AUTOMATION OF IBM MAINFRAME TIME SHARING OPTION ACCESS

Brannon Wilds

South Carolina Department of Health & Human Services

February 3, 2015

3.1.2.1. TSO Access Automation

ID	TSO Automation
Title	Automation of IBM Mainframe Time Sharing Option Access
Type	Process Change and Technical Change
Functional Area	Information Systems/Technology

3.1.2.2. Functional Description

The purpose of this project is to streamline the TSO Access Request Process, eliminate processes where possible through automation, self-service, and consolidation, and is part of a larger initiative from our leadership at the South Carolina Department of Health and Human Services (DHHS) to improve processes.

What is TSO?

TSO is an acronym for an IBM mainframe program that creates a **T**ime **S**haring **O**ption. "TSO fulfills a similar purpose to Unix login sessions. Time-sharing means that many persons can access the operating system concurrently, while unaware that others are also accessing the operating system. It appears to each TSO user that they are the only user on the system. TSO is most commonly used by mainframe system administrators and programmers. It provides: a text editor, batch job support, including completion notification, debuggers for some programming languages used on System/360 and later IBM mainframes, support for other vendors' end-user applications, for example querying IMS and DB2 databases. TSO interacts with users in either a line-by-line mode or in a full screen, menu-driven mode. In the line-by-line mode, the user enters commands by typing them in at the keyboard; in turn, the

system interprets the commands, and then displays responses on the terminal screen." (Wikipedia, http://en.wikipedia.org/wiki/Time_Sharing_Option)

At DHHS, mainframe interaction is via ISPF, which allows for customized menu-driven interaction. "TSO can also provide a Unix-style environment on OS/390 and z/OS via the UNIX System Services command shell, with or without ISPF. TSO commands can be embedded in REXX execs or CLISTs, which can run interactively or in batch." (Wikipedia) DHHS mostly uses batch.

TSO, in its design, limits credentials. IDs can be no more than 7 characters, and passwords can be no more than 8 characters.

How is TSO access granted and why is the current process a problem?

There are three situations in which TSO access is requested, a new access request, a change access request, or a termination request. First, when a new user is being on-boarded into the environment, a ticket would be submitted by the new user's supervisor, on which would be indicated, the desire for TSO access and a justification for said access. The ticket would be assigned to a technician that would review the ticket for its accuracy and validate the justification for such access as is being requested. Upon validation, the technician would create the users account in Active Directory (AD). As a part of account creation, the technician assigns a standard format ID (8 characters), which is transmitted from human resources, and is an exact representation of the user's state supplied user ID, known as SCEIS ID. In addition, the technician must assign a TSO compliant ID (7 characters). The technician must use a web interactive tool, searching for the ID planned to be assigned for duplication to avoid conflicts. The technician will then add the IDs, respectively, in the SAM account and Employee ID fields in AD. At creation in AD, via scripts and x-sub batch jobs, the ID within the Employee ID field creates an

equivalent ID on the mainframe. The technician will create a Tiger Tracks ticket to Clemson, who manages the mainframe from a data base and administrative perspective. The ticket will request the assignment of attributes (permissions) to TSO and any other respective applications or programs being requested to the user's ID. Upon receipt of the ticket Clemson will assign four groups to the ticket, Security, zOS, PCA, and DBA. The security group verifies the justification of access and approves or denies based in large part on the attestation of the DHHS technician's verification. After approval from the security group, the zOS group verifies the existence of the ID on the mainframe. After verification of the IDs existence, the PCA group assigns the appropriate account number and RACF level security groups to the ID for the access being requested. After the correct account number is assigned, the DBA group adds the appropriate program level attributes. Once all of the verifications and permissions are added at Clemson, the DHHS technician verifies the user is able to access the mainframe and all of the appropriate permissions function properly. After verification of access the technician closes both the DHHS ticket and the Tiger Tracks ticket. (See 3.1.2.8 Process Flows and Charts, Appendix I)

The second situation in which TSO access is requested is via a change access request. A change request is when a user already has an account in AD, and in this situation, mainframe access, but needs elevated permissions or permissions to programs not previously attributed access. With a change access request, a ticket would be created by the user's supervisor requesting mainframe access be modified to include TSO. The ticket would be assigned to a technician that would review the ticket for its accuracy and validate the justification for such access as is being requested. Upon validation, the technician would need to assign a TSO compliant ID (7 characters). The technician, as in the new access request process, would use a web interactive tool, searching for the ID planned to be assigned for duplication to avoid

conflicts. The technician then begins a sub-process to change an Employee ID in AD from the standard 8 character ID to a TSO compliant 7 character ID. The technician must first remove all mainframe related groups from the account, save the update to the account, and wait 15 minutes (standard latency between AD and the Mainframe) before moving on to the next step. The technician then must remove the old 8 character ID currently listed in the Employee ID field in AD, save the update to the account, and wait 15 minutes before moving on to the next step. Then the technician would add the new ID and respective mainframe groups, save the update to the account, and wait 15 minutes before moving on to the next step. Upon the addition in AD, via scripts and x-sub batch jobs, the ID within the Employee ID field creates an equivalent ID on the mainframe. The technician then creates a Tiger Tracks ticket to Clemson. The ticket will request the assignment of attributes (permissions) to TSO and any other respective applications or programs being requested to the user's ID. The process from this point to end is the same as a new access request. (See 3.1.2.8 Process Flows and Charts, Appendix II)

The third situation in which TSO access is requested is via a termination request. There are two types of termination requests. One in which all access is requested to be removed and an account disabled. This type is associated with a user's separation of employment. The other in which just a specific access or permission is requested to be removed, but the account left enabled. This type is associated with changes in a user's role, job functions, and/or location. The first type of request has already been automated. When any account in AD, and its respective mainframe access (TSO or otherwise), is disabled, scripts and x-sub jobs remove all permissions and attributes assigned to that ID and subsequently disables the ID on the mainframe. The second type of termination request requires manual intervention. Upon receipt of the request, and after performing the necessary tasks for other access assigned to the account, the

technician assigned will create a Tiger Tracks ticket to Clemson. The ticket will request the termination of attributes (permissions) to TSO and any other respective mainframe applications or programs being requested from the user's ID. Upon receipt of the ticket Clemson will assign three groups to the ticket, PCA, zOS and DBA. The zOS group removes the respective mainframe groups. After the mainframe groups have been removed, the PCA group changes the account number associated with the ID based on the remaining access. After the correct account number is assigned, the DBA group removes the respective program level attributes. Once all of the permissions and attributes are removed and account number adjusted, the DHHS technician verifies the user is able to access the mainframe and all of the remaining permissions continue to function properly. After verification, the technician closes both the DHHS ticket and the Tiger Tracks ticket. (See 3.1.2.8 Process Flows and Charts, Appendix III)

New access and change access requests take an average of 5 business days to complete. Completion of a ticket is defined as verification by the user of the access requested. Termination requests take an average of 3 business days to complete. All only require 3.5 hours of actual work time. The new access requests and change access requests waste result in an average loss of 2 business days (15 work hours) of productivity per request for the user and 3.5 hours per request for the various groups that process the tickets for a total of 18.5 hours per request. The 2 business day loss of productivity is based off of a comparison of user start date and the date of completion. That difference over all access requests (new and change) was averaged to produce 2 business days and thus the 15 hour work hours, 7.5 hour work day multiplied by 2 days. At an average of 23 dollars per hour, that equates to $425.50 lost for each new access or change access ticket. The termination requests do not carry lost time for the user, but do still equate to lost time for the various groups who process the tickets, specifically an average of 3.5 hours

per request. At an average of 23 dollars per hour, that equates to $80.50 lost for each termination request.

Note: The 23 dollars per hour, is an average provided by SCDHHS Human Resources for FTE, TGE, State Temporary employees, and Paid Interns. Contract employee pay was not figured into this average due to disclosure issues. It cannot be verified; therefore it is not figured into the calculation for average pay.

In the twelve month period between October 1, 2013 and October 1, 2014, the DHHS IT Service Desk received 1,381 total access request tickets, 331 of which contained a request for TSO, 24%. There were 253 new access requests associated with TSO, 28% of all new access requests. There were 49 change access requests associated with TSO, 23% of all change access requests. There were 29 terminate access requests associated with TSO, 10% of all terminate access requests. That is a total loss of $130,835.50 during that 12 month period, $128,501 for new and change access requests and $2334.50 for terminate requests. This analysis represents just the losses within these specific processes and does not take into account the opportunity costs associated with the lost time being applied toward other tasks, and thus those applicable savings. (See 3.1.2.8 Process Flows and Charts, Appendix IV)

The greatest count of wastes in the process are related to transportation, over-processing, and defects, which compound wait time. Therefore, despite defects having the largest straight count, the greatest waste is related wait time, as there is a greater number of hours tied to each point of wait time as opposed to the time associated with each point of defect. This is especially true between groups at Clemson, and to a slightly lesser extent between DHHS and Clemson. (See 3.1.2.8 Process Flows and Charts, Appendix V)

How should TSO access be granted?

A root cause analysis (See 3.1.2.8 Process Flows and Charts, Appendix VI) provides that automating the process in whole or in part and/or consolidating responsibilities at Clemson would reduce or eliminate the wastes within the process. Due to separation of authority policies at Clemson, the best solution is to automate as much of the process as is possible. The time loss between the supervisors, users, and DHHS IT Service Desk currently can only be addressed via procedural and policy changes. However, DHHS already has electronic communication, a link, between the AD and the mainframe. An XML driver, known as the AD driver, was installed on one of the five DHHS domain controllers, one of which that is housed at Clemson. This driver was configured to monitor select fields on accounts and group memberships in AD. When an account is created, modified, or disabled, the account has said fields populated or modified, and certain group memberships assigned or unassigned. The AD driver collects all of the account information and group memberships of that account, and then transmits that data, via pearl scripting and web services, to the identity manager (IDM) instance in the DHHS SILO at Clemson. The IDM, based on the data received, creates, modifies, or disables a duplicate instance of the account. The IDM then transmits, via scripting and web service, the data to the mainframe. The mainframe then, based on data received, kicks off scripting and x-sub jobs at both the RACF security and CV (application) level to produce an ID and permissions respective to the data received, modify the account, or disable the account. (See 3.1.2.8 Process Flows and Charts, Appendix XI) This infrastructure can be easily leveraged to automate the addition, modification, and termination of TSO access.

Thus, when a new user is being on-boarded into the environment, a ticket would be submitted by the new user's supervisor, on which would be indicated, the desire for TSO access and a justification for said access. The ticket would be assigned to a technician that would review the ticket for its accuracy and validate the justification for such access as is being requested. Upon validation, the technician would create the users account in Active Directory (AD). As a part of account creation, the technician assigns a standard format ID (8 characters), which is transmitted from human resources, and is an exact representation of the user's state supplied user ID, known as SCEIS ID. In addition, the technician must assign a TSO compliant ID (7 characters). The technician will then add the IDs, respectively, in the SAM account and Employee ID fields in AD. At creation in AD, via scripts and x-sub batch jobs, the ID within the Employee ID field creates an equivalent ID on the mainframe, including the correct account numbers and mainframe permissions. The DHHS technician verifies the user is able to access the mainframe and all of the appropriate permissions function properly. After verification of access the technician closes the DHHS ticket. (See 3.1.2.8 Process Flows and Charts, Appendix VII)

When TSO access is requested via a change access request, a ticket would be created by the user's supervisor requesting mainframe access be modified to include TSO. The ticket would be assigned to a technician that would review the ticket for its accuracy and validate the justification for such access as is being requested. Upon validation, the technician would need to assign a TSO compliant ID (7 characters). The technician then begins a sub-process to change an Employee ID in AD from the standard 8 character ID to a TSO compliant 7 character ID. The technician must first remove all mainframe related groups from the account, save the update to the account, and wait 15 minutes (standard latency between AD and the Mainframe) before moving on to the next step. The technician

then must remove the old 8 character ID currently listed in the Employee ID field in AD, save the update to the account, and wait 15 minutes before moving on to the next step. Then the technician would add the new ID and respective mainframe groups. Upon the addition in AD, via scripts and x-sub batch jobs, the ID within the Employee ID field creates an equivalent ID on the mainframe, including the correct account numbers and mainframe permissions. The DHHS technician verifies the user is able to access the mainframe and all of the appropriate permissions function properly. After verification of access the technician closes the DHHS ticket. (See 3.1.2.8 Process Flows and Charts, Appendix VIII)

Finally, when TSO access is requested via a termination request, there can be two types of termination requests. One in which all access is requested to be removed and an account disabled. This type is associated with a user's separation of employment. The other in which just a specific access or permission is requested to be removed, but the account left enabled. This type is associated with changes in a user's role, job functions, and/or location. The first type of request has already been automated. When any account in AD, and its respective mainframe access (TSO or otherwise), is disabled, scripts and x-sub jobs remove all permissions and attributes assigned to that ID and subsequently disables the ID on the mainframe. The second type of termination request requires manual intervention. Upon receipt of the request, and after performing the necessary tasks for other access assigned to the account, the technician assigned will create a Tiger Tracks ticket to Clemson. The ticket will request the termination of attributes (permissions) to TSO and any other respective mainframe applications or programs being requested from the user's ID. Upon receipt of the ticket Clemson will assign three groups to the ticket, PCA, zOS and DBA. The zOS group removes the respective mainframe groups. After the mainframe groups have been removed, the PCA group changes the account number associated with the ID based on

the remaining access. After the correct account number is assigned, the DBA group removes the respective program level attributes. Once all of the permissions and attributes are removed and account number adjusted, the DHHS technician verifies the user is able to access the mainframe and all of the remaining permissions continue to function properly. After verification, the technician closes both the DHHS ticket and the Tiger Tracks ticket. (See 3.1.2.8 Process Flows and Charts, Appendix IX)

3.1.2.3. Project Plan Summary

In order to implement this project the following tasks need to be completed. A new group, "TSO.RACF," will need to be created in AD. Since, all groups that end with .MEDS, .MMIS, and .RACF are already monitored and transmitted by the AD driver and the IDM, no changes will need to be made at those points in the AD Driver process. A mainframe DBA and an administrator from the zOS group will need to write the scripts and x-sub jobs to produce on the mainframe the creation, modification, and removal of access, based on transmission of the assignment or removal of AD group "TSO.RACF" to or from an account. This includes the augmentation of a system ID to have permissions to make all of the necessary changes, including the assignment of account numbers, within the x-sub job created. Once this is complete, DHHS and Clemson need to test the changes. Since there is no test environment for this infrastructure, the changes will need to be implemented in production, and tested during a scheduled maintenance window, or after normal business hours. Once testing is complete and the changes verified, the changes will need to be communicated to the respective groups at DHHS and Clemson. In addition, training for the new process will need to be held for DHHS technicians. (See 3.1.2.8 Process Flows and Charts, Appendix XIII)

3.1.2.4. Testing

The following is the project test plan. DHHS will create a test account, complete all necessary fields, assign the account to the TSO.RACF group, and save the account. Clemson CSO will read the logs of the AD driver and IDM to ensure creation on IDM and the data was transmitted properly to the mainframe. Clemson zOS will confirm receipt of the data on the mainframe, confirm the proper scripts ran, and confirm creation of the account at RACF. Clemson DBA will confirm the scripts kicked off the proper x-sub jobs, and the proper account number, RACF, and Application permissions were assigned. Once the creation and permissions are verified, DHHS will remove the TSO.RACF group from the account and save the change. All of the steps above will be followed by their respective owners to confirm change of the account numbers and the removal of the permission, while the account remains active. Once the account number and permission change is verified, DHHS will disable the account in AD. All of the steps above will be followed by their respective owners to confirm the account has been disabled at IDM and the mainframe.

During testing, there were errors shown in both the scripting at RACF and in the x-sub jobs. These errors prevented creation of the account in round 1, and proper provisioning in rounds 2, and 3. Changes were made to both the scripting and x-sub code, testing resumed and was successful. Steps were repeated for two more test accounts, and were both successful. The project was then deemed implemented.

3.1.2.5. Communication

Although, the implementation of the project would effect the efficiency of many people and groups, it would only be visible in the changes to the DHHS IT Service Desk and Clemson TSG group procedure. Therefore, communication was drafted for those two groups, and transmitted after implementation.

3.1.2.6. Training

The only groups that saw a change in procedure were the DHHS IT Service Desk and Clemson TSG group. The implementation of this project effectively eliminated all of the manual tasks for the Clemson TSG group however. Therefore, the only group that needed training was the DHHS IT Service Desk. The training consisted of a dissemination of the new procedure, and walk through of case examples including the new group and the addition, modification, and removal of all mainframe related groups to and from test IDs. Training was completed 3 days after implementation.

3.1.2.7. Implementation Analysis

The implementation of this project resulted in a savings of 2 business days (15 hours) of productivity per request for the user and 4 business days (30 hours) per request between the elimination of wait time and work time for the technician that processes the request for a total of 45 hours per request on new access and change access requests. Access requests now take an average of 1 business day to complete. At an average of 23 dollars per hour, that equates to $1035 saved for each new access or change access ticket. Termination requests now take an average of 1 business day to complete as well. Since there was no loss of time or productivity for the user, there were no savings for the user. However, that is a savings of 2

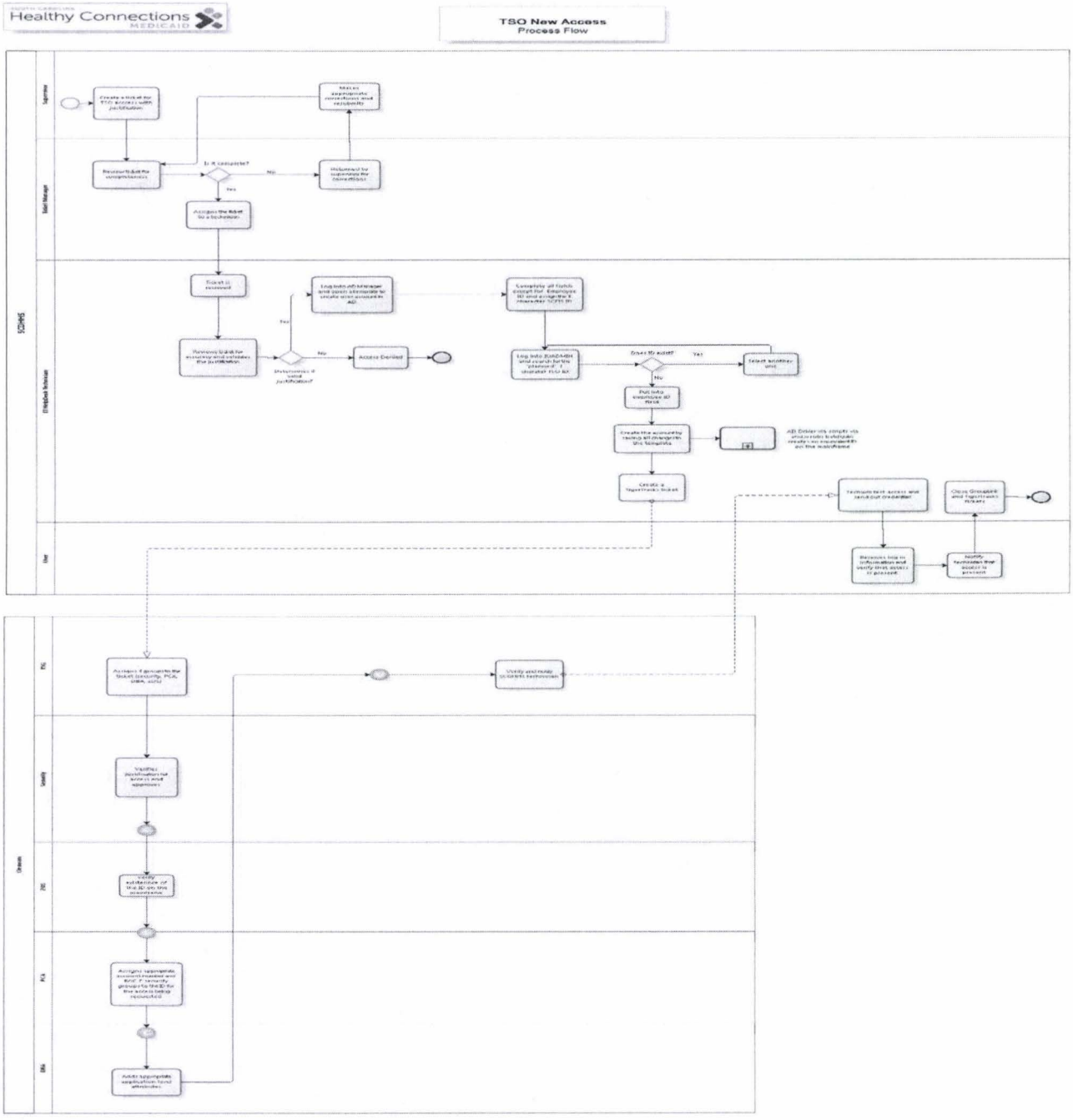
business days (15 hours) for the technician in waiting and work time per request. At an average of 23 dollars per hour, that equates to $345 saved for each termination request.

Implementation of this project resulted in a 72% reduction in identified wastes, 28 of 39 identified wastes. The greatest count of wastes eliminated were 8 of 12 defects, as well as completely eliminating waiting and over production. (See 3.1.2.8 Process Flows and Charts, Appendix X)

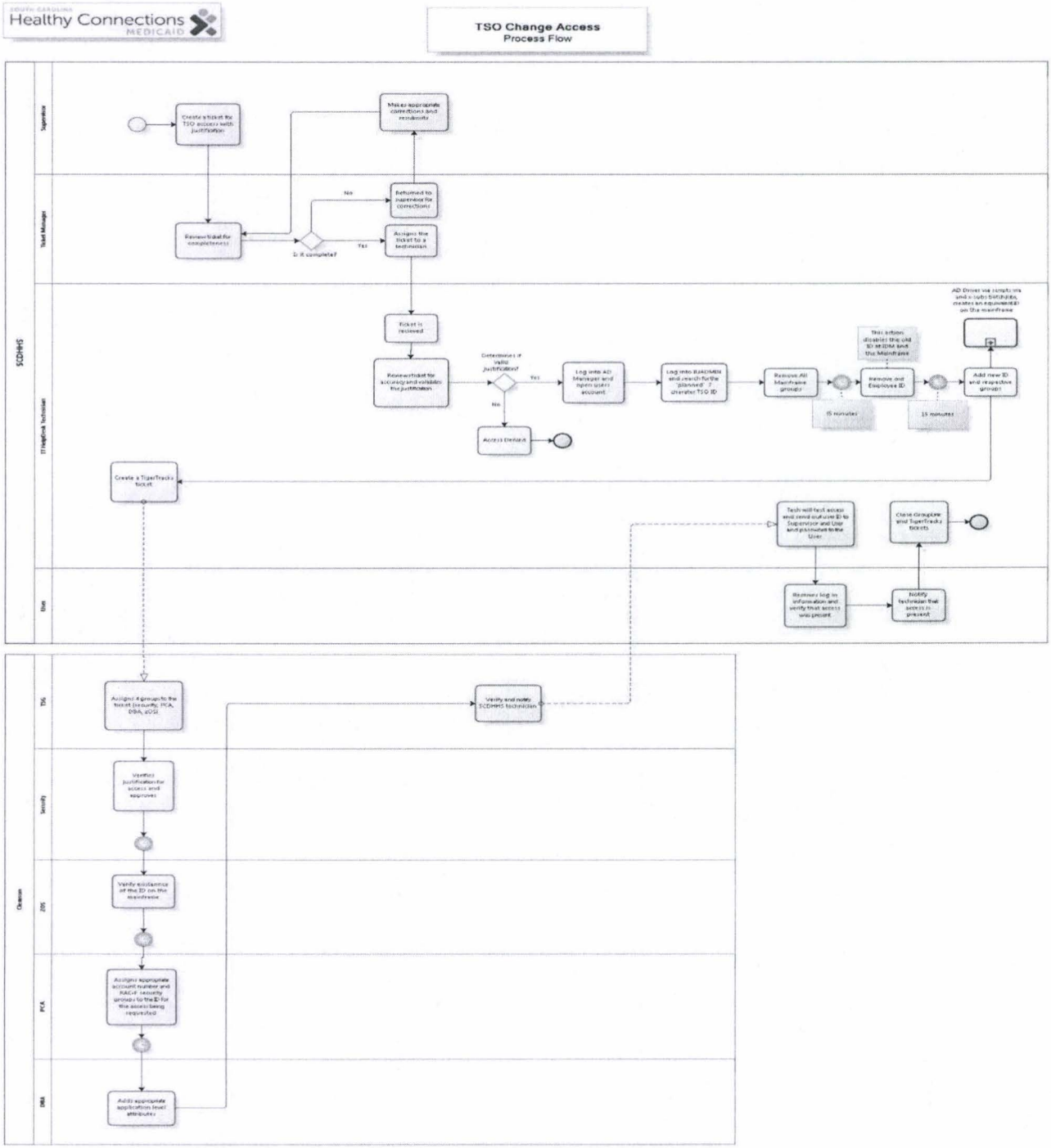
In the month after implementation, October 1, 2014 through November 1, 2014, the DHHS IT Service Desk received 95 total access request tickets, 20 of which contained a request for TSO, 21%. There were 15 new access requests associated with TSO, 25% of all new access requests. There were 3 change access requests associated with TSO, 20% of all change access requests. There were 2 terminate access requests associated with TSO, 10% of all terminate access requests. That is a total savings of $19,320 during that period, $15,525 for new access requests, $3,105 for change access requests, and $690 for terminate requests. If the following months average the same ticket numbers, that would equate to a savings of $231,840 annually. (See 3.1.2.8 Process Flows and Charts, Appendix XII)

3.1.2.8. Process Flows and Charts

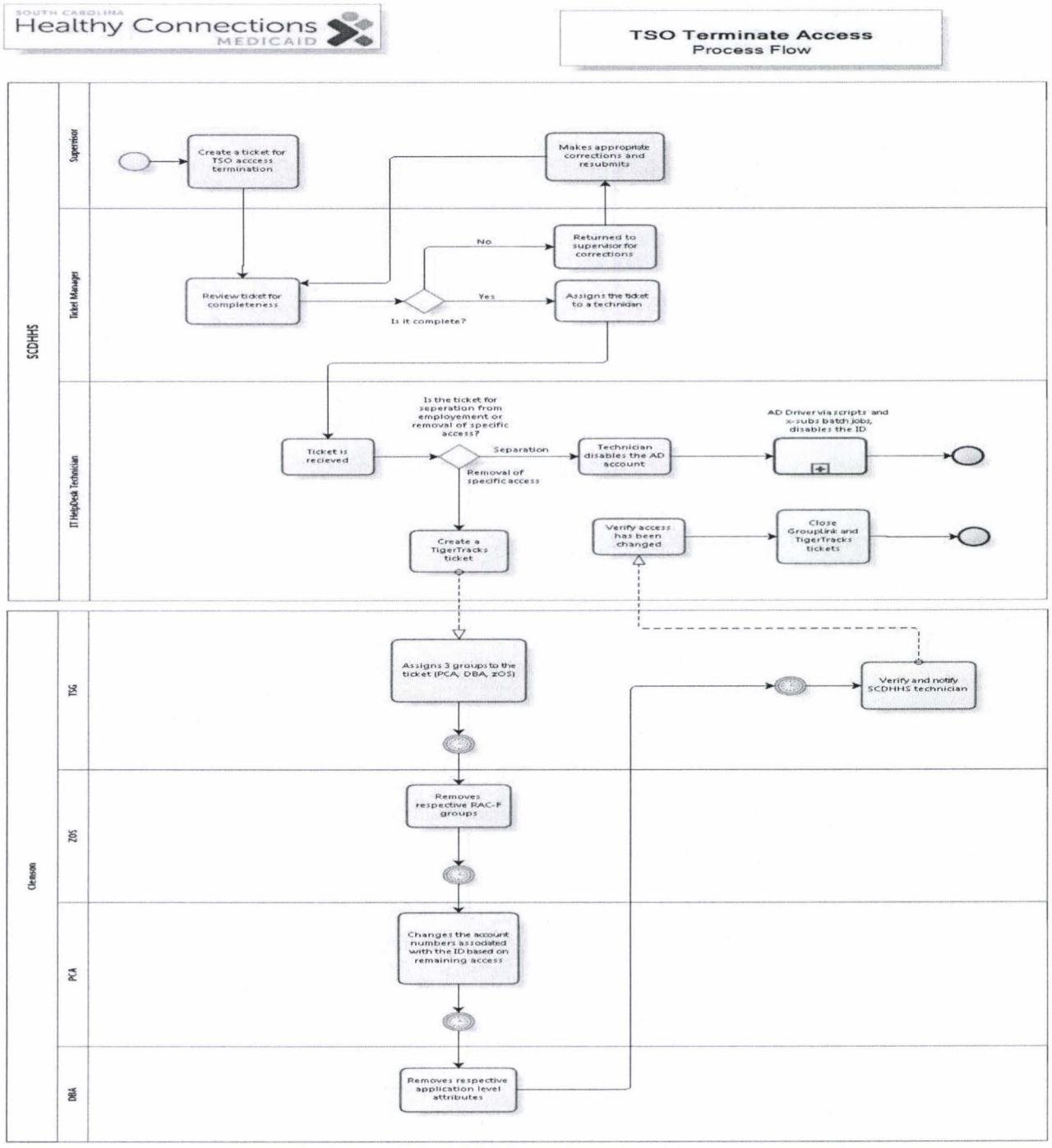
Appendix I. Previous TSO New Access Request



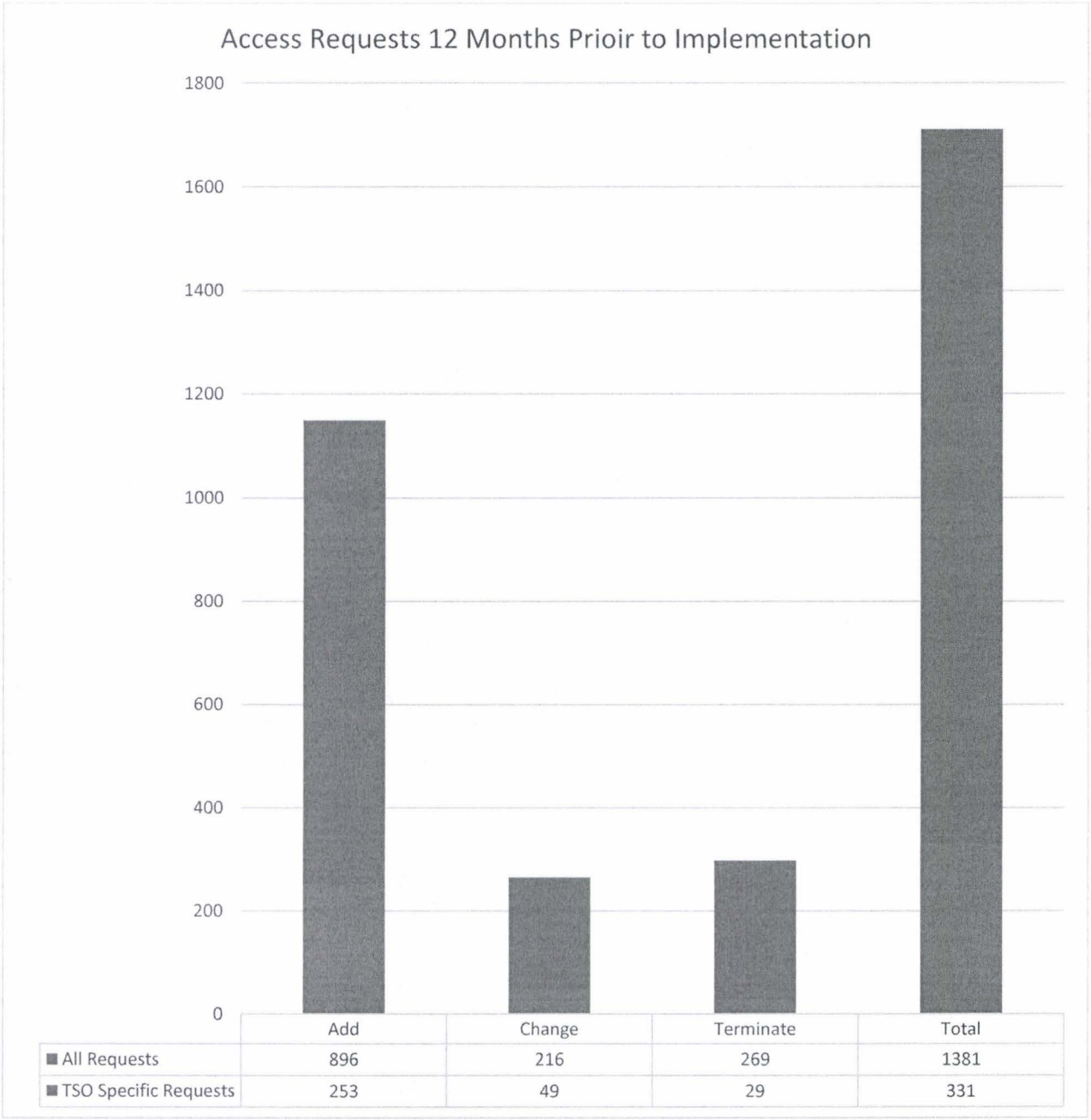
Appendix II. Previous TSO Change Access Request



Appendix III. Previous TSO Terminate Access Request



Appendix IV. Access Requests from October 2013 to October 1014



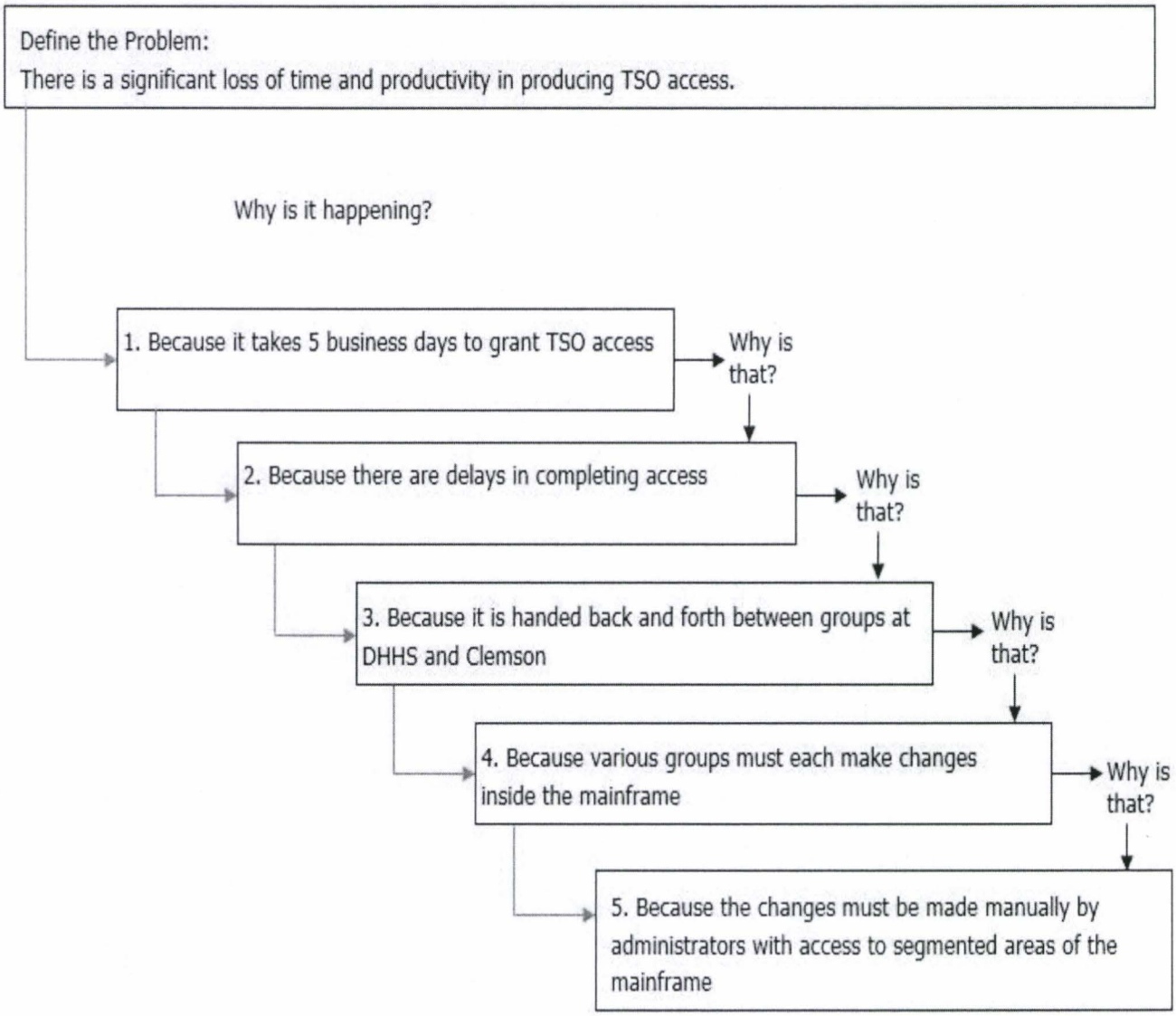
	Add	Change	Terminate	Total
All Requests	896	216	269	1381
TSO Specific Requests	253	49	29	331

Appendix V. "Tim Wood" Waste Analysis Before

	Type of Waste	Identified Waste in Current Project Process	Number
T	Transportation	1. Tickets from users to Helpdesk 2. Tickets returned to users from Helpdesk 3. E-mails to users 4. E-mails to Helpdesk 5. E-mails to Clemson from Helpdesk 6. E-mails to Helpdesk from Clemson 7. TigerTracks tickets to Clemson from Helpdesk 8. TigerTracks tickets to Helpdesk from Clemson	8
I	Inventory	1. Backlog of access request tickets 2. Active access for terminated employees (security lapse)	2
M	Motion	1. Switching back and forth an unnecessary amount of times between the user and the Helpdesk. 2. Switching back and forth an unnecessary amount of times between the Helpdesk and Clemson.	2
W	Waiting	1. Helpdesk must wait for Clemson to perform the requested tasks when creating acces 2. Helpdesk must wait for Clemson to perform the requested tasks when changing access 3. Helpdesk must wait for Clemson to perform the requested tasks when terminating access 4. Users must wait for their access when creating access 5. Users must wait for their access when chaning access 6. Trainers must wait until users receive access before conducting training when creating access 7. Trainers must wait until users receive access before conducting training when changing access	7
O	Overproduction	1. The PCA group at Clemson processes requests one time per day, instead of as they are submitted (real time).	1
O	Over-processing	Tasks must be performed by: 1. Clemson's PCA group 2. Clemson's TSG group (Tiger Tracks Administration) 3. Clemson's zOS group 4. Clemson's DBA group 5. Clemson's Security group 6. DHHS's IT Service Desk group 7. DHHS user's supervisor	7
D	Defects	1. Erroneous information sent from DHHS supervisors to DHHS's IT Service Desk group 2. Erroneous information sent from DHHS's IT Service Desk group to Tiger Tracks (TSG Group) 3. Erroneous information sent from Clemson's TSG group to Clemson's Security group 4. Erroneous information sent from Clemson's Security group back to Clemson's TSG group 5. Erroneous information sent from Clemson's TSG group to Clemson's zOS group 6. Erroneous information sent from Clemson's zOS group to Clemson's PCA group 7. Erroneous information sent from Clemson's PCA group to Clemson's DBA group 8. Erroneous information sent from Clemson's DBA group back to Clemson's TSG group 9. Erroneous information sent from Clemson's TSG group back to DHHS's IT Service Desk group 10. Erroneous information sent from DHHS's IT Service Desk group to the DHHS supervisor 11. Erroneous information sent from DHHS's IT Service Desk group to the DHHS user 12. Erroneous information sent from the DHHS user back to the DHHS's IT Service Desk group	12
		Total Number of Waste Items Identified:	**39**

Appendix VI. 5 Why's Root Cause Analysis

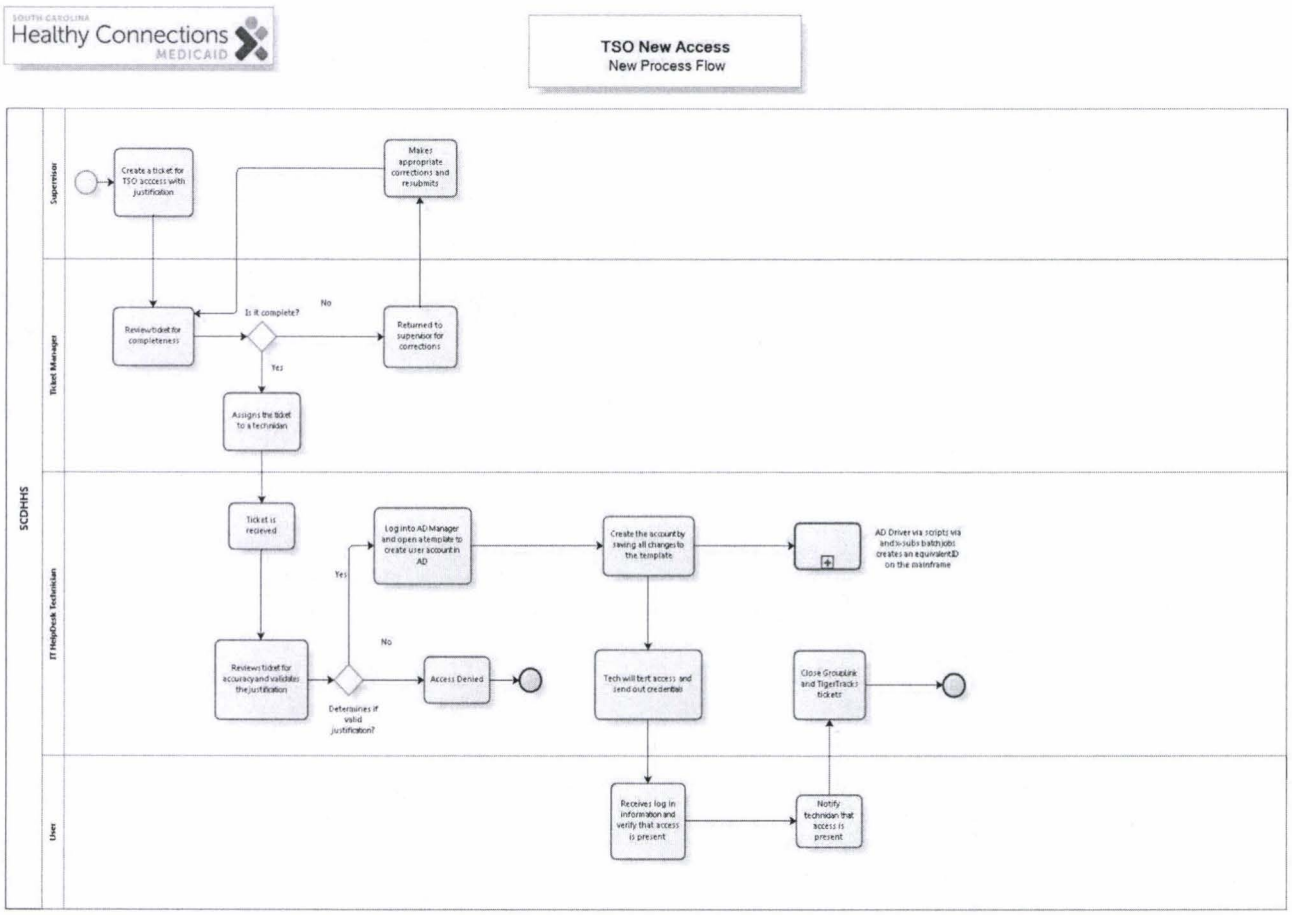
5 Why's Worksheet



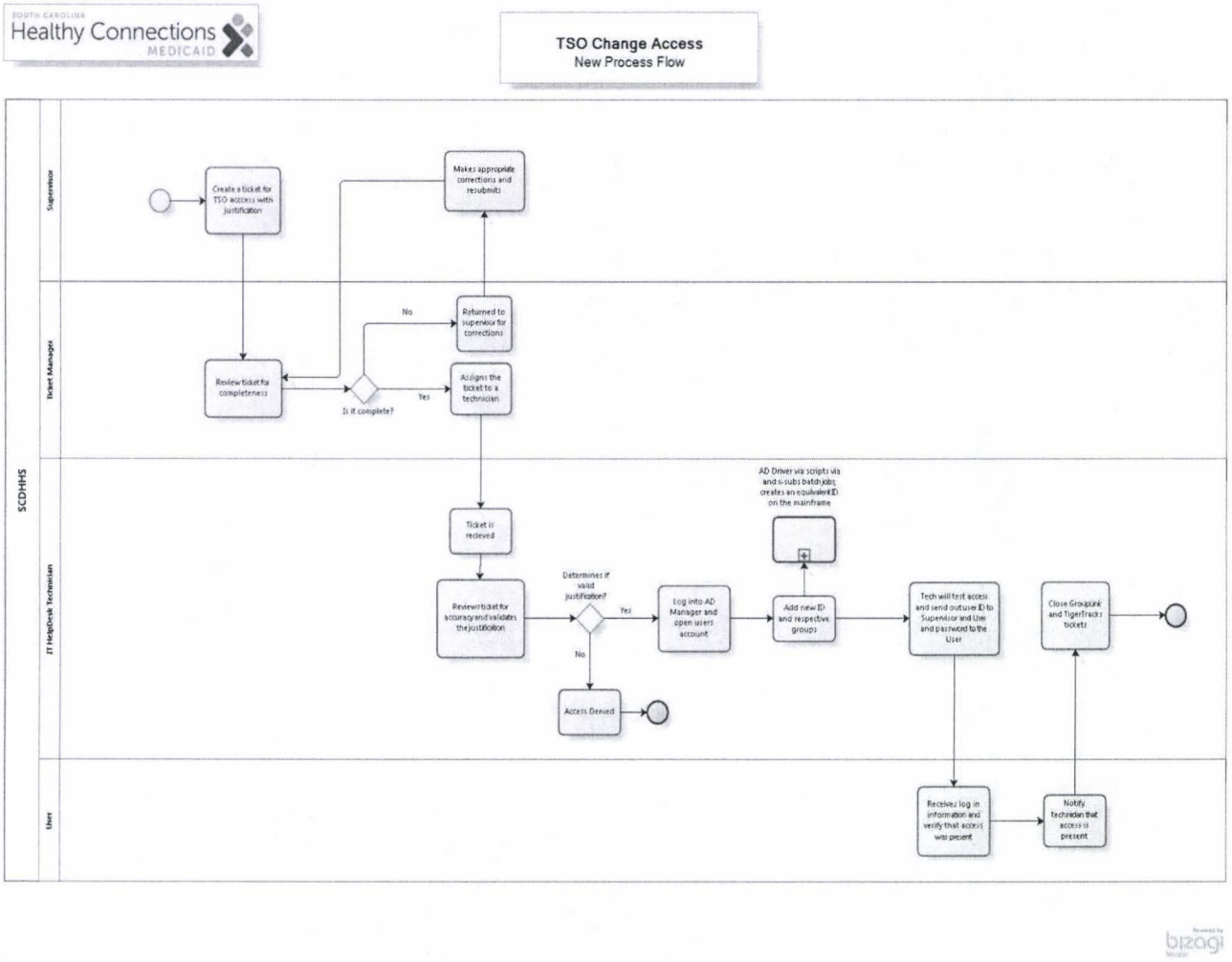
Action:

The process to grant access to TSO should be automated.

Appendix VII. New TSO New Access Request



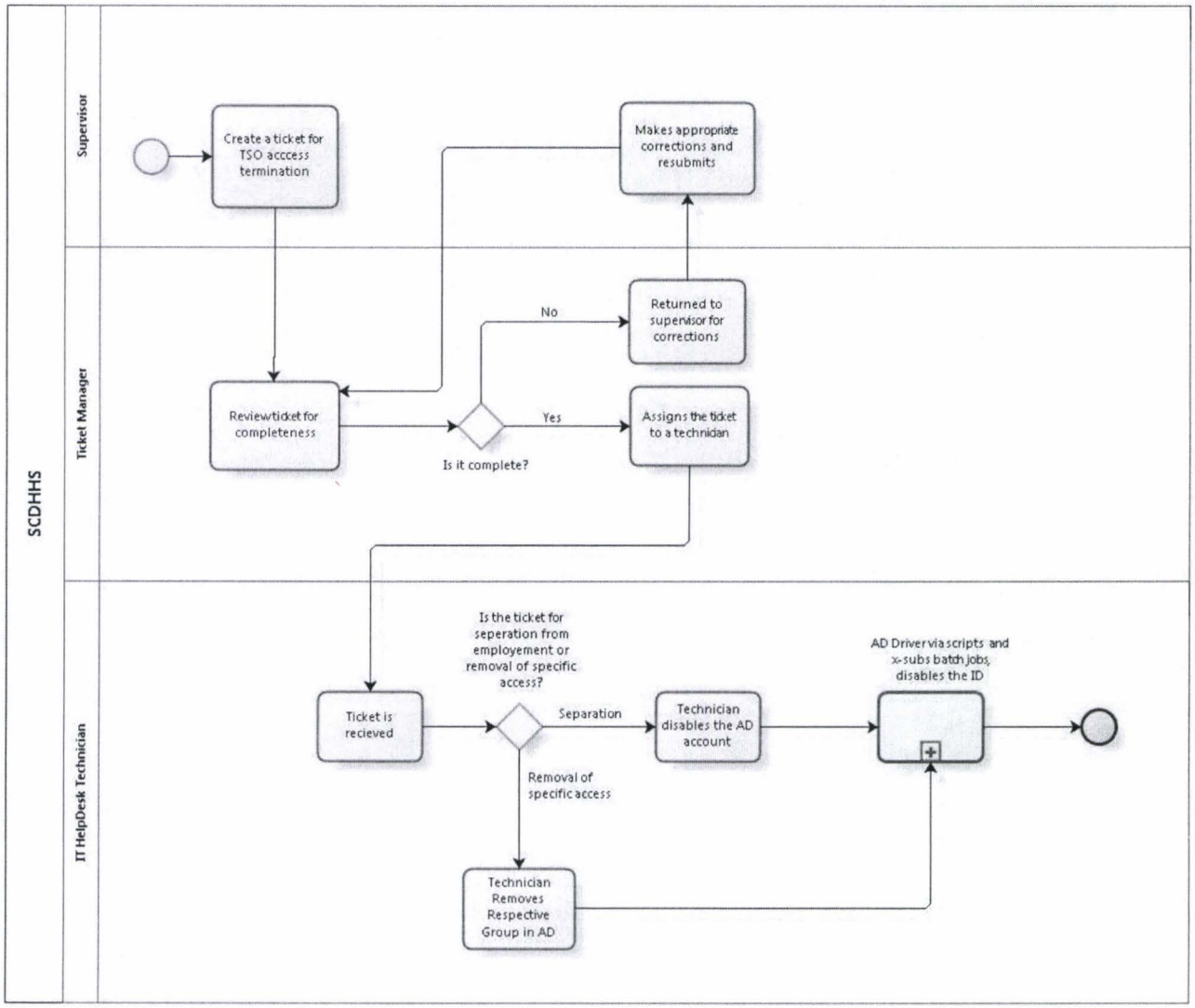
Appendix VIII. New TSO Change Access Request



Appendix IX. New TSO Terminate Access Request

SOUTH CAROLINA Healthy Connections MEDICAID

TSO Terminate Access
New Process Flow

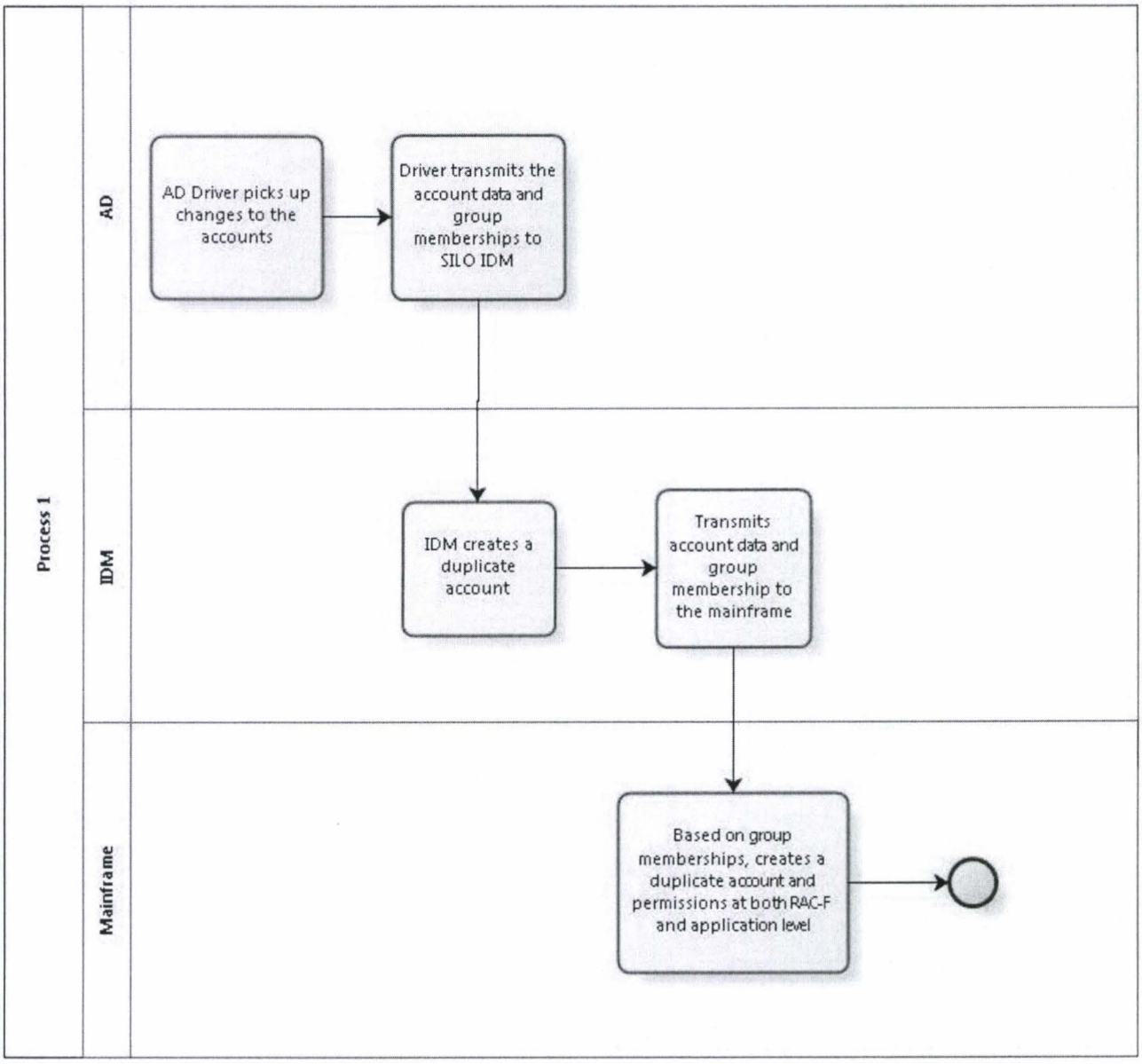


Powered by bizagi Modeler

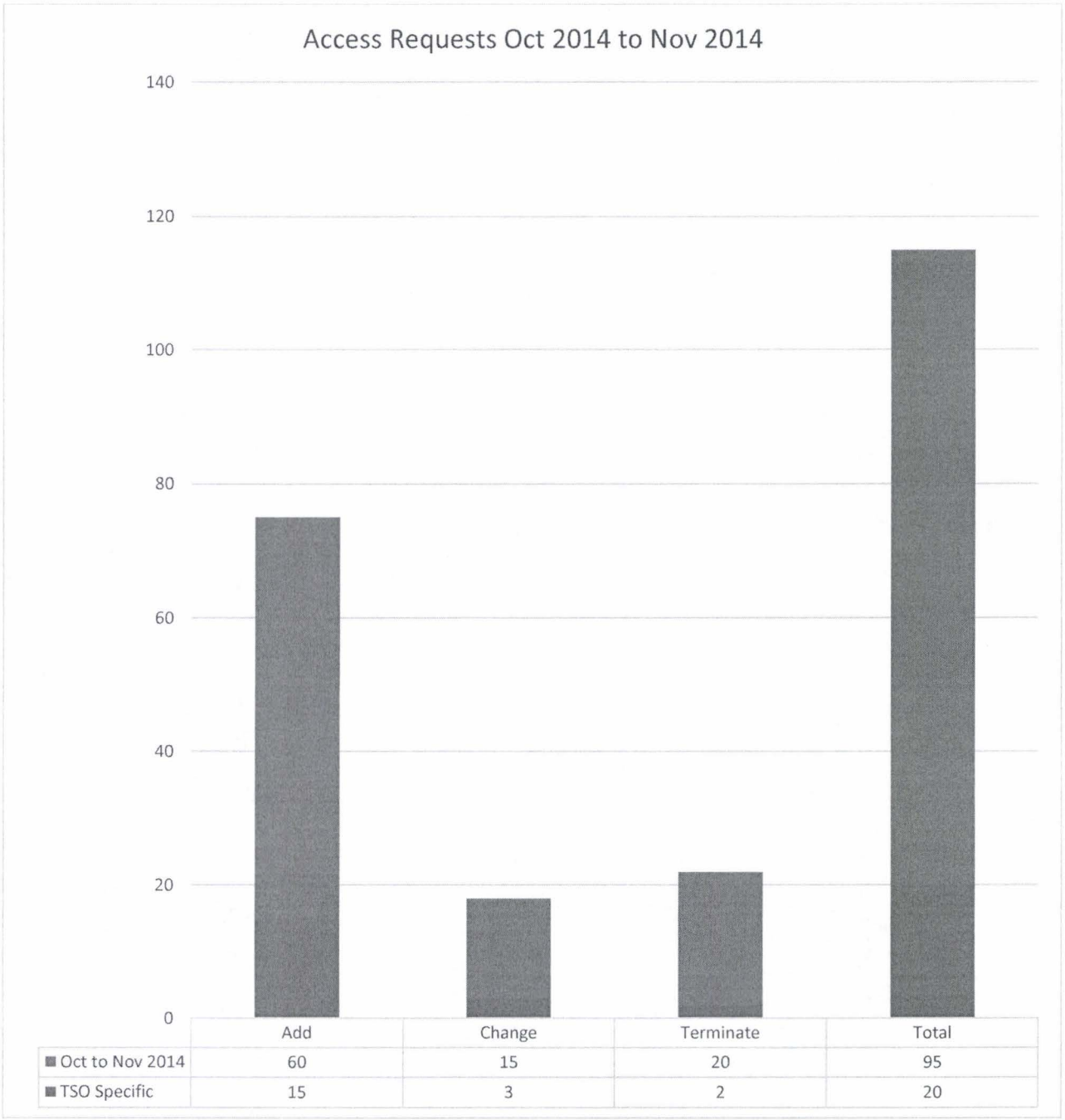
Appendix X. "Tim Wood" Waste Analysis After

	Type of Waste	Identified Waste in Current Project Process	Number Eliminated
T	Transportation	1. Tickets from users to Helpdesk 2. Tickets returned to users from Helpdesk 3. E-mails to users 4. E-mails to Helpdesk ~~5. E-mails to Clemson from Helpdesk~~ ~~6. E-mails to Helpdesk from Clemson~~ ~~7. TigerTracks tickets to Clemson from Helpdesk~~ ~~8. TigerTracks tickets to Helpdesk from Clemson~~	4
I	Inventory	~~1. Backlog of access request tickets~~ ~~2. Active access for terminated employees (security lapse)~~	2
M	Motion	1. Switching back and forth an unnecessary amount of times between the user and the Helpdesk. ~~2. Switching back and forth an unnecessary amount of times between the Helpdesk and Clemson.~~	1
W	Waiting	~~1. Helpdesk must wait for Clemson to perform the requested tasks when creating acces~~ ~~2. Helpdesk must wait for Clemson to perform the requested tasks when changing access~~ ~~3. Helpdesk must wait for Clemson to perform the requested tasks when terminating access~~ ~~4. Users must wait for their access when creating access~~ ~~5. Users must wait for their access when chaning access~~ ~~6. Trainers must wait until users receive access before conducting training when creating access~~ ~~7. Trainers must wait until users receive access before conducting training when changing access~~	7
O	Overproduction	~~1. The PCA group at Clemson processes requests one time per day, instead of as they are submitted (real time).~~	1
O	Over-processing	Tasks must be performed by: ~~1. Clemson's PCA group~~ ~~2. Clemson's TSG group (Tiger Tracks Administration)~~ ~~3. Clemson's zOS group~~ ~~4. Clemson's DBA group~~ ~~5. Clemson's Security group~~ 6. DHHS's IT Service Desk group 7. DHHS user's supervisor	5
D	Defects	1. Erroneous information sent from DHHS supervisors to DHHS's IT Service Desk group ~~2. Erroneous information sent from DHHS's IT Service Desk group to Tiger Tracks (TSG Group)~~ ~~3. Erroneous information sent from Clemson's TSG group to Clemson's Security group~~ ~~4. Erroneous information sent from Clemson's Security group back to Clemson's TSG group~~ ~~5. Erroneous information sent from Clemson's TSG group to Clemson's zOS group~~ ~~6. Erroneous information sent from Clemson's zOS group to Clemson's PCA group~~ ~~7. Erroneous information sent from Clemson's PCA group to Clemson's DBA group~~ ~~8. Erroneous information sent from Clemson's DBA group back to Clemson's TSG group~~ ~~9. Erroneous information sent from Clemson's TSG group back to DHHS's IT Service Desk group~~ 10. Erroneous information sent from DHHS's IT Service Desk group to the DHHS supervisor 11. Erroneous information sent from DHHS's IT Service Desk group to the DHHS user 12. Erroneous information sent from the DHHS user back to the DHHS's IT Service Desk group	8
		Total Number of Waste Items Eliminated:	**28**
		Total Number of Waste Items Remaining:	**11**
		Percentage of Waste Items Eliminated:	**39.29%**

Appendix XI. AD Driver Process Flow



Appendix XII. Access Requests October 2014 to November 2014



Appendix XIII: Acronyms and Definitions

TSO: Time Sharing Option
IBM: International Business Machines Corporation
(SC) DHHS: South Carolina Department of Health and Human Services
Unix: A family of multitasking, multiuser computer operating systems
IMS: IBM Information Management System database
DB2: IBM Database 2, database server products
OS/390: IBM operating system
zOS: IBM operating system
ISPF: Interactive System Productivity Facility
REXX execs: ISPF/TSO batch programs and routines
CLISTs: ISPF/TSO batch programs and routines
AD: Active Directory
SCEIS: South Carolina Enterprise Information System
SAM account: Windows logon name used to support clients and servers
Script: Programming language written/coded to perform web services
x-sub: Mainframe command/job that produces the written/coded tasks when executed
Tiger Tracks: Clemson University Branded ticketing system
CSO: Computing Systems and Operations
TSG: Technical Services Group
PCA: Production Control Administration
DBA: Database Administrator
RACF: Resource Access Control Facility
HR: Human Resources
FTE: Full Time Equivalent
TGE: Temporary Grant Employee
XML: Is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable.
IDM: Identity Management
SILO: from the Greek σιρός – siros, "pit for holding grain" In this instance it is used metaphorically as a separator of data, specifically areas to separate SCDHHS data from Clemson University data.
CV: Central Version

Appendix XIV. Project Plan

Task #	*Requirement*	*Owner*	*Status*
1	Create TSO.RACF security group in AD. OU=Groups, Security, Mainframe.	Brannon Wilds	Completed
2	Change system ID to have permissions to change account numbers	zOS	Completed
3	Write x-subs to create, modify, and remove TSO access	DBA	Completed
4	Write Scripts to kick off x-subs upon transmission of the assignment or removal of AD group "TSO.RACF" to or from an account	zOS	Completed
5	Choose test time (scheduled maintenance window, or after normal business hours)	Bill Carroll	Completed
6	Implement changes in production	DBA, zOS	Completed
7	DHHS and Clemson test changes	Brannon Wilds, Steve Blackburn	Completed
8	Changes communicated to the respective groups at DHHS and Clemson.	Brannon Wilds, Steve Blackburn	Completed
9	Training for the new process held for DHHS technicians	Brannon Wilds	Completed

NOTE: Since, all groups that end with .MEDS, .MMIS, and .RACF are already monitored and transmitted by the AD driver and IDM scripting, no changes will need to be made at those points in the AD Driver process.

Project Contacts

Name	Group	Email	Phone
Steve Blackburn	Clemson DBA	stevenb@clemson.edu	864-656-0155
Ken Culberson	Clemson DBA	CKCUL@clemson.edu	864-656-3794
Jim Blalock	Clemson zOS	CAREY@CLEMSON.EDU	864-656-3680
Jeff Bate	Clemson CSO	JEFF@CLEMSON.EDU	864-650-0448
Brannon Wilds	DHHS IT - Project Manager	wildsb@scdhhs.gov	803-898-2964
Bill Carroll	DHHS IT/Network	carroll@scdhhs.gov	803-898-2765