the JAR files deployed in your current instance. • After installing and running the upgrade conversion compare the JAR files in the new instance to the original instance and document any JAR files that are in the original instance and not the new environment.
Recommendation	Determine the origin of the 3rd party jar file and ensure that it is installed during the upgrade.

Upgrade Best Practices

Upgrade Best Practice Information

The following are some general best practice information to review prior to starting the upgrade process:

Business Process Best Practice	**Retired services**
Description	The Business Processes contain services or adapters which are scheduled for deprecation.
Recommendation	• Some retired services simply need to be replaced by new services. • Some new services will require a Perimeter Server to be deployed. • Some new services will require that the Business Process be entirely re-written.

Business Process Best Practice	**Services which have since been enhanced**
Description	The Business Processes contain services or adapters which have since been enhanced.
Recommendation	Some services require the deployment of a separate component (CLA2 endpoint).

Business Process Best Practice	**Business Processes contain a technique which has been deemed sub-optimal**
Description	The Business Processes contain a technique which has been deemed sub-optimal and for which there exists a Best Practice rule.
Recommendation	Move the Business Processes into separate queues based on the call stack. Business Processes earlier in the call stack should go on early queues, and those later in the call stack go on later queues. This allows you to add more threads to Business Processes in the call stack that execute longer. This mitigation requires queue tuning to accompany the changes.

Business Process Best Practice	**Services or adapters which have no longer recommended parameters**
Description	The Business Process uses a service or adapter which has had a feature configuration which is no longer recommended. For instance, the File System Adapter supports the importFileRequest message, but there are other documented parameters for enabling this behavior.

Recommendation	Use the normal FSA output and input message and setting the deleteAfterCollect parameter to NO.

Business Process Best Practice	**Inefficient XPath**
Description	Maps or Business Processes access process data via XPath syntax which begins with //.
Recommendation	Use the fully qualify XPath.

Services and Adapters Best Practice	**Purpose-Specific adapter configurations**
Description	The adapter configuration is named the same across instances, but each is parameterized to access a different (production, test, or development) resource.
Recommendation	At implementation, these services must be configured for the specific environment once they are installed. Service Configurations need to be migrated like system to like system (between old Production and new Production) and can not be installed across systems (old Test to new Production).

Services Groups Best Practice	**Appropriate for Service Grouping**
Description	The instance is running in a cluster, but the service or adapter is not included in a Service Group.
Recommendation	Refer to the documentation for information on creating Service Groups.

Document Envelope Best Practice	**Use of Validate Input / Output option**
Description	The options of Validate Translation Input and Validate Translation Output are automatically set to yes. This may cause compliance errors that did not exist in the old system.
Recommendation	After upgrading review your Document Envelopes and adjust them as desired.

Document Envelope Best Practice	**Generic IB group envelope**
Description	For Inbound GS Generic envelopes the default setting is Generate FA.
Recommendation	Create an Inbound FA Generic GS envelope to not generate an FA for inbound FA's.

Trading Partner Best Practice	**AS2 partners set up via AS2 Wizard**
Description	Directory paths for the AS2 File System Adapters will need to be updated if they reference the old installation directory path.
Recommendation	Use the AS2 Wizard to update the file system collection and extraction directories if they reference the old installation directory.

Map Best Practice	**Inefficient XPath**
Description	The maps access process data via XPath syntax which begins with //.
Recommendation	For maps (standard or extended rules), update to the fully qualified XPath.

JDBC Pool Best Practice	JDBC Pools have been edited or augmented
Description	JDBC pools exist which are not part of the core product installation.
Recommendation	Define customer-specific pools in jdbc_customer.properties file.

Deployment Architecture Best Practice	Tomcat-in-DMZ for safe B2B communications
Description	The implementation contains components which have since been enhanced. This risk factor is characterized by the presence of a better option for a particular architecture.
Recommendation	Determine whether the Business Process is being used in production.

Additional Reference Information

Retired Services and Adapters

The following is a list of retired services and adapters and the service or adapter which replaces it:

Retiring Service or Adapter Name	Software Version	parentdefname string	Replacement Service or Adapter Name
B2B FTP Client Adapter	3.0, 3.1	B2B_FTP_CLIENT_ADAPTER	FTP Client Adapter
B2B HTTP Client Adapter	3.0, 3.1	B2B_HTTP_CLIENT_ADAPTER	HTTP Client Adapter
B2B HTTP Communications Adapter	3.1	B2B_HTTP_COMMUNICATIONS_ADAPTER	HTTP Client Adapter
B2B HTTP Service Adapter	3.0, 3.1	B2BHttpAdapter	HTTP Server Adapter
Connect Direct Adapter	3.0, 3.1	CDAdapter	Connect Direct Requester Adapter
Connect Enterprise Adapter	3.0, 3.1	CEFTP_ADAPTER	Connect:Enterprise UNIX Server Adapter
EDIFACT CONTRL Generation Service	3.0, 3.1	GenerateCONTRLType	EDIFACT Deenvelope Service / EDI Post Processor Service
EDIFACT CONTRL Reconcillation Service	3.0, 3.1	ReconcileCONTRLType	EDIFACT Deenvelope Service / EDI Post Processor Service
EDIFACT UNB/UNZ Deenvelope Service	3.0, 3.1	DeenvelopeUNBType	EDIFACT Deenvelope Service
EDIFACT UNB/UNZ Envelope Service	3.0, 3.1	EnvelopeUNBType	EDIFACT Envelope Service
EDIFACT UNG/UNE Deenvelope Service	3.0, 3.1	DeenvelopeUNGType	EDIFACT Deenvelope Service
EDIFACT UNG/UNE Envelope Service	3.0, 3.1	EnvelopeUNGType	EDIFACT Envelope Service

Retiring Service or Adapter Name	Software Version	parentdefname string	Replacement Service or Adapter Name
EDIFACT UNH/UNT Deenvelope Service	3.0, 3.1	DeenvelopeUNHType	EDIFACT Deenvelope Service
EDIFACT UNH/UNT Envelope Service	3.0, 3.1	EnvelopeUNHType	EDIFACT Envelope Service
FTP Get Adapter	3.0, 3.1	FTPGET_ADAPTER	FTP Client Adapter
FTP Send Adapter	3.0, 3.1	FTP_SEND_ADAPTER	FTP Client Adapter
HTTP Communications Adapter	3.1	HTTP_COMMUNICATIONS_ADAPTER	HTTP Client Adapter
HTTP Send Adapter	3.0, 3.1	HTTP_SEND_ADAPTER	HTTP Client Adapter
X12 997 Generation Service	3.0, 3.1	Generate997Type	X12 Deenvelope Service / EDIPostProcessorService
X12 997 Reconcillation Service	3.0, 3.1	Reconcile997Type	X12 Deenvelope Service / EDIPostProcessorService
X12 GS/GE Deenvelope Service	3.0, 3.1	DeenvelopeGSType	X12 Deenvelope Service
X12 GS/GE Envelope Service	3.0, 3.1	EnvelopeGSType	X12 Envelope Service
X12 ISA/IEA Deenvelope Service	3.0, 3.1	DeenvelopeISAType	X12 Deenvelope Service
X12 ISA/IEA Envelope Service	3.0, 3.1	EnvelopeISAType	X12 Envelope Service
X12 ST/SE Deenvelope Service	3.0, 3.1	DeenvelopeSTType	X12 Deenvelope Service
X12 ST/SE Envelope Service	3.0, 3.1	EnvelopeSTType	X12 Envelope Service
X12 TA1 Generation Service	3.0, 3.1	GenerateTA1Type	X12 Deenvelope Service / EDIPostProcessorService
X12 TA1 Reconcillation Service	3.0, 3.1	ReconcileTA1Type	X12 Deenvelope Service / EDIPostProcessorService
XML Transformer	3.0, 3.1	XML Transformer Type	DocToDOM, DOMToDoc and XSLT Service Note: One function has not been replaced. Specifying literal XML tags using the CData section, which would be converted to nodes in the Process Data.

Enhanced Services and Preferred Service

The following is a list of enhanced services and preferred services:

Old School Service or Adapter	SI Version	Old School Service Parentdefname string	New Service or Adapter Name
Command Line Adapter	3.0, 3.1	CmdLine	CmdLine2

Services Whose Output has Changed

The following is a list of services whose output has changed:

Service or Adapter Name	Software Version	Service parentdefname string	Change Summary

BP Meta Data Service	3.0, 3.1	BPMetaDataServiceType	From
			`/ProcessData/<CURRENT_WF_WFD_ID><WFD_..._NAME><WFD_..._PERSISTENCE_LEVEL><WFD_..._LIFE_SPAN>`
			To
			`/ProcessData/BPDATA/`

Adapters That Should be in Groups

The following is a list adapters that should be grouped:

Service or Adapter Name	Service parentdefname string
Command Line Adapter 2	CmdLine2

BPMetaData Service Output

In 3.1, the output looked like the example below. The BPML which created this ProcessData explicitly placed the output of the service into the nodes named like firstCallToService:

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ProcessData>
   <firstCallToService>
     <CURRENT_WF_WFD_ID>412_V.3</CURRENT_WF_WFD_ID>
     <WFD_412_V.3_NAME>Migrate_BPMetaDataService</WFD_412_V.3_NAME>
     <WFD_412_V.3_PERSISTENCE_LEVEL>DEFAULT</WFD_412_V.3_PERSISTENCE_LEVEL>
     <WFD_412_V.3_LIFE_SPAN>2880 mins</WFD_412_V.3_LIFE_SPAN>
   </firstCallToService>
   <secondCallToService>
```

```
      <CURRENT_WF_WFD_ID>412_V.3</CURRENT_WF_WFD_ID>
      <WFD_412_V.3_NAME>Migrate_BPMetaDataService</WFD_412_V.3_NAME>
      <WFD_412_V.3_PERSISTENCE_LEVEL>DEFAULT</WFD_412_V.3_PERSISTENCE_LEVEL>
      <WFD_412_V.3_LIFE_SPAN>2880 mins</WFD_412_V.3_LIFE_SPAN>
   </secondCallToService>
</ProcessData>
```

Copyright