Health and Human Services (HHS) Enterprise Systems

Operations and Maintenance Manual

Attachment 1A

Document Control Information

Document Information

Document Identification	Enterprise Operations and Maintenance Manual
Document Name	Operations and Maintenance Manual
Project Name	HHS Integrated Eligibility Systems
Client	State of Connecticut – Department of Social Services
Document Author	Bernie Evans
Document Version	1.0
Document Status	First submission
Date Released	Xx/xx/2017
File Name	Enterprise Operations and Maintenance Manual_v1.0

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised by
1.0	7/18/2018	Initial Submission built primarily from Deloitte's ImpaCT project deliverables	Bernie Evans
1.1	11/6/18	See the highlighted sections in yellow. These sections need yet to be completed.	Bernie Evans
1.2	11/6/18	Added new flow charts for incident/helpdesk support – section 5.3.	Bernie Evans
1.3	11/9/18	Incorporated addition activities and requirements in 5.1 & 5.3. Added table 3: System component ownership by agency. Updated 5.3 flowcharts.	Bernie Evans
1.4	11/19/18	Bookmarks and links: RACI Draft watermark	Bernie Evans
1.5	11/28/19	Added step for HD Support levels 2 and 3 for contacting users for system outages.	Bernie Evans

Document Review/Approval History

Date	Name	Organization/Title	Comments

Distribution of Final Document

The following people are designated recipients of the final version of this document:

Name	Organization/Title
Joe Stanford	DSS Chief Innovations Officer
Vance Dean	DSS IT Director
Saul Mora	DSS IT Manager

Table of Contents

Table of Contents **3**

1 Introduction **7**
1.1 Document Purpose 7
1.2 Scope 7
1.3 Audience 7
1.4 Document Maintenance 7

2 Key Stakeholder List and Contact Information **8**

3 Assumptions and Constraints **9**

4 References and Attachments **10**

5 Operations **11**
5.1 Systems Availability Management 11
5.1.1 Application Monitoring *RACI 12
5.1.1.1 Health Check Tool 13
5.1.2 Technical (Infrastructure) Monitoring 18
5.1.2.1 New Relic (Application performance magic (APM)) 18
5.1.2.2 Uptime 18
5.1.2.3 Foglight 20
5.1.2.4 SIM/SAM 21
5.1.2.5 Data Power 21
5.1.2.6 QRadar 21
5.1.2.7 WhatsUp (network) 21
5.1.2.8 Net Cool (network) 21
5.1.2.9 Cacti (network) 21
5.1.2.10 Wireshark (network) 21
5.1.2.11 Netflow (network) 21
5.1.2.12 Cisco Transport Manager (network) 21
5.1.2.13 Filenet System Monitor (ECM) 21
5.1.2.14 IBM Performance Tool Kit (ECM) 21
5.1.2.15 Other Infrastructure Monitoring Tools 21
5.1.2.16 Capacity Monitoring 21
5.1.3 Communications 22
5.2 Batch Management 22
5.2.1 Inventory 22
5.2.2 Schedule / Calendar 22
5.2.3 Monitoring 26
5.2.4 Manual Execution 27
5.2.5 Batch Validation and Data Correction 27
5.2.6 Reporting 27
5.2.7 Emergency Procedures 29
5.3 Incident Management / Resolution 32
5.3.1 Help Desk Incident Escalation Structure 32
5.3.2 Help Desk Ticketing Systems and Tracking 34
5.3.2.1 Incident Details 35
5.3.3 Help Desk Level 1 Support 38
5.3.3.1 HHS worker encounters an incident 38
5.3.3.2 HHS client encounters an incident 39
5.3.4 Help Desk Level 2 (HD2) App Support 40
5.3.4.1 HD1 Helpdesk contacts HD2 App Support 40
5.3.4.2 HD2 BEST Unsuccessful System Health Checks (Business Hours) 42

5.3.4.3 HD2 BEST Unsuccessful System Health Checks (After Business Hours) 44
5.3.4.4 Oper encounters an Batch incident 45
5.3.5 Help Desk Level 3 Support 46
5.3.5.1 HD3: App Hosting (Application Hosting) 46
5.3.5.2 Incident is escalated to HD3: System Integrator and/or Infrastructure 48
5.3.6 Help Desk Level 3 Support 50
5.3.6.1 Incident is escalated to Vendor SME Support (Including COTS) 50
5.3.7 Incident Escalation Contact List 51

6 Maintenance 54
6.1 Deployment Management 54
6.1.1 Release Management 55
6.1.1.1 Release Planning 55
6.1.1.2 Release Readiness 55
6.1.1.3 Emergency Releases 55
6.1.1.4 Sign-offs 55
6.1.1.5 Post Release Communications 55
6.1.2 Backup/Restore 55
6.1.2.1 Identity and Access Management (IAM) 56
6.1.2.2 IBM IHS Web Server 56
6.1.2.3 IBM WebSphere Application Server (IBM WAS) 56
6.1.2.4 Corticon Business Rules 56
6.1.2.5 FileNet 56
6.1.2.6 Adobe LiveCycle 56
6.1.2.7 PDTX DB2 Database 56
6.1.2.8 Database Backup Process 57
6.1.2.9 Database restore process: 57
6.1.2.10 Adobe LiveCycle 57
6.1.2.11 IBM FileNet P8 57
6.1.2.12 WebSphere Enterprise Service Bus (WESB) 58
6.1.2.13 IBM DataPower Appliance 58
6.1.2.14 ImpaCT Batch with CA ESP 58
6.1.2.15 Informatica PowerCenter 58
6.2 Application 58
6.2.1 Application Releases 59
6.2.1.1 Perform SIT Tests 59
6.2.1.2 Triggering a Deployment 59
6.2.1.3 Code Delivery (Deployment Packaging) 60
6.2.1.4 Change Request Fulfillment 62
6.2.1.5 Facilitate Go/Nogo Meeting for UAT Deployment 62
6.2.1.6 User Acceptance Testing 62
6.2.1.7 Performance Testing 63
6.2.1.8 Facilitate Go/Nogo for Production Deployment 65
6.2.2 Ad-hoc Reporting 65
6.2.3 Reference Table Modifications 65
6.3 Technical (Infrastructure) 65
6.3.1 Licensing 67
6.3.1.1 Software License Renewal 67
6.3.2 Software Upgrades (COTS Products) 67
6.3.2.1 Patch & Upgrade Management 67
6.3.2.2 COTS Release Planning 67
6.3.2.3 DB2 Administration 68
6.3.3 Hardware Upgrades 68
6.3.3.1 Patch & Upgrade Management 68
6.3.3.2 Infrastructure Release Planning 68
6.3.4 System Start-up and Shutdown 69
6.3.5 Data Management 70

6.3.5.1 Data Governance Planning 70
6.3.5.2 Data Refreshes 70
6.3.5.3 Definition and Maintenance 70
6.3.5.4 Data Modeling Analysis and Design 71
6.3.5.5 Detailed Data Design 71
6.3.5.6 Data Implementation 71
6.3.5.7 Database Operations Management 71
6.3.5.8 Training and Test Data Management 72
6.3.5.9 Report Data Management 72
6.3.5.10 Content Management and Audit 72
6.3.6 Disaster Recovery 73
6.3.6.1 Planning and Management 73
6.3.6.2 Backup and Recovery 73
6.3.6.3 VM Backup 73
6.3.6.4 Files 73
6.3.7 Performance Management 73
6.3.7.1 Monitoring 73
6.3.7.2 Testing 73
6.3.7.3 Tuning 73
6.4 Security / User Administration 74
6.4.1 Account Setup and Maintenance 74
6.4.1.1 Administration. 74
6.4.1.2 Coarse-Grain Role Administration 74
6.4.1.3 User Setup and Role Mapping 74
6.4.1.4 Fine-Grain Role Administration 75
6.4.2 Compliance 76
6.4.2.1 Data Security Management 76
6.4.2.2 Audit History 76
6.4.2.3 Audit Content Management 76
6.4.2.4 CMS POAMs 76
6.4.2.5 Data Retention 77

7 Maintenance and Operations Support RACI and Assignment Matrices 78
7.1 RACI 78
7.2 Support Role Assignments 98

8 Overview of the Technical Architecture 105
8.1 Identity and Access Management (IAM) 106
8.1.1 IBM Security Identity Manager (ISIM) 106
8.1.2 IBM Security Access Manager (ISAM) 107
8.1.3 IBM Web Seal Servers 107
8.2 IBM HTTP Server (IHS) 108
8.3 IBM WebSphere Application Server (IBM WAS) 109
8.4 IBM DB2 109
8.5 Corticon Business Rules 109
8.6 Adobe LiveCycle 110
8.7 IBM FileNet P8 110
8.8 SQL Server Reporting Services (SSRS) 111
8.9 WebSphere Enterprise Service Bus (WESB) 111
8.9.1 WebSphere Service Registry and Repository (WSRR) 111
8.10 DataPower Appliance 112
8.11 ImpaCT Batch 112
8.12 EMPI 113

9 List of Environments at the State Data Center 114

Table of Tables

Table 1: Key Stakeholders 8
Table 2: References and Attachments 10
Table 3: System component ownership by agency 11
Table 4: Application Monitoring Tools 12
Table 5: Incident Severity 35
Table 6: Code Development and Deployment Tools 61
Table 7: Regression Testing Tool 62
Table 8: Performance Test Types 64
Table 9: RACI 78
Table 10: Support Role Assignments 98
Table 11: Communications Load Balanced by F5 106

Table of Figures

Figure 1: Help Desk Support Structure 34
Figure 2: Incidents Generated from Workers 39
Figure 3: Incidents Generated from Clients 40
Figure 4: Incidents Generated from Unsuccessful Health Checks 44
Figure 5: Incidents Generated from Unsuccessful Health Checks After Business Hours 44
Figure 6: Incidents Generated from Batch Processes 46
Figure 7: Incident Escalation to App Host 47
Figure 8: Incident Escalation to SI (System Integrator) 49
Figure 9: Incident Escalated to Level 3 Support 51
Figure 10: Major Component Interaction Pattern 106
Figure 11: ISIM/ISAM Interaction Pattern 107

1 Introduction

1.1 Document Purpose

This Operations and Maintenance Manual will be used by State of Connecticut IT Operations and Maintenance staff as well as vendors under contract with statements of work with the State of Connecticut as a tool, to help minimize business disruption by enabling proper management of functional and technical activities during the Pre-production deployment, production, and maintenance phases of the HHS Enterprise Applications System. It contains descriptions for handling exception scenarios and incidents thereby providing an easy-to-follow set of guidelines to effectively support and maintain the HHS Enterprise Applications System solution. This manual allows the technical support staff to successfully manage, troubleshoot and restore the HHS Enterprise Applications System solution in case of an outage.

1.2 Scope

The scope of this document includes the operations and maintenance procedures utilized to support the HHS Enterprise Applications System solution in all its State hosted environments. This manual and the referenced documents are used for all the HHS Enterprise Applications System environments, currently including but not limited to UAT (suite of environments including Training), STG, PROD, PROD-SIM and the Conversion environments.

1.3 Audience

The intended audience for this document is the system administrators and support teams that will perform the operations, administration and maintenance of the HHS Enterprise Applications System. Roles defined for this support are listed below. These groups are staffed by State personnel and vendors that have contracts or statements of work that reference the duties in this manual.
There are bookmarks for sections 5 and 6 that look like this - **%**. Click on them to proceed directly to the RACI chart for this Maintenance or Operations function.

1.4 Document Maintenance

This document is a consolidation of many deliverables and documents that were developed through the early stages of the HHS Enterprise Applications projects. Expectations are that this document will continue to be updated as future projects are added, components are upgraded, and new technologies get applied. However, if the support teams and/or personnel change and the definition and separation of duties and tasks do not, the only modifications that should be needed would be section **7.2** Support Role Assignments.

2 Key Stakeholder List and Contact Information

Table 1: Key Stakeholders

Name	Organization/Title
Joe Stanford	DSS CIO (Lead Approver)
Eric Lindquist	DAS/BEST CTO
Vance Dean	DSS Director (ITS) and the DSS CIO
Saul Mora	DSS IT Manager and Technical Lead

3 Assumptions and Constraints

1. It's an assumption that STG and PRD environments are as identical in infrastructure as possible as far as configuration and capacity. UAT must be the same when comparing system and software configurations but not regarding capacity.

2. It is assumed that the State of Connecticut IT administrators and approved designated vendors maintaining the application will have the necessary skill set and knowledge to apply the maintenance strategies and techniques discussed in this document.

3. Product Installation refers to the installation of the HHS Enterprise Applications System which includes ImpaCT, ConneCT, BIP, and AHCT.

4. State of Connecticut IT has obtained snapshots during installation of the components to be kept as future documentation

5. State of Connecticut IT administrators and approved designated vendors have full responsibility for all the servers that make up the ImpaCT infrastructure including but not limited to Web Seals, IHS, IBM WAS, DB2, Corticon, Adobe LiveCycle, WESB, and EMPI servers

6. All referenced documents will be made available via a central library available to all approved support personnel. Currently, it is this folder: MIS-Sharedfiles:\ITS-Managers\IT HHS

7. ECM team monitors the availability of the FileNet Content Engine Service, Workplace XT, and Content Navigator.

4 References and Attachments

Following is the list of documentation referenced in this deliverable:

Table 2: References and Attachments

Name	Description	Link
ImpaCT Batch Jobs	Schedule with predecessors and successors of each job, the frequencies, and job descriptions	**ImpaCT Batch Jobs.mpp**
ImpaCT Batch Jobs Run Sequence	Chart of batch jobs, execution order, and relationships.	**Batch Jobs run sequence.pdf**

5 Operations

5.1 Systems Availability Management

The availability of the HHS Enterprise Applications System is primarily monitored via software tools and custom monitoring scripts to confirm the availability of the application and its infrastructure components. In addition, the applications are also monitored through manual health checks and reviews of alerts and logs.

The availability of the HHS Enterprise Applications System is addressed through four key areas:

1) Application Monitoring – this includes the monitoring of the HHS Enterprise Applications at a component level.
2) Infrastructure Monitoring – this includes monitoring the java virtual machines, CPU, memory utilization, and other aspects of the infrastructure that hosts the applications.
3) Communication – this includes the escalations and communication process when abnormalities are identified as part of the monitoring processes.
4) Performance Management – this includes managing the performance standards of the application components and conducting infrastructure performance tuning activities that need to be undertaken based on performance analysis conducted and identifying performance issues

Table 3: System component ownership by agency

Responsible Team	Systems Components (AHCT, ImpaCT, BIP, ConneCT)				
AHCT/DSS	App Servers	Corticon Servers	WSRR	Managed File Transfer (MFT)	Enterprise Service Bus (ESB)
	Web Servers	Informatica	Multi-Factor Authentication (MFA)	Batch Servers	Operating Systems
	Database Servers	AHCT DW MS SQL Server	External Load Balancer (formally Akamai)	Application Monitoring	
BEST	SIM/SAM Infrastructure	Networks	VPN	Enterprise SFTP	Load Balancing (F5)
	SIM/SAM Identity Mgmt.	Firewalls	eDir / AD	Security Monitoring	DataPower
	Platform Services - Servers	FileNet Document Mgmt.	Unified Communications	Batch Operations	
	Platform Services - Storage	Disaster Recovery	Exchange/Outlook		

5.1.1 Application Monitoring %

To monitor the availability of the HHS Enterprise Applications, New Relic, a custom application that is named 'ImpaCT Health Check Tool', as well as database queries are executed to confirm the application components are available and performing as planned. The table below highlights the components of the system that are checked, the tool used to check their availability, the frequency in which that check is executed, and the corresponding notifications for that check.

Table 4: Application Monitoring Tools

S No	Component(s)	Process / Tool	Frequency of Monitoring	Type	Notification
1	ImpaCT Online Application, Web Services, Message Queues and Database Connectivity.	**Process:** The availability of these components are checked, results are included via email. **Tool:** ImpaCT Health Check Tool	Every 15 minutes	Automated	An email is sent to App Host & SI support teams Distribution list.
2	Web Application Server Thread Pool	**Process:** Thread pool activity is captured and included in the email notification. **Tool:** ImpaCT Health Check Tool	Every 5 Minutes	Automated	An email is sent to App Host & SI support teams Distribution list.
3	Performance Monitoring of various modules	**Process:** Database queries are executed to capture transaction timing of various modules and system actions. **Tool:** Database Query	Daily	Semi-Automated	The command center report includes the timings captured. This data is analyzed for any anomalies.
4	Average Response time, JVM heap size and garbage	**Process:** New Relic monitors response times and will send an automated alert if the response exceeds the following.	Real Time	Automated	Email notification sent to App Host & SI support teams Distribution list.

	collection Monitoring	• Web Response time >20 sec • Heap Size >90% • Garbage Collection CPU Usage >5% **Tool:** New Relic			

5.1.1.1 *Health Check Tool*

The ImpaCT Health Check tool is a small java program executed in Bamboo on the Bamboo server(s). Standard Software Development Life Cycle (SDLC) processes are used to develop and test it through the normal SDLC process. After successful testing, this tool is migrated to State Staging, Training and Production environments.

The health check tool is used to assess the health and availability of the ImpaCT application at this time. These checks are conducted in the following areas:

- Application Health & Web Service Availability – (#1 in the above table) checks are executed every 15 minutes with automated results sent via email.
- Hung Thread report – (#2 in the above table) provides an export of the hung threads identified in the WebSphere Application server.

Each of the above is described in more detail in the following sections.

5.1.1.1.1 Application Health & Web Service

The Health Check Tool assess the availability of the application in the following areas:

- Application / Web Service URLs
- Database connectivity
- Service Integration Bus Queues / Destinations
- Disk Space & Network Drive Connectivity

Application / Web Service URLs

The following 11 Services are included in the check.

1. PROD DASHBOARD: This is the ImpaCT landing page which gives access to the ImpaCT and ahCT WP.
2. PROD CaseManagement: This is a web service which is invoked from ahCT and ConneCT portals to create and retrieve cases in ImpaCT system.
3. PROD SOLQService: This is a web service which is invoked from ahCT application for SSN verification.

4. PROD AddressValidation: This is a web service to validate the user entered addresses.
5. PROD HPEVS: This is a web service which is invoked during online MMIS transactions.
6. PROD WESB: This covers all the web services hosted on the ImpaCT WESB. This covers all the services hosted on the AppTarget cluster of ImpaCT WESB.
7. PROD MPI: This covers the EMPI services hosted on the EMPI cluster of ImpaCT WESB.
8. PROD OPMService: This web service is used by Office Policy Management team.
9. PROD EDRS: This web service is used to invoke EDRS external verification.
10. PROD Correspondence: This covers all the Adobe related web services used to generate correspondence.
11. PROD Axis: This covers all the Corticon related web services which is used during Eligibility Determination

Sample Output

Component	Server	URL	Status
PROD Dashboard	Webserver1	NA	UP
PROD Dashboard	Webserver2	NA	UP
PROD Dashboard	JVM-A	NA	UP
PROD Dashboard	JVM-B	NA	UP
PROD CaseManagement	Webserver1	NA	UP
PROD CaseManagement	Webserver2	NA	UP
PROD CaseManagement	JVM-A	NA	UP
PROD CaseManagement	JVM-A2	NA	UP
PROD CaseManagement	JVM-B	NA	UP
PROD CaseManagement	JVM-B2	NA	UP
PROD CaseManagement	JVM-C	NA	UP
PROD CaseManagement	JVM-C2	NA	UP
PROD CaseManagement	JVM-D	NA	UP
PROD CaseManagement	JVM-D2	NA	UP
PROD SOLQService	Webserver1	NA	UP
PROD SOLQService	Webserver2	NA	UP
PROD SOLQService	JVM-A	NA	UP
PROD SOLQService	JVM-A2	NA	UP
PROD SOLQService	JVM-B	NA	UP
PROD SOLQService	JVM-B2	NA	UP
PROD SOLQService	JVM-C	NA	UP
PROD SOLQService	JVM-C2	NA	UP
PROD SOLQService	JVM-D	NA	UP
PROD SOLQService	JVM-D2	NA	UP

PROD AddressValidation	WESB-A	NA	UP
PROD AddressValidation	WESB-B	NA	UP
PROD AddressValidation	WESB-F5	NA	UP
PROD HPEVS	WESB-A	NA	UP
PROD HPEVS	WESB-B	NA	UP
PROD HPEVS	WESB-F5	NA	UP
PROD WESB	EMPI-A	NA	UP
PROD WESB	EMPI-B	NA	UP
PROD WESB	EMPI-F5	NA	UP
PROD MPI	WESB-A	NA	UP
PROD MPI	WESB-B	NA	UP
PROD OPMService	WESB-A	NA	UP
PROD OPMService	WESB-B	NA	UP
PROD OPMService	WESB-F5	NA	UP
PROD EDRS	WESB-A	NA	UP
PROD EDRS	WESB-B	NA	UP
PROD EDRS	WESB-F5	NA	UP
PROD Correspondence	Adobe-A	NA	UP
PROD Correspondence	Adobe-B	NA	UP
PROD Correspondence	Adobe-C	NA	UP
PROD Correspondence	Adobe-F5	NA	UP
PROD Axis	Corticon-A	NA	UP
PROD Axis	Corticon-B	NA	UP
PROD Axis	Corticon-C	NA	UP
PROD Axis	Corticon-A2	NA	UP
PROD Axis	Corticon-B2	NA	UP
PROD Axis	Corticon-C2	NA	UP
PROD Axis	Corticon-F5	NA	UP

Database Connectivity

PROD ImpaCT DB: This covers the database availability by pinging the databases servers.

DB Component	Database Server	Database Name	Status
PROD ImpaCT DB1	NA	NA	UP
PROD ImpaCT DB1	NA	NA	UP
PROD ImpaCT DB1	NA	NA	UP
PROD ImpaCT DB2	NA	NA	UP
PROD ImpaCT DB2	NA	NA	UP
PROD ImpaCT DB2	NA	NA	UP

Service Integration Bus Queues / Destinations

Following are the service integration components that are monitored

1. PROD ADOBE SIBUS: This covers the queues on Adobe servers to generate XMLs for notice generation.
2. PROD AppServer SIBUS: This covers the queues created on WebSphere application servers to facilitate XMLs for notice generation.
3. PROD WESB AuditLog: This covers the availability of the audit log queue on ImpaCT WESB to facilitate WESB audit logging.
4. PROD WESB CaseManagementQueue: This covers the availability of the Case Management queues on ImpaCT WESB servers to facilitate the data transfer from ahCT.

Listed below is the sample output.

Component	DestinationQueue	SI Bus	HostName	Status
PROD ADOBEA SIBUSA	Dest_A	Correspondence_BusA	NA	UP
PROD ADOBEB SIBUSB	Dest_B	Correspondence_BusB	NA	UP
PROD ADOBEC SIBUSC	Dest_C	Correspondence_BusC	NA	UP
PROD AppServerA SIBUSA	Correspondence_D	Correspondence_ReadBus	NA	UP
PROD AppServerB SIBUSB	Correspondence_D	Correspondence_ReadBus	NA	UP
PROD AppServerC SIBUSA	Correspondence_D	Correspondence_ReadBus	NA	UP
PROD AppServerD SIBUSB	Correspondence_D	Correspondence_ReadBus	NA	UP
PROD WESBA AuditLogN1	AuditLogQueue	Audit_Log_Bus	NA	UP
PROD WESBB AuditLogN2	AuditLogQueue	Audit_Log_Bus	NA	UP
PROD WESBA CaseManagementQueueN1	CaseManagementQueue	ImpaCT_WESB_Bus	NA	UP
PROD WESBB CaseManagementQueueN2	CaseManagementQueue	ImpaCT_WESB_Bus	NA	UP

Disk Space & Network Drive Connectivity

DISK space is checked for 90% of available space. If space is less than 90% Status will be marked as RED. Following are the various drives that are monitored

1. PROD_ApplicationServer EDrive : This ensures the availability of disk space and network drive connectivity on the VMs that hosted the ImpaCT Application Servers.
2. PROD_Corticon EDrive : This ensures the availability of disk space and network drive connectivity on the VMs that hosted the ImpaCT Corticon Servers.
3. PROD_Adobe EDrive: This ensures the availability of disk space and network drive connectivity on the VMs that hosted the ImpaCT Adobe Servers.

4. PROD_ESB EDrive: This ensures the availability of disk space and network drive connectivity on the VMs that hosted the ImpaCT WESB Servers.

Listed below is the sample output for disk space

Component	Server	Status
PROD_ApplicationServerC EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_ApplicationServerD EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_ApplicationServerE EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_ApplicationServerF EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_CorticonA EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_CorticonB EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_CorticonC EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_AdobeA EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_AdobeB EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_AdobeC EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_ESBA EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_ESBB EDrive	NA	DISK SPACE HEALTHY ON edrive
PROD_NAS EDrive	NA	DISK SPACE HEALTHY ON edrive

5.1.1.1.2 Hung Thread Report

Hung threads health check tool scans the Web Sphere application server for every 5 minutes for hung threads and following details are captured if there are any hung threads

1) Date and timestamp
2) Thread Count and
3) Description of hung thread

Example – [6/2/17 10:08:53:455 EDT] 00000004 ThreadMonitor W WSVR0605W: Thread "WebContainer : 10" (00000040) has been active for 762049 milliseconds and may be hung. There is/are 7 thread(s) in total in the server that may be hung.

ImpaCT Online Application, Web Services, Message Queues and Database Connectivity.	App Host	PMO IT	SI
Web Application Server Thread Pool	App Host	PMO IT	SI
Performance Monitoring of various modules	DB	PMO IT	SI
Average Response time, JVM heap size and garbage collection Monitoring	App Host	PMO IT	SI

5.1.2 Technical (Infrastructure) Monitoring %

Technical system health checks and monitoring must be performed on core infrastructure components, including network, storage components, operating systems, hardware components, database usage, etc. This includes COTS components.

The primary technical monitoring support team will be responsible for coordinating and reporting the status and findings of all other monitoring teams.

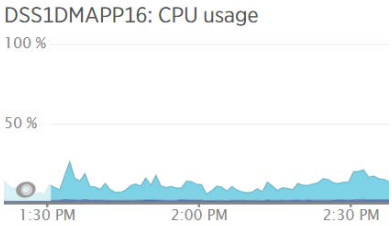
Below are details for the monitoring tools

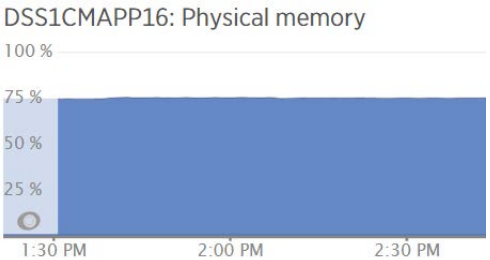
5.1.2.1 New Relic (Application performance magic (APM))

The following are the custom dashboards created in New Relic to check the real time resource CPU, Memory and Disk Space utilization for all VM's for ImpaCT application.

PRD_ImpaCT_VM Dashboard

This dashboard will help administrators to check the CPU and Memory utilization of ImpaCT VMs.





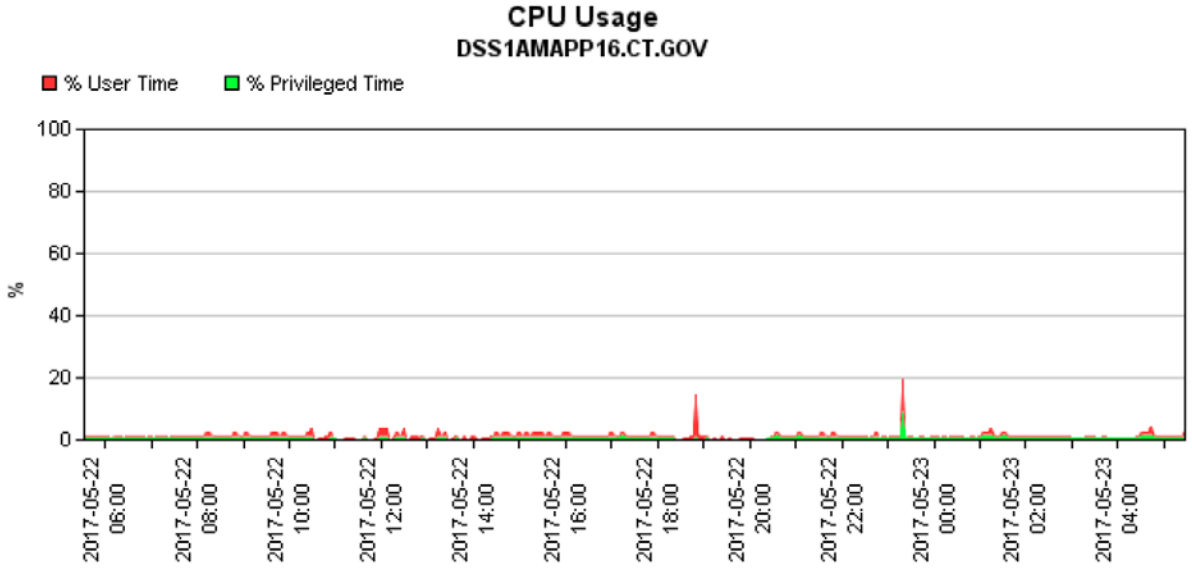
Separate custom dashboards are created for Corticon, Adobe, Batch and WESB servers.

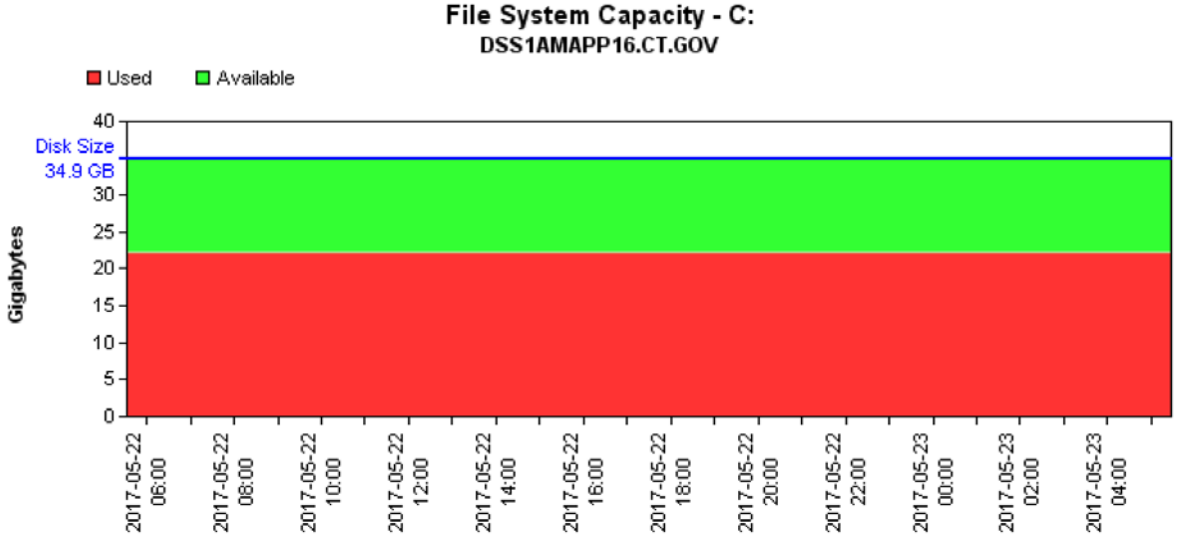
5.1.2.2 Uptime

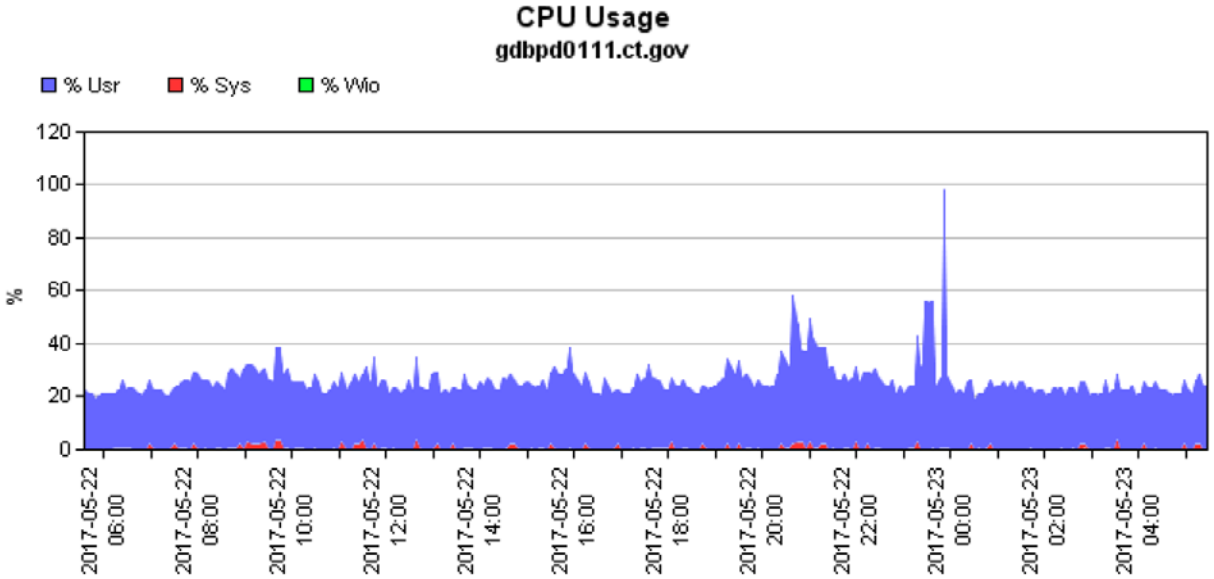
Uptime is configured to monitor resource utilization across ImpaCT servers. The following reports are published through uptime.

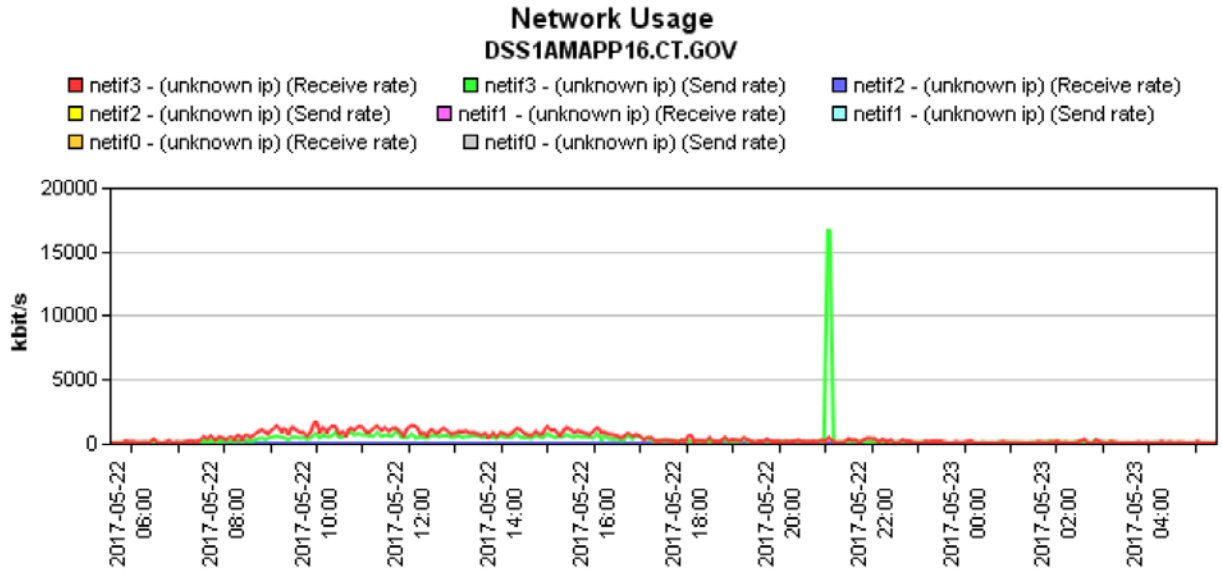
1) CPU, Memory and Disk Usage
2) Database Cluster and
3) Network Usage

Uptime tool is scheduled to run every day at 5:30 am reports above metrics for last 24 hours period. These reports are sent to key stake holders. Sample reports from Uptime are documented below.


CPU Usage
DSS1AMAPP16.CT.GOV
% User Time
% Privileged Time
%
100
80
60
40
20
0
2017-05-22 06:00
2017-05-22 08:00
2017-05-22 10:00
2017-05-22 12:00
2017-05-22 14:00
2017-05-22 16:00
2017-05-22 18:00
2017-05-22 20:00
2017-05-22 22:00
2017-05-23 00:00
2017-05-23 02:00
2017-05-23 04:00


File System Capacity - C:
DSS1AMAPP16.CT.GOV
Used
Available
Disk Size
34.9 GB
Gigabytes
40
30
25
20
15
10
5
0
2017-05-22 06:00
2017-05-22 08:00
2017-05-22 10:00
2017-05-22 12:00
2017-05-22 14:00
2017-05-22 16:00
2017-05-22 18:00
2017-05-22 20:00
2017-05-22 22:00
2017-05-23 00:00
2017-05-23 02:00
2017-05-23 04:00





5.1.2.3 Foglight

Monitors database performance during run time. This tool is used to perform database health checks periodically during online and batch processing. In scope are the DB2 databases that support the HHS Enterprise applications with DB2 as their OLTP as well as Ad-Hoc, Adobe, and ESB, excluding Filenet and SQL/Server databases.

5.1.2.4 SIM/SAM

Monitor system access through the SIM/SAM Identity Management system. Monitor all activities, IAM federation policies, onboarding and de-provision, as well as existing Novell eDirectory and Microsoft Active Directory integrations. Provide troubleshooting and root cause analysis support for incidents involving this hardware and software.

5.1.2.5 Data Power

Monitor external web services connectivity and functionality across the HHS enterprise. Assist with project technical designs. Provide troubleshooting and root cause analysis support for incidents involving this hardware and software.

5.1.2.6 QRadar

Monitor the log entries for errors, and anomalies. Contact State of CT to escalate issues.

5.1.2.7 WhatsUp (network)

5.1.2.8 Net Cool (network)

5.1.2.9 Cacti (network)

5.1.2.10 Wireshark (network)

5.1.2.11 Netflow (network)

5.1.2.12 Cisco Transport Manager (network)

5.1.2.13 Filenet System Monitor (ECM)

5.1.2.14 IBM Performance Tool Kit (ECM)

5.1.2.15 Other Infrastructure Monitoring Tools

The following Infrastructure tools are used by State or Contracted support resources for real-time monitoring and analysis of the production infrastructure.

- **DataPower Appliance** has its own monitoring tool used by the SIM/SAM team. For information on the DataPower O&M activities, refer to “OM-DataPower_v1.docx”.
- **IBM FileNet** P8 Monitoring is used for FileNet system status. ECM team monitors the availability of the Content Engine Service, Workplace XT, and Content Navigator.

5.1.2.16 Capacity Monitoring

Capacity monitoring activities that need to be conducted as per need based on performance baselines defined

- Server memory and CPU status
- Database I/O and tablespace

5.1.3 Communications %

Reporting on status and monitoring metrics must be provided twice weekly for the leadership meetings where the teams to review overall system health and assess any need for additional capacity or other system modifications for the HHS Enterprise Applications system. Coordinate and consolidate information and metrics from all of the monitoring teams.

Please see section 5.3.7 Incident Escalation Contact List

All critical and high severity alerts, failures, threshold and/or security breaches must initiate the Incident Management procedures in section 5.3 of this manual.

5.2 Batch Management

5.2.1 Inventory %

The batch inventory is maintained via a Microsoft Project file posted on Sharepoint. The project file highlights the predecessors and successors of each job, the frequencies, and job descriptions. The sequencing of the batch jobs is also included via a visio diagram.

Document Names:

- ImpaCT Batch Jobs.mpp
  - **ImpaCT Batch Jobs.mpp**
- Batch Jobs run sequence.vsdx
  - **Batch Jobs run sequence.pdf**

5.2.2 Schedule / Calendar %

The HHS Enterprise Applications system is supported by daily, weekly, monthly, quarterly, yearly, and on-demand batch jobs executed based on defined schedule. The HHS Enterprise batches are planned and scheduled using the following key components:

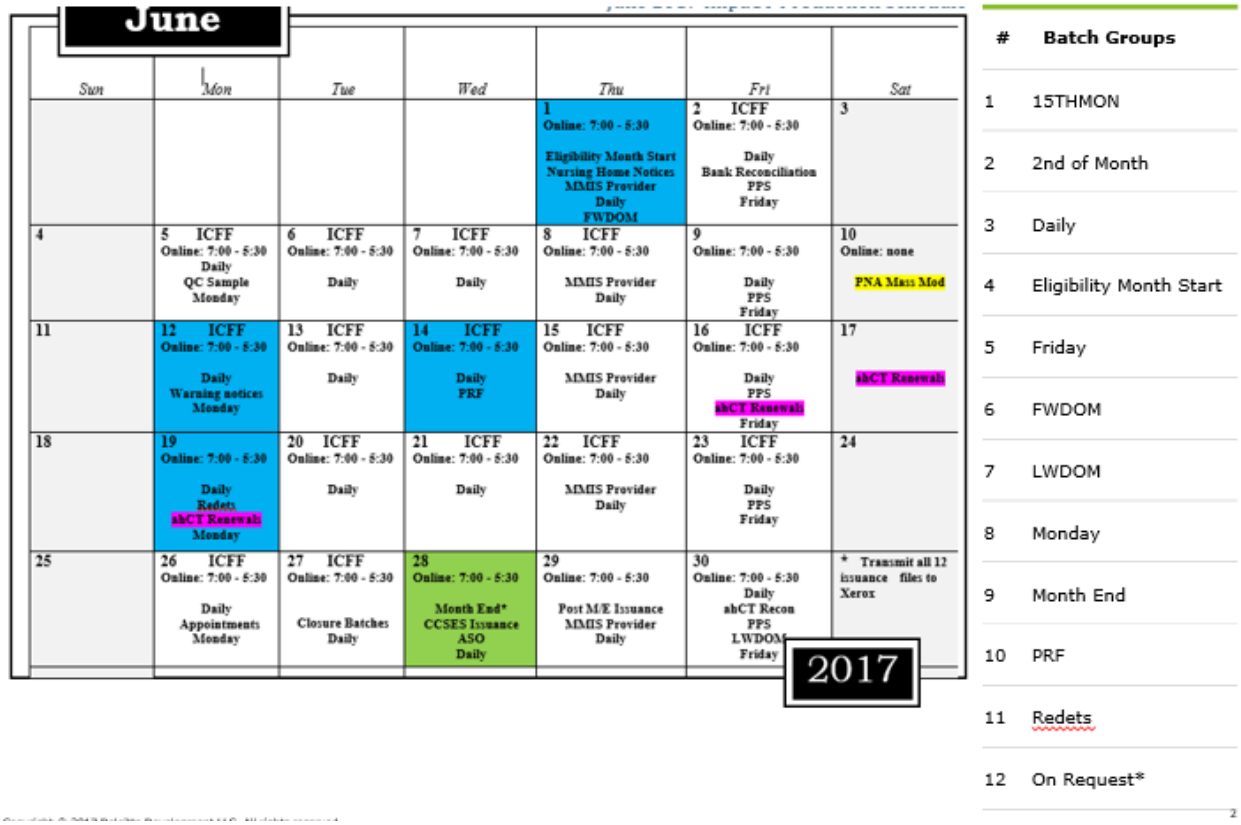
- Calendar – is a planning document jointly created with the inputs of SME, Oper, and the SI teams. The calendar identifies the group of batches planned for a particular day of the week. This is the primary input in creating the batch schedule.
- Schedule – is the executable configuration of the detailed batches, defined within the CA ESP scheduler. This reflects the planning calendar for batch execution.

The steps below outline the process to prepare the batch calendar for the upcoming calendar year.

#	Step	Description	Outcome	Date

1	Yearly Batch Planning Meeting	Each December a planning meeting will be conducted to set the key dates for the upcoming calendar year. EMS calendar should be available as a dependency.	Proposed batch calendar for the upcoming year.	1st week of December
2	Approval of Calendar	Following the distribution of the calendar – key stakeholders will have 5 business days to review and approve the calendar.	Calendar is approved and ready for the schedule to be built in CA ESP	2nd week of December
3	Creation of Batch Calendar in CA ESP	The approved calendar will be loaded into CA ESP by cross referencing the batch job groups (listed on the calendar) with the individual batch jobs listed in the batch inventory (.mpp)	The calendar year schedule will be loaded	3rd week of December

The figure below is a sample of the batch calendar (created as part of step #1 and approved in step #2). The batch groups listed on the right reflect the groups listed within the batch inventory. This reference supports the changes to specific batches required in CA ESP.



June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 Online: 7:00 - 5:30 Eligibility Month Start Nursing Home Notices MMIS Provider Daily FWDOM	2 ICFF Online: 7:00 - 5:30 Daily Bank Reconciliation PPS Friday	3
4	5 ICFF Online: 7:00 - 5:30 Daily QC Sample Monday	6 ICFF Online: 7:00 - 5:30 Daily	7 ICFF Online: 7:00 - 5:30 Daily	8 ICFF Online: 7:00 - 5:30 MMIS Provider Daily	9 Online: 7:00 - 5:30 Daily PPS Friday	10 Online: none PNA Mass Mod
11	12 ICFF Online: 7:00 - 5:30 Daily Warning notices Monday	13 ICFF Online: 7:00 - 5:30 Daily	14 ICFF Online: 7:00 - 5:30 Daily PRF	15 ICFF Online: 7:00 - 5:30 MMIS Provider Daily	16 ICFF Online: 7:00 - 5:30 Daily PPS abCT Renewals Friday	17 abCT Renewals
18	19 Online: 7:00 - 5:30 Daily Redets abCT Renewals Monday	20 ICFF Online: 7:00 - 5:30 Daily	21 ICFF Online: 7:00 - 5:30 Daily	22 ICFF Online: 7:00 - 5:30 MMIS Provider Daily	23 ICFF Online: 7:00 - 5:30 Daily PPS Friday	24
25	26 ICFF Online: 7:00 - 5:30 Daily Appointments Monday	27 ICFF Online: 7:00 - 5:30 Closure Batches Daily	28 Online: 7:00 - 5:30 Month End* CCSES Issuance ASO Daily	29 Online: 7:00 - 5:30 Post M/E Issuance MMIS Provider Daily	30 Online: 7:00 - 5:30 Daily abCT Recon PPS LWDOM Friday	* Transmit all 12 issuance files to Xerox

2017

#	Batch Groups
1	15THMON
2	2nd of Month
3	Daily
4	Eligibility Month Start
5	Friday
6	FWDOM
7	LWDOM
8	Monday
9	Month End
10	PRF
11	Redets
12	On Request*

Once the calendar has been approved, as part of Step 2, the schedule within CA ESP will be built for the upcoming calendar year. To facilitate this process, the previous year's schedule (in this example, 2017) will be carried forward to 2018. Modifications to the schedule will be facilitated via a single RFS including the schedule changes for impacted batch groups for 2018. The table below outlines the process for each batch group for the RFS to update the CA ESP schedule.

#	Batch Group	RFS for 2018

1	15THMON	Not needed, carried over from 2017 *if the 15th of the month falls on a Sunday, it will be automatically moved to the next business day
2	2nd of Month	Not needed, carried over from 2017 *if the 2nd of the month falls on a Sunday, it will be automatically moved to the next business day
3	Daily	Not needed, carried over from 2017 *is loaded for M-F (with exceptions)
4	Eligibility Month Start	Not needed, carried over from 2017 *based on the 1st of the month, if the 1st of the month falls on a Sunday, it will be automatically moved to the next business day
5	Friday	Not needed, carried over from 2017 *is loaded for each F (with exceptions)
6	FWDOM (First work day of the month)	Not needed, carried over from 2017 *Moves based on working days listed in the scheduler
7	LWDOM (Last work day of the month)	Not needed, carried over from 2017 *Moves based on working days listed in the scheduler
8	Monday	Not needed, carried over from 2017 *is loaded for each M (with exceptions)
9	Month End	RFS for the calendar year (2018) That includes the 12 dates for each month for 2018

10	PRF	Included in yearly RFS That includes the 12 dates for each month for 2018
11	Redets	That includes the 12 dates for each month for 2018
12	On Request*	Included in yearly RFS
*******		For the yearly RFS include the no-run dates.

If the calendar needs to be modified during the calendar year, the process outlined above will be repeated for calendar updated.

1. Updates to the calendar will be reviewed by DSS, Oper, and SI.
2. Updated calendar will be approved.
3. An RFS will be submitted to update the CA ESP scheduler to reflect the updated calendar.

Changes to the batch schedule needs an approval from DSS Technology and Business leadership. The approved request is sent to the Oper team for implementation before 7 hours of execution. Details for manual executions are listed as part of section 5.2.4.

5.2.3 Monitoring %

State IT operations will monitor daily executions of the batch cycle.

The procedures are dependent upon the priority of the batch job. Priority A jobs require an immediate response, while Priority B jobs wait until business hours on the following day

Priority A: Critical batch jobs which will impact Individual's benefits, targeted for completion prior to the start of the next business day.
Priority B: Non-Critical batch jobs which are required for business operation, issues identified will be reported and triaged the next day.

First contact of a Priority A failure will be defined within the Oper SOP for Batch execution. The SOP is maintained outside of this document to reflect the current contact information of the "on call" resources.

Everyday, Batch Jobs are run in a sequence define in the Batch Scheduler, as described in 5.2.2 Batch Management Schedule/Calendar. If any Batch Job aborts (fails), State IT batch operation support team is alerted by the Batch scheduler (CA ESP). This team acts as Level 1 (**HD1**)support attempting to triage the issue; and calls L2 support if needed. The State IT Batch Operations (**Oper**) unit follows the Incident Management process described in section 5.3 Incident Management / Resolution when batch failures occur.

5.2.4 Manual Execution %

If DSS or the SI identifies a batch job that needs to be executed out of the regular schedule, it will follow the below process.

- A formal approval request is sent to DSS Technology and Business. When approved, an RFS is created for **Oper** support for schedule changes. The **Oper** team will perform the requested changes and batch monitoring procedures will validate the results for the added job.

- If a job that needs to be executed out of schedule is identified within 7 hours before its execution, DSS Technology and Business POC are reached out via phone/text for approval. Once approved, the **SI** operations team reaches to the help desk **HD1** to create the Footprints ticket (RFS) requesting **Oper** support. The **Oper** team executes the batch according to the ticket details..

5.2.5 Batch Validation and Data Correction %

A log must be kept showing the activities that were performed for each batch cycle. Details of any exceptions must be documented and the Incident Management (section 5.3) steps must be followed for all incidents.

5.2.6 Reporting %

Batch reports are generated on daily basis that include total number of batch jobs executed, job execution times, batch begin and end time, batch job status, processing status, batch job summary, incident details, business impact, root cause analysis and next steps for resolving the issue faced.

Issues identified are tracked by creating an incident according to the following section (5.2.7 of this manual) which includes following details,

1. Summary: <Date> <Batch Name> <Summary of the issue>
2. Description:
    a. Batch affected
    b. Batch Run Date
    c. TOA affected
    d. # of cases, clients or EDGs affected
    e. Summary of the issue
    f. Accurate Description of the issue

Batch incidents created for a known issue is triaged and marked as “Triage Complete” the same night. For new issues, triaging of the incident is tried to be complete on the same night. If not possible, the expectation is that the team will try to complete it by the next business day. The following information should be accurately updated:

- Incident category
- Root cause of the issue
- List of all of the client IDs, Cases or EDGs affected should be attached to the JIRA ticket as a spreadsheet. Will not attach PII data like SSN or to the JIRA

Jobs that impacts a third party’s (Trading Partner) business will be reported immediately, followed by issue triaging/resolution.

Please find sample daily batch report below.

Production Batch Cycle (05/15/2017) Summary					
Batch Cycle Start Time (MM/DD/YYYY HH:MM)	**Batch Cycle End Time** (MM/DD/YYYY HH:MM)	**Batch Cycle Time** (HH:MM:SS)	**DCR Execution & Validation Time** (HH:MM:SS)	**Total Batch Cycle Time** (HH:MM:SS)	**Benefit Amount Issued**
05/15/2017 18:00	05/15/2017 23:40	2:52:00*	2:48:00	5:40:00	$96,635.92
Number of jobs completed successfully			**Number of jobs abended**		
325			1		
Abended batch jobs Summary			**Remarks**		**JIRA #**
IN-CMIR-DLY-FT Corrections Match Daily (ICD-31) - File Transfer			Details provided below		CTIE-67930

*Execution of certain time-based batch jobs are not considered as part of the batch cycle time. (e.g. SVES job executes at 4 pm. Interim conversion jobs run from 2 am onwards). These are run on specific times due to external dependencies.

Command Center Report Batch Summary	
Track	**Affected Processes/Activities**
Benefit Issuance	No issues
Interfaces	No issues
Eligibility	No issues
Correspondence	No issues
Reports	No issues
ahCT integration	**JIRA ID:** CTIE-67637 **Job ID:** ST-AHCTBM-DLY **Number of records failed:** 2 **Business Impact**: The business impact is that worker has to process these transactions manually. **Work around/Resolution**: For these transactions, the automation batch process created a PDF and an eligibility task. The tasks need to be manually worked on by workers.
Task Management	No issues
Interim Conversion	Interim conversion batch jobs cancelled due to delay in ahCT data extract.

JOB GROUP	JOB ID	DESCRIPTION	STATUS	START TIME	END TIME	RUN TIME	TOTAL INPUT RECORDS	RECORDS PROCESSED SUCCESSFULLY	RECORDS NOT PROCESSED (ACTION REQUIRED/ FAILED)	RECORDS NOT PROCESSED (NO ACTION REQUIRED)
Interfaces	IN-QURTS-DLY	40 Quarters	Complete	05/15/2017 16:00:11	05/15/2017 16:00:19	00:00:07	12	12	0	0
Correspondence	CO-START-JOB	Correspondence start job	Complete	05/15/2017 16:00:11	05/15/2017 16:06:25	00:06:14	1	1	0	0
Interfaces	IN-SVES-DLY	svessupport(ICD-06) - creates a send file	Complete	05/15/2017 16:00:32	05/15/2017 16:01:50	00:01:18	372	372	0	0
Interfaces	IN-SVES-DLY-FT	svessupport(ICD-06) - File Transfer	Complete	05/15/2017 16:20:08	05/15/2017 16:20:11	00:00:03	N/A	N/A	N/A	N/A
Framework	FW-BATST-EOC	Changes application to batch mode (read only)	Complete	05/15/2017 17:40:09	05/15/2017 17:40:09	00:00:00	0	0	0	0
Reports	RP-REP-501-DLY	IE-RP-REP-501_FM Batch Validation Report - Daily	Complete	05/15/2017 17:40:24	05/15/2017 17:42:38	00:02:13	N/A	N/A	N/A	N/A
Task Management	TM-SOPR-DLY	Scan optics File transfer batch	Complete	05/15/2017 18:00:11	05/15/2017 18:10:44	00:10:33	N/A	N/A	N/A	N/A
Task Management	TM-SODJ-DLY	Scan optics Processing batch	Complete	05/15/2017 18:11:01	05/15/2017 18:21:29	00:10:27	732	732	0	0
Task Management	TM-SOFT-DLY	Scan Optics Connect files transfer	Complete	05/15/2017 18:21:44	05/15/2017 18:29:04	00:07:19	N/A	N/A	N/A	N/A
Office Management	MO-UTAEP-DLY	Employee transfer (after 352)	Complete	05/15/2017 18:27:06	05/15/2017 18:27:09	00:00:03	8	8	0	0
Application Registration	AR-ARENS-DLY	Cancel not returned applications	Complete	05/15/2017 18:27:07	05/15/2017 18:27:09	00:00:02	0	0	0	0
Benefit Issuance	BI-DCCAU-DLY	Daily DC Cases Address update	Complete	05/15/2017 18:27:08	05/15/2017 18:27:51	00:00:42	688	688	0	0

5.2.7 Emergency Procedures %

Batch jobs are categorized as Priority A or Priority B batch jobs. The restart/rescheduling logic varies based on batch job priority.

Priority A batch jobs have business implications if not handled in the same batch cycle. If priority A batch jobs fail, the batch cycle stops on the thread. Thereafter following steps are followed:

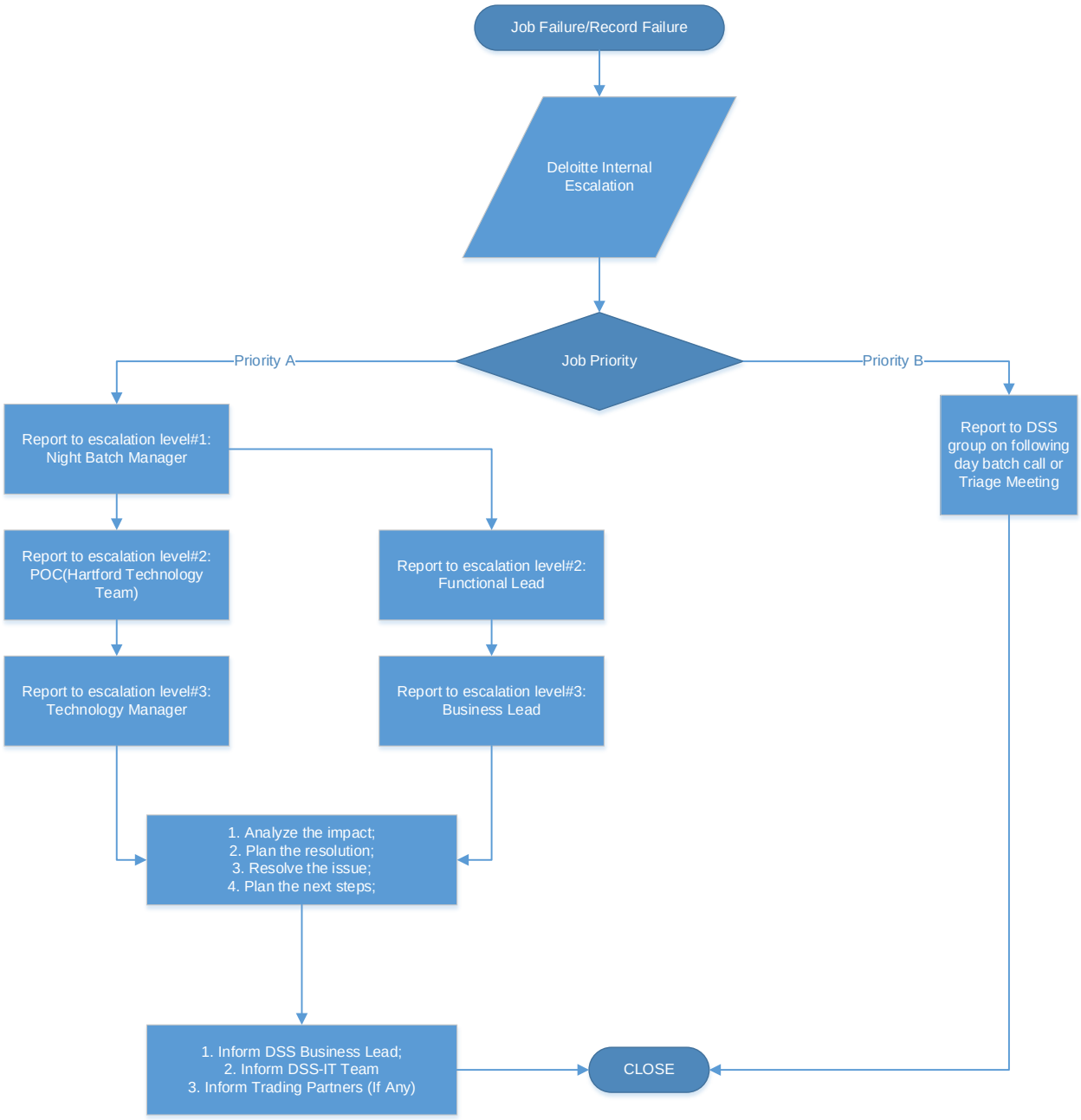
1) Batch Operations **Oper** support team calls the SI batch lead about the failure.
    a. The Batch Operations **Oper** support team will enter the incident into Footprints prior to or shortly after the call to the **SI** batch lead
    b. The **SI** batch lead will enter the incident ticket into any other required tracking systems during or immediately after this call.
2) **SI** batch lead work with Batch Operations **Oper** support team to analyze the reason for failure
3) Based on the analysis, a proposed resolution would be mutually agreed. The resolution can be accomplished in multiple steps if necessary. The immediate need is to successfully complete the job. This may include a Data Correction Script (DCR) to clean up any data issues and then modifications to the Batch job to correct any errors it may contain. Then there is the analysis needed to determine the root cause for the problem if the script error is not the only issue.
4) Once the resolution is reached, resources are lined up by the **SI**.
5) Create a Production incident for the failure.
6) The **Oper** team will reach out the appropriate team (App Hosting Team, DBA team, etc.)
7) **SI** or **HD2** opens the triage bridge
8) Triage the issue
9) Get DSS approval *if required*
10) Fix the issue
11) Execute the DCR, if needed
12) Restart the batch job and process unprocessed cases

If priority B job fails, the batch cycle will move forward.

1) Batch **OPER** lead reaches out to **SI** support.
2) **SI** team analyses the issue
3) Create a Production incident ticket
4) **Oper** team updates ticket with triage information

Based on the analysis, A DCR may be executed and job rescheduled on the following business day.

Please find the escalation workflow below (currently, the Batch monitoring is done by Deloitte).



5.3 Incident Management / Resolution

This section explains the processes and procedures required to respond to outages, defects, and performance issues that might occur when the HHS Enterprise Applications system has a failure or cannot support system functionality or performance. Each event is called a Production Incident. Examples of Production Incidents are users of the system cannot login or functionality has been rendered unavailable, batch processes fail that results in incorrect or no data, or sluggish performance to the point where productivity is harmed. They are identified in several ways; called into the helpdesk, errors are found while monitoring the batch process, automated notifications of hardware failures and software thresholds exceeded, and others. Identifying, tracking, triaging, resolving, and determining root cause are the goals of Incident Management.

The PMO IT team (DSS' IT Management and Project Support) establishes and implements help desk support guidelines and principles. This team also defines procedures and standards for support of incident management and resolution as well as establishing mechanisms in the helpdesk system to generate reports to track efficiency of the help desk process.

5.3.1 Help Desk Incident Escalation Structure %

There are three levels required to support the operations of Incident Management and Resolution.

Help Desk Level 1 (HD1) are the first responders for calls from application users. This group answers the phone, clarifies the issue(s), performs first level health checks, resolves minor issues such as password resets, escalates complex issues to appropriate teams for efficient triage and resolution, and creates the ticket(s) necessary to track the incident.

Help Desk Level 2 (HD2) supports a higher level of triage for the incident(s). This group evaluates the symptoms documented in the Incident ticket and arranges communications with the HD3 App Hosting team if necessary to escalate. There are three teams in this group.

- HD2 App Support is the team that supports incidents that occur during normal work hours receiving the tickets generated from HHS workers using an HHS Enterprise Application or HHS Clients that have called their support linewere unsuccessful. An example of an unsuccessful first level health check is the HD1 HHS resource checking for the applications being available for login first thing every morning.
- HD2 BEST is the team that supports the system monitoring during and after normal working hours supporting the many hardware and software components of the HHS Enterprise Applications System when they receive errors and incidents by either automated notifications or manual monitoring. They can also receive calls from the HD2 Oper team when a batch failure occurs and needs escalation of other support teams. Currently, the procedure for HD2 BEST team to escalate to HD3 App Hosting team is through their internal BEST FootPrints system.
- HD2 Oper is the team that monitors and supports incidents that occur during batch processes. This team is generally self-sufficient as it rarely needs the other HD2 teams to resolve issues as they have their own set of procedures for escalations defined in the Batch Calendar and Schedule. See section 5.2. Also, it is possible but rare that the HD3 teams escalate incidents to HD2 Oper.

Help Desk Level 3 (HD3) leads the effort to return the application functionality as soon as possible as well as the effort to find the root cause of the incident. This group escalates to other level 3 support teams and possibly to Level 3a COTs support if required. This may include creating new tickets for any follow up resolutions when necessary. There are three teams in level 3 of support separated by the anticipated root cause determined by the triage of the incident. Level 3a pertains to the hardware and software vendors for the Commercial Off The Shelf products we currently use. This group is only called from the level 3 support teams.

- HD3 App Hosting is the team that supports resolution of incidents that are suspected to be technical environment based. This team coordinates the inclusion of other teams, provides a conference call 'bridge' when necessary, troubleshoot servers, connectivity, components, and services. This includes but is not limited to; review of system configurations & logs, examining CPU, memory, I/O, throughput, identity access, and system errors and warnings.
- HD3 SI is the System Integrator team that supports the application from where the incident was generated. This pertains to the failure of application's functionality. This includes but is not limited to; examining errors and warnings from application and database logs, screen messages, and system configurations & logs. Multiple applications can have the same HD3 SI team and others may have different teams. Example: Currently: Impact and ConneCT have the same HD3 SI and the EMPI has a different one.
- HD3 Infrastructure is the BEST technical support teams for the hardware and software installation, configuration, and maintenance.

Help Desk Level 3a (HD3a) COTS teams support a very specific high level of triage for the incident(s). This group evaluates the symptoms and their relationship with the configuration of the particular supported hardware or software. Working with all the other associated support teams, this team assists in the effort to return the application functionality as soon as possible and to find the root cause of the incident. There are many teams in this level of support as they represent the expertise and support of all the components of the HHS Enterprise Applications System.

- HD3 teams support resolution of incidents that are suspected to be related to a specific technical component. These teams assist with trouble shooting and root-cause analysis, join conference calls 'bridges' when necessary, troubleshoot servers, connectivity, components, and services. This expertise includes but is not limited to; Database Administration, Operating Systems, Adobe, Corticon, WESB, SIM/SAM, FileNet, F5, Network, Firewall, DataPower, etc.

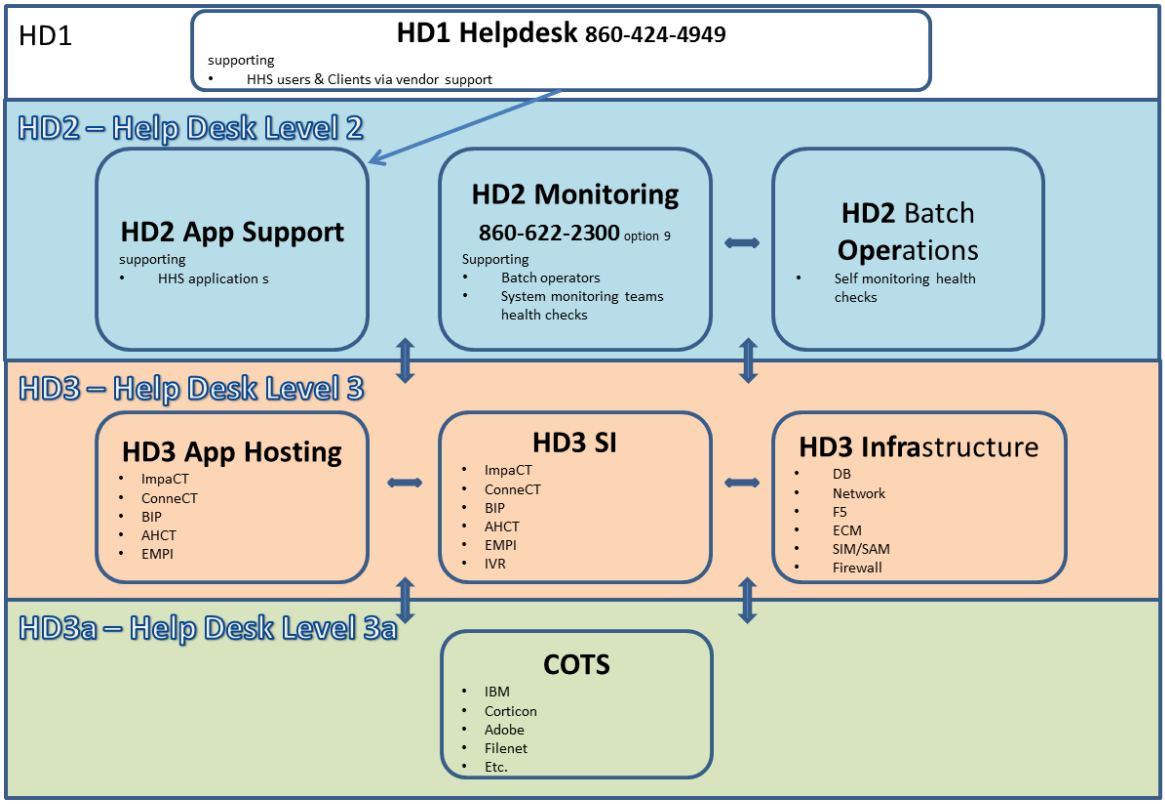


Figure 1: Help Desk Support Structure

5.3.2 Help Desk Ticketing Systems and Tracking %

The HHS Enterprise Applications System has many teams that provide help desk support. At this time, we also have multiple ticketing systems depending on the team and their tracking needs.
Footprints is the State's tracking system. State IT has 2 separate instances that do not integrate at this time. The State-wide version is the primary tracking system for the following teams (but not limited to); App Host, DB, Rel Mgr, Network, F5, SIM-SAM, DP, Oper, MFT, FileNet, Firewall, MFA. The DSS hosted version of Footprints is the primary tracking system for (not limited to); AcctAdmin, HD1, MFA. This document will label these Footprints-SW and Footprints-DSS.
The System Integrators generally have their own tracking system and we currently have 2 of them. Deloitte has JIRA and is the system integrator for the majority of the applications. The system they are

using is JIRA. This is the primary tracking system for (not limited to) the following support teams; HHS EC, PMO, PMO PD,SME, PMO IT, CCB, SI-Deloitte.
The EMPI has another tracking system named Remedy Force used by; SI-Nextgate, App Host-CMA, and DB-CMA.
The COTS vendors also track their own tickets when they are called for support.

The Operations and Maintenance for HHS Enterprise Applications requires the support teams to coordinate and reference ticket numbers of the associated systems when multiple tracking systems are getting utilized for the same issues. This manual will reference the creation, update, status changes, and closure of tracking tickets. This applies to all tracking systems utilized for each issue.

When a Production Incident is determined to be a Change Request and not a Defect by the PMO, PMO PD, or HHS EC, the ticket is categorized as a change request and removed from the Incident Management procedures to be placed in the Release Management queue for prioritization by the CCB for inclusion into a software release.

5.3.2.1 *Incident Details*

Incidents need to be categorized according to their severity. Production Incidents will have the following characteristics to help with the triage process.

- Severity
  - Defines the impact of the incident

Table 5: Incident Severity

Severity Scale	Description	Response Expectation	Escalation Path
CRITICAL	**System or a mission critical component no longer functions** An issue that severely and adversely affects production or system usage; Significant performance degradation, corrupt, lost, misrepresented, or unrecoverable data; system crash, critical business functions not being available leading to loss of worker productivity;	**<u>PROD Environment</u>** **Within 15 minutes (30 mins outside business hours)** • Response from DSS, AHCT or BEST issue owner **Within 4 Hours:** • Time to resolution communicated • Workaround Identified • Resolution / Closure **<u>Non-PROD Environments</u>** **Within 30 minutes (60 mins outside business hours)** • Response from DSS, AHCT or BEST issue owner **Within 4 Hours:**	**Within 30 Mins** • Operations contact **4 Hours** • Supervisor/Lead • Manager • Director • Vendor • CIO

	Examples: • Users are unable to log into the system. • Users can access the system and complete applications and data collection, but eligibility will not run for a case. • Users cannot authorize eligibility results on a case. • Benefits are blocked	• Time to resolution communicated • Workaround Identified • Resolution / Closure *SLA's for Non-Production Issues outside business hours will be applicable during the last 2 weeks of a planned production release or during the last 48 hours of a planned hotfix.*	
HIGH	**Non-systematic issue without workaround** An issue that impacts significant number of customers/workers and adversely impacts a specific business operation. This issue would impact significant number of cases/households (>10% of cases/households affected) every business day and/or affect productivity of significant number of workers every business day (>50% of workers), and has no business acceptable workaround available	**<u>PROD Environment</u>** **Within 2 Hours (4 hours outside business hours)** • Response from DSS AND AHCT issue owner **Within 8 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure **<u>Non -PROD Environment</u>** **Within 4 Hours** • Response from DSS AND AHCT issue owner **Within 8 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure *SLA's for Non-Production Issues outside business hours will be applicable during the last 2 weeks of*	**8 Hours** • Operations contact **12 Hours** • Supervisor/Lead • Manager • Director • Vendor

	Examples: • Reproducible page break • Key non-Eligibility function is malfunctioning for multiple users	*a planned production release or during the last 48 hours of a planned hotfix.*	
MEDIUM	**Non-systematic issue with workaround** Product malfunction or failure with no significant impact; non-critical loss of functionality of the software or impairs some operations, but allows the user to continue using the application. Examples: • Eligibility processes a rare scenario, but the benefit amount was not as expected. Correct benefits can be issued by overriding the eligibility result as a workaround. • Alerts are not routed to the correct queue	**PROD Environment** **Within 8 Hours** • Response from DSS AND AHCT issue owner **Within 12 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure **Non-PROD Environment** **Within 8 Hours** • Response from DSS AND AHCT issue owner **Within 12 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure	**24 Hours** • Operations contact
LOW	**Issue causes an impact to the worker but not to the cases and is minor in nature.** A failure that has little or no impact on the end user's operation. Examples: • On the Relationship screen, the system will not complete reciprocal relationships of parent to child so the user has to complete each	**PROD Environment** **Within 24 Hours** • Response from DSS AND AHCT issue owner **Within 48 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure **Non-PROD Environment** **Within 24 Hours** • Response from DSS AND AHCT issue owner	**24 Hours** • Operations contact

	relationship one at a time. • Cosmetic Issues	**Within 48 Hours:** • Update with estimated time to resolution • Workaround Identified • Resolution / Closure	

5.3.3 Help Desk Level 1 Support %

5.3.3.1 *HHS worker encounters an incident*

5.3.3.1.1 Worker contacts supervisor

*5.3.3.1.2 Supervisor determines if this issue requires training, data correction within the application, or other resolution that does not require IT support. If the incident requires IT support the supervisor contacts the **HD1 Helpdesk** support team at 860-424-4949.*

*5.3.3.1.3 **HD1 Helpdesk** team confirms the incident requires IT support. The **HD1 Helpdesk** team resolves the issue if possible (i.e. reset password). If not, it works with the supervisor on gathering screen shots, further explanations of what steps were followed to get the error or issue, and any other helpful information.*

*5.3.3.1.4 If the user is logged onto an HHS application and having an issue, the **HD1 Helpdesk** team creates Production Incident ticket and escalates the ticket to **HD2 App Support**.*

*5.3.3.1.5 **HD1 Helpdesk** contacts **HD2 App Support**.*

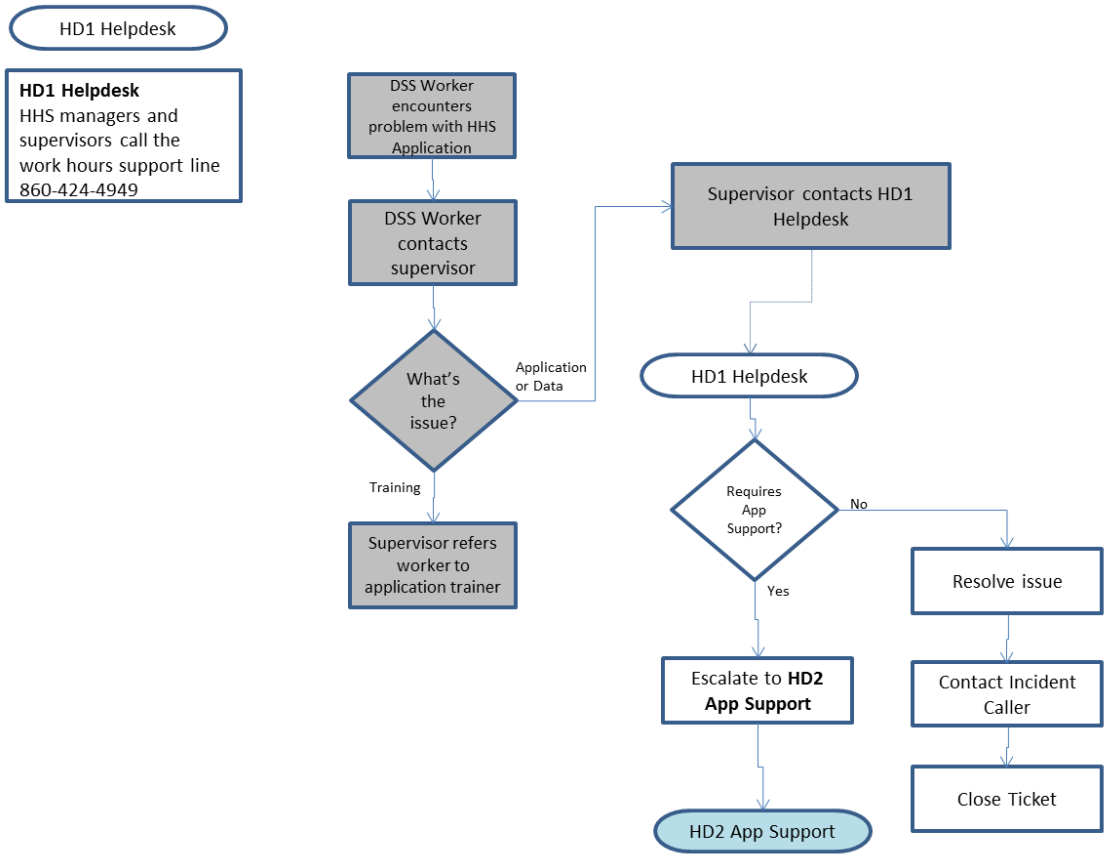


Figure 2: Incidents Generated from Workers

5.3.3.2 *HHS client encounters an incident*

5.3.3.2.1 Client contacts state-wide support call center (current vendor: Conduent)

*5.3.3.2.2 Support specialist determines if this issue is requires training, data correction within the application, or other resolution that does not require IT support. If the incident requires IT support the support specialist contacts the **HD1 Helpdesk** support team at 860-424-4949.*

*5.3.3.2.3 **HD1 Helpdesk** team confirms the incident requires IT support. The **HD1 Helpdesk** team resolves the issue if possible (i.e. reset password). If not, it works with the supervisor on gathering screen shots, further explanations of what steps were followed to get the error or issue, and any other helpful information.*

*5.3.3.2.4 If the user is logged onto an HHS application and having an issue, the **HD1 Helpdesk** team creates Production Incident ticket and escalates the ticket to **HD2 App Support**.*

*5.3.3.2.5 **HD1 Helpdesk** contacts **HD2 App Support**.*

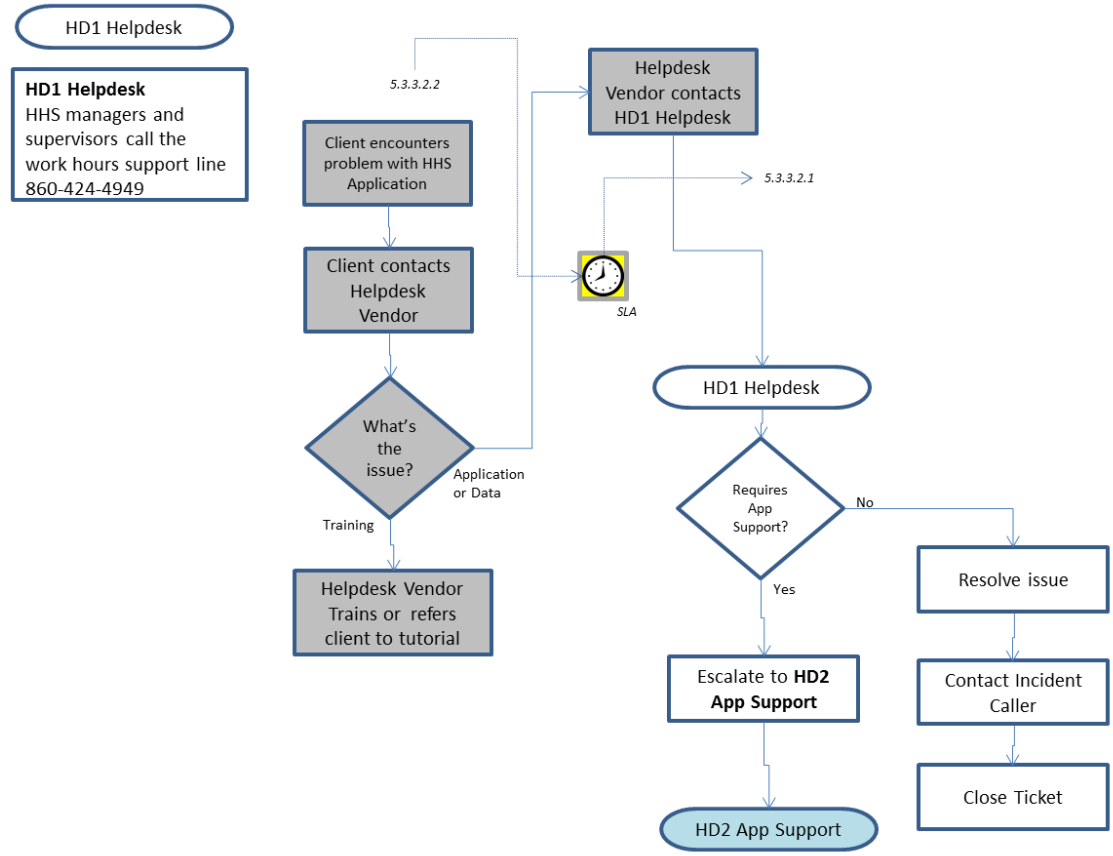


Figure 3: Incidents Generated from Clients

5.3.4 Help Desk Level 2 (HD2) App Support %

5.3.4.1 *HD1 Helpdesk (or other support team) contacts HD2 App Support*

*5.3.4.1.1 **HD2 App Support** team confirms the incident requires IT support and attempts to recreate it if possible. This team contacts the supervisor on gathering screen shots, further explanations of what steps were followed to get the error or issue, and any other helpful information not gathered to date.*

*5.3.4.1.2 Determine if this issue can be corrected by the worker or by the **HD2 App Support** Team.*

*5.3.4.1.3 Assist the worker with resolution or resolve within the **HD2 App Support** team if possible..*

5.3.4.1.4 Determine assignment of severity of the issue to the ticket.

*5.3.4.1.5 If no resolution done, **HD2 App Support** contacts **HD3 App Hosting** while escalating the ticket.*

*5.3.4.1.6 **HD2 App Support** team contacts the user community identifying impact and scope of issue. Critical if the system is experiencing an outage.*

*5.3.4.1.7 Once level 3 support is engaged, the **HD2 App Support** team joins any real time / Conference bridge to support the analysis and communications with the users (workers).*

*5.3.4.1.8 **HD2 App Support** team contacts the users when the system has been returned to full functioning condition.*

5.3.4.1.9 Tickets are not fully closed until the root cause has been determined and documented.

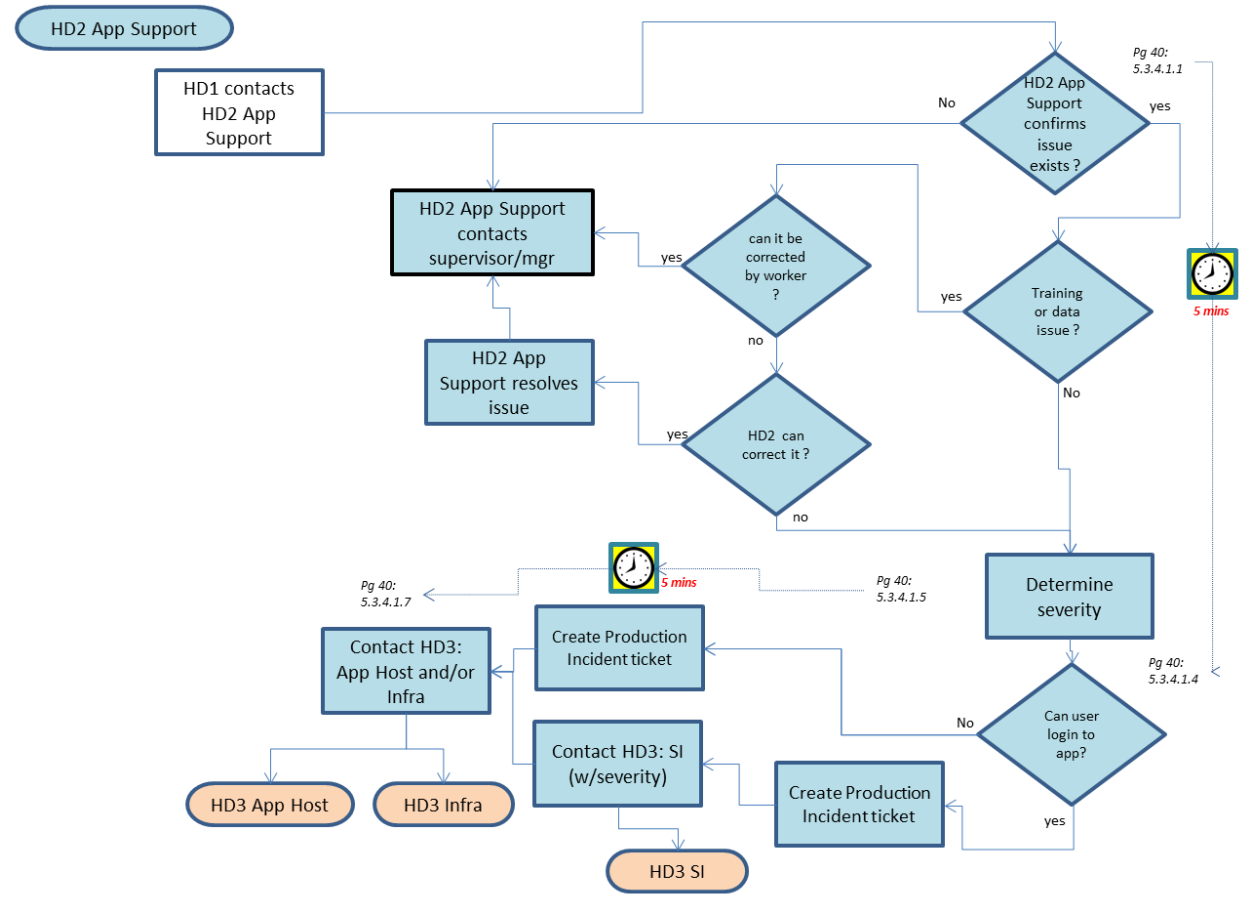


Figure 4: Incidents Escalated to HD2 App Support

5.3.4.2 *HD2 BEST Unsuccessful System Health Checks (Business Hours)*

*5.3.4.2.1 Monitoring tools and automated processes are reviewed by different Monitoring Support Teams (**MST**) for the HHS Enterprise Application system, all of which could generate a Production Incident. Some health checks are done manually by the **HD2 App Support** team by testing logins (first thing every morning) and using monitoring tools such as New Relic. If this is during business hours, either team could be notified; **HD1 Helpdesk** 860-424-4949 or **HD2 BEST** 860-622-2300 option 9; an incident would be logged and the procedures would begin.*

*5.3.4.2.2 Contact **HD2 App Support** to inform them of the issue and contact the business teams if necessary.*

*5.3.4.2.3 If **HD2 BEST** team identifies this as a data issue, can it be corrected through the application? If so, contact the **HD2 App Support** team to correct it or contact the application user who can. If it cannot be corrected through the application then the SI may need to be contacted to begin the data correction.*

*5.3.4.2.4 **HD2 BEST** team works with the health check reviewer on gathering log records, further explanations of what errors or warnings were discovered, and any other helpful information.*

*5.3.4.2.5 If clients cannot login to the application or the system needs to be brought down due to a severity one / critical issue, **HD2 BEST** creates a Production Incident and escalates to the level 3 support team(s).*

*5.3.4.2.6 Once level 3 support is engaged, the **HD3 App Hosting** team provides communications and real time / Conference bridge support for the support teams.*

*5.3.4.2.7 **HD1 HHS** team contacts the DSS business teams when the system has been returned to full functioning condition if it was not available.*

5.3.4.2.8 Tickets are not fully closed until the root cause has been determined and documented.

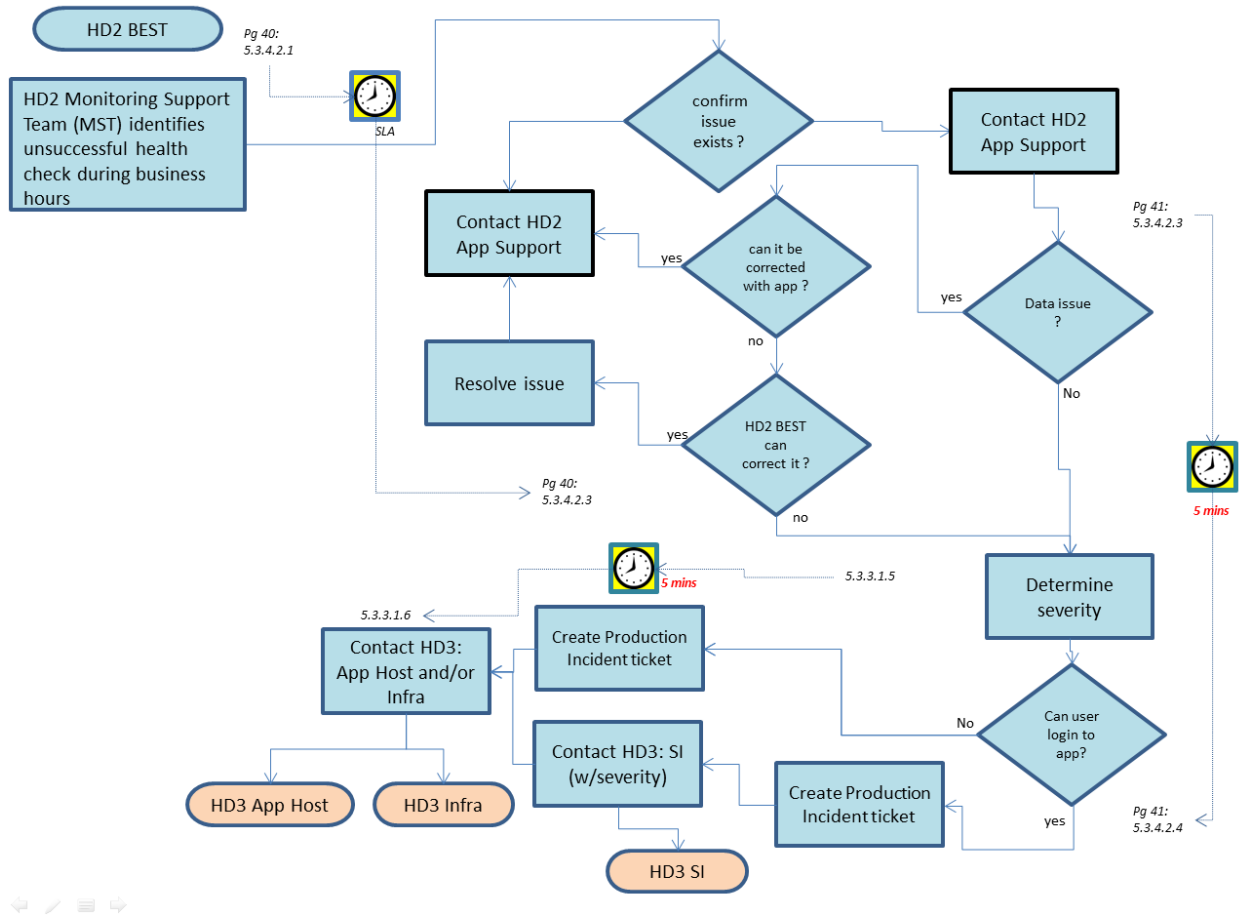


Figure 5: Incidents Generated from Unsuccessful Health Checks

5.3.4.3 *HD2 BEST Unsuccessful System Health Checks (After Business Hours)*

*5.3.4.3.1 Monitoring tools and automated processes are reviewed by Monitoring Support Teams (**MST**) teams for the HHS Enterprise Application system, all of which could generate a Production Incident. After business hours, notifications go to **HD2 BEST** 860-622-2300 option 9; an incident would be logged and the procedures would begin.*

*5.3.4.3.2 **HD2 BEST** creates a Production Incident where it will get escalated to the **HD3 App Hosting** support for triage and analysis..*

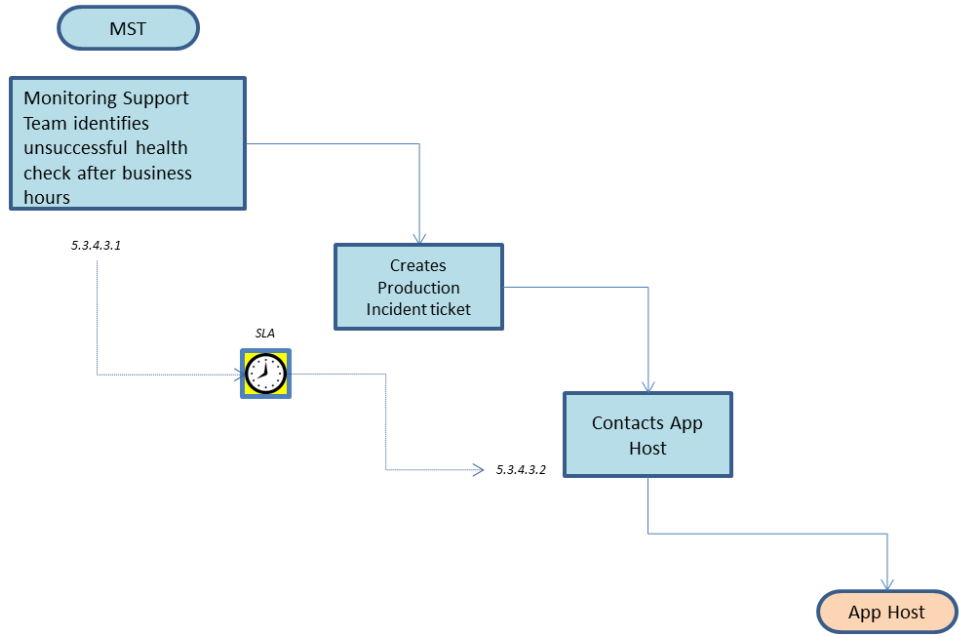


Figure 6: Incidents Generated from Unsuccessful Health Checks After Business Hours

5.3.4.4 *Oper encounters an Batch incident*

5.3.4.4.1 Batch procedures result in an error. The response for each batch failure is documented in the Batch Calendar. This is a high level representation.

5.3.4.4.2 Resubmit the batch if the procedures indicate this is the response.

*5.3.4.4.3 If the batch cannot be immediately resubmitted and the priority of the Batch is 'A', execute the designated call list in the Calendar procedures, contact the **HD3 SI** support team, and establish the conference bridge. If the Batch = priority 'B', follow steps for resolution if they are provided, otherwise create a ticket for resolution at a later time. This ends the activities to support priority 'B' batches. If priority is 'A' – continue…..*

5.3.4.4.4 Participate in the conference bridge and support any batch execution activities that are required. Contact level 3 support if necessary.

5.3.4.4.5 Assist with the resolution of the incident.

5.3.4.4.6 Resume the batch procedures in parallel if the priority 'A' failure steps in the Batch Calendar allow it and the SI team approves. Otherwise resume after the resolution is complete and tested.

5.3.4.4.7 Assist with determining root cause of the failure.

5.3.4.4.8 Tickets are not fully closed until the root cause has been determined and documented.

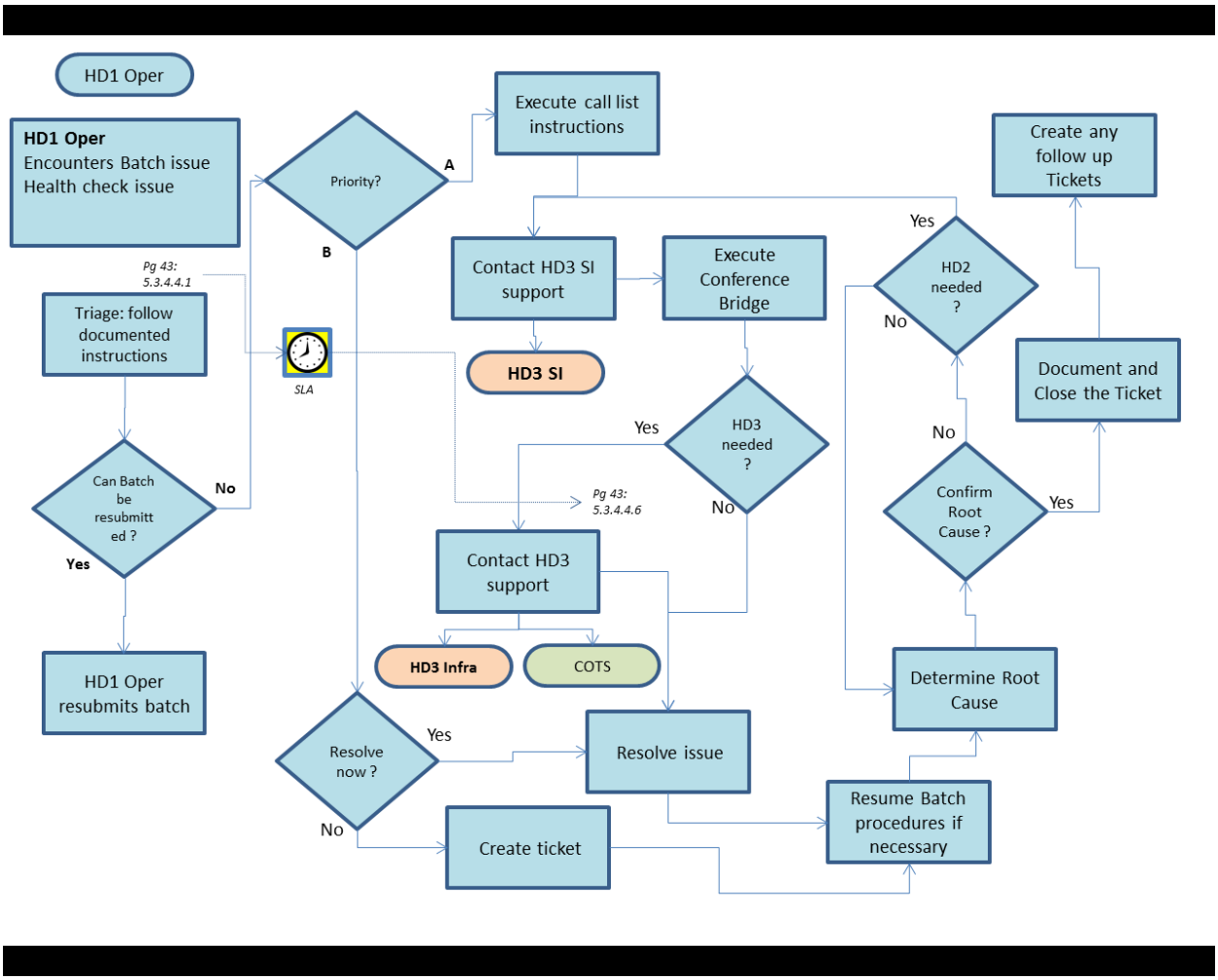


Figure 7: Incidents Generated from Batch Processes

5.3.5 Help Desk Level 3 Support %

5.3.5.1 *HD3: App Hosting (Application Hosting)*

5.3.5.1.1 HD3: App Hosting is contacted or discovers an issue themselves.

5.3.5.1.2 Examine the ticket and its contents and triage.

5.3.5.1.3 Begin work for getting the application fully functional if needed.

5.3.5.1.4 Contact the user community identifying impact and scope of issue or contact HD2 to do the same during work hours. Put up the system maintenance page when appropriate.

5.3.5.1.5 Determine if support from other teams will be required.

5.3.5.1.6 Contact team(s) and start a conference bridge

*5.3.5.1.7 Once the application is fully functional again contact **HD2 App Support** team for communications.*

5.3.5.1.8 Determine root cause of the incident

5.3.5.1.9 Document root and close the ticket

5.3.5.1.10 Create any required follow up tickets

*5.3.5.1.11 **HD2 App Support** team or business user tests and validates the resolution*

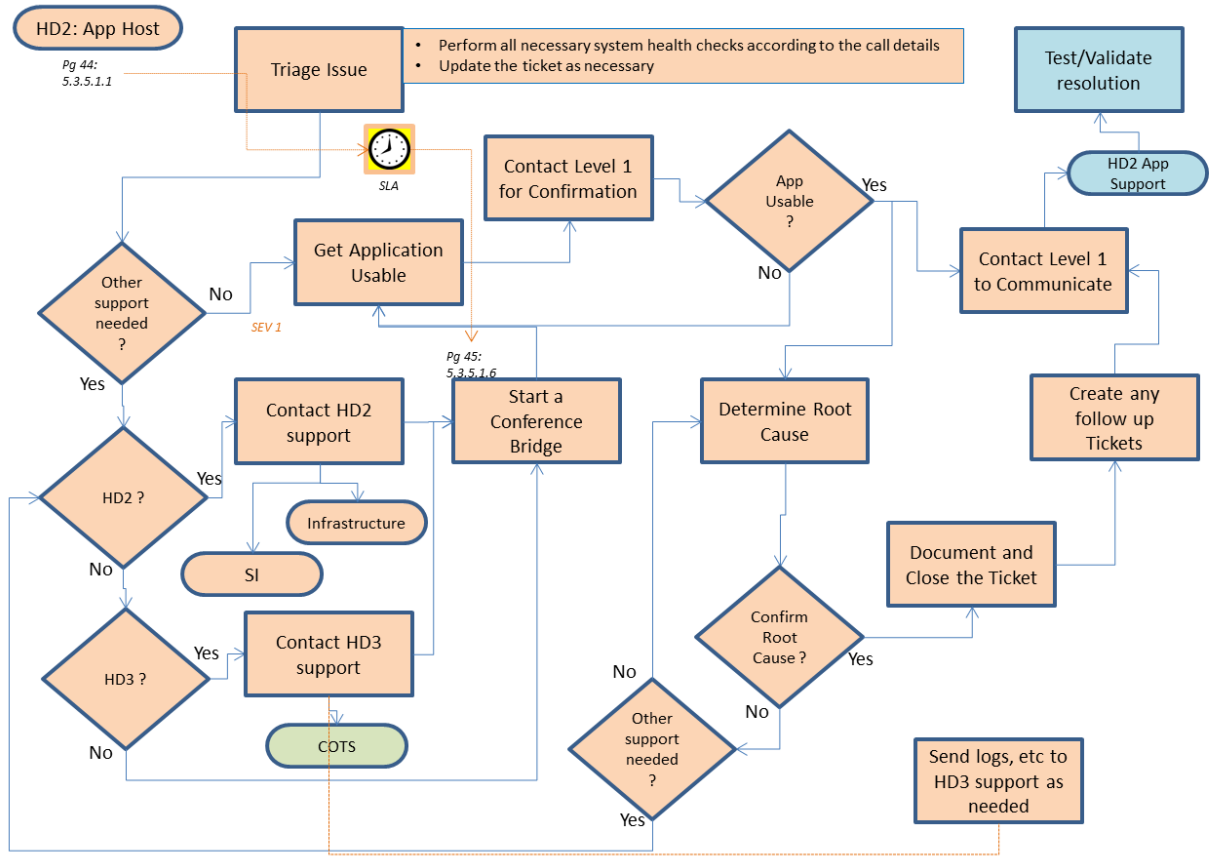


Figure 8: Incident Escalation to HD2: App Host

5.3.5.2 *Incident is escalated to HD3: System Integrator and/or Infrastructure*

5.3.5.2.1 Examine the ticket and its contents and triage.

5.3.5.2.2 Begin work for getting the application fully functional if it is not.

5.3.5.2.3 Determine if support from other teams will be required.

5.3.5.2.4 Determine time to resolution and communicate

5.3.5.2.5 Identify workaround if possible

5.3.5.2.6 Contact team(s) and start a conference bridge if needed

*5.3.5.2.7 Once the application is fully functional again contact **HD2 App Support** team for communications.*

5.3.5.2.8 Determine root cause of the incident

5.3.5.2.9 Document root and close the ticket

5.3.5.2.10 Create any required follow up tickets

*5.3.5.2.11 **HD2 App Support** or business user tests and validates the resolution*

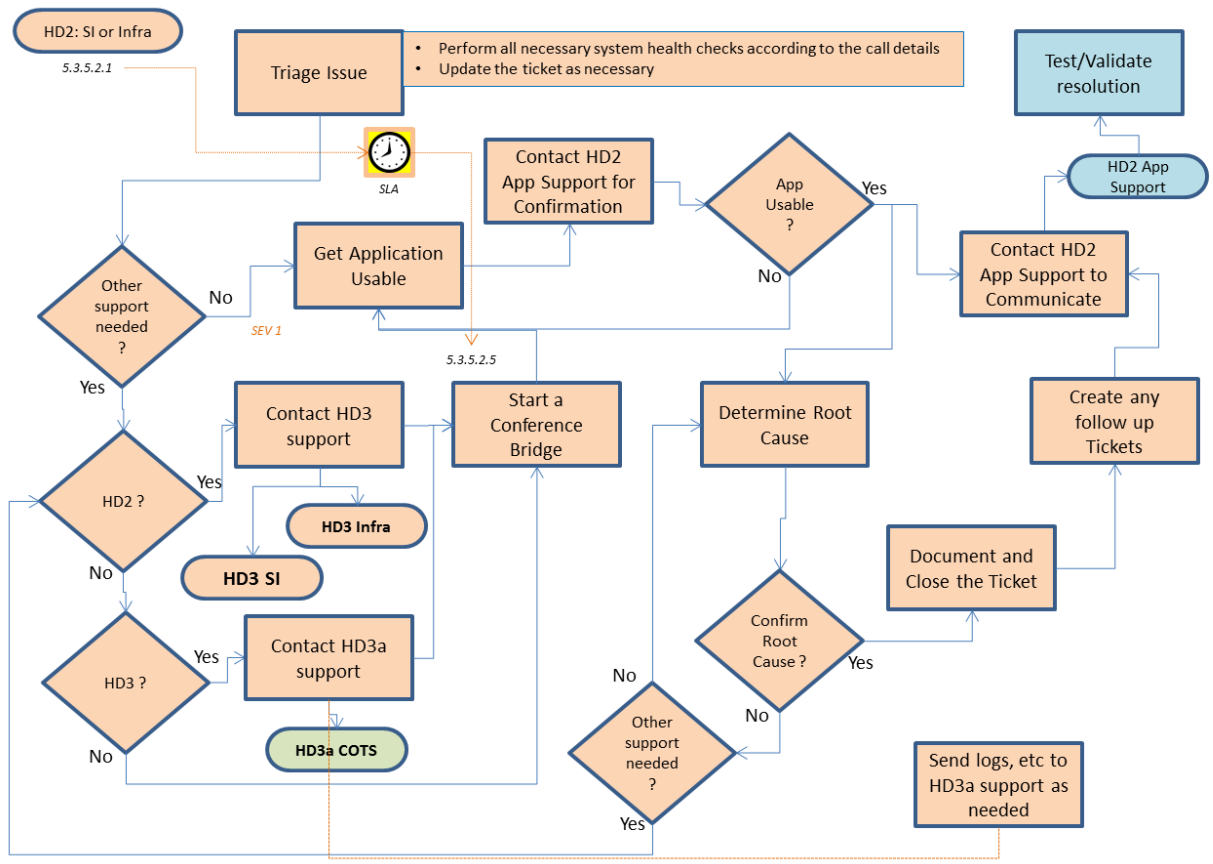


Figure 9: Incident Escalation to SI or Infrastructure (first SLA)

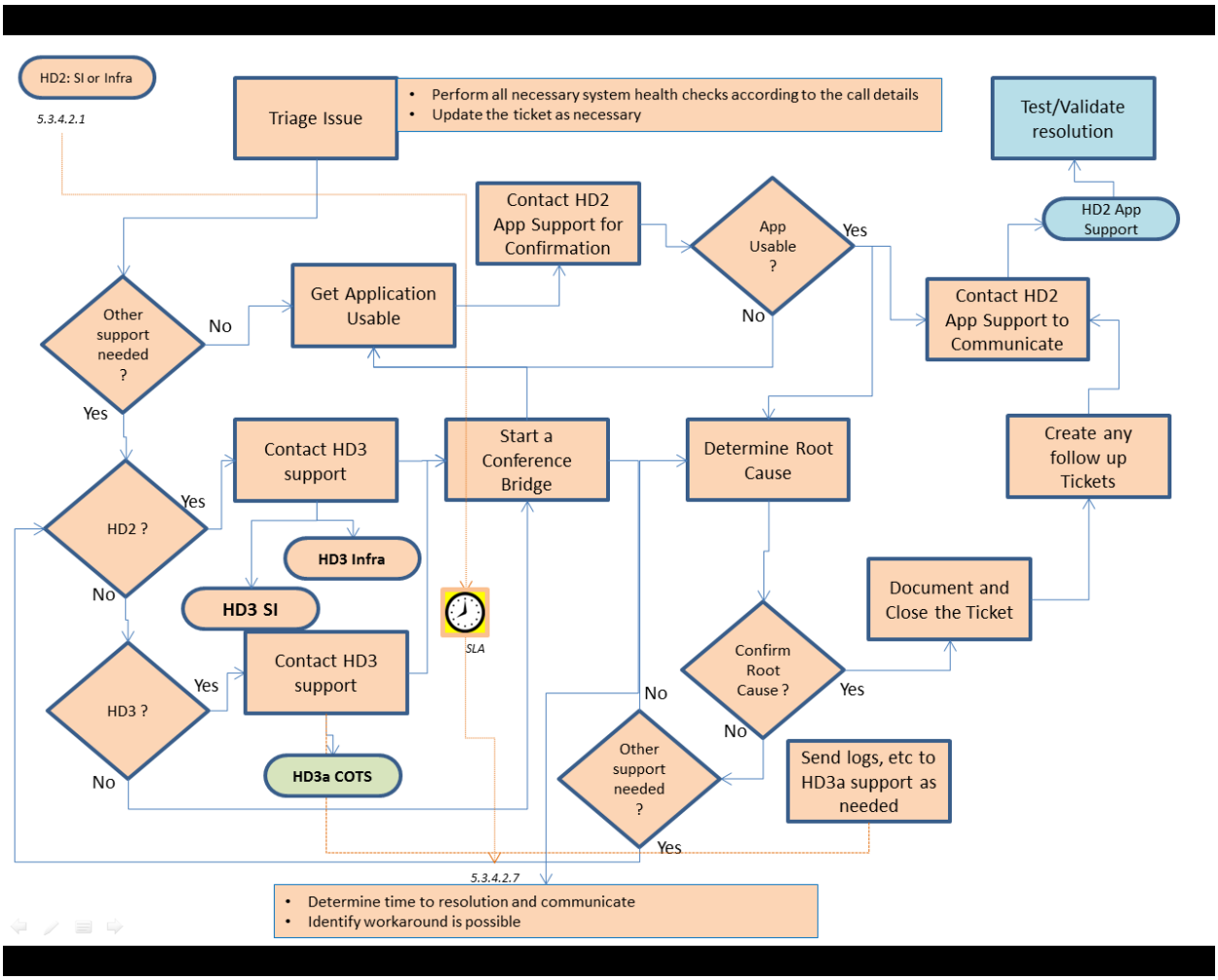


Figure 10: Incident Escalation to SI or Infrastructure (second SLA)

5.3.6 Help Desk Level 3a Support %

5.3.6.1 *Incident is escalated to Vendor SME Support (COTS)*

5.3.6.1.1 Examine/triage the ticket's contents and all sent documentation (ticket contents, logs, screen shots, etc)

5.3.6.1.2 Join conference bridge if it is held.

5.3.6.1.3 Assist with getting the application fully functional if it is not.

5.3.6.1.4 Assist with determining root cause of the incident

5.3.6.1.5 Coordinate with HD3 team for business user tests and validations of the resolution

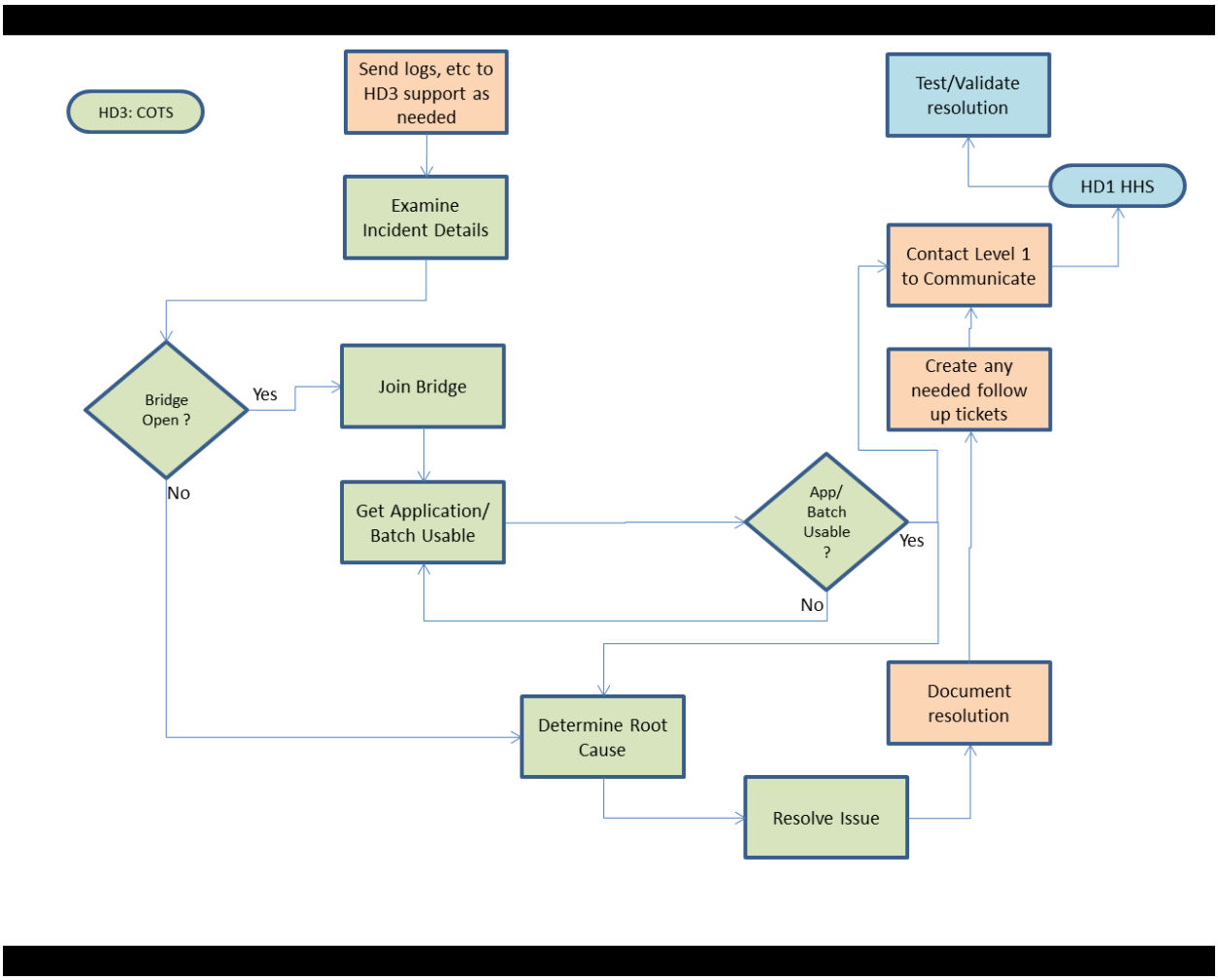


Figure 11: Incident Escalated to Level 3 Support

5.3.7 Incident Escalation Contact List %

Priority Scale	Contact						
	Role	Primary	Primary Cell	Primary Email	Secondary	Secondary Cell	Secondary Email
CRITICAL	Operations contact	DSS ITS Help Desk	860-424-4949	DSS-ITS-Support@CT.GOV			

	App Hosting Lead	Naren Nandi					
	Manager	Saul Mora					
	DSS Director	Vance Dean					
	DSS UAT Manager	Krithika Deepa					
	AHCT Director	Rajiv Chawla					
	Vendor	*App Hosting engages vendor					
	BEST	Eric Lindquist					
	CIO	Joe Stanford					
HIGH	Operations contact	DSS ITS Help Desk	860-424-4949	DSS-ITS-Support@CT.GOV			
	App Hosting Lead	Naren Nandi					
	Manager	Saul Mora					
	DSS Director	Vance Dean					
	DSS UAT Manager	Krithika Deepa					
	AHCT Director	Rajiv Chawla					

	Vendor	*App Hosting engages vendor					
	BEST	Eric Lindquist					
MEDIUM	Operations contact	DSS ITS Help Desk	860-424-4949	DSS-ITS-Support@CT.GOV			
LOW	Operations contact	DSS ITS Help Desk	860-424-4949	DSS-ITS-Support@CT.GOV			

6 Maintenance

6.1 Deployment Management %

This section explains the processes and procedures required to achieve successful deployments of software releases and configuration changes in the enterprise. The many components, services, and products that make up the design of this system have different architectural designs, deployment tools, and support roles. Preparations for a deployment include defining the activities required for each role depending on the scope of the release or configuration change. All required tasks must be defined and packaged in the currently defined deployment tools. Every deployment package must be successfully tested in the System Integration Testing (SIT) environment hosted by the SI. Once the application SIT testing results are accepted, this package can be delivered to the State for scheduling its deployment into a State hosted environment.

6.1.0.1 *Stakeholder Management*

The management of a stakeholder registry of the support teams for all components of the HHS Enterprise Applications System and Platforms and the coordination & scheduling of these resources for all deployment activities, are duties of the Release Manager.

The Test Team conducts UAT for all break fixes done by the M&O team for L2/3 incidents. This also covers the regression testing during UAT that needs to be performed on impacted components
This section outlines the tools used and process followed in managing application source code, releases and deployment across various environments.

6.1.1 Release Management %

6.1.1.1 *Release Planning*

Perform release planning for application release versions, patches, and upgrades. This requires coordination with all technical infrastructure support teams. A schedule must be proposed and approved by all the stakeholders indicated in the registry maintained by the Release Manager.

6.1.1.2 *Release Readiness*

The Release Manager finalizes the Release Schedule after obtaining signoff from all stakeholders on Release readiness and notifies the stakeholders, publishing the calendar.

6.1.1.3 *Emergency Releases*

Release Planning and Stakeholder notification for emergency releases must have full sign off before proceeding

6.1.1.4 *Sign-offs*

Sign offs are also necessary for validations after a release is deployed to assure the application is functioning.

6.1.1.5 *Post Release Communications*

The Release manager publishes Completion of Deployment Communication to all DSS IT stakeholders, DSS Technical Manager, State IT Technical team involved, and PMO, which includes:
• The summary of Change as per the Functional Release Note.
• Completion time of Deployment
• Support Contact information
Thereafter, DSS Technical Manager, in consultation with the Helpdesk Support team, communicates to all stakeholders including business users as necessary.
When the target environment is Production, the Deployment is a sub-set of an overall Release Process that needs various additional communications as defined in the section 6.2.1.

6.1.2 Backup/Restore %

Backups are taken before each major step is executed to provide roll back procedures to return the application to its previous state. This pertains to databases and application/web servers.

As part of STATE IT enterprise process, STATE IT backups all Virtual Machines (VMs)/Servers on the network on a daily basis. If there are corrupted installation files on the server(s), a Request for Service (RFS) opened by STATE IT support team can be initiated to restore the files from previous backup. This is done for all HHS Enterprise infrastructure components. Deployment packages are also archived before every deployment. In the case of any issues with HHS Enterprise applications, a new deployment of the application is moved to the server.

Apart from STATE IT enterprise backup process, a separate VM managed by STATE IT App Hosting team was provisioned to archive and back up all ImpaCT deployment artifacts. All deployment code base

is archived to the archive server should the need arises. If an issue occurred with the software installation, the system will be recovered with the backup taken prior to the software installation.

6.1.2.1 *Identity and Access Management (IAM)*

There's a separate document created by the SIM/SAM team for O&M activities.

For information on the IAM(SIM/SAM) O&M activities, refer to;
Security Identity Management Administration_User Guide_v2.0.docx

6.1.2.2 *IBM IHS Web Server*

After installation and configuration of the IBM IHS Web Server software, STATE IT backup all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WAS server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup.

If configuration changes are required, instructions will be provided in the deployment Playbook as indicated in Section 6.2.1 Code Delivery. The file being changed will be backed up for cases where a restoration is required.

6.1.2.3 *IBM WebSphere Application Server (IBM WAS)*

After installation and configuration of the IBM WebSphere software, STATE IT backup all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WAS server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup.

All deployment package, documents, and artifacts are archived/backup during deployment. If the need occurs to rollback a deployment, the Application Hosting team would refer to the previously deployed artifacts and documents to roll back the deployment.

6.1.2.4 *Corticon Business Rules*

Corticon Business Rules is installed on IBM WAS, STATE IT backup all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WAS server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup.

6.1.2.5 *FileNet*

FileNet system is installed on IBM WAS, STATE IT backup all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WAS server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup.

6.1.2.6 *Adobe LiveCycle*

Adobe LiveCycle is installed on IBM WAS STATE IT backup all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WAS server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup.

6.1.2.7 *PDTX DB2 Database*

STATE IT is fully responsible for the management and maintenance of all DB databases on an enterprise level. Backup procedures are already in place by STATE IT Enterprise team. Regular database restore entails using the most recent backup file to restore the database to the "last known good state". Server backups maintained by STATE IT team can also be used to recover from a disaster.

6.1.2.8 *Database Backup Process*

1. To assist with the backup process, STATE IT DBAs will write scripts to automate the backup process in an online mode while having the ability to do incremental backups **if needed**.
2. It is recommended that a full online backup to be taken before batch cycle, interim conversion and after batch cycle to disk with compression enabled on a daily basis and retain only backup file which was taken after batch cycle to TSM on successful completion of batch cycle.
3. The backup scripts should be set to run on a daily basis using batch job scheduler.
4. It is advisable to have separate directories for each set of backup files, or have a different naming convention for the full backup scripts.
5. The scripts should also have the ability to check disk space and send an email if space is above a certain threshold. In addition, the scripts should either delete/move any backup files older than 2 weeks to a separate location where it can later be removed from the disk.
6. It is recommended to retain the Backup files on TSM for minimum of six months.

6.1.2.9 *Database restore process:*

1. ADHOC database will be refreshed with Production database on daily basis using the latest production online backup taken previous night. Once the IBM DB2 Q Replication testing is completed and approved by client then the Ad-Hoc database will be refreshed near real time using this feature.
2. STG database will be refreshed with Converted data after conversion integration testing is completed. This database will be refreshed through redirect restore process by taking backup of Conversion Integration Environment (CIT) database.
3. Production data may be barred from UAT database and will be never be refreshed with Production database backup. The data of UAT environment will be setup by UAT testing team based on their testing scenario, UAT data will not be refreshed by any other environment on regular basis.

6.1.2.10 *Adobe LiveCycle*

In addition to the regular Enterprise server backups that are being done by STATE IT Enterprise support, all XMLs, PSs, and PDFs files that get generated by Adobe and are archived.

If there's need to restore the Adobe files, STATE IT Enterprise support team will obtain the previous backup from the archived location and provide it to the STATE IT support team to be restored. Adobe LCAs are backed up with the deployment package whenever there's a deployment to the environment. If the need arises, STATE IT support team obtains the archived LCAs within the archived location and deploy it to the server.

6.1.2.11 *IBM FileNet P8*

ImpaCT, ConneCT, and ahCT all share the same IBM Enterprise FileNet system. The STATE IT administrators have their enterprise process in place for FileNet Server backup and restore. STATE IT FileNet administrator has full control of the FileNet servers without the Application support team having any insight.

If changes are required from the application perspective for FileNet, this will be reflected within the ImpaCT code base and would require a re-deployment of the ImpaCT deployment file by the STATE IT support team. Instructions will be provided as part of the deployment Playbook. In order to restore from a previous back up, STATE IT support team will have to recover the back up from the archive location and proceed with the normal deployment process.

6.1.2.12 *WebSphere Enterprise Service Bus (WESB)*

After the WESB servers have been provisioned, the WESB software is installed and configured. STATE IT backs-up all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the WESB server, a Request for Service (RFS) opened by STATE IT support team, will be initiated to restore the files from previous backup

Updates to the mediation modules is migrated as part of the deployment process. All deployment packages are backed up and archived before every deployment.

Any WSDL/XSD changes for the WESB mediation modules (ESB Workflows) deployed on the server will require update on the IBM Data Power and IBM Web Service Registry and Repository (WSRR). DataPower acts as a secure XML gateway for external services. DataPower workflows define the signature of the inbound web services for validating the XML structures for additional security. The backend URLs configured on WSRR repository enables dynamic service request routing should the end point URLs change.

Note: ahCT WSRR is currently being shared between ahCT and ImpaCT as an enterprise service repository. Back-ups on WSRR servers should be run as per the ahCT back-up schedule.

6.1.2.13 *IBM DataPower Appliance*

There's a separate document created by the SIM/SAM team for O&M activities.

For information on the DataPower O&M activities, refer to "OM-DataPower_v1.docx" in Section 3 References and Attachments, Table 1, Document File Name "OM-DataPower_v1".

6.1.2.14 *ImpaCT Batch with CA ESP*

ImpaCT Batch Servers installation and setup is done during the initial infrastructure setup. After the batch server has been provisioned, STATE IT support team creates the Batch folder (E:\ImpaCT_Batches) to host the batch scripts. STATE IT backups all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the Batch server, a Request for Service (RFS), opened by STATE IT support team can be initiated to restore the files from previous backups.

Before STATE IT support team initiates the Batch deployment, a copy of the Batch folder is taken and moved to an archive location. The folder is renamed "ImpaCT_Batches_Build_Number". This backup is used in case there's a need to roll back the Batch folder.

If there's a need to roll back the files to a previous deployment, the administrators will navigate to the archived folder and override the parent Batch folder, E:\ImpaCT_Batches.

6.1.2.15 *Informatica PowerCenter*

After the Informatica servers have been provisioned, STATE IT Informatica administrators installs the Informatica software. During installation, software files and folders are created in the installation folder on the Informatica server. STATE IT backups all VMs/Servers on a daily basis, at an Enterprise level. If there are corrupted installation files on the Informatica server, a Request for Service (RFS), opened by STATE IT support team can be initiated to restore the files from previous backups.

6.2 Application %

Application Maintenance is the process of updating the features and functions of the HHS Enterprise applications with the inclusion of change requests or defects. Application maintenance includes scoping and planning a release. A release consists of application enhancements or fixes planned to be delivered to Production as a package. The scope of a build is determined in advance of its delivery into State hosted environments, allowing development, SIT testing, and a Go/Nogo for UAT.

6.2.1 Application Releases %

6.2.1.1 *Perform SIT Tests*

Provide SIT test results. Document SIT test results in the Release Notes of the Deployment Package. Provide test scripts for all tests required for new functionality in this code delivery. Perform regression tests. Provide regression test results in the Release Notes of the Deployment Package.

6.2.1.2 *Triggering a Deployment*

After a successful SIT validation of a release, then the appropriate approval is provided to migrate the deployment package to the specifically-requested STATE environment(s). This environment is generally UAT but there are circumstances where the environment is changed. As part of the Release and Deployment process, a JIRA ticket is created with the attached Playbook relative to the release. The deployment package is uploaded to the MFT server and an email is sent to the client providing all relevant information (Release#, Package location, and components being deployed) pertaining to the deployment.

The Systems Integrator's Release and Deployment lead schedules a Playbook walkthrough with the State, to educate them on the content of the release and obtain approval to move forward with the deployments to the requested STATE environments.

Upon receiving the formal approval from the DSS Manager, the Release Manager schedules the deployment and creates necessary RFSs for the appropriate deployment. The Release Manager coordinates with the State deployment teams (App Hosting, Data Services, SSRS, etc.) providing them with the RFS# details and the deployment package, all necessary instructions and documents, allowing them to proceed with the deployment.

- As outlined within the Deployment Playbook, the App Hosting team executes the "App Deployment File Transfer" plan to copy the deployment artifacts from the MFT location to the Archive location.
- App Hosting executes the "<environment>-Stopping-All-Servers" to stop all the application servers and execute a backup of the Batch folders, Adobe LCA, Corticon EDS files, Application EAR, and properties files.
- App Hosting sends out an email communication to Data Services indicating that all the servers are down and they can proceed with their deployment activities.
    - Perform the database deployments.
    - Perform reports deployments.
    - Sends out email confirmation on completion of the database or SSRS activities.
        - App Hosting awaits a confirmation from the Data Services team regarding database and reports completion.
- App Hosting performs any manual steps required for the deployment. These steps are detailed in the release's playbook.

- App Hosting execute the “<environment>” plan which performs the automated portion of the deployment of the release components.
- Upon receiving the email confirmation from the Data Services, App Hosting executes the final plan “<Environment>_Starting_Servers” to clear the server cache and start all the application servers.
- Deloitte and App Hosting validates the application to ensure that the application is accessible.
- App Hosting sends out a communication indicating that deployment is completed.
- DSS business proceeds with validations and sends an email communication upon successful completion.
- Deloitte release management team sends out the final communication to all stakeholders indicating the completion of deployment and validations.

6.2.1.3 *Code Delivery (Deployment Packaging)*

This section outlines the tools used and process followed in managing application source code, releases and deployment across various environments.

Release Deployment Package

The Deployment package contains executables to be deployed, deployment playbook and release notes. Deployment Playbook documents all artifacts pertaining to that release along with the location of artifacts. It also contains the sequence of execution and roll back procedures for each component.

- Release Notes

Release Notes must contain documentation of the Defects and Change Request items in scope of the Release, descriptions of the functionality, and their specific test results, regression test results, and test scripts identified to be added to the regression test suite.

- Deployment Playbook

This playbook must contain the instructions for the specific release version in a spreadsheet with the following tabs: Deployment Steps, Roll Back Steps, Technical Release Notes (steps), Database Steps, Automated Components Validations, Validations, and the Contacts Directory
Deployment playbook along with other release artifacts will be reviewed with Key Stake holders at least 24 hours prior to first deployment in STATE IT environments

- Code Package

Code executables and Scripts delivery must include instructions needed for UAT, STG, and PRD deployments using the Bamboo Software. This is an executable package run through the Bamboo administrative tool.

Tools

Listed below in the table are the tools used for HHS Enterprise Applications development, code delivery, and packaging.

Table 6: Code Development and Deployment Tools

Tool	Description
Subversion (SVN) *	Source version control system
Atlassian Bamboo	Continuous Integration System used in the release management of applications and software
Atlassian JIRA *	Issue/Defect tracking management software
Atlassian FishEye	Software used to search, track, and visualize code changes
Rational Application Developer (RAD)	Integrated Development Environment (IDE) is a tool used by developers for application development

*The below describes the interactions between RAD/IDE, Subversion, and Atlassian JIRA.

- Developer uses RAD IDE with the Subversion or Tortoise SVN plug-ins to check-in/check-out code from the SVN repository.
- Code being checked-in to the SVN repository is tagged to a corresponding JIRA Id. During code check-in commit-plug validates Atlassian JIRA database to ensure that specified JIRA Id is present in JIRA and resolution status is un-resolved.

Bamboo Deployment Plans

Bamboo is currently used for code builds and deployments, and is integrated with SVN, JIRA and FishEye. Listed below are the plans created in Bamboo for HHS Enterprise applications.

Bamboo Plan	Description	Environment
Build	Compiles all merged code from developers and create deployment artifacts	Development
DEV/SIT Deployment	Deploy artifacts to pre-State environments	Development, SIT, Scalability
App Deployment file transfer	Transfer artifacts from pre-State to State MFT server	MFT
App Deployment file transfer	Transfer artifacts from the MFT location to the State Archive location	MFT
<Environment>-Stopping-All-Servers	Stopping all IBM WAS servers and copying deployment package from Archive location the deployment working directory and backup all deployment components	UAT
<Environment>	Deploying all the deployment components	UAT
<Environment>_Starting _Servers	Clearing cache and starting all servers	UAT

Application code is maintained in Sub Version under the following repositories:

- Trunk
  - Logical units of code from developers will be checked in to Trunk.
  - Superset of all codebase for an application.
- Branches
  - A branch is created when there is need for a new release.

  - Starting point of the branch will always be last code release to production.
  - All identified release items will be merged to the Branch and build is deployed to DEV and SIT environments.
- Tags
  - A tag is created on top of production release, and will be used for patches or hot fixes

Following completion of initial development and unit testing, developers check-in code into SVN. During code check-in, developers tag associated JIRA ID for the code change. Bamboo is used for triggering build and deployment of code first to integrated development environment. Status of all JIRA items for that release are now changed to DEV Built. Deployment package is created once the build is tested and verified in development environment. Developers will update status of respective JIRA to SIT Build Ready upon successful validation in integrated development environment. Deployment to SIT environments will be done once development team validates build in integrated development environment. Status of JIRA will be updated to SIT BUILT upon successful deployment into SIT environment. Release notes are updated post completion of SIT validations and Status of JIRA is updated to UAT build ready. Deployment playbook along with other release artifacts will be reviewed with Key Stake holders at least 24 hours prior to first deployment in STATE IT environments. Once reviewed and approved Release is now deployed to test environments hosted in STATE IT regions. Status of JIRA is updated to “UAT Built”. UAT team performs testing in UAT environments and updates Status of the JIRA as per test results. Same deployment package will be used across all environments hosted in DSS. Code gets promoted to staging environment for performance testing, as deemed necessary by DSS. Deployment to Production environment happens once GO/NO GO signoff happens with Key Stake holders of the application.

6.2.1.4 *Change Request Fulfillment*

Approved Change Requests are included in the Deployment Package and undergo the regular SDLC lifecycle and cannot be handled or delivered separately.

6.2.1.5 *Facilitate Go/Nogo Meeting for UAT Deployment*

Hold meeting and/or conference call to discuss the test results and the contents of the deployment package. Decision must be made to move forward with the deployment into UAT.

6.2.1.6 *User Acceptance Testing*

The Test Team performs User Acceptance Testing according to the scope of the code delivery and the associated test scripts. New scripts are created as needed.
The Test Team documents the test results, adds test scripts for all tests required for new functionality in this code delivery, creating new ones when necessary. Regression tests are performed using the Qualatia tool, adding test scripts as necessary for new functionality. Documentation of the regression test results is provided as well.

Table 7: Regression Testing Tool

Tool	Description
Qualatia	Regression testing . Suite of test scripts configured to test functionality of the system in a batch mode.

6.2.1.7 *Performance Testing*

Code releases require performance testing after the User Acceptance Testing has succeeded and been approved for promotion into Production. These tests must be done in Staging, utilizing a database of comparable size and complexity as Production. IBM Rational Performance Tester (RPT) version 8.7 is the current tool for this testing. The test results should always show the comparison to the results from the previous performance test for this code base.

Performance Testing Guide link: **Performance Test Configuration_Deliverable_V_1 0.docx**

The Performance Test Configuration defines the processes and approach to support Load Testing, Stress Testing and Endurance Testing of the application.

The objective of the performance testing exercise is to:

- Define a performance baseline and identify performance constraints.
- Assess whether the application and/or system, as built and deployed, can maintain adequate throughput, satisfactory response, and timely completion of operations under different conditions of volume and stress over a designated period of time.
- Determine points at which Extreme, Load or Operational conditions are likely to cause an application or system failure.

Performance testing is primarily designed for high volume and business critical modules of the application/system. The high level scenarios will be documented in consultation with State IT and the State Business Teams. Performance Test Configuration covers Performance Test Strategy, Performance Test Approach, Performance Test Results, and Reporting. The goal is to determine the responsiveness, throughput, reliability, and scalability of the Application and System Architecture under defined workloads of user and Data Volumes. Assessments are done as to whether the system as built and deployed, can maintain adequate throughput, satisfactory response, and timely completion of business operations (defined in the business specification documents) under different conditions of volume and stress over designated periods of time. Performance testing results are then examined to determine points at which extreme operational or load conditions (breaking points) will cause system failure

Objectives of the performance testing exercises are;

- Define a performance baseline
- Assess the solution's production readiness
- Assess the infrastructure adequacy in terms of capacity and stability
- Evaluate whether the solution performs under mutually agreed performance criteria
- Compare performance characteristics of multiple components that are part of the solution and evaluate their system configurations to enable the entire system as a whole perform under defined performance criteria.
- Find the source of performance bottlenecks and establish system constraints.
- Support system infrastructure tuning and fix performance bottlenecks deploying commercially reasonable effort.

Three major types of tests that will be executed to analyse system performance of ImpaCT Solution

(1) Load Test

(2) Endurance Test

(3) Stress Test

These tests are designed to validate the individual components, system performance between platforms, and their supporting infrastructure. The tests will be conducted in a production-like environment to capture the system's accuracy and scalability prior to key production milestones

Table 8: Performance Test Types

Test Type	Objective
Load Test	Identify system performance during nominal higher than anticipated transaction load to create a system baseline. Load testing will be performed on the solution to validate the behavior of the system under both normal and anticipated peak load conditions. During this process, the response times are captured for selected transactions and pages and the server-side metrics are monitored and captured for further analysis. The purpose of this test is to ensure the system's ability to handle anticipated user loads • Baseline Test – Test performed to measure baseline system performance under low user and data volume • User volume Step Tests – Start at a lower load level, and repeat the tests for increasing load levels • Data volume Step Tests - Start at a lower data load level, increasing data load by steps usually loading more data in a controlled manner.
Endurance Test	Identify system performance at 80-90% of baseline for extended period of time to evaluate resource 'leakage'. Testing will be performed to determine if the solution can sustain (on a continuous basis) longer than expected transaction and user load, volume for a duration of 8-12 hours. During this process, the response times are captured for selected transactions and pages and the server-side metrics are monitored and captured for further analysis. The purpose of this test is to ensure the system remains stable over extended anticipated transaction load and user volume.
Stress Test	Analyze system performance and behavior during continuous and excessive load testing to evaluate system stability and reliability during user volume or transaction load spikes. Stress Testing is performed to analyze the application behavior under higher than anticipated production load (transaction, user volume). Stress testing will help identify potential bottlenecks during peak periods and ensure the solution has the ability to handle unexpected spikes in volumes while maintaining acceptable response times. Stress testing may be able to find true capacity and performance boundaries. This is limited by the by the number of concurrent user licenses in Performance Testing tool (currently: 5000 user license). The current sizing is done on an expected load of 4000 Concurrent users and anticipated CPU Utilization of 70%.

6.2.1.8 *Facilitate Go/Nogo for Production Deployment*

Hold meetings and/or conference calls to discuss the test results from UAT as well as from the Performance Testing and the successful deployment of the package through the State environments. Decision must be made to move forward with the deployment into Production.

6.2.2 Ad-hoc Reporting %

The purpose of Ad-Hoc Reporting is to provide business owners with reporting data that is not included in the canned reports. Each report request is handled as an in-scope item of a release and gets packaged into a deployment.

6.2.3 Reference Table Modifications %

Application server restarts are necessary when reference table values are modified as they are loaded into the server's memory. This requires a rolling restart at a minimum.
If there is a larger modification to the reference tables (i.e. metadata) then the full process for Application Deployment is required.

6.3 Technical (Infrastructure) %

6.3.0.1 *Architecture Management*

Analyze component upgrades and new enhancements/ changes to assure they are in line with the defined architecture for the overall solution.

6.3.0.2 *Vendor Management*

Communicate with and manage resolution of Level 3 support requests that require application or technical support from external vendors (IBM, Adobe, Corticon, Filenet, etc).

6.3.0.3 *Infrastructure Validation*

Infrastructure Sanity check across UAT, Staging and Production environments post go-live (after release deployment is complete)

6.3.0.4 *Data Power Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining all Data Power under WebSphere Application Server environments. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.5 *SSRS Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the SSRS Enterprise System supporting HHS Enterprise applications. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.6 *Informatica Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining Informatica Enterprise System supporting the HHS Enterprise applications. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.7 *CA ESP Scheduler*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining State IT CA ESP Scheduler, and scheduling jobs in support of the HHS Enterprise Applications system. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

Define archiving and purge guidelines for file management which includes managing batch data files securely and scheduling archiving and purge activities

6.3.0.8 *IHS Web Server Administration*

This team is responsible for installing, configuring, and administering the IBM HTTP Server (IHS) within the HHS Enterprise Application system with a strong understanding of its configuration settings. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.9 *IBM Websphere Application Server (WAS) Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the HHS Enterprise application WebSphere Application Server environments. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.10 *WESB Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining HHS Enterprise application WESB and WebSphere Application Server environments. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.11 *Content Management (Filenet)*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the object stores in the State IT FileNet Enterprise System that support the HHS Enterprise Application system. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.12 *Adobe Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the Adobe and WebSphere Application Server environments that support the HHS Enterprise applications. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.13 *Corticon Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the Corticon and WebSphere Application Server environments that support the HHS Enterprise Applications system. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.0.14 *Managed File Transfer (MFT)*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the HHS Enterprise Applications Managed File Transfer system. In addition, this team manages the promotion of code and configuration changes through UAT, STG, and production.

6.3.1 Licensing %

6.3.1.1 *Software License Renewal*

This team monitors the Software Inventory for upcoming expiry of Software Licenses. The Software Licenses need to be renewed on time, in order to meet compliance and avoid error/warning displayed by certain software.

6.3.2 Software Upgrades (COTS Products) %

6.3.2.1 *Patch & Upgrade Management*

Perform routine software patch and application upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.

6.3.2.2 *COTS Release Planning*

Perform release planning for COTS patches and upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.

End of Support life of software purchased will be posted on respective vendor sites. DSS will be notified on all software updates that are available. This team reviews available patches and upgrades and plan for upgrades. The following steps are followed in promoting patches / software upgrades

1) Downloads of the latest software patch/upgrade version and shares appropriate license key for installation
2) Systems Integrator(s) download the patch and installs in lower environments
3) Systems Integrator(s) perform application regression testing in lower environments and present test results to DSS IT PMO

4) Upon review and approval a release schedule and full deployment package is published for promoting changes across State environments

6.3.2.3 *DB2 Administration*

This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the HHS Enterprise Database solution in DB2. In addition, this team manages the promotion of code and configuration changes through the SDLC process.

6.3.3 Hardware Upgrades %

6.3.3.1 *Patch & Upgrade Management*

Perform routine software patch and application upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.

6.3.3.2 *Infrastructure Release Planning*

Perform release planning for Infrastructure patches and upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.

This team reviews new releases documentation. The following steps are followed in deploying new infrastructure releases

1) Downloads the latest release version and shares appropriate license key for installation
2) Systems Integrator(s) download the release and installs in lower environments
3) Systems Integrator(s) perform release regression testing in lower environments and present test results to DSS IT PMO
4) Upon review and approval a release schedule and full deployment package is published for promoting changes across State environments

Planning Outages

a. IT request infrastructure upgrade/patch/performance improvement etc.
b. All stakeholders provide approve (Business, IT)
c. Release Manager/along with SI determines the lower environment migration path which includes SIT/UAT environments
d. UAT performs regression testing and provides approval.
e. Release Manager works with DSS/BEST Support teams to confirm Production upgrade schedule.
f. Go/No-Go provides approval for Production upgrade (Communication, meeting not required)
g. Release Managers creates RFS's for DSS ITS and BEST support team.
h. Release Manager coordinates and communicates periodic updates. Dial In is provided.
i. Release Manager confirms completion of deployment and requests business validations
j. In the event of an issue post deployment, Release Manager initiates a call/creates RFS and gets the required support for problem resolution.

6.3.4 System Start-up and Shutdown %

This section provides an overview of the activities needed to start-up and shutdown the HHS Enterprise applications' infrastructure components. The system start-up and shutdown activities will be executed by system administrators. The administrators can navigate to the system components outlined below and execute the required start-up and shutdown steps for the specific components.

The tables below provide the sequencing of infrastructure components to start-up and shutdown the system.

Startup Sequence

S NO	Application	Start Sequence
1	ImpaCT Online	DB2
2	HHS Administrator Tool	DB2
3	DashBoard	DB2
4	WESB	DB2
5	SSRS	MSSQL DB
6	FileNet	FileNet DB
7	Adobe	Adobe DB
8	ISIM/ISAM	DB servers
9	ImpaCT	App Servers
10	HHS Administrator Tool	App Servers
11	Dashboard	App Servers
12	Corticon	App Servers
13	Adobe	App Servers
14	FileNet	App Servers
15	WESB	App Servers
16	ISIM/ISAM LDAP	LDAP Servers
17	ISIM/ISAM	App Servers

Shut Down Sequence

S NO	Application	Shut Down Sequence
1	ImpaCT	App Servers
2	HHS Administrator Tool	App Servers
3	Dashboard	App Servers
4	Corticon	App Servers
5	Adobe	App Servers
6	FileNet	App Servers
7	WESB	App Servers
8	ISIM/ISAM LDAP	LDAP Servers

9	ISIM/ISAM	App Servers
10	ImpaCT Online	DB2
11	HHS Administrator Tool	DB2
12	DashBoard	DB2
13	WESB	DB2
14	SSRS	MSSQL DB
15	FileNet	FileNet DB
16	Adobe	Adobe DB
17	ISIM/ISAM	DB servers

6.3.5 Data Management %

6.3.5.1 *Data Governance Planning*

This support team must work directly with the business Data Stewards, State IT Data Officer, Chief Security Officer, and the Agency Privacy Officer known here as the Data Governance Team.

Assist the Data Governance Team with the development, review, and approval of Data Policies, Standards and Procedures for DSS, HHS, and Statewide. This also includes classifications of Confidentiality and approvals of Data Architecture.

These duties also include troubleshooting and resolving data related issues from incidents and breaches.

This support team must also monitor & ensure Conformance and Compliance with the above Policies and Standards, Procedures, and Architecture.

6.3.5.2 *Data Refreshes*

The Ad-Hoc databases require automated refreshes. This needs to be monitored for successful completion daily by the batch monitoring teams as they are priority A jobs. In the event of failures, this team needs to support triage, work arounds and/or re-executions, and root cause analysis.

The Melissa Data software used for Address Validation needs renewal and a refresh every 3 months. Lack of renewal results in an error message displayed to end user of the ImpaCT application.

All lower environments need data refreshes. Some are defined as automatic and others are on-demand. This team is responsible for the timely execution of data refreshes. This process also includes data masking procedures.

6.3.5.3 *Definition and Maintenance*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Develop & Maintain the Enterprise Data Model
- Analyze & Align With Other Business Models

- Define & Maintain the Data Technology Architecture
- Define & Maintain the Data Integration Architecture
- Define & Maintain Enterprise Taxonomies
- Define & Maintain the Meta Data Architecture

6.3.5.4 *Data Modeling Analysis and Design*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Analyze Information Requirements
- Develop & Maintain Conceptual, Logical, and Physical Data Models
- Manage Data Model Versioning and Integration

6.3.5.5 *Detailed Data Design*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Design Physical Databases, Related Data Structures, and Data Access Services

6.3.5.6 *Data Implementation*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Create, Maintain, Backup, and Restore: all Test Databases
- Establish Data Masking Migration, and Conversion Procedures for Test Data
- Build & Test Data Access and Data Integration Services

6.3.5.7 *Database Operations Management*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Implement & Maintain Database Environments
- Backup & Recover Data. Online Full Incremental Database backups scheduled before batch cycle starts and after the Online Applications go into “Batch” mode (read only) on working days, daily 6:00 pm. Full online backup every Saturday night. After Database backup is performed, check is performed to ensure DB is not going to quiesce mode
- Plan and Implement Data Recovery Procedures
- Set Database Performance Service Levels
- Monitor & Tune Database Performance
- Plan and Implement Data Retention Procedures
- Archive, Retrieve and Purge Data

- Acquire Externally Sourced Data (if applicable)

6.3.5.8 *Training and Test Data Management*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Define and Implement Training and Test Data Needs
- Control Code Values & Other Reference Data
- Create simulated Training and Test Data
- Establish Golden copy of code and Test data
- Define and Implement Training Data Refresh cycles and Refresh frequency for the Training Environment
- Define and Implement Configuration Process for Test Data Management
- Refresh/Replicate Training Data
- Refresh/Replicate Training and Test Data

6.3.5.9 *Report Data Management*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Implement Reporting Infrastructure and Reporting Database
- Establish and institute methods for synchronizing data from the OLTP to the Reporting Database
- Establish and institute methods for synchronizing data from the OLTP to replica databases, masked databases, and the data warehouse
- Define and Implement Procedure for disseminating and Storing Generate Reports
- Define Standards and Implement Access to Ad-Hoc Reporting Databases

6.3.5.10 *Content Management and Audit*

Application database support for all projects within the HHS Enterprise, responsibilities are to;

- Acquire & Store Documents
- Index Document Information Contents
- Support Document Content Repository DB and File Store Analysis
- Support Document Access, Circulation & Update
- Archive, Retrieve & Purge Documents

6.3.6 Disaster Recovery %

6.3.6.1 *Planning and Management*

Manage the Business continuity planning exercise and disaster recovery management steps that need to be performed in case of any unplanned outages

6.3.6.2 *Backup and Recovery*

Perform routine backup/recovery of the application databases and the overall system repositories, file/object stores, and information required for the functioning of the HHS Enterprise Applications system.

6.3.6.3 *VM Backup*

Perform routine backup/recovery of the all VMs

6.3.6.4 *Files*

Perform routine backup/recovery of the all files that are not included in databases and repositories (Input files, output files, XML files, PS files, Log files, MFT files). The files should be available on request

6.3.7 Performance Management %

6.3.7.1 *Monitoring*

Monitor Application and Database Performance regularly on all the services that constitute the HHS Enterprise Applications System.

This includes but is not limited to;

1. Web & Application servers
2. Corticon servers
3. Adobe servers
4. WESB
5. Database I/O
6. Document Retrieval Performance in Content Management

6.3.7.2 *Testing*

Provide performance testing of applications in the Staging as part of SDLC

6.3.7.3 *Tuning*

Perform performance tuning activities based on application-specific performance analysis conducted and identified performance issues identified in section 6.3.7.1 and from Incidents – section 5.3.

6.4 Security / User Administration

Access to the HHS Enterprise Applications system is governed through user accounts (a unique login for each system user) which are supported by the administration of users and roles.

6.4.1 Account Setup and Maintenance %

6.4.1.1 *Administration.*

This support team is responsible for the setup and maintenance of the Identity Access Maintenance system. There are two administrative software tools necessary to accomplish this;

- The IBM ISIM/ISAM Administrator tool is for account creation, uniquely identifying each user and their course grained ability to access applications in the system. This support team is responsible for the setup and maintenance of the IAM system as well as establishing processes/procedures for adding/modifying/removing users and associated user roles. Find the user guide for the use of this tool at this link: **Security Identity Management Administration_User Guide_v4.0.docx**
- The HHS Administrator Tool is a custom application that currently only supports ImpaCT but is designed to encompass all applications in the HHS Enterprise. This is where the account is assigned roles and permissions to the applications There are two support teams for this tool. The first is the Systems Integrator for the development, setup, and maintenance of the software tool. The second is the administrative support team who are the users of this tool, maintaining rolse and permissions for all application users.

Of note: This pertains to all environments. (The account 'JSmith' can only exist once. There cannot be another 'JSmith' for lower environments)

6.4.1.2 *Coarse-Grain Role Administration*

The course grained login account maintenance is accomplished using the SIM/SAM Administrator's Tool.

The information below summarizes the functionality available within the HHS Enterprise applications to add or modify a user's access or system configuration. These modifications are predicated on the completion of DSS's review/approval process for user additions/modifications.

6.4.1.3 *User Setup and Role Mapping*

The ImpaCT application supports user administration for users with the appropriate roles and access. Currently, the support group with this profile (role and permissions) supports core user administration functionality, including:

- Creating & Modifying User accounts (including password changes)
- Creating & Modifying HHS Support Helpdesk accounts (including password changes)
- Suspending and restoring User Accounts & Security Support Helpdesk accounts
- Adding new users
- Modifying Existing user's ability to access applications
- Removing deactivated users

There are currently 5 Coarse-Grain Roles, any combination of which can be added to a particular user.

- External_ImpaCTUser : This role grants access to the ImpaCT application but specifies the user as being external to DSS.
- DSS_ImpaCTUser : This role grants access to the ImpaCT application for internal users.
- DSS_SharedServicesUser : This role grants access to the HHS Administration Tool application.
- DSS_SecurityAdminGroup : This role grants all administrative functions of SIM / SAM
- DSS_SecuritySupportHelpdesk : This role grants partial administrative functions of SIM / SAM

6.4.1.4 *Fine-Grain Role Administration*

There are three types of Role Configurations: screens, reports and field level. Screen level security governs which role can read and/or edit the data on each screen. Reports level security governs which reports each role can search for and download through the ImpaCT Reports Module. Field Level security governs access to editing particular fields or clicking particular buttons.

Once a need is identified for a role's access to a screen, report or field to be adjusted it will first be approved by the appropriate DSS Business Owner and sent to the USG Help Desk.

The sections below highlight the process to update:

- Screen Based Security
- Report Based Security
- Field Level Security
- Adding a New Role

The tool used for roles and permissions maintenance within the applications is currently named the HHS Administration Tool. Please reference this ImpaCT manual for guidance;

User Administration_User Guide_v4.0.docx

- Modifying Existing user's attributed, including:
  - Role, Office and Unit
- Navigating to the Map Role to Business Functions page to
  - Map current roles to business functions
  - View the Map Role to Business Functions – Summary page

6.4.1.4.1 Screen Based Security

Read-Only and Read/Write access to screens is controlled via the Role permission set up. These permissions can be adjusted via the HHS Administration Tool application.

6.4.1.4.2 Report Based Security

Access to reports is controlled via the Role configurations as well. These permissions can be adjusted via the HHS Administration Tool application.

6.4.1.4.3 Field Level Security

Specific fields within the application have an additional layer of security. Upon receiving approval for a field based change, the support team must initiate a Production Incident which will be triaged and logged.

6.4.1.4.4 Adding a New Role

To support testing of a new role and to keep lower environments in sync with Production, new roles will be added through a DB scripting process rather than through the HHS Administration Tool application.

Upon receiving approval for a field based change, the support team must initiate a Production Incident which will be triaged and logged.

6.4.2 Compliance %

This support team must verify that the HHS Enterprise Applications System is compliant with defined security standards, policies and procedures; meeting all State and Federal requirements and guidelines.

6.4.2.1 *Data Security Management*

- Understand Data Privacy, Confidentiality & Security Needs
- Define Data Privacy & Confidentiality Policies & Standards
- Define Password Standards & Procedures
- Design & Implement Data Security Controls
- Manage Users, Passwords & Group Membership
- Manage Data Access Views
- Manage Data Access Permissions
- Classify Information Confidentiality
- Set data encryption settings in databases, data at rest and data in transit

6.4.2.2 *Audit History*

- Monitor User Authentication & Access Behavior (Guardium)
    - Configure software to meet the monitoring requirements
    - For the ImpaCT application. Link: **ImpaCT Action History - Build_v3.03.docx**
        - An Action History module allows authorized users to see user activity (view or edit) through the ImpaCT application itself
        - ImpaCT screens can be turned on or off for Action History logging through the Build Action History screen as detailed thru that screen's online Page Help

6.4.2.3 *Audit Content Management*

- Monitor document access
- Assist with defining retention policies and configure ECM software
    - Define and establish procedures to archive, retrieve, and purge documents
    - Coordinate with the Data Retention Policies defined in section 6.5

6.4.2.4 *CMS POAMs*

- Complete the Plan Of Action Milestones at the required intervals

- Link: **POAM Plan of Action and Milestones.xlsx**

6.4.2.5 *Data Retention*

- Define and establish procedures to archive, retrieve, and purge data.
- Coordinate with the State Library and Database Support Teams to meet policies, standards, and requirements.

7 Maintenance and Operations Support RACI and Assignment Matrices

7.1 RACI

Table 9: RACI

Operations			Description	Responsible	Accountable To	Consulted	Informed
5.1	**Systems Availability Management**						
	5.1.1	**Application Monitoring**					
		System Health Check	ImpaCT Online Application, Web Services, Message Queues and Database Connectivity.	**App Host**	**PMO IT**	**SI**	**PMO**
			Web Application Server Thread Pool	**App Host**	**PMO IT**	**SI**	**PMO**
			Performance Monitoring of various modules	**DB**	**PMO IT**	**SI**	**PMO**
			Average Response time, JVM heap size and garbage collection Monitoring	**App Host**	**PMO IT**	**SI**	**PMO**
	5.1.2	**Technical (Infrastructure) Monitoring**					
		System Health checks on Infrastructure components	Perform System health checks and monitoring that is done on core infrastructure components, including network, storage components, operating systems, hardware components, database usage, etc.	**App Host**	**PMO IT**	**SI**	**PMO**
			New Relic	**App Host**	**PMO IT**	**SI**	**PMO**
			UpTime	**App Host**	**PMO IT**	**SI**	**PMO**
			Foglight	**DB**	**PMO IT**	**SI**	**PMO**
			SIM/SAM Identity Access	**SIM-SAM**	**PMO IT**	**SI**	**PMO**
			Data Power	**DP**	**PMO IT**	**SI**	**PMO**

			Qradar	**QR**	**PMO IT**	**SI**	**PMO**
			WhatsUp (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			Net Cool (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			Cacti (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			Wireshark (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			Netflow (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			Cisco Transport Manager (Network)	**StateNet**	**PMO IT**	**DSSNet**	**PMO**
			FileNet System Monitor (ECM)	**Filenet**	**PMO IT**	**SI**	**PMO**
			IBM Performance Tool Kit (ECM)	**Filenet**	**PMO IT**	**SI**	**PMO**
		System Health checks on COTS components					
		Other Infrastructure MonitoringTools					
			Filenet	**FileNet**	**PMO IT**	**SI**	**PMO**
		Capacity Monitoring					
			Server memory and CPU status	**App Host**	**PMO IT**	**SI**	**PMO**
			Database I/O and tablespace	**DB**	**PMO IT**	**SI**	**PMO**
	5.1.3	**Communications**	Monitoring metrics must be provided twice weekly for the leadership meeting	**App Host**	**PMO IT**	**SI**	**PMO**
	5.1.4	**Performance Management**					
		Performance Management	Manage the performance standards of the application components	**App Host**	**PMO IT**	**SI**	**PMO**
		Performance Monitoring and Tuning	Conduct infrastructure performance tuning activities that need to be undertaken based on performance analysis conducted and identified performance issues	**App Host**	**PMO IT**	**SI**	**PMO**
5.2	**Batch Management**						

	5.2.1	**Inventory**	Maintain and manage the batch job inventory and the sequence	**SI**	**PMO IT**	**SME**	**PMO**
	5.2.2	**Schedule / Calendar**					
			Maintain and manage the Batch Calendar	**SI**	**PMO IT**	**SME**	**PMO**
			Maintain and manage the Batch Schedule	**Oper**	**SI**	**PMO IT**	**PMO**
	5.2.3	**Monitoring**					
		Batch Monitoring	Monitor the start and successful completion of batch jobs, reporting on batch job errors and utilizing notification and escalation mechanisms, routing relevant tickets to Level 2 support and higher as needed. See section 5.2.7. Tool used currently is CA ESP 7.	**Oper**	**SI**	**PMO IT**	**PMO**
			If any Batch Job aborts (fails), Batch **OPER**ation support team is alerted by the Batch scheduler (CA-ESP). This issue needs to be triaged and support teams need to contacted if needed see section 5.2.7.	**Oper**	**SI**	**PMO IT**	**PMO**
	5.2.4	**Manual Execution**	Execution of a batch job manually	**Oper**	**SI**	**PMO IT**	**PMO**
	5.2.5	**Batch Validation & Data Correction**					
			A log must be kept showing the activities that were performed for each batch cycle. Details of any exceptions must be documented and the Incident Management steps must be followed for all incidents.	**SI**	**Oper**	**PMO IT**	**PMO**
	5.2.6	**Reporting**					
			Assure all batch reports are generated	**SI**	**PMO IT**	**Oper**	**PMO**
			Triage all batch failures or issues and resolve immediately if possible. If not, refer to section 5.2.7.	**SI**	**PMO IT**	**App Host**	**PMO**
	5.2.7	**Emergency Procedures**		**SI**	**PMO IT**	**Oper**	**PMO**
			Commmunications to the SI, enter incident ticket in Footprints	**Oper**	**SI**	**PMO IT**	**PMO**
			Create JIRA ticket and coordinate call bridge for triage	**SI**	**PMO IT**	**Oper**	**PMO**

5.3	**Incident Management / Resolution**						
	5.3.1	**Help Desk Incident Escalation Structure**	Establishes and implement help desk support guidelines and principles. Define procedures and standards for support of incident management and resolution.	**PMO IT**	**PMO**	**SI**	**PMO**
			Establish mechanisms in the helpdesk system to generate reports to track efficiency of the help desk process.	**PMO IT**	**PMO**	**SI**	**PMO**
	5.3.2	**Help Desk Ticketing Systems and Tracking**	Establish, implement, and maintain ticketing systems. Implement procedures to cross reference between systems until full integration or single-system design gets designed and deployed.	**PMO IT**	**PMO**	**SI**	**PMO**
		Define incident severity	Categorize incidents by their impact to the functionality of the application. Use this definition to determine the response as far as priority.	**HD1 HHS**	**PMO IT**	**CCB**	**PMO**
	5.3.3	**Help Desk Level 1 Support**					
		HHS Worker encounters an incident	Receive help desk call. Confirm the incident requires IT support and attempt to recreate it if possible. Resolve the issue if possible (i.e. reset password). If not, work with the supervisor on gathering screen shots, further explanations of what steps were followed to get the error or issue, and any other helpful information. Escalated to the level 2 suppor if necessary.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**
			Receive call from level 1 support to create ticket for State (non SI) level 2 support. Assign ticket to the Level 2 support teams accordsing to the details of the ticket.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**

			Provide real time / Conference bridge support for the level 2 incident analysis. Provide communications with the users.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**
		HHS Client encounters an incident	Receive call from Client help desk support. Confirm the incident requires IT support and attempt to recreate it if possible. Resolve the issue if possible (i.e. reset password). If not, work with the Client help desk on gathering screen shots, further explanations of what steps were followed to get the error or issue, and any other helpful information. Escalated to the level 2 suppor if necessary.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**
			Receive call from level 1 support to create ticket for State (non SI) level 2 support. Assign ticket to the Level 2 support teams accordsing to the details of the ticket.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**
			Provide real time / Conference bridge support for the level 2 incident analysis. Provide communications with the users.	**HD1 HHS**	**PMO IT**	**PMO IT**	**PMO**
		Unsuccessful System Health Checks					
			Review of health check tools and testing logins every day. Escalate according to incident type.	**HD1**	**PMO IT**	**PMO IT**	**PMO**
			Review health check tools and examine automated notifications Escalate according to incident type.	**HD2**	**PMO IT**	**PMO IT**	**PMO**
		Incident from Batch process			**PMO IT**	**PMO IT**	**PMO**
			Monitor and respond to Batch incidents according to the documentation in the Batch Calendar	**Oper**	**PMO IT**	**PMO IT**	**PMO**
	5.3.4	**Help Desk Level 2 Support**					

		Infrastructure	Triage incident.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Return application to fully functional status	**HD2**	**PMO IT**	**HD1**	**PMO**
			Engage other supprt teams as necessary.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Provide conference bridge and contact all support teams required.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Contact level 1 support when testing and validations are required.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Provide root cause analysis. Escalate as necessary and track progress. Document results. Create any follow up tickets required.	**HD2**	**PMO IT**	**HD1**	**PMO**
		Application	Triage incident.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Return application to fully functional status	**HD2**	**PMO IT**	**HD1**	**PMO**
			Engage other supprt teams as necessary.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Provide conference bridge and contact all support teams required.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Contact level 1 support when testing and validations are required.	**HD2**	**PMO IT**	**HD1**	**PMO**
			Provide root cause analysis. Escalate as necessary and track progress. Document results. Create any follow up tickets required.	**HD2**	**PMO IT**	**HD1**	**PMO**
	5.3.5	**Help Desk Level 3 Support**					
		SME support	Assist with incident triage. Examine all documentation (ticket contents, logs, etc)	**HD3**	**PMO IT**	**HD2**	**PMO**
			Assist with returning application to fully functional status	**HD3**	**PMO IT**	**HD2**	**PMO**
			Participate with the conference bridge.	**HD3**	**PMO IT**	**HD2**	**PMO**

			Provide assistance with root cause analysis. Document results.	**HD3**	**PMO IT**	**HD2**	**PMO**
			Triages and analyzes infrastructure related incidents. Remediates and validates infrastructure issues. Communicates status of infrastructure related incident triage. Escalates to Level 3a support as needed.	**HD3**	**DSS**	**PMO IT**	**PMO**
			Triages and analyzes service, product related incidents. Remediates and validates service, product related issues. Communicates status of service, product related incident triage.	**HD3**	**HD3**	**PMO IT**	**PMO**
	5.3.6	**Help Desk Level 3a Support**					
		COTS support	Examine/triage the ticket's contents and all sent documentation (ticket contents, logs, screen shots, etc)	**HD3a**	**PMO IT**	**HD2**	**PMO**
			Join conference bridge if it is held.	**HD3a**	**PMO IT**	**HD2**	**PMO**
			Assist with getting the application fully functional if it is not.	**HD3a**	**PMO IT**	**HD2**	**PMO**
			Assist with determining root cause of the incident	**HD3a**	**PMO IT**	**HD2**	**PMO**
			Coordinate with HD3 team for business user tests and validations of the resolution	**HD3a**	**DSS**	**PMO IT**	**PMO**
	5.3.7	**Incident Escalation Contact List**	This represents the roles for maintaining this list within this document.	**PMO IT**	**PMO**	**HD1,2,3**	**SME**

Maintenance							
6.1	**Deployment Management**						
	6.1.0	**Admin**					
		Stakeholder Management	Managing the stakeholder register for all HHSed components of the HHS System and Platform and notifying stakeholders of planned and ad-hoc activities	**Rel Mgr**	**PMO IT**	**PMO IT**	**PMO**
	6.1.1	**Release Management**					
		Release Planning	Perform release planning for application release versions, patches, and upgrades. This requires coordination with infrastructure team.	**App Host**	**PMO IT**	**PMO IT**	**PMO**
		Release readiness	Finalizing Release Schedule and obtaining signoff from all stakeholders on Release readiness.	**Rel Mgr**	**PMO IT**	**PMO IT**	**PMO**
		Emergency Release	Release Planning and Stakeholder notification for emergency releases	**Rel Mgr**	**Rel Mgr**	**PMO IT**	**PMO**
		Release sign-off	Business User Validation and sign-off post release deployment	**SME**	**Rel Mgr**	**PMO IT**	**PMO**

		Post Release Communication	The HHS Release manager publishes Completion of Deployment Communication to all DSS IT stakeholders, DSS Technical Manager, State Technical teams involved, and HHS PMO, which includes: • The summary of Change as per the Functional Release Note. • Completion time of Deployment • Support Contact information Thereafter, DSS Technical Manager, in consultation with "DSS User Support Group (USG)", communicates to all stakeholders including business users of HHS, if and as necessary. When the target environment is Production, the Deployment is a sub-set of an overall Release Process that needs various additional communication as defined in the section "3.0 Communications" of the "HHS Implementation Plan Deliverable".	**Rel Mgr**	**PMO IT**	**PMO IT**	**PMO**
	6.1.2	**Backup / Restore**					
6.2	**Application**						
	6.2.0	**Admin**					
		Architecture Management	Analyze application break fix changes to assure they are in line with the defined architecture for the overall solution as related to L2, 3 incidents	**PMO IT**	**PMO**	**App Host**	**PMO**
		System Patch and Upgrades Management	Perform production deployment activities for all code releases based on packages developed by Systems Integrators and technical support teams.	**App Host**	**PMO IT**	**PMO IT**	**PMO**

	6.2.1	**Application Releases**	Follow State of Connecticut SDLC Process				
		Perform SIT tests	Provide results in the Release Notes	**SI**	**PMO**	**Test**	**PMO**
		Triggering a Deployment	As part of the Release and Deployment process, a JIRA ticket is created with the attached Playbook relative to the release. The deployment package is uploaded to the MFT server and an email is sent to the client providing all relevant information (Release#, Package location, and components being deployed) pertaining to the deployment.	**SI**	**PMO IT**	**Rel Mgr**	**PMO**
		Code Delivery (Deployment Package)					
			Release Notes must contain documentation of the Defects and Change Request items in scope of the Release, descriptions of the functionality, and their specific test results, regression test results, and test scripts identified to be added to the regression test suite.	**SI**	**PMO**	**Test**	**PMO**
			Deployment playbook must contain the instructions for the specific release version in a spreadsheet with the following tabs: Deployment Steps, Roll Back Steps, Technical Release Notes (steps), Database Steps, Automated Components Validations, Validations, and the Contacts Directory	**SI**	**PMO**	**Test**	**PMO**
			Code and Scripts delivery must include instructions needed for UAT, STG, and PRD deployments using the Bamboo software. Provide Release Notes containing	**SI**	**PMO**	**Test**	**PMO**
		Change Request Fulfillment	Approved Change Requests are included in the Deployment Package and undergo the regular SDLC lifecycle.	**Test**	**PMO IT**	**CCB**	**PMO**
		Facilitate Go/NoGo for UAT	Approves Deployment Package for deployment into UAT	**PMO**	**PMO IT**	**SI**	
		User Acceptance Testing	Provide Results to the Project Support Teams	**Test**	**PMO**	**SI**	
			Conduct UAT for new break fixes done by the M&O team for L2/3 incidents. This also covers the regression testing during UAT that needs to be performed on impacted components	**Test**	**PMO**	**SME**	**PMO**
		Performance Testing	Execute performance tests and provide comparison results with the last Major Release's results.	**PerfAdmin**	**PMO IT**	**Test**	**PMO**

			Administer and configure the IBM RPT tool.	**PerfAdmin**	**PMO IT**	**Test**	**PMO**
			Creates, edits, and executes test scenarios by recording interactions with the application. Inspects results after recording test scripts and adjusts the test scenarios as needed.	**PerfTest**	**PMO IT**	**Test**	**PMO**
		Facilitate Go/NoGo for Production	Approves Deployment Package for deployment into Production	**PMO**	**HHS EC**	**PMO IT**	**PMO**
	6.2.2	**Ad-hoc reporting**					
	6.2.3	**Reference Table Modifications**	Application server restarts. Necessary when reference tables are modified as they are loaded into the server's memory.	**App Host**	**PMO IT**	**SI**	**PMO**
6.3	**Technical (Infrastructure)**						
	6.3.0	**Admin**					
		Architecture Management	Analyze component upgrades and new enhancements/ changes to assure they are in line with the defined architecture for the overall solution	**SI**	**PMO IT**	**PMO IT**	**PMO**
		Vendor Management	Communicate with and manage resolution of Level 3 support requests that require application or technical support from external vendors like IBM.	**HD2**	**PMO IT**	**PMO IT**	**PMO**
		Infrastructure Validation	Infrastructure Sanity check across UAT, Staging and Production environments post go-live (after release deployment is complete)	**App Host**	**Rel Mgr**	**PMO IT**	**PMO**
		Data Power Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various Data Power and WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**DP**	**PMO IT**	**PMO IT**	**PMO**

		SSRS Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining SSSRS Enterprise System. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**DB**	**PMO IT**	**SI**	**PMO**
		Informatica Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining Informatica Enterprise System. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**Inform**	**PMO IT**	**SI**	**PMO**
		CA ESP Scheduler	Responsible for evaluating, installing, upgrading, configuring, and maintaining CA ESP Scheduler, and scheduling jobs. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**OPER**	**PMO IT**	**SI**	**PMO**
			Define the archiving and purge guidelines for file management. This also includes managing batch data files securely and scheduling archiving and purge activities	**PMO IT**	**SME**	**CSO**	**PMO**
		IHS Web Server Administrator	Responsible for installing, configuring, and administering IBM HTTP Server (IHS) with a strong understanding of its configuration settings. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**
		IBM WebSphere Application Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**

		WESB Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various WESB and WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**
		WESB Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various WESB and WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**
		FileNet Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining FileNet Enterprise System. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**FileNet**	**PMO IT**	**SI**	**PMO**
		Adobe Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various Adobe and WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**
		Corticon Administrator	Responsible for evaluating, installing, upgrading, configuring, and maintaining various Corticon and WebSphere Application Server environments. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**App Host**	**PMO IT**	**SI**	**PMO**
		Managed File Transfer MFT					
	6.3.1	**Licensing**					
		Software License Renewal	The Software Inventory needs be monitored periodically for upcoming expiry of Software Licenses. The Software Licenses need to be renewed on time, in order to meet compliance and avoid error/warning displayed by certain software.	**Inventory**	**PMO IT**	**SI**	**PMO**

	6.3.2	**Software Upgrades (COTS Products)**					
		System Patch and Upgrades Management	Perform routine software patch and application upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.	**App Host**	**PMO IT**	**SI**	**PMO**
		COTS Release Planning	Perform release planning for COTS patches and upgrades. T Coordinate support teams. Schedule with the Release Manager and PMO..	**Rel Mgr**	**PMO IT**	**SI**	**PMO**
		DB2 - Administrator	This team is responsible for evaluating, installing, upgrading, configuring, and maintaining the HHS Enterprise Database solution in DB2. In addition, this team manages the promotion of code and configuration changes through the SDLC process.	**DB**	**PMO IT**	**SI**	**PMO**
	6.3.3	**Hardware Upgrades**					**PMO**
		System Patch and Upgrades Management	Perform routine software patch and application upgrades. Coordinate support teams. Schedule with the Release Manager and PMO.	**App Host**	**PMO IT**	**SI**	**PMO**
		Release Planning	Perform release planning for infrastructure patches and upgrades. T Coordinate support teams. Schedule with the Release Manager and PMO..	**Rel Mgr**	**PMO IT**	**SI**	**PMO**
	6.3.4	**System Start-up and Shutdown**					
			Execute System Shut Down (ImpaCT)	**App Host**	**PMO IT**	**SI**	**PMO**
			Execute System Start Up (ImpaCT)	**App Host**	**PMO IT**	**SI**	**PMO**
			Modify System Shut Down/Start Up Procedures	**App Host**	**PMO IT**	**SI**	**PMO**
			Execute System Shut Down (EMPI)	**App Host**	**PMO IT**	**SI**	**PMO**
			Execute System Start Up (EMPI)	**App Host**	**PMO IT**	**SI**	**PMO**
			Modify System Shut Down/Start Up Procedures	**App Host**	**PMO IT**	**SI**	**PMO**
	6.3.5	**Data Management**					
		Data Governance Planning	Identify Data Stewards who control the use and definition of business data	**SME**	**PMO**	**CSO**	**PMO IT**

			Identify State IT Data Officer to manage Data Management Functions	**SME**	**PMO**	**CSO**	**PMO IT**
			Identify DSS Data Officer to manage Data Management Functions	**SME**	**PMO**	**CSO**	**PMO IT**
			Develop, Review, Approve Data Policies, Standards and Procedures	**CSO**	**PMO**	**SME**	**PMO IT**
			Classify Information Confidentiality	**CSO**	**PMO**	**SME**	**PMO IT**
			Review and Approve Data Architecture	**CSO**	**PMO**	**SME**	**PMO IT**
			Coordinate Data Governance Activities	**CSO**	**PMO**	**SME**	**PMO IT**
			Manage & Resolve Data Related Issues	**CSO**	**PMO**	**SME**	**PMO IT**
			Monitor & Ensure Regulatory Compliance	**CSO**	**PMO**	**SME**	**PMO IT**
			Monitor Conformance with Data Policies, Standards and Architecture	**CSO**	**PMO**	**SME**	**PMO IT**
		Data refreshes	The Melissa Data software used for Address Validation need renewal and refresh every 3 months. Lack of renewal, Error message is displayed to end user of ImpaCT application	**DB**	**PMO IT**	**SI**	**PMO**
		Definition and Maintenance	Develop & Maintain the Enterprise Data Model	**SI**	**PMO IT**	**DB**	**PMO**
			Analyze & Align With Other Business Models	**SI**	**PMO IT**	**DB**	**PMO**
			Define & Maintain the Data Technology Architecture	**SI**	**PMO IT**	**DB**	**PMO**

			Define & Maintain the Data Integration Architecture	**SI**	**PMO IT**	**DB**	**PMO**
			Define & Maintain Enterprise Taxonomies	**SI**	**PMO IT**	**DB**	**PMO**
			Define & Maintain the Meta Data Architecture	**SI**	**PMO IT**	**DB**	**PMO**
		Data Modeling Analysis and Design	Analyze Information Requirements	**SI**	**PMO IT**	**DB**	**PMO**
			Develop & Maintain Conceptual Data Models	**SI**	**PMO IT**	**DB**	**PMO**
			Develop & Maintain Logical Data Models	**SI**	**PMO IT**	**DB**	**PMO**
			Develop & Maintain Physical Data Models	**SI**	**PMO IT**	**DB**	**PMO**
			Manage Data Model Versioning and Integration	**SI**	**PMO IT**	**DB**	**PMO**
		Detailed Data Design	Design Physical Databases	**SI**	**PMO IT**	**DB**	**PMO**
			Design Related Data Structures	**SI**	**PMO IT**	**DB**	**PMO**
			Design Data Access Services	**SI**	**PMO IT**	**DB**	**PMO**
		Data Implementation	Create, Maintain, Backup, and Restore: Test and Training Databases	**SI**	**PMO IT**	**DB**	**PMO**
			Establish Data Masking Migration, and Conversion Procedures for Test Data	**SI**	**PMO IT**	**DB**	**PMO**
			Build & Test Data Access and Data Integration Services	**SI**	**PMO IT**	**DB**	**PMO**

		Database Operations Management	Implement & Maintain Database Environments	**DB**	**PMO IT**	**SI**	**PMO**
			Acquire Externally Sourced Data (if applicable)	**DB**	**PMO IT**	**SI**	**PMO**
			Plan and Implement Data Recovery Procedures	**DB**	**PMO IT**	**SI**	**PMO**
			Backup & Recover Data	**DB**	**PMO IT**	**SI**	**PMO**
			Set Database Performance Service Levels	**SI**	**PMO IT**	**DB**	**PMO**
			Monitor & Tune Database Performance	**SI**	**PMO IT**	**DB**	**PMO**
			Plan and Implement Data Retention Procedures	**DB**	**PMO IT**	**SI**	**PMO**
			Archive, Retrieve and Purge Data	**DB**	**PMO IT**	**SI**	**PMO**
			Online Full Incremental Database backups scheduled before batch cycle starts and after the ImpaCT Online Application goes into “Batch” mode (read only) on working days, daily 6:00 pm. Full online backup every Saturday night. After Database backup is performed, check is performed to ensure DB is not going to quiesce mode.	**DB**	**PMO IT**	**SI**	**PMO**
		Training and Test Data Management	Define and Implement Training and Test Data Needs	**DB**	**PMO IT**	**SI**	**PMO**
			Control Code Values & Other Reference Data	**DB**	**PMO IT**	**SI**	**PMO**
			Create simulated Training and Test Data	**Test**	**DB**	**SI**	**PMO IT**

			Establish Golden copy of code and Test data	**Test**	**DB**	**SI**	**PMO IT**
			Define and Implement Training Data Refresh cycles and Refresh frequency for the Training Environment	**Test**	**DB**	**SI**	**PMO IT**
			Define and Implement Configuration Process for Test Data Management	**Test**	**DB**	**SI**	**PMO IT**
			Refresh/Replicate Training and Test Data	**DB**	**Test**	**SI**	**PMO IT**
		Report Data Management	Implement Reporting Infrastructure and Reporting Database	**DB**	**PMO IT**	**SI**	**PMO**
			Establish and institute methods for synchronizing data from the OLTP to the Reporting Database	**DB**	**PMO IT**	**SI**	**PMO**
			Establish and institute methods for synchronizing data from the OLTP to replica databases, masked databases, and the data warehouse	**DB**	**PMO IT**	**SI**	**PMO**
			Define and Implement Procedure for disseminating and Storing Generate Reports	**DB**	**PMO IT**	**SI**	**PMO**
			Define Standards and Implement Access to Ad-Hoc Reporting Databases	**DB**	**PMO IT**	**SI**	**PMO**
		Content Management and Audit	Acquire & Store Documents	**SI**	**PMO IT**	**Filenet**	**PMO**
			Index Document Information Contents	**SI**	**PMO IT**	**Filenet**	**PMO**
			Support Document Content Repository Analysis	**SI**	**PMO IT**	**Filenet**	**PMO**
			Support Document Access, Circulation & Update	**SI**	**PMO IT**	**Filenet**	**PMO**
			Archive, Retrieve & Purge Documents	**SI**	**PMO IT**	**CSO**	**Filenet**

	6.3.6	**Disaster Recovery**					
		Disaster Recovery Planning & Management	Manage the Business continuity planning exercise and disaster recovery management steps that need to be performed in case of any unplanned outages	**DB**	**PMO IT**	**DBA**	**PMO**
		DB Backup/Recovery	Perform routine backup/recovery of the application databases and the overall system repositories, file/object stores, and information required for the functioning of the HHS Enterprise Applications system	**DB**	**PMO IT**	**DBA**	**PMO**
		VM Backup	Perform routine backup/recovery of the all VMs	**App Host**	**PMO IT**	**PMO IT**	**PMO**
		File Backup	Perform routine backup/recovery of the all files that are not included in databases and repositories (Input files, output files, XML files, PS files, Log files, MFT files). The files should be available on request.	**MFT**	**PMO IT**	**PMO IT**	**PMO**
		Content Management	Backup & Recover Documents	**Filenet**	**PMO IT**	**SI**	**PMO**
	6.3.7	**Perfomance Management**					
		Monitoring	Monitor & Tune Database Performance for applications and services that constitute the HHS Enterprise Applications System.	**SI**	**PMO IT**	**DBA**	**PMO**
			Monitor & Tune Document Retrieval Performance in Content Management	**SI**	**PMO IT**	**Filenet**	**PMO**
		Testing	Provide performance testing of applications in the Staging as part of SDLC	**PerfTest**	**PMO IT**	**PerfAdmin**	**PMO**
		Tuning	Perform performance tuning activities based on application-specific performance analysis conducted and identified performance issues	**PerfAdmin**	**PMO IT**	**SI**	**PMO**
	6.3.8	**Connectivity**	Test for linked object				
6.4	**Security / User Admin**						
	6.4.1	**Account Setup and Maintenance**					

		Administration	Responsible the setup and maintenance of the IAM system. Including creating users and providing appropriate access to the ISIM/ISAM system. In addition, manage the promotion of code and configuration changes through UAT, STG, and production.	**SIM-SAM**	**PMO IT**	**SI**	**PMO**
			Establish and operate processes/procedures for adding/modifying/removing users and associated user roles in the system (including both SIM/SAM and within the ImpaCT Application).	**SIM-SAM**	**SME**	**SI**	**PMO**
		Coarse-Grain Role Administration	Course Grained Security User and Role Management	**HD1**	**SME**	**SI**	**PMO**
		Fine-Grain Role Administration					
	6.4.2	**Compliance**					
			Verify that the application and related components are compliant with defined security standards (as per approved design)	**SI**	**PMO IT**	**CSO**	**PMO**
		Data Security Management	Understand Data Privacy, Confidentiality & Security Needs	**SI**	**PMO IT**	**CSO**	**PMO**
			Define Data Privacy & Confidentiality Policies & Standards	**SI**	**PMO IT**	**CSO**	**PMO**
			Define Password Standards & Procedures	**SI**	**PMO IT**	**CSO**	**PMO**
			Design & Implement Data Security Controls	**SI**	**PMO IT**	**CSO**	**PMO**
			Manage Users, Passwords & Group Membership	**SI**	**PMO IT**	**CSO**	**PMO**
			Manage Data Access Views	**SI**	**PMO IT**	**CSO**	**PMO**
			Manage Data Access Permissions	**SI**	**PMO IT**	**CSO**	**PMO**
			Classify Information Confidentiality	**SI**	**PMO IT**	**CSO**	**PMO**
			Set data encryption settings in databases, data at rest and data in transit	**SI**	**PMO IT**	**CSO**	**PMO**
		Audit history configuration	Monitor User Authentication & Access Behavior (Guardium)	**Guard**	**PMO IT**	**CSO**	**PMO**
			Monitor QRadar for errors, warnings, and anomalies	**QR**	**PMO IT**	**CSO**	**PMO**
		Content Management and Audit	Audit Document & Content Management	**Filenet**	**PMO IT**	**CSO**	**PMO**

			Archive, Retrieve & Purge Documents	**Filenet**	**PMO IT**	**CSO**	**PMO**
		CMS POAMS	Complete the Plan Of Action Milestones at the required intervals	**CSO**	**PMO IT**	**SI**	**PMO**
		Data Retention	Archive, Retrieve & Purge Data	**DB**	**PMO IT**	**CSO**	**PMO**
			Adherence to State and Federal policies and requirements	**CSO**	**PMO IT**	**SI**	**PMO**

7.2 Support Role Assignments

Table 10: Support Role Assignments

Role		Assignments	Effective Date	Phone	email	After business hours
HHS EC	HHS Executive Committee	Joe Stanford, Janel Simpson,	1/1/2018	860-424-5121	Joe.Stanford@ct.gov;	
PMO	Project Management Office	ImpaCT(Matthew Robertson, Andrea Alfano, Saul Mora); EMPI(Minakshi Tikoo, Justin Cozzens, Tia Tinney)	1/1/18 (ImpaCT, EMPI)			
PMO PD	Project Director	Matthew Robertson(ImpaCT); Minakshi Tikoo(EMPI)	1/1/18 (ImpaCT, EMPI)	Matt 860-424-5811; Minakshi 860-424-5209	Matthew.Robertson@ct.gov Minakshi.Tikoo@ct.gov	Matt 860-263-1705; Minakshi 860-424-5209

SME	Project Manager of Application Business Subject Matter Experts	Andrea Alfano (ImpaCT); Tia Tinney(EMPI)	1/1/18 (ImpaCT, EMPI)	Andrea 860-424-5561; Tia 502-321-3343	Andrea.Alfano@ct.gov; Tia.Tinney@ct.gov	Andrea 860-263-1706; Tia 502-321-3343
PMO IT	IT Project Manager	Saul Mora(Impact, EMPI)	1/1/2018	860-424-5369	Saul.Mora@ct.gov	
CCB	Change Control Board	ImpaCT(Matthew Robertson, Andrea Alfano, Saul Mora); EMPI(Minakshi Tikoo, Justin Cozzens, Tia Tinney)	1/1/18 (ImpaCT, EMPI)			
SI	Systems Integrator	Deloitte-Raama Mani(ImpaCT); NextGate-Justin Cozzens(EMPI)	1/1/18 (ImpaCT, EMPI)	Raama 512-226-4406; Justin	Raamakrishnan.Mani@ct.gov; Justin.cozzens@nextgate.com	
App Host	Application Hosting	Naren Nandy(non-EMPI); CMA-Judy Borrmann(EMPI)	1/1/18 (ImpaCT, EMPI)	Naren 860-622-2515; CMA 518-649-4343	Naren.Nandy@ct.gov; jborrmann@cma.com	Naren 860-622-2515; CMA 518-649-4343

DB	Database	Siva Madduri(non-EMPI); CMA-Judy Borrmann(EMPI)	1/1/18 (ImpaCT, EMPI)	Siva ; CMA 518-649-4343	Siva.Madduri@ct.gov; jborrmann@cma.com	Naren 860-622-2515; CMA 518-649-4343
DBA	Database Administration	Avinash (non-EMPI); NextGate-Justin Cozzens(EMPI)	1/1/18 (ImpaCT, EMPI)	Avinash 860-424-5196; Justin	Avinash.Sajja@ct.gov; Justin.cozzens@nextgate.com	
Rel Mgr	Release Management	Sony George Chandy	1/1/2018		Fnu.Sony.George.Chandy@ct.gov	
StateNet	Statewide Network Connectivity and Security	Gerard Johnson	1/1/2018	860-622-2355	Gerard.Johnson@ct.gov	860-622-2300 option 9
DSSNet	Agency Network Connectivity and Security	Vatsal Desai	1/1/2018	860-424-5414	Vatsal.Desai@ct.gov	860-424-4949

F5	F5 Load Balancing	Vamshi Challa	1/1/2018	860-622-2995	Vamshi.Challa@ct.gov	860-622-2300 option 9
SIM-SAM	Security: Identity and System Accounts Management	Lighthouse	1/1/2018			
AcctAdmin	Accounts Administration	USG(Lucy Alzugary, Mark Greene, Christina Raimondi)	1/1/2018	860-424-4949	ImpaCT.Helpdesk.DSS@ct.gov	860-424-4949
DP	DataPower	Lighthouse	1/1/2018			
HD1	Helpdesk Level 1	DSS USG (business hours); BEST Helpdesk (after hours)	1/1/2018	860-424-4949; 860-622-2300 opt 9	ImpaCT.Helpdesk.DSS@ct.gov; BEST.Helpdesk@ct.gov	860-424-4949; 860-622-2300 opt 9
HD2	Helpdesk Level 2	**AH; SI; CMA; App Host; DB; DBA;** etc.	1/1/2018			

HD3	Helpdesk Level 3	Applicable Product Support Vendor (IBM, Miscrodoft, Adobe, Filenet, Nextgate, etc)	1/1/2018			
Oper	Operators	Paul O'Flaherty; **SI**	1/1/2018	860-622-2468	Paul.O'Flaherty@ct.gov	860-622-2300 option 9
Test	Application Testing	Lorrie Taylor	1/1/2018	860-263-1825	Lorrie.Taylor@ct.gov	860-263-1825
PerfAdmin	Performance Testing Administrator	Deloitte	1/1/2018			
PerfTest	Performance Tester	Deloitte	1/1/2018			
MFT	Managed File Transfer	Will Spigel, Warren Lundquist, Vatsal Desai, John Garvin, Eric Morneau	1/1/2018			
Filenet	Filenet Document Management, Workflow, and Records Manager support	Gary Clauss, Marco Incorvaia, Mayur Sangoi	1/1/2018	860-622-2477, 860-622-2287	gary.clauss@ct.gov, Marco.Incorvaia@ct.gov.DOIT, mayursangoi@fairfaxdatasystems.com	860-622-2300 option 9

FW	Firewall & Security	Andy Vincens	1/1/2018	860-622-2463	Andrew.Vincens@ct.gov	860-622-2300 option 9
MFA	Symantec Multi Factor Authentication		1/1/2018			
CSO	Chief Security Officer	Brian Edwards	1/1/2018	860-424-5412	Brian.Edwards@ct.gov	
QR	Qradar	Mark Donahue	1/1/2018	860-622-2181	Mark.Donahue@ct.gov	860-622-2300 option 9
TW	TripWire	Mark Donahue	1/1/2018	860-622-2181	Mark.Donahue@ct.gov	860-622-2300 option 9
Guard	Guardium	Mark Donahue	1/1/2018	860-622-2181	Mark.Donahue@ct.gov	860-622-2300 option 9
Inform	Informatica		1/1/2018			
Inventory	Software, Hardware, Certificate, and License Tracking	Beth Schroeder	1/1/2018	860-424-5474	Beth.Schroeder@ct.gov	n/a

8 Overview of the Technical Architecture

The HHS Enterprise Applications System solution is designed for future growth and expansion as the state's needs evolve. Figure 1 illustrates the key technology components and interactions of the HHS solution that ensures all the functionalities with the HHS solution functions as required.

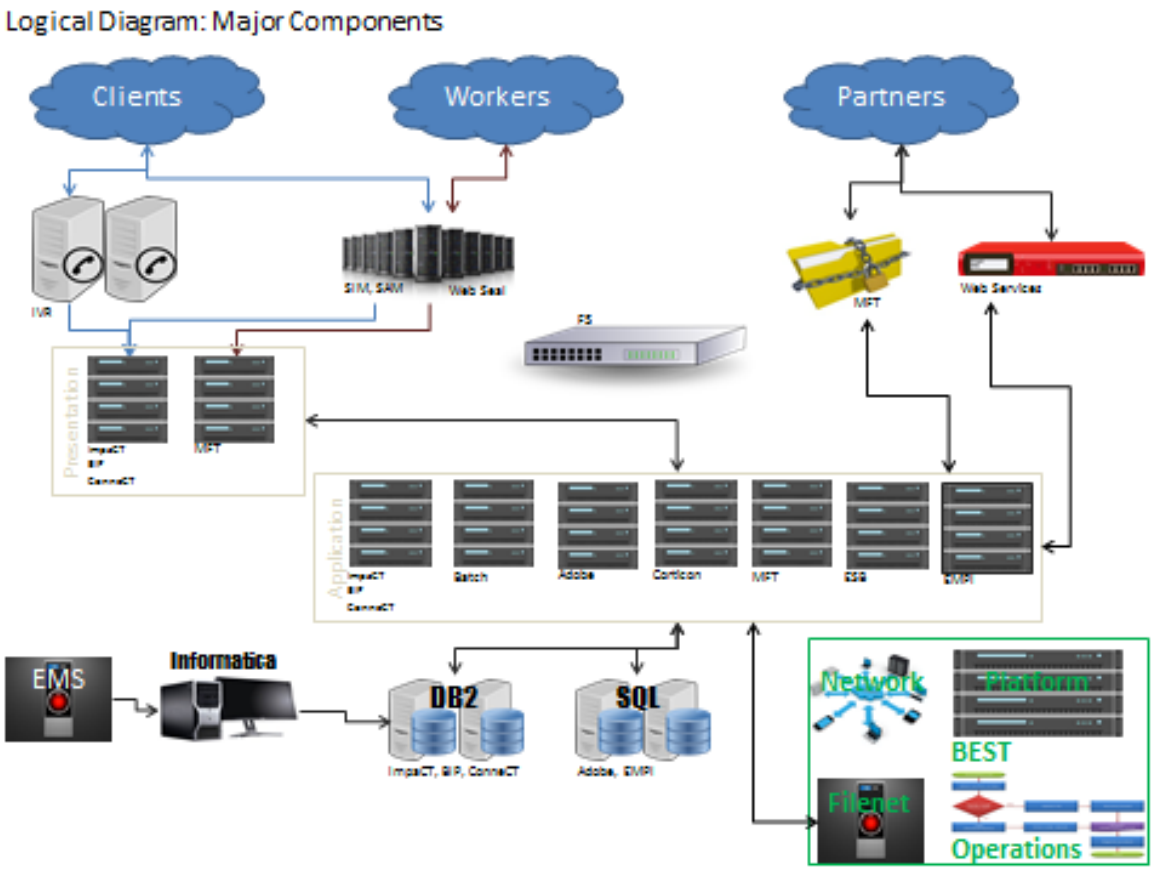


Figure 12: Major Component Interaction Pattern

F5 Load Balancing occurs for the communications between:

Table 11: Communications Load Balanced by F5

Web Seal	Web Server (Presentation Layer)
Application Server	Corticon Server
Application Server	WESB Server
WESB Server	EMPI Server
Batch Server	Corticon Server
Batch Server	WESB Server
Application Server	SSRS

8.1 Identity and Access Management (IAM)

The IAM solution consists of IBM Security Identity Manager (ISIM) and IBM Security Access Manager (ISAM) and interacts with the Web Seal Servers. ISIM performs user provisioning for the HHS Enterprise Applications while ISAM protects the web access.

8.1.1 IBM Security Identity Manager (ISIM)

ISIM provides a secure, automated environment for user administration. ISIM enables System Administrators and Delegated Administrators to efficiently manage users on multiple platforms while enabling data sources access review, deployment, and policy configuration.

8.1.2 IBM Security Access Manager (ISAM)

ISAM provides an authentication framework to enable web security. An authentication framework provides built-in authentication mechanisms and supports external authentication mechanisms. An authorization framework provides “permit/deny” decisions on access requests for back-end applications that are protected by ISAM. For the HHS Enterprise Applications system, ISAM provides authentication, as the authorization will be done through the ImpaCT DB. The user access is inspected and monitored by ISAM.

8.1.3 IBM Web Seal Servers

Web Seal Servers can either be internal or external servers. Internal servers are used for applications that are not exposed to the internet. External Web Seals are used for internet facing application like ConneCT Customer Portal (CP). ImpaCT Worker Portal (WP) uses internal Web Seal servers because it will not be exposed to the internet. IBM Web Seal intercepts web requests from users and validates with the ISAM directory store to authenticate web users by checking its local policy. Web Seal Servers host the static Login and Logout pages for the HHS Dashboard application that’s displayed to the users for authentication.

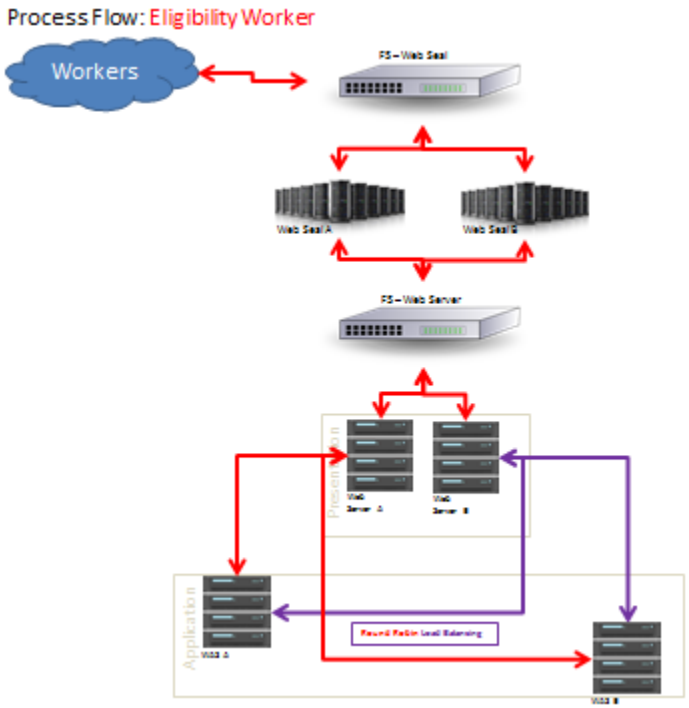
Web Seal also retrieves web contents for an authorized web request, then:

1. Relays the request to the HHS Enterprise Applications
2. Relays the request to the HHS Enterprise Applications Individual Identity Verification and Self-Registration module, should the request be for individual self-registration.

Request bound to the application servers is first intercepted by the Web Seals and interacts with IAM to validate that the user has appropriate privilege to the page he/she is trying to access. In front of the Web Seals are the internal Web Seal F5 (Load Balancer) which forwards the request to either Web Seals.

The DNS name **https://myhomepage.ct.gov** is configured on the Web Seal F5 and resolves to IP 10.60.186.xx. When the user accesses the home page, the F5 Load Balancer routes the request to either Web Seal which then routes the request to the Web Server F5. The Web Server Load Balancer can choose either IBM HTTP Server (IHS) server to process the user’s request. Example: ImpaCT WP provisioned a digital signature from Verisign which is a trusted Certificate Authority to prevent unnecessary warning messages when running the ImpaCT WP application.

Figure 13: ISIM/ISAM Interaction Pattern



8.2 IBM HTTP Server (IHS)

The IHS server forwards all requests received from the Web Server Load Balancer to either application server for processing. Responses received back from the application servers are then sent back to the Web Seal servers to be presented to the user. The Web Servers perform the role of the Load Balancer and send the request to the less busy application server for processing.

8.3 IBM WebSphere Application Server (IBM WAS)

The HHS Enterprise Applications are all hosted on IBM WebSphere Application Server (WAS). All have their own cluster on the WebSphere application server. IBM WAS Application server hosts the application code base because of the flexibility of the server and the security of the Java application which is what the framework is built on. More specifically, it is a software framework and middleware that makes it much easier to manage and deploy applications.

IBM WAS interacts with most of the infrastructure components as illustrated in Figure 11. Request received from either Web Server can be redirected to either application server for processing. If Server A or Server B is unavailable, the ImpaCT application should be still accessible because all the requests would then be routed to the WAS server that's alive.

8.4 IBM DB2

Each DB2 database provides the transactional schemas and record retention functionality of each HHS Enterprise application. DB2 is a relational database which will host the HHS Enterprise Applications system OLTP databases.

In order for the applications to load up, Day Zero data must be present in the databases, as well as all framework data and tables. ImpaCT WP and HHS Administrator (formerly called Shared Services) share the same database but have separate schemas. The Dashboard shares the same schema with HHS Administrator and holds a single table with a list of all course-grained roles in the system.

FileNet has its own DB2 database. SSRS also has its own MSSQL database. SSRS depends on the data within the database to be presented, so it can generate reports and present it to the user from the online application. Batch data is presented in the form of Correspondence reports. The batch processes connect to the DB2 database so that related batch jobs can update respective tables which are used for reporting.

8.5 Corticon Business Rules

Corticon Business Rule Software is used to model the HHS Enterprise Applications' business rules and Business Rules Services that are deployed as Web Services to the Corticon servers. Corticon Business Rules web services are used for Eligibility Determination Services executed through the application.

The F5 Load Balances the communications from the WAS application servers.

For managing the Corticon Web Services, administrators use the Business Rules Server Console which is an application (ServerSessionBean) that is installed on the IBM WAS server using CcServer.ear file.

8.6 Adobe LiveCycle

The HHS Enterprise Applications solution uses Adobe LiveCycle Server for document generation and rendering services. Adobe LiveCycle is used as a document and form platform assisting in capturing and processing of information, delivering of personalized communications and protecting and tracking of sensitive information.

The correspondence generation solution is built on the Adobe LiveCycle platform. It supports both the online and batch correspondence generation requests initiated from the applications. After the batch runs and creates XML files, these files are then converted into .pdf files. The batch correspondence generation service then uploads these pdf documents into the FileNet repository.

The HHS Enterprise Applications solution uses two Adobe LiveCycle servers for file processing, both pointing to a single SQL 2012 database instance. When a request is made from the application to render a report in the form of a pdf, the request is sent from the application to the F5 Load Balancer that in turn forward the request to either Adobe LiveCycle server for processing. Like the Corticon servers, Adobe LiveCycle has its own administrative tool used for deploying and managing the Adobe services. The Adobe LiveCycle tool is also installed and clustered on the IBM WAS servers.

8.7 IBM FileNet P8

The State uses a single FileNet Enterprise system for all HHS Enterprise Applications with a separate object store for ahCT and a single object store for ConneCT CP and ImpaCT WP.

Documents are uploaded from the online application and also generated through the batch. Correspondence files are uploaded to the FileNet server in the form of .pdf files.

Like Adobe and Corticon with multiple clustered servers, there is one FileNet Enterprise system, connected to its own DB2 database. There is no F5 Load Balancing between the Application or Batch servers and the FileNet System.

8.8 SQL Server Reporting Services (SSRS)

For reporting functionalities, the HHS Enterprise Applications system relies on SSRS, server-based reporting platform that provides comprehensive reporting functionalities. The standard reports defined must use the capabilities of the SSRS suite. MS SSRS is an enterprise reporting stack for the HHS Enterprise Applications system.

Reports are viewed from the online applications. A request coming from the HHS Application is routed through the F5 Load Balancer which in turn routes the request to either SSRS server. The reports developed within scope of the original DDI of the applications are accessed through SSRS and retrieved from the OLTP. The SSRS servers are also connected to a DB2 database replicated to the Ad-Hoc DB servers for all future reports development.

8.9 WebSphere Enterprise Service Bus (WESB)

WebSphere Enterprise Service Bus is a managed runtime environment for business integration applications that allows the deployment of standards-based business integration services in a service-oriented architecture (SOA).

Mediation modules that are internal to the Enterprise are installed on the WESB server. External services are also installed on the DataPower Appliance for additional security.

The WESB servers rely on a dedicated DB database for storing service information. Request from the application server for an internal web service is sent via the F5 Load Balancer which in turn forwards the request to either WESB server for a response. WESB will in turn communicate with the WebSphere Service Registry and Repository WSRR where the service is installed.

During the transmission of the request for the external service, a username and password token is sent through the transmission. DataPower takes that credential and validates it against LDAP to see whether or not the username/password has the right to consume the external service.

WESB provides the communications with the Enterprise Master Person Index service (EMPI). There are two EMPI servers with an F5 Load Balancer sitting between the WESB servers and the EMPI servers for balancing requests.

8.9.1 WebSphere Service Registry and Repository (WSRR)

WESB and WSRR work together to provide the service to the application to consume. The WESB host the Mediation modules (the business logic) whereas the WSRR host the Web Service Web Service Definition Language (WSDL) files and the endpoint URLs. During runtime execution, WebSphere Service Registry, and

Repository can be dynamically accessed to select a service provider, or to dynamically enforce an invocation policy. It manages information that enables dynamic binding of service consumers to service providers and allows the infrastructure to enforce registered policies.

8.10 DataPower Appliance

DataPower is used to provide additional security for all the HHS Enterprise Applications web service communications with external partners. Before any external service is consumed, authentication will happen to see whether or not the user has the right to consume the service.

WebSphere DataPower relays web service traffic between HHS Enterprise Applications, WESB and external partners like SSA, OPM, and HP, to provide web security services including:

1. Security Socket Layer connection (SSL) - for secure web service communication
2. XML threat protection - provide protection against XML threats such as Single message XML Denial-of-Service (XDoS), Multiple message XML Denial-of-Service (MMXDoS), Message tampering, SQL injections, XML viruses (X-Virus) and Dictionary attacks
3. SOAP schema validation - validate messages against an XML schema

Two authentication methods are configured to support current services, namely mutual certificate authentication using public CA issued certificates and WS-Security Username tokens. Externally exposed web services require mutual certificate authentication to secure the communication transport layer and WS-Security username token to secure the message layer. Mutual certificate authentication requires both the service consumer and the service provider to present a trusted certificate to negotiate secure encrypted data transmission. WS-Security username token authentication requires the service consumer to send a WS-Security token containing a valid username and password. Service accounts will be issued to service consumers as needed.

8.11 ImpaCT Batch

One of the most critical components of the solution is the batch jobs. The HHS Enterprise Applications application will require a heavy load of scheduled batch processes to be executed in order to operate efficiently and effectively. The HHS Enterprise Applications rely on the batch application, CA ESP agent, and the CA ESP Scheduler to orchestrate the execution of these batch processes in a sequential order.

Batch interacts with most of the HHS Enterprise Applications system components, including FileNet, Adobe, Impact database, Corticon, and SSRS. There are multiple batch servers with a CA ESP agent installed on each. The agents are used to interact with the CA ESP Scheduler on the mainframe and execute the batch jobs on the individual batch servers. The batch jobs are split between the two batch server to increase efficiency and time for executing the jobs. Like most of the other infrastructure components like Adobe and Corticon, the batch servers are not clustered. They serve as standalone servers and host the batch scripts in specific folder location (E:\Data\ImapCT_Batches).

8.12 EMPI

Enterprise Master Person Index (EMPI) is the enterprise solution for creating and maintaining the master data for clients across all HHS Enterprise source systems. As part of this implementation, the EMPI software will be installed and configured with the client information from source systems. All system communications with the EMPI go through the WESB.

9 List of Environments at the State Data Center

HHS Enterprise Environments at the Groton Data Center.

Table 10: Enterprise Environments

Physical Environment	Logical Environments	Description
User Acceptance Testing	UAT	The UAT environment is used to validate that the delivered functionality meets requirements for production deployment. The architecture of the UAT environment is similar to the setup of the production environment.
User Acceptance Testing 2	UAT2	The UAT2 environment is used to test the application in a time-travel mode
Staging	STG	This environment is identical to Production in every way possible. Performance testing and last minute functional testing is done here with the goal of approving the release for Production deployment.
Production	PROD	The Production environment serves as the live environment of the HHS Enterprise applications.
Simulation	SIM	The production simulation environment serves to replicate business cases to conduct what-if analyses in a production-similar environment.
Ad-Hoc Reporting	Ad-hoc Reporting	Report generation environment to generate generic reports that are one-off and are not part of the standard set of reports defined for the ImpaCT solution. This environment will host a copy of the OLTP databases as defined in the Integrated Requirement plan deliverable. Please refer to Integrated Requirements T12.14 and JIRA item CTIE-1029 for further clarifications on this environment.
Triage (CIT3)	Triage	This environment is a copy of Production with less capacity. It exists to have an environment to recreate a Production Incident and troubleshoot to find the root cause and design the fix.
Hotfix (CIT4)	Hotfix	This environment is a copy of Production with less capacity. It exists to have an environment to test the fix for a Production Incident before approving it for Staging and/or Production
Training	Training	
Conversion Environments	Conversion Development	Conversion Development is the environment where the conversion code will be developed and unit tested.

	Conversion Testing	An environment where the transformation logic to convert the legacy data to ImpaCT will be tested.
	Conversion Integration	A UAT-like environment, where the converted legacy data will be tested against the ImpaCT application.
	Mock Conversion	Environment to do test runs to convert all legacy data and verify run time, scheduling, completion and accuracy of the data conversion.

.

`1234567890-=
Qwertyuiop[]\

Asdfghjkl;’
Zxcvbnm,./

~!@#$%^&*()_+
QWERTYUIOP{}|
ASDFGHJKL:”
ZXCVBNM<>?