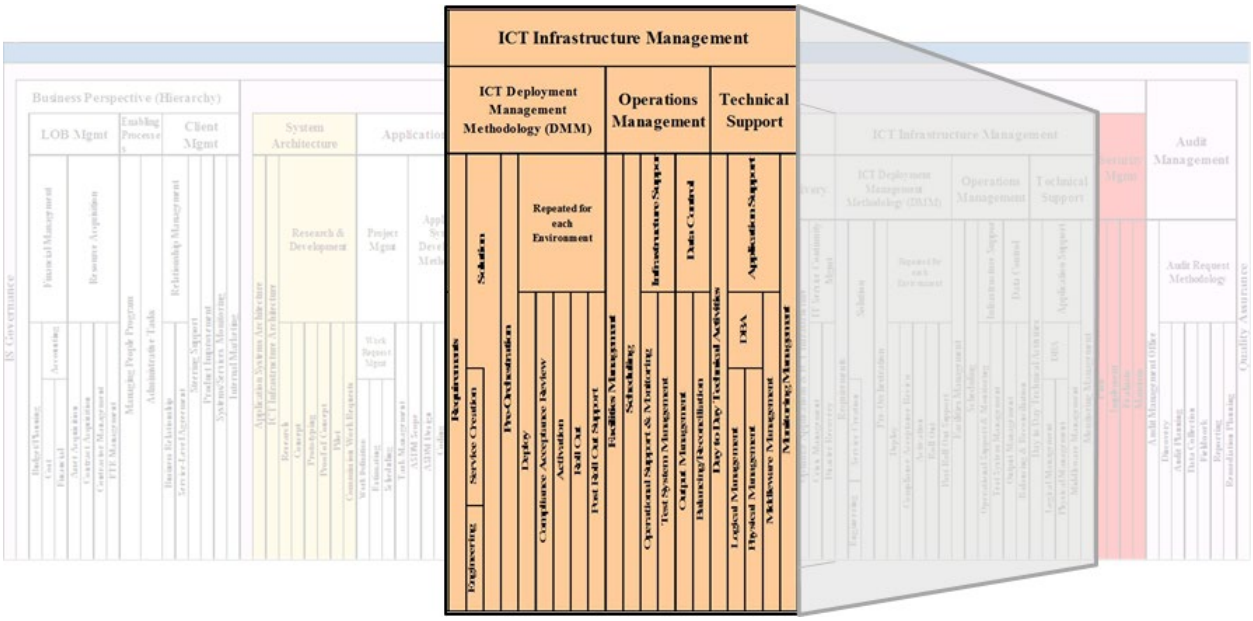
South Carolina

BlueCross BlueShield of South Carolina
is an independent licensee of the
Blue Cross and Blue Shield Association

imagination to Implementation

INFORMATION TECHNOLOGY

# ICT Infrastructure Management




# Information Systems Standards Manual

# Table of Contents

# Table of Figures

# List of Tables

There are currently no tables in this volume.

# Chapter 1 Deployment Management Methodology

The Deployment Management Methodology (DMM) process (Figure 1-1) supports a structured development methodology (life cycle) to administer all aspects of infrastructure requirements definition, design, building, testing, and implementation turnover for Information Communication Technology (ICT) Infrastructure platforms. It is integrated with the Application Delivery Methodology.

The Deployment Management Methodology consists of Solution Deployment and Service Creation, sometimes referred to as "Green Book" and "Blue Book" respectively. Solution Deployment consists of the execution of the sequential phases of Requirements and Solution and the grouping of Deploy, Compliance Acceptance Review, and Activation (the Conveyor Belt). After all the infrastructure has been activated, the Roll Out Phase begins and is followed by the Post Roll Out Support Phase, which continues until Work Request closure. Service Creation defines Infrastructure Service Offerings and consists of the execution of the Engineering Phase.

The ***Integrated Cloud Orchestration System*** is used to design, govern, deploy and track the Infrastructure elements and manage any type of infrastructure, which includes hardware and the software technologies required to use the hardware and run the business application system.

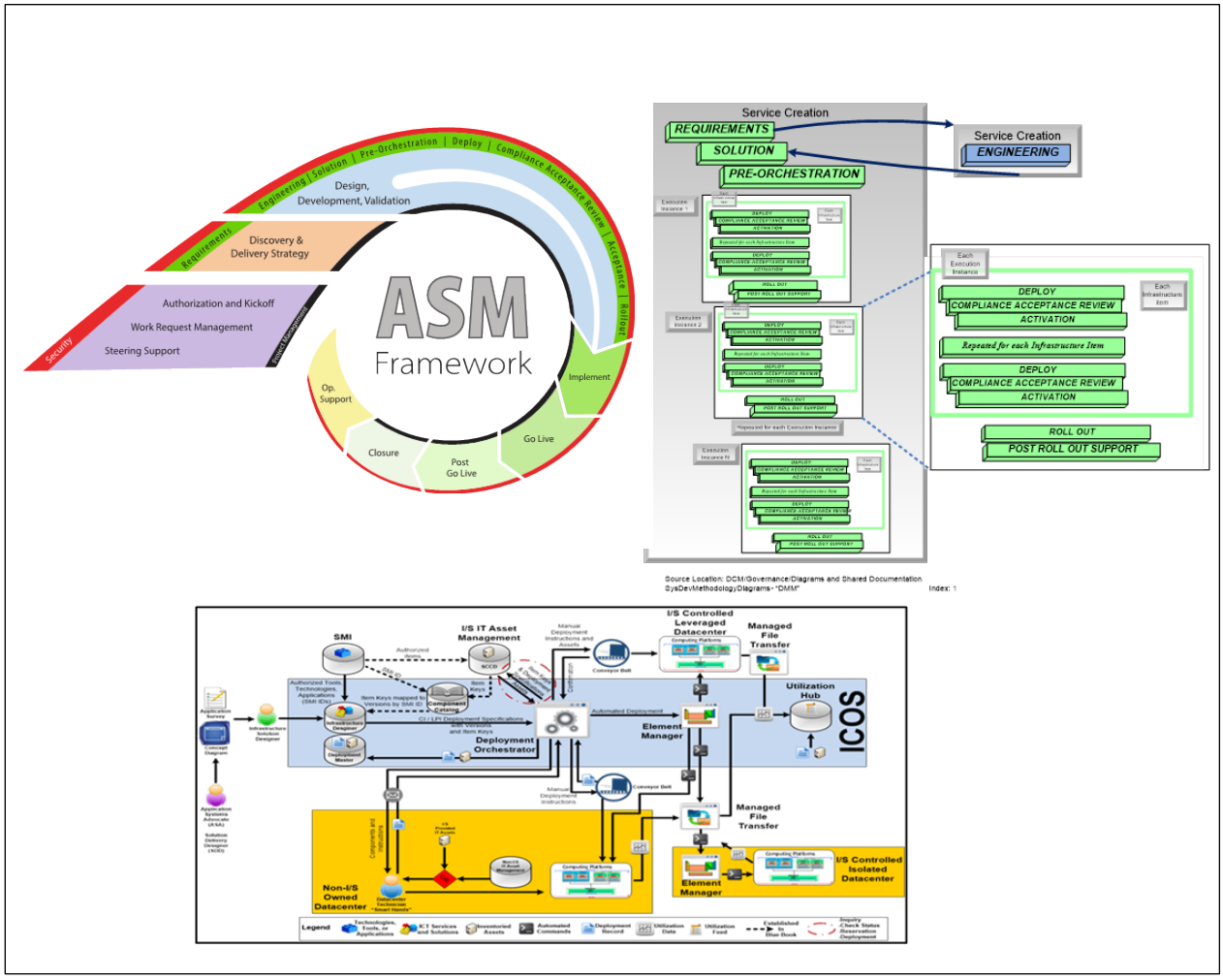



**Figure 1-1** Deployment Management Methodology

# 1.1 Deployment Management Methodology Roles

Infrastructure Solution Designer — The Infrastructure Solution Designer is responsible for the development and implementation of the end-to-end Infrastructure Solution and for ensuring the Infrastructure Solution satisfies the application systems' business and infrastructure needs. The Infrastructure Solution Designer designs the Infrastructure Solution after analyzing the technical requirements for the application system. The Infrastructure Solution Designer remains engaged until the Work Request reaches closure, thereby ensuring that the technical Infrastructure Solution delivered at the end matches the requirements established during the Requirements Phase. The Infrastructure Solution Designer will provide consultation, if needed, to the Work Request Team.

Though there is usually only one Infrastructure Solution Designer for each Work Request, there may be more than one depending on the complexity of the Work Request. In any case, the Infrastructure Solution Designer remains engaged in the Work Request until closure.

Deployment Specialist — The Deployment Specialist converts the Infrastructure Solution design into actual infrastructure consisting of hardware, infrastructure software, servers, networks, and telecommunications infrastructure that are compliant with any security requirements.

Integration Engineer — The Integration Engineer applies infrastructure engineering standards to integrate a final Infrastructure Solution into the current network architecture.

Service Creation Engineer — The Service Creation Engineer leads the engineering activities necessary to define a new Infrastructure Service by translating the Service Creation Request Document into technical engineering diagrams and descriptions.

Security Compliance Specialist — The Security Compliance Specialist discovers any security vulnerabilities.

## 1.1.1 DMM Roles Interaction

While the entire team works closely together, it is important to note how the DMM Roles interact. Figure 1-2 illustrates this interaction.

1. Besides providing technical leadership for the end-to-end Infrastructure Solution, the Infrastructure Solution Designer uses the application infrastructure requirements to design the Solution.
2. The Deployment Specialist converts the Solution design into functioning infrastructure.
3. The Security Compliance Specialist ensures the infrastructure is compliant with security safeguards.

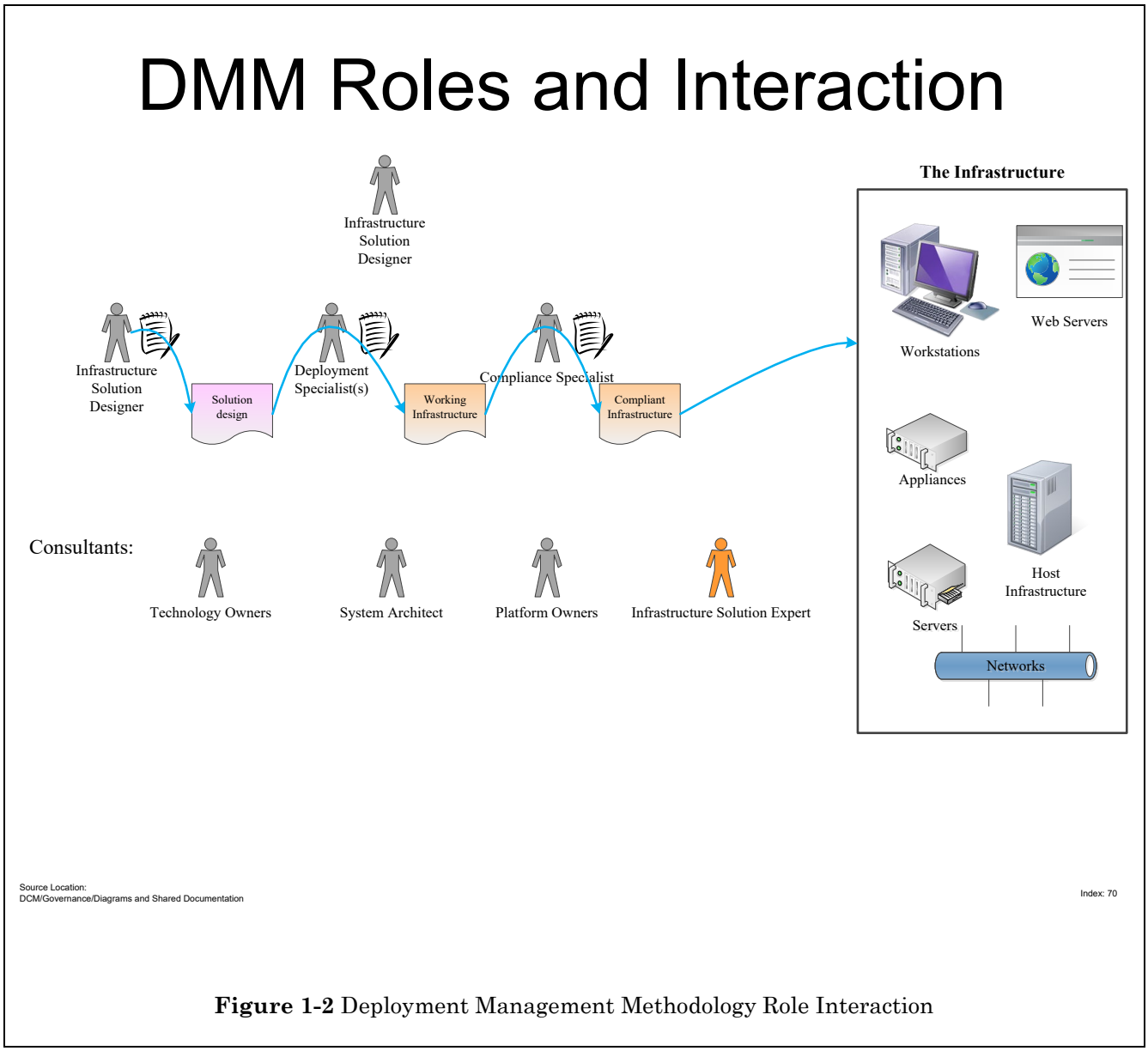



**Figure 1-2** Deployment Management Methodology Role Interaction

## 1.1.2 Testing Roles

Test Designer — The Test Designer is responsible for the development and management of the Test Plan.

Tester — The Tester is responsible for the execution of test plans associated with Work Requests.

# 1.2 DMM Accountability Matrix

Figure 1-3 below shows how the different Roles participate in the various phases of the methodology. This participation is defined with regard to the artifacts, like the Solution Deployment Report, that are produced at different phases and communicate the status and design of the solution at specific points in development.

The Deployment Management Methodology phases are listed along the top. Underneath the phases are the artifacts for those phases, labeled as Artifacts or Deliverables. The Roles are listed down the left side.

Roles assume one of five designations for each artifact.

- A = Accountable for Content — Responsible for the accuracy of the information contained in an artifact.
- D = Delivery of Artifact — Writes, assembles and/or produces an artifact.
- R = Responsible — Managerial or general oversight.
- C = Expected or Frequent Contributor — Provides information and/or a portion of an artifact.
- S = Sign-off — Required to sign off on specific artifacts.

The Project Manager and Infrastructure Solution Designer are listed first, because they have the primary DMM life cycle leadership Roles. The Project Manager has oversight responsibility almost all the way across (R), with some artifact (D) and content (A) responsibility. The Infrastructure Solution Designer is responsible for content (D) for the Requirements and Solution phases and is also accountable (A) for the end-to-end accuracy of the Infrastructure Solution and its deployment.

The Enterprise Architects and the Architect are important contributors during the Requirements, Solution and Engineering phases.

---

**NOTE** This chart is an "ideal" representation of the artifacts and Roles involved in this methodology. The chart is applied as necessary for the Work Request.

---

For more legible or printable copies, see the I/S Lighthouse.

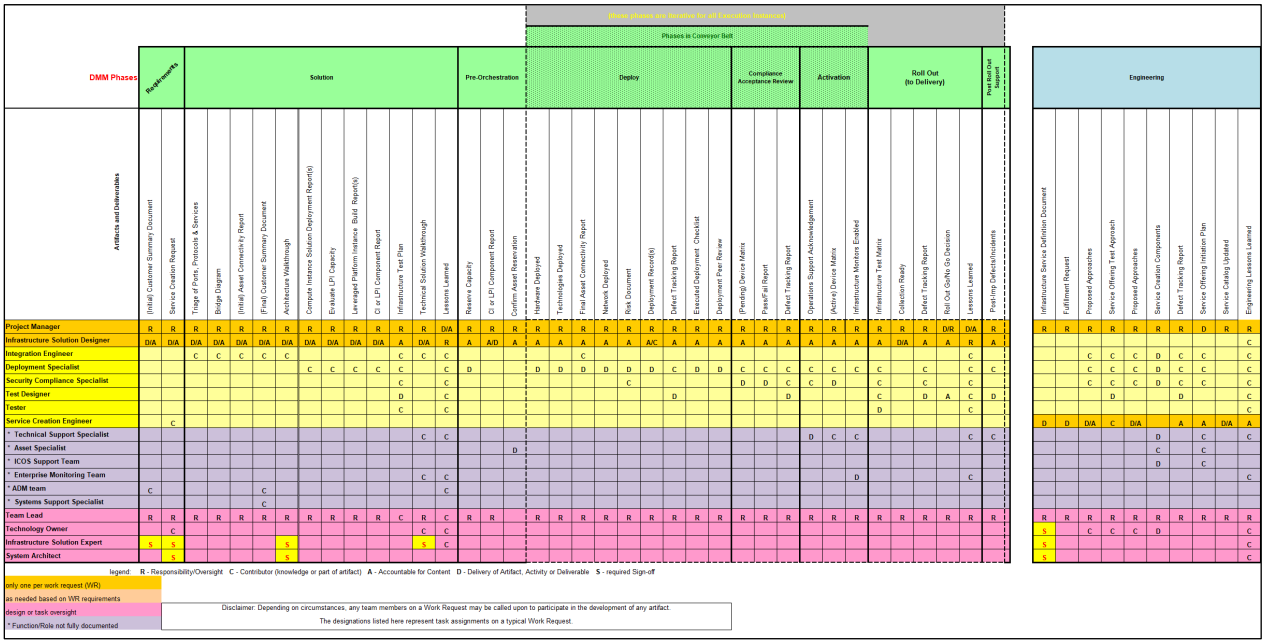



**Figure 1-3** DMM Roles and Deliverables Accountability Matrix

# 1.3 Requirements Phase

The Requirements Phase is the first phase in the ICT DMM. This phase encompasses the processes related to the discovery and high-level documentation and provides estimated infrastructure to meet the business application's requirements, along with the infrastructure requirements for supporting the development of the involved application software.

The aim of this phase is to reach an agreement with the application maintainers on what their specific infrastructure requirements are. The following artifacts are necessary for the Infrastructure Solution Designer to complete the (Initial) Customer Summary Document.

- Approved (Initial) Concept Diagram or ADM Diagram
- The Application Survey(s)
- The Technology Survey(s)
- Execution Instance Diagrams

The Requirements Phase (Figure 1-4) contributes to the Application Systems Management (ASM) Framework Discovery and Delivery Strategy.

---

**NOTE** Use the following list as a guide when viewing this methodology phase diagrams.

- Rectangle icon — an activity
- Output icon — an artifact
- Oval — an input or an output depicting the integration with Application Delivery Methodology
- Dashed Outline — Deliverables that are optional based on particular needs of the Work Request
- Dashed Purple Arrow — Dependency between deliverables
- Pedestrian Crossing symbol — Review required
- Red Star — Key Acknowledgement of Acceptance

---

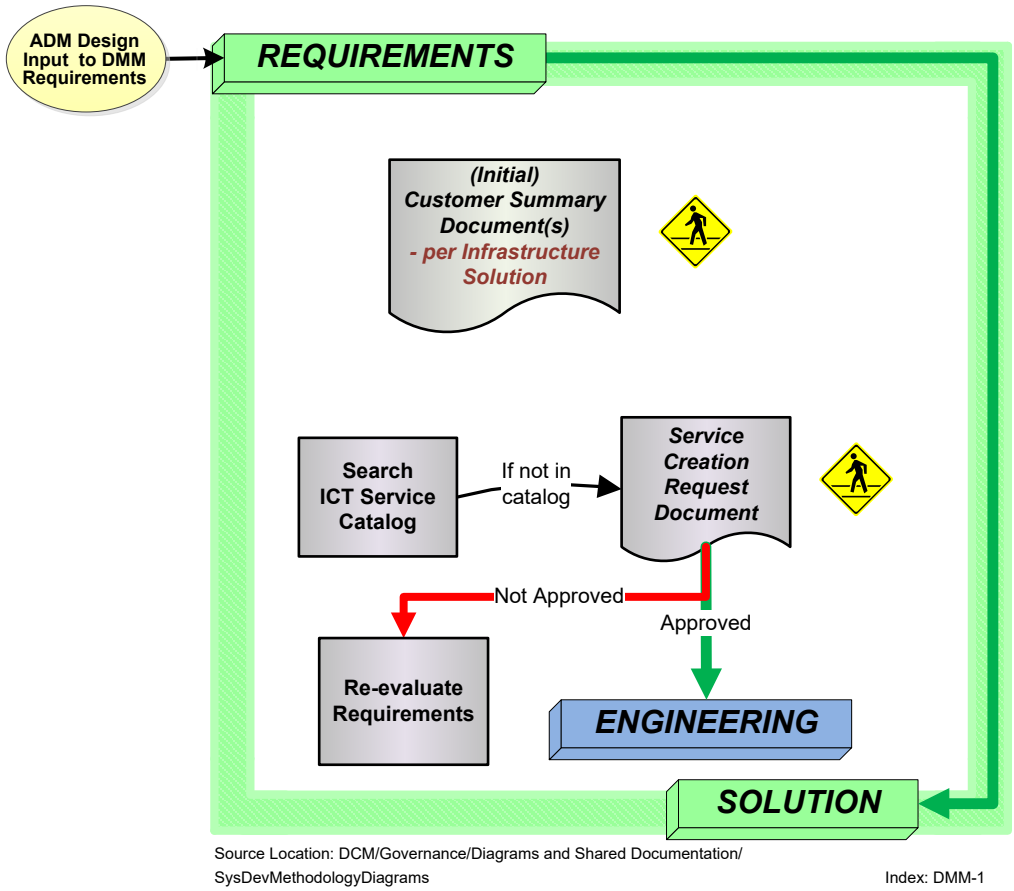



**Figure 1-4** Requirements Phase

**NOTE** If the infrastructure systems affected by the Work Request impact Credit Card Account Information (CCAI), a member from Security, Risk and Compliance Assurance (SRCA) should participate in the Requirements Phase work sessions.

These are the deliverables related to the Requirements Phase.

- (Initial) Customer Summary Document
- Service Creation Request Document

## 1.3.1 (Initial) Customer Summary Document Content

The Infrastructure Solution Designer develops the (Initial) Customer Summary Document using the most current version of the following items:

- Concept Diagram and its Technical Architecture Document, if available
- Application Survey(s)
- Technology Survey(s)
- Execution Instance(s)

Using the ICT Service Catalog, the Infrastructure Solution Designer determines which Infrastructure Service Offerings will be used to develop the Infrastructure Solution. If an appropriate Infrastructure Service Offering is not available in the ICT Service Catalog, the Infrastructure Solution Designer will document the requirements for the Infrastructure Service Offering in the Service Creation Request Document. The Infrastructure Solution Designer will report this information to the Project Manager. The Solution Phase will continue with the available Infrastructure Service Offerings in the ICT Service Catalog but cannot be completed until the requested new or updated Service Offering is available in the ICT Service Catalog.

The (Initial) Customer Summary Document from the Requirements Phase captures the infrastructure requirements in a non-graphical format to support the Work Request. Information that is typically found in the (Initial) Customer Summary Document includes such things as these items:

- General information about the Work Request, including risks and assumptions
- Identification of the application(s) and execution instance(s) impacted
- Solutions impacted by this Work Request
- Information on end-users, such as number and location
- System Availability requirements
- System Recovery requirements
- Scalability requirements
- Data transfer requirements

The Infrastructure Solution Designer reviews the (Initial) Customer Summary Document with the Architect and the Solution System Designer for completeness.

## 1.3.2 Service Creation Request Document

The Service Creation Request Document includes information about a requirement relating to Infrastructure Service Offerings that outlines the required addition or modification of an Infrastructure Service Offering. This document is the means by which to request approval from the Enterprise Architect(s).

The Infrastructure Solution Designer creates the Service Creation Request Document when there is a need for a new Service Offering or a modification to an existing Service Offering.

### 1.3.2.1 Service Creation Request Document Content

The Service Creation Request Document contains:

- The Work Request number and description.
- The Project Manager's name.
- The Infrastructure Solution Designer's name.
- The Infrastructure Service Offering(s) that requires modification (if applicable).
- A list of system requirements that cannot be met by an existing Infrastructure Service Offering.
- The Decision Matrix impact.

## 1.3.2.2 Service Creation Request Document Review

The documentation required for review at the Service Creation Request Document Review is the ICT Service Creation Request Document.

The following is a list of required participants for the Service Creation Request Document Review.

- Infrastructure Solution Designer
- Service Creation Engineer
- Technology Owner(s)
- Platform Owners(s)
- Architect
- Enterprise Architect

After approval from the Architect and the Service Creation Engineer, the Architectural Review process is followed. The Architectural Review process is described in *Adaptive Change* > *Global Standards* > *Reviews* > *Architectural Reviews.*

**NOTE** For BlueCross developed and maintained business application systems, these execution instances typically consist of a Unit, System, and Qual Test environment (execution instance), and the Production execution instance. Having all of these execution instances is typical; based upon certain characteristics of an application system, some test execution instances may not be required.

Deployment of multiple execution instances simultaneously or with some level of overlap is a planning and resource decision that is made by the Work Request Team during the ASM Design, Development and Validation and the DMM Solution phases. It is vital that all Conveyor Belt deliverables and reviews of the ICT Deployment Management Methodology are specifically addressed for each execution instance to be deployed, regardless of whether or not the specific activities overlap.

# 1.4 Solution Phase

The essence of this phase (Figure 1-5) is to define and refine what the infrastructure needs are by focusing on the communication and interactions of the application systems. This will help identify necessary changes to the infrastructure, or whether new infrastructure is required, and to provide detailed infrastructure specifications in the form of actionable items for the Deployment Specialists to make the needed infrastructure changes.

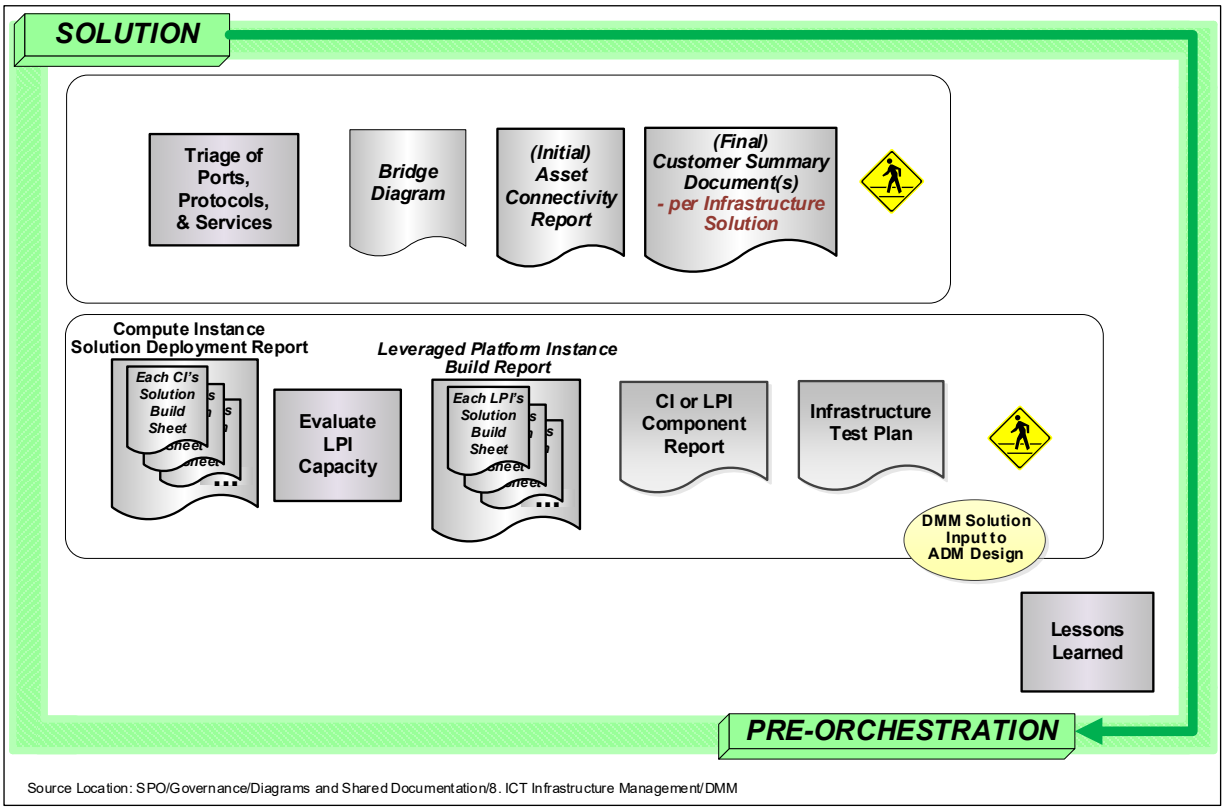



**Figure 1-5** Solution Phase

The Solution Phase encompasses the processes related to the discovery, detailed design, and documentation of the following items.

- Physical and logical network infrastructure
- Physical and logical server infrastructure
- Other leveraged platform infrastructure
- Infrastructure hardware component procurement requirements
- Software component procurement requirements

Using the ***Integrated Cloud Orchestration System***, artifacts are created to ensure the capture of infrastructure technical design specifications in a format that supports the deployment activities for a given Work Request.

These are the deliverables of the Solution Phase.

- Triage of Ports, Protocols and Services Bridge Diagram
- (Initial) Asset Connectivity Report
- (Final) Customer Summary Document
- Compute Instance Solution Deployment Report(s)
- Leveraged Platform Instance Capacity Analysis
- Leveraged Platform Instance Build Report(s)
- CI or LPI Component Report
- Infrastructure Validation Plan

## 1.4.1 Triage of Ports, Protocols and Services

The Infrastructure Solution Designer conducts a triage of the Ports, Protocols and Services, comparing the new connectivity requirements to the allowed list of ports and protocols listed within the Ports, Protocols and Services table. This allows the Infrastructure Solution Designer to document what new connectivity is "Pre-Engineered" and "Pre-Approved" and what connectivity needs to be evaluated by the Integration Engineer. The results of this triage are recorded in the Bridge Diagram.

The Integration Engineer evaluates any requested new connectivity that is NOT "Pre-Engineered" and NOT "Pre-Approved." The Integration Engineer processes this new connectivity into the Ports, Protocols and Services table, including risk identification of certain connectivity that does not meet the current network architectural standards as documented in the Engineering Network Placement and Design Principles department document. The result of the Ports, Protocols and Services Evaluation is an updated Ports, Protocols and Services document or a rejection of the requested connectivity by SRCA.

## 1.4.2 Bridge Diagram

A prerequisite to the Bridge Diagram is the approved Final Concept Diagram or the ADM Diagram. Any changes to the Concept Diagram or ADM Diagram are reflected in the Bridge Diagram.

The Bridge Diagram is a design tool used to provide a logical design comprised of the infrastructure items and the associated traffic flow and protocol including any leveraged infrastructures. The diagram includes the result of the triage of Ports, Protocols and Services performed by the Infrastructure Solution Designer.

The Bridge Diagram that is generated is specific to the given Work Request, produced by the Infrastructure Solution Designer, provides a non-environmental understanding of functionally grouped logical infrastructure items for the given Work Request, and is the result of triaging the impact to the Ports, Protocols and Services.

# 1.4.3 (Initial) Asset Connectivity Report Content

The (Initial) Asset Connectivity Report is a listing of the items on the Bridge Diagram and from the Customer Summary Document. The report's primary purpose is to provide a list of the assets requiring connectivity. The Infrastructure Solution Designer produces the (Initial) Asset Connectivity Report.

# 1.4.4 (Final) Customer Summary Document

During the Solution Phase, the Customer Summary Document created during the Requirements Phase is updated if necessary. For a discussion about this document, refer to the section *Requirements Phase > (Initial) Customer Summary Document Content* above. The document cannot be completed until the application's Final Concept Diagram has been approved by the Enterprise Architect. The (Final) Customer Summary Document is included as part of the ASM Framework design documentation. The document is reviewed again by the Architect.

The Final Customer Summary Document Review follows the same process as the (Initial) Customer Summary Document Review in the Requirements Phase.

## 1.4.4.1 Solution Architecture Review

The first review during the Solution Phase is to review the following Solution Design items:

- Port, Protocols and Services Triage result
- Bridge Diagram
- (Initial) Asset Connectivity Report
- (Final) Customer Summary Document

The following is a list of required participants for this review:

- Infrastructure Solution Designer
- Integration Engineer
- Architect
- Solution System Designer

After this review, the Architect follows the Architectural Review process for the Bridge Diagram. Once approved by the Enterprise Architect, the Infrastructure Solution Designer continues developing the details of the Solution design.

# 1.4.5 Develop Solution Package

## 1.4.5.1 Compute Instance Solution Deployment Report

Once the Bridge Diagram has been approved by the Enterprise Architect, the Infrastructure Solution Designer begins to specify the infrastructure items by developing the Solution Deployment Report, which contains specifications for building and configuring all the infrastructure required to meet the application's infrastructure requirements. This includes physical or logical server attributes, operating systems, IP addressing, etc. By conducting work sessions with Technical Support Specialists and

Deployment Specialist(s), the Infrastructure Solution Designer refines the Solution Deployment Report until it's completed.

### Evaluation of Leveraged Platform Instance Capacity

The Infrastructure Solution Designer consults with the Technology Owner(s) for the available capacity in any existing Leveraged Platform Instances impacted by this Solution. If changes are needed to support the Solution, the Infrastructure Solution Designer will develop the Leveraged Platform Instance Build Reports.

## 1.4.5.2 Leveraged Platform Instance Build Report

The Infrastructure Solution Designer creates the Leveraged Platform Instance Build Report to describe the requirements for any leveraged platform instances that may need deployment or modification for the compute instances.

## 1.4.5.3 CI or LPI Component Report(s)

The Infrastructure Solution Designer creates the CI or LPI Component Report to list all the Infrastructure components that need to be provisioned by Asset Services. This is included in the Solution Review.

## 1.4.5.4 Infrastructure Validation Plan

The Infrastructure Validation Plan describes the validation requirements used to verify that the infrastructure meets the Solution's design and expectations in terms of performance, functionality and reliability. Work Request Team members can use this document to anticipate validation requirements and activities.

The Infrastructure Validation Plan is developed by the Test Designer(s). The following I/S team members should help develop the Validation Plan:

- Tester(s)
- Infrastructure Solution Designer
- Deployment Specialist(s)

### Infrastructure Validation Plan Content

The Validation Plan contains the following information:

- Defined purpose for validation
- Major features and functions that will be tested
- Data Transmission validation
- Impacted validation areas
- Validation timeline considerations
- Validation deliverable dates
- Validation risks, assumptions and contingency plans

- Security requirements for validation
- Access requirements for validation
- Description of validation activities
- List of infrastructure items testable only by Deployment Specialist
- Validation scenarios
- Strategies for automation and performance validation
- Load Test requirements (type, environments, phases and participants)
- Credit Card Account Information validation requirements

## Infrastructure Validation Plan Review

The Infrastructure Validation Plan Review is conducted as part of the Solution Package Review. The identified I/S Testers begin developing the Infrastructure Test Matrix. Refer to *ICT Infrastructure Management* > *Deployment Management Methodology* > *Roll Out* for details.

## Solution Package Review Content

The following items are used in the Solution Package Review:

- Solution Deployment Report(s)
- Leveraged Platform Capacity Analysis
- Leveraged Platform Build Report(s)
- Infrastructure Validation Plan
- (Initial) CI or LPI Component Report

The following is a list of required participants for the Solution Package Review:

- Infrastructure Solution Designer
- Deployment Specialist(s)
- Integration Engineer
- Architect
- Security Compliance Specialist
- Solution System Designer

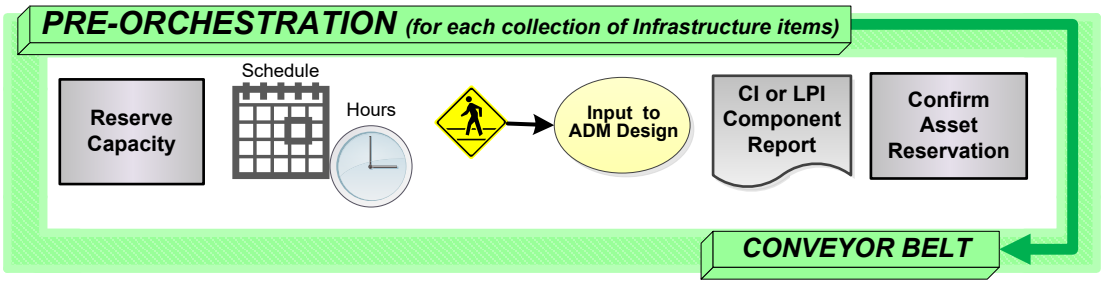
The Solution Package documentation serves as input to the ASM Framework design documentation.

## Lessons Learned

A Lessons Learned session is conducted at the end of the Solution Phase.

# 1.5 Pre-Orchestration Phase

Once the entire Solution for all requested execution instances has been designed, reviewed and approved, the Pre-Orchestration Phase can begin. The essence of this phase (Figure 1-6) is to acquire all the assets needed for the execution instance deployment.




Source Location: DCM/Governance/Diagrams and Shared Documentation/ SysDevMethodologyDiagrams Index: DMM-4

**Figure 1-6** Pre-Orchestration Phase Deliverables and Review

These are the deliverables for the Pre-Orchestration Phase.

- Reservation of the capacity for Leveraged Platform Instances
- Scheduled Dates
- Hours estimates
- Final CI or LPI Component Report
- Asset Reservation

The following is a list of required participants for the Pre-Orchestration Review.

- Project Manager
- Infrastructure Solution Designer
- Team Leads (“queue coordinators”)

# 1.6 The Conveyor Belt

The Pre-Orchestration Phase provisions the infrastructure hardware and software for the Work Request. As the assets are made available to the Deployment Specialist, the Conveyor Belt processes begin. The Deploy, Compliance Acceptance Review and Activation phases make up the Conveyor Belt and are executed for each Infrastructure item. Once all the Infrastructure items for each execution instance are off the Conveyor Belt, the Roll Out Phase begins for that execution instance and then followed by the Post Roll Out Phase. This is depicted in the following diagram (Figure 1-7). The individual phases are described in further detail later in this section.

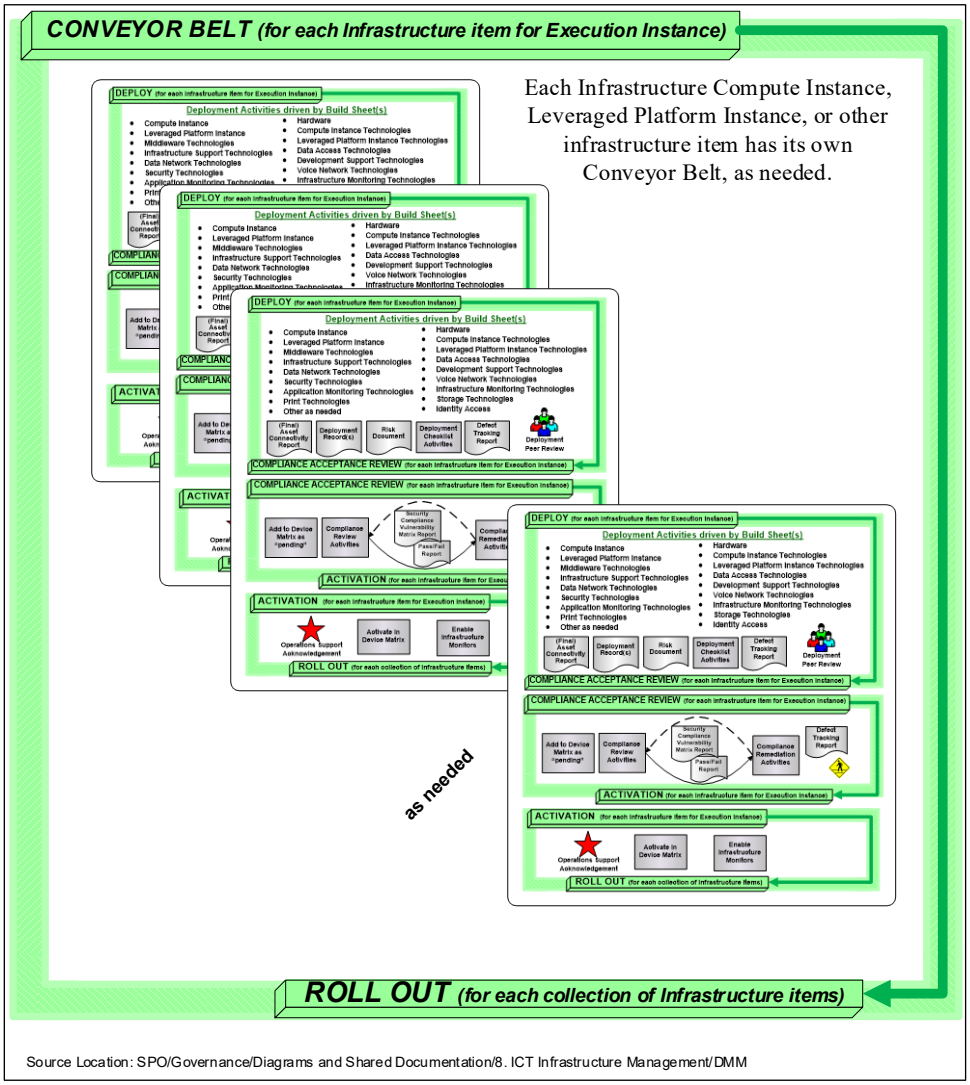



**Figure 1-7** The Conveyor Belt

Figure 1-8 below shows the following Information Communication Technology (ICT) Deployment Management Methodology phases repeated for each requested execution instance.

These multiple Conveyor Belt phases are listed below.

- Deploy
- Compliance Acceptance Review
- Activation

For each execution instance, there is a Roll Out Phase and a Post Roll Out Support Phase.

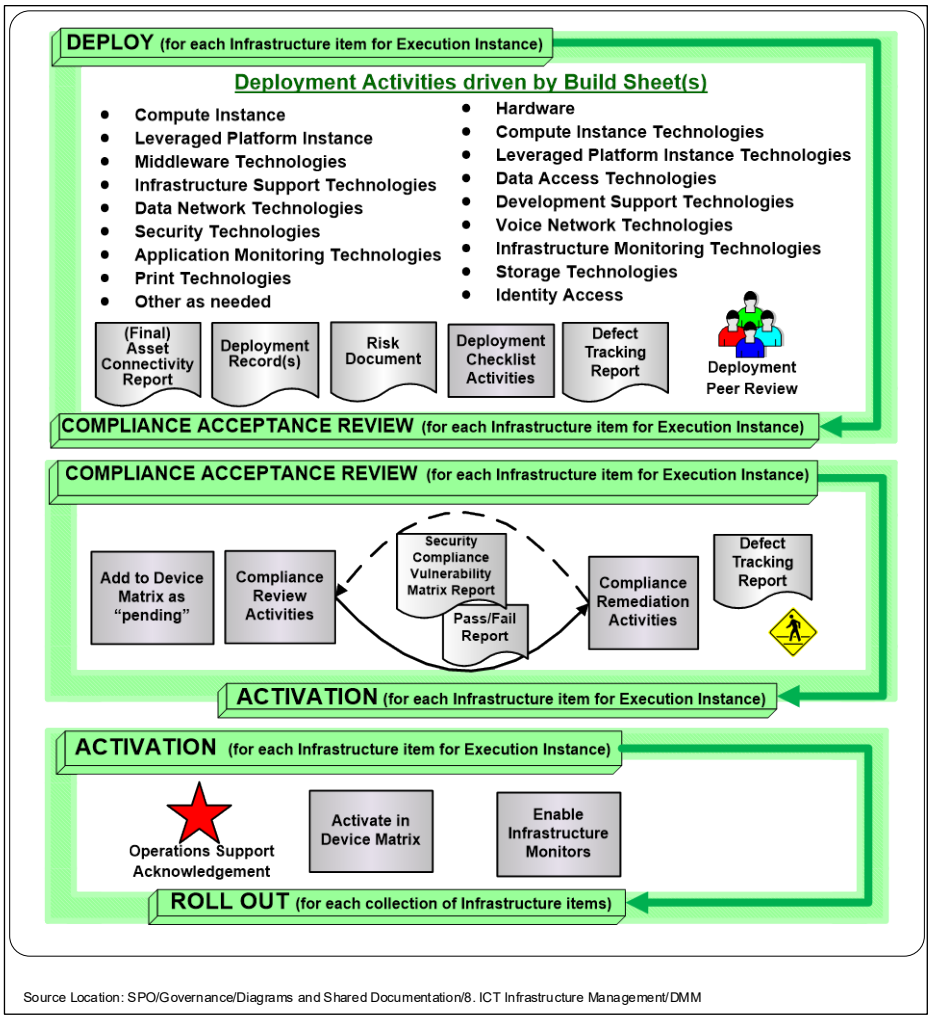



**Figure 1-8** Conveyor Belt Methodology Phases

## 1.6.1 Deploy Phase

This phase (Figure 1-9) encompasses the processes related to the execution of the infrastructure specifications in the Solution Deployment Report to construct physical or logical infrastructure items for an execution instance. This phase is where the required infrastructure is built or modified and includes the installation of hardware, the operating system, any prescribed system management agents, system-level patches, and other technologies for a particular item of the infrastructure.

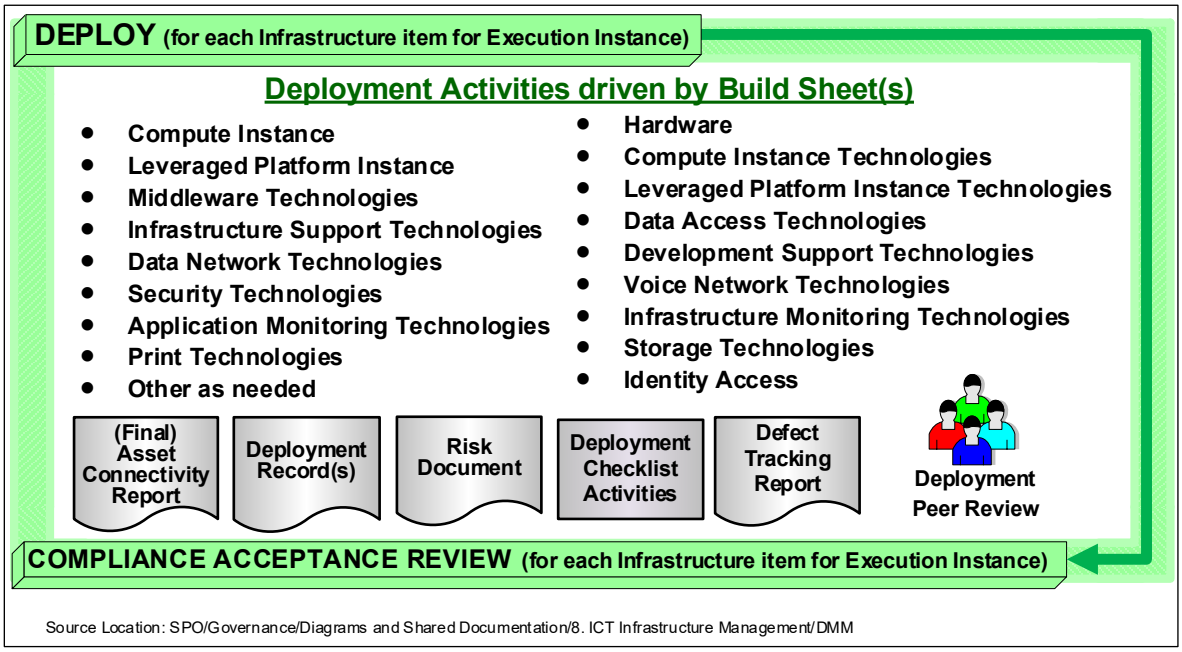



**Figure 1-9** Deploy Phase Deliverables and Reviews

The Deployment Specialists deliver the following infrastructure items:

- Hardware
- Compute Instance(s)
- Compute Instance Technologies
- Leveraged Platform Instance(s)
- Leveraged Platform Instance Technologies
- Middleware Technologies
- Data Access Technologies
- Data Network Technologies
- Development Support Technologies
- Security Technologies
- Voice Network Technologies
- Application Monitoring Technologies
- Infrastructure Monitoring Technologies
- Infrastructure Support Technologies

- Print Technologies
- Storage Technologies
- Identity Access Configuration
- Any other Infrastructure (as needed)
- Deployment Records
- (Final) Asset Connectivity Report, updated by the Integration Engineer

### 1.6.1.1 Network Configuration

The Firewall rules and any other designed network changes are completed either as the deployment of the infrastructure proceeds or after all items have been deployed. The Integration Engineer finalizes the Asset Connectivity Report so that the Work Request documentation contains the connectivity information, as deployed.

### 1.6.1.2 Deployment Peer Review

Using the Deployment Checklist, the Deployment Specialist(s) review the results of the Deploy Phase with their peers.

### 1.6.1.3 Risk Document

The Deployment Specialist(s) develop a Risk Document, if needed, to explain why any infrastructure item has not been made compliant according to the Security Configuration Checklist.

Any security vulnerabilities that cannot be remediated because they conflict with the operating system or the applications requirements must be accounted for in a Risk Document. The individual participating in the process will perform one or more of the following activities: 1) Update an existing document, 2) Submit a new document, or 3) acquire agreement from SRCA for a plan for submitting the documentation with 72 hours of system implementation. All documentation is submitted to Security.Office (email address) or by other means as prescribed by SRCA.

For more details, see *Application Systems Management* > *Project Management* > *Business Risk Identification*.

### 1.6.1.4 Defect Tracking Report

The DMM team records any defects with the deployment or design. The Test Designer coordinates resolution of the defects.

## 1.6.2 Compliance Acceptance Review Phase

This phase (Figure 1-10) encompasses the evaluation of any newly deployed or modified infrastructure hardware or software to ensure that it meets the security requirements of the application and infrastructure software.

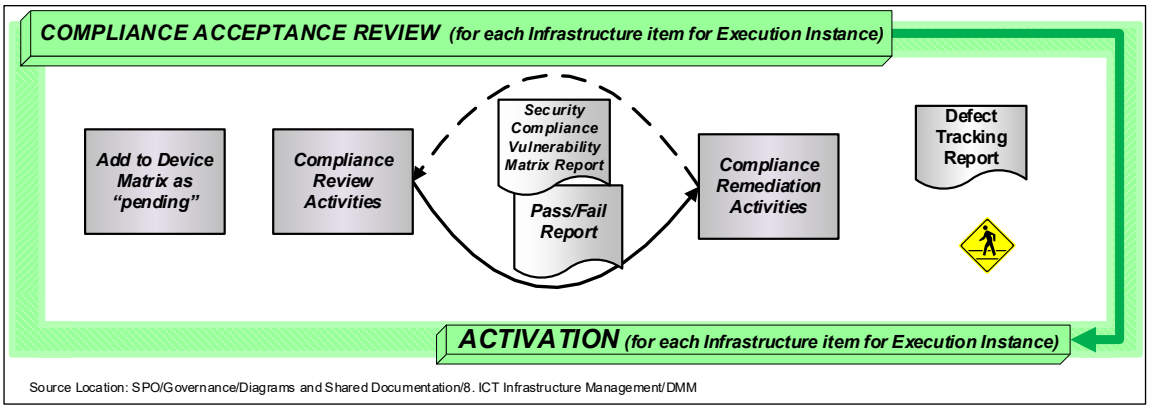



**Figure 1-10** Compliance Acceptance Review Phase

These are the deliverables of the Compliance Acceptance Review Phase.

- Device Matrix updated as "pending"
- Executed (Completed) Security Compliance Acceptance Review resulting in a Compliance-Validated infrastructure
- Security Compliance Vulnerability Matrix Report for Pass/Fail determination
- Defect Tracking Report

The Security Compliance Specialist updates the Device Matrix labelling the infrastructure device as "pending" and then executes the scans for security vulnerabilities. The Security Compliance Specialist documents the results and logs any defects. The defects are resolved either with a Risk Document or with security configuration changes.

### 1.6.2.1 Security Compliance Vulnerability Matrix Report Content

The Security Compliance Vulnerability Matrix Report is the result of the vulnerability scans and presents a point-in-time state of the newly deployed infrastructure. This report is used to determine the platform score for the network enclave. If the score is less than or equal to the average score for the enclave, the infrastructure item "passes" the Compliance Acceptance Review. If the score is more than the average for the enclave, the item "fails" the Compliance Acceptance Review and a defect is logged to remediate.

## 1.6.3 Activation

This phase encompasses the processes related to the transfer of knowledge to ensure BlueCross Operations Support organizations are prepared to support the newly deployed infrastructure. Figure 1-11 depicts the deliverables and reviews involved in the Activation Phase.

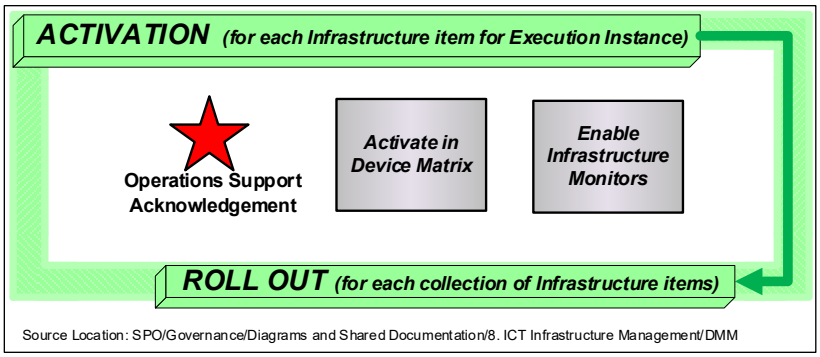



**Figure 1-11** Activation Phase

These are the deliverables of the Activation Phase.

- Operations Support Acknowledgement
- Device Matrix Update
- Enabled Infrastructure Monitors

## 1.6.3.1 Operations Support Acknowledgement

It is vital that the organization that will be responsible for the ongoing support of the new infrastructure be educated in the changes that have occurred. Before the infrastructure is deemed operational, the organization responsible for its support needs to acknowledge this responsibility and their understanding of its items. Operations Support organizations are responsible for ensuring that the information they are provided with is sufficient for them to perform their execution and maintenance functions.

### Operations Support Acknowledgement Content

The content of the Operations Support Acknowledgement consists of updated Work Request documents as listed in the Review section below. These documents provide the Operations Support with the information they need to monitor, manage and maintain the infrastructure.

### Operations Support Acknowledgement Review

The following is a list of required Operations Support Acknowledgement Review participants.

- Operations Support for each infrastructure area affected
- Deployment Specialist(s) to answer any questions

The documentation required at the Operations Acknowledgement Review is listed below.

- Final Customer Summary Document
- Solution Deployment Report(s)
- Leveraged Platform Instance Deployment Report(s)

- Bridge Diagram
- (Final) Asset Connectivity Report
- Deployment Record(s)
- Any Risk Documents describing exceptions to Security Configuration Checklists
- Security Compliance Vulnerability Matrix Report & Pass/Fail result
- Operations Acceptance Checklist

### 1.6.3.2 Device Matrix Update

Once the Operations Support Acknowledgement has reached concurrence, the Security Compliance Specialist updates the Device Matrix by labelling the infrastructure device as "Active." The device will now be scanned for security vulnerabilities on the regularly scheduled scans for the enclave.

### 1.6.3.3 Enabled Infrastructure Monitors

Operations Support notifies the Enterprise Monitoring Systems team to enable the infrastructure monitors, as now the infrastructure items are operational.

## 1.6.4 End of the Conveyor Belt

This concludes the iterative phases on the Conveyor Belt for each execution instance. These iterative phases are repeated so that the execution instances needed by the applications are ready for use during the testing phases.

**NOTE** Once all the infrastructure for the execution instance is marked at "Roll Out Start" in ICOS, the Roll Out Phase can begin.

# 1.7 Roll Out

This phase (Figure 1-12) consists of testing the infrastructure in the execution instance and notifying the Work Request team that the infrastructure collection is now complete.

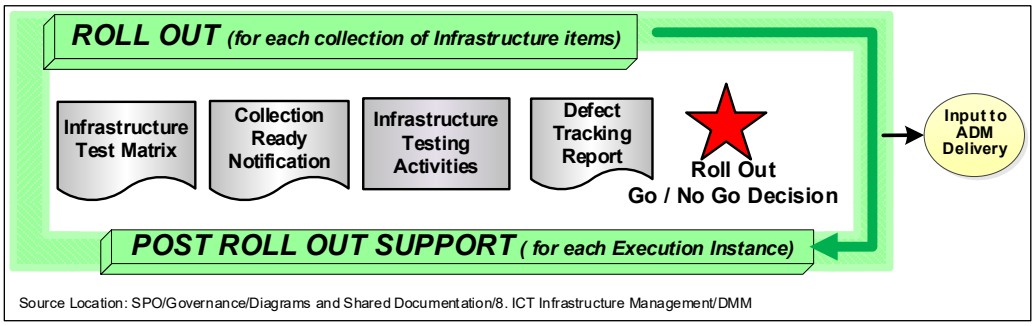



**Figure 1-12** Roll Out Phase

## 1.7.1 Infrastructure Test Matrix

The Infrastructure Test Matrix is a suite of all of the validation cases the I/S Tester(s) intends to execute during the Roll Out Phase to ensure that infrastructure requirements are met and that the complete solution is functioning without error. The Tester begins development of the Infrastructure Test Matrix as soon as the Validation Plan has been completed and completes the matrix during the Roll Out Phase.

### 1.7.1.1 Infrastructure Test Matrix Content

The Infrastructure Test Matrix contains the following information.

- Traceability of test cases to Infrastructure requirements and Deployment Reports
- Structured validation documents (e.g., cyclomatic diagrams), if any have been created
- List of Validation Cases to be tested (test cases may be scenarios defined in the Validation Plan)
    - Each test case must contain the following information.
        - Purpose of the validation
        - Any variations of validation
        - Any variables used
        - Change log
        - Approval status
        - Execution status

### 1.7.1.2 Infrastructure Test Matrix Review

An Infrastructure Test Matrix Review formally reviews and approves the Infrastructure Test Matrix for a given Work Request prior to execution.

The list of participants in the Infrastructure Test Matrix Review should include these Roles.

- Test Designer(s)
- Testers
- Infrastructure Solution Designer
- Deployment Specialist(s)

## 1.7.2 Execution Instance Ready Notification (Collection Ready)

The Infrastructure Solution Designer reviews the results of the Conveyor Belt activity for the infrastructure for this execution instance. If satisfied that the Infrastructure was deployed, is complete and built as described in the Build Report(s), the Infrastructure Solution Designer notifies the Project Manager and Test Designer.

## 1.7.3 Infrastructure Validation Activities

The infrastructure in this execution instance is tested, using the Infrastructure Test Matrix, to ensure that not only is it built to the specification in the Solution Package, but that it works correctly. Data Access groups and connectivity are also tested.

The Defect Tracking Report is produced by the Test Designer.

## 1.7.4 Roll Out Go/No Go Decision

The Test Designer, Infrastructure Solution Designer and the Project Manager determine if the Infrastructure Validation has been completed satisfactorily. The Project Manager records the Roll Out Go/No Go Decision.

### 1.7.4.1 Lessons Learned

A Lessons Learned session is conducted at the end of the Roll Out Phase.

### 1.7.4.2 End of Roll Out Phase

This concludes the execution of the Conveyor Belt and the Roll Out of the Infrastructure for a particular Execution Instance, which is repeated so that the environments needed by the applications are ready for use during the validation phases.

**NOTE** At this point in the life cycle, the infrastructure for this Execution Instance is in "Roll Out Complete" status in ***ICOS***.

**NOTE** Any other execution instances described in the Solution Phase are developed using the Conveyor Belt process and the Roll Out Phase according to the schedule developed by the Work Request team.

# 1.8 Post Roll Out Support Phase

This phase (Figure 1-13) encompasses the processes related to the corrective actions taken to support the newly deployed and operational infrastructure related to infrastructure while the execution instance is being used.

The execution instance, once in the Post Roll Out Support Phase, is considered deployed for operational use. Any issues with the infrastructure are considered Break/Fix Incidents and Work Request Post Go-Live Defects.

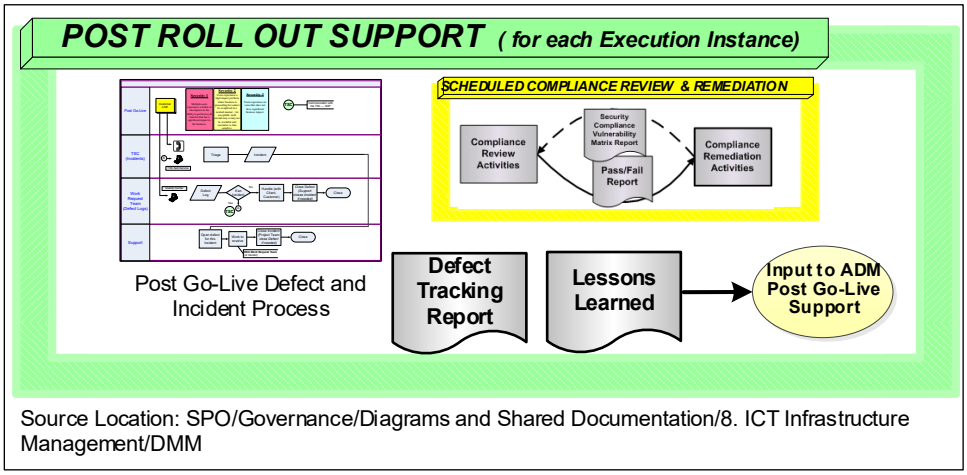



**Figure 1-13** Post Roll Out Support Phase

This phase begins after each Roll Out Phase for each execution instance collection that was deployed and continues until the Work Request is closed. This phase supports the infrastructure after the Work Request teams have loaded their software and during the application testing activities.

These are the deliverables for the Post Roll Out Support Phase.

- Scheduled Compliance Review and Remediation resulting in a Compliance-Tested infrastructure after the application software has been installed
- Defect Tracking Report
- Lessons Learned

## 1.8.1 Scheduled Compliance Review and Remediation

The Scheduled Compliance Review and Remediation encompasses the processes related to the routine evaluation of the deployed infrastructure after the business application code has been installed. The evaluation occurs on a regularly scheduled basis as part of the ongoing Security Compliance work process and ensures that the system continues to remain compliant with security and audit requirements. This deliverable needs to occur after each related Roll Out Phase for the involved Execution Instances.

The Scheduled Compliance Review and Remediation is exercised and the results documented and defects logged. During the Post Roll Out Phase, the defects are resolved or risk documentation is created until any compliance deficiencies have been mitigated.

The Security Compliance Specialist is responsible for exercising the Scheduled Compliance Review and Remediation in a routinely scheduled time frame. The responsible application maintainer and Operations Support will provide the support resolving issues and responding to inquiries during this activity.

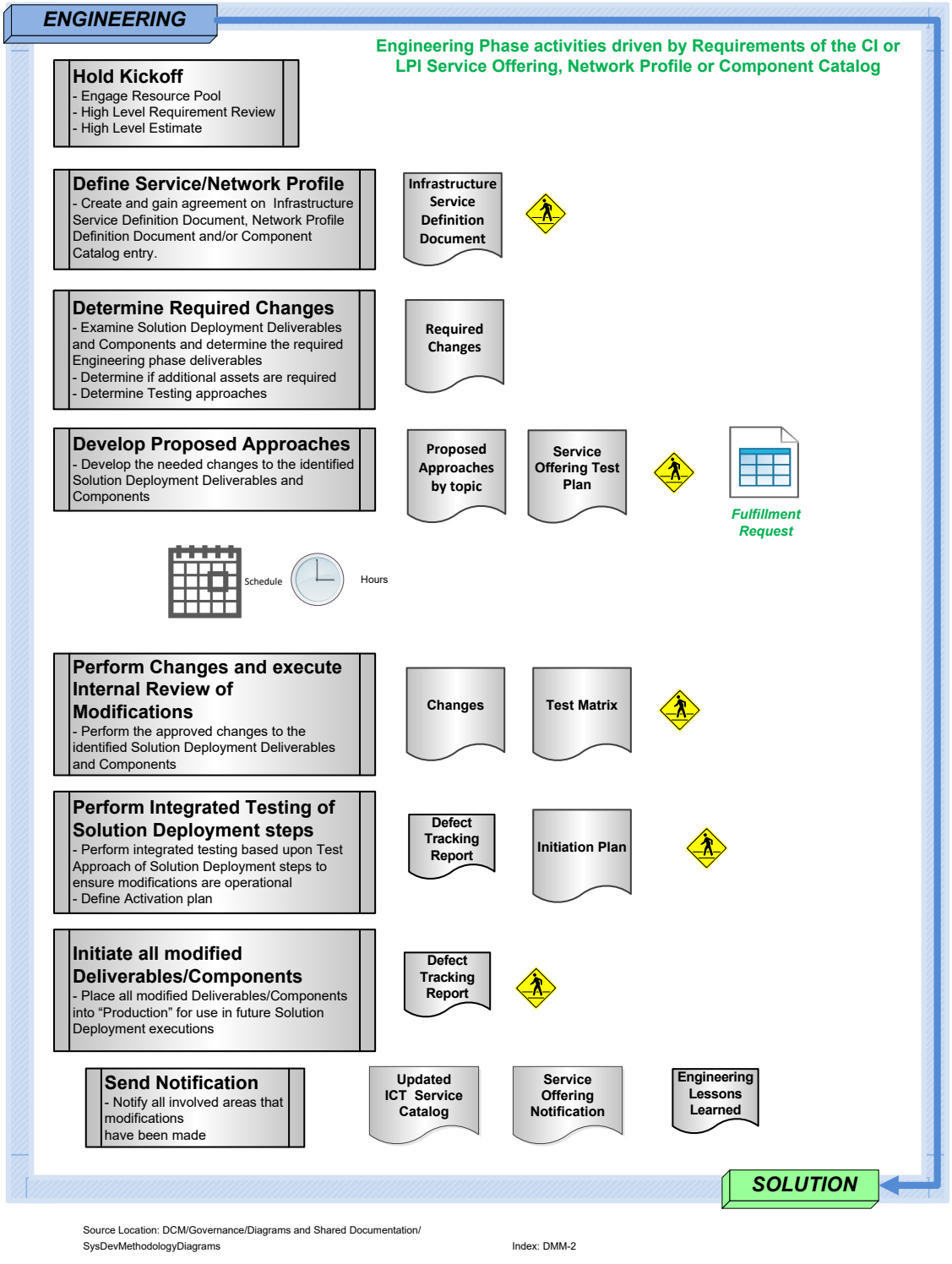
## 1.8.2 Lessons Learned

The Lessons Learned collected earlier in the DMM phases is combined with the Work Request Lessons Learned.

# 1.9 Engineering

Once a Service Creation Request is approved by the Enterprise Architect(s), the Engineering Phase begins.

The Engineering Phase is executed when an Infrastructure Service Offering is needed that is not available in the Information Communication Technology (ICT) Service Catalog. An Infrastructure Service is a combination of approved infrastructure technologies designed to support multiple applications or application systems having common infrastructure requirements. The Service Creation Engineer serves as the primary technical leader for the Engineering Phase.




Source Location: DCM/Governance/Diagrams and Shared Documentation/ SysDevMethodologyDiagrams Index: DMM-2

**Figure 1-14** Engineering Phase Deliverables and Reviews

As shown in Figure 1-14 above, the Engineering Phase is comprised of multiple sub-phases for the creation of a new Infrastructure Service Offering. The sub-phases are described below.

# 1.9.1 Conduct Kickoff

The Engineering Phase Kickoff consists of a meeting with the identified participants (Infrastructure Solution Designer, Platform Owner, Technology Owner, Integration Engineer, etc.). During the kickoff process, the team reviews the Service Creation Request and the Infrastructure Service Offering requirements to identify all of the involved areas and to provide initial time and schedule estimates to the Project Manager.

# 1.9.2 Define Service/Network Profile

The Infrastructure Service Offering is represented in the form of an Infrastructure Service Definition Document stored in the ICT Service Catalog. The Service Creation Engineer creates the Infrastructure Service Definition Document.

## 1.9.2.1 Service Definition Document

The Service Definition Document includes information about requirements relating to Infrastructure Services and outlines the new or modified Infrastructure Service Offering.

### Service Definition Document Content

The Service Definition Document contains these items.

- General information about the Work Request
- The Service Creation Engineer's name
- Platform Owner name(s)
- The Infrastructure Service Offering that needs to be developed
- Decision Matrix Choices and Options
- A list of Network Profiles
- A list of Optional and Standard Technologies

### Engineering Considerations

The Engineering Considerations provide a list of all of the Infrastructure items that must be considered for each Infrastructure Service Offering. The Infrastructure Service Creation Engineer uses this to guide the Service Creation Team during this phase.

- Used during Requirements Phase
    - Desk Procedures
    - CI Service Definition
    - CI Choices & Options

  - Network Profile
  - Network Choices & Options
  - LPI Service Definition
  - LPI Choices & Options

- Used during Solution Phase

  - Desk Procedures
  - Rules for Ports, Protocols, Services
  - Bridge Diagram Format
  - Asset Connectivity Report Format
  - Build Sheet Format
  - LPI Decision Tree
  - Network Decision Tree
  - Solution Deployment Report Format
  - Component Catalog Entries for CI or LPI
  - LPI Placement Rules

- Used during Orchestration Phase

  - Desk Procedures

- Used during Conveyor Belt

  - Desk Procedures
  - Queue Manager & Queue Coordinator Information

- Used during Deploy Phase

  - Desk Procedures
  - Infrastructure Configurations
  - Orchestrator Instructions
  - Element Manager Scripts
  - Security Configuration Checklists
  - Risk Document Desk Procedures
  - Deployment Record Layout
  - Deployment Checklist

- Used during Compliance Acceptance Review Phase

  - Desk Procedures
  - Vulnerability Threshold Values
  - Remediation Desk Procedures

- Used during Activation Phase

  - Desk Procedures
  - Operations Support Acceptance Checklist

- Used during Roll Out Phase

  - Desk Procedures
  - Validation Testing Criteria for CI or LPI

- Used during Post Roll Out Phase

  - Desk Procedures

- Updates to the Data Center Blueprint
- Updates to the Utilization Hub system

### Service Definition Document Review

The documentation required for review at the Service Definition Document Review is the Infrastructure Service Definition Document.

The following is a list of required participants for the Service Definition Document Review.

- Service Creation Engineer
- Integration Engineer
- Technology Owner(s)
- Platform Owner(s)
- Architect
- Enterprise Architect(s)

## 1.9.3 Determine Required Changes

This sub-phase defines all the needed changes to items and deliverables for Solution Deployment to occur, such as tool and template changes. This sub-phase also determines if additional assets are required and determines test approaches. Deliverables include Purchase Request Packets(s), if required, and a Service Offering Validation Approach.

### 1.9.3.1 Determine Tool Changes

The Engineering team determines if any tool changes are required. These changes include, but are not limited to, Infrastructure Designer, Orchestrator(s), Utilization Hub, Component Catalog and Element Manager(s).

### 1.9.3.2 Determine Template Changes

Templates include, but are not limited to, these items.

- Customer Summary Document
- Asset Connectivity Report
- Solution Deployment Report
- Compute Instance Build Sheet(s)
- Deployment Checklist
- Deployment Record
- Security Configuration Checklist

- Operations Support Acceptance Checklist

## 1.9.3.3 Determine Changes to Other Data Sources

Data Sources include, but are not limited to, these items.

- Decision Matrix
- System Master Index
- Architecture Book
- Leveraged Platform Instance Decision Tree
- Device Matrix
- Component Catalog

## 1.9.3.4 Determine Desk Procedure Updates

Desk procedure areas include, but are not limited to, these areas.

- LPI Confirmation and Validation
- Computing Instance Confirmation Raw Material Preparation
- Facilities Confirmation and Validation
- Hardware Preparation Activities
- Facilities Activities
- Operating System Deployment Activities
- Compute Instance Operating System Configuration Activities
- Leveraged Platform Instance Configuration Activities by Platform
- Compute Instance Technology Deployment Activities
- Compute Instance Technology Configuration
- Deployment Checklist
- Compute Instance Baseline Configuration Activities
- Compliance Review Activities
- Compliance Remediation Activities

## 1.9.3.5 Component Catalog Entry

Each entry in the Component Catalog maintained in **the *Integrated Cloud Orchestration System (ICOS)*** describes an Infrastructure item required to deploy the Infrastructure Service Offering. The Service Creation Engineer collaborates with the Work Request team, specifically with Technology Owners and Platform Owners as well as I/S Asset Management, to create the entry.

## 1.9.3.6 Infrastructure Service Offering Test Approach

The goal of this deliverable is to determine the testing requirements for the identified deliverables and items of the new Infrastructure Service Offering. The Service Creation Engineer is responsible for creating the validation approach.

### Infrastructure Service Offering Validation Approach Review

The documentation required for review at the Infrastructure Service Offering Validation Approach Review is the Infrastructure Service Offering Validation Approach.

The following is a list of required participants for the Infrastructure Service Offering Validation Approach Review.

- Service Creation Engineer
- Integration Engineer
- Other participation based upon subject matter

# 1.9.4 Develop Proposed Approaches

This subphase describes specifications for the changes to the previously identified deliverables and items. Participation is determined based on the changes needed. All involved team members will help create approaches.

## 1.9.4.1 Proposed Approaches by Topic

Approaches are created by all involved team members.

## 1.9.4.2 Approaches by Topic Review

The documentation required for review at the Approaches by Topic Review is the Proposed Approach(es).

The following is a list of required participants for the Approaches by Topic Review.

- Participation based upon subject matter

# 1.9.5 Perform Changes and Execute Internal Review of Modifications

This subphase describes the processes related to the creation, modification, and the evaluation of the identified deliverables and items to ensure that they comply with requirements. The completed Infrastructure Service Offerings are the deliverables in this subphase. Deliverables include template updates, tool changes and desk procedure updates. All involved team members should perform changes as identified.

## 1.9.5.1 Perform Changes and Execute Internal Review

Identified Infrastructure Service Offering items are modified by the involved team members.

### Item(s) Review

Each team member conducts a review for the changes. The participants for these reviews include all the involved team members.

# 1.9.6 Perform Integrated Validation of Solution Deployment Steps

This subphase describes the process of performing integration validation of the Solution Deployment Phases based on the Validation Approach to ensure all modifications are operational. Deliverables from this subphase include an Executed Validation Approach and an Initiation Plan. The end-users of the items serve as testers during this subphase.

## 1.9.6.1 Executed Test Approach

Integrated validation is performed on the identified deliverables and items as identified in the Test Approach by all involved team members.

## 1.9.6.2 Initiation Plan

The Service Creation Engineer creates the Initiation Plan and conducts a review with all applicable members of the Infrastructure Service Offering Team.

The following is a list of required participants for the Executed Validation Approach and Initiation Plan Review.

- Service Creation Engineer
- Infrastructure Solution Designer
- Deployment Specialist(s)
- Other participation based upon subject matter

# 1.9.7 Initiate All Modified Deliverables/Components

This subphase consists of the execution of the Initiation Plan to activate the identified deliverables and items for future use in Solution Deployment. The major deliverable from this process is the Executed Initiation Plan. Participation is determined based on the changes needed. This subphase results in placing all identified deliverables and component catalog entries into “production” to be used in Solution Deployment executions.

# 1.9.8 Send Notification

This is the final subphase in the Engineering Phase. All involved areas are notified that modifications have been made and that the service is now available in the ICT Service Catalog. The notification is sent by the Project Manager.

# 1.9.9 Lessons Learned

The Engineering Phase requires its own Lessons Learned session.

# 1.10 Deployment Management Methodology Variation for Workstation Deployment

Workstation installations include both software and hardware covering both Application Systems Management Framework and Deployment Management Methodologies. This section describes the variation in the Deployment Management Methodology.

Initiate installations via a Work Request or a Purchase Requisition (PR) found on the I/S Procurement portal site accessed through My e-Work. Use a PR for either a new or replacement workstation. Deploy all workstations directly to production; there are no validation execution instances. For new employees, the new hire process initiates a workstation procurement with a purchase requisition being created later

## 1.10.1 Requirements and Solution Phases

The Requirements and Solution phases are executed together. The aim of these phases is to reach agreement with the requestors on their specific application and infrastructure business requirements and to define how these are executed.

Requirements are predefined based on the type of workstation needed. The requirements are available by computing platform (Desktop, Laptop, or Workstation) and line of business on the I/S Procurement portal site accessed through My e-Work. Both hardware and software are selected. The purchase requisition, questionnaire, and justification form (if needed) on the portal site are the initial requirements.

### 1.10.1.1 (Initial) Customer Summary Document

Create the (Initial) Customer Summary Document from the Purchase Requisition, justification form and questionnaire. Upon receipt of the paperwork at IS.Procurement@BCBSSC.com, I/S Procurement will review it for anomalies.

---

**NOTE** The (Initial) Customer Summary Document is not printed nor used in the deployment of Workstations.

---

If an appropriate workstation is not available in the Procurement IT Catalog or if there is a need for a new Infrastructure Service Offering or a modification to an existing Infrastructure Service Offering that is not currently in the IT Catalog, the Infrastructure Solution Designer will document the requirements. The Infrastructure Solution Designer completes the “New Hardware/Software Review” Service Request on TSC Self-Service. This Service Request is used to request approval from the Workstation Infrastructure Subcommittee (WISC) and is the equivalent of the Service Creation Request Document. If this request is approved by the WISC, the Engineering Phase is executed, see *ICT Infrastructure Management* > *Deployment Management Methodology* > *Engineering*. If it is not approved, the requirements are re-evaluated.

### 1.10.1.2 Service Creation Request Document

For Workstation, the Service Creation Request Document is replaced with the "New Hardware/Software Review" Service Request on TSC Self-Service.

The review of this request is a review by the Workstation Infrastructure Subcommittee, who approves or denies the Service Request.

If an appropriate workstation is available in the IT catalog, the Infrastructure Solution Designer works with the requestor to understand all of the software and hardware requirements. This is done by completing the Pre-Deploy Checklist. This checklist is used to finalize the requirements and create the final Customer Summary Document. This checklist is signed by the customer when all requirements have been captured.

### 1.10.1.3 (Final) Customer Summary Document

For Workstation, the (Final) Customer Summary Document can be created from the Pre-Deploy Checklist.

A review is held with the customer and the Infrastructure Solution Designer following completion of the Pre-Deploy Checklist when all requirements have been defined.

**NOTE** The (Final) Customer Summary Document is not printed nor used by Workstation.

Once the requirements have been finalized, the Infrastructure Solution Designer creates the Solution Deployment Report. This report contains specifications for building the infrastructure items to meet the requirements.

### 1.10.1.4 Solution Deployment Report

Once the (Final) Customer Summary Document (Pre-deploy Checklist for workstation) is complete, the Infrastructure Solution Designer begins to describe the infrastructure items by creating the Solution Deployment Report.

The completed purchase requisition (Preq) is submitted to I/S Procurement once the requirements have been finalized. This final purchase requisition includes all the requirements for the infrastructure and applications.

## 1.10.2 Deploy Phase

This phase encompasses the processes related to the execution of the infrastructure specification in the Solution Deployment Report to construct the infrastructure items. This phase is where the required infrastructure is actually built or modified. This phase includes the installation of hardware, operating

systems, software and other technologies as required. Once the final purchase requisition is submitted, infrastructure is taken out of surplus or ordered and received.

The activities that take place during the Deploy Phase are detailed in departmental desk procedures. The following is a list of possible actions but is tailored for each workstation based on the Solution Deployment Report.

The Deployment Specialists:

- Build the Hardware.
- Deploy the Operating System.
- Deploy the Technologies.
- Deploy the Software.
- Configure the workstation.
- Confirm the deployment.
- Update the Deployment Record.

# 1.10.3 Compliance Acceptance Review Phase

This phase encompasses the evaluation of any newly deployed or modified infrastructure hardware or software to ensure that it meets the security and audit requirements of the application and infrastructure software. The Security Baseline configurations are applied to the infrastructure by the Deployment Specialist. This imaging takes place in a Workstation Support dedicated area where the 220 VLAN will be used if applicable. However, this is only a requirement for Medicare assets.

## 1.10.3.1 Security Compliance Review

When applicable, the Security Compliance Specialist conducts the Security Acceptance Review, documents the results and logs defects. The defects are resolved or risk documentation is created until any compliance deficiencies have been mitigated.

### Security Compliance Vulnerability Matrix Report

For workstations, the Security Compliance Vulnerability Matrix Report is the Workstation 220 VLAN Report. The 220 VLAN Report is the product of the vulnerability scans and presents a point-in-time posture of the newly deployed workstation(s). This report is the guideline for any necessary remediation, exceptions or justification documentation in order to complete the deployment of the infrastructure. The 220 VLAN Report is required for Medicare assets but will be used for all assets if available.

# 1.10.4 Activation Phase

This phase encompasses the processes related to the transfer of knowledge to ensure BlueCross Workstation Support organizations are prepared to support the newly deployed infrastructure.

## 1.10.4.1 Operations (Workstation) Support Acknowledgement

The organizations that will be responsible for the ongoing support of the new infrastructure should be educated on the changes that have occurred. Before the infrastructure is deemed operational, the organization responsible for its support needs to acknowledge this responsibility and their understanding of its items. Workstation Support organizations are responsible for ensuring that the information they are provided is sufficient for them to perform their functions.

### Operations Support Acknowledgement Content

The content of the Operations Support Acknowledgement consists of updated documents as listed below. These documents provide Workstation Support with the information they need to monitor, manage and maintain the infrastructure.

- (Final) Customer Summary Document (Pre-Deploy Checklist)
- Solution Deployment Report
- Deployment Record
- Security Baseline Exceptions
- Security Compliance Vulnerability Matrix Report (220 VLAN Report)
- Operations Acceptance Checklist (Deploy Log)

# 1.10.5 Roll Out Phase

This phase consists of a notification to the Customer that the infrastructure is now ready, a review, and acceptance by the Customer.

## 1.10.5.1 Customer Acceptance Review

The Customer and Workstation Support are required participants at the Customer Acceptance Review.

The documentation required at the Customer Acceptance Review is the work order from the Integrated Asset Management System that contains all the required hardware and software items for the workstation.

Once acceptance is obtained, the infrastructure is considered deployed for use. Any issues with the infrastructure are considered Break/Fix Incidents.

# 1.10.6 Post Roll Out Support Phase

This phase encompasses the process related to the corrective actions taken to support the newly deployed infrastructure related to application and infrastructure. Any issues with the infrastructure or applications at this point are considered Break/Fix Incidents.

# Chapter 2 Operations Management

## 2.1 Facilities Management

### 2.1.1 Environmental Utilities

Commercial power distribution is obtained from two separate substations located in Columbia, SC. This redundancy greatly reduces the possibility of a commercial power outage, as it is highly unlikely for both substations to fail simultaneously. Each substation provides adequate power to meet all the energy requirements of the facility. Each substation input is connected to its own 1,000 kW Uninterruptible Power Supply (UPS) system, capable of powering the facility for an extended time frame.

If both substations were to fail, the Data Center equipment would be backed up by a redundant pair of lithium-ion batteries. These two strings of batteries provide up to 60-minutes of backup power depending on the current data center equipment load. If one string should fail, the other can handle the entire data center equipment load. The batteries need to provide power for ~30 seconds before the backup diesel generator is automatically started. The 2,000-kW backup diesel generator holds 2,000 gallons of fuel and can be filled by a vendor near the facility if necessary.

Medicare power distribution is obtained from two separate substations located in Columbia, SC. This redundancy greatly reduces the possibility of a commercial power outage, as it is highly unlikely for both substations to fail simultaneously. Each substation provides adequate power to meet all of the energy requirements of the facility. Connected to each substation input is a separate 600 kW Uninterruptible Power Supply (UPS) system, each capable of powering the facility for an extended time frame.

If both substations were to fail, the Data Center equipment would be backed up by a redundant pair of lead-acid batteries. These two strings of batteries provide up to 60-minutes of backup power depending on the current data center equipment load. If one string should fail, the other can handle the entire data center equipment load. The batteries need to provide power for ~30 seconds before two diesel generators automatically start up. The redundant pair of 2,000-kW backup diesel generators hold 2,000 gallons of fuel each and can be filled by a vendor near the facility if necessary.

# 2.2 Infrastructure Support

## 2.2.1 Media Protection

### 2.2.1.1 Equipment and Tape Disposal and Release

#### Disposal

Before being transferred, used as surplus, or donated, any hard drive or systems containing a hard drive owned or managed by BlueCross BlueShield of South Carolina (BlueCross) must be sanitized by reformatting the hard drive in a secure manner or by using an approved wipeout utility. Diskettes and other magnetic storage media that contain any BlueCross data or software must be sanitized when they are no longer needed. Portable media may be reused after overwriting or degaussing, or they may be destroyed. Simply deleting a file is not sufficient to prevent someone from un-deleting the file later. If the system will be donated to an outside organization, it should have a complete operating system installed on it after sanitization.

Prior to removal of any computer equipment, consult with Information Communication Technology Non-Host (ICT NH), the Voice Data Communications (VDC) Help Desk or designated personnel by area for assistance in properly performing the cleansing task and in obtaining an approved wipeout or formatting utility. The area designee must log and sign a certification that the equipment has been properly sanitized using approved software before it can be added to surpluses, transferred, or donated. The area designee should save copies of all certification statements.

Data located on all systems and hard disks sent outside your organization for repair or data recovery should be protected from disclosure by contract with the company performing the service. If a non-disclosure agreement does not exist, then the hard drive of the equipment is removed prior to shipping.

Server hard drives will be physically destroyed if the drives cannot be accessed using the authorized sanitation software. The physical destruction consists of drilling multiple holes through the hard drive case as well as the disk themselves.

All information regarding sanitation or destruction must be maintained for a minimum of five years. All records (Tracking Log and Sanitization Logs) pertaining to server sanitization or destruction must be sent to ICT NH, or the off-site location must ensure proper record retention.

An inventory is maintained of all assets controlled by ICT NH. When a device has been sanitized or destroyed, it is noted in the inventory. Semiannually the sanitization and destruction forms on file are reconciled with what has been indicated in the inventory as being sanitized.

For tape sanitization, an email is sent to CDC.OPS.STORAGE for Corporate/TRICARE, and TAPE.LIBRARY.MED for Medicare with the identifying volume serial number (VOLSER) to be degaussed. The tape librarians will then degauss the VOLSER per the Media Disposition Process. Once the tape has been sanitized, an email containing the date that each VOLSER was degaussed is sent by the associated tape library back to TSM.ADMIN. A hard copy of the response is printed and retained for seven years.

## Release/Reuse/Resource Control

To ensure that all data storage media objects contain no residual data when reused, the BlueCross Data Center regularly erases and reformats all such objects in its Data Center Library.

# Chapter 3 Technical Support

## 3.1 Day to Day Technical Activities

### 3.1.1 Tech Support-Related Schedules

#### 3.1.1.1 CICS System Modifications

CICS system changes - Sunday.
CICS program changes and proc update - Thursday night.
Monitor use of the program for at least a week after the change has been updated.

#### 3.1.1.2 CICS System Table Process Times

Production CICS table updates - Friday (Process time 1:30 p.m.)
Validate CICS table updates - Wednesday & Friday (Process time - 1:30 p.m.)

---

**NOTE** That any table request not received by Tech Support at the stated process times will not be done that day.

---

#### 3.1.1.3 Software Modifications

- IPL - Friday 17:30 Hours
- NON IPL - Tuesday 06:00 Hours

#### 3.1.1.4 Normal Hardware Maintenance Window

- Preventive - Sunday 1700 and 2200 Hours.
- Hardware changes - Sunday 1700 and 2200 Hours.

#### 3.1.1.5 IMS/DB System Modifications

For a modification that requires a PSB or DBD gen, the Database group must be notified 24 hours in advance of the production implementation, in accordance with the following:

- All IMS/DB "SHARED" database application modifications - Tuesday night
- All IMS/DB "NON-SHARED" database application modifications will be moved into production based on the schedule listed in #1 above. The Software Developer will be notified as soon as the PSB/DBD gen is completed.
- Any non-scheduled IMS update JOB, such as a one-time fix, must be approved by the Database area in advance of execution. This includes production fixes at night. The allocation/de-allocation of the database for update purposes will be the joint responsibility of the Software Developer, System Support, and the DBA. The job stream should be set up with a de-allocate as the first job and an allocate as the job after the IMS update. If the job abends, the DBA should

be notified as to whether a rerun is to be attempted. If no rerun is attempted, the DBA will tell Operations to reallocate the database after the database restore job is completed.

## 3.1.1.6 System Software Modifications

Software modifications requiring an IPL to install will require the approval of a VP or AVP of Operations. All changes should be installed on the test system for one week, if possible, before implementing on the production system. If users will be affected by the change, notification should be made to them by Monday of the week of installation. All changes to the production system will be completed before the IPL on Sunday at 5:00 p.m.

Software modifications that do not require an IPL to install will require the approval of the Director of Operations. All changes should be installed on the test system for one week, if possible, before implementing on the production system. If users will be affected by the change, they should be notified one week in advance.

# 3.2 Monitoring Management

## 3.2.1 Enterprise Monitoring System

The Monitoring Observability and Pipeline Systems (MOPS) team has been organized to ensure the optimum uptime reliability of BlueCross BlueShield of South Carolina (BlueCross) systems. The MOPS team is responsible for the development and maintenance of the Enterprise Monitoring System, including:

- The selection of automated monitoring tools (including commercial off-the-shelf applications).
- The design and implementation of all automated monitoring systems used at BlueCross.
- The configuration of automated monitoring tools.
- The writing and maintenance of customer scripts as needed.
- The approval of manual monitoring processes as needed.

The MOPS team documents automated monitoring standards and best practices but does not itself perform application monitoring. Rather, the MOPS team develops Application Monitoring Solutions. The responsibility for using the Application Monitoring Solutions belongs to the appropriate Application Owner, the System Support Groups (SSGs), the Information Communication Technology Operations (ICT Operations) Groups, and the Technology Support Center (TSC).

The TSC, the SSGs, and the ICT Operations Groups respond to the incident tickets generated from the selected monitoring tools through the Event Management System (EVMN). The Application Owners, SSGs and ICT Operations Groups use the trending information provided by the monitoring tools' dashboards and reports.

## 3.2.2 Administration/Governance

### 3.2.2.1 Standards

The standards for the implementation of automated monitoring policies and procedures are defined by the MOPS team.

These standards include:

- All monitoring can generate tickets (optionally, emails can also be sent out).
- The area field is determined by the application being monitored and provided to the MOPS team.
- The application area or SSG is responsible for requesting scheduled downtime. Downtime shall not be handled by the monitoring tool.
- If a customer feels that a monitoring ticket was issued in error, a Service Request ticket should be opened and should include evidence of the error and the correction being requested. Pertinent information may include:

    - Application or server logs contradicting the error in the monitoring ticket.
    - Screenshots from the application or server.
    - Screenshots from the monitoring tool that generated the ticket at the time of the error.

### 3.2.2.2 Manual Monitoring Standards

If the decision is made to develop a manual monitoring solution, the MOPS team, along with the TSC, will provide assistance so that the Application Owner can develop instructions on how to monitor manually. After MOPS management approves, manual monitoring will be carried out by the TSC Incident Management Team. The MOPS team must concur on any manual monitoring procedure.

## 3.2.3 The Downtime Table

The Downtime Table is used to create closed S9 tickets for applications and devices that are undergoing maintenance. The Downtime Table is updated by the TSC using the Downtime application developed by the Event Management Team. The rules and regulations surrounding the Downtime Table are maintained by the MOPS team and ITBS System Experts and Designers.

## 3.2.4 Monitoring Tool Evaluation and Review

All reviews of new monitoring tools are conducted by the MOPS team. Decisions to purchase or replace existing monitoring tools are made by MOPS management and the Systems Architecture area.

Periodically, the MOPS team will review all of the monitoring tools within the their toolkit. They will compare tool functionality looking for overlaps and gaps. If overlaps are found, a validation process will begin to see if any of the tools can be removed from the toolkit.

## 3.2.5 Monitoring Audit Functions

Various tools within the MOPS team toolkit are used to perform audit functions throughout the year and on an ad hoc basis. The MOPS team's monitoring tools and reports can be configured to perform monitoring as needed for applications, infrastructure and meeting audit requirements.

## 3.2.6 Monitoring Tool Data Aggregation

The MOPS team's Aggregation Tool brings in data from servers, appliances, databases, monitoring applications, and other infrastructure devices. Aggregating the data into one tool offers a single pane of glass to operations, applications, and platform teams, allowing for one democratized source of data.

Basic capabilities (such as viewing existing dashboards and writing queries) are available to I/S employees and strategic business partners within other subsidiaries via access to the appropriate security group.

It is recommended that all employees who interface with the Aggregation Tool on an admin/development level complete the fundamentals training course offered by the vendor.

The capability to schedule searches, share dashboards, and alter alerts is available to our customers via the automated change implementation system linking the Aggregation Tool to GitHub Enterprise. Those with access to our internal GitHub Enterprise can implement a change by creating a Pull Request (PR) from the appropriate Branch containing their alterations. The MOPS team will then either request

changes or approve the PR as needed. Changes merged into the Production-level Branch will then appear in the Aggregation Tool.