OPTUM™

Vermont Health Connect HIX Project

Program Management Review

8/18/2014

TABLE OF CONTENTS

1.0 .....EXECUTIVE SUMMARY **3**

2.0 .....BACKGROUND **6**

3.0 .....ASSESSMENT **7**

4.0 .....RECOMMENDATIONS **29**

1.0 EXECUTIVE SUMMARY

The purpose of the Program Management Review is to assess CGI's ability to deliver and identify areas at high risk for schedule noncompliance. This review documents the current state of the Program Management structure, Program Management process (relative to industry best practices) in use by the State of Vermont (SOV) and CGI for the Vermont Health Connect (VHC) implementation. It also includes Optum's recommendations to improve the overall program management activities within the VHC implementation program.

Optum has concluded, based review of the VHC's Program Management documentation and interviews with both SOV and contractor staff, that the project's Program Management structure and processes contributed to SOV's lack of project ownership and CGI's lack of accountability. Additionally, project management processes within the program, do not align with industry best practices and are insufficient or ineffective.

As a result CGI has not met its commitments in the contract and the project has not met the expectations of the SOV. The project team's ability to deliver the remaining contractual requirements is a 'High' risk, and as such, immediate corrective action is required.

Nine months after the implementation of the VHC solution (10/1/13), several critical functional requirements, including Change of Circumstance, Renewals, and SHOP, and over 2,500 non-functional requirements specified in the contract, have not been met. Additionally, there is no agreed upon plan for delivering the missing functional requirements or non-functional requirements.

Key Findings

Optum's assessment is based on the following key findings:

1) Governance – Program Management Structure
    - VHC's system integrator contract to build and implement the VHC solution, sourced its system integration activities and accountability to CGI, as specified in the contract's statement of work (SOW), but did not source ownership and control of these activities. The project's Project Management Plan (PMP), prepared by CGI, does not articulate a governance model that enables this distinction. The PMP depicts segmented teams with little definition of the SOV or joint team roles and responsibilities.
    - 'Ownership' of the project and it's outcomes by SOV is limited, at best. Based on the existing governance model, CGI took control of the project and the SOV ceded ownership.
    - Accountability for program management is unclear. Neither SOV nor CGI believe they are accountable for project outcomes.
    - As CGI disregarded processes in the PMP (prepared by CGI and signed-off by SOV) and industry best practices, the project's lack of control and ownership impacted the ability of the program teams to meet the project's original and/or revised milestones.
    - The project's aggressive schedule necessitated increased collaboration and rigorous processes. Instead, CGI proceeded with project activities without the appropriate SOV participation and without project management processes and controls that follow industry best practices.
    - A project-specific cost/budget management plan does not exist. Because of this, the overall costs are very difficult to define and manage.
    - Key governance principals for establishing/maintaining SOV ownership and control, outlined below, were not applied:
        - An integrated project organization structure – includes both State and SI vendor roles and responsibilities.
        - An integrated master schedule (e.g., Microsoft Project Plan) includes both SI vendor and State resource requirements and dependencies.
        - A deliverable review and approval process and phase gates considers the impact of deliverables not approved in accordance with the project schedule.

- An organization change management work-stream – business driven activities, tasks, roles and responsibilities that manage the impact of the solution on both internal and external stakeholders (and not limited to training).
- Project-specific cost/budget management

Section 3 – Assessment elaborates on these Governance findings.

2) Program Management Process

Project Management Institute (PMI) A Guide to the Project Management Body of Knowledge (PMBOK) defines a project management plan (PMP) as a formal approved document that defines the overall plan for how the project will be executed, monitored and controlled. Project governance provides a comprehensive, consistent method of controlling the project and should be described in the PMP. This deliverable should be updated periodically throughout the duration of the project.

VHC's PMP, version 3.0, dated February 21, 2013, states:

> *Changes to the PMP will be made upon joint VT and CGI agreement, and a revision history will be maintained to document such changes.*

This deliverable has not been updated since it was first published. Several industry standard project management processes are either omitted or insufficient.

Each of the following Project Management processes defined in the PMP is a 'High' risk – Immediate corrective action is required. Significant concerns have been identified.

- Schedule Management – A current comprehensive program schedule does not exist. There are several issues with the schedule that was provided to Optum during this review. CGI has not fulfilled their contractual commitment with regard to this portion of the contract.
- Scope Management – Requirements do not comply with industry best practices, Institute of Electrical and Electronics Engineers (IEEE) standards. This contributes to the challenge of differentiating changes from defects.
- Cost Management – A cost/budget management plan for the project does not exist. This is both a SOV and CGI responsibility.
- Quality Management – People, process, and technology (tools and environments) challenges are impacting quality management. Effective quality management is not limited to solution/application testing activities. Outstanding quality issues are documented in each of Optum's deliverables: Code Review, Transaction Monitoring, Architecture Review, Maintenance and Operations Review, and Quality Assurance Review.

Section 3 – Assessment elaborates on these Project Management Process findings.

3) High Risk for Schedule Non-Compliance

The CGI program team's ability to deliver the remaining contractual requirements is a 'High' risk and as such, immediate corrective action is required.

This risk assessment considers:

- CGI and the project team's track record for meeting project milestones
- The lack of collaboration between CGI and SOV
- The lack of defined and disciplined processes, and related controls
- The lack of an integrated schedule that outlines delivery dates for the remaining requirements.

These risks indicate the likelihood of CGI delivering renewals or other high priority functionality based on executing a project plan is not likely, especially since the plan does not exist.

Section 3 – Assessment elaborates on these Project Management Process findings.

Recommendation(s)

Optum recommendations are summarized below. These recommendations are based on the findings described herein.

1) Optum recommends 'operationalizing' the VHC solution, with the conclusion of CGI's contract on December 31, 2014. 'Operationalizing' establishes an organization to operate, maintain, and enhance the VHC solution, as compared to a 'project team' that is tasked to build and deploy the solution.

   Within the SOV's IT organization structure, an IT Director should lead the following teams or competencies:

   - Project Management Organization (PMO) – Owns the organizations integrated master schedule and manage project management process
   - Business Architecture – Owns the functional solution
   - Application Management / Technical Architecture – Owns the technical solution
   - Quality Management – Owns the delivery of a quality solution
   - Organization Change Management – Owns the stakeholder impact of solution changes and training
   - Hosting – Owns the operations and maintenance of the technical infrastructure
   - Cost/Budget Management – A finance/comptroller function to tracking funding, budget, and expenses

   Note, the competencies may be sourced by SOV resources or third-parties, including CGI.

   The benefit of this model is to clearly establish VHC ownership of the competencies necessary to support the solution and the business long term, and decentralize the competencies allowing SOV to staff internally or externally, as appropriate.

2) Initiate transition to an organization (vs. project) model as soon as possible and target deployment of the recommended model for January 1, 2014. These activities include:
   - Prepare and manage a project delivery plan, in conjunction with CGI and existing subcontractors and the SOV, which delivers a quality solution on a timely basis and enables status tracking and reporting.
   - Prepare a PMP from SOV's perspective, with input from vendor PMPs, as appropriate, and use it to manage the project.
   - Limit CGI's impact on project outcomes by increasing SOV's role (directly or through contractor's) in the following areas:
     - Application (business) architecture – Requirements and design
     - Quality Management – System Integration Testing, performance testing and UAT
     - Maintenance and Operations – Production Defect Tracking and Management
     - Program Management
   - Request from CGI an 'a la carte' based proposal for the first optional year of services. For example, distinguish design, development and implementation (DDI) services, from maintenance and operations (M&O), and hosting. This allows the State to select and procure from a menu of services, without procuring all of their services.
   - Define an organization model based on program requirements. SOV should consider its organization capabilities, strengths, etc. and consider unique aspects (requirements) of VHC to determine the appropriate organization model.
   - Identify candidates to support the model – this federation of services will require an experienced IT Director. This position will be responsible for delivering a VHC solution that meets the SOV business needs and leads a team that can adapt the solution as these needs change. Specific responsibilities depend on the organization model.

Introduction

The following sections of this deliverable describe Optum's approach and further describe maintenance and operations (M&O) findings and recommendations:

- Section 2.0 - Background outlines the Program Management approach to conducting the review.
- Section 3.0 – Assessment documents findings and recommendations
- Section 4.0 – Provides a summarized list of recommendations

2.0 BACKGROUND

The purpose of the Program Management Review is to assess CGI's ability to deliver and identify areas at high risk for schedule noncompliance. Specifically, this review documents the current state of the Program Management structure, Program Management process (relative to industry best practices) in use by the SOV and CGI for the VHC implementation and includes recommendations.

The team met with the following SOV and vendor team members, and attended Risks/Issues/Contingencies/Work-around meetings.

- State of Vermont
  - Lindsey Tucker
  - Stephanie Beck
  - Mark Larson
  - Nick Waringa
  - Jack Green
  - Mike Morey
  - Paul Pratt
  - John Kohlmeyer
  - Justin Tease
- Contractors
  - [redacted]
- CGI
  - [redacted]
- Exeter
- Benaissance
- Archetype

Several requests to meet with CGI to discuss Program Management, specifically regarding the PMP and the MS Project Plan were not accommodated.

The following project documents were reviewed are outlined in the table below.

Status Reports
• AHS – Vermont Health Connect: Weekly Project Report for Vermont Health Connect (VHC), (prepared by Vijay Desai, Josh Kreiger, Tony Thibault, & John Purcell)
• CGI HBE Status Reports
Prior Assessments
• Vermont Health Services Enterprise Initial Implementation Review and Assessment ("Lessons Learned"); prepared by BerryDunn McNeil & Parker, LLC

• Gartner - Vermont Health Services Enterprise Program Bi-Weekly Quality Assurance Status Report (9/28/2013, 10/11/2013)

Contract
• CGI Master Services Agreement, dated December 13, 2012
• Master Service Agreement – Amendment #1, dated February 28, 2013 (includes SOW #1)
• Master Service Agreement – Amendment #2, dated May 1, 2013 (includes SOW #2 SOW-ACCESS Integration)
• Master Service Agreement – Amendment #3, dated August 12, 2013 (includes SOW #4 Hosting Services)
• Master Service Agreement – Amendment #4, dated April 1, 2014
Deliverables
• D02- Project Management Plan v 3.0
• HBE Project Plan (dated 5/23/2014); MS Project Plan
• D14 – Requirements Traceability Matrix
Other Artifacts
• CR Top 50, dated May 26, 2014
• Deliverable Tracking v3 June, 2014
• Operations Assessment, prepare by HES Advisors, June 5, 2014
• Non-IT Project Plan ('00-Master-30May')
• CGI Project Plan Analysis ('140523-PlanAnalysis')

3.0 ASSESSMENT

This section of the document elaborates on findings summarized in Section 1 – Executive Summary.

1) Governance – Program Management Structure

Project governance provides a comprehensive, consistent method of controlling the project. The project's governance must fit within the larger context of the program or organization sponsoring it.

Best Practice, as specified by the Project Management Body of Knowledge (PMBOK)

Observations/Findings and Recommendations

The table below describes Observations/Findings and Recommendations. The scope of this assessment focused on SOV/CGI governance and did not focus on intra-agency governance.

Best practices (e.g., PMBOK) expect project governance to be addressed in either the Project Charter or within the Staffing Management Plan, as part of a PMP.

Observation/Findings	Recommendation
The project's PMP, prepared by CGI, does not provide a sufficient method for controlling the project. It does not articulate a governance model that distinguishes their accountability for performing the activities and delivering the milestones specified in its SOW from SOV's project ownership responsibility.	Near-term: A PMP should be prepared, from the State's perspective, with input from the SI vendor: Lesson Learned: On future projects ensure the SOW or project charter includes the appropriate controls to ensure SOV ownership of project activities and outcomes. These controls should first be articulated in the Contract and then in the PMP. Examples of controls include clearly defined phase gates and issue resolution escalation process.
The SOV team's lack of experience with large-scale system integration projects resulted in a level of trust with CGI after the Master Services Agreement and Statement of Work #1 were executed. Amendment #4 contributes to the project's current state by focusing on outcomes and not mutually agreed upon processes.	Lesson Learned: SOV must staff projects that engage SOV resources (or third party) in project processes and not merely verification of outcomes (deliverables). Focus on process and related controls is critical to achieving expected outcomes for the SOV.
While a Warranty Period is not specified in the Contract, The Master Services Agreement notes, 'Supplier shall provide, on a best commercially reasonable basis, any services SOV reasonably determines are necessary and related to services under any Statement of Work, to cause the Services to meet or exceed the Requirements and achieve Service Levels….' CGI is not staffed to comply with this clause in the contract.	SOV should communicate to CGI specific staffing requirements to accommodate new functionality requests and M&O 'to meet and exceed Service Levels'.
The (SOV) EPMO provides statutory oversight of IT projects within the State, <u>develops and maintains project management artifacts</u>, implements standards for IT project selection, ensures benefit realization of IT projects and manages the State IT project portfolio. It will provide oversight and guidance for the State Project Manager, project management team and Vendor Project Managers.	The project has lacked the appropriate SOV EPMO oversight, artifacts have not been developed, and the gap between the contract, the approved PMP, and the processes currently followed is fundamental to the project's current state. The SOV EPMO should have a defined role and accountability. This role described in the revised project-PMP.

Observation/Findings	Recommendation
The governance model depicted in the CGI PMP segments CGI's team from the SOV team with little emphasis on collaboration and lacks description of SOV project responsibilities. Note, Amendment No. 1 includes position descriptions but these are generic roles and not in context to the project, and do not highlight collaboration. Exhibit 1: Current CGI PMP - Governance Structure for the SOV and CGI Teams (see below) is from the PMP and is the extent of the governance 'description' in the PMP.	Lesson Learned: Role descriptions should highlight collaboration and controls. The following exhibits are included as examples: Exhibit 2:Sample - System Integration Project Organization and Governance model Exhibit 3: Sample - Roles and Responsibilities Note: A diagram does not solve ownership, accountability, and collaboration challenges. It is the outcome of discussions intended to define expectations and resolve issues, and should be used to guide the project execution. SOV needs experienced leadership to drive these discussions going forward. The SOV Executive Sponsor needs a Project (or IT) Director with prior experience leading $50 - $100 million engagements. This leader must be empowered by SOV to make decision on a day to day basis and involve the SOV Executive Committee, as appropriate.
Project organization structure includes a training team, but does not include an Organization Change Management team.	The benefits of an Organization Change Management team are described in the following Project Management Processes – Observations/Findings and Recommendations, Staffing Management section.
A project-specific cost/budget management plan does not exist.	Please refer to the following Project Management Processes – Observations/Findings and Recommendations, Cost/Budget Management section.

Exhibits

The graphic below is provided in the PMP, but not supported by a description of roles and responsibilities. This diagram is not an accurate representation of the current governance structure.

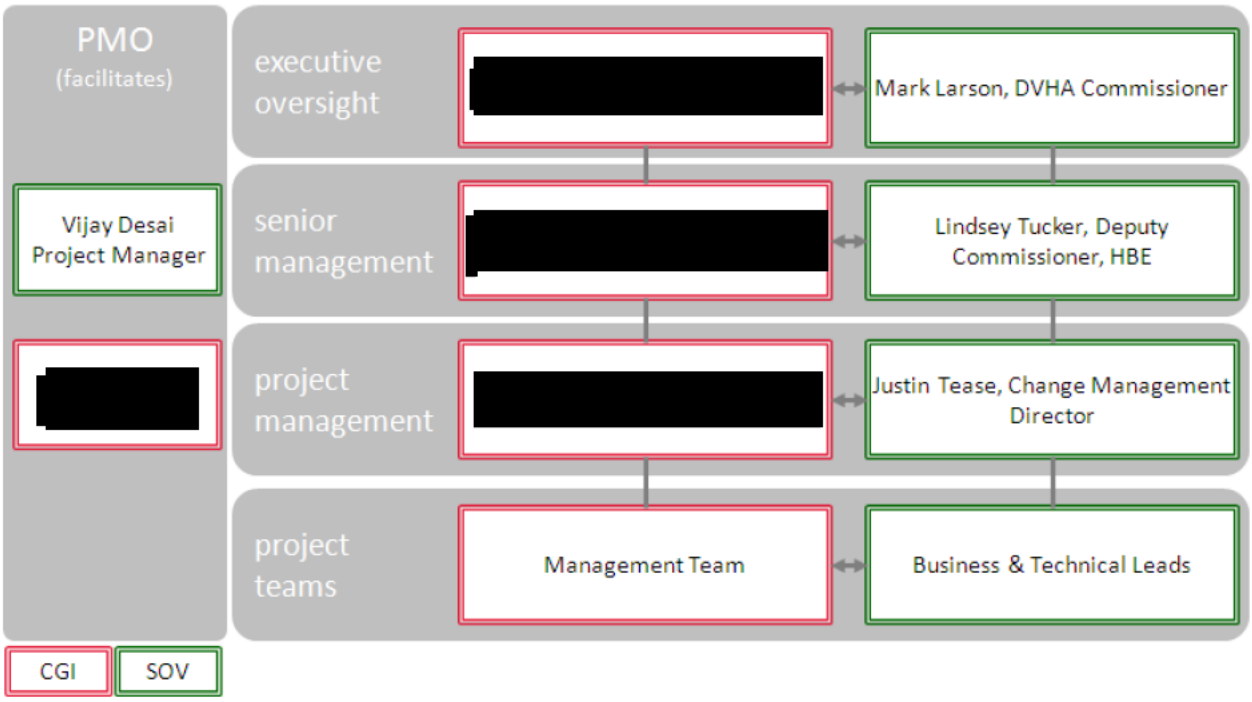


Exhibit 1 - Current PMP - Governance Structure for the SOV and CGI Teams

The following exhibit is a sample System Integration Project Organization and Governance model followed by and exhibit that describes roles and responsibilities that emphasizes collaboration and accountability. These roles and responsibilities should be defined and agreed upon in the PMP.

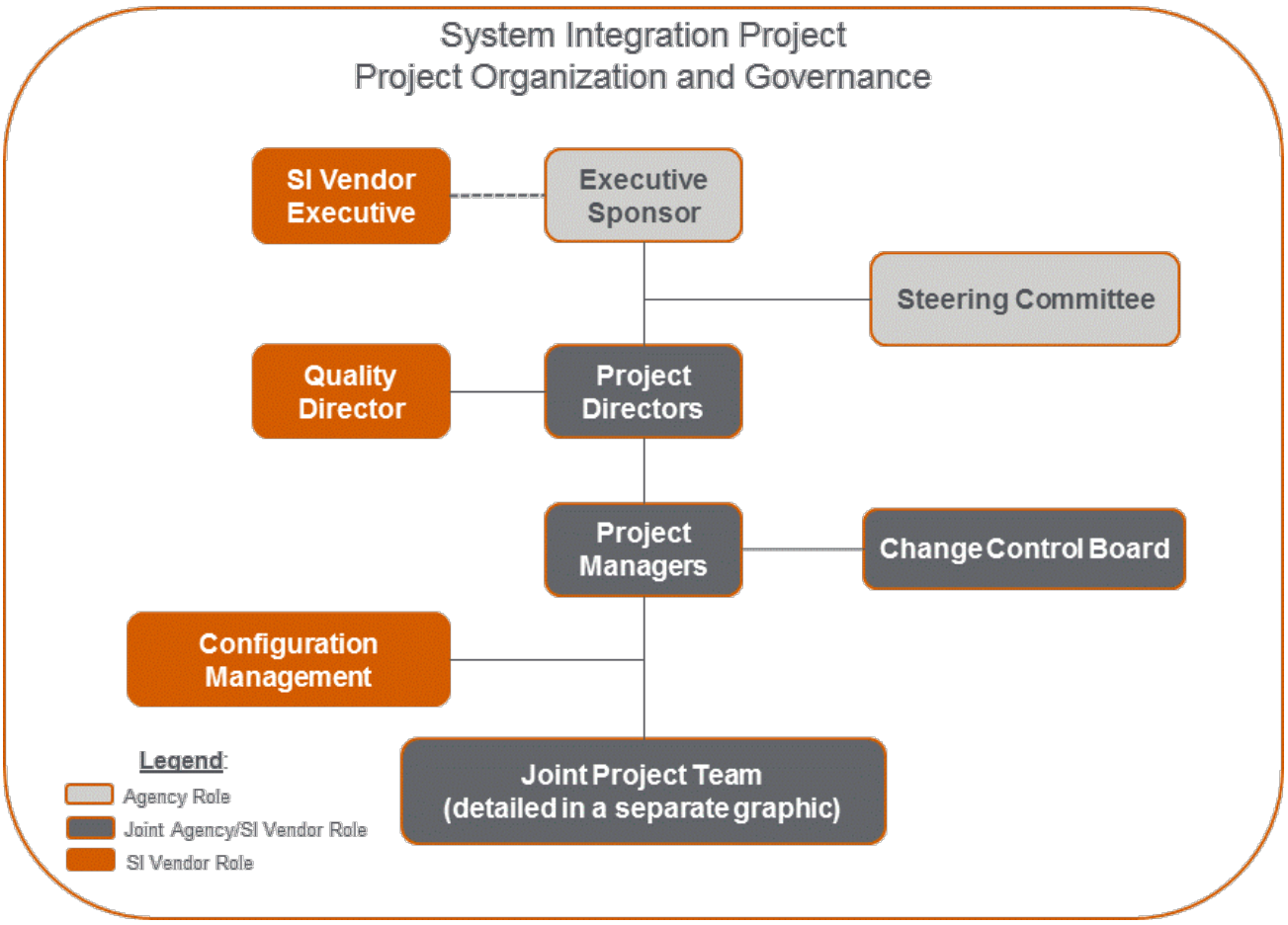


Exhibit 2: Sample - System Integration Project Organization and Governance Model

Sample – System Integration Project Governance Model

Roles and Responsibilities

[Agency Name] is the overall responsible entity, with its collective representatives and organizational units, for the project. [Agency Name] responsibilities include:

- Requesting and securing project funding
- Ensuring sufficient resources
- Reviewing and approving commitments to other agencies and entities
- Reviewing, approving, and supporting project management tools
- Championing the project

Executive Sponsor

The **Executive Sponsor** is the [Agency Name] person for the project with the highest level authority for the project. The responsibilities of the Sponsor include:

- Adjudicate appeals relative to steering committee decisions
- Appoint Committee and Team members
- Attend executive requirements reviews and resolve requirements issues;
- Champion the project
- Contribute to lessons learned
- Support the project director and project manager
- Ensure project staff availability, funding, and contract management
- Ensure user and sponsor acceptance of Project Deliverables and Product Deliverables
- Participate in planning sessions
- Provide management review

Review/accept the initial risk assessment, management plan, project plan, and budget

Steering Committee

The **Steering Committee** provides governance over the direction and support of the project. The steering committee is chaired by the project director. The steering committee member responsibilities include:

- Attendance and participation in steering committee meetings;
- Review and acceptance of deliverables;
- Review of project documents;
- Help to balance long term objectives with closer term project details;
- Review project funding and expenses;
- Champion the project; and,
- Contribute to lessons learned (after major milestones/releases as well as at the end of the project).
- Approve changes to project plan, contract or deliverables.

Project Directors

The **Agency Project Director's** primary responsibility is to provide leadership direction to the team and serve as the point of contact for agency leadership communication. The project director:

- Plans, directs, and oversees the project (including, that deliverables and functional requirements are achieved as defined in the SOW and subsequent project plans)
- Reviews and resolves, or escalates project issues not resolved at lower levels
- Directs State resources assigned to the project, serves as the primary liaison among the project and the Executive Sponsor and Steering Committee, and escalates decisions and issues/risks, as needed
- Provides the agency project manager direction regarding the agency's day-to-day project responsibilities
- Coordinates project-related issues with other related State efforts
- Acts as SI's principle [Agency Name] interface
- Coordinate assignment of temporary personnel to backfill for SMEs assigned to assist with the Design and Implementation Phase of the Project

The **System Integrator (SI) Project Director** has ultimate responsibility for oversight and delivery of the scope of

work specified in the contract. The SI Project Director works collaboratively with the [Agency Name] Project Director to monitor project status, resolve issues, provide resources to the project, and interact with the Executive Steering Committee.

Provides the [Agency Name] Project Director with summarized project status information, supported by draft materials, with the assistance of the [Agency Name] Project Managers, for presentation to the Steering Committee. Additionally, the [Agency Name] Project Director is included as the first level in any escalation of project issues.

Agency's Project Manager

The **Agency Project Manager's** primary responsibility is to manage the project. The project manager:

- Develops initial management and project plans and schedules
- Establishes leadership for a coordinated project effort
- Facilitates documentation of project assumptions, constraints, and critical success factors;
- Contributes to lessons learned
- Facilitates development of the initial risk assessment and ongoing risk management;
- Facilitates meetings
- Ensures that project tasks are assigned and tracked to project schedules
- Establishes and adheres to plans for project change, risk, communication and quality;
- Reports on project status
- Generates the Project Close Report

In addition, specific oversight activities for the project manager include:

- Certification Gates (ensure all documentation is in order)
- Ensure Agency personnel are available to support project as defined in individual plans
- Address any key actions that arise

The SI Project Manager, in concert with the [Agency Name] Project Manager, manages the day-to-day operations of the Project Connect. The SI Project Manager is responsible for:

- Delivery of the Project solution and deliverables that meet [Agency Name]' s acceptance criteria
- Delivery of the project on schedule and within budget as defined in the contract, project charter, and project work plan
- Management of SI resources and contract delivery

Provides the [Agency Name] Project Managers with detailed weekly status reports and ongoing feedback regarding issues or problems encountered. Works closely with the [Agency Name] Project Managers on a daily basis to monitor project progress; reviews the project at specific checkpoints; develops acceptance criteria, where applicable; resolves issues; and develops plans and milestones for upcoming releases. Regularly reviews and confirms with the [Agency Name] Project Managers that agency staff is used effectively on assigned activities.

Agency Team Member

The Project Team Member links the project's vision and the reality. Project Team Members:

- Attend and participate in meetings;
- Participate in the planning process;
- Complete tasks leading to completion and preparation of deliverables;
- Represent functional areas related to [Agency Name] business process and function;
- Report on progress and issues related to the project or individual tasks;
- Champion the project; and,
- Contribute to lessons learned.

The SI Team Members fill several roles including:

- The Functional Team Lead manages the functional aspects of the system so that the new system addresses [Agency Name] requirements and business process needs in accordance with the system development lifecycle methodology. The Functional Team Lead is responsible for:
  - The overall business design of the system and the day-to-day management of the Business Architecture team, which is responsible for defining and verifying requirements and providing functional testing support
  - Providing input to project planning and tracking, providing status reporting, supporting project management plans (issue and risk), and assisting with the delivery of the project on schedule and within budget
  - The Functional Team Lead works closely with the Technical Team Lead, [Agency Name] Business subject matter experts (SMEs), and other project teams to confirm that the business requirements are correctly interpreted and translate into a functional and integrated Project Connect solution. The [Agency Name] Functional Team Lead works side by side with the SI Functional Team Lead to share team

leadership responsibilities, share business and industry knowledge, transfer knowledge of the solution, and gain knowledge and proficiency for the project's development methodology and system technologies.

- The Technical Lead is the project's lead technical resource. This role is responsible for the identification, design, integration, and implementation of the technical platform upon which the application resides. This role is responsible for designing and developing a complete and thorough system architecture that provide integration of infrastructure components, and is responsible for planning for system performance, reliability, and flexibility.
  - The Technical Lead also heads the technology team and is accountable for the day to day management of the team. This role is responsible for providing project planning and tracking, providing status reporting; supporting project management plans, including issue and risk management plans; and assisting with the delivery of the project on schedule and within budget.
  - The [Agency Name] Technical Lead works side by side with the SI Technical Lead to share team leadership responsibilities, gain an understanding of the technical infrastructure design, and gain knowledge and proficiency to support the project's technical infrastructure.
- Technology Analysts/Developers design, program, and modify software-programming applications and software components. They write code, complete programming, and unit test software components assigned to them, including legacy interfaces and data conversion. They are responsible for analyzing and resolving problems identified during testing activities and providing post-implementation development support. Technology Analysts/Developers also create and update system documentation. [Agency Name] Application Developers work side by side with SI Application Developers to design, build, and support the system's software components; learn methodologies, standards, and technical products, and gain application development knowledge and proficiency.

Change Control Board

The Change Control Board (CCB) is comprised of project team members responsible for identifying, reviewing, and recommending changes to the project baselines.

The Board will meet on a periodic basis or whenever a key change or group of changes requires consideration. The [Agency Name] Project Manager will act as its facilitator and will serve as the focal point for consolidation and review of Change Requests and coordinating CCB meetings.

Other individuals may participate in CCB actions at the discretion of the Board.

Budget Analyst

The Budget Analyst supports the tracking and financial elements of the project. The primary roles would include:

- The key point of contact for questions or recommendations on funding/budget items;
- Review budget information – Budget and Program should be on the same page and both agree on information being presented to the steering committee;
- Work with project manager on how to obtain data for analysis;
- Work with Budget Office as necessary for information/reporting/etc.

2) Program Management Processes

The Project Management Plan is a formal, approved document that defines how the project is executed, monitored, and controlled. It may be summary or detailed and may be composed of one or more subsidiary plans, including:

Process Integration Management	*Scope Management*	*Quality Assurance (QA) Management*
Schedule (Time) Management	*Staffing (HR) Management*	*Risk Management*
Cost Management	*Communications Management*	*Procurement Management*

Best Practice, as specified by the Project Management Body of Knowledge (PMBOK)

Observations/Findings and Recommendations

The table below describes PMBOK-based industry ‘Best Practices’ for each management process, ‘Observations/Findings’, and ‘Recommendations’. The scope of this assessment focused on SOV/CGI governance and did not focus on intra-agency governance.

A risk assessment has been designated for each of the following processes based on PMOK’s triple constraint.

Projects need to be performed and delivered under certain constraints. Traditionally, these constraints have been listed as "scope", "time", and "cost". These are also referred to as the "Project Management Triangle," where each side represents a constraint. One side of the triangle cannot be changed without affecting the others. A further refinement of the constraints separates product "quality" or "performance" from scope, and turns quality into a fourth constraint.

The following table summarizes Optum's findings and recommendations for the specific best practice segment included in the VHC project. Optum also has assigned a risk assessment level for each of the project management triangle constraints (Schedule, Scope, Quality, and Cost).

Best Practices	Observation / Findings	Recommendation
Schedule Management – Risk Assessment: High		
Schedule Management – Describes who will be responsible for the schedule and how it will be managed. How frequently will it be updated, how will variances be addressed, and what will be considered an unacceptable variance. Schedule management is the process of ensuring that the project schedule is base lined, maintained, and managed accordingly. • *Milestones* – Describes the milestones of the project. Milestones are significant accomplishments that typically are the culmination of a series of tasks. • *Project Schedule* – A project schedule is the agreed-upon set of tasks, start dates, and finish dates used to guide and monitor the project to completion. • *Dependencies* – Summarize both internal and external schedule/project dependencies.	CGI's 'current' Project Plan was requested, but not provided. The Plan provided was dated 5/23/2014, but it does not reflect current project status. Plans provided in the past have included milestone dates that were not attainable. CGI has noted as an 'Issue' (CGI Weekly Status Report, date June 27, 2014): *'SOV has not shared a UAT Plan. This prevents CGI from planning a go-live date and will delay the next release.* This highlights poor planning and poor collaboration within the project, and does not provide corrective action for the issue. Note, the Contract (Section E – Scope Assumptions) commits CGI to: • Incorporate SOV tasks and estimated level of effort to the project schedule, throughout the lifecycle of the project. This view of SOV responsibility will be tracked through the regular project management approach facilitated by SOV and CGI project management. Note, the PMP commits CGI to: • Project Manager: Update the project plan for team's activities by COB each Friday • The updated WBS will be reviewed at the weekly status meeting • SOV and external dependencies will be reviewed during the bi-weekly status meeting; the status report will provide a three month look ahead at these milestones and dependencies.	Near-Term: Prepare an SOV Project Plan for outstanding project activities that details the SOV activities and depicts CGI milestones as dependencies. This Plan is intended to facilitate coordination but also hold CGI accountable for timely delivery of quality work products. The Plan should incorporate best practices and provides a level of detail that is consistent with the work and demonstrates dates/milestones Lesson Learned: On future projects ensure the SOW/charter and project plans include the appropriate controls to ensure SOV ownership of project activities and outcomes. These controls should first be articulated in the Contract and then in the charter and finally the PMP.

	Issues with the Plan include:
	• Integration – While some SOV milestones are depicted, an integrated schedule with SOV activities does not exist
	• Schedule – Package 2 was not implemented June 8, 2014. A schedule with revised dates does not exist.
	• Tasks – lacks sufficient detail
	  ○ Package 2 System Integration Test
	  ○ Deliverable review and approval
	• Work – work effort outlined in the plan is not commensurate with the specified tasks
	• Dependencies – not sufficiently defined to track the impact of missed dates:
	  ○ Dependencies between Package 2 and Package 3 are not sufficient
	  ○ Dependencies between Package 2, Package 3, and Maintenance and Operations are not depicted in the Plan.	

Scope Management – Risk Assessment: High		
Scope Management - Describes how the project scope will be defined, developed, and verified and how the WBS will be created and defined; and provides guidance on how the project scope will be managed and controlled by the project management team.	Nine months after (10/1/2013) implementation of the VHC solution several key requirements, including Change of Circumstance, Renewals, and SHOP, and over 2,500 non-functional requirements specified in the contract have not been met and there is no agreed upon plan for delivering these. The current PMP documents a Change Management Process that contributes to project governance issues. Approximately 130 Change Requests (CR) are not approved, while 10 have been approved. Contributing factors include: • Requirements are not specified in accordance with industry standards; therefore it's difficult to distinguish defects from new requirements (see below for further description) • There's no agreement on pricing with CGI which does not allow for appropriate cost estimation for each CR. Note, the current CGI PMP states: • If the parties reach an agreement on a CR in writing, and	Near-term: • A mutually agreed upon estimating model to determine the work effort for a CR is necessary for effective Scope Management. An agreed upon estimating model, along with the rate card in the Contract, shifts the focus from CR pricing to impacted artifacts, which then drives pricing. An additional benefit to this approach includes the knowledge transfer that occurs during discussions on impacted artifacts. • Update the PMP to include approved CRs and schedule impacts • Re-baseline the PMP in accordance with industry best practices. • Apply IEEE standards to all new requirements and refine existing requirements in conjunction with the development of testing work products.

	the CR is executed by authorized representatives of the parties, the terms of the Contract shall be modified accordingly…..
	• But currently there is typically disagreement between CGI and the SOV.
	
	The activities to deliver the requirements specified in the CR are not specified in the PMP.
	
	VHC requirements do not comply with industry best practices, necessary for effective Scope Management (IEEE 830 – Recommended Practice for Software Requirements Specifications (SRS)):
	
	• Correct – an SRS is correct if, and only if, every requirement stated therein is one that the software shall meet.
	• Unambiguous – an SRS is unambiguous if, and only if, every requirement state therein has only one interpretation
	• Complete – an SRS is complete, if and only if, it include the following elements:
	  o All significant requirements, whether relating to functionality, performance, design constraints, attributes, or external interfaces.
	  o Definition of the responses of the software to all realizable classes of input data in all realizable classes of situations.
	  o Full label and references to all figures, table, and diagrams in the SRS and definition of all terms and units of measure
	• Consistent – an SRS is consistent if, and only if, no subset of individual requirements described in it conflict
	• Ranked for importance – An SRS is ranked for importance if each requirement in it has an identifier to indicate either the importance or stability of that particular requirement (i.e., essential, conditional, optional).
	• Verifiable (testable) – A requirement is verifiable if, and only if, there exists some finite cost-effective process with which a person or machine can check that the software product meets the requirement.
	• Modifiable – An SRS is modifiable if, and only if, its structure and style are such that any changes to the requirements can be made easily, completely, and consistently while retaining the structure and style.
		Lessons Learned:
		
		• Apply the IEEE standard to new or changed requirements.
		• A clearly defined the Change Control governance model is critical to project success.

	• Traceable – An SRS is traceable if the origin of each of its requirements is clear and if it facilitates the referencing of each requirement in future development or enhancement documentation. Forward traceability of the SRS is especially important when the software product enters the operation and maintenance phase. As code and design documents are modified, it is essential to be able to ascertain the complete set of requirements that may be affected by those modifications.	

Quality Management – Risk Assessment: High		

Quality Management – Describes the approach that will be followed to manage and ensure product quality during the project.
• Describes what metrics will be used to measure quality and how any necessary quality corrections will be implemented.
• Quality is defined as the totality of features and characteristic of a product that bears on its ability to satisfy stated or implied needs.
 	
Quality management is the process of defining the strategy and methods the project will deploy to ensure the project's deliverables are of acceptable quality before they are delivered to the client.
	There are several Quality Management issues that can be categorized by People, Process, and Technology (tools/environment). Detailed findings are included in Optum's QA Review deliverable.
	
	The project's PMP includes a Quality Management section that specifically addresses 'deliverable quality', with a deliverable review approval process that contributes to the project's governance issues.
	
	Of 48 deliverables, 17 are 'approved', based on CGI's deliverable tracker, dated June 2014. This highlights both a quality and a process problem.
	
	An effective Quality Management process is not limited to testing and is intended to address quality issues prior to Testing in the system development lifecycle.
	
	The volume of outstanding defects, nine months after initial implementation (10/1/2013) indicates the Quality Management process is not effective.
	
	A significant contractual commitment (Section E – Scope Assumptions) by CGI is outlined below:
	
	• A System readiness certification document with accompanying test results to the state based on the tasks as described in System readiness assessment and that the following criteria have been met by the System:
	  ○ System meets all functional requirements
	  ○ System meets all non-functional requirements
	  ○ System has passed the System Qualification Test with no known major errors
	  ○ Successful execution of the test scripts(s) for the current test phase.
	  ○ No open critical, major, or average severity defects unless the issue is determined to be low impact and low risk
	  ○ Stability of all modules and components in the test environment.
	• This readiness certification will be the statement that the System has passed all internal testing and is now ready for UAT.
		Please refer to Optum's QA Review deliverable for recommendations.

	Optum's QA Review deliverable documents the project's QA issues, including concerns with the testing process.	

Cost Management – Risk Assessment: High		

Cost/Budget Management – Describes how cost and cost variances will be managed. This section summarizes the cost and effort estimates of the project, documents any known factors that may increase those estimates, and defines how they will be measured throughout the project's life. Cost management is the process of ensuring that a project is completed within the approved budget and that cost variances are proactively managed throughout the project.	The Contract (Section E – Scope Assumptions) commits CGI to:
	• The Vendor is responsible for developing a Cost Management Plan that indicates how project costs will be incurred, controlled, and reported. The plan must include the finalized cost and budget for the project. Cost-related progress report formatting will be developed and included by the Vendor, consistent with State requirements and format, and must include a tracking of costs to the project budget baseline.
	This requirement was removed in a later amendment. As such, CGI's PMP does not include a Cost Management Plan and SOV does not have a project-specific Cost/Budget Management Plan.
		SOV should have a Cost/Budget Management Plan to track project funding, budget, and expenses.
		Additionally, this Plan should:
		• Document roles and responsibilities
		• Describe governance relating to:
		  ○ The allocation of expenses to comply with SOV and federal guidelines.
		  ○ Fiscal-year budget management
		  ○ Reporting

Staffing Management		
Staffing Management – Describes the approach for staffing the project and how resources will be managed throughout the life of the project. This includes resource estimates, project organization charts, roles and responsibilities, and identification of training needs and on-boarding of resources.	The Contract (Section E – Scope Assumptions) commits CGI to the following in its Staffing (HR) Management Plan: • The roles and responsibilities for staffing the different activities, articulating what the Vendor will need to provide and what the State should provide; includes a project-wide RACI chart. **A detailed Staffing Management Plan is described in the PMP, yet not followed.** The Staffing Management Plan includes a staffing model through 2013, with a commitment to update monthly, yet an updated forecast for 2014 has not been provided. As reported in CGI's 6/20/14 Status Report: • **If SOV requires CGI resource support for UAT, then the resources may not be available due to Pkg3 activities** The CGI PMP indicates: • CGI is fully committed to the successful delivery of our projects within the prescribed timeframes. As a company, our highest level of management is engaged and has direct visibility into our projects. • We have identified staffing needs for the VT HBE project – the following is a forecast of staff by month as of February 25, 2013. This will be provided to SOV monthly along with the actual staff levels. • CGI will report the replacement of Key Staff to the SOV IT Manager, provide a resume for the replacement, and will be subject to the SOV's written approval (not to be unreasonably withheld). The Staffing Management Plan does not include SOV resources. Organization Change Management team is not addressed in the Staffing Management Plan. The CGI staffing issues highlighted above and their inability to meet key project milestones indicates their staffing is not sufficient to meet DDI and M&O commitments.	Near-term/lesson learned: Both SOV and CGI should provide staffing models for the duration of the Contract. The Staffing Management Plan should be a clearly articulated staffing plan that address staff acquisition, training, and on-boarding based on specific project resource requirements. In addition, the Staffing Management Plan should be updated on a consistent basis agreed upon by CGI and the SOV. An Organizational Change Management Team should be created to facilitate the implementation of new VHC functionality. The benefits of an Organization Change Management team: • Assist with determining the organization's readiness for change and their capability to change. This includes understanding and communicating the business process reengineering aspects of a new/enhanced solution. • Facilitate internal and/or external stakeholder communications.

Communications Management		
Communications Management – Describes the approach to communicating information to project stakeholders and the public. Outlines the key internal and external stakeholders that comprise the communications audience. Define the approach that will be used to communicate with these stakeholders, including messages, messengers, vehicles, and timing	A Communication Management Plan is described in the CGI PMP. Review of CGI's Weekly Status Report suggests: • The report's structure includes sections typically included in a weekly report (except Action Items, mentioned in the PMP, are missing from the report). • CGI's 5/16/2014 report mentions in the Overall Summary that Package 2 is on-schedule for 6/8/2014 deployment. The following week's report mentions several activities in the Overall Summary but is silent on the Package 2 deployment date. Note, the Contract (Section E- Scope Assumptions) commits CGI to report weekly: • Projected completion dates compared to approved baseline key dates • Actual/projected Project Work Plan dates versus baseline Project Work Plan milestone dates This information is not included in the Weekly Status Report. Additionally, the report includes details without analysis. For example: • The report communicates project activity, but not the status in context to the plan. • There are risk indicators flagged 'red' without corrective actions noted.	Near-term: CGI should revise the Weekly Status Report to comply with Contract commitments. Lesson Learned: The Weekly Status report should be more transparent and emphasize 'course correction' activities. Weekly status should be reported in context to the Plan and highlight CGI's performance against dates in the plan.

Risk Management		
Risk / Issue Management – Describes how risks/issues associated with the project will be managed. Outlines what risk/issue management activities will be conducted and how they will be performed, recorded, and monitored throughout the life of the project. Risk management is the process of identifying, assessing, responding to, monitoring and reporting risks.	Risk Management does not appear to be effective, as risk mitigation and risk avoidance have not been preemptively addresses the project's challenges. The CGI PMP includes a Risk Management Plan with the description of a process flow, and a log to facilitate tracking and reporting project risks. A separate plan describes the process flow and log for project issues. Neither plan sufficiently describes the escalation process. Currently, CGI and the SOV representatives meet on Tuesday and Thursdays to review and discuss issues/risks and related contingencies. The risk below is included in CGI's 6/27/2014 Weekly Status Report: is representative of the project's lack of meaningful risk management: • If UAT identifies 3.3.2.8 defects, then limited options available for providing fixes.	Lesson Learned: A joint PMO, staffed with CGI and SOV resources, must effectively assess the impact of risks on the project costs, schedule, scope, and quality. This assessment should be completed weekly or more often as risks are identified.

Procurement (Contract) Management		
Procurement Management – Describes how goods and services will be procured from outside the project/organization. It includes the contract management and change control processes required to develop and administer contract issues by authorized parties.	The CGI PMP includes a Contract Management Plan. Provides visibility and transparency and addresses how CGI will identify, track, and report on contract terms and conditions to demonstrate how and when they are fulfilled and invoices will be issued. • A deliverable tracking process is described in the Plan, but not followed. • A Performance Management Plan is specified, but not followed. It includes: ○ **Client Satisfaction** – CGI uses a semi-annual client satisfaction survey (Client Satisfaction Assessment Program (CSAP)) to obtain written targeted feedback from client executives and project management	Near-Term: CGI's leadership team should be familiar with the commitments they have made in their project deliverables. Lesson-learned: The joint PMO should define contract commitments and enforce them.

	about the performance of the team. o **Project Performance** – the PMO's primary mechanism for evaluating the team's performance against the baselined schedule is the Schedule. A series of dashboard reports are used to report on the status of milestones, deliverables, and tasks. o **Deliverable Quality** –the team will maintain, measure, and report metrics on the number and types of deviations found in project deliverables. o **Adherence to Solution Service Level Agreement (SLA)** – during production use, reports will be made available to confirm production SLAs related to system performance and service delivery have been met. Examples of CGI commitments not met include: • Each month a tracking report of milestone progress will be made available to SOV including the due dates for milestones per the approved base lined plan, and Actual or Forecast completion dates. Milestone dates that are forecast to be, or are actually late will be shaded yellow, and late milestones that will impact federal milestones will be shaded red. • The performance of tasks against the schedule will be managed on a day-to-day basis through the project plan on the CGI Microsoft Project server instance. Hours will be tracked against planned for tasks and assigned resources. • Task progress will be reported to SOV through weekly updates to the SOV integrated project plan. Each week, CGI will update the percent complete on tasks. Further commentary on tasks that are late or expected to be late will be included in the weekly status report. Review of these commitments with CGI's leadership team indicated they were not familiar with them.	

3) High Risk for Schedule Non-Compliance

Schedule compliance is "High" risk to the on time completion of the remaining project scope. As mentioned earlier, this risk assessment considers:

- CGI and the project team's track record for meeting project milestones
- The lack of collaboration between CGI and SOV
- The lack of defined and disciplined processes, and related controls
- The lack of an integrated schedule that outlines delivery dates for the remaining requirements.

This assessment is based on CGI's delivery track record to-date and lack of a comprehensive integrated project plan.

Observation/Finding	Recommendation
Nine months after (10/1/2013) implementation several critical functional requirements, including Change of Circumstance, Renewals, and SHOP, and over 2500 non-functional requirements specified in the contract. There isn't a current schedule with revised project milestone dates for delivering outstanding requirements. The last published Plan (5/23/14) indicates Package 2 CoC would go-live June 8, 2014 and Package 3 Renewals would go-live July 17, 2014. These dates are not attainable. Interim milestone dates are consistently missed. Exhibit 3 below highlights (yellow) deliverables not approved and dates that have been revised between Amendment #1 and Amendment #3. Note, this table is a subset of deliverables.	In lieu of a CGI project plan, SOV should prepare a project plan with dependencies on CGI Milestones. These milestones will be used to hold CGI accountable and highlight the impact of CGI delays on overall project milestones. SOV must balance a 'date driven' plan with a 'work/resource driven' plan to define milestones that are achievable.
The focus on quality issues diverts the project team's attention from delivering new functionality. CGI is not staffed to deliver the remaining requirements and M&O activities. CGI June 27, 2014 Status Report includes the following risk: *If SOV requires CGI resource support for UAT, then the resources may not be available due to Pkg3 activities.*	As contractually specified, CGI should deliver an updated comprehensive plan, based on a staffing model they contractually committed to, and one that will deliver the remaining scope at the quality agreed upon in the original contract.

Observation/Findings	Recommendation
Until there are substantial changes to project governance and processes, the same processes will likely result in the same outcomes. The following findings are based on CGI's deliverable tracker, dated June 2014: There are 32 deliverables specified in the PMP: • 12 are 'replaced' • 8 are 'approved' • 12 remaining deliverable are not approved 16 additional deliverables (added via 'Change #5') have been added since the PMP was approved (February 21, 2013): • 9 are 'approved' The emphasis in this report has been on people and process, additionally there are technology (e.g., platform and tools) constraints impacting the team's ability to deliver on a timely basis. The issues are documented in the remaining Optum Assessment deliverables.	Please refer to all of the above recommendations.

Deliverable #	Deliverable Milestone	Status	Amend #1 Est Date	Amend #2 Est Date	Amend #3 Est Date
D-14	Requirement Traceability Matrix (RTM)	Approved	4/12/2013	4/5/13	5/9/13
D-15	Requirements Specification Document (RSD)	Approved	4/25/2013	4/18/13	5/9/13
D-16	Test Plan	Approved	5/9/2013	5/8/13	6/25/13
D-17	Business Rules	Pending	5/9/2013	5/9/13	6/25/13
D-18	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
D-19	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
D-20	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
D-21	Interface Control Document	Closed	5/1/2013	4/23/13	6/25/13
D-22	Training Materials	Pending	9/30/2013	8/29/13	6/25/13
D-23	User Manuals	Pending	9/30/2013	8/29/13	7/22/13
D-24	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
D-25	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
D-26	Implementation Plan	Not Approved	7/22/2013	7/8/13	9/10/13
D-27	Contingency / Recovery Plan	Not Approved	7/22/2013	6/11/13	9/18/13
D-28	Data Use Agreement/Data Exchange Agreement/Interconnection Security Agreement	Approved	7/22/2013	6/20/13	9/30/13

D-29	Test Reports	Pending	9/18/2013	8/20/13	9/30/13
D-30	Go-Live Document	Pending	11/7/2013	9/16/13	9/30/13
D-31	Operation & Maintenance Manual (O&M)	Pending	9/10/2013	9/3/13	9/30/13
D-32	Training Plan	Approved	5/22/2013	5/16/13	11/7/13

Exhibit 3: Deliverable Status - Based on CGI Deliverable Tracker (June, 2014)

4.0 RECOMMENDATIONS

This section provides a consolidated list of recommendations.

- Establish a SOV project management team that manages the overall project, with input from each contractor (including CGI). This team's responsibility includes:
  - Prepare an integrated master project schedule with SOV and Contractor (including CGI) tasks, work effort (hours), duration (schedule), and dependencies. This plan should include: Outstanding functional requirements, non-functional requirements, agreed upon new functionality, and M&O tasks.
  - Prepare a SOV-based PMP based on an updated integrated project plan, project status, and processes.
    - Include a cost/budget management plan and staff accordingly
    - Include an estimating model for change requests to determine the project impact: resources, schedule, and cost
  - Similarly, revise system development life cycle processes (e.g., QA and M&O) and staff accordingly.
- Initiate transition to 'operationalize' the project.
  - Identify the appropriate resources to lead and staff the organization
- Share lessons learned with upcoming SOV large-scale system integration projects.

OPTUM™

Vermont Health Connect HIX

Quality Assurance Review

8/18/2014

TABLE OF CONTENTS

1. .....INTRODUCTION 3
2. .....BACKGROUND 5
3. .....METHODOLOGY (PROCESS) 7
4. .....FINDINGS AND RECOMMENDATIONS 13
5. .....STAFFING 24

1. INTRODUCTION

The purpose of this deliverable is to:

- Review UAT testing methodology related to the upcoming Change of Circumstance release.
- Review testing methodologies and processes used by CGI in the testing of the VHC application. This review includes unit/component testing, system/ End-to-End testing, UAT testing, and regression testing.
- Provide an assessment on testing resources and business analysts involved in testing to ensure the proper business acumen is being applied to the testing effort.

After review of the project's QA documentation and interviews with both SOV and contractor staff, Optum has concluded that, while CGI's Test Plan of record (VHC Test Plan – Version 4.0 which is dated September 25, 2013) has some inconsistencies, such as contradicting End-to-End testing responsibilities, and does not fully detail how the data will be refreshed, it has many of the best practices associated with a Quality Test Plan. The major issue is that these practices were not followed. In addition, a lack of SOV formal approved test plans and other quality documents has resulted in a lack of accountability by CGI as it relates to testing. In addition, the lack of an additional environments prevents any testing of multiple releases and limits Performance testing to off hours testing, and does not fully simulate production.

Key Findings (Summary of Gaps)

Optum's assessment is based on the key findings as it relates to Quality, Reporting, Requirements, UAT, Automation, Performance, and Environments. This summary of gaps (deficiencies) include, but are not limited to:

- CGI attempting to promote code to live (package 2) despite the presence of Severity 1 and Severity 2 issues that would cause major problems in production.
- End-to-End testing deficiencies resulting from a lack of clear ownership . Both the SOV and CGI contend the other has accountability for End-to-End testing. Best Practices would indicate this is a phase of testing that belongs with QA/SQA.
- An integrated test environment is necessary to support different phases of testing. Currently, there is one test environment. This prevents any testing of concurrent releases, or the ability to test production fixes in a Test environment In addition, the lack of a Performance environment limits any performance testing to off hours, and the Test environment does not provide an environment that is production like in order to completely test performance.
- .
- Service level agreements do not exist for defect remediation during the testing phase, resulting in undefined timelines for receiving code fixes.
- Root Cause analysis is not performed, which prevents lessons learned improvements.
- There is no true UAT team.
- The majority of test cases that are in the repository are high level scenarios, and are not detailed test cases which would be a best practice. Detailed test cases become more needed when a high turnover rate or augmented staff need to execute test cases during a release.
- There is lack of formal Entrance/Exit criteria review and approval to initiate or conclude a phase of testing.

Recommendations

Optum's assessment results in the following key recommendations:

- The SOV needs to resolve the End-to-End testing responsibilities in order to properly test releases prior to deployment to production. Best practices indicate this is a phase of testing that belongs with QA/SQA. This is not a typical responsibility of the business.
- The SOV needs to assign a UAT Test Manager and team. This manager needs to instill the proper testing fundamentals to combine with the already existing subject matter experts to form a true business test team.
- An investment in an automation framework should be made. This will allow a regression to be run with minimal staff prior to releases being deployed to production. IT should be driving the framework and automation of the testing scripts.. Capturing the regression cases that are needed are typically a joint effort between IT and the business. The execution of this phase is the responsiblilty of QA with assistance from the business if needed.
- There needs to be performance testing strategy developed to properly capture the requirements in addition to establishing key benchmarks for a release.
- Test data planning needs to be done in order to facilitate End-to-End testing. This will also instill confidence in the SOV's partners by having more robust test cases.
- The SOV needs to invest in and upgrade additional environments including:
    - Performance environment as this will allow performance testing to occur and not impact IT/UAT testing.
    - Additional test environments as this will enable concurrent testing of releases.
    - Pre-Prod environment that is fully integrated that will allow for production fixes to be tested prior to being deployed to production.
    - Disaster recovery environment needs to be built out fully and tested.
- Update, approve, and maintain all required documents including but not limited to:
    - Review of requirements
    - Test Plans(System, UAT, Performance)
    - Requirement traceability Matrixes
- Complete the development, testing and implementation of the disaster recovery plan.
- Review and update the current defect management process, and ensure that this process has applicable SLA's, and that the process is enforced.
- Enforce the Entrance/Exit criteria across the SDLC.

2. BACKGROUND

The purpose of the Quality Assurance Review deliverable is to document the status of the current release and to provide recommendations to reduce gaps discovered in the overall testing process.
Optum partnered with appropriate resources from the SOV and vendor(s) to understand the defined program and testing methodology utilized to deliver the current HIX application. Based on the defined methodology implemented, Optum will perform a historical review of the processes executed and artifacts created in the delivery process. Optum will look for evidence of industry best practices being followed and documentation across all phases of the SDLC. Within the testing phase specifically, Optum will review all existing test strategy/plan documentation at both the program and individual testing phase level and identify any gaps in these artifacts. Additionally, Optum will request access to any/all existing test management tools or data repositories to review thoroughness and end SOV disposition of all test execution results material.

Upon completion of the three week review led by an Optum QA Manager, Optum will provide a summary of gaps identified within the QA life cycle and provide recommendations for improvement, including testing tools. This review prioritizes UAT as it relates to the upcoming Change of Circumstance release.

The team met with the following SOV and vendor team members:

- State of Vermont
  - Mark Larson
  - Lindsey Tucker
  - Justin Tease
  - Jill Finnerty
  - Richard Ketchum
  - Tony Thibault
  - Melissa Rancourt
  - Tim Metayer
  - Peter Rhoades
- CGI
  - [redacted]
- Exeter
- Benaissance
- Archetype
- Blue Cross Blue Shield

The team reviewed the following project documents:

CGI Documents and Processes
• Test plans
• Test cases
• Test environment details
• Testing status reports
• Requirements document
• Requirements traceability matrix
• Defect process
• Defect metrics
• Change request process
• SOV acceptance process document
• List of remedy tickets in Live

Information requested from CGI and not made available to the Optum team includes:

- Discussion on the process, roles, schedule, and plans during the following walk-throughs
  - CGI walkthrough of Unit Test/System Test/UAT/Regression
  - CGI walkthrough of Test Plan for current release
  - CGI walkthrough of Requirement Traceability Matrix
- Copies of the test scenarios and scripts used for performance testing
- Parameterized files for performance testing used to pass in data (and what they represent). These files are used to provide data in buld for used during performance testing.
- Load test results from the last six tests that have been executed Load testing is one process of performance testing. For clarity, it is a process that puts demand on a system and measures its response. Load testing is performed to determine a system's behavior under both normal and anticipated peak load conditions.
- End-to-End data flows that have corresponding description of the data connections.

Optum provided CGI several questions along with a meeting request to address these questions. These requests were not met. Questions included:

- During each regression, how do you refresh the data in order to execute the scripts?
- How many of the scripts require database intervention?
- On the average, how long does each test case take to execute?
- Are there any scripts automated? If so, how often do they need to be updated?
- When testing for roles and responsibilities, do you use generic ids/PW for each role?
- Is the majority of your day spent executing?

- Do you have a regression data bed?
- Are there agreed upon SLAs for remediating test defects?
- How defect severity is assigned, and is there a review process to ensure client concurs?
- Is there a detailed test execution plan (day over day expectations of test cases executed)?
- What is the frequency and format of testing status reporting and who is the report sent to?

Optum requested the following Information from CGI and was informed the reports/signoff's do not exist:

- Root Cause Reports
- Entrance/Exit Criteria
- Test Automation Test Plan
- Performance Test Plan

3. METHODOLOGY (PROCESS)

The following defect management diagrams and tables are based on industry best practices using ALM. The defect management process may be tailored over the course of a project if improvement opportunities are identified. All changes are then communicated with stakeholders. The below tables identify these best practices.

This page intentionally left blank

[redacted]

[redacted]

Exhibit 1 – Defect Management Process in HP ALM

This page intentionally left blank

State	Description	Responsibility
[redacted]		

Exhibit 2 – Defect Status Flow

4. FINDINGS AND RECOMMENDATIONS

This section of the document describes specific quality findings and recommendations.

- CGI is attempting to promote code to live (package 2) even though there are clearly issues that will cause major problems in production. For example:
  - There are a number of Severity 1 and 2 defects that still need to be resolved in both System and UAT testing. The majority of these defects have no ETA, and there's also debate on each defect's severity level.
  - CGI has stated that End-to-End testing is the responsibility of the SOV where best practices clearly state the Business, in this case the SOV, does not have the necessary technical skills to test this phase of the SDLC, and that QA or SQA should be responsible for End-to-End testing.
  - There are issues around SOV partners (BCBS, in particular) where both the SOV, and in this case BCBS, feel there has been inadequate testing done.
  - There also has been no evidence of entrance/exit criteria being followed.

- Other findings include UAT testing needs to follow proper UAT testing methodology. Although there is expertise in subject matter expertise, there is no knowledge of testing methodologies or processes.
- A true UAT testing team needs to be created Business should build out a UAT team. Industry Best Practices indicates this team normally comprises of a combination of resources that are SME's and testing analysts. The team would typically be led by a Testing Manager/Lead to ensure that the proper processes are being followed. The size of this team would vary depending on the size of the release. Also, this team should be on a rotating timeframe so that they do not lose the business knowledge.
- There is an inadequate number of environments that puts releases in jeopardy, and a need for more clarity in the daily testing status updates. Recommendation is that all environments should be fully integrated, and are as follows:
    - Test 1
    - Test 2
    - Pre-Prod(replicate of production/live)
    - Production/Live
    - Performance
    - Development/Staging
    - Disaster Recovery

Although a more detailed effort was focused on findings based on the current release, these findings and recommendations are applicable to not only the current release, but, also the program in general. An inclusive list of findings and recommendations is listed below and categorized as follows:

- Quality process and methodologies
- Reporting
- Requirements
- UAT
- Automation
- Performance
- Environments

Observation / Findings	Recommendations
Quality	
High staff turn-over rate on the SI which impacts ability to deliver on time and creates additional effort due to ongoing knowledge transfer activities.	There are many key testing roles(QA Manager, QA Project Lead) that were recently added. There needs to be stabilization on key roles. One of the most effective way to reduce this turnover is to have a positive work environment, and to recognize outstanding performance.
There are 18 BCBS End-to-End test cases for the current release, but, according to SOV partners, there are missing scenarios and these cases were not signed off.	Signoff of test scenarios by the appropriate stakeholders would prevent this and would ensure that the business is in agreement of what is being tested.

Questions to the SI from Optum, along with a meeting request, were not made available to the Optum team including: • During each Regression, how do you refresh the data in order to execute the scripts? • How many of the scripts require database intervention? On the average, how long does each test case take to execute? • Are there any scripts automated? If so, how often do they need to be updated? • When testing for roles and responsibilities, do you use generic ids/PW for each role? • Is the majority of your day spent executing? • Do you have a regression data bed? • Are there agreed upon SLAs for remediating test defects? • How is defect severity assigned, and is there a review process to ensure client concurs? • Is there a detailed test execution plan (day over day expectations of test cases executed)? • What is the frequency and format of testing status reporting and who is the report sent to?	Without conversation and answers to our questions, we cannot make an accurate statement on the SI's skillset. However, we can say, based on observation, there has been a clear lack of accountability in the Quality process area.

Observation / Findings	Recommendations
Reporting	
A daily testing status is reported.	There is a daily testing status, but this needs to be revised to include daily risks/issues and a description of severity 1 and severity 2 defects.
Defects are managed with various tools. There should be one tool that has the complete list of defects. This is specified in the Test Plan, but has not been implemented.	The strategy is in the test plan that each application needs to document defects in ALM regardless of the individual defect tool that the application uses ie Jira, Remedy. This process needs to be followed in order to have a true reflection of the current state of issues.
There is only one test plan that has been signed off by the SOV, and this was in September, 2013. This was an industry standard Test Plan, but the process described in the Test Plan were largely not followed. By not having current signed off test plans and documentation that account for releases past the initial deployment, there is a lack of accountability on who is responsible to test certain functionality or specific phases of the SDLC.	Although there are a number of test plans, they have not been signed off. Each release needs to have a Test Plan and signoff by the appropriate stakeholders. This is a best practice to assure that all parties agree on the testing effort and what is in scope, including the responsibility of the different parties.

Entry/Exit criteria are documented in the signed off test plan, but, this is not followed on any of the testing phases.	Entry/Exit criteria are essential to the successful completion of a release. If you do not know where to start and where to finish then your goals are not clear. Exit criteria is the minimum eligibility or the set of conditions that should be met in order to close a particular project phase. Exit criteria are documented and signed off during the test planning phase and are included in the relevant test plans.
No Root Cause analysis which prevents lessons learned improvements.	At the end of each release, there should be a root cause analysis done in order to provide for a lessons learned and improve the testing process going forward.
End-to-End testing deficiencies as there is no ownership as both the SOV and CGI believe it is not their responsibility. I.e.: Best Practices clearly state this is a phase of testing that belongs to QA/SQA. This needs to be resolved asap as without sufficient End-2-End testing, the release should not be signed off or deployed to production.. The Test Plan that was approved (September, 2013) had no clear ownership of End-to-End as one part of the document indicated that CGI had ownership, and another part of the document had the SOV as owners.	The recommendation for the current release is to review the available test scenarios with SOV's partners, and receive signoff indicating approval of what will be tested. In addition, test cases may need to be added if there are scenarios that are not being covered per the requirements for this release. Going forward, QA, and not the business should be responsible for End-to-End testing.

Observation / Findings	Recommendations
Requirements	
There are a number of requirements that are non-testable as written. Ie: ELM-053, ELM-057, ELM-084	Requirements should be reviewed and any requirements deemed not testable need to be revised.
ALMConnect is used as the Requirements Management tool.	Requirements management tool is available.. Currently, ALMComplete is the tool that is utilized to house the requirements. The next step would be to internally map the rerquirements to the test cases to make sure there is full traceability.
There is a requirement traceability matrix, but, it is incomplete as there is missing data on the matrix. Requirements not covered are EN-031 and ELM-053	Review and update the requirement traceability matrix.

Observation / Findings	Recommendations
UAT	
UAT testing consists of verifying video recordings from CGI and running high level scenarios that they created.	UAT needs to have detailed test cases. These test cases should flow from a business perspective.

There is no UAT test plan.	There needs to be a viable test plan that has signoff from the appropriate stakeholders. A Test Plan should contain at least the below section: 1.Background(platform) 2.Features to be tested 3.Features not to be tested 4.Entrance/Exit criteria 5.Test Deliverables 7 Environmental needs 8.Schedule 9.Resources 10.Risks 11.Approvals
UAT does not use ALM to execute scripts.	The absence of utilizing a testing tool makes the testing effort difficult to manage and difficult to provide metrics.
Lack of testing knowledge and methodology in the UAT area	A dedicated team of UAT testers should exist. This team can rotate periodically so that they do not lose their business knowledge. They need to be trained on proper testing techniques and tools.

Observation / Findings	Recommendations
Automation	
Based on the documents provided, we could not identify an automation test strategy or test plan from CGI or the State of Vermont UAT test team. We did find a general comment on CGI's test plan that stated Automation would be utilized when applicable. Access to the CGI test participants could not be established during this assessment period to inquire about the document. In speaking with the CGI and the SOV UAT Test Manager, it is our understanding that a formal test plan or strategy was not documented. The strategy appeared to be ad hoc in nature based on our conversation, but we did not directly ask if he had specific documentation regarding test strategy or planning. We were trying to understand the type of testing being created and executed and the amount of changes the application is experiencing based on a test development schedule. We were unable to assess a test strategy addressing application stability.	An automation strategy and team needs to be established early to properly support the scripting of the application and to understand and support test case regression development.
Based on our conversation with the State's UAT Test Manager, we discovered that the use of the open source automation tool "Selenium" is being used to assist the State UAT testers. The Test Manager trained the UAT test team to use the Selenium IDE (which is an available record and playback Selenium plugin in the Firefox browser) to perform record and playback scripts that were primarily utilized to relieve the UAT testers from entering the same redundant application flow required data into web pages that assisted them in getting to different areas of the application to perform more in depth manual testing. The risk of using the Selenium IDE only is that you can only use it with the Firefox Browser. The UAT tester is not testing the application in Internet Explorer, which the Test Manager stated most of the SOV population uses to access the Vermont HIX site.	In order to have automation, an investment in a tool needs to be made that fits the application and the type of testing that needs to be performed. Selenium is not currently utilized by the SOV as an automation regression tool for UAT, yet has the capability. Optum recommends this be leveraged, with the proper skilled automation professional resources, along with a customized framework and integrated test data management system (TDM) to provide unattended regression automation.

The Test Manager shared that the UAT test cases are housed in Excel spreadsheets and any Selenium IDE record and playback scripts, that are utilized to perform the redundant test steps, are documented in this spreadsheet as part of the test case. Selenium IDE scripts are an integral part of a great percentage of the UAT test cases being successfully executed. The UAT testing SMEs are State workers that know the business flows very well and are the test case designers for the UAT tests. These are primarily testers that were formally CSR's or BA's. They all have intimate knowledge of eligibility and enrollment within Medicaid and within the Exchange and understand very well what they are testing. This however often leads to test cases that are not fully documented and based on any requirements. If these test cases are to be automated by professional automation engineers then these Excel test cases may need to be analyzed and reverse engineered to extract the SME subjective nature embedded in the record and playback Selenium scripts.	Optum recommends that any formal automation effort that is considered, that these SME's would be engaged early to extract the subjective nature of some of the steps from their test cases and particularly selenium scripts in order to build out the automated framework components addressing navigation, error handling and test data management.
Upon speaking to the Test Manager, there are no skilled regression automation resources on the team. That said, everyone on the team appears to know how to utilize the Selenium IDE embedded in the Firefox browser. The programming skillset needed to interface with the more robust Selenium API/Web Driver components or any of the highly marketed automation tools programming interfaces is nonexistent. The Test Manager is the only skilled automation engineer for the State testing efforts. Unfortunately, he has resigned from his job effective 6/27. His resignation imposes a risk to the Selenium IDE automation scripts being used by the UAT testers in their Selenium IDE created scripts. Some custom Selenium Java code was created and is being used. If that code needs updating to address changes that the portal application may undergo, then any and all automation may stop to be useful without someone with the skillset to fix / enhance this custom code.	Hiring automation consultants to carry out an automation strategy with an automation tool, the consultants are versed in, is a prerequisite for enabling robust unattended regression automation. The skills the UAT team possesses are solely around the Firefox browser Selenium IDE only. This automation utility is being utilized solely as a vehicle to drive efficiency in the many redundant test steps needed to get to particular application areas and application states to do manual testing in those desired areas.
There appears to be some test data management in the test cases the UAT testers are creating, but there has not been enough time to investigate this to confidently say there is or is not. Optum did observe that a date embedded in the record and playback Selenium script needed to be updated in order for the automated script to continue. These are common TDM automation disciplines handled by seasoned automation engineers versed in test automation and automation test data management practices.	In order to have a robust automation suite, test data will need to be managed and integrated into the automation regression suite with resources familiar with automation TDM disciplines. Understanding the test environments data refresh and cycling schedule needs to be understood so extraction of test data can be engineered to support automation run iterations in single or multiple test environments.

An automation regression effort which includes an automation tool and skilled automation resources does not exist.	If Selenium is used as the automation tool, the cost of the tool will be minimal. The cost that the State will need to incur will be in securing highly skilled Selenium automation resources that could stand up a robust automation effort and provide back to the State a repeatable set of automation scripts, giving the leverage to run repetitive regression testing on demand by any test team member. All this will need to be embedded in an automation framework that hides the core programming and exposes the ability to create test cases with no direct programming expertise by the manual testing teams. This is where the State will incur the cost of automation even with a free open source tool, such as Selenium
There is a single test environment that is shared for all testing and some development. This is a high risk for successful automation, as this environment is not managed for any single purpose of testing only. It is not a dedicated test environment. Development builds could be pushed into this environment without notice according to the Test Manager. Ownership of this environment is not clear and would need to be better understood to see it as an opportune location to embed automated regression suites of tests.	Before any test automation is considered, that either a new test environment dedicated to testing is created or a highly regulated shared environment be established and managed to support test automation. All application instability needs to be eradicated as much as possible via a test environment scheduling process or governance to promote application stability. Data management needs to be understood in this environment equally to support an automated regression bed.

Observation / Findings	Recommendations
Performance	
No application performance testing strategy and practice is in place. The end users become the quality testers of each release which impacts application availability and stability.	A performance testing plan needs to be put in place. The plan is the responsibility of the SI, and the plan should include: • When to run (entrance criteria) • Gathered Performance Requirements • Data needed • Environments • End User Role Determination and Counts • Results Analysis • Benchmark Establishment • Execution Tool • Execution Plan • Monitoring • Change Control Process
Based on the documents provided, there was no evidence of a Performance RTM.	Performance requirement must be traceable from: • Business Requirements • System Design • Architectural Design • Development
Of the 25 non functional requirements listed, six of 25 were application performance related. • Application performance requirements were in testable format • Missing from requirements are specific end user profiles • Lack of user scenarios with definition criteria	Recommendation is to have clearly defined traceable testing scenarios with measurable success criteria.
Upon discovery and documentation received, application performance testing is conducted in a testing environment that is used for other types of testing (i.e. UAT and SIT).	The performance environment should be a mirror image of production. As an option, Performance testing can be run in an alternate environment, but, the tests need to be run off hours, and configuration changes in order to address concurrent users, etc. will need to be done.

No insight into the volume or nature of the test data required or any evidence of Data Management plan.	Performance testing should always include a clearly defined test data management plan, which is reviewed and signed off prior to the start of testing. This plan can be separate or imbedded in the QA Test Plan. This is an activity that is the responsibility of the SI. The sections of this plan should include: -Data Governance -Data Architecture Management -Data Development -Data Operations Management - Data Security Management - Meta-Data Management - Data Quality Management
Load / Stress testing results not provided.	The difference between Load and Stress testing In Stress testing, the focus is on breaking the system under test by overwhelming its resources or by taking resources away from it (in which case it is sometimes called negative testing). The main purpose is to make sure that the system fails and recovers gracefully. A load test is conducted to understand the behaviour of the system under a specific expected load. This load can be the expected concurrent number of users on the application performing a specific number of transactions within the set duration. This test will give out the response times of all the important business critical transactions Both are important and fall under overall Performance testing. Before a release is promoted to Production, Performance should be signed off by the appropriate stakeholders.
Performance test monitoring plan contain best practices monitoring tool which is LoadRunner.	LoadRunner is used as both a performance and monitoring tool. Additional tools that are used for in distributed environments for monitoring are: • Dynatrace • HP OpenView • DC Rum • Perfmon • Rstat D

Although (5) environments exist, there are only (2) fully integrated environments. CGI stated they are contractually obligated to only have (2) environments fully integrated.	The lack of integrated environments prevents multiple release testing and a fully functional training environment. Also, without a performance environment, there is a risk that the test environment will crash due to the stress and load that performance puts on the servers. The recommendation is to fully integrate existing environments and build a performance environment that mirrors production.

Observation / Findings	Recommendations
Environments	
Disaster recovery environment is not built out. In case of a disaster at the primary Data Center site, the RTO and RPO objectives cannot be met.	The DR environment needs to be built out and then a plan developed for failover testing. Further as discussed, the recommendation for building out fully integrated environments are: • Disaster recovery environment needs to be built out fully and tested. This testing is monitored against a detailed DR Test Plan. The SI is responsible for developing and executing this plan.
A lack of integrated environments that are necessary to support different phases and different releases of testing is missing.	There are only two fully integrated environments. This prevents multiple releases from being tested in addition risks on performance and the ability to test production issues. Existing Environments need to be built out to be fully integrated. • Performance environment as this will allow performance testing to occur and not impact IT/UAT testing. • (2) test environments as this will enable concurrent testing of releases. • Pre-Prod environment that is fully integrated that will allow for production fixes to be tested prior to being deployed to production. • Disaster recovery environment needs to be built out fully and tested. At that point, a detailed DR Test Plan needs to be developed and executed. • Production/Live environment

5. STAFFING

This section documents the findings and recommendations for the assessment of testing resources and business analysts involved in testing.

Observation / Findings	Recommendations
Staffing	
SOV Current level of staffing dedicated to UAT: • A dedicated number of resources to focus on UAT are absent. Best Practices recommend there is an overall UAT Test Manager/Lead along with a number of dedicated resources that are rotated so as to keep resources current with business and still provide the proper testing support. • One of the major functions of a UAT Test Manager/Lead would be to develop the UAT Test Plan and communicate the number of resources needed to sufficiently test the release. • Currently, SOV has a dedicated Test Manager, but, in observation, lacks the necessary skillset and support to perform these tasks. There are also a number of SOV employees that are SME's, but, lack the testing knowledge or methodology necessary to perform a valid UAT testing effort.	SOV should implement the following: • Assign FTE's to support UAT of Package 2 and Package 3. This would enable SOV to rotate resources in and out of UAT on a rotating basis so as not to lose testing and business knowledge. • Assign a UAT Test Manager/Lead responsible for creating the UAT Test Plan for Package 2 and Package 3. • Partner with Optum during UAT of Package 2 and Package 3 to increase knowledge of UAT processes and procedures..This will enable Knowledge Transfer for testing practices to SOV and also Subject Matter Expertise from SOV to be exchanged to Optum.
CGI was asked to participate in a meeting with their QA Texas team which they declined. Without this information it is not possible to measure the team's expertise and skillsets. However, what is evident is there have been numerous changes in the QA Leadership area from the Test Manager/Lead to the QA Project Manager. • The turn over in CGI staff frequently resulted in CGI resources not being able to fully address Optum questions because they were not involved/aware of circumstances in question. • The lack of knowledge in data manipulation and automated regression for test cases indicates there is not a high degree of skillset from a CGI tester standpoint.	The skillset and expertise of testers should be further addressed with CGI. Where skills and expertise are lacking, testers should be replaced with more knowledgible resources.

OPTUM™

Vermont Health Connect VHC

Maintenance and Operations (M&O) Review

8/27/2014

TABLE OF CONTENTS

1.....EXECUTIVE SUMMARY **3**
2.....BACKGROUND **5**
3.....RECOMMENDATION FOR CLOSING GAPS **6**
4.....FUNCTIONAL ORGANIZATIONAL CHART **25**
5.....OPEN ENROLLMENT **28**
6.....DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN **29**
7.....DOCUMENTATION OF VHC PLATFORM **31**
APPENDIX **36**

1. EXECUTIVE SUMMARY

The purpose of this deliverable is to:

- Review CGI's M&O plan and capabilities with respect to supporting the current VHC deployment as well as future use of the platform by additional HSE programs (e.g., IE, MMIS)
- Document process gaps with a focus on improving stability and readiness for open enrollment
- Provide an assessment of the State's HSE platform and the VHC solution from an M&O perspective

After review of the project's M&O documentation and interviews with both SOV and contractor staff, Optum has concluded that CGI's M&O plan, processes, and capabilities are not sufficient given the service level agreements outlined in the contract and the platform's volume of change. The impacts of these deficiencies include:

- No disaster recovery (DR) plan has been formalized and; therefore, no DR exercises have been successfully conducted. There is no confirmed ability to successfully restore the production environment even though the contract contains full requirements around recovery times of four hour Recovery Time Objective (RTO) and 30 minute Recovery Point Objective (RPO).
- Incidents are being closed without conducting proper root cause analysis. The Remedy (incident repository) data shows that incidents are closed without proper resolution or reference to a problem ticket to address the root cause of the incident. This leads to resources performing manual workarounds versus fixing the incident's root cause.
- Service Level Agreements (SLAs) relative to monitoring, measurement, and reporting needs to be documented and agreed to by both SOV and CGI. CGI has improved their severity 1 and severity 2 SLA compliance, but consistently fails to meet their severity 3 and severity 4 SLAs. Response time SLAs are consistently missed based on the reporting CGI provides to SOV. Platform availability and stability cannot be measured without SLAs being accurately captured, measured, and reported.
- The majority of the required documents to be produced by CGI are incomplete or not approved by SOV. For a full list and current status of these documents refer to section 7.0 - Document of VHC Platform.

Key Findings

Optum's assessment is based on the following key findings:

- The VHC system remains in a state of constant change since its 10/1/2013 original deployment. Major functionality including Change of Circumstance and Renewals has yet to be delivered. Changes are being introduced twice per week making it difficult for the M&O team to know if something is a defect (introduced during the development lifecycle) versus an incident (introduced post-deployment). Not having completed and signed off documentation causes confusion and allows CGI to classify a reported incident to be working as designed.
- CGI states they are operating in a steady state although the volume of change is still very large. CGI has all of the core elements of a functional steady-state M&O organization documented within their M&O handbook (not approved by SOV) , but they are lacking in the management of core elements, such as defects, incidents, problems, availability, stability, events, and Key Performance Indicators (KPIs) reporting.
- ITIL process flows exist within the M&O handbook but are not approved by CGI or SOV.
- RACI diagrams are at too a high level. They need to match the process flows and must be signed off by CGI and SOV.

- KPIs have not been defined nor reported by CGI as required by the contract. Without these KPIs the real status of VHC is not fully known. The amount of effort required to eliminate the backlog of 200+ incidents cannot be determined.
- Less than 1% of incident tickets have corresponding problem tickets which is almost 7% lower than Optum's experience. This low rate shows that many incidents are closed with no root cause known or remediation
- Defects from the development lifecycle exist, but are not consistently tracked or reported. By not tracking these defects, it is difficult to determine the number of defects, the number remaining open, and the status of the fixes completed by CGI. When the fix is made, the business operations team should be made aware that the manual workaround is no longer necessary.
- Gaps are apparent in the communication process between CGI and its sub-vendors. This lack of common knowledge and requirements leads to increased incidents, missed SLAs, and defects from User Acceptance Testing.

Recommendations

Optum's assessment results in following key recommendations:

- SOV should assign an overall owner for M&O of the VHC platform. This owner should be accountable for compliance with all contractual obligations between CGI and SOV and to ensure compliance with their M&O handbook (not approved by SOV).
- Update, approve, and maintain all required documents including but not limited to:
  - System design documents so that future enhancements have an accurate design for enhancement and maintenance.
  - Process flow documents for incident, problem, change, event, availability and performance management.
  - RACI diagrams for all approved process flows down to the task level.
  - KPIs defined, measured, and reported.
- Complete the development, testing, and implementation of the disaster recovery plan. Execution of this DR plan should be repeated until all issues have been resolved and the requirements of four hour RTO and 30 minute RPO have been achieved.
- Conduct proper root cause analysis on all incidents to properly detect recurring incidents and to remedy the root cause. This process can also be used to detect potential issues within core infrastructure components that may impact availability and performance of the platform.
- Enhance the defect tracking capabilities from initial detection through implementation in production.

Introduction

The following sections describe Optum's approach and further describe M&O findings and recommendations:

- Section 2.0 - Background outlines HSE assessment objectives and Optum's approach for preparing the finding and recommendations outlined throughout this deliverable.
- Section 3.0 – Recommendation for Closing Gaps contains gaps relative to ITIL standards and processes.
- Section 4.0 – Functional Organizational Chart includes a functional organization chart for systems capabilities including the level of M&O staffing needed to support those capabilities.
- Section 5.0 – Open Enrollment describes a process for continuous improvement.

- Section 6.0 – Disaster Recovery and Business Continuity Plan provides a recommendation for how to improve disaster recovery and the Business Continuity plan.
- Section 7.0 – Documentation of VHC Platform provides an assessment of the status of M&O system documentation.
- Appendix includes graphics that support our findings and recommendations.

2. BACKGROUND

The purpose of the Maintenance and Operations Review deliverable is to:

- Review CGI's M&O plan and capabilities with respect to supporting the current VHC deployment, as well as, future use of the platform by additional HSE programs (e.g., IE, MMIS).
- Document process gaps with a focus on improving stability and readiness for open enrollment.
- Provide an assessment of the State's HSE platform and the VHC solution consisting of the following:
  - Evaluation of the ability of the VHC IT platform to support multiple System Integrator vendors working on parallel development streams.
  - Evaluation of current vendor implementation of Information Technology Infrastructure Library (ITIL) based operational processes including; but not limited to, change, release, configuration, incident, problem and escalation management.
  - Evaluation of CGI organizational structure and staffing levels, CGI's capability to develop steady state M&O, and CGI's roles and responsibilities to ensure operation of the VHC in accordance with state contract requirements and service level agreements.

The team met with the following areas:

- State of Vermont
  - Lindsey Tucker
  - Mike Morey
  - Tom Mulhall
  - Jay Martin
  - Nicole Weidman
  - Melissa Rancourt
  - Tony Thibault
  - Peter Rhoades
  - John Kohlmeyer
  - Lauren McTear
  - Rick Ketcham
  - Jack Green
  - Jim Heintz
- CGI

  [redacted]
- Exeter
- Benaissance
- Archetype
- Blue Cross Blue Shield

A list of project documents reviewed is in the Appendix, See Figure 8 – Documents Reviewed List.

Information requested from CGI and not made available to the Optum team includes:

- Organization chart
- Productivity metrics around Incidents and problems
- Resource roles and the number of resources in each role
- Resource skill levels
- Known manual workarounds due to outstanding defects or missing functionality
- Disaster Recovery Plan
- Business Continuity Plan
- Daily checklist of manually performed tasks

Without having this information Optum was not able to properly:

- Determine if CGI has the proper team size and skills to support the VHC
- Determine how much additional workload has been placed on SOV for performing these manual workarounds and for how much longer they need to be performed.
- Determine how much effort is required to complete and validate the Disaster Recovery Plan CGI originally developed.
- Determine how much manual work is being done by the M&O team to keep the system operating and any risk associated within these manual tasks.

3. Recommendation for Closing Gaps

This portion of the document contains documentation of the gaps relative to ITIL standards and processes:

3.1 Service Level Agreements versus Industry Standards

While CGI's contract includes clearly articulated Service Level Agreements, neither CGI nor SOV are monitoring related performance and compliance.

Background

CGI's self-reporting shows that they are meeting the severity 1 and severity 2 incident SLA, but that is primarily due to lower volumes that are the result of inappropriately downgrading high priority incidents to severity 3 or severity 4. CGI's performance on severity 3 and severity 4 incidents suggests they do not have sufficient resources to handle the current backlog of incident and problem tickets.

The Contract's SLAs are included in Appendix – Figure 7 Service Level Agreements.

Observation/Findings and Recommendations

The table below outlines SLA Observation/Findings and Recommendations.

Observation/Findings	Recommendations
The documented SLAs match what other states are using for initial implementation. Lack of reporting from CGI makes it impossible to measure adherence to them.	Conduct working sessions between SOV and CGI to document the approach for measuring and weekly reporting each SLA. For additional information on SLAs see the following sections; 3.3 Incident Management, 3.4 Problem Management, 3.6 Availability Management, 3.7

	Performance Management and 3.12 Capacity Management.
SLAs match what other states are using but are being measured at too high of a level. For example, VHC is either up or down. There are several Vital Business Functions (VBFs) within the VHC platform and each should be measured. For example, response times should be measured and reported for Plan Selection versus Enrollment.	Conduct working sessions between SOV and CGI to define SLAs for each VBF and the approach for measuring and weekly reporting.
System availability is not being measured nor reported properly. The only evidence provided on availability was data on portal response times.	Conduct working sessions between SOV and CGI to document how to measure and report availability to the VBF level on a weekly basis.
Since the DR plan is not complete and approved, there is no ability to achieve the stated SLA goal of four hours RTO and 30 minute RPO.	CGI needs to finish the DR plan and submit to the SOV for review and approval. Once approved, the plan should be regularly tested at the secondary site and revised where needed. A formal approval process for the content on the plan and the results of execution should be implemented.
There is a lack of reporting around incident management SLAs. There are several reports showing incident data but none of them measure or report results against SLAs. Basic KPIs for incidents are not being captured or reported.	Conduct working sessions between SOV and CGI to define and monitor each incident management SLA and report results weekly.
The CGI and Benaissance resources that were interviewed were not aware of documented SLAs within the Contract - Amendment 2 and, have not been reporting them to SOV.	SOV should review the documented SLAs with both CGI and Benaissance and implement reporting processes for the contracted SLAs.
Even though the SLAs are documented the Contract doesn't clearly show how they are to be measured. For example, the start time for an SLA is not clear (e.g., Does it start when data is sent to a vendor or does it start when the vendor receives the data)?	SOV, CGI, and Benaissance should define how the existing SLAs are to be measured and reported including a Responsible, Accountable, Consulted, and Informed Model (RACI) for each service level.

3.2 Current level of application monitoring versus desired level by the state

Refer to 3.6 Availability Management sections, 3.13 Capacity and Transaction Monitoring assessment.

3.3 Incident Management

The increased attention to M&O activities by SOV is helping to improve the incident management process over the past couple of months. Work needs to continue to mature this process so that process flows, RACI diagrams, and KPIs are documented, reviewed, and approved by SOV and CGI. All incidents related to the VHC should be recorded and tracked within the Remedy repository even if the incident ownership resides with an outside entity. This process is required so SOV has one location for all incidents that impact VHC. CGI did not provide resource levels dedicated to incident management. Therefore it is not possible to determine if they can support the anticipated new incident influx and the current 186 open incidents.

Background

An incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or degradation in, the quality of that service.

Incident management is the process which is responsible for managing the lifecycle of all incidents. The key objective of incident management is to restore the IT service for the user per agreed-upon service levels.

Examples of incidents include:

- Entire application or service not available
- Medicaid cases not being sent to Access
- Carrier integration failures
- Part of an application or service is not available
- Degradation in response time, reported by a user or as identified by an automated alert
- Hardware is down that impacts the performance of an application or function
- Automatic alert indicating a potential disruption to service

The incident management process is reactive. The process either results in a workaround or a restoration of service. The incident management process is not intended to understand or remedy the underlying cause of the incident or ensuring the incident does not reoccur. The problem management process addresses root cause and remediation.

Best Practice KPI's

These are defined as:

- Number of incidents per severity
- Number of incidents per VBF
- Number of incidents per business/organizational area
- The average time to achieve incident resolution
- The number of incidents handled within the agreed upon Service Level Agreements for that type of incident or configuration item.
- The total estimated time to resolve the incident backlog needs to be reported.
- Reporting of incidents at each stage of the incident management process (e.g. open, closed and remaining open)
- Number of reoccurring incidents

Recommended Level of Reporting

- Incident reporting should be on a daily, weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in green, yellow and red.
- Reports for management should be created:
    - Management reports help identify trends and allow review of the health of the process. Setting a level on certain reports may be appropriate as may be categorizing the report as strategic, operational or tactical.
    - Major incidents logged and resolved. Severity 1 incidents should be fully described.

- Summary of incidents that are still to be resolved.
- The number of incidents attributable to different business/organization areas.
- Relevant financial information. Including a cost per incident summary.

Observation/Findings and Recommendations

The table below outlines Incident Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Having M&O and development shared resources creates inconsistencies with incident management ownership and accountability.	The CGI vendor staffing model should align dedicated resources to incident management.
M&O activities for incident management should be clearly defined. The flow diagram created lacks the details around the Incident process at the person/role level. The RACI diagram created lacks the details around the incident process at the person/role level.	A detailed flow diagram should be created to show the incident process at the person/role level. A detailed RACI diagram should be created to show the incident process at the person/role level.
Incidents are a critical KPI which should be documented, agreed upon and reported on a weekly basis. CGI has been reporting incidents at a high level.	KPIs should be part of the standard reporting for the M&O team and senior management. More details around incidents need to be included within these reports including actual versus targeted SLAs.
Multiple tools such as Remedy, ALM, Gemini and Salesforce are used to track all issues. These multiple tracking tools do not create a consistent repository for tracking Incidents.	All problem tickets should be recorded in a single repository for improved management of incidents.
Workarounds for incidents as a remedy of incidents are used on a widespread basis. However, the number of these workarounds count not be determined.	SOV and CGI should provide the framework to define what an acceptable work-around is. All workarounds should be documented in a single repository and have reference to a given incident.

3.4 Problem Management

CGI started creating problem tickets within Remedy on 1/9/2014 and since then, they have created 34 tickets. All 34 were categorized as severity 3 or severity 4. To date 21 tickets remain open. CGI creates a problem ticket for less than 1% of the incidents they close (3,383 year to date) which is well below the Optum average of 8%. This would indicate that CGI is not performing detailed root cause analysis for many of the incidents which lead to an increasing number of manual workarounds.

Background

A problem documents an underlying cause of one or more incidents.

Problem management is the process for managing the lifecycle of all incidents.

The problem management process drives root cause analysis to identify a permanent solution and to manage the implementation of remediation activities.

Risk - Problem risk levels define the urgency of resolving a problem based on:

- The priority of the incidents related to the problem
- The number of previous incidents related to a given problem ticket
- The impact of the problem on VBFs
- The likelihood of future impact

Best Practice KPI's

These are defined as:

- Number of problems per severity
- The severity may inherit the severity from the incident
- Number of problems per VBF
- Number of problems per business/organizational area
- Average time to achieve problem resolution
- The number of problems handled within the agreed upon Service Level Agreements for that type of problem
- Average productivity per problem
- The total estimated time to resolve the backlog of open problems
- Reporting of problems at each stage of the incident management process (e.g. open, closed and remaining open)
- Number of reoccurring problems

Recommended Level of Reporting

- Problem reporting should be tracked on a daily, weekly, monthly and annual basis. Graphical representations should be created for period-over-period comparisons.
- Trending should be shown in green, yellow, and red.
    - Problems tickets need to capture the estimated time to resolve each problem. This provides priority guidance and highlights the total effort trending analysis to close all open problems. This will help guide appropriate M&O staffing levels.
        - Management reports help identify trends and allow a review of the health of the platform. Setting a level on certain reports may be appropriate such as categorizing the report as strategic, tactical, or operational.
            - Major problems logged and resolved. High impact problems should be fully described.
            - Summary of problems that are still to be resolved.
            - The number of problems attributable to different business/organization areas.
            - Relevant financial information. Including a cost to resolve per problem summary.

Observation/Findings and Recommendations

The table below outlines Problem Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
M&O processes and responsibilities for problem management are not clearly defined.	SOV and CGI needs to agree to the process flow and create a detail RACI diagram so that all tasks and corresponding roles and responsibilities are known to both parties.
SOV team relies upon the vendor to record, resolve, code, test and deploy and drive problem changes to the production environment.	SOV should increase its engagement in problem ticket monitoring and increase testing visibility and responsibility.
Some problems are fixed utilizing a workaround process. It is not documented how many workarounds currently exist.	The established and agreed upon workarounds need to be documented throughout the system.
KPI reporting to the M&O team, SOV and senior management is lacking details for management of problems.	KPI reporting for problems should be introduced to drive improved stability and problem productivity.
Incidents that required a long- term solution are tracked as problem tickets. Optum experience shows 8% of incident tickets require a problem ticket. VHC/CGI is averaging less than 1%.	SOV and CGI need to document what is an acceptable workaround for an incident. Many states work with the SI to define the meaning of what an acceptable workaround is. Real life examples should be used whenever possible. The definition of an acceptable workaround should be updated as new and approved examples are discovered. Both parties should agree that root cause analysis is not required, otherwise a problem should be created.

3.5 Change Management

Although progress is being made within this area, there is a need to mature the process so that all changes to the production environment are reviewed and tracked. Changes are still occurring at a higher than desired level and it is recommended to slow down the volume of changes to increase productivity and protect the production environment.

Background

Change management is the ITSM process and discipline to ensure that standardized methods and procedures are used for efficient handling of all changes.

The key objective of change management is to minimize the impact of change-related incidents upon service quality and, consequently, improve the day-to-day operations of the organization.

The goal of change management is to prevent impact to the production environment when change is introduced. It is also to ensure that IT and the business can be aligned and can be kept aligned.

Best Practice KPI's

These are defined as:

- Number of outages due to changes (planned unavailability)
- Number of unplanned outage/unavailability due to changes
- Number of emergency changes

- Number of unauthorized implemented changes
- Number of backed-out changes
- Number of incidents caused by changes
- Number of refused changes by Operational Change Review Board (OCRB)
- Average change closure duration

Recommended Level of Reporting

- Change reporting should be tracked on a daily, weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in green, yellow, and red.

Observation/Findings and Recommendations`

The table below outlines Change Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
The existing change management process does not define a separate path for break-fix changes.	Clear change management guidelines are needed for break-fixes.
The change management tool is Share-Point based and initially didn't integrate with the incident and problem management tool (Remedy). Recent changes have been made to adhere to the process.	The change management tool needs to be integrated with problem tickets, incidents, requirement traceability matrix, and CMDB etc.
Release frequency (twice a week) is high and results in significant effort for change coordination. The frequency of releases poses a challenge to regression and user acceptance testing cycles.	Release frequency needs to be reduced so that proper testing cycles can be performed and release coordination can be reduced.
OCRB form classifies changes as per the defined system architecture only and doesn't tie-back to the impacted "critical business functions". Objective "risk assessment" is not done for changes.	The critical business function being impacted for a given change should be captured so that all impacted parties can be notified of the change. This will allow those business units the ability to review and communicate any changes to existing business process resulting from the change.
Standard change reporting doesn't exist.	Change reporting is needed for objective visibility into change management.
OCRB seems to be the only way CGI M&O SMEs learn about the change controls going in with a release.	M&O involvement in the SDLC process is needed. Formal Release Entry Framework (REF) * needs to be adopted to ensure that M&O SMEs are consulted during all phases of an upcoming release.
Automated end-to-end production validation is not in place after a release.	An application level release validation plan needs to be created and kept updated.

More info is in sections 3.3 Incident and 3.4 Problem and 3.5 Change

* Release Entry Framework is a practice of knowledge transfer from the DDI resources to M&O resources. Quarterly meetings are held with DDI and M&O to review the deliverable schedule for the next three months. DDI and M&O resources begin working on knowledge transfer during the design phase of the system development life cycle and continue engagement until the end of the warranty period.

3.6 Availability Management

There is not an existing report showing the availability of the VHC platform or its components. The contract clearly states the requirements around availability measurement and reporting, however, there is no evidence that those requirements are being met. CGI should meet these documented requirements within the contract and what is stated within their M&O handbook.

Background

Availability management is the ITSM process used to ensure that systems are available for use according to the Service Level Agreements (SLAs).

Best Practice KPI's

These are defined as:

- Percentage of actual uptime vs planned uptime
- Percentage of unplanned outage/unavailability due to changes

Recommended Level of Reporting

- Availability and performance reporting should be tracked on a daily, weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in green, yellow, and red.

Observation/Findings and Recommendations

The table below outlines Availability Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Section 4.2 in O&M manual describes CGI's approach to availability management.	Complete, review, approve and implement the practices as documented in O&M manual.
Standardized reporting is missing for availability KPIs and SOV has less visibility in these measurements.	Define, review, approve and implement the recommended level of KPI reporting.
A total of 122 severity 1 incidents & 356 severity 2 incidents from 10/1/13 through 6/9/14 indicate that availability management is ineffective.	Root cause analysis should be performed for any severity 1 or severity 2 incidents which cause an unplanned outage to the production environment. Based on the findings of this root cause analysis steps should be taken to avoid repeat incidents from occurring.
Post-incident review documents for high severity incidents do not consistently point to permanent fixes.	High severity incidents causing unplanned outages to production should follow an Accelerated Problem Management (APM) path. The goal of APM is to thoroughly resolve those problems causing the greatest impact as quickly as possible. The M&O team should conduct a meeting the next business day. Individuals involved in restoring the incident are required to attend the meeting or provide a well-informed representative. During the initial meeting, root cause analysis and potentially resolution tasks are identified and assigned. The M&O team then continues to manage and drive the problem until it is closed.

Observation/Findings	Recommendations
SLAs for severity 1 incidents are met only 73% of the time and SLAs for severity 2 incidents are met only 78% of the time.	Perform a deep dive to review the root cause of missed SLAs. SLAs can be missed for a variety of reasons ranging from lack of proactive monitoring to incidents not being remediated. Each missed SLA should be reviewed to determine what improvements need to be made so that SLAs can be met 100% of the time.

3.7 Performance Management

Performance management is the subset of tools and processes in IT for the collection, monitoring, and analysis of performance metrics

The key objective of the performance management is to minimize the impact of performance-related incidents upon service quality.

Performance management can be subdivided as:

- Network performance management
- System performance management
- Application performance management
- Business transaction performance management

The goal of performance management is to ensure that a system component available and meeting the desired performance.

Best Practice KPI's

These are defined as:

- Percentage of CIs monitored for performance
- Percentage of service requests due to poor performance
- Response time of network vs SLAs
- Response time of system vs SLAs
- Response time of applications vs SLAs
- Response time of key business transactions vs SLAs

Recommended Level of Reporting

- Performance management reporting should be tracked on an hourly, daily, weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in green, yellow, and red.

Observation/Findings and Recommendations

The table below outlines Performance Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
[redacted] provided by SOV contains SLAs for network and capacity utilization. Each requirement is clearly documented and these NFRs were part of the contract between CGI and SOV. We were provided with only one report which showed data around performance management (VHC Avail20140607).	The architecture review assessment also conducted contains information around detail recommendations for improvement. M&O teams typically work closely with infrastructure teams to monitor, report and improve upon system performance. A detail deep dive review should be included involving the M&O and infrastructure teams.
The contractual response time SLA (90% <5 seconds) has been missed each and every week according to the VHC Avail20140607 document. This report does show basic performance information around portal response times but lacks the requirements stated within the NFRs.	The M&O team should work with the CGI hosting team to document, measure and report out on all of the NFRs related to performance management. SOV should be better informed as to how CGI is capturing and reporting out these performance SLAs.
[redacted] document provided by SOV contains SLAs for network and capacity utilization. Each requirement is clearly documented and these NFRs were part of the contract between CGI and SOV. We were provided with only one report which showed data around performance management (VHC Avail20140607).	The architecture review assessment also conducted contains information around detail recommendations for improvement. M&O teams typically work closely with infrastructure teams to monitor, report and improve upon system performance. A detail deep dive review should be included involving the M&O and infrastructure teams.

3.8 System Operating Controls

The VHC platform sends critical enrollment and financial information to both sub-vendors and carriers on a daily basis. There have been several reported issues with data being transmitted from one source to the other unsuccessfully and the problem going unnoticed for days.

Background

The Enterprise System Operating Controls program works across IT systems and identifies gaps introduced during data interchange, across various system interfaces.

- Create a culture obsessed with the criticality of operating controls from inception, through design, development, testing, implementation, and ongoing support.
- Compulsively validate operating controls exist, are effective, and are attended to with appropriate level of criticality.

Identifying and addressing gaps in Enterprise System Operating Controls across processing environments will reduce quality issues.

Best Practice KPI's

These are defined as:

- **Efficiency:** Measures the timeliness and productivity of the process.
- **Execution:** Measures process output and accomplishment.
- **Effectiveness:** Measures process quality and impact.
- **Workforce:** Measures workforce utilization and maturity.
- **Program:** Measures the program level impact and performance.

Recommended Level of Reporting

- The controls dashboards need be shared daily, weekly, monthly and annually.
- The program level KPIs need to be shared monthly and annually.
- Operationalize reports to reduce manual effort.

Observation/Findings and Recommendations

The table below outlines System Operating Controls Observation/Findings and Recommendations.

Observation/Findings	Recommendations
An "Executive_1_Pager" report is being generated to look at the high level statistics of VHC.	The data-points of this report need to be traced back to establish "operating controls" amongst various system interfaces.
A "Daily Data Integrity" report is being generated that trends the various data-integrity issues and Top 20 Citizen Impacts.	The data-points of this report needs to be traced back to establish "operating controls" amongst various system interfaces.
No acknowledgement-mechanism is in place for the interchange of data/files between VHC, Carriers, Benaissance and Medicare etc. This results in issues being unnoticed until SLA expires.	Robust controls need to be implemented across technical interfaces to ensure that technical and functional issues causing data-losses are identified 'as they happen'.
There is no periodic reconciliation in place between VHC, Benaissance, carriers, Medicare, etc.	Weekly monthly reconciliation is needed to ensure consistency of data and to address issues before they cause bigger impact.
Lack of system operating controls for the 834 and 820 transactions.	Perform a deep dive for both 834 and 820 transactions for missing functionality, monitoring and controls.

3.9 Service Request Process

Background

A service request is a small enhancement that includes discretionary changes that are charged against the 2,000 budget specified in the contract.

There are two types of service requests: 'standard' requests and 'non-standard' requests.

- The current CGI contracts M&O handbook states that standard service requests must meet the following requirements:
  - Is included in the client's contract
  - Is requested for configuration items (CI's) available in the product catalogue
  - Has parameters defined: SLA, volume and description are detailed
  - The solution for the execution is known
  - Does not require an infrastructure change request to be executed and completed
- All other service requests that do not meet all of the above criteria are considered non-standard service requests (NSSR). There are six types of NSSR.
  - Contractual agreements – requests described in a client contract that may require a change request to be implemented or can have a document as deliverable (e.g., analysis).
  - Evolution - requests that are client (or CGI CPMO/CDM) initiated and are not defined in the client contract (e.g., new service introduction or change to an existing service is included in this category).
  - Infrastructure – requests initiated by service support and delivery teams that impact the infrastructure of more than one client or that is used for internal improvements.
  - Internal project – requests initiated by a stakeholder within CGI organization which require modifications to the infrastructure, business and organization.
  - Known error – requests used to implement a fix or solution within the problem management process flow.
  - Continuous improvement – request initiated by a CGI member that can be a procedural change, can target cost reductions or new revenue, can target quality improvements, can focus on inter-unit collaboration or identify different ways of using new or existing tools, etc.

Service requests are reviewed in a group forum called the Pre-Change Control Board (PreCCB). The Pre-CCB defines the effort and tries to determine the path the service request should follow.

Some efforts are triaged and sent to Archetype to provide a data extract or a report of required data.

Technical service requests are added to Remedy.

In addition the vendor CGI has agreed to support a 2,000 hour budget set aside for minor new development requests. These service requests are brought to the PreCCB team to evaluate and determine next steps. This PreCCB meeting may rule out the request or ask CGI to perform an analysis estimate or add the request to the queue for completion. The PreCCB group also prioritizes service requests.

If the request is deemed too large of an effort, it will be directed to be a new business request and require a full scale development effort.

Observation/Findings and Recommendations

The table below outlines Service Request Observation/Findings and Recommendations.

Observation/Findings	Recommendations
SOV seems to be concerned about the work being charged against the allotted 2,000 hour budget. Communication on what is or is not being placed in this support category is unclear. Recent examples show that requests to Archetype are being included in the 2,000 hour discretionary budget.	The service request process should be reworked to describe better examples of what are discretionary and non-discretionary requests. In addition, SOV should know how the request will be billed and who will work on the effort to determine the correct course of action.

3.10 Audit Support

Throughout the year SOV will be asked to participate in audits which will include the VHC platform. CGI will need to also participate and the question around funding will need to be decided. Is it an amendment to the existing contract or should it come out of the existing M&O funds? Typically the required involvement from the vendor is small and should come from the existing M&O budget unless some complicated reporting is required to satisfy an audit request. If that is the case, it should draw funding from the discretionary pool of funds already established between SOV and CGI.

Background

The only reference to external audits came from the CGI M&O Handbook Exhibit 40: Security Management Activities and Touch points on pages 51 and 52.

Observation/Findings and Recommendations

The table below outlines Audit Support Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Eventual audit support required by CGI is not mentioned in either the contract, NFRs or the M&O Handbook	SOV should work with CGI and include external audit support as part of the existing M&O contract and it should be added within the M&O handbook.

3.11 Configuration Management

Configuration management is the ITSM process and discipline used to identify, maintain and verify information on IT assets and configurations.

Background

The goal of configuration management is to have accurate information about the IT assets and enable informed decision making for incident, problem, change, release and capacity management activities.

Configuration management provides clear understanding of relationships between Configuration Instances (CIs) and their impacts.

Best Practice KPIs

These are defined as:

- Percentage of CIs monitored for performance
- Compliance with annual attestation requirement by each service level owner

Recommended Level of Reporting

- Configuration reporting should be tracked on a weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in green, yellow, and red.

Observation/Findings and Recommendations

The table below outlines Configuration Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Configuration management is part of CGI O&M Manual – section 1.4.9. Change management and release management sections of the manual also refer to configuration management.	Implement the process as per the manual.
Configuration management database (CMDB) for the System Integration (SI) components doesn't exist.	Create a comprehensive CMDB, accounting for key software and hardware components.
OCRB form used in change management doesn't refer to CIs.	OCRB form and all upcoming processes for change and release management should refer to CMDB.
Impact of a change is not derived using a CI repository.	CMDB should be the principal source to assess the potential impact/risk associated with a change.

3.12 Capacity Management

The requirements are clearly stated within the contract and CGI is not meeting them. Within the CGI M&O manual there is capacity documentation but no evidence the process is being followed.

Background

Capacity management is the ITSM process and discipline used to ensure that the installed base of applications is prepared to support organic growth over time.

The Goal of Capacity Management

The goal of capacity management is to fine tune applications and infrastructure components to improve performance, reduce consumption, and delay or avoid frequent upgrades. This enables businesses to get more out of existing IT resources and to contain IT cost.

Best Practice KPI's

These are defined as:

- Percentage of network bandwidth used
- Percentage of response-time SLAs not met
- Percentage of Configuration Items monitored for performance
- Percentage of service requests due to poor performance
- Response time of key infrastructure components vs SLAs
- Response time of key business transactions vs SLAs

Recommended Level of Reporting

- Capacity utilization and availability reporting should be tracked on a daily, weekly, monthly and annual basis. Graphical representations should be created for period over period comparisons.
- Trending should be shown in Green, Yellow, and Red.

Observation/Findings and Recommendations

The table below outlines Capacity Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Section 4.3 of M&O Manual describes the intended capacity management process but no formal capacity plan has been shared.	Create and share a comprehensive capacity management plan.
Capacity forecasts for the upcoming "Annual Enrollment Period" do not exist.	Forecast AEP capacity requirements using data-models and provision accordingly.
Capacity monitoring reports not being shared regularly with SOV.	Share regular daily/weekly/monthly reports as per activity 90.3 of O&M Manual.
A number of Infrastructure and Capacity changes continue to be implemented without mapping them to a plan.	Tie all infrastructure and capacity changes back to Capacity Management Plan and Remedy incidents. Continuously improve the plan to minimize capacity-related incidents.
Response time SLA (90% <5 seconds) is being missed by over 100%.	Perform deep dive analysis to identify root cause of missed SLA's. SOV has asked CGI to define how they are gathering this information so that it can be compared to the requirement noted within the contract.

3.13 Product Lifecycle Management

The VHC platform represents a robust but complex assortment of hardware and software components working in concert to provide a healthcare exchange solution that will meet the needs of the State of Vermont. All of these components have lifecycles (e.g., they are introduced by vendors, maintained for finite periods of time, and then retired from the market).

Product Lifecycle Management provides a proactive, structured process for upgrading software products supporting business applications. The process ensures that deployed software product versions are within the general available support provided by vendors and current with versions in general use by CGI and their vendors.

Background

CGI and its subcontractors are responsible for the entire information technology needs of VHC. It is their responsibility to ensure the software used meets the vendor supported versions

Observation/Findings and Recommendations

The table below outlines Product Lifecycle Management Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Detailed information around all VHC software products and their current versions should be kept updated on a regular basis.	Optum was not provided information showing this information but understands the SOV has such a list. Optum didn't observe a process to maintain this list on a regular basis (every 6 – 12 months)

3.14 Escalation

The basics of process and documentation around escalations within M&O exist within the M&O handbook but are not maintained on a regular basis. The documents are outdated and a monthly process should be established to keep them current given the amount of resource transitions.

Background

The M&O team manages the communications and escalations around all high priority Severity 1 and Severity 2 incidents. Key resources from both SOV and CGI should be aware of any impact to the VHS platform during normal operating hours. Even during maintenance windows critical issues may need to be escalated so that the key resources are aware of potential outage and can inform the proper parties which may be impacted. Escalations can take many forms from email to text messages to war room conference calls.

.

Observation/Findings and Recommendations

The table below outlines Escalation Observation/Findings and Recommendations.

Observation/Findings	Recommendations
The escalation list shows that it is not being maintained based on the names of CGI resources who are no longer on the account. See Figure 11 Resource Contact List	Maintain escalation documentation when there are resource changes or at regular intervals.
The process for escalation of high severity incidents exists by evidence of Exhibit 58 and Exhibit 59 located within the M&O handbook. It needs to be reviewed and updated on a scheduled basis. See Figure 10 Incident Escalation Sub-Process	
The contact list should be periodically reviewed for accuracy to verify the correct SOV employees are listed.	SOV should decide which resources, besides BASU, should be notified for various high severity escalations, along with their preferred method of communication. Optum – added last paragraph in previous recommendation
Escalation notification	

3.15 High Level Incident Reporting

Please refer to Section 3.3 Incident Management.

3.16 Metrics and Reporting

See additional metrics information in the various sections above.

Metrics and reporting is documented within the contract, NFRs and CGI M&O Handbook covering all ITIL processes. CGI is producing some of those required metrics but falling short on the majority of them. There is no current shared folder or SharePoint location where CGI posts these reports. Several different SOV resources report that they need to repeatedly ask CGI for reports around metrics and KPIs. Throughout the various sections of this assessment we identify the required, missing and best practice KPIs which should be reported out on a regular basis.

Background

Without having readily available reports of metrics and KPIs available, the true status of the platform is not fully known. Metrics and reports are critical tools in allowing sound decisions around the current platform. Without these available, there is no way to assess if the platform is within acceptable control limits.

Observation/Findings and Recommendations

The table below outlines High Level Incident Reporting Observation/Findings and Recommendations.

Observation/Findings	Recommendations
Several different SOV resources report that they need to repeatedly ask CGI for reports around metrics and KPIs.	CGI should store the reports they are generating to a common folder or SharePoint locations where SOV resources can access them.
Metric and reporting guidelines are documented within the contract, NFRs and CGI M&O Handbook covering all ITIL processes. Evidence of these was not provided by either CGI or SOV resources.	Further review of each metric, KPI and report requirements should be conducted with CGI. A detail action plan should be created and tracked until all requirements are met.

3.17 Parallel Development and Code Migration Paths

The SOV is looking to enhance the current VHC platform with missing functionality while at the same time leveraging it for other critical applications to take advantage of Integrated Eligibility.

Background

There are two releases going into production each week beside the major enhancements being developed like Change of Circumstance and Renewals. With all of this change occurring there needs to be an organized way of moving code changes into production following a documented SDLC process while not losing any code enhancements due to the code contention issues.

Current code promotion flow and SDLC path

[redacted]

Proposed code promotion flow and SDLC path

[redacted]

Observation/Findings and Recommendations

The table below outlines Code Migration Path Observation/Findings and Recommendations.

Observations	Recommendations
[redacted]	[redacted]
Throughout the onsite assessment there was little to no escalation around the current quality of the production environments. There is a high volume of changes occurring and there were concerns about code contention and how configuration items flow from development to production environments.	Further review of the environments should occur, measuring the quality of data, as well as, code and configuration management promotion processes.

4. Functional Organizational Chart

This section includes a functional organization chart for systems capabilities including the level of M&O staffing needed to support those capabilities. Assessment activities included:

- Reviewed the vendor's M&O roles and responsibilities and staffing levels.
  - CGI was asked to share information related to their current M&O team's roles and responsibilities and staffing levels which they declined. The following information from their M&O Handbook was provided along with interviews of key SOV resources.
    - From an M&O steady state roles perspective, CGI has everything accounted for and no glaring absence of required roles.
    - From a steady state staffing perspective dealing with a large volume of production defects and incident tickets, they are understaffed.
  - To determine the correct staffing level CGI would need to provide additional information including productivity factors for incidents and problems. CGI was asked for this data and once again declined to provide the data. With over 200+ open incidents and using a conservative 2.5hrs per incident ticket productivity factor, they have 500 hours of additional effort required to eliminate the backlog.
  - See Figure 5 CGI Unofficial Organization Chart, Figure 6 State of Vermont M&O Org Chart and Figure 9 Roles and Responsibilities within the Appendix.
- Reviewed the current staffing level dedicated to M&O functions versus desired amount.
  - A steady state M&O model leverages dedicated resources to focus their attention on M&O related activities. Even with a dedicated team there are times when other tasks are done due to the environment they are operating within. This is normally a very small percentage to help the DDI team when needed and at times the DDI team should be expected to help out the M&O team during high severity incident resolution. CGI does follow this dedicated model approach but did indicate there is sharing of resources occurring between DDI and M&O due to the backlog of defects and functionality still needing to be delivered. CGI declined to provide any data showing how much of the M&O team's efforts are going to non – M&O activities.
- Assessed skills of current M&O team to understand expertise and skillsets.

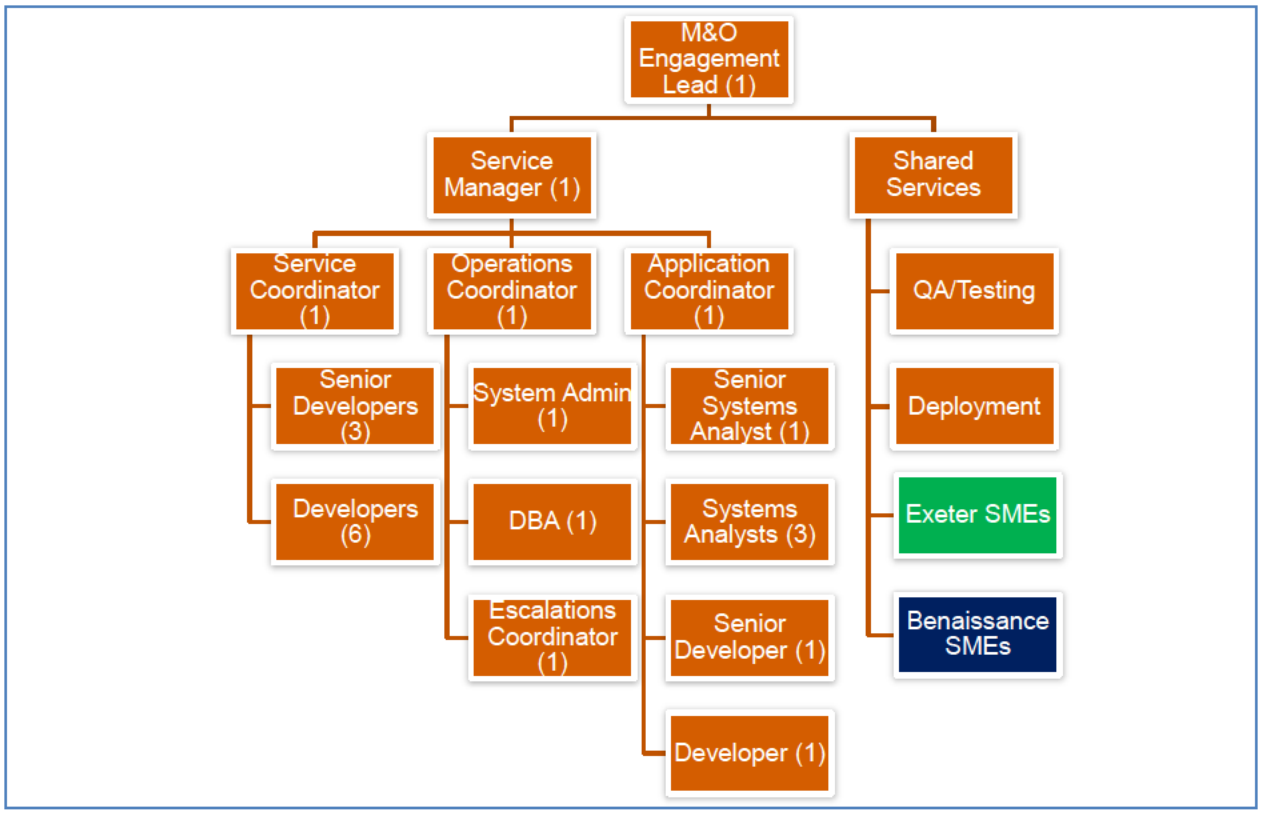
- CGI was asked to provide some form of skills assessment of their current M&O team which they declined to provide. Without this information it is impossible to measure the team's expertise and skillsets.

Observation/Findings and Recommendations

The table below outlines Organization Chart (Capabilities) Observation/Findings and Recommendations.

Observation/Findings	Recommendations
CGI was asked to provide some form of skills assessment of their current M&O team which they declined to provide.	Obtain this information to measure the team's expertise and skillsets. Without the information the expertise and skillsets are unknown.-
The following roles are not clearly established: O&M Engagement Lead, Service Manager, Service Coordinator, Operations Coordinator, Application Coordinator, Senior Developers, Developers, Senior System Analyst(s), Database Administrator, System Administrator, Escalations Coordinator, QA/Testing Lead, Deployment Lead, Release Package Analyst, Exeter OneGate subject matter expert, Exeter Siebel subject matter expert, Benaissance subject matter expert.	The Organization Chart below depicts a model appropriate for VHC. M&O steady state team size should range from 25 to 30 resources based on findings from this assessment. Deeper dive sessions would be required to finalize the overall team structure and size. A RACI Matrix is also provided.

M&O Proposed Organization Chart



Proposed M&O RACI

	VHC IT	VHC Business	M&O	Hosting	Exeter	Vendors / Other 3rd party
• ITIL Tools & Processes	C	I	A/R	R	C	C
• Monitoring	I	I	A/R	R		R
• Incident Management	C	C	A/R	R	R	C
• Problem Management	C	C	A/R	R	R	R
• Change Management	C	C	A/R	R	-	R
• Configura ion Management	C	-	A/R	R	-	-
• Availability Management	C	C	A/R	R	-	-
• Service level Management	C	C	A/R	R	-	-
• Performance Management	C	I	A/R	R	R	-
• Capacity Management	C	I	A/R	R	-	-
• Adaptive Maintenance	C	I	A/R	R	C	-
• Service Requests	C	I	A/R	I	-	-
• Disaster Recovery	C	C	A/R	R	-	-
• Compliance/Audit	C	C	A/R	R	-	-
• DD&I to OM transition	I	I	A/R	I	-	-
• Dashboard reporting	I	I	A/R	R	-	-

The M&O RACI chart is based on the following definitions:

- (R) Responsible – Those assigned to performed the work required to complete the task. Those who do the work to achieve the task. There is typically one role with a participation type of responsible, although others can be delegated to assist in the work required (see also RACI below for separately identifying those who participate in a supporting role).
- Accountable – The person or group ultimately responsible for completion of the task
- Consulted – The person or group(s) that are asked to provide input in the process and in making decisions. This often includes the project Subject Matter Experts (SMEs)
- Informed – The person or group(s) that are communicated to about the status of a tasks or event. This may be one-way communications.

5. Open Enrollment

An open enrollment readiness process is an Optum Best Practice for assuring improvement from one open enrollment period to the next. The goal of an open enrollment readiness process is to improve the availability and stability of critical application components during the open enrollment period. The process also ensures that the platform has enough capacity for expected operations and forecasted growth. Collaborative discussions between SOV and CGI are needed to identify and remediate risks.

Background

CGI does not have a documented plan to work towards an improved open enrollment for 2015.

Observation/Findings and Recommendations

The table below outlines Open Enrollment Observation/Findings and Recommendations.

Observation/Findings	Recommendations
No Open Enrollment plan.	Create Open Enrollment plan. Review of critical problems posing potential threats to open enrollment. Since there is no documented plan this has not been done. From a high level these are the steps to be followed: • Identify infrastructure, application, and vendor services that are in scope and assign a resource to own each component. • Request the assigned resource to evaluate the IT service's current state, project load volumes, and identify and communicate any potential risks. • Develop remediation strategies. • Monitor progress of remediation efforts, transactional volumes, response times, incident occurrences, change activity and respond accordingly. • Capture lessons learned for continuous process improvement.
Current manual SOV workarounds are not documented.	Review of current manual workarounds being done by current vendor which could pose a threat to open enrollment if they are not remediated.

6. Disaster Recovery and Business Continuity Plan

This section provides a recommendation for how to improve disaster recovery and the Business Continuity plan.

- Review of vendor's M&O disaster recovery plan highlighting areas of concern
- Review of the state's business continuity plan highlighting areas of concern

A Disaster Recovery Plan (DRP) is a documented process or set of procedures to recover IT infrastructure in the event of a disaster. The document should specify procedures an IT organization is to follow in the event of a disaster. The DRP is a comprehensive statement of actions to be taken before, during and after a disaster. The disaster can be natural, environmental, or man-made.

The Goal of Disaster Recovery

The basic objective of any Disaster Recovery Plan is to minimize downtime and data loss. The primary objective is to protect the organization in the event that all or a part of its operations and/or computer services are rendered unusable. The plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will prevail.

Risk:

- The Plan needs to be created, periodically reviewed and approved by all interested parties.
- A Physical secondary site must be built out
- Best practices require a DRP to be tested on an annual basis.

Risk Mitigation:

- Minimizing downtime and data loss is measured in terms of two concepts: the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). RTO is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. RPO is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

A Business Continuity Plan (BCP) is a plan to continue operations if adverse conditions occur, such as a storm, a fire or a crime. The plan includes moving operations, (recovering operations) to another location if a disaster occurs at a worksite or datacenter. For example if a fire destroys an office building or datacenter, then the people and business or datacenter operations would relocate to a recovery site.

Best Practice KPI's

A DRP needs to encompass many needs at various levels. These KPIs should be scored with a grid showing impact of loss and risk point values.

- Conduct an annual exercise at the alternate facility
- A Business Continuity Plan (BCP) needs to be created and updated annually
- Conduct an annual tabletop exercise
- Review recovery strategies for RTO and RPO

Recommended Level of Reporting

- Business impact analysis: Identify the financial impact over time resulting from loss of a business process; includes identification and ranking of plausible events that could disrupt business processes.
- Plan development: Define a plan that includes people, processes, and systems that will be involved in a disaster recovery event.
- Training, testing, and exercising: Train all participants in the disaster recovery procedures, and then test plans on an ongoing basis through simulated exercises.
- Continuous improvement: Review and update the disaster recovery plan based on testing and exercising.

Observation/Findings and Recommendations

The table below outlines Open Enrollment Observation/Findings and Recommendations.

Observation/Findings	Recommendations
The CGI vendor staffing model does not align dedicated resources to Disaster Recovery support for Vermont.	Appoint a planning committee to oversee the development and implementation of the DRP. The planning committee should include representatives from all functional areas of the organization.
A DRP is documented but it has not been executed.	Complete the development, testing, and implementation of the disaster recovery plan. Execution of this DR plan should be repeated until all issues have been resolved and the requirements of 4 hour RTO and 30 minute RPO have been achieved.
A conceptual offsite DR facility (Philadelphia area) is described in the CGI M&O handbook. Our findings conclude this site is not built out for Vermont's needs. The vendor has no date when this critical DR site will be built out.	A DR site needs to be built, tested, maintained, and supported by CGI.
SOV DR coordinator identified that a production database was corrupted in September 2013. Tape backups were able to restore the database within a few days.	The backup and recovery process should be clearly documented including hardware, operating system, hosting environment and application components as a fallback approach until the disaster recovery plan can be completed and fully functional.
No Business Continuity Plan (BCP) for resources was presented.	A Business Continuity Plan (BCP) must be created, reviewed and approved with AHS (Agency of Human Services). SOV should work with AHS to coordinate the BCP along with the disaster recovery plan.

7. Documentation of VHC Platform

An assessment of the status of documentation of system artifacts needs to be completed, including a list of documents which are missing or in need of updates and an annotation of required changes.

CGI has not fully delivered completed documents required by the contract, including many of those stated within the Non-Functional Requirements section. CGI continues to work on these deliverables as they deem necessary.

Either CGI needs to complete these documents and review them with SOV or SOV should complete the various M&O documents they already started documenting. Without having completed and approved documents readily available to SOV, it is very difficult to identify defects versus incidents.

Document	Current State	Recommendations
Availability Management	Draft document exists	CGI's M&O Manual contains lots of information around availability management. Even though this M&O manual hasn't been approved by SOV it is a good starting point to review, update and sign off on. It is critical that this be completed and baselines established so that accurate metrics can be captured and reported on the availability of the connector
Batch Run Books	Exist	CGI produced examples of batch run books which contained everything expected except rerun/restart procedures. All batch run books should be updated to include run/restart procedures
Batch Schedule	Exist	According to CGI only 2 batch jobs exist.
Business Continuity Plan	Does not exist	SOV should take the lead on this
Capacity Management	Draft document exists	Document exists and CGI and/or SOV should complete this document to determine a baseline of the current process.
Change Management Flow	Draft document exists	Over the past couple of months lots of work has been done to improve the documents and process within this area. The documents are basically complete except for final review and approval by both CGI and SOV.
Change Management RACI	Draft document exists	CGI and/or SOV should review the existing RACI diagram and validate it covers all sources of changes and impacted parties.
Configuration Management Flow	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process.
Configuration Management RACI	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process.
Disaster Recovery Plan	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process. After the document has been completed it should be tested until both CGI and SOV sign off on its successful completion.
Escalation Contact List	Exist	Needs to be updated on a monthly basis or utilize email distribution groups which can be updated as attrition occurs.

Escalation Process Flow	Exist	Needs to be updated to include additional SOV resources or utilize distribution groups which can be updated as attrition occurs.
Event Management	Draft document exists	Within the unapproved CGI M&O manual, event management is thoroughly discussed. CGI should show SOV evidence that the documents reflect the current state of their event management within the production environment. Once this review is completed, the document should be updated to reflect any required changes.
Incident Process Flow	Draft document exists	Both CGI and SOV have draft versions of the Incident Process Flow. A decision should be made to adopt one of them and then both parties should review and sign off on it. The CGI version had a couple of cases where an incident can be closed without proper cause while the SOV version was complete except for being reviewed and approved by CGI.
Incident Process KPIs	Exists	KPI's have been documented and in some cases reported on. CGI should review the NFR's around Incident Process KPI's and add them into their documentation and reporting process.

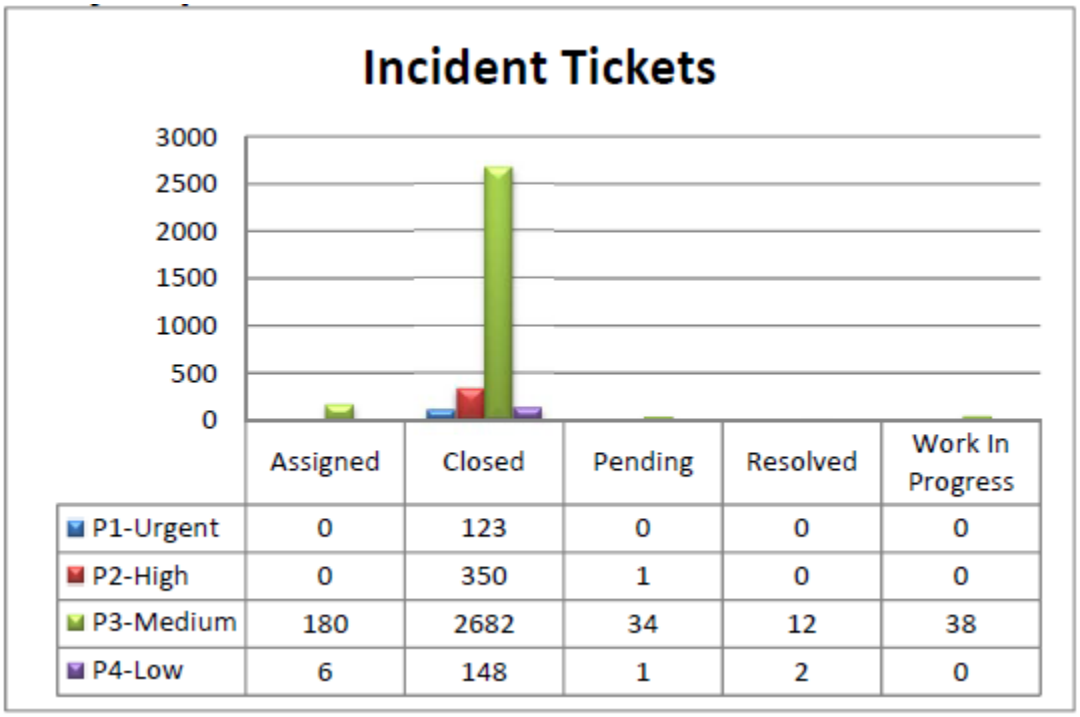
Document	Current State	Recommendations
Incident Process RACI	Draft document exists	CGI and/or SOV should review this document to make sure it contains all steps and impacted parties.
M&O Handbook	Draft document exists	Although this document has not been approved by the SOV, it contains useful information and is what the CGI M&O team is following. Both parties should review and validate that the information within this document properly reflects the current state of the connector and is the process which the CGI M&O team is following.
Monitoring	Draft document exists	CGI has documented how they planned on monitoring the connector but have failed to show proper evidence that they are indeed following their documentation. CGI should review this information with the SOV including how and what they are capturing within their monitoring.
Performance Management	Draft document exists	CGI has produced information around this area but it needs to include more data around what and how they are capturing this information. Without including this level of information the SOV will not know if the reported response time is from the first byte coming back on the GUI or all data being populated on the GUI.
Problem Management Flow	Draft document exists	Both CGI and SOV have draft versions of the Problem Management Process Flow. A decision should be made to adopt one of them and then both parties should review and sign off on it. As with the Incident Process Flow, the SOV version of the document was the most complete.
Problem Management KPIs	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process.
Problem Management RACI	Draft document exists	CGI and/or SOV should review this document to make sure it contains all steps and impacted parties.
Release Calendar	Draft document exists	With the rapid pace of changes still occurring within the platform a stable and accurate release calendar is hard to maintain. As the pace of change slows

		down a release calendar should be maintained and followed showing all known releases over the course of a full year.
Service Level Agreements	Draft document exists	SLA's are documented within the CGI M&O manual as well as within the NFR's. What needs to be included within these documents is how CGI is capturing and reporting on these SLA's so that both parties agree they are accurate and complete.
Service Level Management	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process.
Service Request Management	Draft document exists	CGI and/or SOV should complete this document to determine a baseline of the current process.
System Design Document	Draft document exists	An extensive and inclusive SDD exists which reflects the desired state of the connector versus the current implemented version. This document should remove those items which have yet to be delivered and update those areas where the implemented version is different from what was previously documented.

APPENDIX

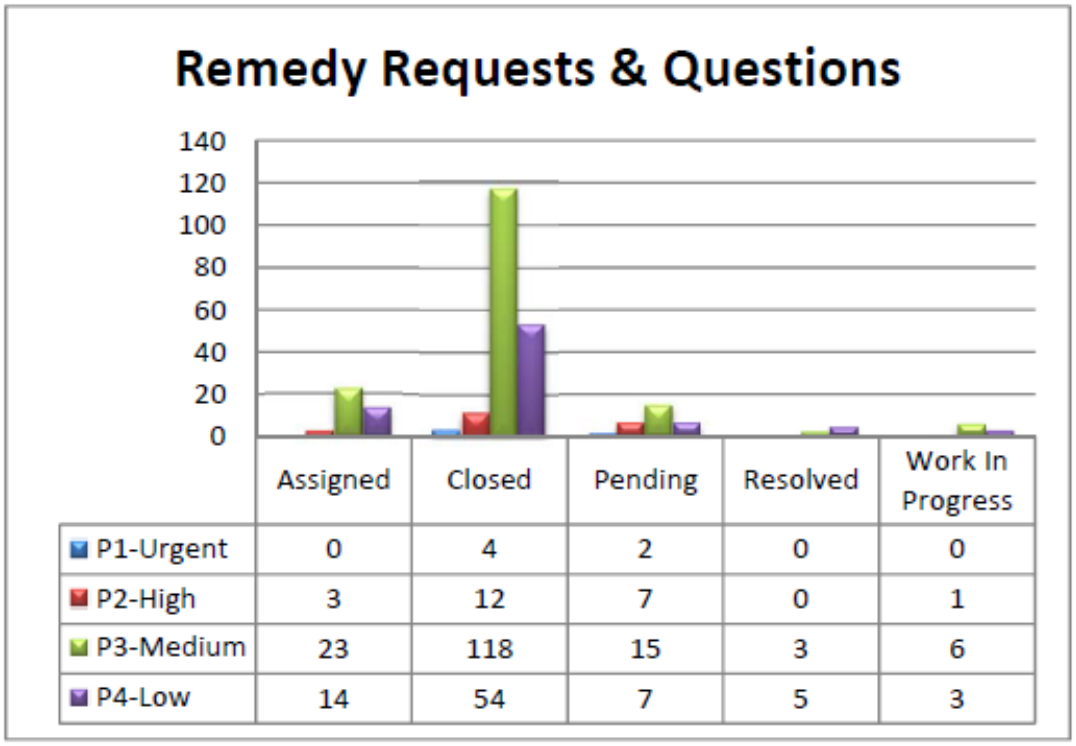
VT Health Benefit Exchange
HBE Status Report
05/17/14 – 05/23/14

Remedy Report Dashboard



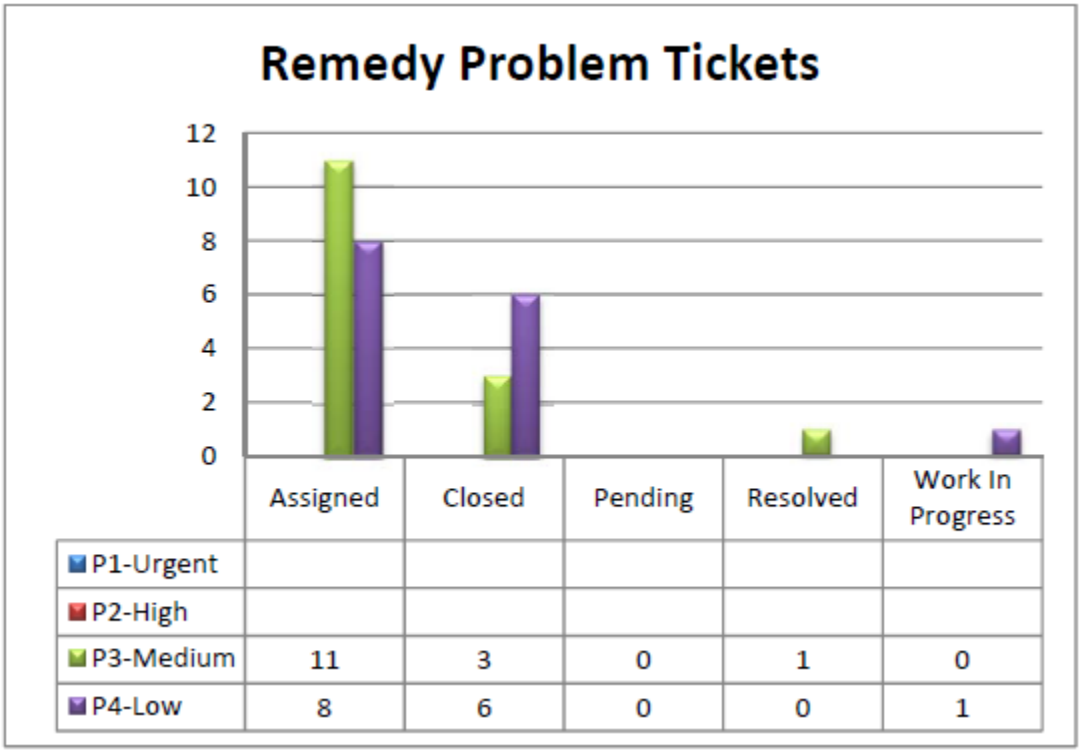
	Assigned	Closed	Pending	Resolved	Work In Progress
P1-Urgent	0	123	0	0	0
P2-High	0	350	1	0	0
P3-Medium	180	2682	34	12	38
P4-Low	6	148	1	2	0

Figure 1 - Incident Ticket Report



	Assigned	Closed	Pending	Resolved	Work In Progress
P1-Urgent	0	4	2	0	0
P2-High	3	12	7	0	1
P3-Medium	23	118	15	3	6
P4-Low	14	54	7	5	3

Figure 2 - Remedy Requests and Questions



	Assigned	Closed	Pending	Resolved	Work In Progress
P1-Urgent					
P2-High					
P3-Medium	11	3	0	1	0
P4-Low	8	6	0	0	1

Figure 3 - Remedy Problem Tickets

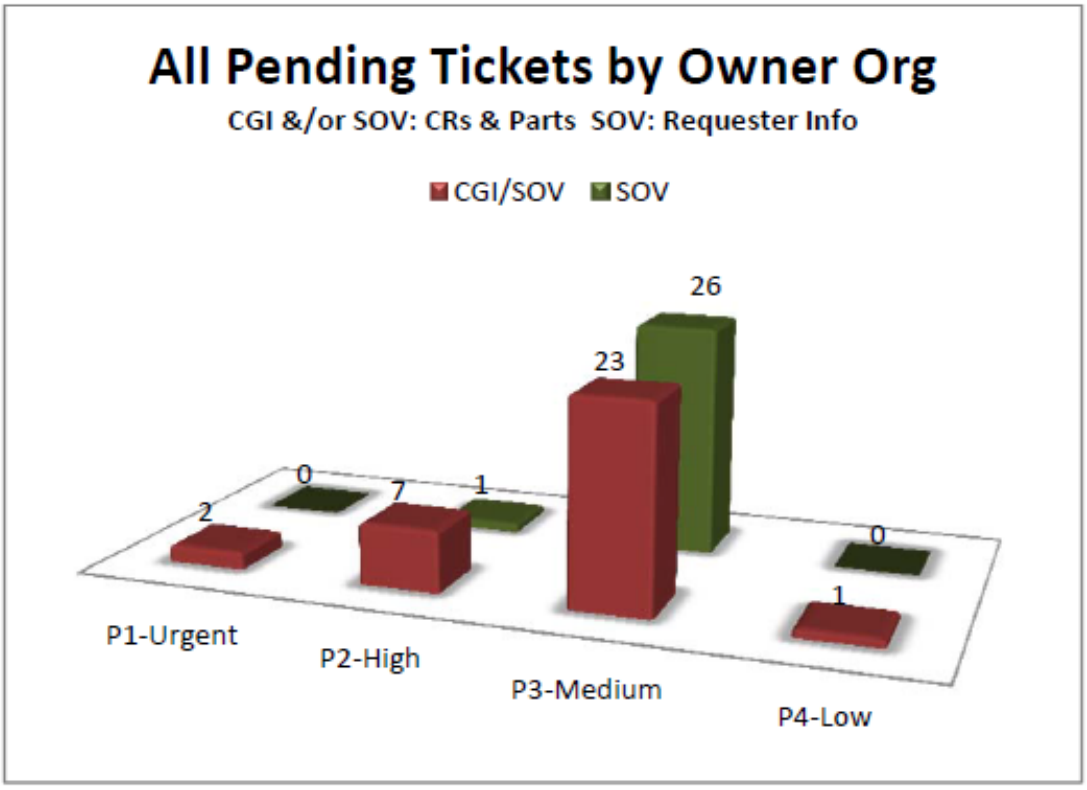


Figure 4 - All Pending Tickets by Owner Org

ITIL Process
[redacted]
Metrics and Reporting
[redacted]
Miscellaneous
[redacted]
Infrastructure
[redacted]
CGI Documents
[redacted]

Figure 5 - Documents Reviewed List

5.2.2 Roles and Responsibilities

This section describes the responsibilities of the person or group(s) shown on the organization chart. This section describes the function and owner for the roles identified in Exhibit 21.

Exhibit 22: Operations and Maintenance Roles and Responsibilities

Role	Responsibility
CGI IS/IT Steering Committee	▪ Monitors and reviews the delivery of CGI services through regular meetings whose frequency this Committee will determine. ▪ Reviews CGI- overall performance and discussrs the progress and resolution of any outstanding issues that could interfere with the delivery of CGI's services. ▪ Discusses SOV business strategies and outlook. ▪ Identifies any major planned SOV or CGI initiatives. ▪ Identifies situations where SOV can benefit from CGI's assistance. ▪ Ensures that effective decisions are made in order to meet SOV and CGI's business objectives. ▪ Makes the decisions necessary to ensure the business relationship proceeds smoothly. ▪ Approves any service changes that will have a major impact on the overall budget. ▪ Approves this Operational Framework.
CGI Service Delivery Teams	▪ Responsible for delivering the services based on the processes illustrated in Section 5 of this document.
CGI Account Manager	▪ Owns the SOV relationship and manages this business relationship according to the services outlined in this Framework. ▪ Provides direction and leadership to SOV on technology trends related to their use of CGI services and identifies and presents any new initiatives or business opportunities. ▪ Proactively seeks opportunities for improvement in operating effectiveness and cost. ▪ Co-ordinates periodic reviews of SOV Business Plans and outlook. ▪ Provides reports on CGI's monthly commitments, agreements and achievements to the CGI Management Office for consolidation into a CGI monthly report for SOV.
CGI Service Managers	▪ Ensure all CGI Service Delivery Groups understand their service commitments. ▪ Ensure that all SOV VHC service commitments are met by coordinating end-to-end service delivery. ▪ Manage the reporting and statistical information associated with the delivery of CGI services to SOV VHC. ▪ Ensure acceptance and production-readiness of new services by testing new products with the appropriate CGI Service Delivery Units. ▪ Communicate with SOV staff during incidents. ▪ Track all high/medium priority incidents to satisfactory resolution. ▪ Attend weekly Change Management meetings with CGI Change Control to review all outstanding change requests. ▪ Provide updates to this Operational Framework no less than once yearly.
Configuration Manager	▪ Obtains appropriate hardware. ▪ Installs and maintains application server software and database. ▪ Creates software repositories, schedules software deployment, is visibile on software installation status and deploys software applications. ▪ Restarts the application server and web service, if necessary. ▪ Establishes and manages application promotion approval processes. ▪ Prepares and distributes application release notes.

Role	Responsibility
Application(s) Administration	▪ Administers system management, monitoring, and development tools. ▪ Sets up, maintains, and supports the various environments, has a detailed understanding of database technology and troubleshoots systems issues. ▪ Installs and upgrades the Oracle server and application tools. ▪ Reviews performance, maintenance and utilities associated with each structure. Reviews backup and recovery strategies. ▪ Manages physical database resources and monitors database/subsystem performance issues. Plans for backup and recovery of database information. ▪ Reviews, where required, the purge/archive criteria. Assists in developing purge/archive criteria and procedures for historical application data. ▪ Reviews and monitors system and instance resources to insure continuous database operations (i.e., database storage, memory, CPU, network usage, and I/O contention).
Server Hardware/OS Maintenance Administration	▪ Performs daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviews system and application logs, and verifies completion of scheduled jobs such as backups. ▪ Performs daily system monitoring, verifies the integrity and availability of all hardware, server resources, systems and key processes, reviews system and application logs, and verifies completion of scheduled jobs, such as backups. ▪ Repairs and recovers from hardware or software failures. Coordinates and communicate with impacted constituencies. ▪ Applies OS patches and upgrades on a regular basis and upgrades administrative tools and utilities. Configures/ add new services as necessary. ▪ Performs ongoing performance tuning, hardware upgrades, and resource optimization as required. Configures CPU, memory, and disk partitions, as required. ▪ Creates backup images of Virtual Machine configurations and copies to Recovery Site, as necessary. ▪ Provisions new Virtual Machine instances per specifications on request. ▪ Restores Virtual Machine Instances as needed.
Desktop/Client Administration	▪ Restores Virtual Machine Instances as needed Installs, maintains, and troubleshoots issues on workstations. ▪ Implements, configures, and maintains desktop security system. ▪ Develops and distributes images for new and existing computers. ▪ Troubleshoots computer problems in a timely manner. ▪ Ensures routine maintenance on personal computers. ▪ Audits computers for presence of virus protection and installs new anti-virus software. ▪ Loads software when appropriate. ▪ Troubleshoots desktop issues. ▪ Tests new software for compliance with present technology. ▪ Monitors personal computers for illegal software. ▪ Maintains adequate spare peripherals to be used as needed.

Figure 6 - Roles and Responsibilities Chart

5.18.1 Incident Escalation Sub-Process

O&M Team Members continuously monitors the status of Severity 1 and Severity 2 incidents through to resolution. When technical and/or managerial resources need to be enlisted to resolve the incident in a timely manner and within the SLA, CGI escalates the incident and notifies SOV according to the guidelines in Exhibit 58.

1. Escalate the incident to CGI/VHC Infrastructure Lead if it is determined that the issue is infrastructure related
2. Open a Remedy ITSM ticket through integration with the relevant ticket information. This is a ticket to the PDC Ground because the issue is with the Date Center.
3. Update the incident within the Remedy ITSM system

Exhibit 58: Incident Escalation Timing

For incidents classified as…	Escalation happens…
Severity 1	When incident is identified
Severity 2	30 minutes after ticket creation unless resolved

Escalation occurs in the following sequence:

- CGI/VHC Tier1 Infrastructure
- CGI/VHC – Depending on the application error, this could be: Training, WebPortal, Siebel, OneGate, etc.
- CGI/VHC Development Manager
- CGI/VHC Operations Lead
- CGI/VHC Operations Director

OPTUM™

Vermont Health Connect HIX

Architecture Review

8/18/14

TABLE OF CONTENTS

1.....EXECUTIVE SUMMARY **3**
2. .....BACKGROUND **4**
3. .....ARCHITECTURE DIAGRAM **11**
4. .....FINDINGS / RECOMMENDATIONS **15**

1. EXECUTIVE SUMMARY

This report documents Optum's system architecture assessment with focus on the VHC application's adherence to industry standard and state (e.g. Oracle) Service Oriented Architecture (SOA) guidelines, and describes findings and recommendations.

Optum has concluded, based on a review of the VHC's architecture documentation and interviews with both SOV and contractor staff, that:

- The VHC architecture is sufficient to support the healthcare exchange and Medicaid needs of the people of Vermont for the foreseeable future, provided the population of the state does not grow significantly and user concurrency remains at current levels.
- Over 2500 non-functional requirements remain unmet.
- [redacted]

Architectural issues exist in the Exeter OneGate solution which will make further scaling of the solution to handle other elements of state government affairs such as driver licenses or SNAP registration difficult, these issues include:

i. Screen generation inefficiencies
ii. OPA's dependence on affinity based clustering ("sticky sessions")
iii. Lack of scalability certification and testing of the OneGate product by Exeter

.

Key Findings

Optum's assessment is based on the following Key Findings:

- Undelivered functional requirements – There are over 125 CRs still to be closed as of 6/25/2014.
- Undelivered Change of Circumstance capability
- Lack of a holistic, business level application and service monitoring strategy leveraging Oracle products.
- Undelivered non-functional capabilities impact the ease of use for the residents and employees of the State of Vermont.
    - Over 2500 non-functional requirements (NFRs), by State of Vermont count, remain open
- [redacted]
- Member's premium payments are sent to carriers in the same transaction as subsidies

Recommendations

Optum recommendations are summarized below. These recommendations are based on the findings described herein.

- Refactor service calls to leverage Oracle Service Bus (OSB)
    - Fully instrument environment for business level event notification
- Address partial payment with carriers issue with Benaissance
    - Separate and process the member's premium payment and the state subsidy (VPA) as separate transactions to the carrier
    - Develop a robust enrollment reconciliation process
- Implement a comprehensive configuration management process to migrate configuration changes from development to higher level environments – covered in the M&O report
- Leverage Oracle replication to create a live copy of the production DBs for OLAP purposes
- Fully adopt an MDM strategy including technical integration and a full data governance strategy
- [redacted]

- o [redacted]
- Additio al Act ivies to Consider
  - o Develop LOE for Oracle Service Bus implementation and instrumentation

Introduction

The following sections of this deliverable describe Optum's approach and further describe M&O findings and recommendations:

- Section 2.0 - Background outlines the approach used for preparing this deliverable.
- Section 3.0 – Architecture Diagram provides an end-to-end VHC application architecture diagram, color coded to designate concerns.
- Section 4.0 – Findings/Recommendations describes specific concerns and recommendations to improve the performance, stability, and scalability while improving the ability to proactively identify and remediate issues.

2. BACKGROUND

This report documents Optum's system architecture assessment, with focus on the VHC application's adherence to industry standard (e.g. Oracle) and state Service Oriented Architecture (SOA) guidelines, and describes findings and recommendations. Review of the system architecture included:

- Review of Enterprise Architecture reports and assessments conducted on individual solution components, integration of these components, and their implementation statuses as compared to expectations set forth in the scope of the CGI's contract requirements and artifacts related to individual solution components and current integration and implementation statuses: SOA, Oracle Identity and Access Management (IAM), Master Data Management (MDM), Siebel, Oracle Policy Automation (OPA), WebCenter Content/Capture, OneGate, and LifeRay into the VHC.
- Review of architecture and implementation of interfaces to external systems, including federal, other State of Vermont, Insurance Carriers, and Benaissance (premium processing) interfaces.
- Review of all Security and Privacy related assessments, documents, artifacts, and the current Plan of Action and Milestones (POAM) remediation status.

The scope of the assessment included VHC's set of commercial off-the-shelf (COTS) applications customized and integrated for the purpose of supporting the VT Health Exchange. Specifically, it includes the following:

- The Exeter OneGate product stack consists of:
  - o LifeRay Portal
    - Provides dynamic user interface
  - o Oracle Products
    - Oracle Policy Administration (OPA) rules engine
  - o A customized Siebel instance
    - Customer Relationship Management (CRM)
    - Plan data storage
    - Workflow capabilities
- Supporting the Exeter implementation:

- o Oracle Service Bus (OSB)
- o Oracle Identity Management (OIM, OAM, OVD, OAAM)

- Additionally, outside of the OneGate product, the State of Vermont integrates with:
  - o Benaissance and Carrier systems
    - ▪ 820 generation
    - ▪ Enrollment integration
    - ▪ Premium billing/payment
    - ▪ Serves as financial system of record
  - o Oracle WebCenter
    - ▪ Document management
  - o Thunderhead
    - ▪ Notices
  - o Oracle Business Intelligence Enterprise Edition (OBIEE)
    - ▪ Reporting
  - o Oracle Identity and Access Management (IAM)
    - ▪ ID Proofing
- Custom code written for Vermont
  - o Integration to the Federal Data Hub
  - o Integration to Benaissance
  - o Integration to carriers
  - o ACCESS
  - o MDM

All of these are individually solid products, it is the integration of, and functional modifications to them that limits the overall architecture scalability, adds risk, and increases complexity to the solution. With such aggregation of technologies, challenges are found in the integration between, and configurability of, these components. In this case, CGI was retained as the systems integrator and primary developer to provide this service.

In parallel with the application architecture assessment, a four phase security review was conducted:

- Discovery
  - o Identified requirements via discussions with State of Vermont
- Information Gathering
  - o Obtained materials from State of Vermont:
    - Detailed POA&M action plans
    - POA&M status management spreadsheet
    - Security Assessment Report
  - o Obtained control family priority from NIST 800-53r4

- Analysis
  - Categorized detailed POA&M action plans by control family
  - Assigned control priority, per NIST 800-53r3/4
  - Reviewed and summarized POA&M plans, to identify systemic issues
  - Identified potential risk exposure
  - Developed remediation recommendations
- Recommendations
  - Recommendations were developed to help address systemic challenge areas identified
  - Resolving the systemic challenges is expected to result in reductions in the identified control gaps areas, as well as preventing additional control gaps in the future.

The team met with the following SOV and vendor team members, and attended Enterprise Architecture\Business Analyst\Vendor meetings.

- State of Vermont
  - Lindsey Tucker
  - Rick Ketcham
  - Tom Mulhall
  - Jenn Loughran
  - Elizabeth McMullen
  - Claus Lund
  - Jack Green
  - Mike Morey
  - Chad Loseby
  - Chris Durfee
  - John Kohlmeyer
  - Justin Tease
- Contractors
  - [redacted]
- CGI
  - [redacted]
- Exeter
- Benaissance
- Archetype

The following project documents were reviewed:

Architecture Documents
• [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]

Business Analyst Support Documents
• [redacted]
Prior Assessments
• Vermont Health Services Enterprise Initial Implementation Review and Assessment ("Lessons Learned"); prepared by BerryDunn McNeil & Parker, LLC
Contract
• CGI Master Services Agreement, dated December 13, 2012

3. Architecture Diagram

This portion of the document contains a documented end-to-end VHC application architecture diagram. The diagram is color coded using the following:

[redacted]

VOC Application Architecture

[redacted]

This page intentionally left blank.

4. FINDINGS / RECOMMENDATIONS

This section of the document describes specific concerns and recommendations to improve the performance, stability, and scalability, while improving the ability to proactively identify and remediate issues. The observations/findings and recommendations are categorized as follows:

- Infrastructure documentation review
- SOA Strategy and Implementation
- LifeRay Portal
- Siebel Implementation
- Exeter Implementation
- ACCESS
- Master Data Management (MDM)
- Benaissance Implementation
- Reporting
- Governance / Process
- Security

A risk assessment is included with our Security assessment findings and recommendations.

This section also includes implementation status for the following:

- SOA Implementation
- Oracle Identity and Access Management (IAM)
- Master Data Management (MDM)
- Siebel
- WebCenter Content/Capture
- Oracle Policy Automation (OPA)
- OneGate
- LifeRay

Observations / Findings	Recommendations
Infrastructure	
The Disaster Recovery environment is not in place	Rebuild the Prod (UAT) environment from a defined specification. • Test and rework the specification until the Prod environment meets the needs and can be reliably built from the specification. • Build new stage and disaster recovery environments off the certified production specifications.
SOA Strategy and Implementation	
The Vermont Enterprise Architecture Framework (VEAF) is tightly in line with Oracle published Service Oriented Architecture (SOA) guidelines	NA
[redacted]	[redacted]

Observations / Findings	Recommendations
The monitoring, reporting, and dashboarding capabilities of the Oracle SOA stack are not fully implemented. • Use of these capabilities will provide service timings for each component at the atomic transaction level including, service performance and access to XML message payloads. Another valuable element of the Oracle monitoring integration is the ability to trigger alerts. • For each service defined in the Oracle Service Bus proxy, service errors and timing thresholds can be defined that can send email alerts and provide real-time statistics through the Oracle Business Activity Monitor (BAM) dashboard. BAM provides visibility into the lifecycle of a business transaction (e.g. Consumer application processing) as it spans multiple components of the overall architecture. • [redacted]	Full implementation of OEM and BAM products: • Instrumentation of all services with alerts to notify on error or exceeding the defined performance threshold. • Construct a BAM-based, real time dashboard displaying the SLA performance at any giving time. • Evaluate the business transaction to ensure that all impacted components have a corresponding agent interacting with OEM/BAM. • [redacted]

Observations / Findings	Recommendations
LifeRay Portal	
Web site response time is consistently scored as "Egregious Failure" - NFR H5.1.68 - UI level transaction should complete in 5 seconds (on average) • The average screen load time, as tested, sits at 9-11 seconds, none below 9. • [redacted] • The UI requires too many "next" responses. As noted, due to the dynamic screen generation there are times where only one or two questions are presented. Each time "next" is pressed, the [redacted]	Work with Exeter to on product changes to minimize the number of screens presented to the user and the number of calls to the back-end required to create a page. Explore with Exeter product flow, page design, and caching technologies which can be added to the infrastructure to better serve pages.
[redacted] • [redacted]	Work with Exeter/Oracle on product changes to eliminate this design flaw. Due to low concurrency, these have not been impactful yet. Schedule scale and performance threshold tests to understand the break point of these two limitations.
Solution lacks a "purpose built" feel: • The value adds for an offering is providing the business process around the capability. While the rules are impressive, there are not sufficient integration points for business process (e.g. Plan and rate validation, customer service scripting and workflow).	Work with Exeter and systems integrator to identify and develop more integration points such as plan and rate validation in core application.
[redacted] • [redacted]	[redacted] • [redacted] • [redacted] • [redacted] • [redacted]

Observations / Findings	Recommendations
Siebel Implementation	
[redacted] • [redacted] • [redacted] • [redacted]	Do not consider upgrading HIX Siebel instance unless it is a part of an Exeter product upgrade. Exeter should partner with Oracle to understand version issues to mitigate compatibility risk. Do not leverage HIX Siebel instance for any work outside of HIX.
Siebel workflow not sufficiently enabled. NFR SLN12.1.41 - Solutions shall enable central workflow alerts and transactional status. Solutions shall centralize pending work items for the user as in a work queue • Currently, all work requests sit in a single Siebel queue for all work items, not for individual users. State of Vermont users execute queries against the list of work to find items to process	Work with Exeter to improve integration with Siebel. Build out workflow using Siebel to create and manage individual work queues. Exeter needs to coordinate more closely with Oracle to understand version issues and how they can mitigate compatibility risks.
[redacted] ▪ [redacted] ▪ [redacted]	[redacted]

Observations / Findings	Recommendations
Exeter Implementation	
Exeter rules implementation for Medicaid and HIX rules are logically coupled: • The Vermont rules sit as a layer atop the Federal rules. This makes maintenance between VT specific and Federal rules difficult. • VT had expressed a need to be able to independently manage the state specific rules (e.g. Medicaid). This is enabled by the layering of State rules atop of the Federal rules, where the state rules will "override" the Federal rules. While physically separate there is a logical interdependency between the tiers of rules that present a testing and configuration management challenge. This interdependency must be addressed if the State moves forward with its plan to manage their portion of the rule set.	Work with Exeter to develop a defined process and strategy for rule creation/customization. Ensure State of Vermont originated rules are logically separate to avoid Exeter update challenges. • Note: The layering ability within OPA allows the state to create a separate and logically isolated set of rules in support of integrated eligibility for services that extend beyond HIX/Medicaid rules
ACCESS	
[redacted] • [redacted]	[redacted] • [redacted]

Observations / Findings	Recommendations
Master Data Management	
[redacted]	
[redacted]	

Observations / Findings	Recommendations
Benaissance Implementation	
Partial Premium Payments are being improperly managed: • The SOV decision to communicate aggregated Vermont Premium Assistance (VPA) member premium amounts as the member portion of the premium appears to conflict with the timing of the actual payments. This results in scenarios where carriers will interpret an incremental payment as a partial payment and mark the consumer as delinquent. NOTE: This is not a Benaissance best practice as executed in other implementations.	Communicate VPA and Member premium amounts as separate values: • The 834 to the carrier would need to be modified to treat the member and VPA portions of the premium as separate values. • Carriers would need to create an additional AR (split bill) to treat the VPA as a separate payment. ○ NOTE: This is the accountability of the carrier as HCR defines rules for when a carrier can terminate a member based on member payments (separate from State and Fed payments). We consulted with the UHC Carrier division that has implemented exchanges to confirm this assumption. • Carriers would implement rules to only mark the member as delinquent when the member portion is not received.
Missing enrollment reconciliation is not occurring • Enrollment discrepancies between the Benaissance and Siebel can result in billing issues. This would be addressed through a proactive enrollment recon between the two systems, prior to the billing cycle. NOTE: This is a Benaissance best practice and is executed at its other implementations.	Institute a two-sided enrollment reconciliation process: • Help to reach the root cause of discrepancies • Benaissance is currently capable of producing a monthly enrollment recon file. This capability would be turned on. • A similar file will need to be generated from Siebel. • Implement a compare process (automated or manual) to produce a delta report. • SOV operations would manually work the delta report to resolve discrepancies between the systems.

Observations / Findings	Recommendations
Reporting	
[redacted] • [redacted] • [redacted]	Leverage Oracle replication to create a live copy of the production DBs for OLAP purposes: • Archetype would shift their current datamart jobs to query against the OLAP replica.
[redacted] • [redacted] • [redacted]	Explore adding a tool for larger dataset analysis.
Due to a OneGate architectural design issue, there exists no full lifecycle view of applications: • Currently, there exists no view/report showing all applications in process. • [redacted]	Implement one of the following three Options: 1. Create a report for case managers that allow them to see the apps in progress. 2. Develop an applet to pull application information from the staging tables and makes it searchable/visible to case managers. 3. Use the data in the staging tables to create a case when an application is started. ○ Intercept the submit and look for an existing case before creating a new one.

Observations / Findings	Recommendations
Governance / Process	
Configuration Management is inconsistent. • Specified in NFRs CM-01.01-00, NFR CM-01.01-01, and NFR CM-01.01-02 Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. • Plan data is entered directly into the each instance of Siebel (Dev / Test / Prod / Etc.). • Configuration changes are not uniformly moved through the various dev / test / stage environments, but rather migrated on an ad hoc basis – varying by type with impacts including: ○ Plan Data ○ Security ○ Dropdowns ○ Screen Options ○ Testing and Training	Configuration should migrate through environments not be manually entered. Implement a configuration management process to migrate configuration changes from development to higher environments. • All configuration in higher environments should be imported from lower environments. • Configuration should not have environment specific information.

Enrollment reconciliation is not occurring with Carrier. • Enrollment discrepancies between the exchange and carriers can result in customer expectations not being met, such as: o Enrollment timeliness o Fulfillment issues o Billing issues	Reconciliation is important to the process of discovering the root cause issues and proactively address discrepancies between the exchange and carriers. *Recon options:* ▪ State performs recon o Carriers need to produce a monthly enrollment recon file o Carriers send recon file to the state o An extract is pulled from Seibel of all enrollments for that carrier. o The state performs a recon between the state and carrier files ▪ Contract a third party (FFM model) ▪ Create an automated compare ▪ Perform a manual compare o The state notifies the carrier of recon issues works with the carrier to resolve discrepancies. ▪ Carrier performs recon o Carriers need to produce a monthly enrollment recon file of enrollments for that carrier and sent to the carrier. o The Carrier performs a recon between the state and carrier files. o The Carrier notifies the State of recon issues works with the State to resolve discrepancies.

Security Review and Risk Assessment

Observations / Findings	Recommendations
[redacted]	
[redacted]	[redacted]
Vendor relationship management and coordination – HIGH Risk **CGI is listed as primary (presumably due to relationship with PDC)**	
Optum observed: • Requested vendor documentation not provided. • Contract terms, roles, and responsibilities not fully defined. Risk Ineffective vendor relationships can result in: • Support gaps due to unclear roles and responsibilities. • Uncertainty concerning accountability and liability. • Reduced visibility to activity status and security posture. Audit/assessment findings, due to missing information.	As detained in the Optum PMP deliverable, SOV needs to better : • Define and clarify roles and responsibilities. • Ensure contracts reflect all requirements, roles, and responsibilities. • Actively engage vendors to maintain communication, and follow up on issues. • Improve oversight and monitoring of PDC.

Observations / Findings	Recommendations
[redacted] – HIGH Risk **Primarily CGI or shared between CGI and SoV**	
[redacted]	[redacted]
[redacted] – HIGH Risk **Primarily SoV, or shared between CGI and SoV**	
[redacted]	[redacted]
[redacted] – HIGH Risk **Primarily shared between CGI and SoV**	
[redacted]	• [redacted] • [redacted]
Incomplete Documentation (not addressed above) – Medium Risk **Primarily CGI or shared between CGI and SoV**	
Risk Lack of documentation can result in procedural errors, and impact ability to satisfactorily respond to audits.	SoV: • Monitor to ensure appropriate documentation exists and is maintained. CGI: • Create required documentation. • Implement processes to maintain documentation.

Observations / Findings	Recommendations
[redacted] – **Medium Risk** **Primarily CGI as developer of original POAM**	
[redacted]	[redacted]
Security Architecture Recommendations	
Based on the limited review done during this assessment, additional architecture / technology assessments would be recommended for the following capabilities: • [redacted]	

Implementation Status

The following tables describe Implementation Status and include our findings from the State of Vermont implementation of the following architectural components:

SOA Implementation
As specified in NFR SLN 1.1.2 and NFR SLN 4.1.62 a service bus strategy has not been implemented on the Vermont HealthConnect implementation. This limits the alignment to the SOV SOA Architecture guidelines as well as system extensibility through standard and customary SOA methods. In addition, service level governance, monitoring and alerting are not automated as part of Vermont HealthConnect and is mainly manual and/or derived from log files. This negatively affects the architecture is as follows: • Lack of a centralized service repository • Lack of centralized bus security • Lack of centralized bus routing • Lack of centralized service invocation • Lack of centralized service level monitoring • Lack of centralized/reusable transformation

Oracle Identity and Access Management (IAM)
[redacted]

Master Data Management (MDM)

Implementation is incomplete for:

- Eligibility alert updates
- MDM data sync with Siebel

Siebel to uses MDM contact when possible vs creating a new contact
Need to resolve the existing duplicate
    Add Address
    Add Account/Organization/Employer information
ACCESS Combined contact is not being used to further update MDM
The components to support visibility events from ACCESS are installed but currently disabled based on an SOV request

Siebel

[redacted]

WebCenter Content/Capture

- Thunderhead notices are not released, appears to be stuck in defining the Notices
- Using a Manual Notice Transmission process - Need to transition to Thunderhead

Oracle Policy Automation (OPA)

This architectural element was delivered as a part of the Exeter solution and not customized by the State of Vermont. State of Vermont's architecture build-out provides a sufficient environment to support current usage.

OneGate
This architectural element was delivered as a part of the Exeter solution. Customizations to the Exeter code for SOV require validation each time an upgrade to the application is made. State of Vermont's architecture build-out provides a sufficient environment to support current usage.

LifeRay
This architectural element was delivered as a part of the Exeter solution and not customized by the State of Vermont. State of Vermont's architecture build-out provides a sufficient environment to support current usage.

OPTUM™

Vermont Health Connect HIX

Code Review

8/18/14

TABLE OF CONTENTS

1. .....EXECUTIVE SUMMARY 3
2. .....BACKGROUND 4
3. .....COMPONENTS ASSESSMENT 5
4. .....CODE REVIEW RESULTS 7
5. .....RECOMMENDATIONS 8
APPENDIX A – CODE REVIEW CHECKLIST 9
APPENDIX B – QUALITY CODE EXAMPLES 18
APPENDIX C – DETAILED CODE REVIEW RESULTS 27

1. EXECUTIVE SUMMARY

The purpose of the code review deliverable is to:

- Identify the key components of the VHC Solution that present the greatest vulnerabilities and determine assets requiring a code review
    - Focus will be placed on code structure and the use of industry standard coding practices which enable integrity and optimal performance
- Document code review results
- Provide recommended improvements/actions
- OneGate code was not turned over for review

Optum has concluded, based on the code review, the interface framework between the OneGate product and other internal (e.g. Benaissance) and external (e.g. Carriers) components do not following industry standards for design and development. This has led to inefficiency in performance and maintainability.

As a result, future enhancements to the interfaces may require rewrite of the code as it is not extensible in its current state. System performance will also be impacted requiring additional infrastructure resources to manage these interfaces since they haven't been designed efficiently.

Key Findings

Optum's assessment is based on the following key findings:

- The code review revealed several significant findings that fall into two basic areas of review: Performance and maintainability. Out of the 176 items reviewed, only 27 modules were evaluated as high quality in the area of performance and maintainability.
    - Performance – The largest impact to performance is going to be the improperly defined objects that are putting a burden on the java virtual machine (JVM) by causing the garbage collection process to run more often than warranted.
    - Maintainability – The number one item that came up in almost every class was the lack of documentation explaining what the purpose of the class and APIs and why there was specific logic in them. Poorly documented APIs lead to confusion when enhancements need to be made in future releases. This leads to extended development times and potential coding mistakes.

Specific findings are described in Section 4 – Code Review Results.

Recommendations

Optum's recommendations are summarized below:

- Update the project's Quality Assurance process to include periodic code reviews based on mutually agreed industry best practice.
- Perform root cause analysis on the relationship between code quality issues and open defects.
- Establish a process for future enhancements that incorporates the new coding standards into a future code updates.
- Prioritize remedy of code quality issues with outstanding defects and change requests.

Introduction

The following sections of this deliverable describe Optum's approach and further describe the Code Review findings and recommendations:

- Section 2.0 - Background outlines the approach used for preparing this deliverable
- Section 3.0 – Components Assessment describes the rational for selected code for review and criteria for evaluating the code
- Section 4.0 – Code Review Results documents findings from the code review
- Section 5.0 – Recommendations describes recommended next steps in response to the findings
- Appendix A – Code Review Checklist documents standards and guidelines that provided the criteria for the review
- Appendix B – Code Quality Examples provides 18 examples of code that does not comply with the criteria and a preferred alternative
- Appendix C – Detailed Code Review Results provides a spreadsheet documenting the results for each object reviewed

2. BACKGROUND

Code quality is an important aspect of system quality and maintainability. Poor quality code exhibits the following characteristics:

- Not well documented
- Not well structured
- Inconsistent due to lack of standards, or not following standards

This can lead to a number of problems:

- The system is difficult to maintain
- The system does not gracefully handle adverse conditions
- The system does not behave consistently across various system components

Quality code is readable, consistent, and well-constructed, built on a solid foundation of standard classes and proven coding patterns. This results in a high-quality, consistently resilient system and the ability to maintain the system with confidence and avoid unexpected errors.

Optum's code review approach was based on:

- Using our previous architecture review experience in Hawaii as input for selecting the functional components to be reviewed.
- Interviewing SOV team members, including enterprise architects, to identify pain points with interaction between systems. (Rich Ketcham, Seamus Loftus, Michael Lapera, Justin Tease, and Chad Loseby)
- Interviewing project vendors to understand how they managed their software development lifecycles, build processes and deployment strategies.
- Review of SOV documents [redacted]

3. Components Assessment

VHC code targeted for review was narrowed down through interviews with the various teams from SOV, CGI, Benaissance, BCBS, and Exeter. The selection of code also considered our experience from similar engagements and our familiarity with the stability of VHC's architecture.

Based on the interviews, it was concluded that the 'hot-spots' were within the interfaces between the OneGate product and Benaissance, Carriers, Fed-Hub, and CoC.

Code Review Criteria
The following criteria, based on industry best practices, were used to assess code quality.

Code Review Criteria	
Criteria	**Criteria Description**
Maintainability	
Code style	'Code Style' review includes the following items: brace location, line length, method, variable, class naming standards, and appropriate white space.
Comments	Comments are frequently redundant, but comments but should be provided if the developer did something unusual or it aids the ability of another developer to later modify the code. For example, "The first result from this third-party system is always null due to a bug on their end." This also applies to complex functions or algorithms.
Externalized Configuration	'Externalized Configuration' review looks for things that are likely to change—number of items on a page in a paginated list, or the options in a dropdown list—and ensures they're modifiable without changing the code. This also includes confirming that they are pulled from your standard location, whether that's a database or a file on a file system, or another location.
No Commented Code	If code is commented out, it should be deleted. Source control can be used to restore code, if necessary.
Duplicate Code Checks	'Duplicate code checks' looks for code performing similar functions; this is an opportunity for refactoring and/or removing duplication. This frequently occurs when a developer is working in an unfamiliar area of the system, or when the system is large and has many utility classes and methods.
Embedded Policies	'Embedded Policies' looks for rules or policies that have been embedded into the code which would make it difficult to change; policies should use an external policy engine.

Code Review Criteria	
Criteria	**Criteria Description**
Performance	
Input Validation	'Input Validation' confirms that input from the end user is scrubbed and encoded and confirms that third-party utilities are all surrounded with appropriate try-catch blocks and error handling.
Code Testability	'Code Testability' ensures interfaces can be mocked, and that test frameworks can exercise methods. It's best to keep the constructor slim and put any logic in a method that the constructor calls, which also renders that method testable.
Unit Test Exists	'Unit Test Exists' checks for unit and/or integration tests that go beyond "assert true". The process and expectation for Unit Test should be established by the Quality team and it is often measured by proxy through checking the coverage level.
TODOs	'TODOs' review determines if its use is acceptable. For example, a "TODO: implement security restrictions" might be okay as long as it's fixed before deployment, but it may not be acceptable prior to deployment.
Loops	"Loops' review checks for length and appropriate exit criteria and for speed. Loops that have many objects may be too slow. This falls into the category of frequent mistakes for many developers.
Existence Checks	'Existence Checks' confirms that an object exists before using it. This helps put error handling close to the source of the problem. This is particularly true for anything obtained from a location outside the system (e.g., the response to a call to another system, or a file read off the file system).

Code Assessed
A cursory review of all 176 artifacts was performed to give a high-level view of the current state of the code. From this cursory review Optum identified 46 classes that were auto-generated and were not candidates for review and 103 classes that required an in-depth review. Each artifact was then assessed across each applicable assessment area and a quality and criticality rating was assigned.

Quality Ratings
The following table defines our quality ratings and their meanings:

Quality Rating	Meaning
Low	The code artifact diverges significantly from expected quality criteria.
Medium	The code artifact contains some variation from the expected quality criteria.
High	The code artifact follows all expected quality criteria.

Criticality Ratings
The following table defines our criticality ratings and their meanings:

Criticality Rating	Meaning
Low	This measure of quality has minor impact to the overall stability, maintenance, and/or usability of the system.
Medium	This measure of quality has some moderate impact to the overall stability, maintenance, and/or usability of the system.
High	This measure of quality has significant impact to the overall stability, maintenance, and/or usability of the system.

4. Code Review Results

The following dashboard includes charts that summarize our code review results:

- The chart on the left depicts quality levels by criticality
- The chart on the right presents quality/criticality rank determination for all reviewed items
- An overall quality/criticality index is also provided

The charts are based on the review of the twelve code review criteria listed in Section 3. Each class was evaluated using the twelve items and each item was scored as an independent workable task. This allowed for a capture of the effort of work required at a finer level than rolling it up to each class.

[redacted]

Issue Summary

The above graph shows the rankings for the key areas we focused our code review on:

- Green shows items that are deemed not a critical impact to the application
- Yellow has a medium impact to the application
- Red was a major impact to the application

The N/A represents those sections that were not evaluated because they were auto-generated classes or interface type classes that did not have any notable code to evaluate.

The code review revealed several significant findings that fall into two basic areas of review: Performance and maintainability. [redacted] Specific issues are described in the following sections.

Performance

[redacted]

- **Impact:** Ongoing performance of the system
- **Impact Level:** Medium to High

Maintainability

[redacted]

- **Impact:** Ongoing maintenance of the system and the ability to perform automated testing
- **Impact Level:** High

5. RECOMMENDATIONS

Optum's recommendations, as an outcome of our code review, include:

- Update the project's quality assurance process to include periodic code reviews based on mutually agreed industry best practice. This includes establishing code quality criteria that serve as the basis for the review.
- Perform root cause analysis on the relationship between code quality issues and open defects
- Establish a process for future enhancements that incorporates the new coding standards into a future code updates
- Prioritize remedy of code quality issues with outstanding defects and change requests

APPENDIX A – CODE REVIEW CHECKLIST

This appendix contains the code review checklist.

#	Item/Description	Standard/Guideline?
	File Organization	
1	Each Java source file contains at most one public class or interface.	Standard
2	The base name of the source file is the same as the name (with the same case) of the public class or interface. Exception: If a Java source file does not have a public class or interface, its base name can be anything.	Standard
3	A package is a self-contained group of related classes.	Standard
4	The classes within a specific package should match the classes within the software design class diagram.	Standard
5	Each Java source file has the following mandatory sections and is laid out in the following order: - Package Statement - Import Statements - File Header - Class and Interface Declarations	Guideline
6	The first non-comment line of a Java source file is the package statement and it is mandatory for every Java source file. The naming convention for the package statement is: package org.vt.<function> For example: package org.vt.framework; package org.vt.client.dao; package org.vt.utils.logger; package org.vt.utils.exception;	Standard
7	No Java source file belongs to the "default" package.	Standard
8	There is one import statement for each class imported from a package as shown in the following example: import org.vt.client.dao.CreateCaseDAO; import org.vt.client.dao.UpdateCaseDAO; import org.vt.framework.exception.DataException; Remove unused import statements from the Java class	Standard
9	The file header is needed to capture information about the file as a whole.	Guideline
	Class and Interface Declaration	
10	Static attributes, also known as class attributes, are given valid values at the time of declaration.	Guideline
11	All interfaces are inherently abstract; this keyword should not be explicitly included in the declaration of an interface.	Guideline
12	First the public class variables, then the protected, then the package (no access modifier), and then the private static variables should be declared.	Guideline
13	Each static variable is declared in a line by itself.	Standard
14	A Javadoc comment for each static variable immediately precedes it.	Standard
15	Any static initializers for class variables immediately follow the class variable declarations.	Standard
16	All interface fields are inherently public, static, and final; these keywords should not be explicitly included in the declaration of an interface field.	Guideline

#	Item/Description	Standard/Guideline?
17	Each constructor has a method header (Javadoc comment for the method) immediately preceding it.	Guideline
18	The methods in a class or interface are grouped by functionality rather than by scope or accessibility.	Guideline
19	Each method has a method header (Javadoc comment for the method) immediately preceding it.	Standard
20	All interface methods are inherently public and abstract; these key words should not be explicitly included in the declaration of an interface method.	Guideline
21	The first line of the Javadoc comment (/**) for classes and interfaces is not indented; subsequent Javadoc comment lines each have 1 space of indentation (to vertically align the asterisks).	Standard
22	The opening brace for a Class / Interface statement is on the next line at the same indentation level as the Class / Interface statement.	Standard
23	The closing brace for a Class / Interface statement is on a line by itself aligned with the indentation level of the Class / Interface statement.	Standard
24	Any instance or class variables are not be made public without good reason.	Guideline
	Naming Convention	
25	The prefix of a unique package name is always written in all-lowercase ASCII letters and should be one of the top-level domain names, currently com, edu, gov, mil, net, org, or one of the English two-letter codes identifying countries as specified in ISO Standard 3166, 1981. Subsequent components of the package name vary according to an organization's own internal naming conventions. Such conventions might specify that certain directory name components be division, department, project, machine, or login names. Examples: **com.sun.eng**; **com.apple.quicktime.v2**	Guideline
26	Interface names are capitalized like class names. Example: **interface RasterDelegate**; **interface Storing**	Standard
27	Methods should be verbs, in mixed case with the first letter lowercase, with the first letter of each internal word capitalized. Example: **run()**; **runFast()**; **getBackground()**	Standard
28	Variables names are mixed or proper case starting with a lower case first letter. They should not start with underscore _ or dollar sign $ characters, even though they are both allowed. They should be short yet meaningful and the choice of a variable name should be mnemonic.	Guideline
29	The names of variables declared class constants and of ANSI constants are all uppercase with words separated by underscores ("_"). (ANSI constants are avoided, for ease of debugging.) Example: **static final int MIN_WIDTH = 4** **static final int MAX_WIDTH = 999** **static final int GET_THE_CPU = 1**	Standard

#	Item/Description	Standard/Guideline?
	Member Functions should be named using a full English description, using mixed case with the first letter of any non-initial word capitalized. It is also common practice for be a strong, active verbthe first word of a member function name to be a strong, active verb. openAccount() printMailingLabel() setFirstName(String aName) setAccountNumber(int anAccountNumber) save() delete()	Standard
	Getters/Setters are member functions that return the value of a field. You should prefix the word 'get' to the name of the field, unless it is a boolean field and then you prefix 'is' to the name of the field instead of 'get.' getFirstName()getAccountNumber()	
	Loop counters: It is generally accepted to use the letters **i**, **j**, or **k**, or the name '**counter**.' **i**, **j**, **k**, **counter**	Standard
	Boolean getter member functions: All boolean getters must be prefixed with the word 'is.' Ifyou follow the naming standard for boolean fields described above then you simply give it the name of the field. **For Ex: isPersistent(), isString(), isCharacter()**	Standard
	Coding Convention	
30	Accessor member functions: Consider using lazy initialization for fields in the database. Use accessors for obtaining and modifying all fields. Use accessors for 'constants". For collections, add member functions to insert and remove items. Whenever possible, make accessors protected, not public	Standard
31	Fields: Fields should always be declared private. Do not directly access fields, instead use accessor member functions. Do not use final static fields (constants), instead use accessor member functions. Do not hide names. Always initialize static fields	Standard
32	Classes: Minimize the public and protected interfaces. Define the public interface for a class before you begin coding it. Declare the fields and member functions of a class in the following order: **Constructors, finalize(),public member functions, protected member functions, private member functions, private field**	Standard
33	Local variables: Do not hide names. Declare one local variable per line of code. Document local variables with an endline comment. Declare local variables immediately before their use. Use local variables for one thing only	Standard
	Code Syntax	
30	Tabs are used as the unit of indentation. Tab size is set to 4.	Guideline
31	Lines longer than 100 characters are avoided; Note: Examples for use in documentation should have a shorter line length - generally no more than 70 characters.	Guideline

#	Item/Description	Standard/Guideline?
32	When an expression will not fit on a single line, it is broken according to these general principles: - Break after a comma - Break before an operator - Prefer higher-level breaks to lower-level breaks - Indent the subsequent lines 1 space beyond the parenthesis. - If the above rules lead to confusing code or to code that is skewed towards the right margin, just indent eight spaces instead.	Guideline
33	Line wrapping for if statements uses the eight-space rule since conventional (fur space) indentation makes reading the body more difficult.	Guideline
34	Three acceptable ways to format ternary expressions are provided below. **alpha = (aLongBooleanExpression) ? beta : gamma;** **alpha = (aLongBooleanExpression) ? beta** **: gamma;** **alpha = (aLongBooleanExpression)** **? beta** **: gamma;**	Guideline
Comment		
35	Java programs have two kinds of comments: documentation comments and implementation comments.	Standard
36	Javadoc comment (/**…*/) starts in the same column as the Class / Interface statement that follows it.	Standard
37	Implementation comments are delimited by /*...*/, and //.	Standard
38	Documentation comments (known as "Javadoc comments") are Java-only, and are delimited by /**...*/.	Standard
39	This comment (/*...*/, not a Javadoc comment) should contain any class-wide or interface-wide information that was not appropriate for the Class / Interface documentation comment.	Guideline
40	This comment (/*...*/) should be started from the line immediately following the opening brace of the Class / Interface definition and is indented one level relative to the Class / Interface statement.	Guideline
41	Code comments are clear and concise.	Guideline
42	Comments are necessary or helpful.	Guideline
43	Java code for the most part is self-documenting so the use of comments can be kept to a minimum.	Guideline
44	Implementation comments can be block comment, single-line comment, trailing comment or comment to take out code.	Guideline
45	Comments are not enclosed in large boxes drawn with asterisks or other characters.	Guideline
46	Comments do not include special characters such as form-feed and backspace.	Guideline
Comment- Block Comment		
47	Block comments are used for the Copyright Header, File Header, Class / Interface implementation comment	Standard
48	Block comments can also be used within methods to describe data structures and algorithms. Block comments inside a method should be indented to the same level as the code they describe.	Standard
49	A block comment should be preceded by a blank line to set it apart from the rest of the code.	Standard

#	Item/Description	Standard/Guideline?
0	Block comments have an asterisk "*" at the beginning of each line except the first.	Standard
51	Block comments can start with /*-, which is recognized by indent(1) program as the beginning of a block comment that should not be reformatted.	Standard
Comment- Singe-Line or Trailing Comment		
52	Short comments appear on a two lines indented to the level of the code that follows, otherwise, if a comment cannot be written in a two lines, it should follow the block comment format.	Standard
53	A blank line precedes a two-line comment.	Standard
54	Very short comments are shifted far enough to separate them from the statements; If more than one short comment appears in a chunk of code, they should all be indented to the same level.	Guideline
55	Trailing comments can be used with package and import statements; The trailing comments that are split into multiple trailing comments should all be indented to the same level.	Guideline
Comment- End-Of-Line Comment		
56	End-Of-Line comments are not used on consecutive multiple lines for text comments	Guideline
Statements		
57	Each line contains at most one statement.	Guideline
58	The enclosed statements are indented one more level than the compound statement.	Standard
59	The opening brace is at the end of the compound statement on the same line.	Standard
60	The closing brace is on a line by itself and is indented to the same level as the compound statement.	Standard
61	Braces are used around all statements, even singletons, when they are part of a control structure, such as an 'if', 'if-else' or 'for' statement.	Standard
62	A 'return' statement with a value should not use parentheses unless they make the return value more obvious in some way.	Standard
63	Flow control blocks are enclosed within curly braces.	Standard
64	The opening brace of a flow control occurs at the end of the same line as the declaration. The closing brace starts a new line and is indented to match the beginning of the corresponding declaration.	Standard

#	Item/Description	Standard/Guideline?
65	The if-else class of statements has the following form: **if (condition) {** **statements;** **}** **if (condition) {** **statements;** **} else {** **statements;** **}** **if (condition) {** **statements;** **} else if (condition) {** **statements;** **} else {** **statements;** **}**	Standard
66	A 'for' statement has the following form: **for (initialization; condition; update) {** **statements;** **}**	Standard
67	An empty 'for' statement (one in which all the work is done in the initialization, condition, and update clauses) has the following form: **for (initialization; condition; update);**	Standard
68	Avoid the complexity of using more than three variables, when using the comma operator in the initialization or update clause of a 'for' statement.	Standard
69	A 'while' statement has the following form: **while (condition) {** **statements;** **}**	Standard
70	An empty 'while' statement has the following form: **while (condition);**	Standard
71	A 'do-while' statement has the following form: **do {** **statements;** **} while (condition);**	Standard

#	Item/Description	Standard/Guideline?
72	A 'switch' statement has the following form: **switch (condition) {** **case CGI:** **statements;** **/* falls through */** **case DEF:** **statements;** **break;** **case OPTUM:** **statements;** **break;** **default:** **statements;** **break;** **}**	Standard
73	There should be a comment where the break statement would normally be every time a case falls through.	Standard
74	Every switch statement should include a default case.	Standard
75	A 'try-catch' statement has the following form: **try {** **statements;** **} catch (ExceptionClass e) {** **statements;** **}** or desire a finally block: **try {** **statements;** **} catch (ExceptionClass e) {** **statements;** **} finally {** **statements;** **}**	Standard
	White Spaces	
76	Two blank lines are always used in the following circumstances: - Between sections of a source file. Sections include Copyright Header, Package Statement, group of import statements, and File Header - Between class and interface definitions	Guideline
77	One blank line are always used in the following circumstances: - Between methods - Between the local variables in a method and its first statement - Before a block comment or a single-line comment - Between logical sections inside a method to improve readability. - After the last instance variable	Guideline
78	Blank spaces are used in the following circumstances: - A keyword followed by a parenthesis should be separated by a space.	Standard

#	Item/Description	Standard/Guideline?
79	A blank space is not used between a method name and its opening parenthesis.	Standard
80	A blank space appears after commas in argument lists. - All binary operators except . should be separated from their operands by spaces. Blank spaces should never separate unary operators such as unary minus, increment ("++"), and decrement ("--") from their operands.	Standard
81	The expressions in a 'for' statement are separated by blank spaces. For example: **for (expr1; expr2; expr3)**	Standard
82	Casts are followed by a blank space. For example: **myMethod((byte) aNum, (Object) x);** **myMethod((int) (cp + 5), ((int) (i + 3)) + 1);**	Guideline
	Miscellaneous Practices	
83	Class names are used instead of using an object to access a class (static) variable or method.	Standard
84	Avoid assigning several variables to the same value in a single statement.	Standard
85	Embedded assignments are not used in an attempt to improve run-time performance.	Guideline
86	Parentheses are used liberally in expressions involving mixed operators to avoid operator precedence problems.	Standard
87	The use of static methods is avoided. All methods should be non-static unless there is a truly good reason to make them static.	Guideline
88	Since String objects are immutable, to save resources (memory) the StringBuffer class should be used when you have to make a lot of modifications to Strings.	Standard
89	Each web page must be developed to be ADA compliant	Standard

90	Organize the Code
	
	InCorrect:
	anObject.message1();
	anObject.message2();
	aCounter = 1;
	anObject.message3();
	Correct :
	anObject.message1();
	anObject.message2();
	anObject.message3();
	aCounter = 1;
		Standard

91	Destructors: Java does not have destructors, but instead will invoke the finalize() member function before an object is garbage collected. Implement the **finalize()** method to release any resources used by object for efficient memory management.	Standard
92	Never catch any Exceptions that are not Checked Exceptions. All Run Time Exceptions should be left to either application or web container for handling.	Standard
93	Logging should be implemented with appropriate level while handling with a catched exception. Do not use printStackTrace();	Standard
94	avoid using stored procedures	Guideline
95	Action classes should be light. All Business logic should be moved to business layer	Standard

#	Item/Description	Standard/Guideline?
96	Unused methods must be removed from the code	Standard
97	Redundant code e.g. Default constructor	Standard

APPENDIX B – QUALITY CODE EXAMPLES

Example #1 – Comments

There are no comments. Please refer to the next page for an example of proper comments for this module.

[redacted]

Example #1 – Comments - Preferred

The same module with proper comments.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

APPENDIX C – DETAILED CODE REVIEW RESULTS

Detailed code review results are documented in the attached spreadsheet.

VT_HIX_Code_Revie
w_Assessment_Score

OPTUM™

Vermont Health Connect HIX

Transaction Monitoring

8/18/2014

TABLE OF CONTENTS

1.0 .....EXECUTIVE SUMMARY **3**
2.0 .....BACKGROUND **5**
3.0 .....HIGH-LEVEL KEY TRANSACTION MAP (CONTEXT DIAGRAM) **8**
4.0 .....MAP ANALYSIS REPORT **9**
5.0 .....RECOMMENDATIONS **11**

1.0 EXECUTIVE SUMMARY

The purpose of Transaction Monitoring deliverable is to help provide an understanding of the system components used to support key transactions within the Vermont Health Connect (VHC) Health Insurance Exchange (HIX). The high-level key transaction map (context diagram) also indicates where problems were suspected and/or observed within each transaction.

Optum has concluded, based on review of the VHC's architecture and transaction monitoring documentation, and interviews with both SOV and contractor staff, that:

- [redacted]

The lack of communication between the SOV and CGI and transparency of documentation, impacts the partnership and synergy for resolving ongoing system issues; and the ability to move forward with future enhancements on the VHC system. However, through extensive interviews with both parties, there were clear areas of improvement identified.

As a result, VHC users continue to encounter problems within the following transactions:

- [redacted]

Key Findings

Optum's assessment is based on the following findings:

- Key transactions that were identified by the VHC include:
  - Default transactions (as determined from the Hawaii assessment)
    - Login & Registration
    - Application
    - Plan Selection
    - Enrollment
  - Vermont Specific Transactions
    - Payment/Financial (Benaissance)
    - Carrier Enrollment (820's and 834's)
    - Federal Hub
    - Medicaid / ACCESS
- Existing or potential issues with VHC business transactions include:
  - Data Integrity
    - [redacted]
  - [redacted]

        - [redacted]
    - Escalation path of key issues was ineffectiveApplication/Transaction Performance
        - SOV and CGI did not report chronic performance issues within VHC
        - Existing CGI performance reports, shared with SOV, show SLA violations
            - Daily Response Time Report shows transaction response time averages between 8 and 11 seconds
                - SLA states 5 seconds or below
        - Insufficient performance reporting
            - Only discovered one performance report produced by CGI (Weekly Basis)
            - No real-time or near real-time performance dashboard for application health
- [redacted]

CGI should perform performance testing in an environment more closely aligned to the Live environment.

Recommendations

Optum recommendations are summarized below. These recommendations are based on the findings described herein.

- Implement a comprehensive monitoring strategy, at both the infrastructure and application layers, that will include:
    - Availability monitoring
        - Ensuring the VHC is available for posted availability hours
        - Synthetic and external monitoring tools. (See section 5 for specific recommendations)
    - Performance monitoring
        - Ensuring that the VHC is performing within the agreed upon SLA
        - End-User Experience monitoring (See section 5 for specific recommendations)
    - [redacted]
    - Key Performance Indicators
        - Identifying key performance indicators will allow thresholds and dashboards to be configured to portrait current VHC system health
- Leverage existing monitoring tools and/or implement new monitoring tools to support the monitoring strategy
- Provide the SOV technology and management teams with a real-time dashboard representing the current performance health of the VHC

Introduction

The following sections of this deliverable describe Optum's approach and further describe Transaction Monitoring findings and recommendations:

- Section 2.0 - Background outlines the approach used for preparing this deliverable.
- Section 3.0 – High-level Key Transaction Map provides a graphic that summarizes findings from the review of VHC's targeted business transactions by specific architecture components.
- Section 4.0 – Map Analysis Report elaborates on the Map provided in Section 3.0.
- Section 5.0 – Recommendations provides more details on the recommendation summarized earlier, based on the documented findings.

2.0 BACKGROUND

The purpose of Transaction Monitoring is to assess the VHC key business transactions, specifically existing transactions that encounter issues, and to review existing monitoring activities. The objective of the assessment is to help identify infrastructure and application issues. The diagram, in Section 3, contains observations and reports of issues Vermonters currently experience when attempting to utilize the VHC. There is not a comprehensive monitoring toolset in place, limiting data driven observations and reports for these transactions. As a result, interviews and document analysis were the main source of input for this assessment.

An assumption was made that the State of Hawaii's Exeter LifeRay Portal implementation and CGI's Oracle Identity Management implementations were the same. However, through the investigation process, there were differences found in the robustness in the SOV infrastructure solutions. The SOV infrastructure has more high availability features and supporting load balancing designs. Thus, mitigating some of the HHC issues experienced with database connection pools.

The team met with the following SOV and vendor team members and attended Enterprise Architecture\Business Analyst\Vendor meetings:

- State of Vermont
  - Lindsey Tucker
  - Rick Ketcham
  - Tom Mulhall
  - Jenn Loughran
  - Elizabeth McMullen
  - Claus Lund
  - Jack Green
  - Mike Morey
  - Chad Loseby
  - Justin Tease
- Contractors
  - [redacted]
- CGI [redacted]
- Exeter
- Benaissance
- Archetype

The following project documents were reviewed:

Architecture Documents
• [redacted]
Business Analyst Support Documents
• [redacted]
Prior Assessments
• Vermont Health Services Enterprise Initial Implementation Review and Assessment ("Lessons Learned"); prepared by BerryDunn McNeil & Parker, LLC
Contract
• CGI Master Services Agreement, dated December 13, 2012

3.0 HIGH-LEVEL KEY TRANSACTION MAP (CONTEXT DIAGRAM)

The following matrix provides a high-level transaction map.

- The rows are based on the architecture components included in the scope of our assessment:
  - Exeter
    - Oracle Identity Management
    - HTTP/WebGate
    - Portal
    - Oracle Policy Automation (OPA)
    - Oracle SOA
    - Siebel
  - Third Parties
    - Benaissance
    - Federal Hub
    - Carrier Systems
  - SOV
    - ACCESS
- The columns are based on the key business transactions selected for monitoring:
  - [redacted]

The table below outlines the criteria used for our assessment:

Transaction Review Criteria	
Criteria	**Criteria Description**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Using these criteria, the following color coding was applied to the matrix:

Transaction Review Criteria	
Color Code	**Description**
Light Teal	[redacted]
Green	[redacted]
Yellow	[redacted]
Orange	[redacted]
Red	[redacted]
Thin/Diagonal Stripes	[redacted]

[redacted]

4.0 MAP ANALYSIS REPORT

The Map Analysis Report contains analysis and comments describing the criteria and color codes applied.

As mentioned in the Background (section 2), there was an assumption that the State of Hawaii's transaction mapping and assessment was going to be the same, or similar, as to the State of Vermont's VHC. However, through meetings and document review, this does not seem to be a safe assumption.

As outlined in the Key Transaction Map (shaded by diagonal lines), many of the transactions mapped use the same platform as Hawaii (also assessed by Optum). The color designation leverages the Hawaii findings. Similar to Vermont, the Hawaii assessment lacked tools to support detailed analysis, but each

of the transactions noted were reviewed with Exeter and assessed for performance tuning opportunities based on input from their developers.

The following table describes the basis for each cell in the transaction map:

VHC-specific Transactions Reviewed	
Findings	**Recommendations**
• [redacted]	[redacted]
• [redacted]	[redacted]
• [redacted]	[redacted]
• [redacted]	[redacted]

[redacted]	
• [redacted]	[redacted]

[redacted]

5.0 RECOMMENDATIONS

This section of the deliverable summarizes transaction monitoring opportunities.

The VHC transaction map (above) has been derived by interviewing SOV staff, vendors, CGI, and review of existing documentation. It is imperative that a data driven review be completed using monitoring tools that analyze all aspects of the VHC system [redacted] Optum was not granted access to any existing monitoring tools controlled by CGI.

[redacted]

Optum recommends a three step approach to achieve this:

1) Create a comprehensive monitoring strategy that will support an end-to-end monitoring solution. That strategy should address:
    - Availability monitoring
    - Performance monitoring
    - Fault Domain Isolation
    - Key Performance Indicators
2) Deploy monitoring tools in production and pre-production environments
    - Leveraging the monitoring tool data during load tests is key
3) Instrument VHC system health dashboard, displaying:
    - Current system events – availability and performance
    - End-user experience (page response time averages)
    - System tier health (Website/database/application/adapters)

<u>Existing tools in use for VHC</u>

- [redacted]

- [redacted]

Recommended tools to supplement and/or replace existing tools for VHC

- [redacted]

Deployment of these tools, in all environments, will support the monitoring strategy of a comprehensive end-to-end solution. Further gap analysis of existing toolsets will be needed to determine the need of the proposed recommended toolsets.