Introduction
This document serves to address questions and provide more clarity about the HSEP Operational Framework in the following areas:

- What is Maintenance & Operations (M&O)?
- HSEP Change Control Process
- Service / Cloud Provider Onboarding

What is Maintenance & Operations (M&O)?
The M&O function is delivered by a Service Provider on behalf of SOV Agency or department. The Function supports the day-to-day care and feeding of the technology infrastructure and applications that are required to meet the Service Level Agreement and fulfill contractual obligations. The M&O team utilizes the OF processes defined this section to perform their tasks in a consistent manner.

In context of the VHC, CGI as the cloud Service Provider provides the M&O function. Activities include, but are not limited to:

- Software delivery and defect/bug tracking
- Release (inclusive of SDLC activities) and Change management
- Response to SOV inquiries and requests
- Incident and Problem resolution
- Monitoring
- Knowledge Management that includes training, standard operating procedures, work instructions, process development
- Maintenance of Service Levels and Service reporting

HSEP Change Control Process

Introduction
Figure 1 represents the high level Change Control process that exists today on HSEP with VHC as the only client. The State’s expectation is that future vendors will follow this process as other clients are brought on board. As this occurs, other business units (MMIS, PBM, IE) and other vendors representing them will participate in these teams as needed.

Scope
The process in Figure 1 highlights the process for functional changes initiated by the business. Technical changes initiated by the Service Provider (e.g. application patch, hardware changes) bypass the Pre-Change Control Board (CCB) and the CCB and go directly through the Operational Change Review Board (OCRB).
For the swim lanes above the following HSEP teams and groups are involved:

**Business**

Represents any business unit represented on HSEP. The business will often initiate the change

**Pre-Change Control Board (CCB)**

A regularly scheduled meeting with both State & Vendor representatives, this team is represented by State and vendor leads that include both business and IT. This group reviews all Change Requests submitted by business units. Their goal is to assess each RFC for validity, completeness and impact prior to requesting a rough estimate from vendor and forwards to the Change Control Board.

**Change Control Board (CCB)**

This team oversees, approves and tracks proposed changes. Its members include key members from State and vendor project, operations and IT teams. Reviews impact with appropriate resources (i.e. Business, Legal, Technical, and Security). Approves and/or rejects Change Requests, prioritizes, formally requests level of effort and cost from vendor.

**Operational Change Review Board (OCRB)**

Works with vendor to develop and adhere to deployment and release plan. This is the final State review before the change is deployed into the production environment. This step ensures the State is satisfied with test results, technical Impact and communicating end user impact & training needed.
Enterprise and Federated Approval for Changes

Certain Changes can impact multiple services, agencies, clients & vendors due to technology dependencies. For instance, an upgrade to a database that provides eligibility information to multiple applications/services can have adverse effect across the HSEP environment. In this scenario, it is expected that all designated SoV business unit “Change Managers” represent their Service and participate in the “Enterprise” Operations Change Review Board (OCRB).

In certain cases where a Change only affects one service and does not have cross-service impact, approval for changes can be federated to the individual business unit Change Manager.
Service / Cloud Provider Framework

SoV understands that each service provider will utilize their own unique methodology consisting of organizations/skills, processes, procedures, standards and tools. Additionally, each SoV department and agency that interfaces with the provider may also bring their own service framework. This introduces a gap that presents risk in the delivery of services and managing the day-to-day operations including customer support. The OF is defined to bridge this gap by using the processes, organization and automation to more quickly indoctrinate new providers into the HSEP service.

Operational Framework for SoV

The SoV Operational Framework is based on industry good practices (e.g. the IT Infrastructure Library – ITIL) and provides a model for how SoV governs, manages, delivers and supports services to its internal and external customers. The concept allows for consistent delivery of service management processes and practices regardless of whether a Private, Public or hybrid cloud strategy is adopted. Figure 5 shows the framework strategy.

The framework is presented here in Figure 2 for aligning SoV’s strategy with the Service Provider’s. The Service Onboarding (documented further below) methodology is a repeatable set of activities that are required to align the Service Provider and the Business’s people, processes and technology.
The Service Onboarding methodology is a repeatable set of activities that are required to align the Service Provider and the Business’s people, processes and technology. For processes where the business actively participates day-to-day with vendor (e.g. Incident, Problem, Change, Request, Knowledge), the following macro steps must be followed:

a) Evaluate and assess the business process with the business units

EAs meet with business to determine existing operational processes, tools, Responsibility/Accountability/Consulted/Informed (RACI) matrixes, Governance and detailed information relevant to the Operational Framework (OF).

b) Evaluate Service Provider processes and tools
Enterprise Architects and the business meet with Service Providers to determine Provider’s operational processes, tools, Responsibility/Accountability/Consulted/Informed (RACI) matrixes, Governance and detailed information relevant to the Operational Framework processes.

c) Identify gaps discovered in steps a) and b) (e.g. Incident, Change, Problem)
d) Harmonize process, people and tools into common OF framework. The harmonization step provides:
   - Training on the existing OF and gaps identified
   - Workshops to plug the gaps between the OF, Service Provider and the Business
   - Develop RACIs, standard operating procedures (SOPs) and
   - Structured walk-through of processes prior to go-live

For those processes that the business is not active in day-to-day, SoV validates that the Service Provider’ processes are in place and being executed. These processes include, but are not limited to: Availability, Capacity, Security, Continuity, Release and Event Management.

**Figure 3: Service Onboarding activities for each OF process area**

**Legend:**

- **Future:** Automating Configuration Management is a more mature process and therefore compliance is expected to be a longer-term roadmap item

- **Verification:** Indicates that SoV’s role within this process is to validate that documentation exists and the process is being followed
HSEP Operational Framework Clarity Statement

Service Support

Service Support focuses on the delivery of agreed services to the business consumers (i.e. customers and end-users) by the Service Provider. This includes managing the underlying technology, people, processes and partners that contribute to the delivery of business services. Doing so helps achieve service excellence while improving efficiencies which lead to cost reduction.

Service Support functions and processes are governed and managed by the Service Provider with input from the business.

Event Management

The goal of event management is to manage recurring events and prevent them from causing larger issues. An event is a detectable occurrence that has significance within an applicable environment (Production, Staging, etc.). These events may be detected through monitoring of infrastructure or changes to configuration items. The purpose of event management is to detect events and determine the appropriate action to take if any. Items which are considered events may include sustained spikes in system utilization or consecutive unsuccessful logins to a host.

Within the context of the HSE and SoV’s cloud strategy, external vendors will be managing and supporting the event management initiative.

Business Involvement and Current State

HSEP business units do not need to be concerned with Event Management and how this is achieved by the Service Provider. It is imperative however that the EA team understand what the vendor is monitoring, the thresholds configured within their tools and the processes by which the Incident Management process is engaged.

Currently the Service Provider has instrumented monitoring tools and logging for both infrastructure components and applications. The informal and undocumented process includes the following steps:

- Monitoring tools trigger alerts based upon preset thresholds
- Administrators review and validate these alerts
- Subject Matter Experts are notified based upon severity to investigate for false positives
- If the event is determined to affect the Services or any of its dependencies then an Incident is opened

It is imperative that all Service Providers have a documented Event Management strategy that includes integration with Incident and Problem Management processes.

This process is reusable for other Services beyond the VHC, but the detailed monitoring tools and process for validating, verification and correlating events will be left up to each individual Service Provider.

Incident Management

An incident is an unplanned interruption to a service. The goal of Incident Management is to restore normal services as quickly as possible to minimize an incident’s impact on the business. Escalation procedures should be in place if incidents cannot be resolved quickly. The purpose of incident management is to ensure that incidents are tracked, reported and processes are continuously improved to enhance customer satisfaction and business effectiveness.
The Incident Management process may also be executed to pre-empt a possible interruption. For instance, if a queue is beginning to fill up that may possibly lead to an interruption, the Incident Manager may wish to execute the Incident Management process.

**Business Involvement and Current State**

Anyone can uncover and log an Incident through the pre-determined process and this includes end-users, business users and technical admins. If the Service Provider uncovers an Incident, Business Units must be notified that an incident has occurred based upon the Priority (Impact + Urgency) of the Incident and within time constraints dictated by Service Level Agreements within the contract.

For the VHC, a process exists inclusive of notification, logging, escalating and closing Incidents and service levels associated.

For HSEP, Incidents are used to log technical issues and not functional issues. The VHC uses Service Requests within the Case Management system for logging non-technical interactions with various business groups. Business units have also been using Service Requests to log technical “Incidents” with the Business Application Support Unit (BASU). “Service Requests” should not be confused with Incident Tickets or Change Requests (see below). They are different and follow a separate process.

This Incident Management process has been established for long-term repeatability by multiple Services and Providers.

**Problem Management**

The goal of Problem Management is to minimize the adverse effect of incidents and problems caused by errors and to proactively prevent future occurrences. The purpose of Problem Management is to discover the root-cause of a problem and prevent its re-occurrence (or minimizing their impact). Also documenting and recording workarounds within a known error database requires tight integration with other processes like Change, Incident and Configuration management.

**Business Involvement and Current State**

The business must collaborate with the Service provider to ensure that Problems are managed through closure and risks are properly assessed.

The Problem Management process is currently being established and documented. The informal process being followed includes:

- Reviewing Priority 1 and some Priority 2 Incidents for candidates for Problem Management and root cause analysis
- A Problem ticket is opened and defects are managed
- If a permanent fix is determined the Change Management/Release Management processes are followed (see below)
- Once the fix is implemented, the Problem is closed

This process is being established and improved upon for long-term repeatability by multiple Services and Providers. The details for Root Cause Analysis and tools used will vary from provider to provider.

**Service Transition**

Service Transition Management manages the change, release, and deployment of HSE services into production successfully. This section covers the following Service Transition processes and activities.
HSEP Operational Framework Clarity Statement

Change Requests

This process is tied closely with Change Management. Change Requests trigger the request fulfillment process that handles inquiries and requests for existing and/or new services such as new functionality or products. For instance, the business may request that a new user be provisioned (or removed), user privileges be enhanced or that a text field within a web page be modified.

Change Requests may require approval by SoV or the provider prior to fulfillment of the request -- for instance prior to elevating a user’s privilege or before application modifications can be made. Some Change Requests (e.g. Changes to application functionality) may go through the Change and Release Management process.

SOV Case Management system defines its tickets or cases as “Service Request”. The term “Change Request” is used to differentiate.

Business Involvement and Current State

Requests that are not the “Inquiry” type follow the existing documented process which includes:

- SoV business units and agencies submit Change Requests, typically through the business lead within their organization
- The Request is submitted to a committee, the Pre- Change Control Board (Pre-CCB) to review the Change Request for validity, completeness and risk
- After validation the request is submitted to the formal Change Control Board (CCB) for approval
- Once approved, the Change and Release Management process is engaged

This process has been established for long-term repeatability by multiple Services and Providers. See Figure 1 for the repeatable process in place today.

Change and Release Management

The objective of Change and Release Management is to allow beneficial change to an HSE service while minimizing disruption to those services. The goals for change management include:

- Protecting HSE services while reducing risk associated with changes to environments (e.g. Production, Staging, Disaster Recovery)
- Ensuring standardized methods are used for the efficient and prompt handling of all changes
- Ensuring changes impacting users are recorded

The purpose of release management is to build, test, and deliver services specified by the functional and non-functional requirements within service design. This provides the means to deliver services while meeting the overall objectives of the business and the end-user.

Business Involvement and Current State

The OCRB assesses the overall risk to the pending release prior to implementation. The OCRB is built to include all current and future Services (as required), regardless of the department, agency or Service Provider. The OCRB is made up of:

- The Cloud / Service Provider
- Business representation
- EA representation
- Any additional Subject Matter expert required to assess the release from a preparedness and risk perspective (e.g. application/infrastructure expert, test engineer, release lead)
The OCRB assesses the following (not an exhaustive list):

- Changes approved by the CCB
- Infrastructure Changes proposed by the Service Provider that do not go through the Change Request process
- Tests performed and resulting validation (including UAT)
- Environments tested for the release
- Complexity of the change
- Back Out plans
- Conflicts with other pending releases and critical operating windows
- Time required to implement the release and validate against agreed maintenance windows
- Other technical dependencies and impacts
- Skills and personnel implementing the change
- Post implementation reviews
- Process improvements

Once approved, the Service Provider implements that change within the determined window.

This process has been established for long-term repeatability by multiple Services and Providers. See Figure 1 for the repeatable process in place today.

Knowledge Management

The purpose of Knowledge Management is to ensure that the right information is delivered to the right person, at the right time, enabling informed decision making. Knowledge can be anything from the sharing of perspectives and ideas to detailed Standard Operating Procedures to contracts. The goals include:

- Relevant information is always available to the right users
- Reducing the need to rediscover knowledge
- Efficient services with improved quality
- Clear and common understanding of the value of the service

Part of SoV’s Knowledge Management is a system called Service Knowledge Management System (SKMS). SKMS is a unified portal that presents meaningful information about Services. This meaningful information comes from raw data collected by mature IT organizations that concerns infrastructure, applications, the Service Desk, and monitoring systems. The SKMS enables SoV to mine data from Service Providers both internally and externally and should be considered as a way to better manage the business of IT. The SKMS is unrelated to Case Management as Case Management’s goal is not to manage the business of Information Technology.

To achieve the above, the organization must also have the institutional wisdom to be able to operationalize the transformation of raw data (from any source) into something that benefits the business. Negotiating with external Service Providers to open relevant data marts for extraction is another consideration for success.

Business Involvement and Current State

An Enterprise Knowledge Management system does not exist within the SoV. Each Service Provider and SoV business unit currently has their own mechanism for storing knowledge.
HSEP Operational Framework Clarity Statement

For the VHC, there are two repositories that are being proposed for use and a process for ensuring that Knowledge is reviewed, approved and retired appropriately and that access controls are effectively set as required.

Service Asset and Configuration Management

Service Asset and Configuration Management (SACM) provides a logical model that manages and tracks service assets and components within a Configuration Management System (CMS). The CMS is a set of tools and databases used to capture and store a provider’s configuration data. There are two aspects:

- **Asset Management**: Is responsible for tracking and reporting on the value and ownership of financial assets throughout their lifecycle.

- **Configuration Management**: Configuration Management is responsible for recording and maintaining information about Configuration Items (CIs) and their state, and the relationships between all components (virtual or otherwise). A CI is any component that needs to be managed in order to deliver an IT service. The Configuration Management Database (CMDB), which is part of the CMS, is a centralized repository in which this information is managed. It is composed of CIs such as Virtualization Services, contracts, hardware, or software elements and is intended to be the single source of truth for the State’s configuration data.

Configuration Management delivers a model for HSE services and the infrastructure that supports it by recording the relationships between CIs.

Asset Management is critical to SoV’s strategy because it helps in the following areas:

- Track software licenses purchased as part of the supported Service (e.g. Oracle licenses used with the VHC)
- Tracks hardware assets, OS and VM licenses purchases as part of the SoV private cloud (VCOE) service
- Track assets to Services to help calculate the total cost for providing the ongoing service to the department or agency

**Business Involvement and Current State**

A SoV Enterprise-wide Configuration Management process does not exist as it relates to HSEP. Each individual agency and department may have internal strategies, including manual tracking of Assets.

Currently the Configuration Management processes are immature and siloed for the VHC Service Provider.

A formal process is being developed for the VHC, but each provider will have their own tools and mechanisms for SACM. Industry good practices and non-functional requirements will be used to evaluate the Service Provider’s adherence to this process.

More mature execution includes the deployment of discovery tools that exist today on the market for capturing system configurations and configuration item dependency maps that help with impact analysis during Incident and Change Management.
HSEP Operational Framework Clarity Statement

Service Level Management

Service Level Management negotiates and manages Service Level Agreements with the provider and helps to continuously improve processes and the design of services in accordance with the agreed service level targets. Service Level Management is also responsible for ensuring that all Operational Level Agreements and Underpinning Contracts are appropriate, and to monitor and report on service levels.

The scope for Service Level Management within the HSE consists of the following processes:

Availability

The goal of availability management is to ensure the availability of HSE services to both internal and external users. The availability targets are based upon the Service Level agreements within internal and external vendor contracts. Management and oversight of availability service levels help EA and SoV in general work with providers to improve the underlying architecture and technology used to enable the HSE services.

Capacity

Capacity Management is a process that extends across the Operational Framework. A key success factor in managing capacity is ensuring it is considered during the design stage. Capacity Management is supported initially in Service Strategy where the decisions and analysis of business requirements and customer outcomes influence the development of patterns of business activity, levels of service and service level packages. This provides the predictive and ongoing capacity indicators needed to align capacity to demand.

The goal of capacity planning is to ensure that sufficient capacity exists within the Service Provider environment and that they align and meet the contractual service levels and those agreed to by the agency and department services they support.

Capacity Management also provides a point of focus and management for all capacity and performance-related issues that may occur.

Information Security

The goal of the Information Security process is to align IT and business security ensuring that information security is effectively managed in all service and Service Management activities.

Information Security needs to be considered within the overall HSE governance framework and meet compliance and regulatory requirements.

IT Service Continuity

The goal of IT Service Continuity Management (ITSCM) is to support the overall Business Continuity Management process by ensuring that in the event of a disruptive event, the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales.

As technology is a core component of most business processes, continued or high availability of IT is critical to the survival of the business as a whole. This is achieved by introducing risk reduction measures and recovery options. Like all elements of ITSM, successful implementation of ITSCM can only be
achieved with senior management commitment and the support of all members of the organization. Ongoing maintenance of the recovery capability is essential if it is to remain effective. The purpose of ITSCM is to maintain the necessary ongoing recovery capability within the IT services and their supporting components.

**Business Involvement and Current State**

The business participates in the review of Service Level reports and improvement meetings with each vendor. These meetings should be scheduled periodically with the Service Provider to review these reports against the contractual Service Level Agreements. A governance structure and process should exist for holding each Service Provider accountable and a mechanism for escalating non-compliance.

A non-documented, informal process is followed today for the VHC and reports do exist that are developed by the Service Provider.

**Continuous Service Improvement**

Continuous Service Improvement (CSI) is an essential concept within the Operational Framework. CSI must be consistently applied in order to progress each phase and process area within the Framework to achieve increased efficiencies. In addition, integration between the processes, people and technology used to enable the Framework and adhere to good practices is mandatory.