

Directive of Strate Proprietary Limited

Special Gazette No S14-2016

Strate Directive SA.10

Risk Management



To cater for the management of risks in the Strate environment, including testing and disaster recovery, applicable to Participants and Business Partners¹

*Contents of this material are protected under South African copyright law. No part of this material may be copied, completely or partially, either electronically or manually, without the written consent of Strate (Pty) Ltd
This material remains the sole property of Strate (Pty) Ltd.*

INDEX

1. INTERPRETATIONS AND DEFINITIONS

2. REQUIREMENTS

Disaster Recovery Tests

Technical Difficulty and Business Continuity

Communication Networks

ANNEXURE A

ANNEXURE B

ANNEXURE C

¹ 'CSD' changed to 'Strate' throughout the document with effect from 22 August 2016



1. INTERPRETATIONS AND DEFINITIONS²

In this Strate Directive, any interpretation, word, or expression to which a meaning has been assigned in the Strate Rules bears a meaning so assigned to it.

‘Business Partner’ means a party which is not a Participant and which electronically interfaces with Strate to perform an essential market function;³

‘JSE’ means the JSE Limited Registration Number 2005/022939/06;

‘Production Environment’ means the systems and related infrastructure used for an entity’s day to day operations;

‘Secure’ means to ensure the integrity and confidentiality of the information by taking appropriate reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of the information, and unlawful access to or processing or use of the information;⁴

‘STRATE Supervision’ means the supervision division of Strate headed by the Head of Supervision and set up by the Controlling Body in terms of the Strate Rules;⁵ and

‘Strate System’ means the computer system or systems and associated network or networks operated or used by Strate for the purpose of clearing and settlement of Securities, or for any other purpose performed by Strate in terms of the Act;

‘SWIFT’ means Society for Worldwide Interbank Financial Telecommunications.

² ‘Rules’ and ‘Directives’ changed to ‘Strate Rules’ and ‘Strate Directives’ throughout the document with effect from 22 August 2016

³ Amended with effect from 1 August 2014

⁴ Amended with effect from 5 December 2015

⁵ Definition inserted with effect from 1 August 2014

Directive of Strate (Pty) Ltd

Registration Number 1998/022242/07



2. REQUIREMENTS

Disaster Recovery Tests

- 2.1.1 A Participant must conduct the disaster recovery test referred to in Strate Rule 8.1.8 at least once every 6 (six) months, and report the results of such test to STRATE Supervision in accordance with Annexure A within 30 (thirty) days from the date of the test.⁶
- 2.1.2 Where a test conducted in terms of clause 2.1.1 is unsuccessful, a Participant must, within 10 (ten) Business Days from the date of the previous test, advise STRATE Supervision of the circumstances leading to the failure as well as its plans to conduct a subsequent disaster recovery test. The timing of the subsequent test shall be agreed with STRATE Supervision and shall be dependent upon the nature and consequences of the failure (e.g. systems/functionality impacted, availability of appropriate work-around solutions as a temporary measure). Where a subsequent test is still unsuccessful, a Participant must repeat this re-testing process until it conducts a successful disaster recovery test.
- 2.2 A Participant and Business Partner must test, in accordance with Strate's annual testing calendar:⁷
- 2.2.1 the Participant's or Business Partner's Production Environment to Strate's disaster recovery site, and
- 2.2.2 the Participant's or Business Partner's disaster recovery sites to both Strate's Production Environment and disaster recovery site.
- 2.2.3 On successful testing, Participants and Business Partners must complete the form in Annexure B and email it to Strate-HelpDesk@strate.co.za and Strate-Supervision@strate.co.za.
- 2.2.4 Where a test conducted in terms of clauses 2.2.1 or 2.2.2 is unsuccessful, a Participant or Business Partner must within 10 (ten) Business Days from the date of the previous test, advise Strate of the circumstances leading to the failure as well as its plans to conduct a subsequent disaster recovery test. The timing of the subsequent test shall be agreed with Strate and shall be dependent upon the nature and consequences of the failure (e.g. systems/functionality impacted, availability of appropriate work-around solutions as a temporary measure). Where a subsequent test is still unsuccessful, a Participant must repeat this re-testing process until it conducts a successful disaster recovery test.

Technical Difficulty and Business Continuity⁸

- 2.3 A Participant and Business Partner must, for each disruption of its Production Environment:

⁶ Amended with effect from 22 August 2016

⁷ Amended with effect from 1 August 2014

⁸ Section amended with effect from 6 August 2015



- 2.3.1 submit to Strate a technical difficulty log as described in Annexure C, within 30 (thirty) minutes after the Participant or Business Partner identifies the technical difficulty. The Participant or Business Partner must provide as much information as is known at the time of completing the log;
 - 2.3.2 send to Strate a status update every 1 (one) hour, which communication could be sent via email; and
 - 2.3.3 on closure of the incident, submit to Strate the technical difficulty log described in clause 2.3.1, completing the additional information that was not available when the Participant or Business Partner first identified the technical difficulty.
- 2.4 A Participant must move its operations to its disaster recovery site after a maximum of two hours of continued disruption of its Production Environment by a Severity 1 (one) technical difficulty as described in Annexure C.

Communication Networks

- 2.5 A Participant must have a minimum of 2 (two) Secure messaging systems, or 2 (two) different communication network service providers to provide Secure messaging communications between the Strate System and the Participant, and must ensure that it can communicate effectively through the alternative messaging system or communication network service, in the event that the primary messaging system or communication network service provider becomes unavailable.⁹

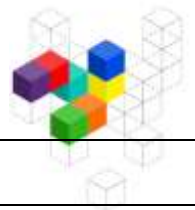
⁹ Amended with effect from 1 August 2014



ANNEXURE A

Disaster Recovery "DR" Testing Results Report

| Information required | Guide | Response |
|---|---|----------|
| 1. Confirm the physical address of the site where DR testing was conducted. | E.g. Off-site DR location address. | |
| 2. Date(s) the test was conducted? | Actual dates and duration of the test. | |
| 3. Describe the systems that were tested with a brief explanation of the use of each system. Also describe whether network testing was conducted, (dedicated backup lines or Telkom cutover). Were linkages with associated internal and external entities tested | Internal custody system, e-mail, SWIFT, financial packages etc. | |
| 4. Confirm the time taken to recover each of the above systems tested? | Please provide specific times. | |
| 5. Describe the recovery methodology used as well as how the integrity of the recovered data was confirmed to be correct? | Restore to point in time backup, roll forward of log data, hot restart etc. Did users / auditors take before and after images of data for comparison / checking purposes Did users / auditors test the functionality of the recovered system? | |
| 6. Explain which of these systems are critical for the effective functioning of daily operations. | Please list from the above mentioned systems. | |
| 7. Detail the parties who participated in the DR testing. | Participant staff, other Participants, JSE, SWIFT, treasury operations, information technology division etc. | |
| 8. Please provide full detail of what the test covered. | What was the objective/purpose of the test? | |
| 9. Please provide full details of the results of what was tested (per system if appropriate). | Was the objective/purpose of testing achieved? | |
| 10. Please provide detail of what was | | |



| | | |
|---|---|--|
| excluded from testing. | | |
| 11. Please confirm when testing of the above excluded items has been scheduled for? | | |
| 12. List any issues that were raised / recommendations that were made after the DR testing. | E.g. To get more staff involved in testing, to include treasury in next planned testing etc | |
| 13. With respect to question 12 above, confirm which recommendations have been implemented to date, as well as the planned schedule for the implementation of recommendations at a future date. | | |
| 14. Confirm how long back-up tapes /records of your systems are archived for. | Please provide an exact time period, as well as the cycle and frequency of backups. | |



ANNEXURE B

**STRATE'S DR TEST
TESTING CONFIRMATION**

INSTITUTION _____

CAPACITY PARTICIPANT

BUSINESS PARTNER

1. We confirm that we participated in the DR Testing, of the Strate System conducted by Strate on _____; and were able to connect to Strate.
2. We are satisfied that the content and scope of the test was sufficient to connect to the Strate Production Environment and / or disaster recovery site. (Please delete where not applicable.)¹⁰

NAME OF INDIVIDUAL/S: _____

CAPACITY / ROLE: _____

SIGNATURE: _____

DATE: _____

WHO WARRANT THAT THEY ARE DULY AUTHORISED TO SIGN THE ABOVE.

¹⁰ Points 1 and 2 amended with effect from 1 August 2014



ANNEXURE C

Technical Difficulty Log

Please ensure that the duly completed log is e-mailed to strate-supervision@strate.co.za and strate-helpdesk@strate.co.za

Date

Time difficulty was identified

Time difficulty arose

Time difficulty was resolved

Name of Participant / Business Partner / Strate

Market impacted:

| | |
|-------------------|--------|
| Bonds | No |
| Equities | No |
| Money Markets | No |
| Inform the market | Yes/No |
| Contact Person | |
| Contact Number | |

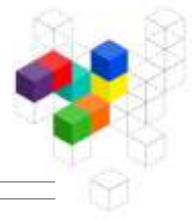
Systems Impacted

| | |
|---|----|
| Internal Custody System | No |
| SAFE / CMFE (FRONT END STRATE SYSTEM / CENTRAL MESSAGING FRONT END) ¹¹ | No |
| SAFIRES | No |
| SWIFT | No |
| WAN (Wide Area Network) | No |
| E-mail | No |
| Facsimile | No |
| UFE (Bonds) | No |
| MMFE (Money Market Securities) | No |
| ETME (Money Market Securities) | No |
| Other (please specify) | |

Nature of Technical Difficulty

| | |
|----------------------------------|----|
| Not Receiving Incoming Messages | No |
| Outgoing Messages cannot be sent | No |
| Status Intimations Not Received | No |
| Power Failure | No |
| Building Evacuation | No |
| Other (please specify) | |

¹¹ Amended with effect from 19 December 2016



Severity of Technical Difficulty

Severity (please select severity using below key as a guide): 1

| Severity | | Explanation |
|----------|--------|--|
| 1 | High | Significant impact to entity reporting the difficulty and external parties. Causes disruption to normal business operations. Extension to operational windows is required – E.g. SAMOS windows to be extended Downtime anticipated to be longer than one hour. |
| 2 | Medium | Some impact to entity reporting the difficulty and external parties. Causes disruption to normal business operations. Extensions to operational windows may be required. Workaround exists. E.g. Use of SAFE / CMFE / MMFE as an alternative to an internal system. ¹² Downtime anticipated as no longer than one hour. |
| 3 | Low | Minimal impact to entity reporting the difficulty or any external parties. No extensions to operational windows required. Manual workaround exists. E.g. e-mail. |

Comments:

Please provide an explanation for having rated the technical difficulty as you have above:

Anticipated Down Time¹³

| | |
|-------------------------|----|
| Less than 30 minutes | No |
| 30 minutes to 2 hours | No |
| 2 hours to 4 hours | No |
| Longer than 4 hours | No |
| Not known at this stage | No |

¹² Amended with effect from 19 December 2016

¹³ Note deleted with effect from 6 August 2015