Paper 200-2007

How Shall we Secure the BI Enterprise

Paul E. Christenson, Blue Cross and Blue Shield of Minnesota, Eagan, MN
Jerry A. High, Blue Cross and Blue Shield of Minnesota, Eagan, MN

ABSTRACT

Your company has elected to deploy the SAS® Enterprise BI Server as their enterprise wide analytical platform. Congratulations! You are the SAS Administrator. This is a good thing, but there is much more involved than loading software on a server. You will need to determine how to make SAS BI work with your company's security, quality assurance, and application deployment guidelines. When we started this journey at Blue Cross and Blue Shield of Minnesota (BCBSM), we found a number of security and operational requirements to consider:

- The system will support both internal & external customer groups with thousands of named users.
- The system will support separate logical server instances for Development, Integration testing, Quality Assurance testing and Production.
- The system will support multiple development teams.
- The system will support users of SAS® Web Report Studio, SAS® Enterprise Guide®, and traditional Unix command line SAS.
- The system will support multiple customer groups and customer hierarchies.
- The system will support the control of users by a central security team.
- The system will support code deployment to the Q and P environments by a centralized deployment team.

This paper will cover how BCBSM, categorizes its analytical users into roles and how we use SAS® 9.1.3 SP4 with SAS® Management Console 9.1, BI Manager version and SAS® Enterprise Guide 4.1 running on AIX 5.3 SP 3 to meet the security, development and deployment needs of our user communities.

INTRODUCTION

Many companies have embraced Business Intelligence (BI) software. It has a lot of appeal. Reports are accessed via a browser, management of the server software is done on one server, analysts can create and deploy reports at will, and security of the framework can be readily managed within the BI tool. If only it was that easy.

In the real world, reports can indeed be accessed via a browser. However, if you want to create a robust enterprise level BI framework that can support application development standards and provide controlled access to reports and information, you will find yourself with a number of obstacles that need to be handled. Typical application development requires testing prior to deployment to production status, driving the need of multiple server environments. Security departments in most companies require central administration with audits, driving the need for external authentication/authorization models. Many enterprise data warehouses are stored in a RDBMS that may require highly tuned queries to return results in "web time". As a result, highly customized SQL routines are common, driving the need for developing reports under SAS Stored Processes. These reports then need to be promoted across servers as they move into production for all users.

At BCBSM, we faced many of these challenges as we deployed the SAS Enterprise BI Server. In this paper, we will discuss a number of considerations for deploying a successful enterprise ready environment that integrates with standard IT frameworks and processes.

We will first begin with a brief description of the user community, providing definitions of users and the components that they would typically utilize. From there we discuss the change management process used to promote code/reports from development to production. With that understanding, we move into security considerations. Here we look at security from two viewpoints, administration of the framework and development of reports.

With the groundwork laid, we will go into greater detail about how we initially set up our environment to support an externally facing web site. Through the use of directory folders and Access Control Tables (ACTs), we provided a development framework that allowed us to develop, test and promote reports to our production web site. As with any new implementation, there are lessons to be learned and improvements to be made. We share a few of these and describe our next steps as we prepare to move into our second phase of our BI rollout.

BCBSM BI USER COMMUNITY

Figure 1 and Table 1 describes the relationship of the different user types in our business intelligence community and the functionality in the SAS Enterprise BI Server being made available to them.

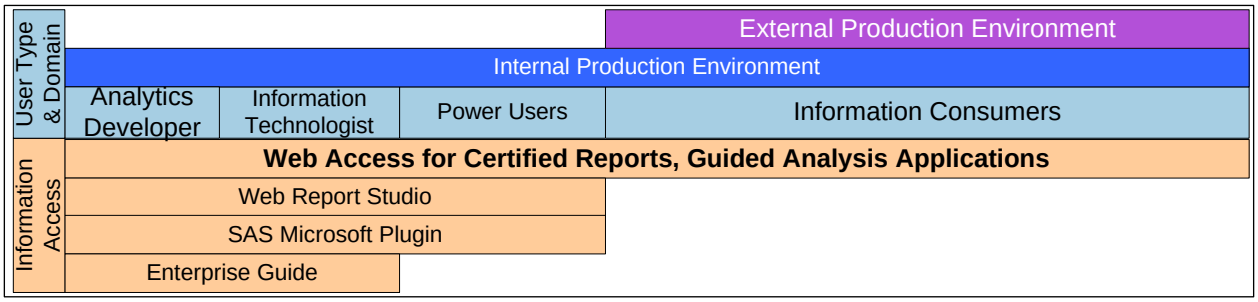

Figure 1

Table 1

ANALYTICAL CONSUMERS	DESCRIPTION	INTERNAL USER	EXTERNAL USER
Information Consumer	Decision maker who wants accurate information in a predefined layout in a timely manner. Access needs to be intuitive.	Executives, Directors, Department Managers & Business Analysts	Company Benefit Analysts & Healthcare Consultants
Power User	Subject matter expert needing flexible access to content and predefined analysis techniques.	Business Analysts, Departmental Managers & Subject Matter Experts	n/a
Information Technologist	Business analyst responsible for in-depth analysis and ad hoc reporting.	Traditional SAS Analyst	n/a
Analytics Developer	SAS developer whose work follows a change management process	Report Writers, SAS Application Developer, Java Developers	n/a

SAS® Metadata server provides significant flexibility for administrating access to functionality and group security rights for users. BCBSM has used SAS Technote TS-750 "Securing SAS®9 Business Intelligence content Managed in Metadata" as a starting point for developing security access patterns. Defining the security patterns to support the development and certification of content and applications has been an ongoing process. The remainder of this document will focus on the security patterns needed for creating, testing and deploying certified content into production.

CONTENT DEVELOPMENT AND CHANGE MANAGEMENT

For applications and content to be defined as certified, the content must follow a repeatable change management process. Figure 2 displays the environments used to support this process at BCBSM.

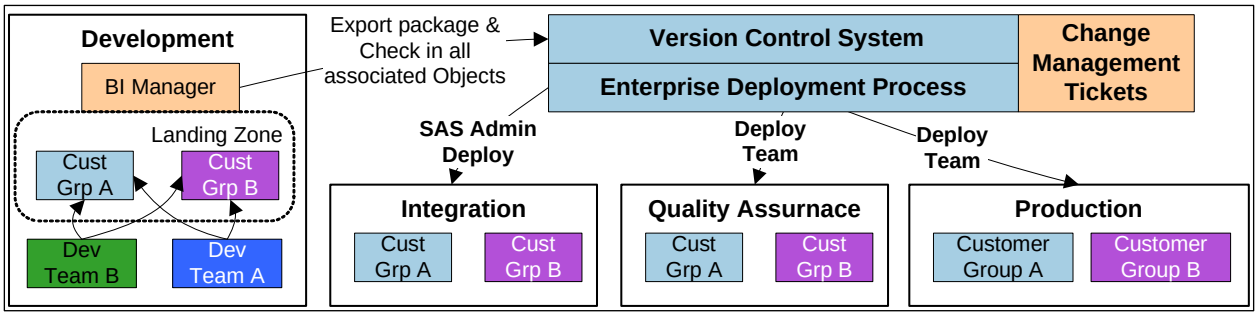

Figure 2

Definitions of the environments used for application development are defined as follows:

DEVELOPMENT: This environment is used by development teams to create content and applications based on documented requirements. Completed objects must pass a peer review and are unit tested by the development team. When content has passed unit testing, the content components are bundled into a release and kept under version control. A deployment package for that release is then created by the SAS Administrator.

INTEGRATION: The release package is deployed to this environment by the SAS Administrator using the automated deployment process. The release is system tested by the development team to verify that the package was built correctly with all of the correct component versions.

QUALITY ASSURANCE: Deployment of content to this environment is done by a Central Deployment Management (CDM) team. The CDM team only deploys content after all steps in the change management process have been performed and approved through a change management ticket. The Quality Assurance (QA) team performs a full set of quality testing based on the original requirements and any associated regression testing. If defects are found then the development team works on updating the release in the Development environment and the process is repeated. Performance testing is done by SAS Administration using automated load testing tools.

PRODUCTION: After QA testing is completed and approved, another change management ticket is created for the CDM team to deploy the new release into production during a scheduled deployment window. After the content is deployed a verification test is made in production. If the release does not pass verification the previous release is redeployed to production.

SYSTEM ADMINISTRATION GROUPS & ROLES

For successful deployment of reports and content within the SAS BI framework there are a number of system administration and support teams that need specific access in the various environments. Table 2 lists the teams and the system access they require to perform their duties.

Table 2

ADMINISTRATION TEAMS	REQUIRED ACCESS	SAS GROUPS & ROLES
SAS Administration team	Configuration and maintenance of SAS environment.	Restricted Administrator*
	Support Web Content Developers.	Web Report Studio Administrator
	Manage web pages and portlets displayed to users.	Portal Administrator
CDM Team	Deployment of all applications to QA and Production environments.	Deploy Group
		Restricted administrator*
Central Security Team	Enterprise wide management of security access for BCBSM	Security Administration**
Database Access	Manage access to the database. The group holds the database application ID and encrypted password. The authorization domain is setup up for the specific database source.	Database Group
Trusted User Web Access	Web accounts that are authenticated by a corporate LDAP repository need to have access to a trusted user account for passing authentication into SAS Metadata.	WebUser Group

* Restricted Administrator is a setting in the Trusted Administrator.txt configuration file.

** Security Administration is defined as a separate role in our environment but is not currently supported by SAS. Batch load scripts are created for the Security team to load users from a central LDAP repository.

DEVELOPMENT AND TESTING GROUPS

As with the administration of the framework, report writers, application developers and testers also need specific access in the environments to deploy certified content. Table 3 lists the teams and the system access they require.

Table 3

DEVELOPMENT TEAMS	REQUIRED ACCESS	SAS GROUPS & ROLES
Content Development Teams	Enterprise Guide used in development environment. User can create stored processes. Uses default authorization.	Enterprise Guide Developer
	Access to Web Report Studio and published stored processes.	Web Report Author
	Web Access to team development content in Portal or Microsoft plug-in.	Dev Team Web group
Unit Tester	Simulate customer web and plug-in access for unit testing before exporting content from development.	Customer Web group
Integration Tester	Simulate customer web and plug-in access for integration testing of deployment package.	Customer Web group
QA Team	Simulate customer web and plug-in access for regression and quality assurance testing in the QA environment.	Customer Web group

For the first phase of development BCBSM used SAS Enterprise Guide to create web reports using stored processes. BCBSM has configured the SAS Portal for single sign on using a trusted user ID and a centralized LDAP server that manages all web authentications. A developer can then have multiple web accounts for testing content at different stages in development or for different types of customers. These groups only exist in the Development, Integration and Quality Assurance environments.

SAS METADATA SETUP FOR EXTERNAL DEVELOPMENT (PHASE 1)

For the first use of the SAS BI Environment, BCBSM chose to release an external facing interactive reporting application using stored processes. The SAS Metadata server in development was configured with the following rules in mind:

- Developers can create content in their personal area.
- Group members can move and view stored processes into the team area.
- Development teams cannot access each other's development areas.
- SAS Administrators can access all areas and use BI Manger to promote code to the landing zone that matches the folder configuration in production.

Using Management Console 9.1 you can create groups for the administrators, development teams and customer simulation groups for unit testing. Figure 3 shows the layout of these groups in the User Manager Plugin. A developer can have one Enterprise Guide account with "DefaultAuth" set for the Authentication Domain. A developer's web accounts all have Authentication Domain set equal to "Web" and all accounts belong to the WebUser group (Trusted User). The Database Access group holds the user ID and password for the database application ID and has "DBAuth" set for the Authentication Domain. SAS System Services, Team Web groups and Team EG groups gain access to the database through membership in the Database Access group.

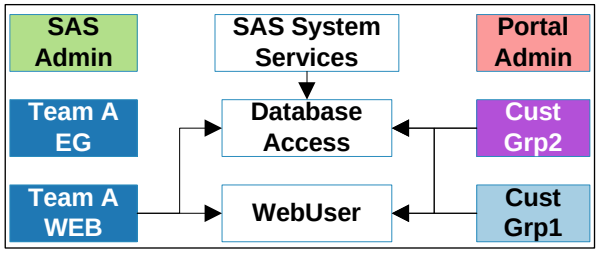

Figure 3

SETTING UP ACCESS CONTROL TEMPLATES

By putting the user groups into Access Control Templates (ACTs) access management for all the components in SAS Metadata is simplified. Figure 4 shows the different ACTs that were created for Phase 1. The first step is to modify the default ACT using the Authorization Manager. By adding the SAS Admin group at this level Administrators have access to all objects. By denying read and write metadata for the Public group only named users can access the Information Delivery Portal. The ACTs for development teams and customer groups listed below can be used as pattern templates for new groups.

Access rights key
RM: Read Metadata
WM: Write Metadata
R : Read

Default ACT

GROUP	WM	RM	R
PUBLIC	D	D	D
SASUSER	G	G	G
SAS Administrator	G	G	G
SAS System Services	G	G	G
SAS Admin Group	G	G	G
Deploy Group	G	G	G

Public Read Only ACT

GROUP	WM	RM	R
SASUSER	D	G	G
SAS Admin	G	G	G

SAS Admin Only ACT

GROUP	WM	RM	R
SASUSER	D	D	D
SAS Admin	G	G	G
Deploy Group	D	D	D

Portal Admin Only ACT

GROUP	WM	RM	R
SASUSER	D	G	G
SAS Admin	G	G	G
Portal Admin	G	G	G

Dev Team A -- ACT

GROUP	WM	RM	R
SASUSER	D	D	D
TeamEGDev	G	G	G
TeamWebDev	D	G	G

Dev Team B -- ACT

GROUP	WM	RM	R
SASUSER	D	D	D
TeamEGDev	G	G	G
TeamWebDev	D	G	G

Customer Group 1 ACT

GROUP	WM	RM	R
SASUSER	D	D	D
CustGrp1	D	G	G

Customer Level 2 ACT

GROUP	WM	RM	R
SASUSER	D	D	D
CustGrp2	D	G	G

Figure 4

METADATA FOLDERS AND ACTS

The SAS Management Console plugin BI Manager 1.3 is used to create folder hierarchies and ACTs. The Authorization tab on the folder is used to associate an ACT to the folder.

Figure 5 shows the folder layout and are color coded for the applied ACT. Under the BI Manager folder, a master folder (BCBSM) was created for stored process development. Separate folder hierarchies for each development team were created and the team ACT was applied. If desired there may be multiple user specific folders beneath the team folder. The Landing Zone folders have the same layout as Production. Any changes to STP parameters for production are made in the Landing Zone. A developer will only have read access to the Landing Zone for unit testing by being a member of a customer group. The SAS Administrator uses a Deploy account to move content from the Team Development area to the Landing Zone using BI Manager.

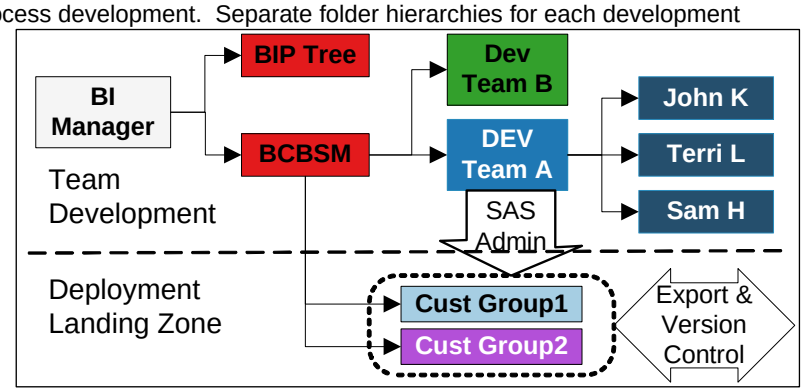

Figure 5

The personal development folders (dark blue) are the one exception BCBSM has to using ACTs for authorization management. A developer's EG user ID is manually added and given full access. One of the developer's web accounts is granted RM and R access and the team account is denied WM access.

PHYSICAL PATHS AND ACTS

Access to physical file paths is managed in Authorization Manager. When a source directory with a UNIX path is created for a development team, be sure to add a description since there is no unique name. The Team ACT can then be applied to the Source Directory. The developer will then be limited to these directories for saving stored processes. A developer's personal directories are granted the same access as their personal folder. Figure 6 shows the path to Source Directories and custom portlets in the Resource Management plugin.

By adding the Portal Admin ACT to the Public Permission Tree a developer cannot delete portlets and, if there is a customer specific portlet, access can be limited by applying the customer group ACT.

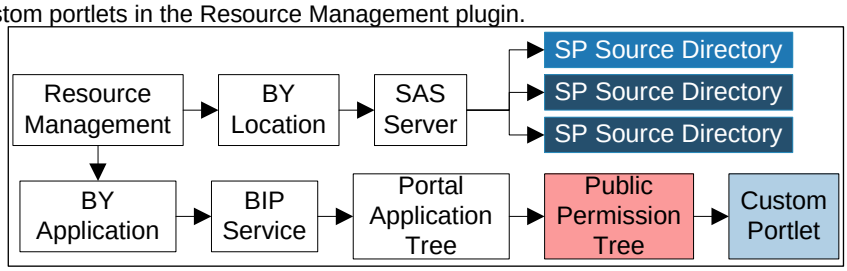

Figure 6

SECURITY CONFIGURATION FOR I,Q & P

Only System Administration and customer groups are needed in the Integration, Quality Assurance and Production environments. Developer's web access to customer groups in Integration is for system testing. The QA team has web access in the QA environment. And finally, external customers and business support personnel have web access in the Production environment. Figure 7 shows the simplified folder layout and applied ACTs.

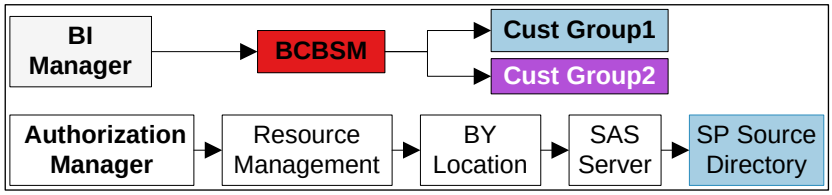

Figure 7

POSTMORTEM (PHASE 1)

Using the change management approach presented, we have developed and deployed 10 releases of our external web site. Overall, the web site has been well received by our external clients. Internally, we went through initial growing pains developing and using IT processes for SAS and Java code development. We can summarize our experience as follows:

- What worked
  - Version control of BI Manager Packages.
  - Stored processes deployed across multiple servers.
  - Folder level group security.
- What did not work
  - Under BI Manager V1.3 we experienced unexpected deletion of metadata artifacts from the development space.
  - The developer personal workspace was difficult to manage.
  - The BCBSM directory structure did not support using stored processes in Web Report Studio.
  - The development team found it difficult to manage concurrent multiple release tracks.

SAS METADATA SETUP FOR INTERNAL DEVELOPMENT (PHASE 2)

After reviewing our phase 1 results, it was decided to give development teams more autonomy in managing content releases. BI Manager 1.4 has some new features that could help with this goal.

- Issue number SN-V9-017860 "Parameter definitions associated with all Stored Process may be inadvertently deleted if a Stored Process that contains parameters is re-imported into the Foundation repository via BI Manager" has been fixed
- By modifying the WRS.DEFAULT.CONFIG file, Infomaps and Stored Processes can be developed in the system generated "My Folder" Space for an individual developer.
- Libraries and tables can be exported with BI Manager.

Table 4 shows the new groups being added to improve the development work flow.

Table 4

NEW USER TYPES	REQUIRED ACCESS	SAS GROUPS & ROLES
Development Team Lead	Enterprise Guide used in development environment. Can create stored processes. Uses default authorization.	Enterprise Guide Developer
	Manage team's Web Report Studio development	Web Report Administrator
	Simulate customer web and plug-in access	Customer Web group
	Write metadata access for supported customer groups	TeamLead
	Migrate content from Team Development space to Landing Zone	BI Manger 1.4 Restricted Administrator Access
All Administration group	Central access control for Multiple administration groups	AllAdmin

To avoid conflicts between ACTs at the same level in the Identity Hierarchy, all system administration groups are made members of the ALL Admin group. This would include:

- SAS Admin Group
- Deploy Group
- SAS System Services

For the same reason the Team Lead group will be a member of the Customer groups. Figure 8 shows how ACTs will be updated to support the new layout for the development environment.

The blank in the ACT table indicates that for a permission is neither granted or denied.

Default ACT

GROUP	WM	RM	R
PUBLIC	D	D	D
SASUSER	G	G	G
SAS Administrator	G	G	G
SAS System Services	G	G	G
All Admin	G	G	G

Public Read Only ACT

GROUP	WM	RM	R
SASUSER	D	G	G
SAS Admin	G	G	G
All Admin	G		

Dev Team A -- ACT

GROUP	WM	RM	R
SASUSER		D	
TeamEGDev	G	G	G
TeamWebDev	G	G	G
All Admin		G	

Customer Group 1 ACT

GROUP	WM	RM	R
SASUSER		D	
CustGrp1		G	G
TeamLead	G		
All Admin		G	

Figure 8

Whenever SASUSER has permissions denied, a group that is defined in the Default ACT also loses that permission one folder down. For the system administration groups to keep their access consistent, the All Admin group is granted the same access that the SASUSER group is being denied in a ACT.

To simplify content promotion reports, Infomaps, Stored Processes and Library definitions all are located under one folder hierarchy for a developer or team. Figure 9 shows the layout of folders and their associated ACTs. The creation of personal folders (tan) is managed by the system when a user is granted access to Web Report Studio. The Shared folder (gray) has a grant write metadata for the All Admin group directly on the folder ACE.

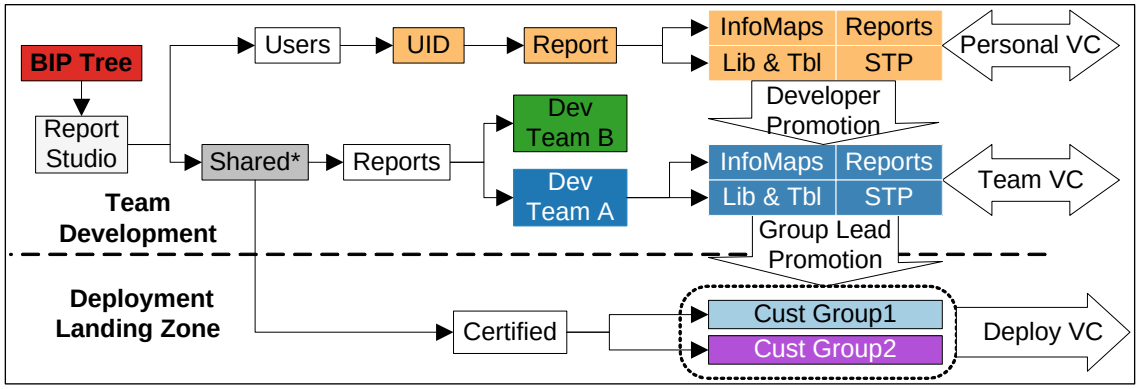

Figure 9

Individual developers can work on components and when they are ready, move them into the team space for code review and unit testing. After unit testing is passed the team lead can move the associated objects into the certified customer area and configure them for deployment.

CONCLUSION

Using groups, roles and ACTs greatly simplifies management of user security needs in SAS metadata for managing a development and change control process. More than anything, we found that careful thought and planning is needed to assure a successful enterprise deployment. It is also important to understand your corporate architecture framework in order to integrate the BI tool into your enterprise.

As with any product, improvements can always be made. Hooks for version control tools would greatly enhance multiple development tracks. Personal and team repositories that support child to parent repository code promotion would further enhance developmental workflow. These along with other recommendations are being considered by the SAS Institute for future releases.

REFERENCES

TS-750 -Securing SAS®9 Business Intelligence content Managed in Metadata. Retrieved February 21, 2007, from: http://support.sas.com/techsup/technote/ts750.pdf

SN-V9-017860 BI Manager "Import" may cause metadata to be destroyed for all stored processes that contain parameters in SAS 9.1.3 Service Pack 4. Retrieved February 21, 2007, from: http://support.sas.com/techsup/unotes/SN/017/017860.html

ACKNOWLEDGMENTS

The authors would like to thank Scott Sweetland and Diane Hatcher from the SAS Institute for their guidance in digital plumbing.

RECOMMENDED READING

SAS® 9.1.3 Intelligence Platform: Security Administration Guide, Second Edition. Retrieved February 21, 2007, from: http://support.sas.com/documentation/configuration/bisecag.pdf

Best Practices for SAS® Metadata Server Change Control. Retrieved February 21, 2007, from: http://support.sas.com/documentation/whitepaper/technical/MetadataServerchngmgmt.pdf

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Paul Christenson
Blue Cross and Blue Shield of Minnesota
3535 Blue Cross Road
Eagan, MN, 55122-1154
(651) 662-4422
E-mail: paul_e_christenson@bluecrossmn.com

Jerry A. High
Blue Cross and Blue Shield of Minnesota
3535 Blue Cross Road
Eagan, MN 55122
Work Phone: 651-662-8548
E-mail: jerry_a_high@bluecrossmn.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.
Other brand and product names are trademarks of their respective companies.