



Disaster Recovery (DR)
Capability Statement for
Clients – APAC



Confidentiality Statement

This document and any links or attachments may contain copyright material of SAI Global and/or information that is confidential and subject to privilege. If you are not the intended recipient of this document, please contact SAI Global immediately. In this case, you must not read, print, disseminate, copy, store or act in reliance on this document or any of the accompanying attachments; and you must destroy all copies of this document. This notice should not be removed.

Table of Contents

Confidentiality Statement.....	2
Table of Contents.....	3
SAI Global Disaster Recovery Capability	4
Summary	4
Technical Solution Overview.....	4
Documentation	4
DR Testing Overview	4

SAI Global Disaster Recovery Capability

Summary

The SAI Global (SAIG) Disaster Recovery Plan (DRP) for the Asia Pacific Operations allows continued provision of services to its client base if its Production IT&T environment is compromised by a disaster. The DRP covers critical customer and corporate systems across all SAIG operations (i.e. Property Services, Information Services, Compliance, and Assurance).

SAIG has selected a hot-site DR strategy that contains dedicated infrastructure and network connectivity for the recovery of critical IT applications and services. The selected strategy will allow the recovery of these applications and services for the continuation of business operations within the tolerances identified by the business stakeholders.

Technical Solution Overview

The disaster recovery strategy is based on the replication of the production application data, database and server images to the DR environment. SAIG IT&T have selected Terremark's Miami data centre as the site for the DR Hosting Centre for our Americas regional operations, and Terremark's Amsterdam data centre as the site for the DR Hosting Centre for our EMEA regional operations. The DR solution is based on Terremark's Disaster Recovery as a Service (DRaaS) Virtual Disaster Recovery (VDR) solution. This provides for the replication of in scope data, applications and server configurations to a dedicated SAIG DR environment via Terremark's host based replication software. If a disaster is declared Terremark and SAIG will activate the VDR environment and redirect the business network to the Terremark Miami data centre.

Documentation

The DR environment and network infrastructure are supported by a detailed documented Disaster Recovery Plan (DRP). The documentation includes a:

- Management DRP which is the framework for the recovery;
- Corporate IT&T Recovery Manual for infrastructure recovery; and
- Business Unit Recovery manuals, containing specific business application recovery and verification procedures.

DR Testing Overview

The SAIG comprehensive DR test and maintenance program ensures that the DRP and associated recovery processes are tested regularly.

The selected DR service allows SAIG to perform testing that is non disruptive, does not have any impact on the Production environment and does not require any Production outage.

The DR test process is similar to the “real” recovery process but the integrity of the DR environment is maintained and not impacted during the DR test. The facilitation of the activation of the DR test environment is the same as an actual DR activation but instead of disabling the Production environment and starting the DR environment as “Production” the DR test is performed in an isolated test environment. At the completion of the DR test any changes to the DR environment are discarded and the environment is reverted to standby mode.

SAIG does not perform DR testing that exposes Production operations to unnecessary risk. This includes the live failover of the Production environment to the DR environment, to perform testing. The selected strategy and solution is not based on high availability and has not been designed for switching individual or all applications between sites other than in an actual live DR scenario. The DRP and underlying strategy is for a full site recovery and if invoked, will then result in all SAIG Production operations switching over to the DR site. The selected DR test strategy will adequately test the DR infrastructure, applications and services without exposing critical internal and client services to unnecessary system interruptions or outages. To maintain integrity of Production data, testing of interfaces to external organisations are not performed during DR tests and the DR application environment is not open to the Production network.

All DR test activity is planned, measured and recorded to ensure transparency of process and continuous improvements are identified to streamline processes for the best possible outcome to SAIG and its clients.