# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

**SECTION G5  
TEAM 7**

**SMART CONTRACT PRODUCT (SCP)**

**DISASTER MANAGEMENT PLAN**

# 

# 

# 

# 

# 

# 

# 

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 21-3-2019 | 1.0 | Initial write-up | Kenny Kwek, Ong De Lin, Janell Lee, Mark Tan, Lau Jun Rong |
|  |  |  |  |

Table of Contents

[Revision History](#_bcpu8aolxur) **2**

[Disaster Recovery Statement](#_n27ip7soe50k) **5**

[Purpose](#_so5wv6n5diku) 5

[Emergency - Triggering Events](#_7b7iphedjt2w) **5**

[Emergency Alert, Escalation and DRP Activation](#_t4llbjm0muwc) **6**

[Plan Activation](#_hdx7xuz29ik) 6

[Updates of Disasters](#_j6xb7cmxwxbz) 6

[Notification Calling Tree](#_iv174390d4j9) 6

[Alternate Recovery Site](#_4m1teyd1qmv2) 7

[Critical Business Processes](#_ednoljmvbkhi) **7**

[Critical Technologies](#_pqmp8ngd953n) **8**

[Contact Information](#_mcc7m12b6ajo) **8**

[Key Appointment Holders](#_etzf7imbyvi) 8

[Disaster Recovery Team](#_79hldh8rcio2) 8

[External - Vendors and Customers](#_d0yd5mewhnk8) **9**

[Recovery Time Objective & Recovery Point Objective](#_ubilywwlv3ny) **9**

[List of Potentially Affected Vendors](#_lpou17rd47yl) **10**

[Vital Documents](#_o3kkcpcqm3xa) **10**

[Disaster Recovery Event Recording Form](#_glk0qn4hn8wl) 10

[Risk Management](#_468vm2qrchy2) 10

[Disaster Recovery Team](#_5phqw0gsg6ux) **10**

[Roles and Responsibilities](#_vk0syi9jkoyx) **10**

[Disaster Recovery Education](#_bykanwtqfzgd) **11**

[Disaster Response Actions for SCP](#_vjuwrj3nd932) **11**

[Disasters relating to SCP Termination](#_lyqgqukwowo6) 12

[Disasters relating to configuration files of SCP](#_8gnxuhgqdq9t) 12

[Disasters relating to documentation](#_3bjnwptvqyph) 12

[Disasters relating to External Triggers e.g. Flooding](#_sypctmg45zv2) 13

[IT Network Architecture Diagram](#_nfl2r3wp6xon) **13**

[Recovery Sites](#_ydhw2cu78whg) **14**

[Disaster Recovery Plan Review](#_tch97i60s3km) **14**

[Testing Frequency](#_vpbr3qpb3kss) 14

[Types of Testing](#_ttyp0dt6bo24) 14

[Assessing Test Effectiveness](#_3ipwracza3ax) 15

[Plan Updating](#_fitpksovukz5) 16

[Post-Review Standard of Procedures](#_t6af1x1ksret) **16**

# 

# Disaster Recovery Statement

## Purpose

The principal objective of the disaster recovery document is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. As such, the main goals of the Disaster Recovery Plan is broken down into the three components below:

***Prevention*** *(pre-disaster)*

The pre-planning required to **minimize the overall impact of a disaster** on systems and resources. This pre-planning also **maximizes the ability of an organization to recover from a disaster**.

***Continuity*** *(during a disaster)*

The process of maintaining critical business processes and critical technologies. Continuity measures **prevent the whole organization from folding** by preserving essential systems and resources.

***Recovery*** *(post-disaster)*

The steps required for the **restoration** of all systems and resources to full, **normal operational status**.

Additional objectives include the following:

1. Ensure prompt response to disasters
2. Achieve rapid and effective recovery
3. Ensure Disaster Recovery Plans are consistently updated
4. The need to ensure that all employees fully understand their duties in implementing such a plan
5. The need to ensure that operational policies are adhered to within all planned activities
6. The need to ensure that proposed contingency arrangements are cost-effective
7. The need to consider implications on other company sites
8. Disaster recovery capabilities as applicable to key customers, vendors and others

# Emergency - Triggering Events

The key triggers that would lead to activation of the DRP are:

|  |  |
| --- | --- |
| Internal Trigger Events | 1. SCP instance is terminated 2. SCP configuration files are corrupted 3. Documentations are corrupted |
| External Trigger Events | 1. Flooding 2. Fire 3. Pandemic 4. Power Supply Cut |

# 

# Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

## Plan Activation

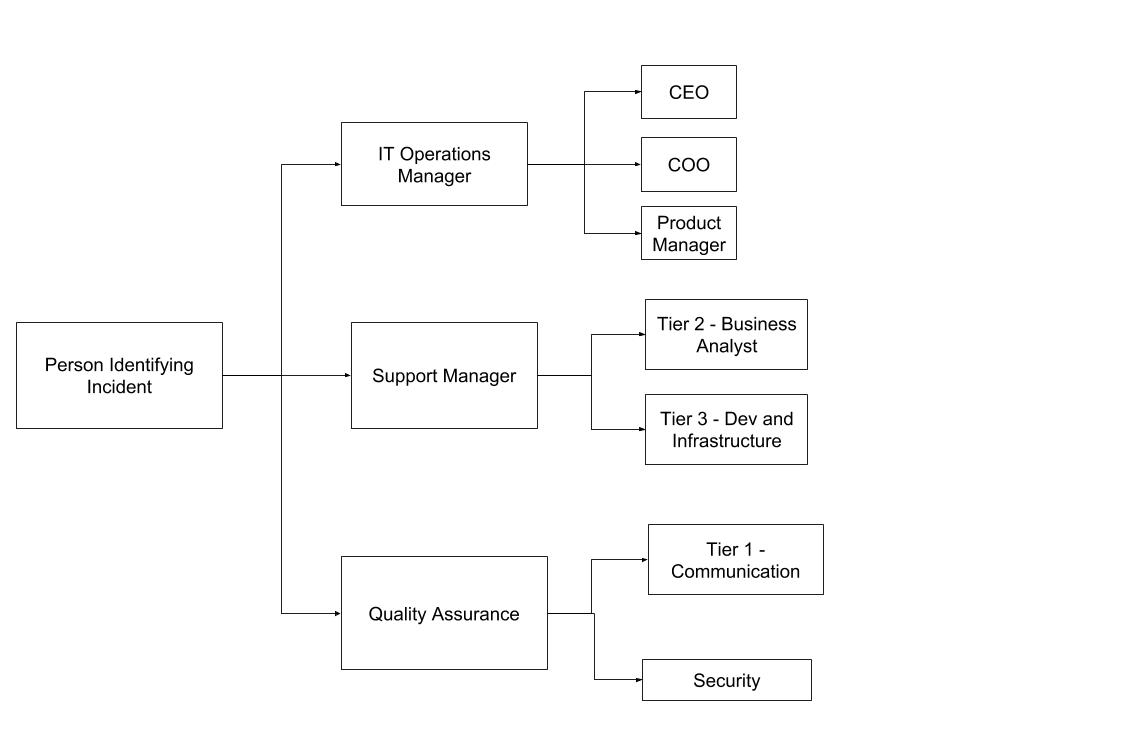
In most situations, the DRP activation will be set in motion by the key appointment holders or business heads. However, in some cases, the IT Operations Team may play the role of escalating a situation if it is assessed to be a potential disaster.

## Updates of Disasters

The team can use the IS214-ESM-G5 or IS214-Project Channel in telegram, email and [corporate website](https://sites.google.com/a/smu.edu.sg/is214-enterprise-system-management/assigments) for the latest information on the disaster and the organization’s response.

### Notification Calling Tree

The team has formulated a notification calling tree to disseminate the information in the event of a disaster. This will identify concerns and potential impacts of the disasters, keeping the stakeholders in the loop.



The notification should entail the following:

|  |  |
| --- | --- |
| **Components** | **Description** |
| **Details of disaster** | Concise but detailed description of disaster |
| **Nature of disaster** | Security, network, etc. |
| **Potential impact of disaster** | Qualitative and quantitative aspects of the disaster’s impact |
| **Actions undertaken as of reported time** | What actions have been taken so far to mitigate the disaster |
| **Actions to be taken until disaster has been recovered** | High-level details of how to recover disaster |

## Alternate Recovery Site

If necessary, [13.229.69.55:8000](http://13.229.69.55:8000) will be used as the back up site for SCP.

# Critical Business Processes

The ability to identify and quantify which critical business processes that, when not functional, may damage a company’s reputation or ability to operate, is a critical stage in the Disaster Recovery process. Overall resilience capabilities should be prioritized to mitigate any interruption and depends on the disaster scenario.

As part of prioritizing which business processes are critical in the disaster, the timing of interruption, likelihood level, duration of disaster, staffs required to meet the recovery objective, operational impact, financial impact and recovery time required will be considered.

The IT Operations Manager should also explore and quantify the above mentioned aspects to initiate the Business Impact Analysis process, which will be linked to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) assigned to the disaster.

# Critical Technologies

Critical Technologies to be considered in the event of a disaster are documented in our Configuration Management Description.

[Refer here for our Configuration Management Description for SCP](https://docs.google.com/document/d/1C66wkecV_y7yzAwERyNJXGGmhnepqWcQg9Xt7GJhsCk/edit#heading=h.70uqyy8yrc9g)

# Contact Information

## Key Appointment Holders

|  |  |
| --- | --- |
| **Role** | **Contact** |
| Chief Executive Officer | [is214ceo@gmail.com](mailto:is214ceo@gmail.com) |
| Chief Operating Officer | [is214coo@gmail.com](mailto:is214coo@gmail.com) |
| Product Manager | [is214pm@gmail.com](mailto:is214pm@gmail.com) |

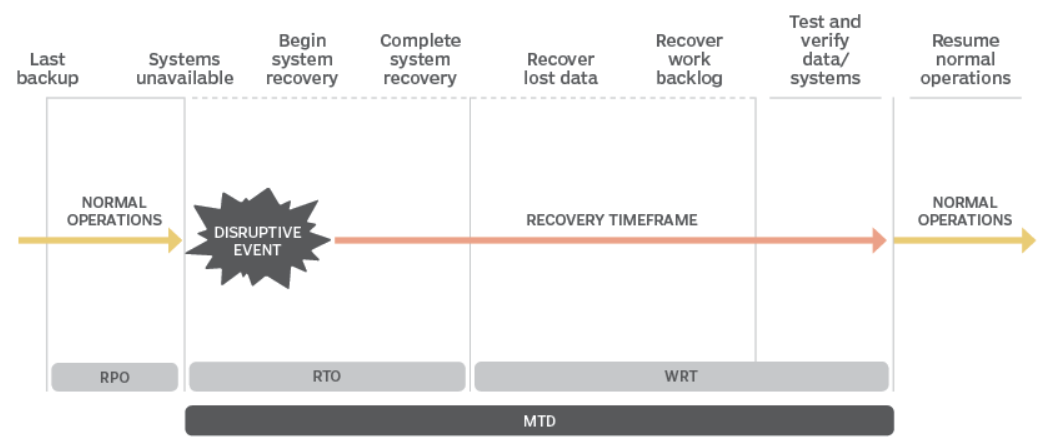
## Disaster Recovery Team

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Contact** |
| Kenny Kwek | IT Operations Manager &  Support Manager | [kenny.kwek.2017@sis.smu.edu.sg](mailto:kenny.kwek.2017@sis.smu.edu.sg) / 9620 1737 |
| Ong De Lin | Quality Assurance | [delin.ong.2017@sis.smu.edu.sg](mailto:delin.ong.2017@sis.smu.edu.sg) / 8168 9456 |
| Lee Jia Ern, Janell | Tier 1 - Communication | [janell.lee.2017@sis.smu.edu.sg](mailto:janell.lee.2017@sis.smu.edu.sg) / 8285 7148 |
| Tan Rong Jian Mark | Tier 2 - Business Analyst | [mark.tan.2017@sis.smu.edu.sg](mailto:mark.tan.2017@sis.smu.edu.sg) / 8405 7248 |
| Lau Jun Rong | Tier 3 - Dev and Infrastructure & Security | [junrong.lau.2017@sis.smu.edu.sg](mailto:junrong.lau.2017@sis.smu.edu.sg) / 9297 1479 |

# External - Vendors and Customers

As of 1 April 2019, the key external vendors include Fantasma Web Services, Website Developer Partner. Additionally, other than the public users of the corporate website, the key external customers do not include any VIPs.

# Recovery Time Objective & Recovery Point Objective



In the case of a disaster, there are several critical recovery points to keep track of and they include the following:

1. **Recovery Point Objective (RPO)**, maximum sustainable data loss based on backup schedules and data needs
2. **Recovery Time Objective (RTO)**, The duration of time required to bring critical systems back online
3. **Work Recovery Time (WRT)**, The duration of time needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered)
4. **Maximum Tolerable Downtime (MTD)**, The duration of the RTO plus the WRT.
5. When either critical business operations or normal operations resume

Since the WRT, MTD and when normal operations can be resumed all depend on the RTO and RPO, only both the key elements of the RPO and RTO will be addressed in the Disaster Response Actions section in this document. As a part of assessing and assigning the appropriate RPO and RTO, a Business Impact Analysis will be conducted based on the business impact too, as aforementioned.

However, the actual RPO, RTO, WRT, MTD and resume of normal operations will be recorded in the Disaster Log as part of the documentations for an actual or simulated disaster.

# List of Potentially Affected Vendors

As of 1 April 2019, the vendors who may be affected in the case of a disaster include the following:

* Fantasma Web Services

# Vital Documents

## Disaster Recovery Event Recording Form

[Disaster Log for SCP](https://drive.google.com/a/smu.edu.sg/open?id=18Y7SEbKjh0AQzuJe5aDhI9WzQhGfvOUAZCB7lvUkIG4)

## Risk Management

There are many potential 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 business disruption which could arise from each type of disaster.

[Refer here for our risk management for disaster](https://docs.google.com/document/d/1h-C6a4NbqMNK1USP-VG5You4Wk1ooi1Jw6p7E5zowUQ/edit)

# Disaster Recovery Team

When an incident occurs the DRT must be activated. The DRT will then try to troubleshoot the incident while waiting for instructions from the Business Recovery Team (BRT) to decide the extent to which the DRP must be invoked. The BRT consists of senior representatives from the main business departments.

The DRT's responsibilities include:

1. Respond immediately to a potential disaster
2. Assess the extent of the disaster and its impact on the business and application
3. Maintain vital services and return to normal operation;
4. Ensure employees are notified and allocate responsibilities and activities as required
5. Restore key service as per business requirements
6. Recover application as usual after the incident as per business requirements

# Roles and Responsibilities

IT Operations Manager & Quality Assurance

IT Operations Manager & Quality Assurance are the owners of the Disaster Management process. They are responsible for all aspects of its coordination.

The role includes responsibility for:

* Acting as the liaison with personnel responsible for Disaster resolution
* Form a disaster recovery team (DRT) to resolve disaster
* Ensuring Disasters are resolved
* Ownership and management of the Known Error Record
* Coordinating major review of disasters

Support Manager, Tier 1 - Communication, Tier 2 - Business Analyst, Tier 3 - Dev and Infrastructure & Security

Solving disasters may be handled by internal technical support team members. When disasters occur, the IT Operations Manager & Quality Assurance may formulate a DRT that is made up of resources with specific expertise.

# Disaster Recovery Education

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise, everyone who participates will learn from these exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that DRT are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens

Data backup

In preparation of a disaster, ensure that the employees are aware of where to store their files and documents so as to make sure that all files are included in the backup. In order to avoid corruption of data and/or data loss, anti-virus installations and education on how viruses are spread are also essential.

Disaster Recovery Actions

In preparation of a disaster, ensure that the employees are also clear about who to contact in an emergency and actions they can carry out to maintain the business’ productivity even during the recovery period. If a 3rd party service is used, ensure that there is a personnel assigned in the company, with the role of contacting the service in order to facilitate the recovery efforts. With regards to the contact information, ensure that it is also stored off-site to counter the possibility of a fire, flood or other event leading to a loss in contact information data.

# Disaster Response Actions for SCP

Depending on the extent of the disaster, the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) will also be adjusted according to the instructions from the business heads.

In the case whereby the disaster has caused an SCP termination, corrupted SCP configuration files and/or corrupted documentations, the steps relating to the respective disasters will then be carried out to attempt to achieve restoration and maintain communication with the key appointment holders.

## Disasters relating to SCP Termination

|  |  |
| --- | --- |
| **Current Version** | **Backup Version** |
| **Build:** SCP 1.2.0  **Deployed ports:** 8000(default), 8001 and 8002 (gunicorn) | **Build:** SCP 1.2.0  **Deployed address:** <http://3.1.221.255:8000/> |

**Recovery Point Objective (RPO)**: 24 hours

**Recovery Time Objective (RTO)**: 2 hours

1. If the current version of SCP is inaccessible and DRT is unable to restart the instance in time, DRT shall re-assign the domain name of <https://esmscp.tk> to the backup’s address. The backup instance is continuously running.
2. The DRT will then continue their efforts to restart the instance and re-assign the domain name back to the current version.
3. Inform COO of disaster.

## Disasters relating to configuration files of SCP

|  |  |
| --- | --- |
| **Current Version** | **Backup Version** |
| Configuration files on server | Automated AMI Backups |

**Recovery Point Objective**: 24 hours

**Recovery Time Objective**: 2 hours

1. If the instance is not stopped, stop the instance
2. Detach current volume
3. Attach latest working AMI as current volume
4. Restart instance
5. Test that the application is working correctly, else repeat step 1

## Disasters relating to documentation

|  |  |
| --- | --- |
| **Current Version** | **Backup Version** |
| [Github Url to access official documentations](https://github.com/delinhquentz/G5T7-SCP) | [Google Docs Url to access backup documentations](https://drive.google.com/drive/u/1/folders/1ll3WJqvWTUZYGJLE2-1zEUW0yM-l5d32) |

**Recovery Point Objective**: 24 hours

**Recovery Time Objective**: 2 hours

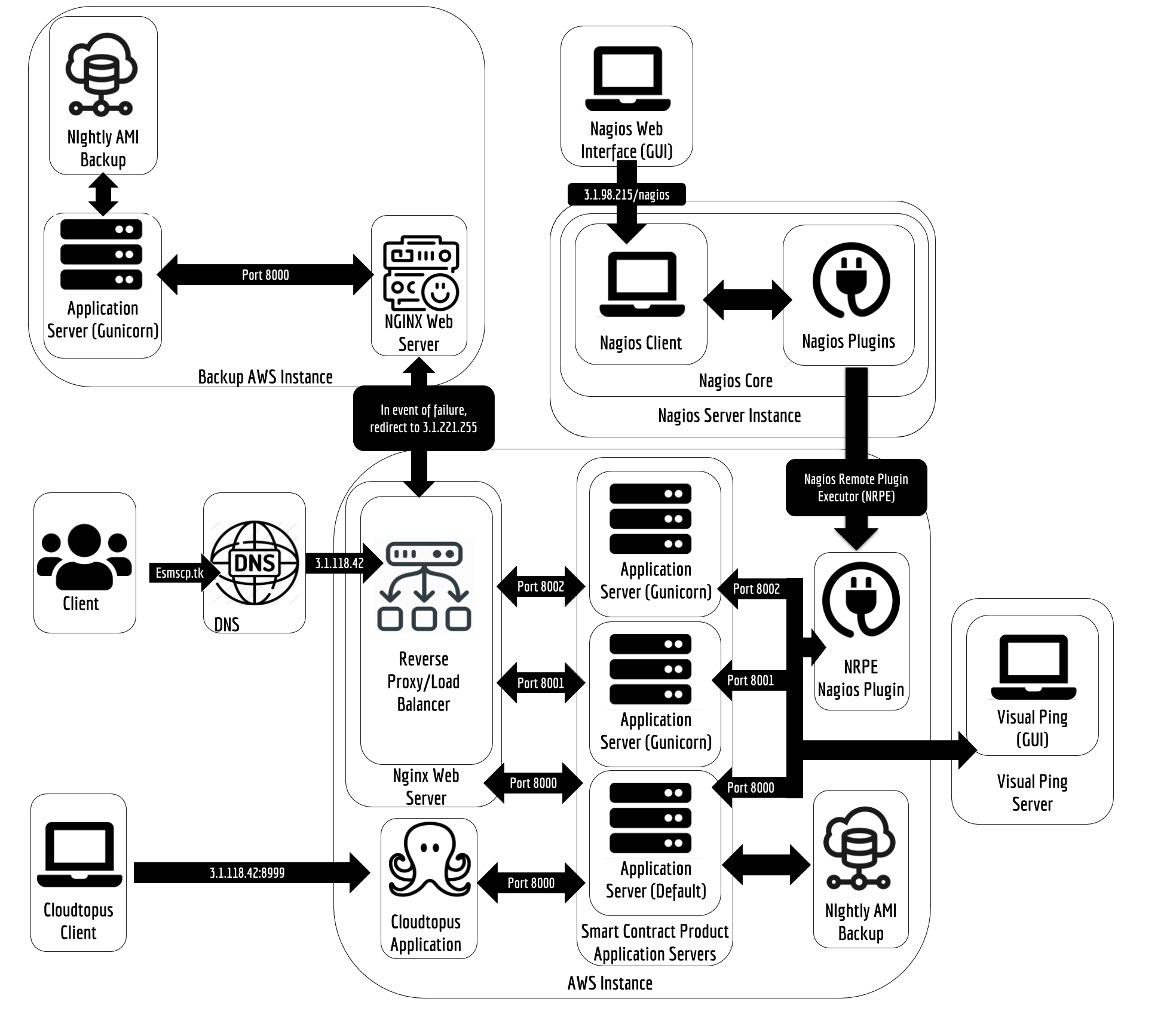
1. If documentations on Github Url are missing, check if there is a latest version of the respective documentations on Google Docs.
2. If so, download and push to git.

## Disasters relating to External Triggers e.g. Flooding

The affected entities of the disaster will be determined and documented, including details of the following:

* What disaster occurred
* Effect of the disaster on
  + People
  + Infrastructure
  + Applications
  + Data
* Entity affected by disaster corresponding to the effects of the disaster

# IT Network Architecture Diagram



# Recovery Sites

DRP Documentation Storage

Copies of all documentations will be stored on the team’s github and google drive folder. Each member of the Disaster Recovery Team will be issued a copy of this plan.

Backup Strategy

Documentations and SCP’s configuration files are backed up. The team has implemented an Automated AMI backup which backs up the configuration files of SCP and is utilizing a warm standby. Using a warm standby will help the team to reduce switching time between the live site and the backup site.

# Disaster Recovery Plan Review

In conjunction with maintaining the DRP, a review of the DRP will be conducted at regular intervals with the following goals:

* Assess how effective the DRP is in an actual and simulated disaster scenario
* Documenting potential changes after assessing the effectiveness
* Documenting actual changes to the DRP

Initial testing of the DRP will be conducted in phases on Sundays and after normal business hours to minimize disruption to the service. A combination of the checklist test and the structured walk-through test is suggested for initial testing before attempting more extensive testing.

Subsequent testing of the DRP will then be conducted during normal business hours, after determining the modifications to the plan.

## Testing Frequency

For new Disaster Recovery Plans, a quarterly or semi-annual test is recommended for the first year. After this initial period, semi-annual or annual tests should be required as per the [Technology Risk Management Guidelines (TRMG) by the Monetary Authority of Singapore (MAS)](http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf).

## Types of Testing

Structured Walkthrough Testing

Disaster Recovery Team members meet to verbally walk through the specific steps of each component of the disaster recovery process as documented in the disaster recovery plan. The purpose of the structured walk-through test is to confirm the effectiveness of the plan and to identify gaps, bottlenecks or other weaknesses in the plan.

Checklist Testing

This test determines if sufficient supplies are stored at the backup site, contact details are updated and necessary documentations are adequate and available. The DRT reviews the DRP and identifies key components that should be current and available. The checklist test ensures that the organization complies with the requirements of the disaster recovery plan, as preparation for a disaster.

Simulation Testing

During this test, the organization simulates a disaster so normal operations will not be interrupted. Testing can include the notification procedures, temporary operating procedures, and backup and recovery operations. A disaster scenario should take into consideration the purpose of the test, objectives, type of test, timing, scheduling, duration, test participants, assignments, constraints, assumptions, and test steps. [*(Refer to the Disaster Scenario Simulation Template)*](https://docs.google.com/document/d/1N_vZmH62OIw4XVT6DXJGrF9nKHTrxieV6SelFXBJqdg/edit?usp=sharing)

Parallel Testing

Under this test, historical transactions are processed against the preceding day’s backup files, which involves the Automated AMI backup that backs up the configuration files of SCP. All reports produced in the Automated AMI backup for the current business date should agree with those reports produced at the existing processing site.

Full Interruption Testing

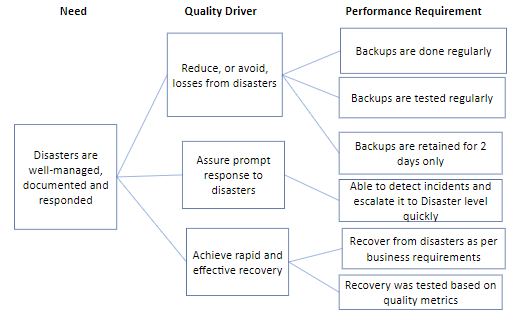
This test activates the entire disaster recovery plan, meaning it will be costly to conduct and could disrupt normal operations. Therefore, it should be approached with caution.

Adequate time must be scheduled for the testing and the duration of the test should be predetermined to measure adequate response time. Additionally, it is advised that this test should not be scheduled at critical points in the normal business processing cycle.

## Assessing Test Effectiveness

In order to verify the effectiveness of the test(s) conducted, the following CTQs and KPIs are to be considered, as per ITIL guidelines.

Critical-to-Quality (CTQs) & Key Performance Indicators (KPIs)



## Plan Updating

It is necessary for the Disaster Recovery Plan (DRP) updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Operations Manager & Quality Assurance.

# Post-Review Standard of Procedures

To wrap up the reconstitution and recovery process of the Disaster Recovery process, the following points have to be ensured:

* No threats have remained unaddressed
* No remaining after effects of the disaster
* All team members have returned to their original roles
* All resources deployed for the recovery have been relocated to where they are needed
* The disaster recovery efforts are completely over
* Lessons learnt that could lead to improvements are recorded

Addressing the part on documenting the lessons learned as a result of the disaster, so as to guide the business in making the appropriate improvements, the following steps would be taken as well:

1. Analyze the cause and source of disaster.
   1. Commision an investigation team
   2. Collection of data and interviews with all affected staff
   3. Analyze insights using RCA methods
2. Formulate procedures to prevent some or all aspects of a similar disaster occurrence
   1. Include RACI matrix, assign responsibilities to roles
3. Implement procedures and document disaster for archiving purposes.
4. Conduct a post-action review to evaluate all member’s actions during the disaster
   1. Purpose is to identify loopholes and areas of improvement to increase efficiency of future disaster management, **not** for blaming.
   2. Reassign roles/tasks accordingly as per evaluation