CloudSense™

IT Business Continuity & Disaster Recovery Plan

Version 1.0
Last Updated: January, 2025
Document Code: TRI-POL-0115

Legal Notices

The information in these materials is confidential and proprietary of the Company and is provided for informational purposes only. Company and its affiliates assume no responsibility for any errors that may appear herein. Company reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of the Company to notify any person of such revisions or changes. COMPANY MAKES NO EXPRESS GUARANTEES OR ANY GUARANTEES IMPLYING LEGAL INTENT WITHIN THIS DOCUMENT. The content of this document is not intended to represent any recommendation on the part of the Company.

This document may provide access to or information on content, products, or services from third parties. Company is not responsible for third party content referenced herein or for any changes or updates to such third party sites, and you bear all risks associated with the access to, and use of, such websites and third party content. Company and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Document Control

This document is primarily intended for internal use only. It is against corporate policy to disclose documentation to third parties (including customers) without the necessary approval. Any exception to this policy must be approved by the SaaS Ops VP.

Table of Contents

Information Technology Statement of Intent

This document delineates the company policies and procedures for technology Disaster Recovery ("DR"), as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes recommended procedures for all the products. Additional details pertaining to a specific product may be documented in a Product DR Appendix.

In the event of an actual emergency situation, modifications to this process may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and support of the business continuity targets.

Policy Statement

Corporate management has approved the following policy statements:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key operational activities.
- The disaster recovery plan should be periodically tested preferably in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the product recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- To ensure that all staff fully understand their duties in implementing such a plan;
- To ensure that operational policies are adhered to within all planned activities;
- To ensure that proposed contingency arrangements are cost-effective;
- To understand the criticality of the product and its specific components;
- To consider implications on other products.

Dependencies

While this DR Plan is outlined based on the provision or services, it must be noted that the product SaaS Ops services and the DR Plan itself is dependent on underlying service provision by 3rd parties, such as AWS and therefore is dependent on the provision of their input and support for the implementation of its disaster recovery efforts. Whilst effort and arrangements are in place to attain the specified RTOs and RPOs and mitigate as far as possible impacts from third parties, certain emergencies may arise from these 3rd party services that could be outside the company's direct control.

DR Personnel Responsibilities

For each product, the DR team will be constituted and tasked with:

- Preparation of the DR Plans for a specific product;
- Preparation of Test Plans to periodically test the DR Plans in a simulated environment;
- Carrying out these test plans and report on the outcome from these tests;
- Identifying areas where the DR Plans could or need to be improved and determine how these improvements should be carried out;
- Obtaining approvals for implementing these improvements;
- Applying these improvements and retest to confirm the successful attainment of the target improvements;
- Maintaining the details of the DR Plan on an on-going basis and especially after any major changes are carried out to the product architecture, its components or the underlying IT infrastructure.

Product DR Team Members

The team is similar to the one involved in the regular incident management process and includes the SaaS L1/L2, Product CTO, SaaS Ops VP and Engineering SVP.

Key Personnel Notification Call-out

The notification of a DR incident will follow the normal incident management process which is automated through JIRA and PagerDuty (or similar software) to have the respective DR team notified as soon as possible.

External Contacts

External Contacts are considered to be those critical resources that are required for the planning of the DR process as well as those required for a successful recovery in the event of an emergency.

The contact information for the External Contacts for the Product is included in the Product specific documentation.

Other Internal Documents

Any additional documentation for each product is included in the respective internal Product Operations and DR documentation as well as Corporate material.

The documents that are directly related to this main DR Planning document are:

- Product Specific SaaS Ops Documents
- Company Policies and Procedures

1 Plan Overview

1.1 Plan Reviewing and Updating

The DR Plan ("DRP") updating process is carried out in a structured and controlled manner. The overall DR Plan as well as the Product SaaS Ops documentation are reviewed at least once a year or after the occurrence of a DR Incident.

The main resources that are involved in the periodic Product DR Plan review and update primarily include the Product DR team members as specified above. Other resources such as DBA and infrastructure specialists are also involved as required.

Whenever changes are made to the DRP, they are evaluated and logically tested and, where applicable, the appropriate amendments are made to the product support and recovery materials. This review and update process follows normal change control procedures under the control of the SaaS Ops VP.

1.2 Backup Strategy

The overall standard backup strategy is aligned around backing up critical systems and data so as to allow for recovery to the specified RPO within the defined RTO for the particular product.

The standard backup strategy is applied for all products and unless otherwise stated for a specific product or product component, backups are taken on a daily basis.

1.3 Risk Management

There are many potentially disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of product disruption which could arise from each type of disaster ranging from day-to-day occurrences such as the failure of a particular Virtual Machine, Database or network connection, to the less likely but more severe situations such as total system outage.

The key cross product potential disasters have been assessed as follows:

Potential Disaster	**Probability Rating**	**Impact Rating**	**Brief Description Of Potential Consequences & Remedial Actions**
Flood	1	5	This is protected against by AWS own protection mechanisms on Cloud Services as per its compliance with ISO27001
Fire	1	5	
Tornado	1	4	
Electrical storms	3	3	
Act of terrorism	1	5	
Act of sabotage	1	5	
Electrical power failure	2	4	
Loss of communications network services	4	4	
Loss of DB Instance	2	3	Standard DB Incident Management in place to recover DB within defined RTO. Various products also have client instances which would limit impact to one client.
Loss of Application Instance	2	3	Standard Incident Management in place to recover an application instance within defined RTO. Various products also have clustered instances which can absorb loss of an application instance. Others have client instances that would limit impact to a single client.
Loss of Web Server Instance	2	3	Standard Incident Management in place to recover an instance within the defined RTO. Various products also have clustered instances which can absorb loss of an application instance. Others have client instances that would limit impact to a single client.
Virus Attack	2	4	Standard Instance Recovery within the specified RTO will be affected In the event that the Anti-Virus protection fails and results in a system failure.
Application level network failure	1	3	Normally multiple network routings

Probability: 1=Very Low, 5=Very High   Impact: 1=Minor annoyance, 5=Total Non-Availability

1.4 Recovery Point Objective

The standard Recovery Point Objective across all products has been defined as aiming to recover to the last usable daily backup position. This is on a reasonable commercial endeavors basis.

If specific products or product components have different RPOs, they are documented in the respective Product DR Appendix document.

1.5 Recovery Time Objective

The standard Recovery Time Objective across all products has been defined with the aim to recover the product to the standard RPO level in 4 hours. This is on a reasonable commercial endeavors basis.

If specific products or product components have different RTOs, they are documented in the respective Product DR Appendix.

2 Emergency Response

2.1 Plan Triggering Events

Key trigger issues that would lead to activation of the DRP are loss or failure of:

- Multiple critical servers
- Critical databases
- Total system
- Communications including networking components
- Power

2.2 Activation of Emergency Response

When an incident in the Plan trigger event occurs, a request will be raised in the ticketing system as per the normal incident response procedure. The Emergency Response Team ("ERT") is made up of the same resources as those involved is normal incident management process that includes the:

- Product CTO
- L1 & L2 Support
- L1 & L2 SaaS
- SaaS Ops VP
- Engineering SVP

The ERT will then decide the extent to which the DRP must be invoked. Responsibilities of the ERT are to:

- Respond immediately to the incident;
- Assess the extent of the incident and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery to maintain vital services and return to normal operation;
- Ensure staff and any required third party support teams are notified, allocate the responsibilities and activities as required.

2.3 DR Management Procedures

The management of the disaster recovery process will follow along the same lines as the normal incident management.

All the DR team members must be conversant with the procedures defined in the normal Incident Response Manual as well as the DR Appendices covering the specific products.

The main steps in this Incident Management process can be summarized as follows:
If a ticket has not already been raised, then

L1/Support must:

- Create a Jira ticket with Priority: Showstopper, Type: SaaS Incident.

L1 must:

- Post product outage information in the incident and product chatrooms;
- Invite the L1 on coverage, L1 product experts, L2 product experts, assigned SaaS Ops VP for the product, product support and anyone needed from the maintenance or engineering team to join the meeting bridge;
- Use the respective **Product DR Appendix** or **Playbook** to solve the incident and return the product to normal operational status.

L2 and greater (if escalated) must:

- Work on solving the issue as soon as possible;
- Report to L1 the Estimated Time to Resolve;
- Create the linked tickets for related work items required for other units as necessary:
  - Tickets to Engineering to assist with fixing the issue or applying hotfix if required;
  - Tickets to Central Services if part of the system is managed by that team;
  - Tickets to AWS if the recovery necessitates their input or support;
  - Tickets to other third parties, such as Google, MongoDB Atlas if their services are on the critical path for recovery.

SaaS Ops VP must:

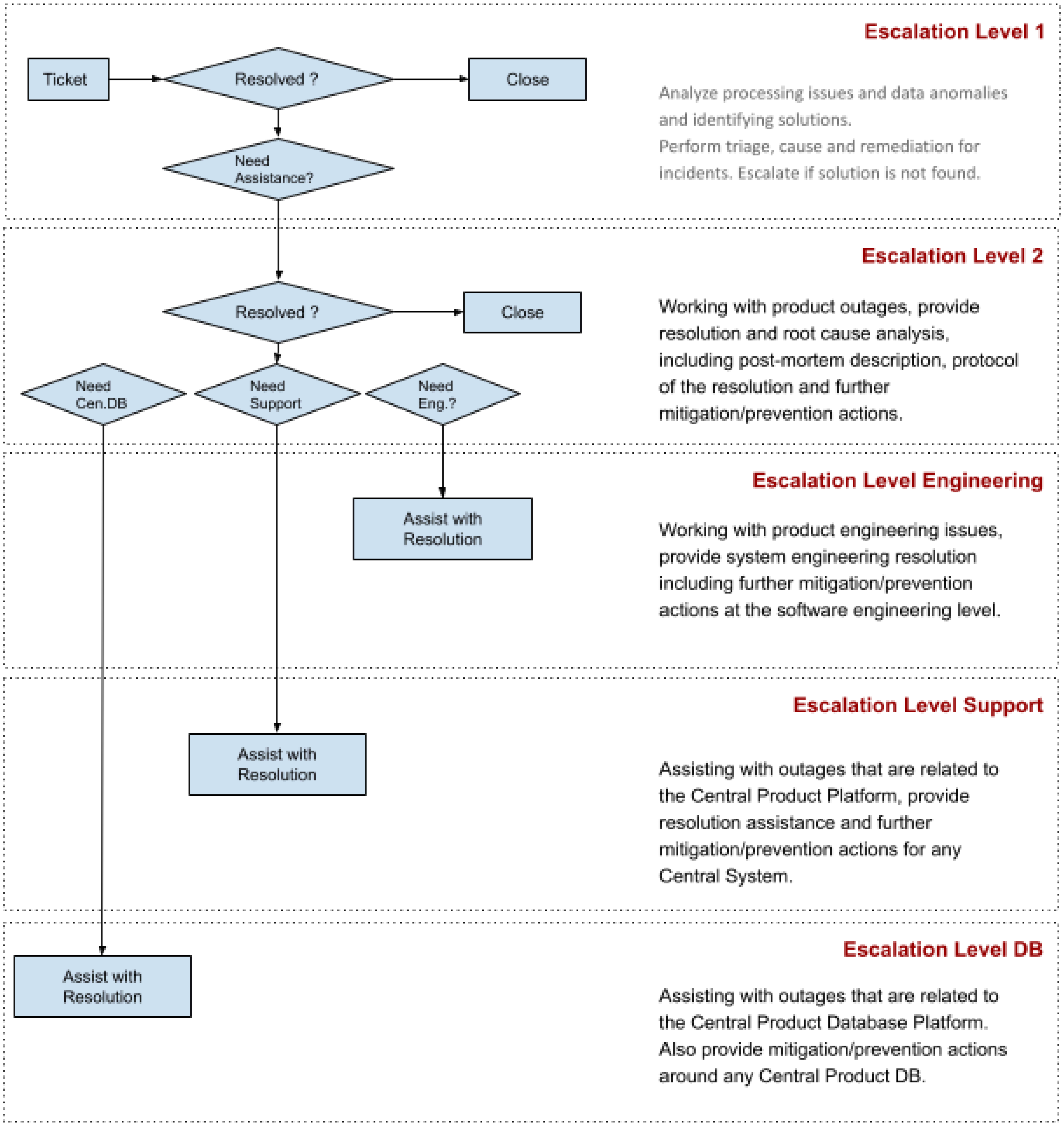
- Monitor progress of recovery and provide any input required to DRT to help expedite the recovery process;
- Assist in resolving issues that arise around the SaaS Operations during the recovery process;
- Interface with third parties as required.

Product CTO must:

- Monitor progress to recovery and provide any input required to DRT.

Further details for the DR response are noted in the Incident Management Manual.

2.4 DR Procedure Flow Overview



Escalation Level 1

Analyze processing issues and data anomalies and identifying solutions.
Perform triage, cause and remediation for incidents. Escalate if solution is not found.

Escalation Level 2

Working with product outages, provide resolution and root cause analysis, including post-mortem description, protocol of the resolution and further mitigation/prevention actions.

Escalation Level Engineering

Working with product engineering issues, provide system engineering resolution including further mitigation/prevention actions at the software engineering level.

Escalation Level Support

Assisting with outages that are related to the Central Product Platform, provide resolution assistance and further mitigation/prevention actions for any Central System.

Escalation Level DB

Assisting with outages that are related to the Central Product Database Platform. Also provide mitigation/prevention actions around any Central Product DB.

2.5 Contacting DR Staff

Product Managers will serve as the focal points for their product, while designated staff will communicate with other staff to discuss the crisis/disaster and the DR immediate plans. Staff who cannot reach other staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster and the response being undertaken.

2.6 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.7 Communication with Customers

During a DR event, the product Customer Support staff will communicate with the respective product customers and advise them of the current status with respect to the DR progress as well as the expected time for the recovery to be completed.

Should there be any substantial changes during the recovery process that impacts the completion of the recovery process, customers will be notified of these changes by the product Customer Support staff and advised on the expected target for recovery completion.

3 DRP Exercising & Testing

Disaster recovery plan exercises are an important part of the plan development process. Plan exercising ensures that disaster recovery teams are familiar with their assignments and, more importantly, are confident in their capabilities.

The Disaster Recovery Plans are tested when significant changes are brought into the environment to ensure that the plans are still fully applicable and that the standard or product specific RPO and RTO can be achieved.

Depending on the changes to the systems, the testing can be in the form of:

- **Paper test:** Individuals read and annotate recovery plans;
- **Walkthrough test**: Groups walk through plans to identify issues and changes;
- **Simulation**: Groups go through a simulated disaster to identify whether emergency response plans are adequate;
- **Parallel test**: Recovery systems are built/set up and tested to see if they can perform actual business transactions to support key processes. Primary systems still carry the full production workload;
- **Cutover test**: Recovery systems are built/set up to assume the full production workload. You disconnect primary systems.

This testing is normally carried out on environments that are separate from the production environment but are representative of the production environment.

This testing also allows for identification of possible improvements to the DR Plan that would improve the overall recovery process as well as the recovery time.

Results from the DR plan testing are communicated to the relevant product management team as well as the product operations support team so that they can identify solutions that could preempt failures and be in a better position to respond when incidents occur.

3.1 Testing Methodology

Plan

The Test Plan is built around what could go wrong in the product environment and aims to cover what is most critical in the disaster recovery plan, especially for mission-critical components.

The Test Plan should typically include:

- What are the steps to be carried out;
- Any parameters or external content (e.g. scripts) that are required to execute the specific step;
- What outcome is expected from each test step;
- What counts as a successful test or an unsuccessful test.

Testing can be carried out in an actual live environment (e.g. UAT, Production) or in an environment specifically designated for DR testing. The latter option is valid and preferred as long as it is truly representative of the environment it is simulating.

If the test is carried out in a live environment, as opposed to a DR test environment, the team must have established the details for how to return to normal operations in the least time possible and without data loss if one of the tests fails.

Notify

Make sure that you notify all potentially affected users of the system that is part of a test, and how it might affect their productivity. Most tests on actual live environments will need to be done on the weekends or late at night to minimize any downtime. Another benefit of this approach is that if something does go wrong, there is more time to make it right before the system is again heavily utilized.

Of course, with certain products there really is no “good” time for downtime. Also, some situations might call for doing mid-week tests to simulate actual system loads. If the test exceeds the expected duration or problems are encountered, make sure interested parties are updated with progress reports and expected return to normal operations.

Execute

Execute your test according to the defined test plan and use the documented disaster recovery plan to recover. Here is where institutional knowledge can be developed and documented so all can benefit. And that leads to the next step.

Record

Make sure to record the test and its results using the respective DR Test Results Form. Record not only the steps undertaken and the actual outcome, but also whether the recovery tracked according to plan. Key points to record are any steps that have been left out from the Test Plan or the actual DR Plan as well as what details are not well documented.

This is one area that is normally weak and it must be ensured that all the relevant details are captured during the test as “lessons learned”.

Review and Improve

Once the test results have been gathered and documented, it is essential to review the whole test and outcomes. The aim of this review is to:

- Dissect the test,
- See what went right,
- See what went wrong, and
- Identify improvements that are necessary for the next test plan or test cycle.

Once the respective improvements have been document, it is essential to:

- Plan for the implementation of these improvements;
- Get approval for any additional budget that may be required to implement the improvement(s);
- Track that the improvements are actioned and completed.

Closing the loop on the DR Test Plans in this manner is the best way to get future benefit from subsequent tests.

4 Maintenance and Training

4.1 Plan Maintenance

The plan must be reviewed and updated to reflect major changes to the SaaS Ops procedures that may be required to be included in this DR Plan. It is the responsibility of the SaaS Ops VP to maintain the plan which process may be delegated by the VP to specific SaaS Ops individuals as deemed necessary by the SaaS Ops VP.

4.2 Training

The SaaS Ops VP is responsible for ensuring that all recovery team staff have the knowledge and skills necessary to implement the plan and carry out essential tasks of the Disaster recovery Plan. It is important that the staff completes the mandated corporate policies and procedures training.

5 Document Management

Revision History

REVISION	DATE	POSITION	DESCRIPTION
1.0	January, 2025	SaaS Ops VP	Initial Document

Approval History

REVISION	DATE	POSITION
1.0	January, 2025	Product CTO