Business Continuity

Introduction

With over twenty years experience in designing and delivering robust cloud based software solutions to UK businesses, we've learnt that service-interrupting events can occur at any time. That's why we work hard to ensure we deliver consistent performance so that your business can continue without disruption.

This paper outlines the systems of prevention and recovery that we apply to Quill's suite of cloud software products and services.

Infrastructure

To ensure **fast, scalable and consistent** performance, Quill's core server infrastructure is built on Google Cloud Platform (GCP) **London UK region**, which is divided into three isolated zones each with independent power, cooling, networking and control planes - effectively three data centres in one - with Quill's servers distributed across these zones.

Power, cooling and fire prevention

Redundant power systems, diesel engine backup generators, cooling systems, fire detection and suppression equipment, and remote monitoring are all employed to keep things running **24x7** and ensure uninterrupted services.

Connectivity

As **Premium Tier** clients, our services are delivered over GCP's well-provisioned, low latency, highly reliable network: with at least three independent paths between any two locations on the network to ensure that traffic flows even in the event of a disruption.

Resilience and scalability

Quill's server resources are load balanced across three zones to provide a **highly available** service and we can quickly **scale up** when demand increases to prevent any degradation in performance to existing customers.

Transparent maintenance

Live migration ensures there is no disruption to Quill's systems when GCP scheduled maintenance work occurs, such as: firmware or operating system upgrades, hardware replacements, network or power grid maintenance etc. This is automatic and transparent.

DDoS protection and mitigation

Our software and network architecture is designed with best practices in mind such as: proxy based load balancing; API rate limiting; and the ability to quickly scale up. This, in addition to other GCP features, ensures our architecture is as resilient to Distributed Denial of Service attacks as possible.

Sustainability

At Quill, we strive to reduce our environmental impact and choose Suppliers that support that ethos. GCP is committed to **carbon neutral** operations and purchases enough renewable energy to match or exceed consumption for all of its operations globally.

Uptime and monitoring

Quill targets an overall Service Level Objective uptime of 99.5% in any given month, subject to proper operation of the customer's IT environment, save in cases of planned maintenance or force majeure events.

We use a combination of monitoring methods including: **real time metrics** that show us the current health of our services; **automated alerts** when certain thresholds are exceeded; and **historic analysis** to identify trends or unusual activity.

Please note that we reserve the right to schedule planned "maintenance windows" from time to time (outside of normal working hours) to perform routine checks or updates. We notify our customers in advance of any planned maintenance windows, specifying start/end times.

Disaster recovery (DR)

The multi-regional and multi-zonal nature of our GCP infrastructure forms the core of our DR planning.

Regions & Zones

We will always default to the GCP **London UK region** except in extreme circumstances where we may utilise an alternative region e.g. within the EEA.

Recovery Point Objectives (RPO)

Data backups are taken hourly, daily (overnight) and, in the case of Interactive Accounts, prior to month-end completion. All backups are stored **cross-regionally** (within EEA) and **multi-versioned** using **encryption-at-rest** throughout.

Recovery Time Objectives (RTO) for critical outages

We target a best endeavours RTO of four (4) consecutive working hours to resolve critical outages, from the point where our monitoring mechanisms detect the issue; save for where the outage is planned maintenance, force majeure, or any other exceptions as detailed in your service agreement.

For the purpose of this document, we are defining a “critical outage” as an extreme disruption incident affecting all Quill customers across multiple services.

Our UK based Support team handles other more general issues or those affecting specific users that are reported directly by customers. The team can be contacted by email: support@quill.co.uk or by phone: 0161 236 2910 (option 1) during normal working hours.

Your RPO and RTO

When calculating your own RPO/RTO numbers for your business, please consider all suppliers that your operation depends on, such as telecoms & internet providers, IT equipment support providers, banking IT systems, third party case or document management systems etc., in addition to Quill’s services.

Security

Please see our sister “Spotlight on Security” document for further details.

Changes to this document

Quill’s Business Continuity and Security strategies are dynamic and evolving processes undergoing constant scrutiny and evaluation and are therefore subject to change without notice.