computerframeworks
ABN 61 087 798 909
Suite 1, Level 9
109 Pitt Street
Sydney NSW 2000

☎ +61 2 9232 7007
+61 2 9232 7799
office@cfworks.com.au
www.computerframeworks.com.au

White Paper:

Reporting Solution Architecture

Reporting Solution Architecture

THE PROBLEM

Old systems in growing organizations require an extensive system upgrade that would offer significantly greater dependability, higher performance, and self-service. Companies require this upgrade in order to maintain growth and stability through efficiency melded harmoniously with accuracy. Computer Frameworks was engaged to assess and develop the required software.

THE SOLUTION

Computer Frameworks designed a system upgrade project, which is a software development project for replacing an end-user system with a new, server-oriented system offering greater dependability, higher performance, and self-service. This document covers the overall Solution, including aspects of functionality, technologies used to implement, software architecture, hardware requirements, and business continuity.

1 System Context

1.1 System Context Diagram

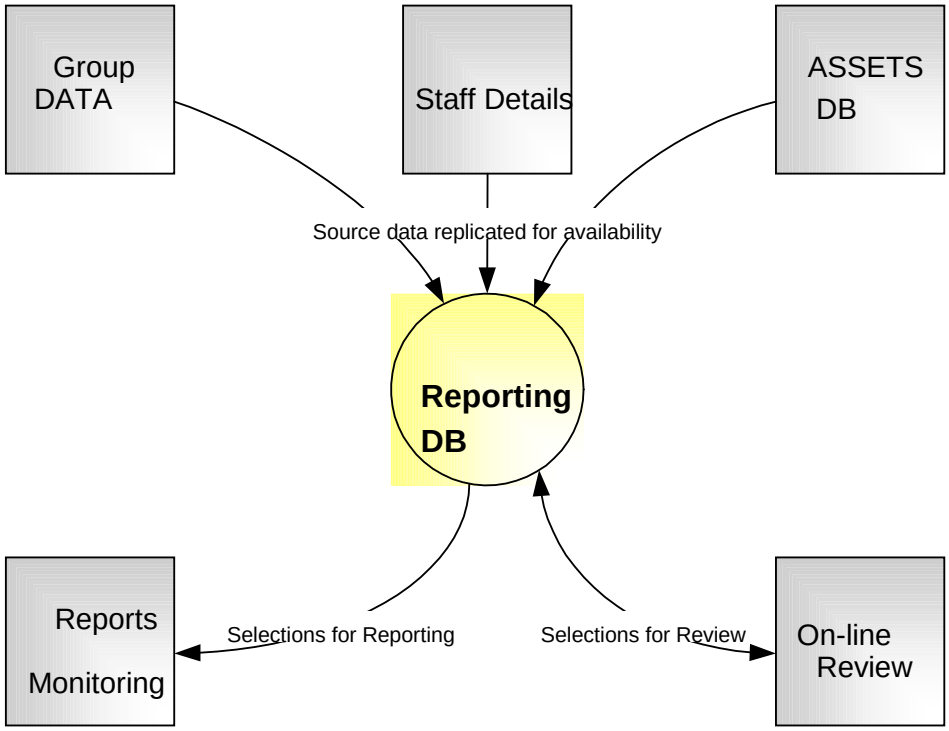

Figure 1-1 System Context Diagram

1.2 Interfaces

There are several types of interface, the Group Data, which is a database that holds information on clients across the Group. The Staff data that holds staff detail because the reporting DB requires some details about people and staff positions. This data will be sourced from an INFORMIX database and STAFF DB, which originally sourced its data from the Peoplesoft database. The third is the assets database, which is simply an operational system for the management of company assets. The reporting database, which is for the active users of the application, it creates reviews, reports and performing selections against the candidate data. The staff members in the reporting database needs to be able to access this interface while they are online.

1.3 Users and Transactions

The users of the Reporting DB application will range in computer experience from expert to complete novice and at times, there will be “guest” reviewers brought in to assist with specific reviews and reports. These people will naturally have had little or no exposure to the application. At present there are 15 afore mentioned reviewers, who go into the field to perform their reviews and reports.

For other users of different applications, they will be able to obtain their review data from the Reporting DB and import it into their system.

2 Solution Architecture

2.1 Summary of Business Requirements

See Diagram below.

2.2 Application Architecture

The Solution will be a client / server application. Due to the requirement for the Solution to operate both in a fully networked environment and in a mobile, disconnected environment, the Solution will support both the traditional client / server model as well as an "off-line" mode whereby data excerpts can be loaded into a local database from a CD.

The server will be a Microsoft Windows 2000 Server computer with a Microsoft SQL Server 2000 database server. This database will utilise DTS Import Packages to extract the necessary data.

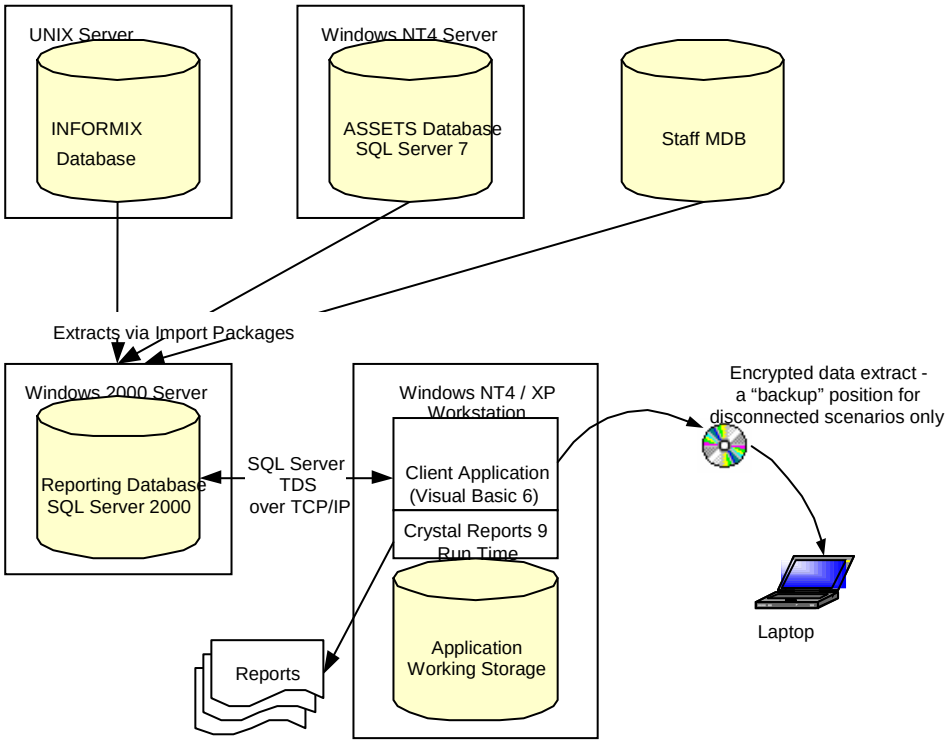

Figure 2-1 Application Architecture

The client application will be a Microsoft Visual Basic 6 application running on either Windows NT4 Workstation, or (if available) Windows XP Professional.

Much of the application will be coded as database stored procedures, leveraging the data manipulation strengths of the SQL Server 2000 database when in online mode. For offline mode, the same functionality will be simulated with stored queries in JET, or duplicated with stored procedures in MSDE 2000 (using the same script code).

For working in off-line mode, the Solution will provide for extraction of data from the server to a file for loading into Application Working Storage on the client. The file will be encrypted / decrypted using the Microsoft Crypto library. Once encrypted, the file can be burned to a CD for distribution to remote sites.

Reporting from the application will be implemented using Crystal Reports, allowing for printed-paper as output, Adobe Acrobat PDF file, Microsoft Excel .xls, and Microsoft Word document, amongst other options.

2.3 Data Architecture

2.3.1 Database Server

The server will use Microsoft SQL Server 2000 for data storage. Most of the data will be sourced from the Group database, however, due to availability issues with this database, the necessary data will be extracted on approximately a nightly basis and stored in the Reporting DB database server.

Staff information will be refreshed from Peoplesoft on a regular basis.

This provides an opportunity to divide the Reporting DB database into two pieces: infrequently imported data, and day-to-day running data. Segregating the data in this way offers the option of physically separating the tables across two file groups, providing greater flexibility as itemised below.

- Future scalability is easily provided for, as the separate file groups can be moved to separate I/O channels and disc sub-systems without the need to restructure the whole database
- Maintenance activities can be organised more efficiently according to the frequency with which the different data is updated: imported data in an IMPORTS file group can be consistency checked and backed up after import, e.g. monthly, whereas day-to-day data in the PRIMARY file group can be consistency checked and backed up more frequently
- Recovery after a failure is assisted by reducing the impact of losing one data file
- Recovery after a failure is assisted by allowing infrequently changing data to be preloaded on a hot standby system or Disaster Recovery system, so that only the PRIMARY file group needs to be restored from tape

Additionally, it is recommended that the data files be placed on striped disc volumes, preferably on a disc sub-system organised as a single RAID 0,1 volume. RAID 0,1 provides disc striping for increased performance, as well as disc mirroring for redundancy. Alternatively, the more cost-efficient RAID 5 organisation can be used, which gains redundancy through data parity information storage, but at a cost to update performance.

2.3.2 Application Working Storage

Application working storage on the client PC is subject to security standards, and as such any data in local storage must be encrypted. Because the standard desktop offering for Reporting DB staff includes Windows NT4 Workstation, which does not support encrypted file systems; the database must be capable of implementing data encryption.

The preferred tool for implementing robust, high-performance single-user databases on Windows is MSDE 2000. However, this does not implement encryption, instead relying on the EFS within Windows 2000 or Windows XP. It is planned that in a later phase of the project, Reporting DB client application will be deployed to Windows XP Professional and at this time, MSDE 2000 will be utilised for application working storage.

In the initial phase of the project, however, application working storage will be implemented using the Microsoft JET database, which supports encryption of data.

2.4 Network and Data Flow

The Reporting DB central server will be a Microsoft SQL Server 2000 service running under Windows 2000 Server on a server computer at the Production site.

The Reporting DB server will have network access to perform data extracts from GROUP and ASSETS (phase 2) at scheduled or *ad hoc* times. The volume of data transferred from the GROUP database is estimated to be between 10 and 20 gigabytes. This data transfer will most likely occur monthly, with the possibility of infrequent *ad hoc* transfers. Because of the size of the transfer, a high-speed network link will be required. It is recommended that the Reporting DB server be collocated with the GROUP server on the same 100 Mbps Ethernet subnet. It is assumed that similar requirements will exist for ASSETS, but this is yet to be investigated.

2.5 Application Security

2.5.1 User Authentication

All users of the Solution must be authenticated before access is granted. User authentication by the Solution will be aligned with Microsoft user authentication policies, as detailed below:

- All passwords must be at least eight alphanumeric characters long.
- Passwords will not display on their screen when users enter their passwords.
- Passwords must be forced to change every 26 to 30 days.
- A password history of at least 15 previous passwords will be denied reuse.
- All new user or reset passwords will be set up as expired passwords. Expired passwords must be changed the first time they are used. Unused expired passwords will be revoked / disabled after 14 days.
- Inactive accounts will be locked / disabled after 60 days (configurable in the Solution)
- Users will be revoked / disabled from the system after 5 unsuccessful attempts to enter their password. Once revoked, Users must call their HELP Desk to have their password reset.
- Passwords must not be:
    - Held in clear text;
    - Included in job control or configuration listings
    - Stored in the Programmable Function (PF) keys of personal computers,
    - Stored in spreadsheet or word processing macros, or within applications

User authentication will be implemented by storing user Ids and encrypted passwords in the database. The passwords will be encrypted with MD5, a one-way hash algorithm. Using a one-way hash ensures that passwords cannot be decrypted. Because it is possible to discover a password sing a brute-force approach, the encrypted password field will not be accessible to any user connection.

To support user authentication in offline mode, the mobile computer's user must initialise their password on the mobile computer (e.g. laptop) when in online mode so that they can be authenticated against the main database. A separate MD5 hash of their password will then be generated for storing in the encrypted application working storage database.

2.5.2 User Restrictions

Users will be restricted in their actions in the Solution by their assigned Roles (Groups) and Permissions.

The solution will have a variety of specific permissions defined, to a level of detail sufficient to permit or deny each high-level action in each functional module of the System. For example, the Selections module might have different available permissions for viewing, executing, and modifying a selection.

A range of roles will be established, each with a different set of granted permissions. To align with the functional requirements documentation, these roles will be called Groups. The following roles are known to be required, as stated in the functional requirements:

- System Administration
- Business Administration
- Senior User
- User
- Guest User

2.5.3 Database Security

All database connections will be authenticated connections with defined levels of restricted access.

Connections to the database server will be made using 128-bit SSL connections. This will ensure that all data that moves across the network from the server to the clients will be encrypted.

It is possible, but not recommended, to place the database files in encrypted folders using the Encrypted File System (EFS). Whilst this offers additional physical security over the data, it can adversely affect the server in the following ways:

- Data retrieval and update performance will incur approximately a 5% penalty for the additional processing required to encrypt / decrypt each file system block
- System recovery after a failure may become more complex, as the disc files will only be readable by the SQL Server user (typically SYSTEM), and there is anecdotal evidence that file recovery procedures without the correct user token are problematic at best
- Thus, frequent, verifiable data backups will become even more crucial to any business continuation plan

As such, it is recommended that EFS not be used for the server database files. Instead, proper physical security and security procedures should be instigated to ensure that the files could not be accessed in any way other than by secured database connections.

All data storage on the client computer will be encrypted. It is anticipated that the client computers initially will have Windows NT4 Workstation, so the application working storage will be a JET database with JET data encryption

2.6 Implementation Technologies

2.6.1 Application Development

Class	Product	Purpose	Comments
Development Tool	Visual Basic 6	Developing the Reporting DB client application	• Capable of calling most Windows API system functions • Must be patched with at least Service Pack 5
Reporting	Crystal Reports 9	Developing reports to be distributed with the Reporting DB client	• Capable of producing printed reports and disk files in a variety of formats • Runtime-only environment required for client computers to run reports • Runtime to be deployed as part of Reporting DB client install
ActiveX Components	Microsoft Data Access Components 2.6 service pack 2	Components for manipulating data in databases from program logic	• Includes OLE-DB sub-system and drivers for common databases, including Microsoft SQL Server • Includes ADO 2.6 components for providing data access to Visual Basic and VBScript • MDAC 2.6 is not currently compatible with Microsoft SQL Server clustering; not a Reporting DB requirement
ActiveX Components	JET 4.0	Components for managing ISAM databases	• Allows manipulation of JET databases including .MDB files • Supports encryption of databases

Database Server	MSDE 2000	Database management and storage for Reporting DB client when disconnected	• Programmatically compatible with SQL Server 2000 • Has no support for encryption of databases; relies on operating system

2.6.2 Database Server

Class	Product	Purpose	Comments
Operating System	Windows 2000 Server	System services for running database server	• Must be patched with at least Service Pack 2 at install, recommend Service Pack 3
Database Server	Microsoft SQL Server 2000	Database management and storage for Reporting DB	• Must be patched with at least Service Pack 3 • Full Text Search option not required • English Query option not required

2.6.3 Client Computer – Initial Target

Class	Product	Purpose	Comments
Operating System	Windows NT4 Workstation	Desktop for workstations and laptops	• Must be patched with at least Service Pack 6a at install
Application	Reporting DB Client	Client application for Solution	• Installation of this application includes following components
Reporting	Crystal Reports 9 Runtime	Run the pre-written reports deployed with Reporting DB client	• Does not supply users with tools for developing their own reports
ActiveX Components	Microsoft Data Access Components 2.6 service pack 2	Components for manipulating data in databases from program logic	• Includes OLE-DB sub-system and drivers for common databases, including Microsoft SQL Server • Includes ADO 2.6 components for providing data access to Visual Basic and VBScript • MDAC 2.6 is not currently compatible with Microsoft SQL Server clustering; not a Reporting DB requirement
ActiveX Components	JET 4.0	Components for managing ISAM databases	• Allows manipulation of JET databases including .MDB files

2.6.4 Client Computer – Final Target

Class	Product	Purpose	Comments
Operating System	Windows XP Professional	Desktop for workstations and laptops	• Must be patched with at least Service Pack 1 at install
Application	Reporting DB Client	Client application for Solution	• Installation of this application includes following components
Reporting	Crystal Reports 9 Runtime	Run the pre-written reports deployed with Reporting DB client	• Does not supply users with tools for developing their own reports
ActiveX Components	Microsoft Data Access Components 2.6 service pack 2	Components for manipulating data in databases from program logic	• Includes OLE-DB sub-system and drivers for common databases, including Microsoft SQL Server • Includes ADO 2.6 components for providing data access to Visual Basic and VBScript • MDAC 2.6 is not currently compatible with Microsoft SQL Server clustering; not a Reporting DB requirement
Database Server	MSDE 2000	Database management and storage for Reporting DB client when disconnected	• Programmatically compatible with SQL Server 2000 • Has no support for encryption of databases; relies on operating system

2.7 Hardware Requirements

2.7.1 Database Server

Component	Minimum	Recommended
Computer System	Compaq ProLiant • High-Availability Intel server • 1 or 2 Pentium III CPU • Up to 4GB RAM • Hot-plug power, fans	Compaq ProLiant ML370 G3 • Intel Server • 1 or 2 Xeon CPU • Up to 12GB RAM • Redundant power, fans
Processor	1 x Pentium III @ 1.2GHz	2 x Xeon @ 2.8GHz
RAM	512MB RAM	1GB RAM
Hard Discs	3 x 36GB Ultra Wide SCSI RAID Controller using RAID 5	5 x 36GB Ultra Wide SCSI RAID Controller using RAID 0,1
Network	As necessary for CBA environment	100MHz Ethernet or better

2.7.2 Client Workstation

Component	Minimum	Recommended
Computer System	Dell GX-200 • 1 Pentium III CPU • Up to 1GB RAM	Compaq EVO D320 ST • 1 Pentium 4 CPU • Up to 1GB RAM
Processor	1 x Pentium III @ 500MHz	1 x Pentium 4 @ 2GHz
RAM	128MB RAM	256MB RAM
Hard Discs	10GB IDE	40GB IDE
Network	As necessary for CBA environment	As necessary for CBA environment

2.7.3 Client Laptop

Component	Minimum	Recommended
Computer System	IBM series 240 • 1 Pentium III CPU • Up to 1GB RAM	Compaq EVO N610c • 1 Pentium 4 CPU • Up to 1GB RAM
Processor	1 x Pentium III @ 500MHz	1 x Pentium 4 @ 2GHz
RAM	128MB RAM	256MB RAM
Hard Discs	30GB IDE	40GB IDE
CD / DVD	CD-ROM	DVD-ROM
Modem	56Kbps	56Kbps
Network	As necessary for CBA environment	As necessary for CBA environment

The Solution will support a configuration whereby only one removable storage device is available at any given time, allowing the use of laptops that require the floppy disk drive and CD-ROM drive to be interchanged as required.

2.8 Disaster Recovery / Business Continuity

2.8.1 Data Backups

Data backups will be required on a regular basis, as historic selections and reviews and reports will be stored on the Reporting DB database server, along with user administration data. The recommended strategy is to perform a full backup once a week, and smaller, differential backups, each night in between (with the possible exception of Sunday night).

Each time a data extraction from GROUP is brought into Reporting DB, a full backup should be run regardless of where in the backup schedule the extraction / import occurs. This will prevent a blowout in the size and required time for a differential backup.

Alternatively, since the data will be segregated into two file groups, the GROUP extract data could be backed up separately whenever it is refreshed, and the other data backed up fully each night. NB: differential backups are only possible against the complete database, not individual file groups; in addition, transaction logs will need to be explicitly added to the backup.

Because of the confidential nature of the data stored in the Reporting DB database, the backups of this database should be made with encryption enabled, and tight physical security maintained over the tapes

themselves. If encrypted backups are not available with the backup software used, then physical security will become critical.

2.8.2 Disaster Recovery

Similarly to Business Continuity, if the database server is destroyed through some catastrophic event and a Disaster situation is declared, then the Reporting DB database server will need to be established on an alternate server. It is recommended that a suitable DR server be provisioned to meet the minimum server specification above, however it would be possible to share one SQL 2000 Server for multiple applications in DR to assist in reducing the cost to the business. The DR plan for Reporting DB should follow the DR plan for the GROUP database.

To ensure that the database can be recovered from backup tapes, either the original or duplicate backup tapes will need to be taken to the DR centre for restoring the server.

Since the backup tapes will most likely be required for both BCP and DR, it is recommended that the full backup tapes are duplicated and copies held at the DR site. Additionally, each time a differential backup is taken, the previous differential backup should be taken to the DR site. Then BCP can occur with the latest tapes, DR is guaranteed of being no more that 48 hours out of date, and there will still be a good chance that the latest differential can be recovered and taken to the DR centre for a more recent recovery.

2.9 Configuration Management

The Solution is delivered as a Microsoft SQL Server 2000 database with stored procedures, and a Windows GUI application.

All source materials used to create and maintain the system will be stored in a version control system with configuration management methods applied to track releases and release assemblies.

2.9.1 Database

The database will be deployed by means of scripts and data loads. The scripts will create tables, referential integrity constraints, views, triggers and stored procedures. The data loads will be implemented as DTS scripts.

Any changes to the database, both during the initial build phases of the project and during the maintenance phase, will be implemented via scripts so that changes can be exactly reproduced in development, test and production environments.

2.9.2 Client Application

The client application will be implemented by means of Visual Basic source code compiled into an executable; the Crystal Reports run time; and an assortment of ActiveX controls and components including MDAC and JET or MSDE.

Deployment of the client application will be via an installation program, which will install the client application executable, the run times, and ActiveX controls and components.

The client program will create the JET or MSDE database for local application working storage (offline mode) on the first time run of the program. For MSDE, the user of the client application should be logged in to the computer, so that EFS will use the correct private key to encrypt the database.

All items required for deployment will be stored in the version control system.