OWNER:	ISSUE DATE:	VERSION:
CUST-DEV2	13/12/2010	1.01

TAXATION AND CUSTOMS UNION DG

SUBJECT:

DLV-0.1-1_Set up, Install, Operate and Maintain the IT and Telecom Infrastructure

CUST-DEV2

[REMOVED]

DOCUMENT HISTORY

Version	Date	Description	Action (*)	Pages
0.01	13/08/2010	Creation	I	All
0.02	22/10/2010	Internal Review	R	All
0.03	25/10/2010	Submitted for Information		
0.04	03/11/2010	Internal Review	I/R	All
1.00	15/11/2010	Submitted for Acceptance		
1.01	13/12/2010	Re-Submitted for Acceptance		

(*) Action: I = Insert R = Replace

TABLE OF CONTENTS

LIST OF TABLES

TABLE OF FIGURES

1 INTRODUCTION

The procedure for Set up, Install, Operate and Maintain the IT and Telecom Infrastructure has been created under SC02.

1.1 References

RD#	Title	Originator	Version	Date
[RD1]	Framework Quality Plan	CUST-DEV2	1.00	

Table 1-1: Reference documents

1.2 Acronyms and Abbreviations

A table with the used Acronyms and Abbreviations can be found in Annex 19 of the FQP.

2 WP.8.6.2 INFRASTRUCTURE MANAGEMENT

The development and test environment required is described using different views, these being:

- An infrastructure architecture blueprint detailing the hardware components needed for delivering the required development & test environment;
- An application executing architecture blueprint detailing the COTS software services needed for running the developed business applications within the development & test environment;
- A development architecture blueprint detailing the tools needed for developing and maintaining the applications within the development & test environment.

(These three views are described in more details below).

2.1 Infrastructure architecture blueprint

The below diagram represents the proposed hardware infrastructure for the build & test environment using a consolidation and virtualisation approach in the server infrastructure. The hardware components needed for this infrastructure are:

- Three Sun Sparc Enterprise M5000 servers running Sun solaris 10, each containing 4* 2.4 GHz SPARC64 VII four-core processors (2 CPU boards with 2 CPUs each and 5 MB on chip L2 cache), 64 GB system memory, 4 * 146 GB SAS hard disks, 1 DVDROM, 2*Gb Ethernet pors, 2* I/O tray with 4 PCI-E and 1 PCI-X slots, 4 power supplies and 2*4GB HBA cards;
- Two Sun Fire X4170 servers running VMWare's vSphere4, each containing 2 Xeon 5540 2,5 GHz CPUs, 16 GB system memory, 2*146 GB SAS hard disks and 1 4GB HBA card;
- One Sun Fire X2270 server running Windows Server 2003 and containing 2 Xeon 5504 2 GHz CPUs, 4 GB system memory, 2*500 GB SATA hard disks and one 4 GB HBA card;
- One Storagetek 2540 Fiber channel Array containing 5*600 GB 15 Krpm hard disks and 2*512 MB cach FC HW raid controllers;
- One additional ST25X0 600 GB SAS 15 Krpm hard disk and 5 additional ST25X0 1 TB SATA 7,2 Krpm hard disks;
- One Storagetek SL24 tape library including a tape autoloader LTO SCSI tape drive and 24 tape slots all using FC interface;
- Two LTO Gen 4 tape packs, each containing 20 tapes;
- One CISCO MDS 9124 SAN Switch with 24 ports each 4 GB/S of which 8 ports active;
- Seven FC server connect cables of 2M;
- One CISCO Catalyst 3750 network switch with 48 10/100/1000T ports;

- Two Sun Server Racks of 42U each including a jumper cable kit, 2 PDUs and filler panel kit.

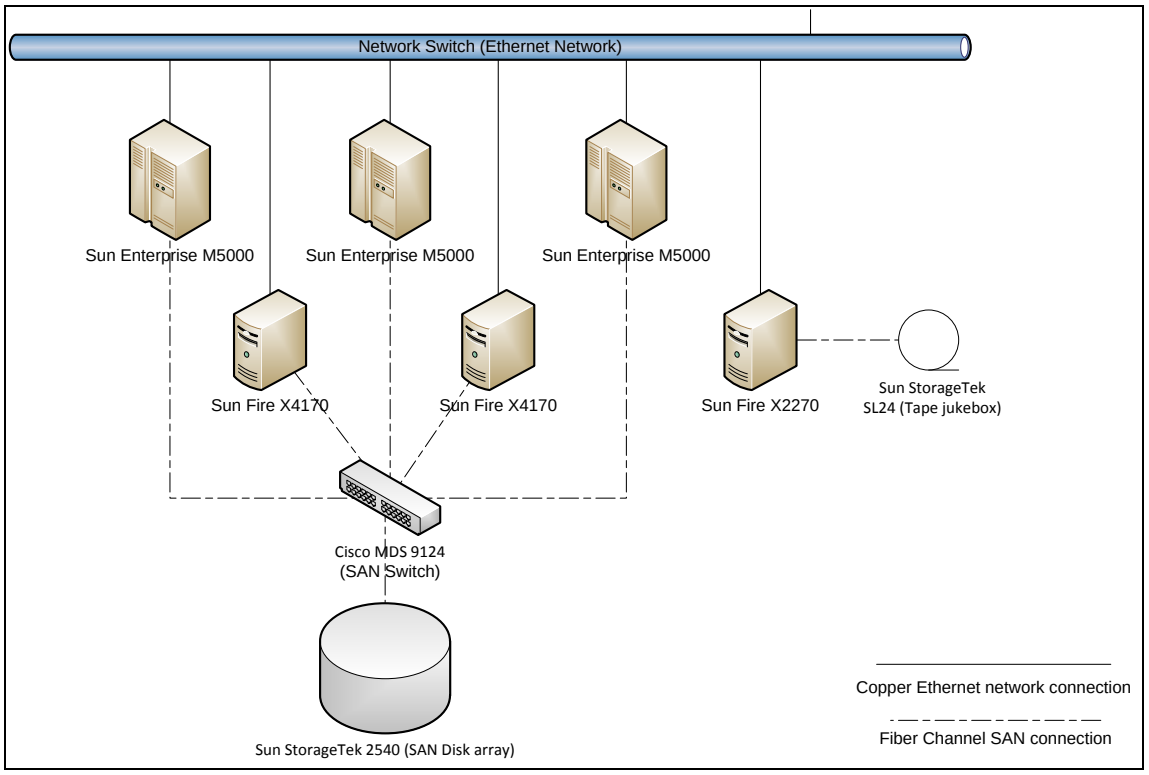

Figure 2-1: Dev and Test Infrastructure Blueprint

The above defined hardware infrastructure will be the foundation for building the required development & test application execution architecture blueprint.

2.2 Application Execution architecture blueprint

Each Sun Enterprise M5000 will be split into two dynamic domains. The resulting 6 domains across the three servers will have as key function:

1. The Build and Unit Test environment for the different Weblogic applications;
2. The Systems Integration Test environment for the different Weblogic applications;
3. The Factory Acceptance Test environment for the different Weblogic applications;
4. The Oracle Database Management systems for the different applications within the build, Integration & FAT test environment;
5. The performance and production reference environment for the Weblogic applications;
6. The Oracle Database Management systems for the applications within the performance and reference environment.

Each dynamic domain will be further divided into independent containers allowing grouping of related applications and also the isolation of an application requiring a specific configuration. The definition of the amount of containers needed and the grouping of which applications to put together will be done as part of the detailed analysis. From a conceptual point of view it is possible to group all Weblogic applications running within the TATAF Architecture framework. The CS/MIS & TTA applications will be grouped in a second container. Any other Weblogic applications like CSE/CTP Lite will be put in a third container.

A similar principle of grouping into containers can also apply for the database systems. Here it is suggested to group databases by environment.

The Sun Fire X4170 servers will run several virtual servers within VMWare. Here also it will need to be defined during the detailed design which applications can be grouped together within the same virtual server. Applications like SSTA, STTA and the TTA end user console will be running inside this server. It will be required to set up different type of environments like build/unit testing, system integration testing and FAT on this server. One Sun Fire X4170 server will mainly run the Oracle Database Management systems required for the CS/MIS and CS/RD applications.

The Sun Fire X2270 is a dedicated server to the operations management of the backups and will not run any DG TAXUD applications as such.

The Sun enterprise M5000 configuration proposed above still has the ability to scale up and add another two domains by adding additional hardware (CPUs, Memory, I/O board, System Hard Disks). This possibility can be useful in case that release upgrades of COTS software (Solaris, Oracle, Weblogic) will need to be initiated.

The diagram below presents the high level application execution architecture setup.

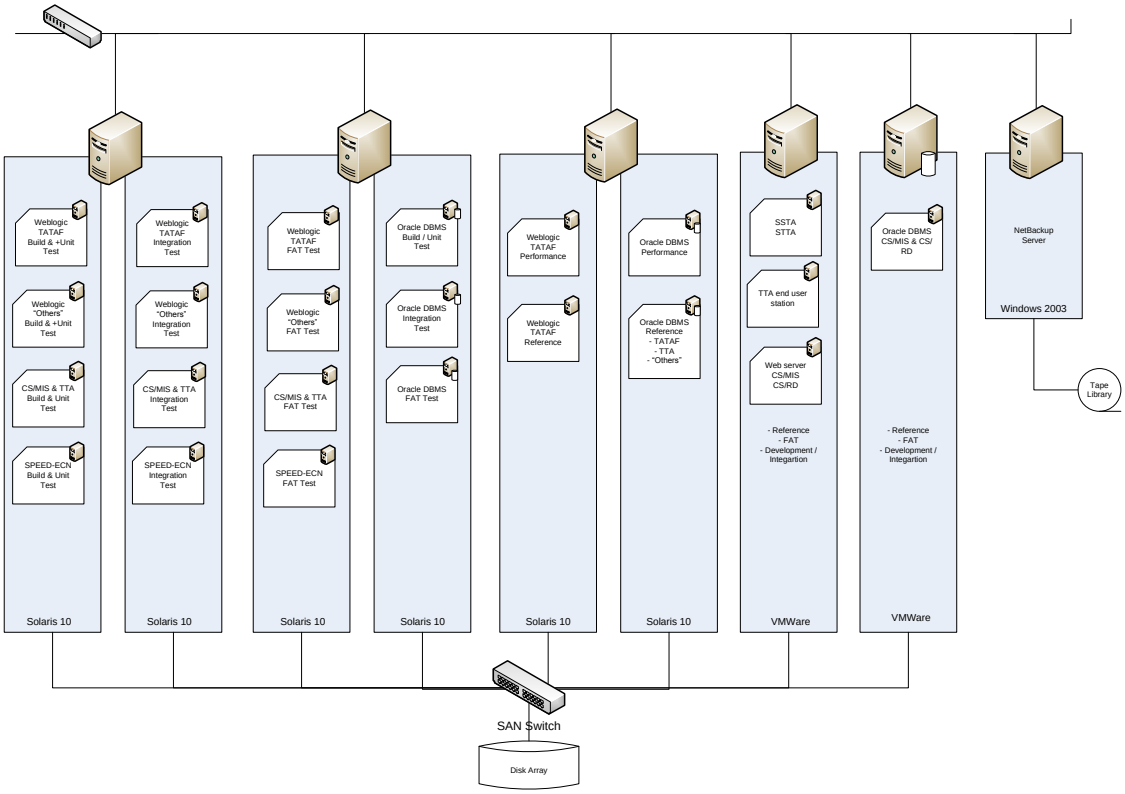

Figure 2-2: High level setup of the development and test server architecture

2.3 Development architecture blueprint

The below diagram shows the key development architecture blueprint elements that will be used. These elements will be based on a mix of locally desktop installed toolsets and central server components provided through the Accenture ADT Web Hosting environment. The components to the left of the Internet cloud are components that the CUST-DEV2 contractor resources will use locally such as Rational Software Architect (RSA), ADT Workbench. These components in some shape or form interact with the ADT Web Hosting services on the right side of the Internet cloud.

Web Hosted Service Application Architecture (Rational)

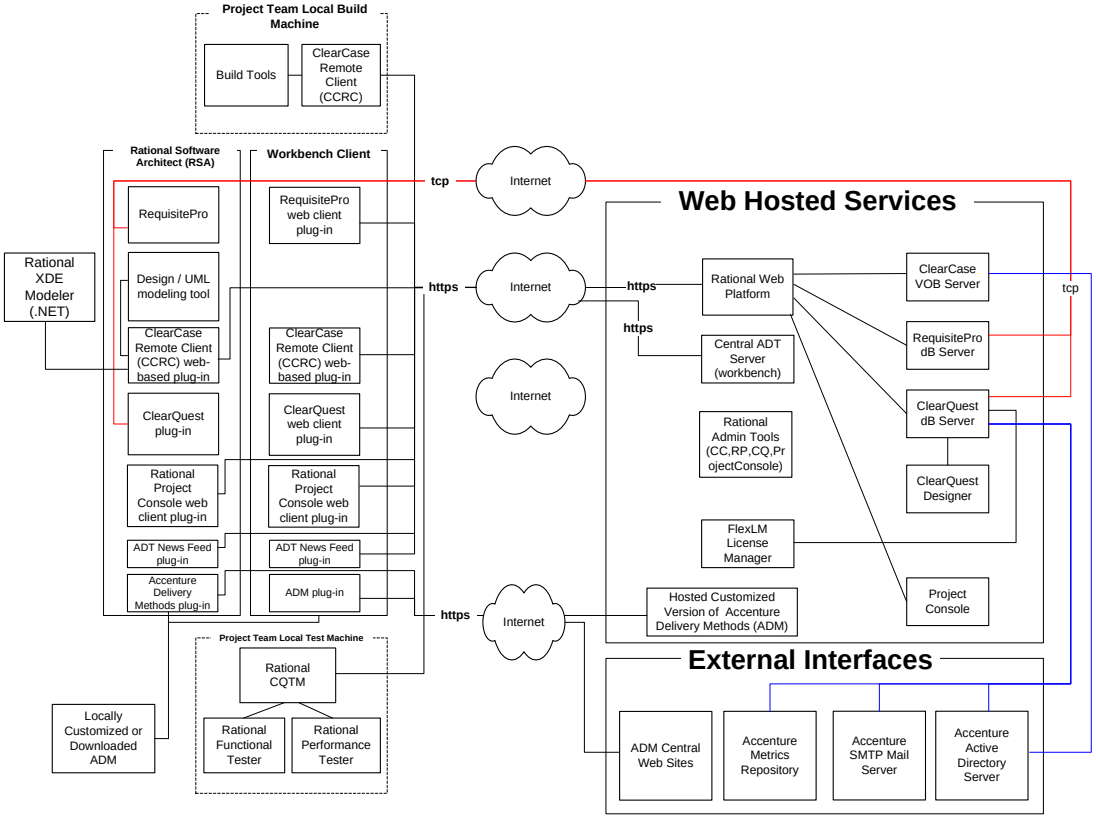

Figure 2-3: Application architecture of the ADT Web Hosting environment

2.4 Security and DRP

2.4.1 Environment

The ADT Hosted environment consists of mainly the following applications – Rational ClearQuest, ClearCase, RequisitePro, ProjectConsole and Microsoft Project Server. Each of these applications can be disabled immediately should any security issue be identified.

Any changes to the environment are reviewed and approved by the SDL (Service Delivery Lead). In the case of network changes affecting multiple clients, these have to be reviewed and approved by the Change Advisory Board – which is made up of a member from each client team.

Detected outbreaks are escalated to the operations centre (ITOC) where they work to identify if the attack is malicious or suspicious and the threat level of the incident. If the threat is serious and ongoing, they will escalate to the CIRT team for high priority follow up. If the situation is lower priority, they will work to identify and isolate the threat.

Incidents are escalated to the Director-Information Security, and based upon risk/impact may then be escalated up to and including global Situation Management Committee,

which is comprised of Sr. Level Executives. The process calls out that if client systems or data are potentially involved within an incident, the client will be notified per the mutually agreed upon procedures established for the project.

2.4.2 Physical Security

The data centres that house the Company (Accenture) servers or data have, at a minimum, basic physical security measures to protect Company systems. Company systems will be stored in a locked room with floor-to-ceiling walls. Doors to the server room have an auditable entry mechanism (e.g., card reader) that records which enters and leaves. Data Centres further require a PIN entry as well as a key card to enter the Data Centre. Only authorized personnel have access to server rooms. Vendors and guests must be escorted by an authorized person while in the Data Centre, and must sign in and out in a written log.

Hardware and software are located in a multi-tenancy infrastructure, though customer project data are segregated.

Only the lead infrastructure architect from the ADT hosting team has physical access to the environment.

Any personnel asking for physical access have to obtain specific permission from the SDL assigned to the client. The company housing the client servers will have a support team that has access to the servers, but outside of those personnel no one is granted access without permission. It is assumed that if the SDL grants access, then all research on this individual has been conducted at a prior time.

2.4.3 Network Security

The network is protected physically.

Data going between Client and ADT Hosting environment goes over internet using Secure Sockets Layer (SSL) enabled HTTPS protocol.

Intrusion Detection Systems (IDS) that recognize network attack signatures is used where the Accenture network connects to outside networks.

The IDS appliance is Symantec IDS.

Accenture global CIM (Centralized Infrastructure Management) organization captures inbound and outbound traffic on the network circuits. The logs are maintained for review as necessary.

When an intrusion is detected, a real-time alert is sent to a global Network Security team. This team has a planned response which includes alerting the local network support teams.

2.4.4 Host Security

The system is protected by hardening and firewalls. Externally facing web servers are placed in a Demilitarized Zone (DMZ). Application servers and database servers are

placed in a Quarantine Zone (QZ) and VPN connection is required when the access is necessary.

Specific actions are taken on each server to lock down vulnerabilities to them. There is a 300 step process to ensure that each server's settings match the Accenture standard of server hardening.

A test was also conducted to ensure that all necessary security patches are applied which in turn reduces known vulnerabilities as well.

Security patches, fixes and updates for host OS and database servers are certified by Accenture Global Security team and are then applied on ADT hosting servers on monthly basis. Application software like Rational tools are certified by ADT Development team and are then applied to ADT hosting servers every three months.

ADT hosting system has monthly vulnerability assessments executed By Accenture Global Security team and vulnerabilities are repaired in a timely manner. Any vulnerabilities that cannot be repaired due to specific business needs, or if such repair interrupt required functionality in the system, security exceptions must be submitted and approved. A defined process is in place to determine the patches to be applied and their corresponding risk levels. Accenture uses vendor notifications as well as Symantec Deepsight for most of the platforms.

Anti-virus detector is installed on all servers. It is both signature and anomaly based.

2.4.5 Application Security

The password must be changed every 75 days and must meet all of the following requirements:

- The password length must be at least seven characters.
- The password must be different from the previous six passwords.
- The password must NOT be derived in any way from the Enterprise ID.
- The password must contain characters from three of the following four classes:
  - Upper Case
  - Lower Case
  - Numerals
  - Special Characters
- The password cannot contain spaces.
- The password cannot contain non-anglicized characters. (Examples: é, ö, Ø, ñ, å)

ADT users are LDAP authenticated.

ADT client team Point of Contact (PoC), e.g. Client defines what user account should be created, updated, or terminated.

Penetration/vulnerability auditing is performed by Accenture Global Security team. ADT hosting team does not perform testing on regular basis.

ADT hosting team monitor the usage of ADT tools every month. The system monitors for each user on what tools he/she has been using.

2.4.6 Web Security

Rational applications use Apache while Microsoft Project Server uses IIS. All ADT applications, except Rational ClearCase, use Microsoft SQL server 2005 (SP2) as the back-end database server. Rational ClearCase has a special database system - versioned object base (VOB).

2.4.7 Database Security

Each client project has its own database for each application.

2.4.8 Cryptography

For Confidential applications, is required a minimum 128-bit encryption (e.g. SSL) for all communications outside of an Accenture GTN Data Center. In the ADT hosting environment, asymmetric RSA algorithm is used.

RAS is used.

2.4.9 Backups

There is daily full database backup, as well as incremental backup every four hours. These backups are put to tape during System backups, which are done on a nightly basis.

A copy of the production data is replicated from one NetApp Device to another at a separate location, and this is done through a VPN tunnel between the two sites. The site that holds the replicated data is also a secure Data Center. Tape backups are stored at Iron Mountain.

The tapes are sent off-site to a facility that is located at least 200 miles from the Data Center.

Test restores are completed biannually.

Backup media that have reached the end of their lifetime are sent through a machine that magnetizes the tape, and then destroys it to ensure no data can be obtained from it.

2.4.10 Contingency Planning

Accenture has a Disaster site that is located about 700 miles from the production facility.

The SLA to get the client back up and running at a different site is 48 hours.

Testing: full functionality was brought online at the secondary facility and testing was done to ensure the integrity of the DR site.

The DR plan will be tested on a yearly basis.