

Business Continuity Plan – Manual Processing

Application: ODA Solution

Program Name: Optus Digital Agency (ODA)

Program Number: TB982

Document Identification

|  |  |  |
| --- | --- | --- |
| Document ID | Version | Issue Date |
| BCP ODA | 0.6 | 10 Aug 2012 |

PROPRIETARY NOTICE

This document contains confidential information. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and to not disclose this information to any person outside of Optus without the written permission of the author.

Contents

1. About this Document 1

1.1. Purpose 1

1.2. Audience 1

1.3. IT Disaster Recovery Development Overview 2

1.4. Definitions 2

1.5. Acronyms 2

2. Approach 4

2.1. SODA failure: Re-create SODA transactions 4

2.2. iProcess Failure: Retrigger iProcess transactions 5

2.3. TSA Failure: Replay SODA transactions 6

2.4. Non Recoverable Catastrophic event 7

3. ODA Systems DR Categories and Process Availability 9

3.1. ODA Systems DR Categories 9

3.2. Summary of Key Business Process Availability 9

4. Document Control and Approval 11

4.1. Responsibilities 11

4.2. Approval 11

4.3. Distribution 12

4.4. Version Control 12

4.5. Reference Documents 12

4.6. Related Documents 12

# About this Document

## Purpose

The purpose of this document is to outline the manual process to remove customers from the ODA product in the instance of a non-recoverable disaster of the infrastructure that supports the product.   
It also covers restoral of the ODA service components at a high level where the problem is not catastrophic.

## Audience

* Program Managers
* IT Program Managers
* Lead Architects
* Service Managers
* IT Disaster Recovery Team
* Business Owners

## IT Disaster Recovery Development Overview

ODA has an exemption from Disaster recovery.

See attachments –



## Definitions

|  |  |  |
| --- | --- | --- |
| **Business Continuity Planning** | | The preparation that enables Optus to resume business as quickly and efficiently as possible if a crisis occurs. It includes:   * continuity planning before a crisis; * crisis management during and after an incident; * alternative / manual processes that allows the business to continue (even if at a degraded service level) until business as usual; * recovery plans for IT environment, network environment and facilities. |
| **IT Disaster** | A potentially catastrophic event or series of events that disables IT services and therefore threatens the viability of the Company and requires a focused response. An IT disaster could meet one or more of the following criteria:   * loss of life and/or multiple casualties; * loss of a major IT facility or strategic asset; * extensive damage to IT systems or associated network greater than $1m; * long term business interruption greater than 5% monthly revenue; * serious or permanent damage to the company image; and * long term impact on the company’s ability to deliver products and maintain customer service.   Examples are:   * major fire/explosion; * loss of a Data Centre; * loss of network connectivity to one or more data centres; * loss of a business critical IT application;   (NOTE: ‘Loss’ implies substantial damage, comprehensive or total loss; where restoration is beyond the scope of day to day local management.) | |

## Acronyms

|  |  |
| --- | --- |
| **BCP** | Business Continuity Plan |
| **ODA** | Optus Digital Agency |
| **MTO** | Maximum Tolerated Outage |
| **DR** | Disaster Recovery |
| **HA** | High Availability |
| **TSA** | The Search Agency (3rd party vendor) |
| **FSSG** | Focus Staffware Support Group |
|  |  |
|  |  |

# Approach

At a high level order processing for the Optus Digital Agency product goes from SODA > iProcess > TSA. The BCP approach for recovery differs depending upon which of the systems fails. The ODA solution has a DR exemption on some systems due to their High Availability status. See section 3 of this document for IT descriptions of HA as well as DR categorisation of each system.

Where any major fault occurs on the ODA solution, SODA front-end access will be made unavailable and Command Centre notification issued to internal users. This would stop any new orders and self-serve changes whilst restores are being performed. Such a method is to reduce the challenges in synchronising systems as data gaps will be reduced by not allowing new and change orders (ie new orders won’t add to data gaps between systems).   
Although not being able to sell the product during such times is a negative customer experience the risk in allowing orders to be captured and then hitting subsequent provisioning problems and delays is considered to outweigh this.

The two main internal support areas are IT Web Support, Service Operations and externally TSA. In some instances all groups will be involved in identifying and troubleshooting an issue. In otherwords in the continuity steps described below although one area is identified as the prime – the other 2 groups may also be involved in assisting with issue resolution.

## SODA failure: Re-create SODA transactions

In the instance of a data gap that has resulted from SODA system being down prior to back-up; the high level approach is to review iProcess (or TSA) backups and logs to establish the gap. Transactions missing from SODA then need to be recreated in SODA based on this backup/log information. There are 2 scenarios that can occur in this instance as outlined below.

**Scenario 1**: ~~SODA~~ > iProcess > TSA

This scenario covers where SODA system is not available; however there are (very recent) transactions that have flowed from SODA into the downstream systems. In this case there would be a data gap between SODA and the downstream platforms. In more technical terms SODA database crashes after iProcess sent site deployment request to TSA.  
  
As SODA backups would not have captured the most recent transactions iProcess would contain current data. [In transferring data from SODA to iProcess there are 2 callbacks made from iProcess - an acknowledgement callback and a completion callback.] In this instance some transactions that have only been acknowledged in SODA (and not captured in one of the SODA hourly back-ups) will be lost by SODA and need to be restored via iProcess.

**Impacts:**   
SODA users would be impacted by this type of outage –both end-users attempting self-serve changes and Sales staff trying to place new provisioning orders would be impacted and not able to access the platform.

**Identification/Detection of issue** –   
- Site deployment call back from TSA fails.  
- Customer contacts Optus support advising website not provisioned (or change made not reflected on web site).  
- TSA and Optus monitoring  
**Continuity Steps** -

|  |  |  |  |
| --- | --- | --- | --- |
| **Task** | **Who** | **Contact** | **Duration** |
| Recover SODA DB from backup | IT Web Support | Sanjib Biswas | Based on SLA |
| Engage IPG DB | IT Web Support | Sanjib Biswas | Based on SLA |
| Restore from previous back-up (Restart databases) | IPG DB | Senthil Thirunavukkarasu | Based on SLA |
| Extract delta data from iProcess and reload to SODA | IPG DB | Senthil Thirunavukkarasu | Based on SLA |
| Re-trigger the failed callbacks | TSA | TSA resource | Based on SLA |

Note where re-triggering the original failed callbacks, manual intervention may be required if these fail a second time; it is expected a business SODA user would need to be engaged to re-key information into SODA where the replayed failed callbacks fail a second time.

**Scenario 2**: ~~SODA~~ > iProcess > TSA

This scenario covers where SODA to iProcess call fails and then SODA system suffers an outage. In this case Customer self-serve and Sales transactions not captured in the hourly back-up would be completely lost. This is data which was only ever in SODA and lost before being transferred into iProcess so it would not be in any logs or back-ups. The only option available to identify Sales transactions is to search in OPOM for accounts provisioned with the ODA recurring charge and confirm these are provisioned/linked to a website in SODA. Self-serve transactional data would not be recoverable at all.

**Impacts:**   
SODA users would be impacted by this type of outage –both end-users attempting self-serve changes and Sales staff trying to place new provisioning orders would be impacted (system access would be unavailable).  
Data loss would occur for orders in SODA prior to back-up; exposure to lost data would be the volume of transactions per hour (new orders and self-serve changes).

**Identification/Detection of issue** –   
- SODA application monitoring  
- Customer contacts Optus support advising website not provisioned (or change made not reflected on web site).  
- Sales unable to access SODA or place orders  
- TSA and Optus monitoring  
**Continuity Steps** -

|  |  |  |  |
| --- | --- | --- | --- |
| **Task** | **Who** | **Contact** | **Duration** |
| Recover SODA | IT Web Support | Sanjib Biswas | Based on SLA |
| Identify infrastructure exception | Service Operations | Bindu Subhadramma | Based on SLA |
| Compare OPOM with SODA | Service Operations | Bindu Subhadramma | Based on SLA |
| From OPOM/SODA compare contact customers with recurring charge but no website (SODA data) | Business | Customer Service or Telesales | Based on SLA |

## iProcess Failure: Retrigger iProcess transactions

In the instance of a data gap that has resulted from iProcess systems being down the high level approach is to re-trigger orders once system is up/available.

**Scenario**: SODA > ~~iProcess~~ > TSA

This scenario covers where iProcess system is not available. Such an outage would impact end customers insofar as self-serve changes would not flow through. Similarly no new websites could be deployed during this period.

**Identification/Detection of issue** –   
- IT Web Support, Transaction Management team (TMT), FSSG find iProcess down based on alarm or alert.  
- OV alarms (application monitoring)  
**Tasks** -

|  |  |  |  |
| --- | --- | --- | --- |
| **Task/Action Step** | **Who** | **Contact** | **Duration** |
| Rebuild/Restore iProcess | ODA iProcess L3 support (FSSG), IPG Unix, IPG DBS, Service Operations | Bindu Subhadramma, | Based on SLA |
| Retrigger iProcess transactions | TMT, Service Operations, MAS | Bindu Subhadramma, Tim Burgess, Ray Link | Based on SLA |

## TSA Failure: Replay SODA transactions

In the instance of a data gap that has resulted from TSA systems being down the high level approach is to replay transactions from SODA (which is considered to be the source of truth system into downstream systems).

**Scenario**: SODA > iProcess > ~~TSA~~TSA Primary (front) database crashes before site deployment/change completes. In other words iProcess submitted a site deployment or site redeployment request to TSA. TSA primary database crashes. No callback goes to iProcess in this instance to confirm site deployment or redeployment.

This scenario covers where TSA system is not available. Such an outage would impact end customers insofar as existing websites would currently be unavailable whilst TSA systems are being recovered. Similarly no new websites could be deployed during this period and recent self-serve changes may not be reflected on the customers’ domain.

**Identification/Detection of issue** –   
- TSA find data corruption based on Nagios alarm or alert.  
- TSA reporting/data feed finds mismatch on calls.  
- OV alarams  
- Customer contacts Optus support to advise website not working (or change made not reflected on web site).  
**Tasks** -

|  |  |  |  |
| --- | --- | --- | --- |
| **Task/Action Step** | **Who** | **Contact** | **Duration** |
| Recover TSA servers (Optus have infrastructure ownership and TSA application ownership) Task is to switch front DB’s (from DB01 to DB02) | TSA (via call from IT Web Support team) | TSA resource (Sanjib Biswas) | Based on SLA |
| Complete pending site deployment callback’s | TSA (via call from IT Web Support team) | TSA resource | Based on SLA |
| Identify gaps between TSA Servers and SODA | IT Web Support & TSA | Sanjib Biswas TSA Resources | Based on SLA |
| Identify gaps between TSA Servers and iProcess | Service Operations | Bindu Subhadramma TSA Resources | Based on SLA |
| Replay SODA | IT Web Support | Sanjib Biswas Bindu Subhadramma | Based on SLA |
| Re-trigger transactions bot in DB02 from iProcess | TMT, Service Operation | Bindu Subhadramma, Tim Burgess | Based on SLA |

Note that self-serve changes made in the last 24 hours may be lost in this instance and customers will need to re-do their changes as we will have no other record to replay the change.

## Non Recoverable Catastrophic event

In the instance of a non-recoverable event on the ODA product the approach is to contact customer, de-provision product and adjust charges.  
The below process outlines the steps to be taken (also reflected in process flow diagram) –

|  |  |  |  |
| --- | --- | --- | --- |
| **Task** | **Who** | **Contact** | **Duration** |
| Identify non-recoverable infrastructure error (i.e. deemed catastrophic) | Dictated by # of users complaining about the issue – ie when it has become a Sev 1 all dictated by incident management process | IT and Product Management |  |
| Extract Active customer list | IT – dependent on which system available (ie SOS, SODA or iProcess) | SODA – Sanjib Biswas iProcess - Bindu Subhadramma |  |
| Define Customer Communications | Product Manager/Marketing/Legal | Andrew Kim |  |
| Contact Customers with Communication | Product Manager/Marketing | Andrew Kim |  |
| De-provision product on Optus Systems (i.e. VOIP, bolt-on) | Care MAS | Robert Hanimyan Ray Link |  |
| Establish if Customer wants to retain Domain and arrange for transfer | MAS | Ray Link |  |
| De-provision anything remaining | Care MAS | Robert Hanimyan Ray Link |  |



# ODA Systems DR Categories and Process Availability

The below tables have been sourced from the IT ODA High Availability document. See References section for link to the full document and more detailed information on support hours for each component system.

## ODA Systems DR Categories

|  |  |  |
| --- | --- | --- |
| **System Name** | **DR Category** (Hot, Warm, Cold) | **Justification** |
| SODA (Sales) | Warm | Platform is on a VM cluster. If server goes down, V Motion initiates a new session immediately. No Cross data centre DR. |
| iProcess (ODA EIP) (Provisioning) | Warm | Platform is on a VM cluster. If server goes down, V Motion initiates a new session immediately. No Cross data centre DR. |
| TSA (Provisioning and Customer Self-Serve) | Cold | No HA or DR at this stage. Will be addressed via different Program. Business to prioritise DR capability post go live |
| Customer Websites | Warm | High Availability required to meet website SLAs provided. Cross Data centre DR a lower priority. Will be addressed via different Program. Business to prioritise DR capability post go live |

## Summary of Key Business Process Availability

|  |  |  |  |
| --- | --- | --- | --- |
| **Process** | **Internal SPOF?** | **Outage Scenario** | **Outage Business Impact** |
| Sales Order Capture – SODA | No – Fully Clustered with automatic switchover | Negligible for single failure | Can accept orders but Domain Name or ABN Check will fail as long as External Interface is down |
| iProcess Order Processing | No – Fully Clustered with automatic switchover | Negligible for single failure | Orders sitting in iProcess Queue can be retriggered once system is up |
| Site Deployment from iProcess | Yes – TSA Account DB Server | 12Hrs for either Server or DB Rebuild & Restore | New customer - No New site deployment  Existing customer, requested changes to site won’t be processed |
| Site Deployment from TSA | Yes – TSA Account DB Server and WebServer DB | 12Hrs for either Server or DB Rebuild & Restore | New customer - No New site deployment  Existing customer, requested changes to site won’t be processed |
| Self-Serve – Customer Access | Yes – SaasConnect | 6 Hrs. to manually switch over to 2nd Server | Customer unable to log-in until service is restored |
| Site Deployment – Self Serve | No - but manual switchover for Jboss Servers | 6 Hrs. to manually switch over to 2nd Server | Customer may have to re-enter details for the requested changes to their website. |
| Customer Website | No – Fully clustered NFS + a webserver failover. | Negligible for single failure | Website not accessible from internet |

## System Back-ups

|  |  |  |  |
| --- | --- | --- | --- |
| **Back Timings** | **SODA DB** | **iProcess DB** | **TSA DB** |
| How long does backup take to run? (with today’s current data size) | 30 mins | 10 mins | 30 mins |
| What is the maximum time a backup may take to run? (with today’s current data size) | 1 hour | 1 hour | 1 hour |
| How long does it take to restore from a backup? (with today’s current data size) | 1.5 hours | 1 hour | 2 hours |
| How far back historically do backups go (weeks, months)? (Daily backups indicated in field, although weekly and monthly retention of backups occurs as well.) | 5 weeks | 5 weeks | 40 days |
| Are backups only on deltas since previous back-up taken or are they full back-ups of entire DB? (incremental throughout the day but full backup daily) | Full daily | Full daily | Full daily |
| Are back ups D2D (disk to disk) or D2T (disk to tape)? | D2T | D2T | D2D |

## Note on Testing of Back-up’s

In the case that DB has become corrupt and still functioning testing a restore will not bring that corruption to the surface; unless you are lucky enough for the restore process to glitch due to the particular corruption. This highly unlikely as system would glitch while it performs read and write operations to the DB during normal operation.   
Ongoing and routine maintenance with regular health checks on the databases can only prevent the scenario of a back-up containing a corruption from occurring and carrying on for an extended period of time passing the retention period of the backed up data.

# Document Control and Approval

## Responsibilities

Responsibilities for this document have been assigned as follows:

| Role | Responsibility | Assigned to | Position |
| --- | --- | --- | --- |
| Document Approver | Approve the issue of each version. | Adam Russell | Business Program Manager |
| Document Owner | Overall responsibility for document accuracy and distribution list. | Andrew Kim | Product Manager |
| Document Author | Prepare the document to the Document Owner's specification. | Toby Store | Business Process Analyst |
| Reviewers |  | Jesse Snow  Robert Hanimyan Dante Lorredo Ronny Effendi Sanjb Biswas Bindu Subhadramma |  |
| Document Controller | Version control and distribution to nominated document holders. | Toby Store |  |
| Address of Document Controller | Optus Centre Sydney - 1 Lyonpark Road, Macquarie Park NSW 2113 | | |
| Copyright | This material is copyright. No part of this document may be reproduced in any form, stored in a retrieval system or transmitted without the prior written permission of Optus Communications Pty Ltd. | | |
| Confidentiality | This document is classified Commercial in Confidence. It is subject to a confidentiality agreement between the recipient organisation and Optus Communications Pty Ltd. Its contents must not be divulged to third parties. | | |

## Approval

If this table does not contain the signatures of the nominated approvers, you have an unapproved copy. Contact the Document Controller for more information.

I have reviewed this document and authorise it for issue:

| Approved by | Title | Signature | Date |
| --- | --- | --- | --- |
| Adam Russell | Business Program Manager |  |  |
| Andrew Kim | Product Manager |  |  |
| Dante Lorredo | IT Project Manager |  |  |
| Sanjib Biswas | IT Web Support |  |  |
| Bindu Subhadramma | IT Project Manager |  |  |
| Robert Hanimyan | Customer Support Manager |  |  |

## Distribution

|  |  |
| --- | --- |
| This document is located in Shared Folder: | \\Scfs8492\consumerdelivery$\86-Digital Life\01. Program List\Digital Agency\4. Processes\BCP |

| Personnel with Access to Shared Folder | Personnel who Require Hard / Soft Copy |
| --- | --- |
| ODA Program Team |  |
|  |  |
|  |  |
|  |  |

## Version Control

| Version | Date | Section | Nature of Amendment | Amendment Author |
| --- | --- | --- | --- | --- |
| 0.1 | 5/7/2012 | All | Document Created | Toby Store |
| 0.2 | 16/7/2012 | 2.2 | Data gap sections added | Toby Store |
| 0.3 | 23/7/2012 | Many | iProcess failure section added and updates to other areas based on 20/7 workshop; reference to ODA HA added | Toby Store |
| 0.4 | 23/7/2012 | Many | Numerous updated after individual meetings with IT Web Support, Service Operations, Care and IT PM team. As well as written feedback. | Toby Store |
| 0.5 | 27/7/2012 | Many | Document clean-up and issue for final feedback. | Toby Store |
| 0.6 | 10/8/2012 | 1.3, 3.3 & 3.4 | Backup information added (2 new sections). As well as additional exemption mail added in 1.3 | Toby Store |

## Reference Documents

| Reference Document | Version | Date | File Location |
| --- | --- | --- | --- |
| SODA (Ender entry) | N/A |  | <http://ender/show_app.php?app=4962> |
| iProcess (Ender entry) | N/A |  | <http://ender/show_app.php?app=5582> |
| TSA (Ender entry) | N/A |  | <http://ender/show_app.php?app=4963> |
| ODA High Availability | V1.2 | 9-July-2012 | [\\Scfs8492\consumerdelivery$\86-Digital Life\01. Program List\Digital Agency\4. Processes\BCP\ODA High Availability - V1 1 - ACR Edits.pptx](file:///\\Scfs8492\consumerdelivery$\86-Digital%20Life\01.%20Program%20List\Digital%20Agency\4.%20Processes\BCP\ODA%20High%20Availability%20-%20V1%201%20-%20ACR%20Edits.pptx) |
| DR Exemption certificate | N/A |  | [\\Scfs8492\consumerdelivery$\86-Digital Life\01. Program List\Digital Agency\3. Solution Designs\DR Exemption certificate.docx](file:///\\Scfs8492\consumerdelivery$\86-Digital%20Life\01.%20Program%20List\Digital%20Agency\3.%20Solution%20Designs\DR%20Exemption%20certificate.docx) |
| SLA | 5 | 4-April-2012 | [\\Scfs8492\consumerdelivery$\86-Digital Life\01. Program List\Digital Agency\4. Processes\SLAs](file:///\\Scfs8492\consumerdelivery$\86-Digital%20Life\01.%20Program%20List\Digital%20Agency\4.%20Processes\SLAs) |

## Related Documents

| Related Document | Version | Date | File Location |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

End of Document