CAS360

Cloud ASIC corporate compliance solution

CAS 360 SECURITY WHITE PAPER

bgl.

www.bglcorp.com

1. Overview of BGL's Web Applications

BGL Corporate Solutions Pty Ltd (BGL) is a privately owned Australian company and Australia's leading developer of self-managed super fund (SMSF) administration and corporate compliance software solutions.

BGL's cloud solutions include CAS 360, the next generation cloud corporate compliance software solution, and Simple Fund 360, Australia's leading cloud SMSF administration software solution.

BGL software solutions are used to administer over 70 percent of SMSFs. CAS, the world's leading corporate compliance software solution, is used in over 45 percent of Australian companies.

CAS 360 has changed the way ASIC corporate compliance work is done in Australia. CAS 360 automatically downloads Annual Company Statements and Company Debt reports from ASIC each day. The Annual Review process compares ASIC and CAS 360 data automatically and then prepares the Annual Reviews for clients. Debt is managed and deadlines for lodgement of documents is all controlled through smart alerts.

Simple Fund 360 has revolutionised the SMSF administration space, with intelligent algorithms that significantly reduce the amount of time required to process an SMSF. Simple Fund 360 is the complete SMSF compliance solution that automatically matches bank, broker, corporate action and dividend data overnight using BGL's SmartPost technology, while Australian Securities Exchange's (ASX's) managed funds and international share prices provide daily portfolio valuations.

BGL has been providing software solutions to accountants, SMSF administrators, lawyers, financial planners and professional firms for over 25 years. The economies of scale that BGL's services offer, together with our cloud hosting provider Amazon Web Services™ (AWS), make it possible for BGL to provide higher levels of physical and digital security than many of our clients have on their own systems.

2. Data Security

BGL's infrastructure and online software security is regularly reviewed by external security specialists. These highly trained security specialists run penetration tests to systematically identify and exploit security flaws within the CAS 360 web application as per the Application Security Verification Standard 2.0 Open Web Application Security Project (OWASP). OWASP is a worldwide notforprofit charitable organisation focused on improving the security of software.

In addition to running regular external tests, CAS 360 servers run the latest UNIX based operating system firewall and perimeter based security policies protected against unauthorised service access. Daily logging and monitoring of requests are performed to ensure that the connected internal clients are the authorised hosts.

3. Data Backup Controls

CAS 360 has been designed to support missioncritical databases. Databases are replicated across multiple servers and across multiple availability zones.

Complete backups of data occur every hour together with nightly backups to storage solutions that deliver highly scalable, durable, and reliable cloud storage for backup.

4. Security Standards are used

BGL's CAS 360 application is signed by an SSL certificate meaning all data transferred between BGL and your Internet Browser is encrypted.

The CAS 360 SSL connections utilise the latest perfect Forward Secrecy. This security feature uses a derived session key to provide additional safeguards against the eavesdropping on encrypted data.

This prevents the decoding of captured data, even if the secret longterm key is compromised. The load balancer utilise the latest Elliptic Curve Cryptography (ECDHE) cipher suites. Most major browsers now support these newer and more secure cipher suites. BGL encourage clients to use up to date browsers to make use use these stronger cipher suites for communication.

Access is username and password protected and passwords resets are emailed to the user's email address. Users can only access information that they have permission to view. Access in CAS 360 is rolebased meaning that the Practice Administrator has complete control who can access your information. All Users have an audit trail which is logged including IP Address.

Sensitive fields in databases are encrypted at rest. (more information in section **11. Encryption of Data**)

5. Hosting

All 360 data is currently stored in Australia using multiple AZs

5.1 BGL uses world class Hosted Data Centres

BGL's chosen Data Centre is located in Australia and isolated from BGL's own internal office networks. Only strictly controlled BGL staff with authorisation can remotely access the servers which house the data. BGL regularly review access control and when an employee no longer has a business need for these privileges, his or her access is immediately revoked.

BGL uses AWS's worldclass, highly secure data centers utilizing stateofthe art electronic surveillance and multifactor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis.

5.2 Storage Device Decommissioning

When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The chosen data centre uses the techniques detailed in DoD 5220.22M ("National Industrial Security Program Operating Manual ") or NIST 80088 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry standard practices.

5.3 Security Controls

The Data Centre built on an environment with extensive and validated security and controls, including:

- Service Organization Controls 1 (SOC 1) Type 2 report (formerly SAS 7011 Type II report), with periodic independent audits to confirm security features and controls that safeguard customer data.
- ISO 270001 Certification, an internationallyrecognized security management standard that specifies leading practices and comprehensive security controls following the ISO 27002 best practice guidelines.
- PCI DSS12 Level 1 compliance, an independent validation of the platform for the secure use of processing, transmitting, and storing credit card data.
- Relevant government agency and public sector compliance qualifications, such as an ITAR compliant environment.

5.4 Service Availability

Whilst BGL intends that the Software will be available 24 hours a day, seven days a week, 365 days a year, it is possible that on occasions the Software may be unavailable for reasons within the control of BGL (ie: for scheduled or unscheduled Software updates) or for reasons outside the control of BGL (ie: the data centres have power outages and all backup generators fail). BGL will use reasonable endeavours to notify you in advance of any planned outages and will notify you as soon as possible of any unplanned outages.
BGL will use commercially reasonable efforts to make the Software available with an uptime percentage of at least 99.9%.

BGL Service Status page can be found here https://status.bgl360.com.au/

6. Privacy of data

BGL treats all data with utmost privacy.

BGL complies with the Privacy Amendment (Notifiable Data Breaches) Act 2017.
BGL has a documented Notifiable Data breach policy and Response Plan.
BGL's privacy policy can be found at http://www.bglcorp.com/about-bgl/privacy-policy

7. Monitoring

- Amazon services utilised to monitor server and database health.
- Third party software utilised for additional monitoring of servers of application
- Email and SMS alerts sent to relevant staff of any critical alerts

8. Data management lifecycle (creation, storage, retention, removal)

BGL retains customer data for 5 years after your subscription expires. You are able to delete your own data at any point before the 5 years expiration date.
Server Management is handled by Amazon Web Services.

When a storage device has reached the end of its useful life - **For more information please refer to 5.2**

9. Incident handling

Processes to identify incidents/breaches/vulnerabilities in AWS environment

- BGL utilise CloudTrail to monitor all API access to Amazon infrastructure. All CloudTrail logs are then pushed to CloudWatch and alert metrics are then created for multiple action events.
- 3 unauthorised attempts into the system will block the system and send notification
- Amazon SNS notifications are sent out for any authorised breaches for actions.

10. Encrypted connections between BGL and Amazon

- No infrastructure is located at BGL's offices. All infrastructure is hosted by AWS
- All access to AWS Production environment is limited to BGL's office and via VPN

11. Encryption of data

- BGL provides 256bit SSL encryption for user login and all subsequent data.
- Critical or identifiable fields such as TFN's are encrypted at rest using 256bit Advanced Encryption Standard
- To find out more about data encryption read Encrypting Data at Rest https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf
- Access to S3 and database is controlled by IAM policies http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
- Developers do not have access to production data.

12. Data Backup

- By setup, the RDS is doing Auto Backup once every 24 hours, operated by AWS.
- As a second backup plan, a manual RDS snapshot is taken every hour. So the shortest reversible pointintime is shorten to ONE HOUR

13. Disaster Recovery

All infrastructure is MultiAZ. Application spans across multiple Availability Zones. Redundant instances for each tier (e.g. web, application, and database) of an application are placed in distinct Availability Zones thereby creating a multisite solution. All persistent data is replicated to 2 places.

Disaster Scenario	Expected RTO (what will client handle)
AWS EC2 Failure in Single Availability Zone	Zero no impact
AWS EC2 Failure in Multiple Availability Zones	1 Hour

14. Cloud Subscription Agreement

BGL's cloud software subscription agreement can be found here
https://www.bglcorp.com/wp-content/uploads/2018/06/BGL-Cloud-Software-Subscription-Agreement18.pdf