Eskom	Standard	Technology

Title: **EMS AND DMS MASTER STATION COMPUTER SYSTEM DISASTER RECOVERY STANDARD**

Unique Identifier:	**240-72942279**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**2**
Total Pages:	**13**
Next Review Date:	**May 2025**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Kenneth Brown	Steven Papadopoulos	Richard McCurrach
Dx PTM&C – Control and Automation Chief Engineer	PTM&C Control and Automation T&S Manager	PTM&C Senior Manager
Date: 21 Apr 2020	Date: 22/04/2020	Date: 5 May 2020

Supported by SCOT/SC

Marlini Sukhnandan

Telecontrol SC Chairperson

Date: 22 Apr 2020

PCM Reference: **Design System; Unique Identifier: 240-44509543**

SCOT Study Committee Number/Name: **Telecontrol and SCADA Study Committee**

Content

1. Introduction

The Transmission EMS and Distribution DMS Master Station SCADA computer systems have been classified as Mission Critical. This was based on their function in the operating, monitoring and control of the interconnected power system. The rating was performed by Strategy and Risk Business Unit in the Enterprise Resilience Division. Subsequently, Eskom identified a requirement to align the disaster recovery (DR) of these computer systems accordingly and ensure that their DR solutions are aligned with business continuity plans.

Furthermore, increasing cyber-attacks have become one of the biggest disaster threats to control systems. This has prompted the inclusion of recovery from such attacks in the DR solution.

This standard describes the computer architecture, layout, interconnectivity and functionality that can be achieved with a best practice DR solution.

2. Supporting Clauses

2.1 Scope

This document serves to define and document separate disaster recovery solutions applicable to the EMS and DMS SCADA Master Station computer systems.

The solutions may not be immediately achievable due to technical limitations on existing equipment or project scopes and activities as well as financial constraints; however it shall be used as a design reference for the specification and procurement of upgrades and new systems.

The aim of this document is not to produce a detailed specification, therefore product and vendor specific functionality shall not be included. Implementation may take many years to achieve; therefore the solutions are generic and adaptable to changing technology and applicable through multiple life cycles of these systems.

This DR standard removes the complexity of having different DR solutions based on a specific time frame or degree of destruction.

The standard allows implementation by varying degrees. System owners are responsible for extent of deployment in order to achieve the required business continuity. This shall be documented in the system owner's DR plans.

The standard describes Master Station requirements, but the solutions are dependent on infrastructure from surrounding providers such as telecommunications and substation equipment. Technical decisions made during normal operations and maintenance impact these environments and having this document may steer these decisions to achieve a preferred DR solution in the future.

Clearly identifying the Master Station DR boundaries also ensure those surrounding computer systems and their associated software applications and data is included in other DR solutions.

2.1.1 Purpose

The purpose is to define and document a disaster recovery solution that is applicable to the EMS and DMS SCADA Master Station computer systems.

2.1.2 Applicability

This document shall apply to the Transmission System Operator and Distribution Divisions.

2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] ISO 9001 Quality Management Systems.

[2] Eskom Cyber Security Standard for Operational Technology, unique identifier 240-55410927.

[3] Eskom IT Disaster Recovery Strategy, unique identifier 240-47615255.

2.2.2 Informative

Not applicable

2.3 Definitions

2.3.1 General

Definition	Description
Master Station	Refers to the physical site where the Energy Management and SCADA Computer Systems and control rooms are located.

2.3.2 Disclosure Classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
AGC	Automatic Generation Control
BIOS	Basic Input Output System
BME	Bandwidth Management Equipment
DMS	Distribution Management System
DMZ	Demilitarised Zone
DR	Disaster Recovery
DTS	Dispatch Training Simulator
EMS	Energy Management System
HMI	Human Machine Interface
ICCP	Inter Control Centre Protocol
IPS	Intrusion Prevention System
OS	Operating System
PCU	Process Control Unit
SCADA	Supervisory Control and Data Acquisition
UPS	Uninterruptable Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMS	Wide Area Measurement System
WAN	Wide Area Network

2.5 Roles and Responsibilities

The responsibility to implement this document will lie with the Distribution Operating Units as well the Transmission System Operator, supported by the relevant sections of Power Delivery Engineering, Information Management and SCOT.

2.6 Process for monitoring

The implementation of this document at OU level will be monitored by the Standards Implementation function at OU level. The DMS Oversight Committee and the SCOT Telecontrol and SCADA Study Committee will monitor implementation at a national level.

2.7 Related/Supporting Documents

Not applicable

3. Concerns with Current Disaster Recovery Solutions

Current SCADA disaster recovery systems consist mainly of an off-line environment, possibly with the computers and databases from different suppliers. The databases are sometimes out of date and maintenance is a significant amount of work. Furthermore these systems have the following disadvantages:

- Telecommunications between DR Site and substations was manually switched from the Main site
- Testing posed a risk to the electrical power system as downtime to the SCADA systems was inevitable. Since outage times for DR testing was therefore kept to a minimum, problems were seldom detected or resolved during such a short time frame.
- Specific hardware problems and performance issues where only detected during a test, which often prompted the DR test having to be re-done.
- Although testing of the DR site for a limited period could have some degree of success, there was no guarantee that the system would run for months at a time.
- Testing of DR was usually planned when Power System events were minimal; this created only a degree of confidence.

4. Disaster Recovery Solution

4.1 Assumptions

This standard assumes a disaster based on a worst case scenario in which an entire Master Station site is totally destroyed and an alternate site is to be in operation for the duration of 6 months. It is estimated that a new main Master Station site can be re-established within 6 months. This includes the Telecommunication equipment and circuits that are routed through or via the main site.

This standard includes the recovery of systems after a cyber-attack, using a worst case scenario of all equipment been compromised from a BIOS level, operating systems, embedded OSs, 3RD party software applications, databases and the backups thereof.

Even though the telecommunication for the Master Station redundancy is included in the DR solution, it is acknowledged that Eskom Telecommunications would be responsible for their own disaster recovery.

Manual activation of the DR site shall be avoided. It must be assumed that the maintenance personnel who may assist with a manual switch-over is not available after the disaster.

4.2 Exclusions

The following is specifically excluded from the disaster recovery solution:

- Human resources.
- Reasons and probability for disaster.
- Recovery of power systems.
- Selection of physical DR sites.
- Topics that are covered in other Business Continuity Plans.
- Substation equipment (although interface requirement is included).
- Scenarios based on different time frames. The requirement is for the DR site to be operational for 6 months.
- Generation local control systems.
- Metering
- WAMS
- Computer systems connected to Corporate and Enterprise Networks (although interfaces on EMS and DMS to these systems to be included).
- Building facility requirements, such as UPS, access control and air-conditioning.
- Theoretical DR definitions and concepts.

4.3 Minimum requirements

The minimum requirement at the DR site shall be the following:

- Interface equipment to telecommunications.
- Communication Front-end computers, Data concentrators and ICCP Servers.
- Application/SCADA Backend computers.
- Historical Information Systems.
- HMI computers.
- Infrastructure used for population of EMS and DMS operational databases and display creation.
- Infrastructure for maintenance and cyber security.
- Infrastructure for system build as described in chapter 8.
- Interface to Enterprise Network.
- Power Network optimisation and reliability tools
- Transmission requires Scheduling and Dispatch tools.
- Transmission requires the interfaces to remote HMI workstations deployed at Distribution Control Centres.
- Transmission requires ICCP connectivity to Distribution and not for international customers.

4.4 Solution for Transmission

The DR solution is a hot standby system that can be used under normal conditions in an operational mode, in-order to guarantee its functionality and availability if a disaster occurs. Therefore, the real time use of the DR functionality of a Master Station computer system located at the DR site is to be adopted.

A permanent dedicated connection from the DR site to the substation, plant or remote ICCP server is required; telecommunications routes and equipment shall be diverse and separated from the Main site.

An architecture where redundant connectivity is provided to the Main site via the DR site is an acceptable solution in providing redundant connectivity from the substation and/or plant to the Main Site.

The preferred solution requires a replication of the Main site at the DR site, to allow for fully independent operation per site.

Data replication and synchronisation between Main and DR site requires real time data synchronisation of less than 4 seconds. This is indicated in Figure 1; the coloured lines depict data and application connectivity at a logical level and are the main components to achieve SCADA functionality.

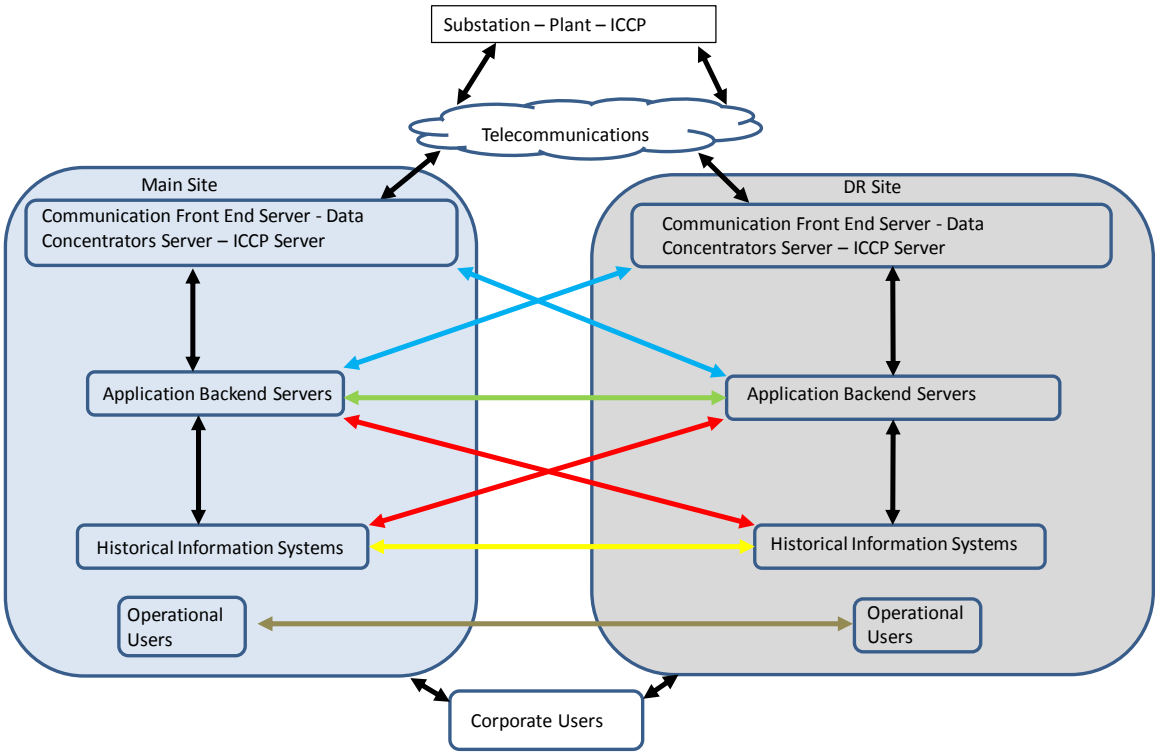

Figure 1: EMS DR solution

The logical connectivity shown in Figure 1 is as follows:

- The Blue lines indicate application interaction between the Application Backend Servers located at both sites and the Communications Front End servers, Data Concentrator Servers or ICCP Servers located at the alternate site. This connectivity can be achieved by mapping an entire server's functionality on the Backend or mapping individual data points. When a data source is declared as failed or invalid, pointers proceed down a programmable hierarchical list to the next valid source. The software performs monitoring on the primary data source for validity and when declared valid will be automatically reinstated as the source of data. The selection of data from multiple sources is carried out on the Application backend, and is a function of the real time database; therefore all applications make use of the valid data-source at that moment in time; including the displays generated for the users of the system. This This functionality is transparent for the users of the system and they are unaware of where the data is being sourced from at any given moment. The benefit is operational use can be made of the infrastructure at the DR site.

- The green line indicates application interaction between the sites Application Backend Servers, the purpose for this is to insure synchronisation of data types that are not sourced from the plant, such as input from users, data from corporate and solutions generated from programs. Certain applications such as AGC and the function of issuing controls to plant, have to select a site that is the master. An additional role is to take over the connectivity indicated by the blue line which may become disabled or may initially not exist.
- The Red line indicates application interaction to Historical systems, and its purpose is to insure that whichever Application Backend is running in the Master role is populating all Historians. If the functionality of the green line is fully achieved, population of Historian is performed locally from Application Backend Server; the Red line role in the future might be for redundancy purposes only.
- The Yellow line indicates synchronisation of Historians software or configuration of databases and not for synchronization of actual data as this is taken care of by the Red lines. Specific data types that are entered into the HIS will require replication to the alternate sites HIS. It could replace the functionality of the Red and Green if they experienced failure.
- The Brown line indicates connectivity of all Operational Users access to either system, independent of their physical location.
- The Black lines indicate the normal connectivity.
- Corporate Users include application interaction and data flows between the Operational systems and corporate systems. Due to cyber security risks the DR system shall have the ability for Corporate Users to connect to it but this will only be enabled when required.

Systems and functionality that require local interaction must still be provided at the DR site, these include, systems used for database population, power application software not residing on Backend, computer maintenance and systems used for the development of MMS functionality. Figure 1 excludes, quantity, Cyber Security, redundancy at each site, secure zones, physical connectivity and WAN.

The system architecture shall ensure that the data-source is transparent to all users. DR computer testing and training of users to switch between systems and sites will not be required.

To meet the requirement for the 6 month use of the DR site, it will require an N-1 redundant configuration.

A management solution for computer system maintenance will have to detect failures; with an N-3 redundant configuration Power System users will not be able to detect any failure.

Ownership of DR solution should not be outsourced to a neighbouring Division. The ownership of the DR solution shall reside with the system owner in the Operating Unit. The physical hosting of computer infrastructure by a neighbouring division should only be considered based on physical proximity. A control room to be provided for DR purposes should perform a daily business function; plans should indicate where this function will be relocated during a disaster.

Using the same system manufacturer at the DR site with identical versions of hardware, OS, software applications and databases will reduce maintenance of the DR significantly.

5. Solution for Distribution

There shall initially be a single DR site for all Distribution OUs that will be situated at a national location. The DR site shall have the ability to connect to all Distribution RTUs in the regions. Eskom Telecoms will be required to reroute all the RTU telecommunication links to the DR site.

The site shall have the capability of being a fully operational facility when one of the OU DMS systems requires it in the event of a disaster. Therefore the requirements of the largest OU DMS system shall be catered for. Systems and functionality that require local interaction must be provided at the DR site; these include workstations and desks, etc.

There shall be a permanent dedicated telecommunication connection from the OU DMS system to the DR site.

To meet the requirement for the 6 month use of the DR site, it will require an N-1 redundant configuration.

The DR site shall also a management solution for computer system maintenance that will have to detect failures of the system or component thereof.

Using the same system manufacturer at the DR site as that of the OU with identical versions of hardware, OS, software applications and databases will reduce maintenance of the DR significantly.

Figure 2, 3 and 4 illustrate the proposals on how to achieve this strategy.

Figure 2 illustrates the rerouting of the RTU communication links to the DR site from the BME situated in the same physical location/building as the Distribution control centre. The benefit of this option is that there is no design changes required and chop-over failures can be resolved quicker. The disadvantage of this option is that in the event of a DR where the BME no longer exists, the communication links to the DR site will also be lost.

Figure 3 illustrates the rerouting of the RTU communication links to the DR site from the Eskom Telecommunication high sites. The advantage of this option is that in the event of a DR where the BME no longer exists, the communication links to the DR site will still be available.

Figure 4 illustrates the rerouting of the RTU communication links to the DR site from the BME which is hosted at a physically separate physical location from the DMS control centre (including the RCMs and PCUs). There shall also be redundant fibre links between this offsite facility and the control centre. The disadvantage of this option is that design changes are required and there are addition cost implications. Distributed support from the SCADA staff will also be required.

The option chosen to achieve this strategy will be based on the technical and economic feasibility of the option at the time of implementation.

Additional DR sites shall be made available as the business becomes capable and the other options become technically and economically feasible. Some of the factors that will influence the location of the additional sites will be geographical location, financial impact, availability of telecommunication infrastructure, human resources, etc.

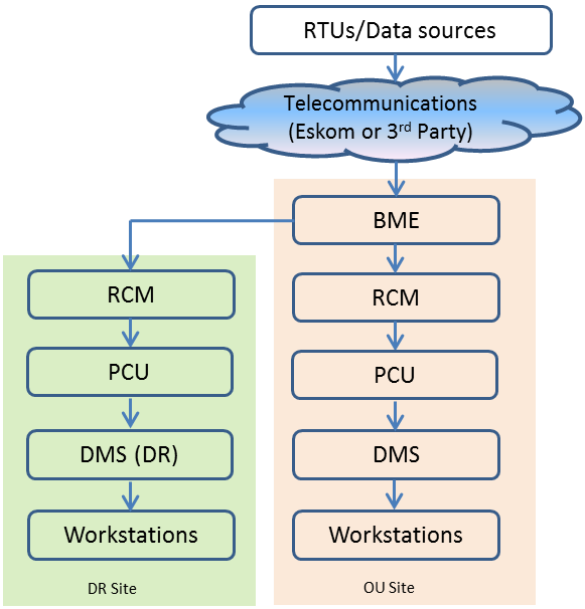

Figure 2: DMS DR solution (rerouting from the BME)

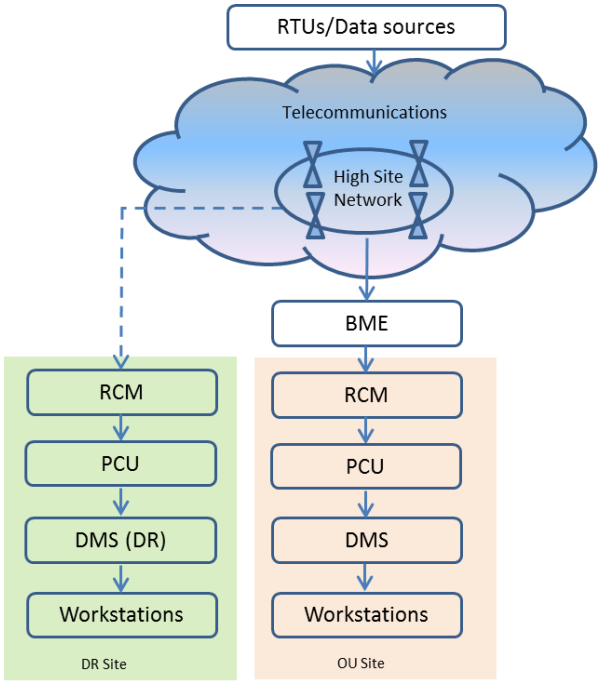

Figure 3: DMS DR solution (rerouting from the high sites)

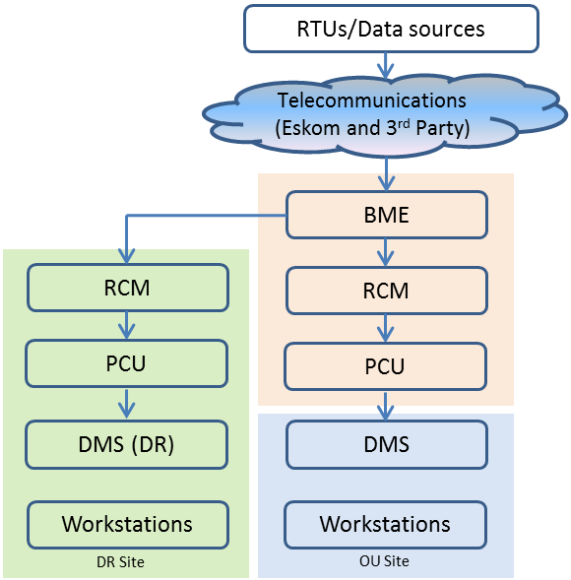

Figure 4: DMS DR solution (off-site front end system)

6. Advantages and benefits

The advantages of the proposed solutions in Section 4 and 5 are:

- Redundancy from Master Station computers into the substation equipment.
- Database and software alignment between Main and DR site is maintained and discrepancies are easily detected. If maintenance staff, do not keep these systems aligned it will have an impact on the current operation of the power system.
- The DR site can locally populate surrounding systems like Historical Information Systems, which negates the need of performing backups and transferring them off-site.

- It forces Main and DR systems to have identical hardware, software, databases, and performance and availability characteristics.
- It negates the need for performing manual backups; the Main site and DR site have N-1 redundancy, in theory more than 3 failures have to occur before downtime and data loss is experienced.
- Having a Hot Standby DR with live data, lends itself for other uses such as, running simulations, replaying events and providing historical snap shots, all of which are computer intensive and can degrade performance.
- Offers the ability for Communication Front End computers or Data Concentrators to be remotely located and the transferring of data through higher bandwidth telecommunications circuits to Master Station sites. The benefit is a reduction of individual Tele-control telecommunication circuits running from the Main sites to each remote plant location. In future IPPs will offer this type of connectivity using ICCP.

Benefits for the maintenance of the SCADA system are the following:

- Fault finding of remote problems is easier as comparisons can be performed.
- Faults occurring on DR site can be alarmed and attended to in real time.
- Maintenance tasks such as upgrades to hardware and certain database updates can be achieved on Main system, during this time data can be obtained from DR site.
- Provides an easier method of detecting and identifying where problems are. Example; if both Masters are unable to communicate with the substation equipment the fault is more than likely with the substation equipment.
- Specific faults that occur after hours, can be attended to the next working day, this will reduced call outs and travelling after hours.
- Deployment of updates and antivirus software can initially be rolled out and tested to the DR system before deployment on Main system.
- Database updates can be deployed and tested at the site not running as master

7. Cyber Security

The implementations of the DR solutions are to be aligned with the Eskom Cyber Security Standard for Operational Technology (240-55410927) [2]. There shall be adequate cyber security isolation between Main and DR site computer systems which shall comprise of the following:

- Firewalls with IPS and the ability to provide physical isolation.
- VPN and VLAN deployment up to individual software modules.
- Software applications to include incoming data interrogation and filtering based on type, size, and jitter. When data changes sources it should be alarmed if there was a change in statuses, digital indications and invalid or unhealthy flags.
- Corporate user access to data in DMZ Historians should be achieved by exporting data out of this DMZ into a corporate Historian. This is a far safer mechanism and provides an additional boundary. Corporate user requirements for Operations data can be sourced from the corporate Historian.

8. System build

After a disaster event or security compromise has been detected, backups and intensive logging can occur for post event analysis. The next action is to disconnect all connectivity to DMZs, external connections and remote access users via VPN, full isolation of the system is required, and a system build has to be done locally.

Each site should have a local deployment server, with read only storage capability. The software and data stored in this location are sources that have been validated as secure.

BIOS updates, OS installation, Software application installation and database deployment should be able to be achieved locally over the network and manually activated.

The sequence to build up the system usually starts with the Communication Front End, Data Concentrators and ICCP servers. Connectivity to plant shall be in a phased approached and to be established as soon as possible, as certain SCADA functionality can commence. Following this is the build of the Application Backend Servers, database population, and operator usage can commence. Following this is the build of the Historians and connectivity to DMZs and external systems.

To insure that real time database security is achieved, validation processes can interrogate and perform comparisons on previous versions. This can be done twice, when backups are made and when backups or databases are deployed.

9. Authorisation

This document has been seen and accepted by:

Name and surname	Designation
Carlos Betencourt	Portfolio Manager (Tx)
Deon van Rooi	Dx PTM&C – Senior Manager (acting)
Kenneth Brown	Dx PTM&C – Control and Automation Chief Engineer
Les Fenn	Eastern Cape OU – SCADA Management Manager
Malcolm van Hart	Middle Manager Dx DMS CoE
Marumo Kgare	Western Cape OU – SCADA Management Manager
Mervin Mottian	SCADA Managers Forum Chair
Michael Rawson	Free State OU – SCADA Management Manager
Rishi Hariram	Tx PTM&C – Control and Automation Chief Engineer
Rosalette Botha	Corporate Specialist (EMS)
Sanjiv Bandu	KZN OU – SCADA Management Manager
Thuli Tladi	Distribution Master Station – SCADA Management Manager
Xolani Mkala	Gauteng OU – SCADA Management Manager

10. Revisions

Date	Rev	Compiler	Remarks
May 2020	2	Kenneth Brown	Second Issue No technical changes
Sept 2014	1	G Ive	First issue Addition of a separate Distribution strategy

11. Development team

The following people were involved in the development of this document:

- Rosalette Botha
- Rishi Hariram
- Michael Rawson

- Kenneth Brown
- Cliff Nkuna

12. Acknowledgements

Not applicable