IT SERVICE MANAGEMENT FAQ

Version: 1.3
Date: February 2011

Table of Contents

1.0 Introduction

Class Super (Class) provides a managed service via hosted hardware and software. In the Information Technology industry this is known as the Software as a Service (SaaS) delivery model.

Our clients trust us with their valuable and confidential data, and therefore it is natural for questions to be asked about its stewardship as well as the measures taken to ensure system availability.

At Class we strive to be open about our IT policies and facilities. This document has therefore been created to outline the basic IT policies and procedures that relate to these matters.

2.0 Data Stewardship

2.1 Where is the data stored?

The entire production system is run at our hosting location provided by a specialist hosting service provider, Macquarie Telecom. We use their internet connectivity, rack space and power. The system is run on equipment owned by Class. The data is stored in storage devices within the equipment owned and operated by Class.

In addition to this, data is located at two backup locations under the direct control of Class (see section 2.4 for additional detail.)

Macquarie Telecom's certifications and standards provide the highest level of surety that Class' data storage is only accessible to authorised staff.

2.2 Who controls the data?

The data is controlled entirely by Class. If for any reason Class requires other parties to handle data (e.g. such as contractors and specialists) then appropriate reciprocal arrangements (such as Non Disclosure Agreements) are put in place to safeguard the data. Access to the data is only granted on an as required basis; the hosting organisation does not have access to the data. Even physical access is limited as Class' racks are located in locked cages.

2.2 Who owns the data?

The SMSF administrator owns the data even though it is held on Class' servers.

2.3 What if I want to take my data and leave?

Class provides users with full access to all of their fund and accounting data. Class allows users to export all their fund and report data in an XML format readable by Excel, web browsers and many other tools.

2.4 Data backup

Class has a replica of the production hardware located at the hosting location (this is outlined in greater detail in the System Availability section below). An automatic data replication service duplicates the production data on to the alternative "warm standby" system every fifteen minutes.

The automatic data replication service also sends a data backup to a Data Recovery location in an Australian CBD data-centre in another state.

In addition to all these provisions, a manual off-site backup occurs daily and is stored at Class' offices. This storage device is then rotated to a further off-site location.

2.5 Data corruption

It goes without saying that Class implements very stringent coding and testing practices that ensure that the system will not corrupt data. In particular, Class has individual development, testing and acceptance testing environments, through which releases undergo a rigorous testing regimen.

However, Class also implements a Point-In-Time snapshot log replay system. The snapshots are taken daily and log files are produced every 15-minutes. The snapshots and log files are then retained for an entire fortnight. Historic daily snap-shots are retained for 3 months.

3.0 System Availability

3.1 Network connectivity

Our hosting partner, Macquarie Telecom, is a highly regarded hosting provider that provides a managed network service. Whilst 100% availability is not technically achievable due primarily to the requirement for periodic scheduled maintenance, numerous mechanisms are in place to achieve high network availability. For instance, scheduled maintenance is carried out during non-peak periods.

No production services are located at Class' offices, and therefore production services are unaffected if Class' own internet connection were to fail.

3.2 Monitoring

Macquarie Telecom monitors the availability of their services, namely power and network access. Class monitors all other aspects of system availability directly via an active monitoring system with alerts used to trigger a response when a parameter being monitored does not reside within general operational limits.

Class' monitoring system is located within Class' offices, and therefore it accesses the production system remotely. If network connectivity fails then the monitoring system will detect this outage.

The monitoring system monitors a number of key parameters from basic equipment health and capacity metrics (CPU, I/O, disk space, network) up through the application stack to the operation of system sub-components and ultimately the availability of the external system to the user base.

Security and audit monitoring is also implemented and facilitates the security measures described below.

3.3 What happens if… Hardware failure & recovery

The most basic level of protection against hardware failure is implemented by the use of RAID redundancy for the key storage drives. In particular, the ZFS RAID-Z2 dual-parity system is used that can recover from multiple drive failure.

The second level of protection is the availability of a "warm standby' replica of the hardware (also located at Macquarie Telecom.) If a more substantial hardware failure occurs, then the operation of the entire system can be moved to this replica (named the "secondary leg".)

3.4 What happens if… Site failure / DRP / BCP

Class maintains an entire off-site replica of the Class System on Brennan IT's Infrastructure as a Service (IaaS) platform. This replica is hosted in their Primary Data Centre, and is kept up-to-date using data updates shipped at a maximum interval of 15-minutes (during business hours.) This system addresses Class' RPO (Response Point Objective,) and leverages Brennan's extensive hardware redundancy.

3.5 Total Cost of Ownership (TCO)

Class' technology value proposition is based heavily on its Infrastructure as a Service (IaaS) underpinnings. Attempting to replicate the level of security, scalability and access that Class' infrastructure provides would require the need to implement and maintain the following components and services:

- Server & redundant hardware, communications and power – including ongoing upgrades
- High frequency backups – stored offsite
- Security – Firewalls, Penetration Testing, Patch & Software updates, Incident Response
- Disaster recovery planning
- Monitoring & Experienced IT team

This level of infrastructure for a typical accounting practice running a traditional SMSF administration application would cost in the order of $60k per annum based on market prices current as at February 2011.

4.0 System security

4.1 Privacy and access control

Class' entire system is based on the concept of access on a need-to-know basis only. This is coupled with the use of privileges based on individual credentials. These are mapped in a highly granular fashion to ensure an individual user has access to only the data that they are entitled to view and modify. Clients are entirely partitioned off from each-other.

Physical access to the data storage devices is similarly restricted to an as-required basis.

The "access on a need-to-know basis" principle is also applied to Class staff.

4.2 Intrusion protection – cyber-crime and hacking

The term Intrusion in this context applies to Systems and the Communications Channels that connect users to those systems.

As well as the access control mechanisms described above, a number of other measures are implemented to prevent intrusion:

- Firewalls – limit access to required protocols only
- Proactive patch and update installation for key security related components
- Use of Anti-Virus software

All connections containing private session data are protected using a 128-bit encrypted channel. The protocols used also confirm the servers' identities though the use of site certificates.

4.3 Layered architecture

The use of a layered architecture (with a clear separation of User Interface, Business Logic and Data Access code) protects against most opportunistic intrusion techniques such as SQL injection. Appropriate validation is also used to guard against such attacks.

4.4 Penetration testing

Whilst Class has implemented many architectural and operational measures to prevent security breaches, it is best practice to conduct Penetration Tests to verify the efficacy of those measures empirically.

As such, Class ensures Penetration Tests are conducted on a regular basis.