Disaster Recovery Plan
Starling Systems
Deliverable #15 - Draft I

STARS

Shared Tribal Automation Reporting System

Contract # 04-06

Accepted on:
March 29, 2005

Starling
Systems

Starling Systems
711 S. Capitol Way, Suite 301
Olympia, WA 98501

DISASTER RECOVERY PLAN
TABLE OF CONTENTS

Introduction

The Disaster Recovery Plan for the Inter Tribal Council of Arizona's (ITCA) Shared Tribal Automation Reporting System (STARS) describes steps to take in the event of a significant loss of service. Data processing outages could result from small scale events such as an extended power outage or processing errors that result in corrupted data, or from large scale disasters such as earthquakes, bombs, fire, flooding and flood water, storms, etc.

In addition to describing how ITCA would respond to natural disasters, sections are also included that address more common human errors and equipment malfunction. These risks are addressed by both risk mitigation and detailed recovery procedures.

The STARS Disaster Recovery Plan consists of these major sections:

Risk Analysis
This section describes specific risks that we perceive as threats to the continued operation of automated services and mitigating factors for each risk.

Preparation and Disaster Recovery at the Central Processor Site
This section describes procedures and standards that will be used to prepare for and recover from facility, equipment, and data loss at the Central Processor Site (CPS).

Preparation and Disaster Recovery at Clinic Sites
The section describes procedures and standards that will be used to prepare for and recover from facility, equipment, and data loss at ITCA clinic sites.

Disaster Recovery Test Plan for the Central Processor Site
This section describes the plan for a live test of disaster recovery procedures at the Central Processor Site.

Disaster Recovery Test Plan for a Clinic Pilot Site
This section describes the plan for a live test of disaster recovery procedures at the clinic pilot site.

There are also three Appendices in this deliverable:

Appendix A. Disaster Recovery Test Plan for the Central Processing Site
This section outlines the Disaster Recovery Test Plan for the CPS including:

- Preparation
- Synchronization server test procedure

- Consolidated data server test procedure
- Test cleanup

Appendix B. Disaster Recovery Test Plan for a Pilot Clinic
This section outlines the Disaster Recovery Test Plan for the pilot clinic including:

- Preparation
- Test procedure
- Clean up

Appendix C. STARS Manual Backup Form
This form will be used by local agency staff to gather participant information when the automated system is temporarily unavailable.

Risk Analysis

With the completion of the STARS project, continued operation of services to WIC clients will be largely dependent on access to functioning automation hardware and software components. This section describes the primary risks to the availability of automation components and summarizes mitigating tasks and infrastructure for each risk.

Risk	Mitigation
A local agency WIC facility is damaged by a disastrous event.	Technology architecture uses standard off-the-shelf equipment and configuration so installation and repair of components can be completed at a relatively low cost in a short duration. ITCA operations staff will collect and maintain a database of local agency technical resources and contacts.
A server is damaged or stolen resulting in loss of network and database services, and/or loss of database transactions.	Servers are low cost and have a standard configuration for easy repair and replacement. Databases are backed up or synchronized on a regular basis to off-site locations. Disaster recovery procedure is well defined and tested.
A physical disk drive on a server is damaged resulting in loss of database services, and/or loss of database transactions.	Central processor site servers are configured with fault tolerance architecture. Other site data servers are configured with mirrored physical drives so that all database transactions are stored on both devices.
A check printer is damaged or stolen resulting in the loss of capability to print food instruments.	ITCA maintains replacement printers in Phoenix and will ship Federal Express.
A workstation is damaged or stolen resulting in a loss of access by a single WIC staff.	ITCA maintains replacement workstations in Phoenix and will ship Federal Express.

Risk	Mitigation
A laptop server is damaged or stolen resulting in a loss of the mobile WIC database and all data entered since last synchronization.	ITCA maintains replacement laptops in Phoenix and will ship Federal Express. SCI and ITCA will develop a procedure for the user to backup the database log file onto a jump drive.

The following sections of this document describe in more detail the procedures and preparation that ITCA will use to mitigate these risks, and to respond to disastrous events that occur in spite of our best efforts at mitigation.

Assumptions

This plan is written within the context of a constantly changing set of system maintenance responsibilities and methods used by local agencies. This Disaster Recovery Plan assumes the following:

1. The Central Processor Site will be located at ITCA offices in Phoenix, Arizona.

2. ITCA will operate the Central Processor Site.

3. ITCA local agencies are responsible for providing physical structures within which the STARS system is deployed at clinic sites.

4. ITCA local agencies are responsible for maintaining local area network infrastructure (if required) at facilities where the STARS system has been deployed. ITCA may assist the local agency with funding, implementation, and/or support of a local area network infrastructure.

5. ITCA local agencies are responsible for maintaining a telecommunication connection to the clinic WIC server at the clinic as described in Deliverable 10 - Telecommunications Requirements. ITCA may assist the local agency with funding and/or implementation of a telecommunication connection.

6. ITCA is responsible for warranty repair and replacement of servers, workstations, and check printers provided by the STARS project to local agencies.

Preparation and Disaster Recovery at the Central Processor Site

Events that may result in recovery and restoration operations at the Central Processor Site (CPS) include loss of the physical structure, loss or destruction of workstations or printers, loss or destruction of one or more servers, and loss or corruption of data. Recovery steps and standards for each type of loss are described below.

Loss of the CPS Physical Structure

STARLING assumes that the loss of the CPS physical structure would be associated with a more extensive loss of ITCA services. The disaster mitigation and recovery procedures for the STARS CPS are assumed to be incorporated into the overall ITCA Disaster Recovery Plan.

To fully mitigate the loss of the CPS physical structure, ITCA will identify a backup facility that can serve as a temporary CPS facility for a period of up to 3 months. This backup temporary facility should be identified by ITCA by the start of the pilot test. There will be some additional moderate costs to retain a backup facility that must be negotiated with the backup facility provider. STARLING proposes in this document that Starling Consulting offices in Olympia be the site of this temporary facility, given the fact that Starling operations staff will most likely play an important role in recovery. ITCA may choose a different backup facility but costs to ITCA will certainly be higher and the amount of time before full services can be restored will require a longer duration. If ITCA chooses Starling to host the backup facility, the two parties will negotiate an amendment to the contract that addresses costs and timeliness.

Loss of physical structure includes both partial and full loss of use. If loss of use is partial, the existing site must be sufficiently restored to permit full operation. ITCA staff must ensure the adequacy of security, ventilation, air conditioning, power supply, and weather protection before qualifying a damaged structure for resumption of services.

In the event of damage or loss of the CPS physical structure, the ITCA operations manager will convene an emergency assessment meeting in Phoenix within 24 hours of the event. Starling operations staff will attend the meeting by telephone conference. The agenda for the emergency assessment is to determine if the current physical structure can be repaired within 5 business days or whether to transfer the CPS to the temporary backup facility.

If a determination is made to transfer the CPS to the temporary backup facility, ITCA and Starling will make a best effort to have the new backup facility in production within 5 business days. The procedure for transfer will include these steps:

1. ITCA will procure or otherwise arrange for replacement servers to be delivered to the backup facility. If most effective and timely, ITCA may ask Starling to procure or arrange for a replacement server.

2. Starling operations staff will configure the replacement servers based on specifications in the STARS Operations manual. Starling operations staff will connect the replacement servers to a local area network that is secured by firewall and password protections. Starling will complete the implementation of the replacement equipment within 2 business days of delivery of the replacement servers.

   If ITCA chooses a different backup facility, ITCA staff will be responsible for configuration of the replacement servers and implementation of the backup facility.

3. The backup facility must be able to provide bandwidth requirements specified in Deliverable # 10 - Telecommunications Requirements Plan. The Starling Operations Center will already have the required bandwidth if ITCA selects Starling for a backup facility.

4. Starling will provide system operations services as specified in the Help Desk Plan for the backup facility at rates provided in Starling's RFP response.

5. Once the facility, servers, and telecommunications have been fully installed and tested by Starling operations staff, Starling will install/recover databases and applications to the CPS servers and re-establish database synchronization using the procedures described below. Starling will transfer the fully qualified domain name of the CPS email server to the replacement email server to re-establish synchronization services. Starling will complete the final configuration of the replacement CPS within 2 business days of receipt of system backup tapes from ITCA.

   If ITCA chooses a different backup facility, Starling will work with ITCA operations staff to test the installation of the backup facility.

6. When ITCA has restored their on-site CPS facility, ITCA staff will procure, install, and configured servers at the restored site as per the Operations Manual.

7. Upon notification by ITCA that the servers are ready, Starling will send an operations staff person to Phoenix with backup tapes of the temporary servers and work with ITCA to complete the restoration and transfer of the fully qualified domain name. This work will be completed over a weekend.

Damage or Destruction of Work Station Computers and Printers at the CPS

This procedure assumes the simple loss of a single piece of equipment in the CPS without damage to the physical structure or to any CPS servers.

ITCA operations staff will arrange for the repair, replacement, and configuration of workstations and printers. The central site workstation computers and printers are standard components that can be easily replaced either by procurement or from the ready supply that ITCA will maintain for clinic sites.

Because this equipment is solely for the use of the ITCA system operator or other staff, the standard of timeliness for repair or replacement should match the general standard for ITCA technical support.

Loss or Destruction of CPS Servers

The primary risk associated with the loss of the consolidated database server or email synchronization server, is disruption of synchronization relationships between the CPS consolidated database and remote databases at clinics and the ITCA central office. Recovery from disrupted synchronization is described in the following section.

The procedure for recovery of a CPS server includes these steps:

1. ITCA will procure or otherwise arrange for replacement servers to be delivered to the CPS. ITCA will complete this delivery within 2 business days of the loss of the server. If the affected server is the consolidated data server the backup server will be temporarily reconfigured as the data server.

2. ITCA operations staff will configure the replacement server based on specifications in the STARS Operations manual within 2 business days of the loss of the server.

3. ITCA operations staff will reconnect the server to the telecommunication network and CPS local area network within 2 business days of the loss of the server.

4. Upon replacement of the server, ITCA operations staff will conduct a test of the appropriate function of the restored server (i.e. file and print, database generation and synchronization, email, communications, etc.) within 1 business day of replacing the server.

5. ITCA operations staff will restore the replacement server with backed up information from tape. Restoration and validation of backup data will be completed within 1 business day after replacing the server.

6. If the replaced server is the consolidated database server and synchronization was disrupted, ITCA staff will execute the Synchronization Recovery procedure described below.

Recovery of Database Synchronization Relationships

The most common (although rare) loss of a synchronization relationship is caused when the sequential stream of exchanged messages between the consolidated database and a clinic is corrupted. Sybase Adaptive Server Anywhere (ASA) synchronization mitigates this risk by requiring an acknowledgement of every synchronization message by the receiving database. A message sent by a database is not discarded until it has been acknowledged by the receiving database. If the receiving database receives a message out of sequence, the message is discarded and the receiving database sends an acknowledgment requesting the appropriate sequence. This automatic re-sequencing repairs most synchronization problems without operations staff even being aware there was a problem.

If the databases are not able to automatically re-synchronize, the DBA must intervene by applying unacknowledged synchronization transactions from the clinic database log into the consolidated database, then re-extracting the clinic database and reinstalling the new extraction at the clinic. While this procedure is being completed, clinic staff may not use the database. This procedure may take several hours (depending on caseload size) but it can usually wait until after business hours at the clinic, unless the DBA determines that there is substantial risk that transactions may be lost (i.e. the clinic server hardware is malfunctioning).

A "worst case" recovery scenario involves the consolidated central database being corrupted or lost and having to be recovered from tape, resulting in a loss of synchronization relationships between the consolidated database and one or more remote databases. This scenario presents with transactions originating from a remote site having been sent, recorded, acknowledged, and then lost by the consolidated database and the acknowledgement message being received and processed by the originating remote database.

The recovery process for this scenario is to manually bring each clinic database to the CPS and run a procedure that compares data between the systems and updates the consolidated database from clinic database. The clinic database is then re-extracted from the consolidated database and the new extract is delivered back to the clinic. In the worst case, this would have to be done with every local agency clinic that has a distributed database on-site.

To mitigate the risk of this “worst case scenario,” the ITCA Database Administrator will follow these procedures:

1. Ensure that daily processing of banking procedures has been completed.

2. Database synchronization processing (DBREMOTE) will always be run manually as a batch process at the Central Processor Site by ITCA operations staff.

3. Immediately following the manual synchronization processing, ITCA personnel will make a daily backup of the consolidated database server and store the backup tape in a secure facility that is off-site (i.e. in a different building than the ITCA building).

Because daily banking and database synchronization are the only transactions recorded on the consolidated database, these procedures will ensure that the worst-case scenario described above will not occur.

Preparation and Risk Mitigation at the Central Processor Site

Certain actions should be taken to minimize the risk of disaster at the Central Processor Site. These actions include modifications to the facility, the procurement of specialized hardware, and the maintenance of off-site backups and archives.

Specifications for the Central Processor Site should include:

- A hardened machine room with combination lock access and climate control.

- Filtered and dedicated power supply to servers and telecommunications equipment.

- Racks for servers and other equipment.

- Uninterruptible Power Supply (UPS) for servers and telecommunications equipment.

Other procedures and activities for mitigating risk at the Central Processing Site include:

- ITCA will implement procedures to backup all central processing site servers every day with offsite storage of backups on a daily basis.

- ITCA will maintain an archive of synchronization logs to mitigate risk of synchronization disruption.

- The Consolidated Data Server will be configured with RAID5 physical devices using hot-swappable drives providing substantial protection from database downtime in the event of a device failure. ITCA will maintain an adequate spare parts inventory to ensure no loss of data due to a hard disk failure.

- The Synchronization Server will be configured with the same components and capacity as the Consolidated Data Server so that the Synchronization Server may be pressed into service as a temporary Consolidated Data Server.

- All servers will be secured against viruses with Virus Protection services. Starling Systems has good experience with Norton virus protection software.

Preparation and Disaster Recovery at Local Agency Sites

Events that result in recovery and restoration operations at ITCA local agency facilities include loss of the physical structure, loss or destruction of workstations or printers, loss or destruction of one or more servers, and loss or corruption of data.   Recovery steps for each type of loss are described below.

The disaster recovery procedures are described here for local agencies. References to “local agency technical staff” include both ITCA and local IT staff.

Standard Configurations for Servers and Workstations

An important aspect of Starling’s technical architecture is to mitigate disaster risk by the use of standard configurations. These configurations are addressed in detail in the Operations Manual but some details are described here to illustrate the approach to disaster recovery.

Standard Server Configurations

The Starling transfer system requires that two components operate at the local agency: an Adaptive Server Anywhere database service, and the clinic application (Client Services). These components will be operated on a 'WIC Server' deployed by ITCA at each local agency.

There is no "special" configuration of the WIC server required except to make adequate disk and memory capacity available to the database service and clinic application. These capacity requirements are variable based on the number of WIC staff working concurrently at the clinic. For the purposes of hardware replacement in the event of a disaster or malfunction, the replacement server should have similar (or better) computing speed, hard disk capacity, and RAM to the server being replaced.

Starling will supply ITCA with an installation CD and written instructions for installing the ASA database service software and the clinic application. The installation CD may be installed on the server at each local agency and installations can then be completed from the server. The written instructions will recommend a call to the ITCA help desk for assistance while installing the database software and clinic application. The ITCA help desk will send replacement CDs by overnight express service upon request in the event of the loss of an installation CD.

Once the installation of the database software and clinic application has been completed locally, ITCA operations staff will complete the installation of the clinic database. ITCA operations staff will work with local agency staff to set up security and telecommunications access to the server.

Standard Workstation Configurations

Because of the remote nature of most WIC clinics, Starling's technical architecture uses a "very thin client" configuration for workstations. In order to access the clinic application, a workstation must be configured in two ways: an ODBC entry must be created that references the ASA database service, and a shortcut ICON must be created that references the clinic application. The clinic application includes a utility that can be run from the server that creates the ODBC entry on the workstation. The ITCA help desk can guide a local agency technical staff or even WIC program staff through these two simple steps.

Loss of Physical Structure

Each local agency will determine whether a facility is structurally ready to provide automation services. If a new facility is required, the following steps will be completed:

1. Identify and prepare a new facility – the local agency will locate a new facility for WIC operations. Local agency technical staff will identify locations for the server and other central equipment, and will check the adequacy of security, air conditioning, and power supply.

2. Connect facility to telecommunications network – Local agency staff will install telecommunications equipment and link the facility to the ITCA wide area telecommunications network.

3. Cable local area network – Local agency staff will install or arrange to install telecommunications drops serving users.

4. Replace facility hardware – Local agency staff will procure and install replacement workstations, server(s) and printers equivalent in functional aspects to the original.

ITCA may assist with or provide funds to the local agency for the previous steps.

5. Reinstall software – ITCA operations staff will re-extract the facility database and install the database with application software at the facility. ITCA staff will ensure that the server has been properly configured for the ASA database service and the application software. See Standard Configurations section above.

Temporary Operations Using Mobile Technology

The identification and preparation of a new facility may take several months. In the interim, the ITCA operations staff can configure a laptop and mobile network to be established at a temporary site in the community (i.e. fire station, community center, church, etc.). The following steps will be completed:

1. ITCA operations staff will re-extract the clinic database from the consolidated server.

2. ITCA system operator will download the extracted database onto the laptop along with the latest version of the Client Services application.

3. ITCA system operator will prepare additional laptops to serve as mobile workstations and assemble and test the mobile network.

4. ITCA will arrange for the shipment of the mobile equipment to the affected community along with written instructions for operation of the mobile network.

5. Local agency staff will provide services in the community as an Independent Mobile clinic.

Assuming the availability of the ITCA system operator, the laptops should be ready to transport within 24 hours of the request.

Damage or Destruction of Work Station Computers and Printers

For equipment provided by the STARS project, ITCA will repair or replace and configure the equipment. The workstation computers and printers are standard components that can be easily replaced either by procurement or from the ready supply that ITCA will maintain for clinics. Starling will provide a configuration program to ITCA technical staff for the simple configuration required of workstations.

Local agencies will be responsible for repair and replacement of other equipment. To configure a workstation to access the Client Services application, local agency staff can call the ITCA help desk. See the Standard Configurations section above.

Loss or Destruction of Facility Servers

The primary risk associated with the loss of the remote site server is disruption of the synchronization relationship between the remote server and the consolidated database at the Central Processor Site. Recovery from disrupted synchronization is described in a previous section of this document.

The procedure for recovery of a remote site server includes these steps:

1. For equipment provided by the STARS project, ITCA will repair or replace and configure the equipment. The servers are standard components that can be easily replaced either by procurement or from the ready supply that ITCA will maintain for clinics. Starling will provide a configuration program to ITCA technical staff for the simple configuration required of servers. See Standard Configurations section above.

   Local agencies will be responsible for repair and replacement of other equipment. To configure a server to host the clinic database and Client Services application, local agency staff can call the ITCA help desk.

2. Local agency staff will reconnect the server to the telecommunication network and local area network.

3. ITCA operations staff will connect remotely to configure and test the server to perform its intended function, including installation of database engines, executable code and databases.

4. ITCA operations staff will extract a new remote database from the consolidated database server, download the new extract to the server, and re-establish the synchronization relationship.

Starling recognizes that there is at least one local agency where the "server" is a stand-alone laptop that may be replicated only periodically. Starling will work with ITCA staff to configure a database log backup procedure that stores the backup on a USB drive.

During the time that a server is unavailable, clinic staff may not provide automated services and must use the STARS Manual Backup Form (See Appendix C). Once a server has been prepared by ITCA and local agency staff, ITCA staff can make the server operational within 24 hours.

Preparation and Risk Mitigation at the Clinic and Central Sites

Certain actions will be taken to minimize the risk of disaster at clinic sites. These actions include modifications to the facility and the procurement of specialized hardware.

Since the remote WIC facilities are often not under the operational control of ITCA technical staff, ITCA has limited capability to mitigate risks. However, certain actions will be taken to minimize the risk of disaster at WIC facilities. These actions are primarily focused on data backup, data synchronization, and minimizing response time to equipment failure.

- Local Automatic Backup

  Each local agency server will be installed with a USB-drive. At the end of each business day, the clinic server will be configured to automatically backup the clinic database log file onto the USB drive.

- Data Synchronization

  The synchronization of data to the central consolidated database creates a virtual backup of all clinic data. ITCA and Starling installation team will configure each clinic and central office server to synchronize one or more times per day. The final configuration schedule will depend on the reliability, performance, and function of the ITCA telecommunications network upon which synchronization exchanges will occur. In all cases, synchronization will be initiated at least once per day.

- Repair and Replacement Services

  ITCA will provide repair and replacement services. Replacement equipment will be staged at ITCA offices in Phoenix to enable them to meet this requirement.

Procedures for Equipment Replacement and Repair at Remote Sites

Earlier sections of this document describe general recovery procedures for major disasters. This section describes detailed recovery procedures for human error and equipment malfunctions that are less serious, but also are more likely to occur than a major disaster.

- Check Printer Failure

  A check printer failure will temporarily prevent a WIC clinic from printing checks. In the event of a printer failure the following steps will be taken:

  1. The ITCA help desk will contact ITCA operations staff to repair or replace the printer.

  2. If there is a second check printer in the clinic, the help desk will instruct and assist in setting up the second printer to provide print services until the replacement arrives.

  3. If there is no backup printer, the WIC clinic will begin operating using manual backup procedures (See Appendix C. STARS Manual Backup Form). WIC staff will be trained to use manual backup procedures during system training.

  4. When the printer arrives, ITCA and/or local IT staff will install the replacement, configure and test the printer.

  5. The person repairing the equipment will notify the ITCA help desk that the call has been closed.

  6. The person repairing the equipment will transport the printer to their repair facility.

  7. WIC staff will resume automated operations and complete data entry resulting from manual backup procedures.

  8. Check printers should be repaired or replaced within 1 business day.

- WIC Server Major Failure (Including Server Disk Failure)

  A WIC Server major failure will temporarily prevent the WIC clinic from providing any automated services. A major failure results in the loss of data from both disk drives. The clinic's database must be re-extracted from the consolidated database and downloaded to the clinic. All transactions made since the last synchronization are at risk of being lost.

  In the event of a WIC Server major failure the following steps will be taken:

1. The ITCA help desk staff will instruct the local agency staff to remove the USB drive (which will have the most recent backed up log file) and arrange for the USB drive to be delivered to ITCA offices in Phoenix as soon as possible.

2. The ITCA help desk will instruct WIC clinic staff to begin operating using manual backup procedures (See Appendix C. STARS Manual Backup Form).

3. When the USB drive is delivered to ITCA, the Database Administrator will recover database transactions from the backed up log file on the USB drive, then extract a new facility database.

4. ITCA will install the new database extract on a replacement server and dispatch a repair person to the facility with the replacement server.

5. When the repair person arrives they will install the replacement server on the network backbone, and configure and test (See Standard Configurations section above).

6. The repair person will notify the ITCA help desk that the call has been closed.

7. The repair person will return the damaged server to their repair facility.

8. WIC staff will resume automated operations and complete data entry resulting from manual backup procedures.

The recovery of data transactions from the USB drive and replacement of the server should be completed within 2 business days.

- Workstation Failure

  A workstation failure will temporarily prevent the WIC clinic from providing automated services from that workstation.

  In the event of a workstation failure the following steps will be taken:

1. The ITCA help desk will dispatch the repair person to the facility with a replacement workstation.

2. When the repair person arrives they will install the replacement workstation on the network backbone, and configure and test (See Standard Configurations section above).

3. The repair person will notify the ITCA help desk that the call has been closed.

4. The repair person will return the workstation to their regional center for repair.

The replacement of a workstation should be completed within 1 business day.

Disaster Recovery Test Plans

The appendices to this deliverable contain disaster recovery test plans for the central processor site and the clinic pilot site. These disaster recovery test plans are assumed to be incorporated into the overall ITCA Disaster Recovery Plan and are written as if ITCA operations staff are fully responsible for conducting the tests. The initial running of these tests, during the Acceptance Test and Pilot Test phases of the project, will be conducted jointly with Starling operations staff directing ITCA operations staff.

Central Processor Site Test Plan

During the final weeks of the Acceptance Test, ITCA and Starling operations staff will fully configure the Central Processing Site and populate the production database server with migrated vendor and participant data from the WIC Ed system. Starling will extract a clinic database and place it on a different server (i.e. a separate server from the CPS server).

ITCA operations staff will then simulate the loss and recovery of each server in the Central Processing Site. See Appendix A for a detailed Disaster Recovery Test Plan for the Central Processing Site.

Clinic Pilot Site Test Plan

During the pilot test period, ITCA will conduct a test of disaster recovery procedures for the pilot site by simulating the total loss of the clinic WIC server. This test will be carried out on a day when the clinic is not providing WIC services to minimize the impact on WIC services.

The Pilot clinic will be in full production during the pilot test, so these tests will be conducted in a true production environment. See Appendix B for a detailed Disaster Recovery Test Plan for the Pilot Clinic.

Appendix A: Disaster Recovery Test Plan for the Central Processing Site

This test will be conducted in the final weeks of the Acceptance Test.

Preparation

Fully configure the Central Processing Site with these servers:

- Synchronization Server (Exchange email service)
- Consolidated Data Server

For the purposes of the test, provide an additional server:

- Clinic server

The additional server will be used to simulate a clinic server during the test. They can be re-allocated after the test to other uses.

ITCA staff will use migrated WIC Ed vendor and clinic data to populate the consolidated data server. Extracts will be created for the simulated clinic and deployed on the clinic server.

The database extract will be configured to use the SMTP protocol for synchronization, and email accounts will be created on the Synchronization Server for the consolidated database and the clinic extract.

Full tape backups will be made of all CPS servers.

The test will be conducted by ITCA operations staff members. The test will be observed by other ITCA, BCA, and Starling staff. The test will take place entirely on-site at the Central Processing Site.

Synchronization Server Test Procedure

This test will simulate the complete loss of the Synchronization Server. The scenario is this: Sometime in the late evening, the Synchronization Server has a hard disk failure that destroys the Exchange email database that holds all of the email accounts for clinic server synchronization. Of the 13 clinic servers that normally exchange synchronization messages each night, about half have already completed their connection and dropped off synchronization messages (which have been destroyed by the crash). For the rest of the night, all other clinic servers try to synchronize but fail due to the crashed Synchronization Server.

The ITCA operations staff initiate connection to the CPS at 8:00 A.M. MT to run the routine Replication Report against the Consolidated Data Server, which indicates that only about half of the clinics succeeded. After some investigation, ITCA operations staff determine that the Synchronization Server is not operating and that the machine just won't start. At this point, the Disaster Recovery procedure for replacing the Synchronization Server begins.

1. Clear all synchronization messages by forcing replication on all servers (Synchronization and Clinic).

2. Use the Client Services application on the Clinic server to create a new WIC applicant. Force a replication on the Clinic server. This creates an incoming message in the Synchronization Server. Do NOT force a replication on the Consolidated Data server.

3. Shut-down the Synchronization Server and disconnect it from the network. This simulates a dead server. Note that the new client transaction messages are now "destroyed."

4. The Backup Server will be used to temporarily host the Synchronization Service until a backup server can be brought in. The Consolidated Data Server will be pre-installed with Exchange 2003 and the fully qualified domain name of the Exchange Server so that it can be recognized by clinic servers.

5. ITCA Operations staff will recover the Exchange email database from the backup tape onto the Backup Server. Confirm that email addresses are in the Exchange service for the Consolidated, and clinic servers. Delete any replication messages in those mailboxes.

At this point, the Synchronization Server has been recovered and is ready to resume service. The only problem is that the replication message has been lost (new client). In the scenario described above there could be hundreds of messages lost. The remainder of the test demonstrates how SQLAnywhere will automatically repair the loss of synchronization messages.

6. On the Clinic server using the Client Services application, create another new WIC applicant. Force a replication on the Clinic server. This will create another incoming message for the Consolidated Data server.

7. Force a replication on the Consolidated Data server. The Consolidated Data server will detect a gap in sequence for the Clinic messages (the "destroyed" messages) and will respond to the clinic server asking for a re-send of those missing messages.

8. Force a replication on the Clinic server. The clinic servers will receive the re-send request and send the missing messages.

9. Force a replication on the Consolidated Data server which will now have the missing messages.

10. Use ISQL on the Consolidated Data server to confirm that the new client records have been received. Confirmation of these records on the Consolidated Data server signifies a successful test.

In a production environment, once the Synchronization Server has been brought back on line, ITCA help desk staff would telephone each of the clinics and ask a WIC staff person to double click on the "Force Synchronization" icon on the clinic server desktop. This will protect the previous day's transactions and bring the Consolidated Data server up to date for creation of check issuance files for FSMC, the Banking Services contractor.

Consolidated Data Server Test Procedure

This test will simulate the complete loss of the Consolidated Data Server. The scenario is this: Sometime in the late evening, the Consolidated Data Server has a hard disk failure that destroys the consolidated ITCA database that holds all of the STARS system data. Throughout the night clinics continue to synchronize, dropping off messages in the Synchronization Server which is unaffected by the Consolidated Data Server crash.

The ITCA operations staff initiate connection to the CPS at 8:00 A.M. MT to run the routine Replication Report against the Consolidated Data Server, which fails to respond. After some investigation, ITCA operations staff determine that the Consolidated Data Server is not operating and that the machine just won't start. At this point, the Disaster Recovery procedure for replacing the Consolidated Data Server begins.

1. Clear all synchronization messages on the clinic server by forcing replication.

2. Use the Client Services application on the Clinic Server to create a new WIC applicant. Force a replication on the Clinic server. This creates an incoming message in the Synchronization Server. Do NOT force a replication on the Consolidated Data server.

3. Shut-down the Consolidated Data Server and disconnect it from the network. This simulates a dead server.

4. The Backup Server will be used to temporarily host the Consolidated Data Service until a replacement machine can be brought in. ITCA Operations Staff will use a written procedure to configure the Backup Server with SQLAnywhere RDBMS to host the consolidated database.

5. ITCA operations staff will recover the consolidated database from the backup tape onto the Backup Server. Confirm that the database is operational by using ISQL.

6. At this point, the Consolidated Data Server has been recovered and is ready to resume service.

7. Force a replication on the Consolidated Data server which will now apply the messages that were waiting in the Synchronization Server.

8. Use ISQL on the Consolidated Data server to confirm that the new applicant records have been received. Confirmation of these records on the Consolidated Data server signifies a successful test.

Test Cleanup

1. Connect all of the original machines back into the CPS network.

2. Remove the Exchange 2003 from the Consolidated Data Server.

3. Remove the consolidated database from the Backup Server.

4. Re-allocate the temporary Clinic server for other uses.

Appendix B: Disaster Recovery Test Plan for the Pilot Clinic

This test will simulate the loss of a clinic data server at a real WIC clinic that is already in production. The test will be conducted on a Saturday within a month after the pilot test has been started.

The test will be conducted long distance and remotely. ITCA operations staff will be working from the Central Processing Site. An ITCA central office staff person will participate from the pilot clinic. The test will be observed by other ITCA, BCA, and Starling staff on-site in Arizona.

Preparation

ITCA will prepare a replacement server to replace the server that will suffer a simulated crash at the pilot clinic site. The replacement server will be configured with SQLAnywhere RDBMS and Terminal Services. It will also be loaded with the most recent version of the Client Services application. This will be a standard configuration for servers that are kept ready as replacements by ITCA.

The ITCA central office staff person who is on-site at the clinic will initiate the test by calling the ITCA help desk. ITCA operations staff will ask the ITCA program staff person to double click on the “Force Synchronization” icon on the pilot clinic server desktop to ensure that all transactions have been received at the CPS. ITCA operations staff will connect to the CPS to force replication at the consolidated site. ITCA operations staff will use the Daily Replication report to confirm that the clinic has successfully synchronized.

Test Procedure

This test will simulate the malfunction of one of the server’s hard disks late in the afternoon. Clinic staff will experience a system lockup and call the ITCA help desk. The help desk will determine that there is a server problem and initiate a repair and replacement call with ITCA. The test steps are:

1. ITCA operations staff will direct the ITCA central office staff person to logon to the Client Services application and select a random client. For that client, the ITCA central office staff person will change the client’s family address and print checks for a month. This will create a number of transactions on the clinic database that have not been synchronized to the CPS.

2. ITCA operations staff will direct the ITCA central office staff person to find the database log file and copy it to a backup device. This simulates the ability to get the database log file from either of the server’s hard disks.

3. ITCA operations staff will direct the ITCA central office staff person to shut down the server and to go out for coffee while they await the arrival of help from Phoenix.

4. The ITCA staff person who is at the clinic will email the database log file to ITCA operations to speed up the test. In a real production environment, it may take much longer for the log file to get to ITCA operations.

5. Upon notification that the server has been shut down and the coffee break started, ITCA operations staff will manually apply the database log file sent from the clinic to the consolidated database.

6. ITCA operations staff will re-extract the clinic database at the CPS.

7. ITCA operations staff will copy the new extract onto the replacement server and confirm that it is operational.

8. ITCA operations staff will transport the replacement server to the pilot clinic giving the staff there an ETA so they can enjoy their coffee.

9. ITCA operations staff will meet the clinic staff and replace the server, connecting it to the network and to the telecommunications link. ITCA operations staff will boot the server and confirm that the database is operational and the server is configured for that clinic.

10. The ITCA central office staff person will use the Client Services application to confirm that the address and check records that were created at the beginning of the test are in the database brought from Phoenix. Confirmation of those changes indicates a successful test.

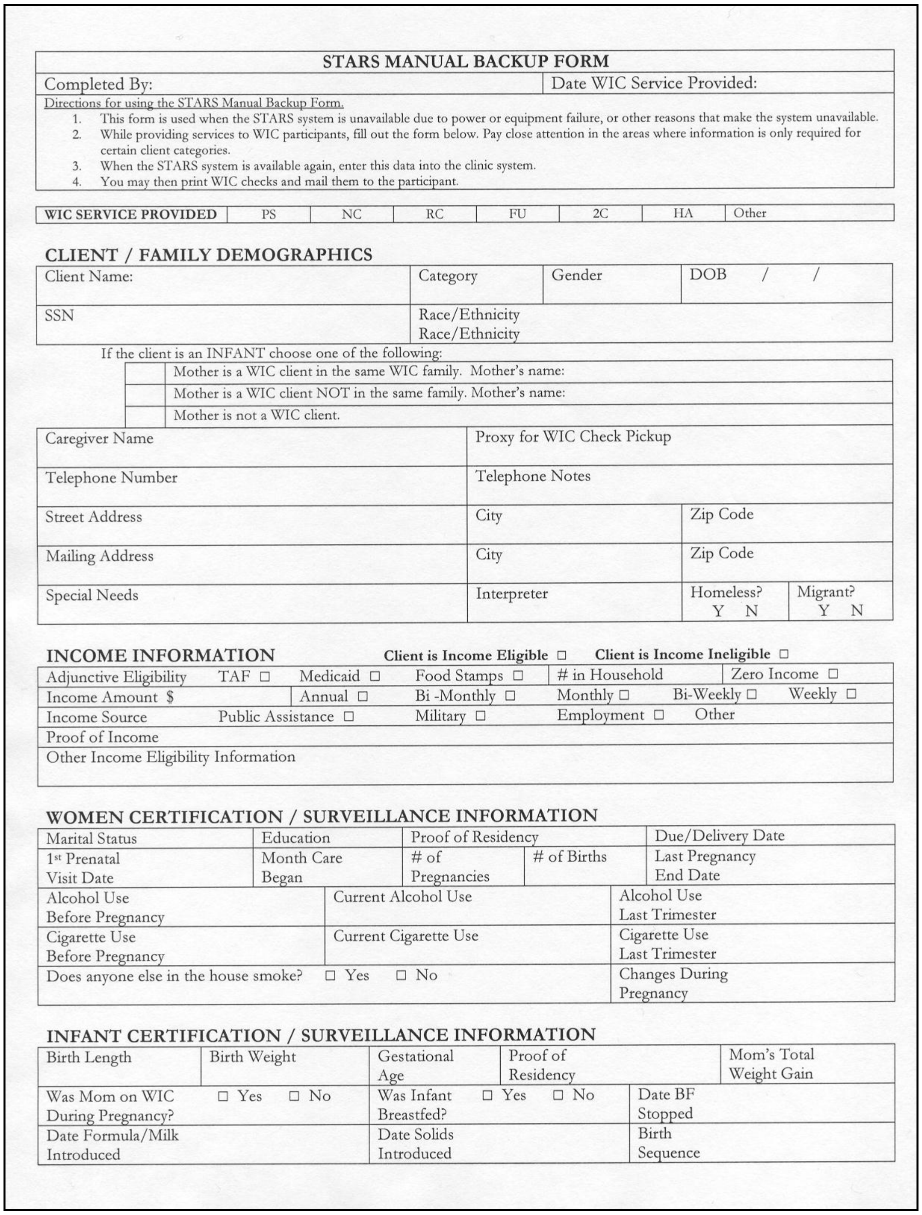
Clean Up

1. The ITCA central office staff person must be sure to Void the checks and change the address of the client's family back to its previous value.

2. ITCA operations staff will return the replaced server to Phoenix where it will serve as a future replacement.

Appendix C: STARS Manual Backup Form

The STARS Manual Backup Form will be used by local agency staff to gather participant information when STARS is temporarily unavailable. The sample below was developed for the Kansas WIC system (KWIC). It will be revised to include ITCA STARS specific data fields.



STARS MANUAL BACKUP FORM

Completed By:	Date WIC Service Provided:

Directions for using the STARS Manual Backup Form.

1. This form is used when the STARS system is unavailable due to power or equipment failure, or other reasons that make the system unavailable.
2. While providing services to WIC participants, fill out the form below. Pay close attention in the areas where information is only required for certain client categories.
3. When the STARS system is available again, enter this data into the clinic system.
4. You may then print WIC checks and mail them to the participant.

WIC SERVICE PROVIDED	PS	NC	RC	FU	2C	HA	Other

CLIENT / FAMILY DEMOGRAPHICS

Client Name:	Category	Gender	DOB / /
SSN	Race/Ethnicity Race/Ethnicity		

If the client is an INFANT choose one of the following:

	Mother is a WIC client in the same WIC family. Mother's name:
	Mother is a WIC client NOT in the same family. Mother's name:
	Mother is not a WIC client.

Caregiver Name	Proxy for WIC Check Pickup		
Telephone Number	Telephone Notes		
Street Address	City	Zip Code	
Mailing Address	City	Zip Code	
Special Needs	Interpreter	Homeless? Y N	Migrant? Y N

INCOME INFORMATION

Client is Income Eligible □ **Client is Income Ineligible** □

Adjunctive Eligibility	TAF □	Medicaid □	Food Stamps □	# in Household	Zero Income □
Income Amount $	Annual □	Bi -Monthly □	Monthly □	Bi-Weekly □	Weekly □
Income Source	Public Assistance □	Military □	Employment □	Other	
Proof of Income					
Other Income Eligibility Information					

WOMEN CERTIFICATION / SURVEILLANCE INFORMATION

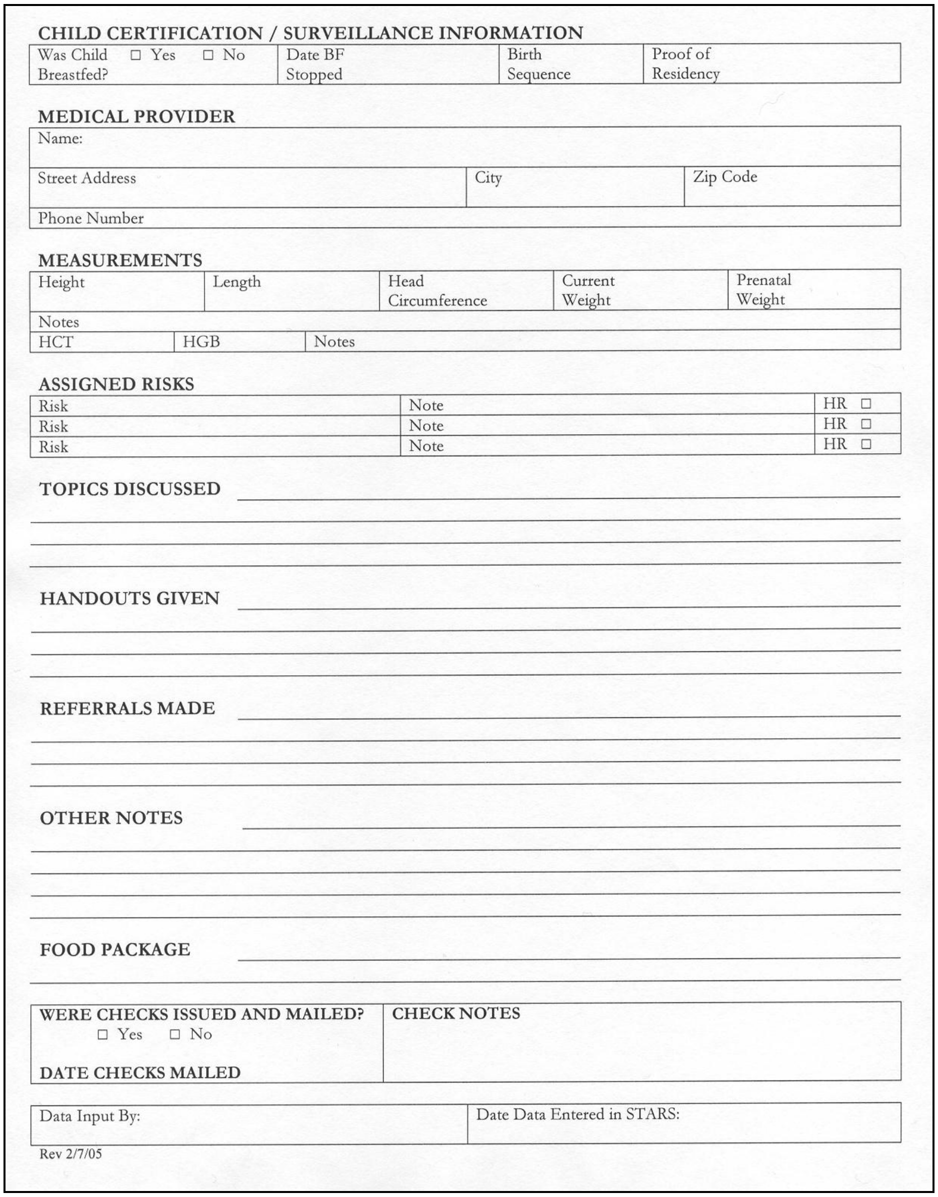
Marital Status	Education	Proof of Residency		Due/Delivery Date
1st Prenatal Visit Date	Month Care Began	# of Pregnancies	# of Births	Last Pregnancy End Date

Alcohol Use Before Pregnancy	Current Alcohol Use	Alcohol Use Last Trimester
Cigarette Use Before Pregnancy	Current Cigarette Use	Cigarette Use Last Trimester
Does anyone else in the house smoke? □ Yes □ No		Changes During Pregnancy

INFANT CERTIFICATION / SURVEILLANCE INFORMATION

Birth Length	Birth Weight	Gestational Age	Proof of Residency	Mom's Total Weight Gain

Was Mom on WIC During Pregnancy? □ Yes □ No	Was Infant Breastfed? □ Yes □ No	Date BF Stopped
Date Formula/Milk Introduced	Date Solids Introduced	Birth Sequence



CHILD CERTIFICATION / SURVEILLANCE INFORMATION

Was Child Breastfed? □ Yes □ No	Date BF Stopped	Birth Sequence	Proof of Residency

MEDICAL PROVIDER

Name:		
Street Address	City	Zip Code
Phone Number		

MEASUREMENTS

Height	Length	Head Circumference	Current Weight	Prenatal Weight
Notes				
HCT	HGB	Notes		

ASSIGNED RISKS

Risk	Note	HR □
Risk	Note	HR □
Risk	Note	HR □

TOPICS DISCUSSED ______________________________

HANDOUTS GIVEN ______________________________

REFERRALS MADE ______________________________

OTHER NOTES ______________________________

FOOD PACKAGE ______________________________

WERE CHECKS ISSUED AND MAILED? □ Yes □ No DATE CHECKS MAILED	CHECK NOTES

Data Input By:	Date Data Entered in STARS:

Rev 2/7/05