STC Cloud Services

Business Continuity & Disaster Recovery Brief

Version: 1.0

Date: 21/02/2019

TABLE OF CONTENTS

1. Business Continuity Introduction

The purpose of every business continuity & disaster recovery plan is to minimize the impact of any predictable or unpredictable interruption event on business processes. Business continuity and resiliency services help businesses avoid, prepare for, and recover from a disruption.

This document will provide a brief overview of practices undertaken by STC Cloud to maintain its business continuity, and controls regarding disaster recovery.

2. Cloud Deployment Models

The main differences between cloud service categories relate to how BC/DR control is shared between STC and Customer, which in turn affects the level of responsibility for both parties. It should be noted that, other than in a self-managed private cloud scenario, the Customer rarely has any control over hardware, and it is the degree to which virtual components, applications and software are managed by the different parties that differentiates the cloud service categories. As a general rule, SaaS provides Customers with the least amount of control, whereas IaaS offers the most control for the Customer.

BC DR Responsibility	Cloud Service Models		
	IaaS	PaaS	SaaS
Data – Volumes, Files, Databases	Customer	Customer	Customer
Application	Customer	Customer	STC Cloud
Platform – Operating System, Virtual DC	Customer	STC Cloud	STC Cloud
Infrastructure – Hypervisor, Cloud Dashboard	STC Cloud	STC Cloud	STC Cloud
Physical Infrastructure – DC, Connectivity, Hardware	STC Cloud	STC Cloud	STC Cloud

Figure 1: Indicative BC/DR Responsibility based on Cloud Deployment Models

In all deployment models, and particularly in public cloud environments, it is important for all parties to understand the specific elements of the cloud service model used and its associated risks. Any cloud deployment model that is not fully self-managed is by nature a shared responsibility model, where a portion of responsibility for the cloud service falls under the realm of STC Cloud and a portion of responsibility also falls to each Customer. The level of responsibility that comes on STC or the Customer is determined by the cloud service category being utilized, for example, IaaS, PaaS or SaaS.

STC wants to work with their Customers to understand their business continuity and compliance needs. As Cloud BC/DR is a shared responsibility, STC wishes to maintain open communication to avoid any misunderstandings or gaps in responsibilities.

3. Business Continuity Considerations

3.1. BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING

STC Cloud analyzed its critical infrastructure and essential system components and designed measures to avoid and lessen disruptions and outages. These measures include creating plans, processes and policies to support the recovery of systems, what steps to take before, during and after a disruption or outage. These plans include business & operational strategies, which are tested and corrected over a period of time, so that possible disruption scenarios and events are incorporated. Regular testing is also conducted to verify the failover of power, utilities, systems and networks.

STC Cloud have internal processes to manage incidents, disruptions and events to people or infrastructure. 24/7 monitoring and alerting mechanisms, and cross-skilled teams are present to respond to any anomalies. Data recovery strategies are designed, and tested to counter different levels of data loss – component level, server level, or complete data center level. Backup of customer workloads are not taken, unless they are part of additional data backup services.

STC Cloud regularly assesses its cloud DCs and infrastructure for availability risk and single point of failure identification. Threats, vulnerabilities and risks are identified, rated and mitigated to meet the accepted level of risk, to fulfill service availability obligations. Ongoing assessment and mitigation of potential vulnerabilities is also performed, along with enterprise-level risk assessment to identify and manage risks to business services as a whole. This process considers risk via processes, new technology, business rules, or human mistakes, regional regulatory and environmental risks into consideration.

3.2. DATA CENTERS

STC Cloud Datacentres are specifically designed to withstand faults, while maintaining availability of adequate power, cooling and utilities. There are multiple power sources to the DCs, and active power lines from different power stations. DCs are also equipped with backup power to operate in sufficient capacity, via UPS and redundant generators, in case an incident or power outage. Automated fail-overs are deployed to ensure redundant resources are taking over the load, until the primary resources are back online.

Climate control manages heat and maintains optimum operating temperature for devices, servers and other hardware, which reduces the chances of hardware outages. Humidity levels are also maintained to prevent static buildup within the DC. Entire DC area, and staging facility is protected by fire detection & suppressions systems, which include appropriately placed fire extinguishers, automatic release systems, multiple sensors such as smoke, water, and heat sensors.

All these sensors and DC systems are continuously monitored, so that issues are immediately identified. Appropriate preventive maintenance is designed as per equipment guidelines, to maintain the performance and reliability of the equipment. Preventive maintenance, along with timely detection of issues (corrective maintenance) allows STC Cloud DCs to monitor and operate their DC equipment as per service availability requirements.

3.3. NETWORK & CONNECTIVITY

Internet backbone is provided via redundant STC links, and all internal connectivity is an High-Availability design, which results in each network component (device power, port, cable) being redundant and having automatic fail-overs to ensure seamless connectivity for the cloud infrastructure.

3.4. CLOUD INFRASTRUCTURE

STC Cloud infrastructure maintains redundancy in its design and has clustering between its multiple cloud controllers, and network bonding between them, operating in High-Availability mode, to ensure network and data are both resilient to device failures. STC has identified critical cloud components needed to deliver promised SLAs to customers, and apply appropriate BC/DR practices for them. System backups are taken across multiple, isolated locations to recover cloud services in case an incident or outage happens. STC Cloud has also maintains its hypervisors on availability zones, which allows customers to choose and design resilient system infrastructure for their high availability & demanding applications.

3.5. MONITORING PERFORMANCE & CAPACITY

STC Cloud continuously monitors its infrastructure and their performance, to ensure each asset supports the cloud services' availability requirements. Benchmarks are established, beyond which alerts are generated to add more resources or replace certain assets, in case of performance degradation. Capacity plans are formed and revised, based on usage trends and customer demands. These plans are put in force, when certain benchmarks are reached, so that customer requirements are fulfilled, and service availability is not hampered.

3.6. AUDIT & CERTIFICATIONS

STC Cloud DCs are designed, built, operated and certified in-line with international Uptime specifications. STC Cloud has undergone various independent audits to ensure it has implemented appropriate information security controls and mitigated its business & IT risks. STC currently manages ISO 27001, ISO 27017, CSA STAR and PCIDSS compliances, along with regulatory requirements such as CITC's CCRF and local cyber security mandates.

4. Customer Responsibilities & Guidelines

In addition to the business and risk considerations, the implementation of BC/DR controls in a cloud environment requires specialized technical knowledge and skills. It is therefore crucial that, prior to migrating business operations into a cloud environment, the Customer engage its technical, legal, due diligence, information security and compliance teams to work together to define its needs and evaluate potential cloud service offerings against those needs. Clear policies and procedures should be agreed between Customer and Cloud Provider for business continuity requirements. Responsibilities for operation, management and reporting should be clearly defined and understood for each requirement and acknowledged, in writing, in contractual agreements.

4.1. SERVICE PROVIDER EVALUATION

Below steps can be followed by customers looking to migrate/evaluate our cloud services:

- UNDERSTAND your risk and business continuity requirements first.
- CHOOSE a deployment model that aligns with your and your industry's business requirements.
- EVALUATE different service options.
- KNOW what you want from your Cloud Provider.
- REQUEST written assurances that controls will be in place, and periodic verification (e.g. certifications, accreditations) that controls continue to be maintained.
- REVIEW service and written agreements periodically.

4.2. GUIDELINES TO MANAGE BC/DR IN STC CLOUD

Customers are always in control and responsible for their data and workloads. Following are guidelines for Customers to organize their workloads, and plan their business continuity:

- Identify critical data, applications, systems, and take regular backups.
- Monitor their infrastructure, ensure their capacity management plan and apply the required security controls for their services.
- Maintain redundancy by deploying workloads on different zones or across multiple cloud nodes (DCs) or more than one site of cloud service.
- Apply Security Groups, limit access based on business needs, to prevent unauthorized access to VMs.
- Make use of additional STC Cloud services like BKaaS, Object Storage, DRaaS or other tools & services.
- Conduct a BCP assessment and failover testing for their infrastructure & services.
- Implement BC/DR best practices for people, process, and the virtual infrastructure
- Cloud customer's business continuity and disaster recovery plans should include scenarios for loss of the cloud provider's services.
- Determine who to contact if an incident occurs, or other events that require investigation, identification, notification, reaction, or any legal actions.